

# Unit 6

## Router Management

### Overview

#### Description

With today's networks growing exponentially, management is a key to quality of network performance. People depend on their networks and performance issues can cause devastating problems for the user.

It is important to establish a benchmark, a baseline of performance for all the network's equipment, to use for comparison when monitoring a network. This benchmark allows the network manager to become familiar with the entire system so that he/she may

- Know the signs of potential problems.
- Prevent problems before they occur.
- Diagnose existing problems.
- Track network growth to plan for future network expansion.

This unit discusses the Simple Network Management Protocol, SNMP, used by network managers to monitor and manage networks, including detail discussions of the MIB (management information base), and events and traps.

#### Unit Table of Contents

This unit contains the following three lessons:

| Lessons  | Pages   | Length  |
|--|---------|---------|
| Lesson 6-1: Simple Network Management Protocol | 238-266 | 5 hours |
| Lesson 6-2: Management Information Base        | 267-292 | 5 hours |
| Lesson 6-3: Events and Traps                   | 293-314 | 5 hours |

---

## Lesson 6-1: Simple Network Management Protocol

### At a Glance



Beginning in the late 1970's, computer networks grew from small, easily managed networks to large, internetworks of thousands of computers spread across the world, using different operating systems. By the mid-1980's, it became apparent that there was a need for a management protocol.

Five areas of network management were defined by the ISO:

- **Fault management**—Deals with detecting failures in the network.
- **Configuration management**—Deals with configuring all the elements of a network.
- **Security management**—Deals with providing security for the network, for example, passwords.
- **Performance management**—Deals with the quality of service, e.g. usage levels by individual workstations.
- **Accounting management**—Deals with monitoring network resource usage, for example, printers.

The first network management protocol developed to address these management areas was the Simple Network Management Protocol, or simply SNMP. SNMP is a simple internetworking management protocol developed to collect performance and management information from devices on a network and to monitor their activity. It is part of the TCP/IP protocol suite and specifically uses the User Datagram Protocol, UDP.

### What You Will Learn

After completing this lesson, you will be able to do the following:

- Describe SNMP and its purpose in routing.
- Identify SNMP architecture and message formats.
- Configure a SNMP community name on the Nortel Networks ARN using Site Manager.
- Configure access rights for a community and assign managers (IP addresses) to that community.
- Recognize and correct an access problem on the ARN that is related to community access rights.

## Tech Talk



- **Agents**— Software that enables a device to respond to manager requests to view or update MIB data, and send traps reporting problems or significant events.
- **Benchmark**—A benchmark is a baseline of a network device's performance.
- **Community Name**—In SNMP, the community name is a password shared by the network management station and the agent.
- **Managed Objects** — An object holding network management information, characterized by an identifier, a value, implementation requirements, and valid operations.
- **Management Information Base**— A logical database made up of the configuration, status, and statistical information stored at a device.
- **Managers**—The software component on the network management station that issues requests to the agent.
- **Network Management Station**—The NMS is a workstation that can configure and monitor network devices, and receive network performance data.
- **Object Identifier**--A string of numbers derived from a global naming tree, used to identify an object.
- **Protocol Data Unit**—The PDU is the section of the SNMP message that contains information sent to and from the NMS and agent.
- **Trap**--A message that reports a problem or a significant event.
- **User Datagram Protocol**—UDP is a connectionless transport method used to transmit messages between the NMS and the agent. UDP is a standard member of the TCP/IP protocol suite.
- **Variable**— A variable is an individual instance of a managed object.

## SNMP Architecture

SNMP is used to gather standardized information about network device configuration and performance using the UDP protocol from the TCP/IP protocol suite. It operates independently on the network and because it uses UDP, a connectionless protocol, it does not require a two-way connection with network devices.

There are four main components to SNMP.

- The agent.
- The management information base (MIB).
- The community.
- The network management station.

### Network Management Station

The network management station, NMS, is generally a dedicated workstation that can configure and monitor network devices, and receive network performance data. Sometimes referred to as just the management station or SNMP client, it houses the SNMP application software known as the manager. In the case of Nortel Networks, the Site Manager workstation is the NMS for the network routers.

### Agents

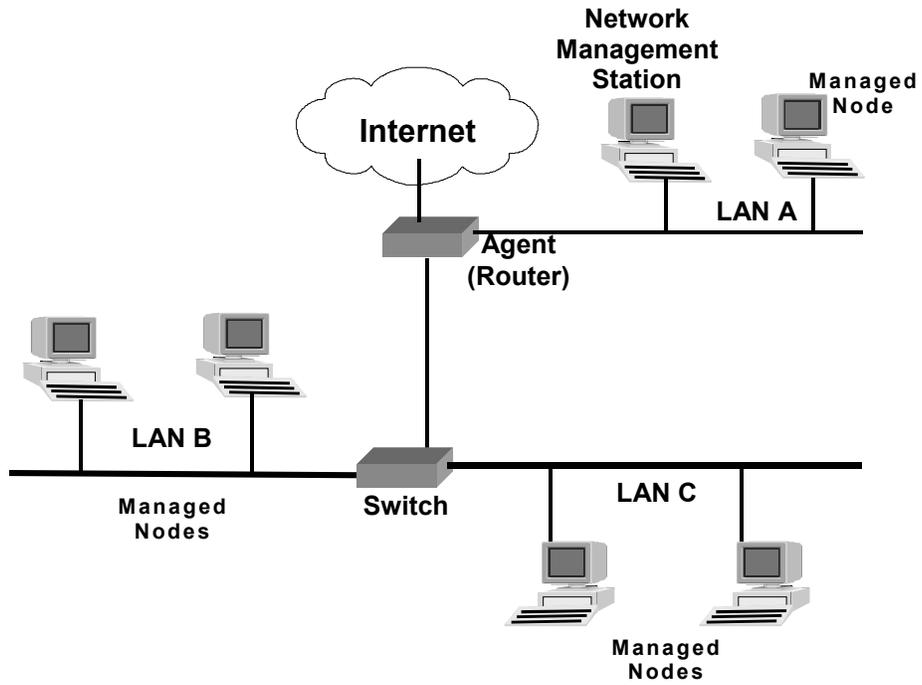
The network devices that are being monitored and managed by the management station are called managed nodes or objects. The agent is the software component in a managed object, for example, workstation or router, that sends network performance data to the network management station. The agent responds to the SNMP requests sent by the manager and sends messages indicating problems or the existence of a specific pre-defined condition on the agent. Pre-defined conditions are specific situations that the network manager defined using SNMP, for example, the hard drive memory is full, indicating that the network manager must increase the memory of the hard drive on the agent.

In the past, managed objects were usually bridges or routers, but today hubs, gateways, and workstations may also be managed objects.

For the purpose of this lesson, the agent resides on the routers within a network.

---

## SNMP Components: The Network Management Station and the Agent



### Management Information Base

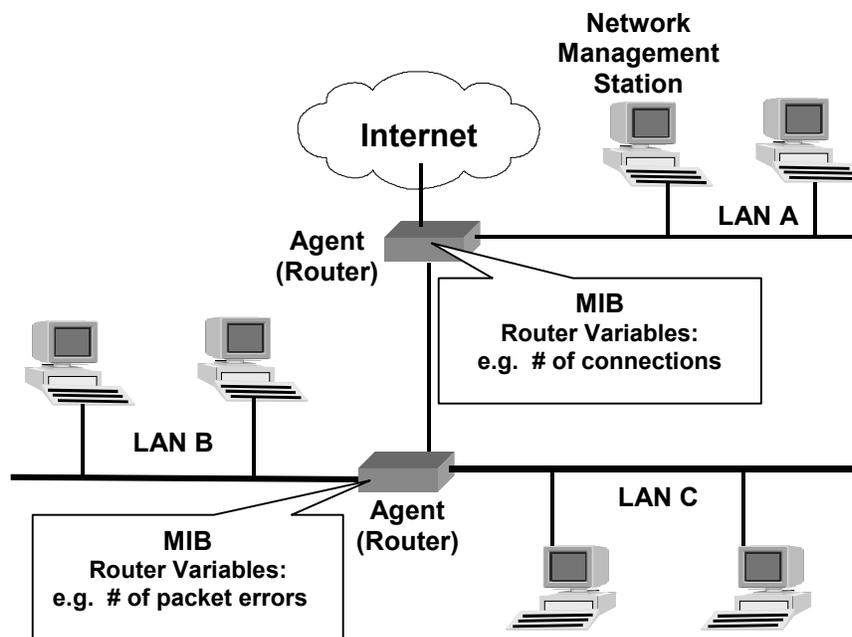
The management information base, MIB, is the database of network configuration and performance information that is stored on the agent for access by the manager. The database contains information, or variables, such as:

- The number of packets sent by the agent.
- The number of packets received by the agent.
- The record of packet errors.
- The number of connections.

Each network device has a set of variables, or parameters, that are defined by their MIB and are accessed when the manager requests information from the agent. The manager can issue a command to change the variables in the MIB.

---

### The MIB is a Database of the Agent's Network Performance Variables

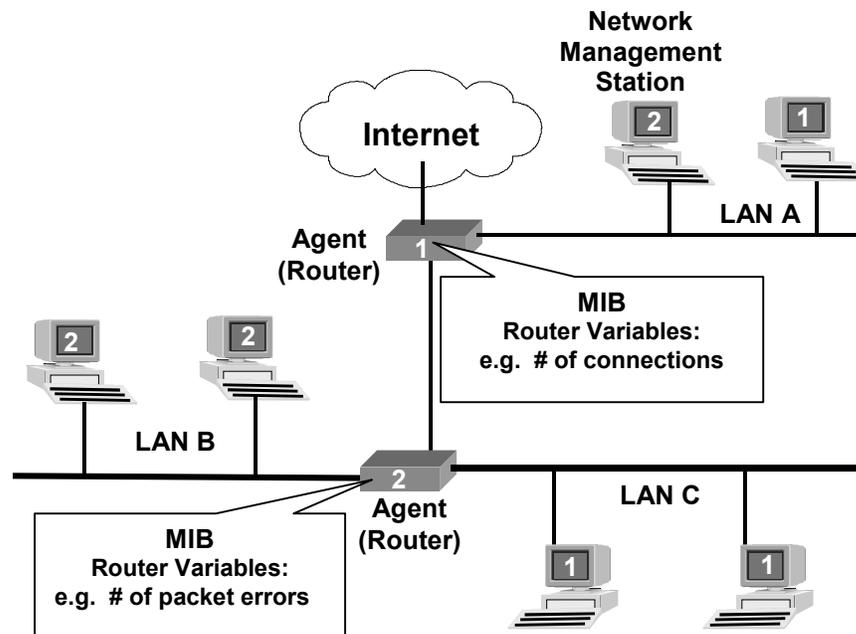


## Community

There can be literally hundreds of networks interconnected together, which represent many different organizations within the entire internetwork. In order to isolate each organization as a separate management group, each organization is assigned a community name. The exchange of SNMP messages occurs only within network devices located in the same community.

One can think of the community name as a password used for security. The validation process consists of the agent comparing the incoming community name with those configured on the router.

## Two Communities: 1 and 2



In the illustration above, each device is a member of one of two communities established through SNMP, 1 or 2. Members of community 1 can only exchange SNMP messages with other members of community 1. The same holds true for those members of community 2; they can only exchange SNMP messages with other members of community 2. All members of a community have the same access rights. A community can be either “read only” or “read and write” MIB variables on a device. Read only means a device can only view configuration and performance information, but not change any settings. Read and write means a device can view and change configuration and performance information.

## Check Your Understanding

- ◆ Diagram an internetwork of LANs. Assuming that SNMP is the management protocol used to monitor and manage your internetwork, label the SNMP components and define what the purpose of each of the components.

## SNMP Commands

One key word in SNMP is “simple.” That is because there are only five commands that can be issued to an agent.

- **getRequest** (read only)
- **getNextRequest** (read only)
- **getResponse** (read only)
- **setRequest** (read/write)
- **trap** (read only)

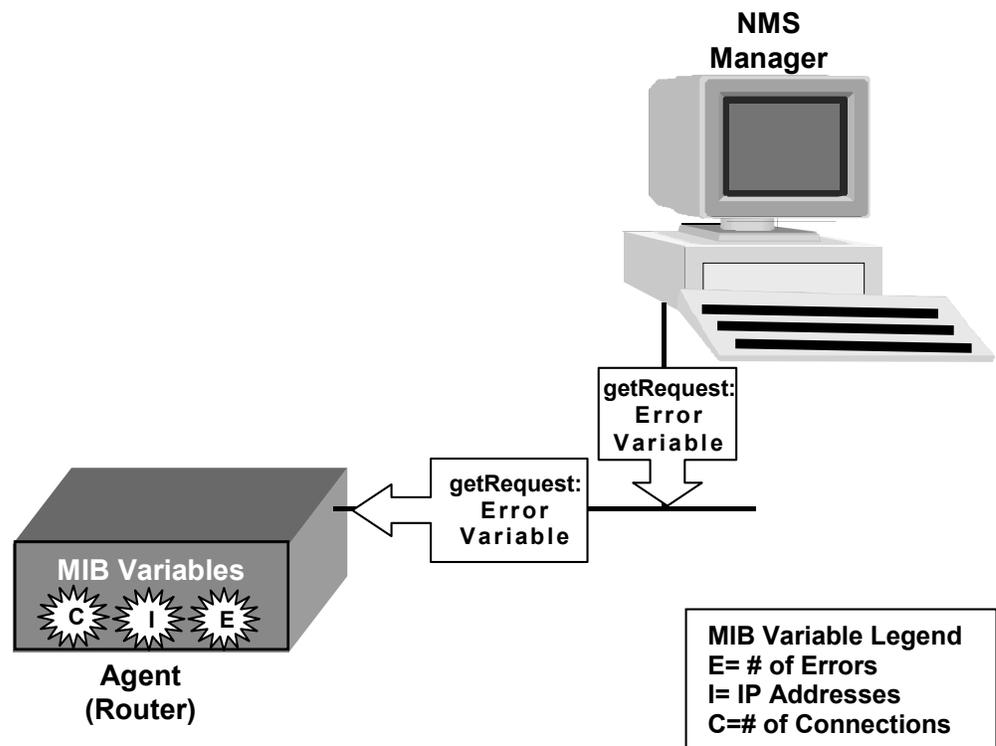
Many applications send an explicit command that results in an immediate response, for example, “reboot” causes the computer to immediately turn off and restart. Within SNMP, a command is issued to either monitor or modify a variable stored in the MIB of the agent. The manager controls the operation of the agent by issuing commands that change, or set, a variable in the MIB.

SNMP commands are either read-only or read/write commands. Read-only commands are used to monitor variables in the agent. Read/write commands are used to set, or change, variables in the agent.

### Read-Only Commands

The **getRequest**, and **getNextRequest** commands are read-only commands, in that the manager can only read the information stored by the agent. These commands cannot make any changes to the variables in the agent's MIB. The **getResponse** and **trap** commands from the agent are also read-only commands.

### SNMP **getRequest** Command

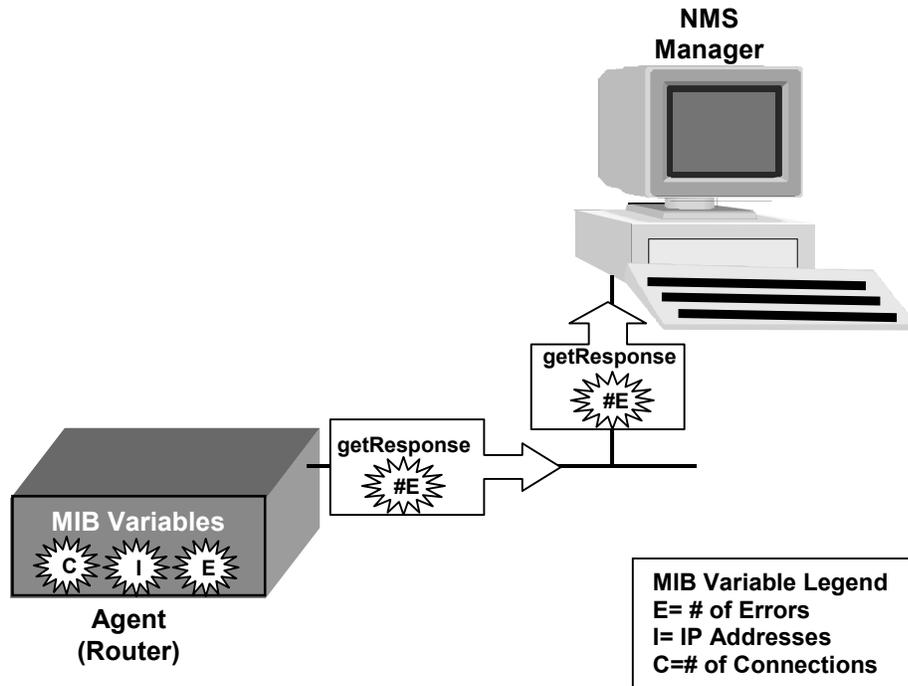


The manager sends a **getRequest** command to the agent to acquire information about a specific variable. The **getNextRequest** command is issued by the manager to request the agent to send the next variable, allowing the manager to receive a series of related variables.

In the illustration above, the manager sent a **getRequest** command requesting information from the agent about the number of errors that have occurred.

---

## SNMP getResponse Command

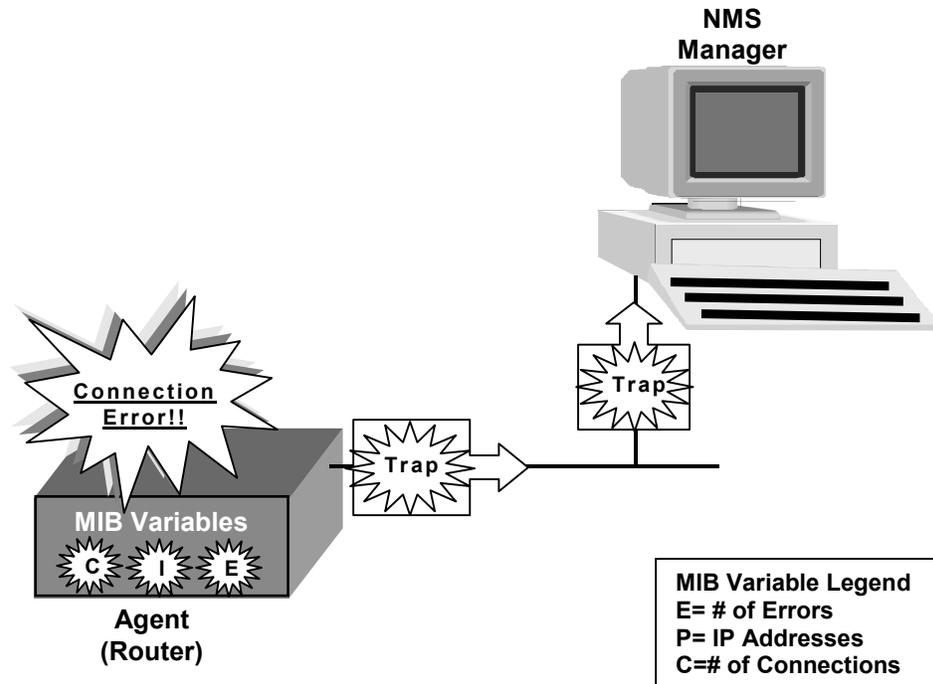


The agent sends back the information on the variable requested by the manager using the **getResponse** command. In this case, the agent sends the number of errors that have occurred.

The **trap** is an unsolicited message used by the agent to inform the manager when certain conditions or extraordinary events have occurred, for example, the hard drive of a device has run out of memory.

---

### SNMP Trap Command



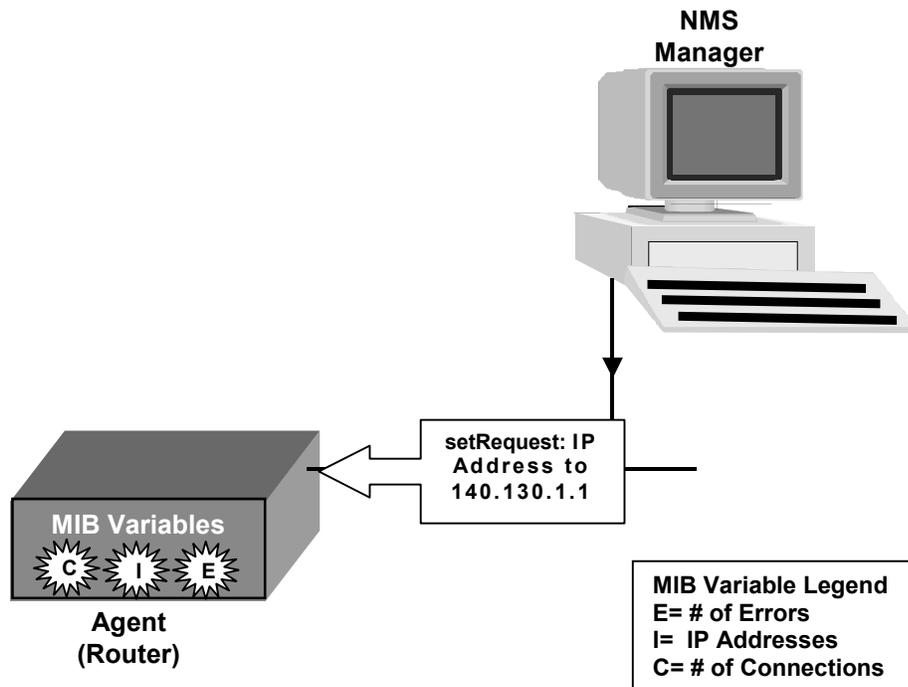
In the illustration above, the agent uses the **trap** command to notify the manager that an error has occurred in one of its connections, for example, a port has been disabled. A trap is sent to the manager without the manager first requesting the information.

### Write-Only Command

The **setRequest** command is write only. The manager sends a **setRequest** command along with a value for a MIB variable to the agent that instructs the agent to apply the specific setting to a variable.

---

### SNMP setRequest Command



In the illustration above, the manager sent a **setRequest** to the agent setting the IP address variable to 140.130.1.1.

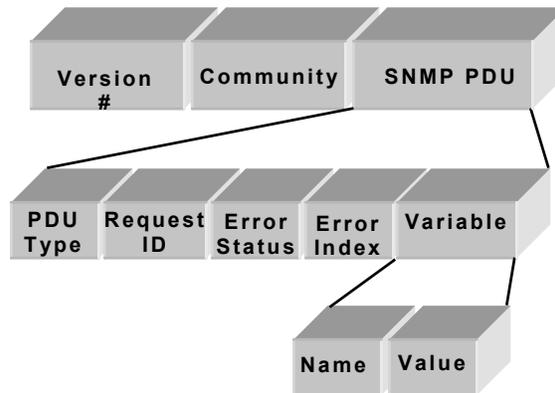
## SNMP Message Format

Every SNMP message is formatted with three basic sections, the version number, the community name, and the protocol data unit (PDU). The PDU is the section of the SNMP message that contains information sent to and from the NMS and agent.

There are two formats for the PDU.

- The SNMP PDU is used for the **GetRequest**, **GetnextRequest**, **GetResponse**, and the **SetRequest** commands.
- The trap PDU is formatted for the **trap** command.

### SNMP PDU Message Format



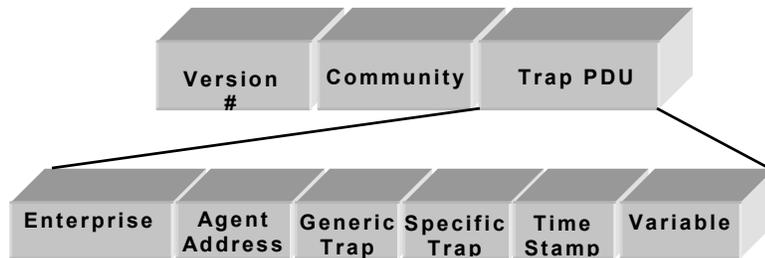
The SNMP PDU has five basic sections:

- **PDU Type**—Codes for the type of SNMP command the PDU represents.
  - 0= GetRequest.
  - 1= GetnextRequest.
  - 2= GetResponse.
  - 3= SetRequest.
  - 4= Trap.

- **Request ID**—Contains a number ID for each PDU.
- **Error Status**—A numeric code to indicate the presence of an error. A zero is used for no errors.
- **Error Index**—A numeric code to indicate in what variable an error occurred.
- **Variable**—Contains the variable information and has two subsections, name and value.

---

### Trap PDU Message Format



The Trap PDU has six basic sections:

- **Enterprise**—The vendor’s product ID.
- **Agent Address**—The network address of the agent.
- **Generic Trap**—Numeric code that identifies the type of generic conditions that result in a trap message (for example, 2 = link down).
- **Specific Trap**—Numeric code that identifies a specific trap condition programmed by the network manager for monitoring.
- **Time Stamp**—Records the time a specific trap occurred.
- **Variable**—Consists of the variables that contain information on what caused the trap.

### **Check Your Understanding**

- ◆ Choose an SNMP command and diagram the exchange of information between the NMS and the agent.
  
- ◆ Explain the similarities and the difference in the architecture between the SNMP PDU and the Trap PDU.



## Try It Out

### SNMP Management

In this lab you will learn how to:

- Configure a SNMP community name on the Nortel Networks ARN using Site Manager.
- Configure access rights for a community and assign managers (IP addresses) to that community.
- Recognize and correct an access problem on the ARN that is related to community access rights.

During this lab, work in teams of three. Record your experiences, results, speculations, and conclusions in your portfolio. Write a summary of your activities and results.

#### Materials Needed:

- Nortel Networks' Advanced Remote Node (ARN) Router
- Classroom Network
- Windows 95 PC
- Site Manager
- Any Word Processor (e.g., MS Word)
- Pen/Pencil and Paper
- Student Portfolio

#### Part One: Creating a Community

1. Enter the Configuration Manager in Dynamic mode.
2. From the Configuration Manager, add a community called "secure."
  - a. Click Protocols.
  - b. Click IP.
  - c. Click SNMP.
  - d. Click Communities.
  - e. Click Community.
  - f. Click Add Community.



- a. Change the system name that appears on the main Site Manager screen.

### **Part Two: Changing the Public Community to Read-only Access**

1. Use the Configuration Manager in dynamic mode and edit the public community to make its status read-only.
2. Remove the IP address 0.0.0.0 (world access) as manager from the public community.
3. Add the IP address of your Site Manager station to the router's list of managers in the public community.
4. Back out of the Configuration Manager without saving your changes.
5. Change your router connection to use the public community.

### **Part Three: Recognizing Access Restrictions**

1. With a connection to the router using the public community, try to change the system name again. Does the name change? Can you explain why?
2. Back out of the Configuration Manager without saving your changes.
3. Try to attach to another router in the network. Can you establish a Site Manager session with another router?
4. Repeat step 2.
5. Exit the remote router. Do not save changes.
6. Change your router connection back to **secure**.
7. Go to the TI and invoke the Nortel Networks proprietary SNMP security mechanism:
  - a. Enter **wfsnmpmode 3**.
  - b. Enter **wfsnmpkey test** ("test" is a key or password).
8. Using the Configuration Manager in dynamic mode, give the community public read/write access. In the process of giving public read/write access you will be prompted to enter the key that you defined in the previous step.

9. Return world access (0.0.0.0 as a manager) to the community public.
10. Exit the Configuration Manager without saving the configuration.
11. Go to the TI and return the router to SNMP trivial mode as **wfsnmpmode 1**.

**Rubric: Suggested Evaluation Criteria and Weightings**

| <b>Criteria</b>  | <b>%</b>   | <b>Your Score</b> |
|--|------------|-------------------|
| Complete record of procedural results.                       | 25         |                   |
| Summary, analysis, synthesis and conclusions                 | 50         |                   |
| Organization and summary in format suitable for reproduction | 25         |                   |
| <b>TOTAL</b>   | <b>100</b> |                   |

## Stretch Yourself



### Windows 95 System Monitor

There are other programs that can help a network manager monitor performance on local and remote computers. Windows 95 and 98 have built-in system tools that allow you to monitor system performance. One of these tools is the System Monitor. When changes are made to the workstation's system configuration, System Monitor shows the effect on the overall system performance. With the information gathered using System Monitor, a network manager can justify hardware upgrades and changes that improve performance.

In this exercise you will establish a performance benchmark of your workstation's configuration. This information should be recorded in your portfolio for future reference. You can use this benchmark throughout the course to compare the changes in performance of your workstation.

#### Materials Needed:

- Windows 95 PC
- Windows 95 System Monitor
- Any Word Processor (e.g., MS Word)
- Pen/Pencil and Paper
- Student Portfolio

#### Install and Run System Monitor

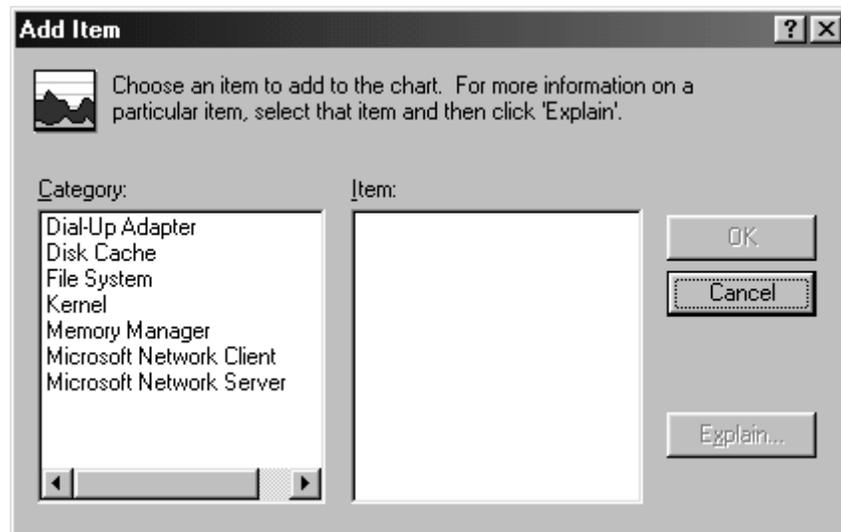
1. Check to see if your workstation has the System Monitor already installed. It should be listed under the Accessories and System Tools menu. If it does, then the installation steps can be skipped.
  - a. Click the Start menu.
  - b. Choose the Control Panel under Settings.
  - c. Click Add/Remove Programs.
  - d. Click Windows Setup.
  - e. Make sure Accessories is checked in the Components list.
  - f. Click Details.
  - g. Make sure System Monitor is checked, if not check it and click OK.
  - h. Click OK again to install System Monitor.

2. To run System Monitor:
  - a. Click the Start menu.
  - b. Click Run.
  - c. In the dialog box, type **sysmon**.

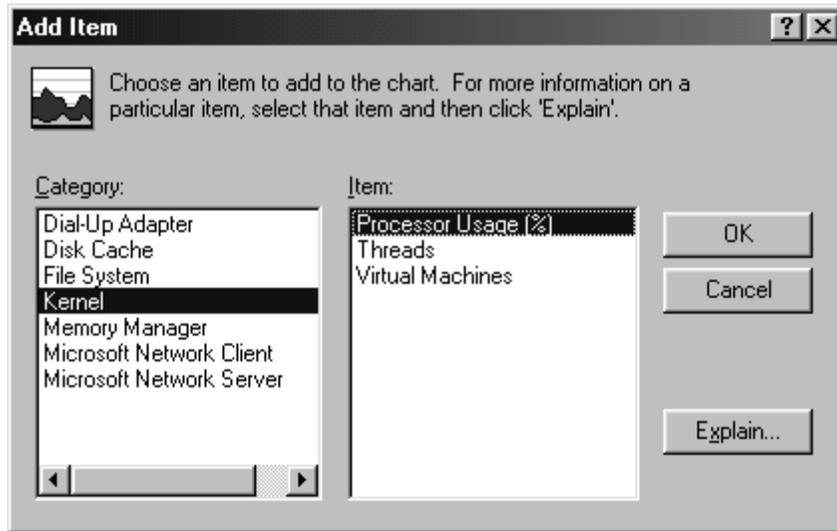
### Establish a Benchmark of Performance

With System Monitor running, you can add or delete items that you want to monitor. There are many systems you can view, and several ways to display the information using System Monitor's options. Following these instructions will guide you to how to change what you monitor and how you display the information. Once you have the basics, it is up to you to decide what resources you wish to monitor and how you want to display the information.

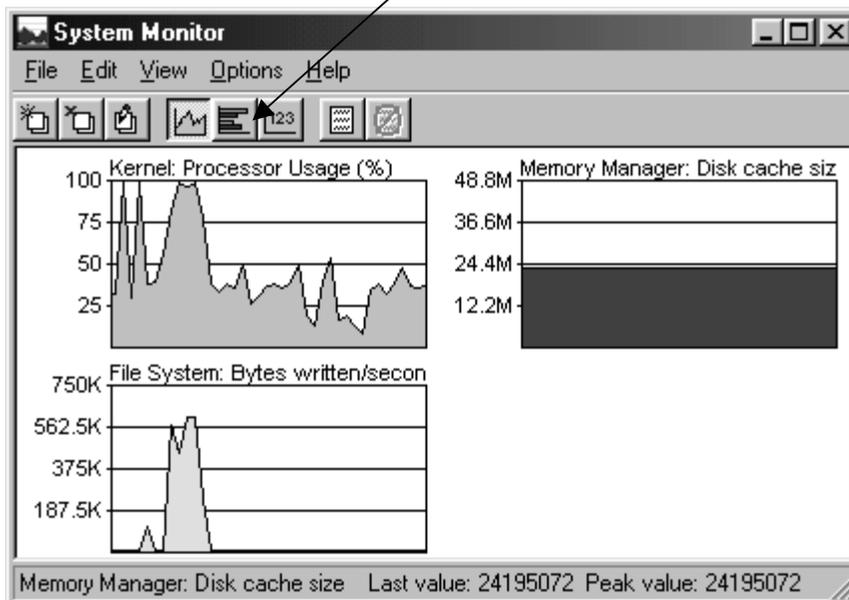
1. With System Monitor running, click the Edit menu.
2. Click Add Item.
3. A display box will appear with several resources that can be monitored.



- At this point, you may select a category to monitor, for example, Kernel, and an item under that category. (Kernel is software that operates at the heart of the operating system and manages vital parts of the system, such as memory.).



- Click OK to start monitoring. You can add or remove items to your monitor as you experiment. The Explain button displays information on the item selected to help you understand what will be monitored.
- The System Monitor displays the information in one of three views, line charts, numeric charts, or bar charts. You can change the view from the view menu or from the icons on the Monitor window.



7. The System Monitor displays information in terms appropriate for the specific resource being monitored. For example, the Kernel: Processor information is displayed as the percentage of usage over time. For the File System: Bytes Written information is displayed as the number of bytes written per second. Explore each resource and record how the performance information is displayed.
8. After you have set-up the resources you want to monitor, take a screen shot of the System Monitor to record the baseline of performance.
  - a. To take a screen shot, use the Alt+Prnt Scrn keys together. This will place a picture of the screen on the computer's clipboard.
  - b. Open a new document in Microsoft Word.
  - c. On the Edit menu, select Paste to paste the screen shot into the document.
9. Write a description of your workstation's performance from the information you gathered using System Monitor and your screen shot.
10. After you have recorded the benchmark for your workstation, try making changes that will alter the display in System Monitor, for example, open a document, access the Internet, or access a file on the school's server.
11. Record the changes that took place in System Monitor and make a screen shot of the display.
12. Write a description comparing the displays from added activity to the benchmark. How did increasing activity on the workstation affect its performance?

**Rubric: Suggested Evaluation Criteria and Weightings**

| Criteria  | %          | Your Score |
|---|------------|------------|
| Accurate and concise description of benchmark                                       | 25         |            |
| Insightful comparison of benchmark to performance changes from workstation activity | 50         |            |
| Neat and concise record keeping   | 25         |            |
| <b>TOTAL</b>  | <b>100</b> |            |

## Network Wizards

### Researching SNMP Software

Many router manufacturers create their own SNMP software packages to accompany their products. These SNMP software packages are often written with a specific product in mind. As a network manager, you will need to be familiar with many different SNMP software packages since you will undoubtedly interface with many different vendor products.

#### Materials Needed:

- Windows 95 PC
  - Internet Connection (optional)
  - Any Word Processor (e.g., MS Word) or Spreadsheet (e.g., MS Excel)
  - Pen/Pencil and Paper
1. Using multiple sources (for example, the Internet, telephone interviews, site visits) available to you, research at least two SNMP software packages that are currently used by router manufacturers.
  2. Document a comprehensive comparison of the selected SNMP packages. Include in your documentation what manufacturer uses the package, what hardware is supported by the package, what type of user interface is used (that is, DOS commands or Graphical User Interface), and how are the packages compared in software reviews (for example, user-friendly?).
  3. Create a comparison chart that someone unfamiliar with these software packages could reference to determine which package is best for their use.
  4. Choose one SNMP package to recommend and defend your choice in a short essay.



5. Document all resources used to complete this assignment.
6. Share your results in class discussion.

**Rubric: Suggested Evaluation Criteria and Weightings**

| Criteria  | %          | Your Score |
|---|------------|------------|
| Clear and concise documentation of research results | 30         |            |
| Analytical defense of SNMP choice                   | 30         |            |
| Clear and understandable product comparison chart   | 30         |            |
| Documentation of resources                          | 10         |            |
| <b>TOTAL</b>  | <b>100</b> |            |

---

## Summary

In this lesson, you learned the following:

- The description of SNMP and its purpose in routing.
- The identification of SNMP architecture and message formats.
- How to configure a SNMP community name on the Nortel Networks ARN using Site Manager.
- How to configure access rights for a community and assign managers (IP addresses) to that community.
- How to recognize and correct an access problem on the ARN that is related to community access rights.

## Review Questions

Name \_\_\_\_\_

### Lesson 6-1: Simple Network Management Protocol

#### Part A

1. Describe the Simple Network Management Protocol.
  
2. List five management areas defined by the ISO for which SNMP was developed to monitor and manage.

#### Part B

Match the definition with its SNMP component.

| Component          |    | Definition  |
|--------------------|----|---|
| 1. _____ MIB       | A. | A dedicated workstation that can configure and monitor and management network devices using SNMP.   |
| 2. _____ Agent     | B. | The database of network configuration and performance information.                                  |
| 3. _____ NMS       | C. | The network device that is being monitored and managed.   |
| 4. _____ Community | D. | An organized management group with the same name. Often thought of as a password used for security. |

Define the purpose of each of the SNMP commands. Identify which are read-only and which are write commands.

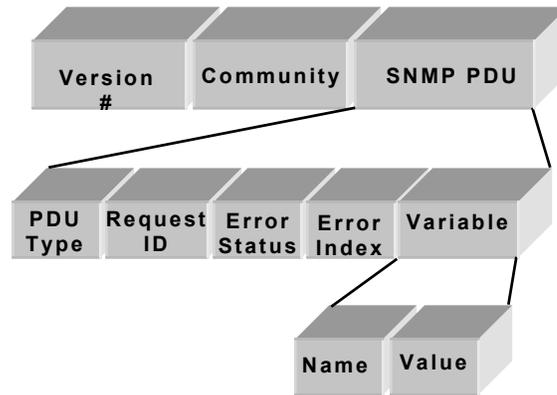
1. GetRequest-
  
2. GetResponse-
  
3. GetnextRequest-

4. Trap-

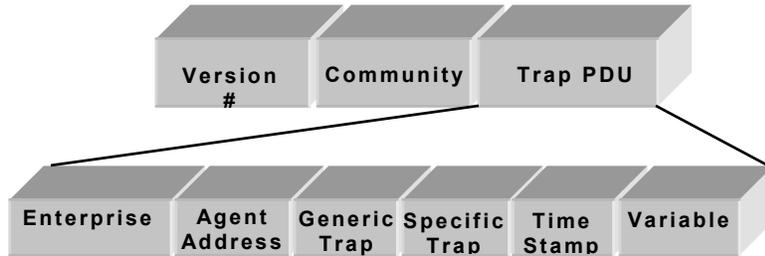
5. SetRequest-

**Part C**

1. Identify the message format and label each section.
2. Define the purpose of each section.
  - a. Name of the message format:SNMP PDU



3. Identify the message format and label each section.
4. Define the purpose of each section.
  - a. Name of the message format: Trap PDU



---

## Scoring

### Rubric: Suggested Evaluation Criteria and Weightings

| Criteria   | %  | Your Score |
|--|----|------------|
| Part A: Describe SNMP and its purpose in routing | 10 |            |
| Part B: Identify SNMP architecture and           | 40 |            |

|   |            |  |
|---|------------|--|
| message formats   |            |  |
| Part C: Identify SNMP architecture and message formats  | 50         |  |
| <b>TOTAL</b>  | <b>100</b> |  |
| <b>Try It Out:</b> Configure a SNMP community name on the Nortel Networks ARN using Site Manager. | <b>100</b> |  |
| <b>Stretch Yourself</b>   | <b>100</b> |  |
| <b>Network Wizards</b>  | <b>100</b> |  |
| <b>FINAL TOTAL</b>  | <b>400</b> |  |

---

## Resources

Causey, J.F., Wille, C., Glenn, W.J., Adamson, J. (1998). Sam's Teach Yourself MCSE TCP/IP in 14 Days. *Sam's Publishing*, Indianapolis, Indiana.

Digital Equipment Corp. (1997). Network Management Terms, Available On-line: <http://www.digital.com/netview/products/olannech/sld001.htm>.

Palmer, M.J. (1998) Hands-On Networking Essentials with Projects, *Course Technology, Inc.* Cambridge, Massachusetts.

Tittel, E., Hudson, K., & Stewart, J.M.. (1998). MCSE Exam Cram: TCP/IP, *Certification Insider Press*, Albany, New York.