Enterprise

CHAPTER

23

Using Network Monitor

About Chapter 23

The focus of Chapter 23 is on Network Monitor, a Windows NT Server administrative tool that enables you to monitor your network's performance by capturing, viewing, and analyzing network packets.

After a brief overview, the chapter outlines the steps to install Network Monitor on a Windows NT Server computer.

Next, the chapter presents in-depth coverage of how to use Network Monitor to capture network packets. Starting and stopping a capture, configuring a capture filter, and saving captured data are covered.

Finally, once a capture has been performed, Chapter 23 explains how you can use Network Monitor to view and analyze the captured packets.

This chapter includes one hands-on lab. In this lab you'll install and use Network Monitor on your own Windows NT Server computer.

Chapter 23 contains some great information, but can be considered optional reading unless you're preparing for the Enterprise exam. This chapter maps to the "Monitor network traffic by using Network Monitor" objective for the Enterprise exam.

What Is Network Monitor?

Network Monitor is a Windows NT Server administrative tool that makes it possible for you to capture, view, and analyze network traffic (packets). Network Monitor doesn't ship with Windows NT Workstation.

Network Monitor can be used to view network statistics, such as: percent of network utilization, number of frames per second, number of broadcasts per second, and so forth. This packet analysis tool is useful in troubleshooting network problems and protocol problems. It is also useful to determine current network utilization, as well as for trend analysis and network capacity planning.

Network Monitor is capable of capturing entire *packets* (also referred to as *frames*) from the network, and of analyzing the contents of each of these packets. Packets can be viewed and interpreted when captured, or saved to disk for later analysis.

The version of Network Monitor that ships with NT Server 4.0 is designed to capture only packets addressed to, or sent from, the Windows NT Server computer running Network Monitor. A more robust version of Network Monitor ships with Microsoft Systems Management Server.

The primary difference between the two versions of Network Monitor is the capability of each product to use the promiscuous mode of the computer's network adapter: The version of Network Monitor that ships with NT Server 4.0, by default, is *not* used in promiscuous mode; the version that ships with System Management Server, by default, *is* used in promiscuous mode.

Promiscuous refers to a network adapter's ability to receive packets not addressed to that network adapter. A *non-promiscuous network adapter* can only receive packets addressed to that network adapter. A *promiscuous network adapter* can receive any packets transmitted on the local network segment. Whether a network adapter functions in promiscuous mode depends upon the design of the network adapter (most network adapters are capable of functioning in promiscuous mode) and the driver used for the network adapter.

The following sections explain how to install Network Monitor, and how to use Network Monitor to capture and view network packets.

Installing Network Monitor

Network Monitor consists of two parts: the *Network Monitor Tools*, and the *Network Monitor Agent*. Both parts are installed together using the Network application in Control Panel.

If the Network Monitor Agent is already installed, *it must be removed* before you can install the combination Network Monitor Tools and Agent.

Network Monitor requires a network adapter that uses an NDIS 4.0 driver. Check the Windows NT Hardware Compatibility List *(HCL)* to see which network adapters are supported.

TO INSTALL NETWORK MONITOR ON A WINDOWS NT SERVER COMPUTER, FOLLOW THESE STEPS:

1. Select Start ➪ Settings ➪ Control Panel.
2. In the Control Panel dialog box, double-click the Network icon.
3. In the Network dialog box, click the Services tab.
4. If Network Monitor Agent is *not* installed on the computer, skip to Step 6.

   If Network Monitor Agent *is* installed on the computer, you must remove it to install Network Monitor. On the Services tab, highlight Network Monitor Agent in the Network Services list box. Click the Remove command button.
5. A warning dialog box appears. Click the Yes command button to continue. Windows NT removes Network Monitor Agent.
6. On the Services tab, click the Add command button.
7. In the Select Network Service dialog box, highlight Network Monitor Tools and Agent, as shown in Figure 23-1. Click OK.
8. A Windows NT Setup dialog box appears. Ensure the correct path to your Windows NT Server source files (usually the `i386` folder on your Windows NT Server compact disc) is listed in the text box. Edit this text box if necessary. Click the Continue command button.
9. Windows NT copies source files and installs Network Monitor Tools and Agent.
10. The Network dialog box reappears. Click the Close command button.
11. Windows NT performs various bindings operations.

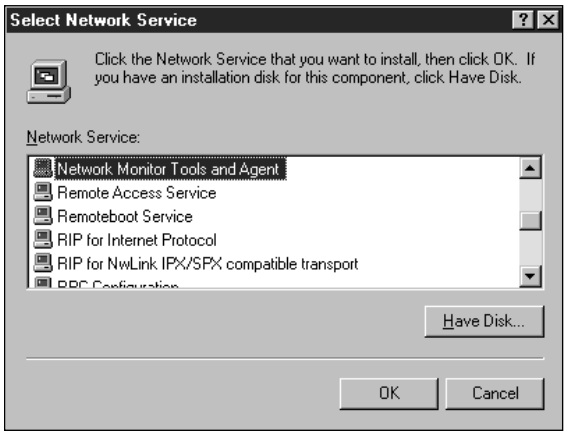


FIGURE 23-1 **Installing Network Monitor**

12. A Network Settings Change dialog box appears, indicating you must shut down and restart the computer for the new settings to take effect. Click the Yes command button to restart the computer.

Using Network Monitor to Capture Network Packets

Network Monitor can be used both to capture and view network packets. The next few sections focus on capturing network packets. Before you actually use Network Monitor, it's a good idea to take an introductory look at the look and feel of its primary interface.

To access Network Monitor, from the Windows NT Server desktop, Select Start ⩾ Programs ⩾ Administrative Tools (Common) ⩾ Network Monitor.

The Network Monitor main dialog box is shown, after a capture has been performed, in Figure 23-2. (Until a capture is performed, no statistics appear in this dialog box. The process of capturing is explained in the following sections.) Notice this dialog box is called the Capture Window, and four different scrolling list boxes are contained within it. Each of these scrolling list boxes is called a *pane* (as in a window pane).

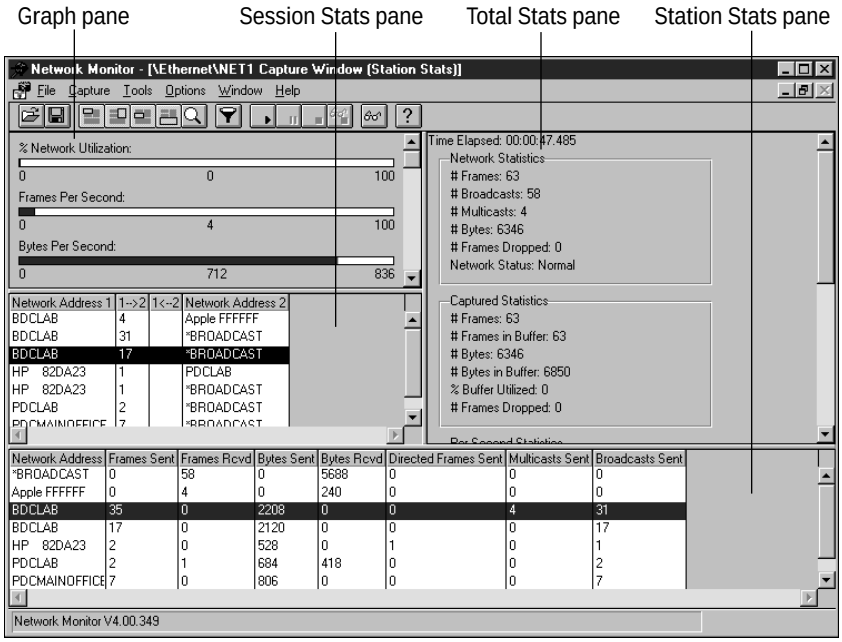


FIGURE 23-2 **The Network Monitor Capture Window dialog box**

Each of the four panes in the Network Monitor Capture Window dialog box displays different data and has a unique name. The four panes are: the Graph pane, the Total Stats pane, the Session Stats pane, and the Station Stats pane.

The *Graph pane*, which is the scrolling list box located at the upper left corner of the dialog box, displays five bar graphs. Each of these graphs depicts various network packet statistics, including: % Network Utilization, Frames Per Second, Bytes Per Second, Broadcasts Per Second, and Multicasts Per Second.

Figure 23-3 shows an entire Graph pane, with all five bar graphs displayed.

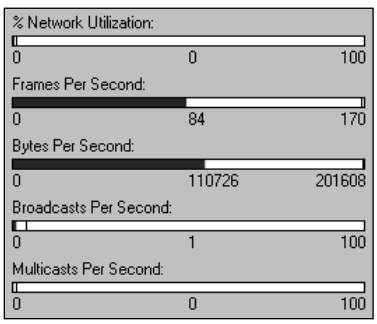


FIGURE 23-3 **The Graph pane in the Network Monitor Capture Window**

The *Total Stats pane*, which is the scrolling list box located at the upper right corner of the dialog box, displays five different types of statistics in five different sections. The sections listed are: Network Statistics, Captured Statistics, Per Second Statistics, Network Card (MAC) Statistics, and Network Card (MAC) Error Statistics.

Figure 23-4 shows an entire Total Stats pane, with all five sections displayed.

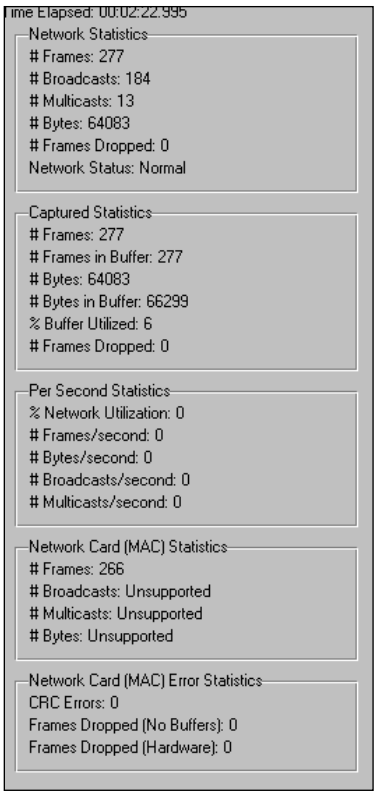


FIGURE 23-4 **The Total Stats pane in the Network Monitor Capture Window**

The *Session Stats pane*, which is the scrolling list box located in the middle of the left side of the dialog box, displays a summary of packets transmitted between pairs of computers or network devices on the local network segment. Each computer or device in this section is listed as a network address or a computer name.

Two statistics columns are shown between the pairs of network addresses/computer names. The first statistics column displays the number of packets sent

(during the capture period) from the computer or network device in the Network Address 1 column to the corresponding computer/device in the Network Address 2 column. The second statistics column displays the number of packets sent (during the capture period) from the computer/device in the Network Address 2 column to the corresponding computer/ device in the Network Address 1 column.

The *Station Stats pane,* which is the scrolling list box located across the bottom of the dialog box, displays several statistics associated with each computer/ network device that transmitted and/or received at least one packet captured from the local network segment during the capture period. Statistics shown include: Frames Sent, Frames Received, Bytes Sent, Bytes Received, Directed Frames Sent, Multicasts Sent, and Broadcasts Sent.

Now that you have an understanding of the primary Network Monitor interface, you're ready to learn how to use Network Monitor to capture packets and view captured data.

Configuring Network Monitor to Capture Using Promiscuous Mode

By default, the version of Network Monitor that ships with Windows NT Server 4.0 uses a special mode of the NDIS 4.0 driver, called "*local capture only*."

"Local capture only" is used primarily for two reasons: It minimizes the amount of processor utilization (promiscuous mode can use as much as 30 percent of total processor utilization), and it increases network security (not everyone should be able to capture and read all packets on the network segment).

Some NDIS 4.0 drivers don't correctly implement the "local capture only" mode. These drivers can capture packets sent *to* the Windows NT Server computer, but *not* the packets sent *by* the Windows NT Server computer. To remedy this situation and to allow Network Monitor to capture packets sent both to and sent by the Windows NT Server computer, Network Monitor must be reconfigured to use the promiscuous mode of the NDIS 4.0 driver.

A by-product of forcing Network Monitor to use promiscuous mode is that Network Monitor can then capture *all* packets transmitted on the local network segment (instead of only packets addressed to or from the Windows NT Server computer on which Network Monitor is running). Being able to capture all packets transmitted on the local network segment can be useful when you are trying to troubleshoot a

network problem or perform other network analysis tasks. The next section explains how to configure Network Monitor to capture using promiscuous mode.

in the real world

Microsoft only supports the use of promiscuous mode for the version of Network Monitor that ships with Systems Management Server. However, Microsoft recommends using promiscuous mode in conjunction with the version of Network Monitor that ships with NT Server 4.0 when an NDIS 4.0 driver doesn't correctly implement the "local capture only" mode.

Practically speaking, though, you can force Network Monitor to use almost any network adapter in promiscuous mode. If you do this, you will put more load on your processor, but you can capture all packets sent on the local network segment.

caution

One final word of caution on this—using the NT Server 4.0 version of Network Monitor in promiscuous mode (except to remedy a situation where a network adapter doesn't correctly implement the "local capture mode") might be considered a violation of the Windows NT Server licensing agreement.

TO CONFIGURE NETWORK MONITOR TO USE THE PROMISCUOUS MODE OF THE NDIS 4.0 DRIVER:

1. Select Start ➪ Run from the Windows NT Server desktop.
2. The Run dialog box appears. Type **regedt32** in the Open drop-down list box. Click OK.
3. The Registry Editor dialog box appears. Select Windows ➪ HKEY_LOCAL_MACHINE on Local Machine.
4. Double-click the + sign next to `SYSTEM`. Double-click the + sign next to `CurrentControlSet`. Double-click the + sign next to `Services`. Double-click the + sign next to `bh`. Highlight the `Linkage` folder.
5. Find the Bind value (located in the right-hand part of the dialog box).

   Figure 23-5 shows the Registry Editor dialog box at this point. Notice the Bind value is highlighted on the right side of the dialog box.

   Note the portion of the entry for the Bind value that *directly follows* the first\Device\listing in the entry. (In the example shown, this is Elnk31.) Write down this information for future use.

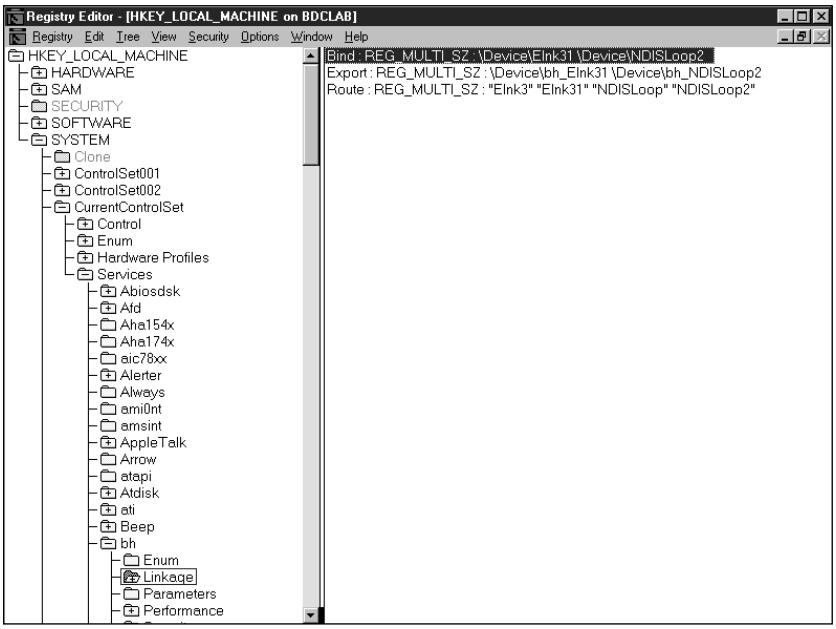


FIGURE 23-5 Using Registry Editor to determine Network Monitor bindings

6. Highlight the `Parameters` folder.
7. Select Edit ➢ Add Key.
8. The Add Key dialog box appears. Type **ForcePmode** in the Key Name text box. Leave the Class text box blank. Figure 23-6 shows the Add Key dialog box correctly configured. Click OK.
9. The Registry Editor dialog box reappears. Click the `ForcePmode` folder you just created.
10. Select Edit ➢ Add Value.
11. The Add Value dialog box appears. In the Value Name text box, type the value you noted in Step 5. (For example, Elnk31.) In the Data Type drop-down list box, select REG_DWORD. Figure 23-7 shows the Add Value dialog box correctly configured. Click OK.
12. The DWORD Editor dialog box appears. In the Data text box, type **1**. (Don't type the period at the end.) Click OK.
13. The Registry Editor dialog box reappears, as shown in Figure 23-8. Notice the new value has been added to the Registry (at the upper right side of the dialog box). Close the Registry Editor.
14. Shut down and restart your computer for this Registry setting to become effective.

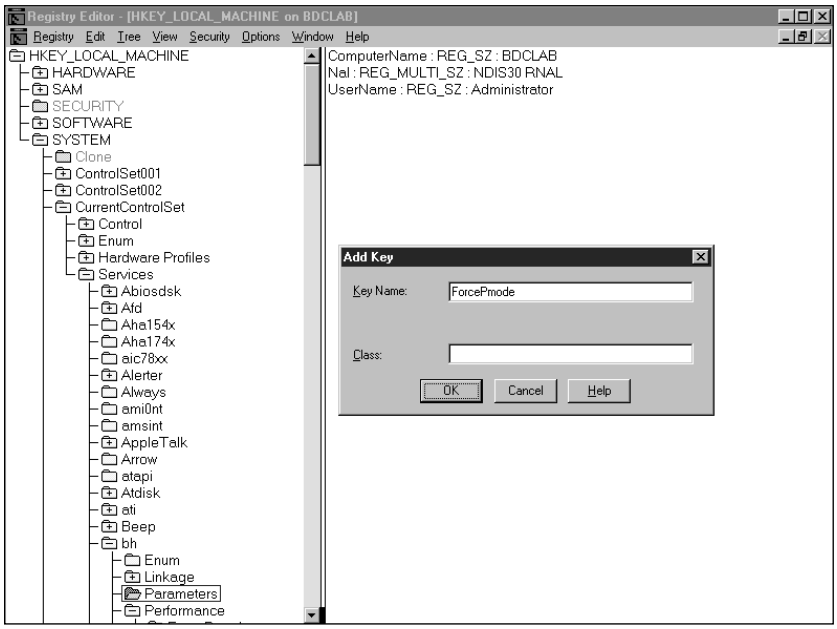


FIGURE 23-6 **Adding a key to the Network Monitor Registry settings**

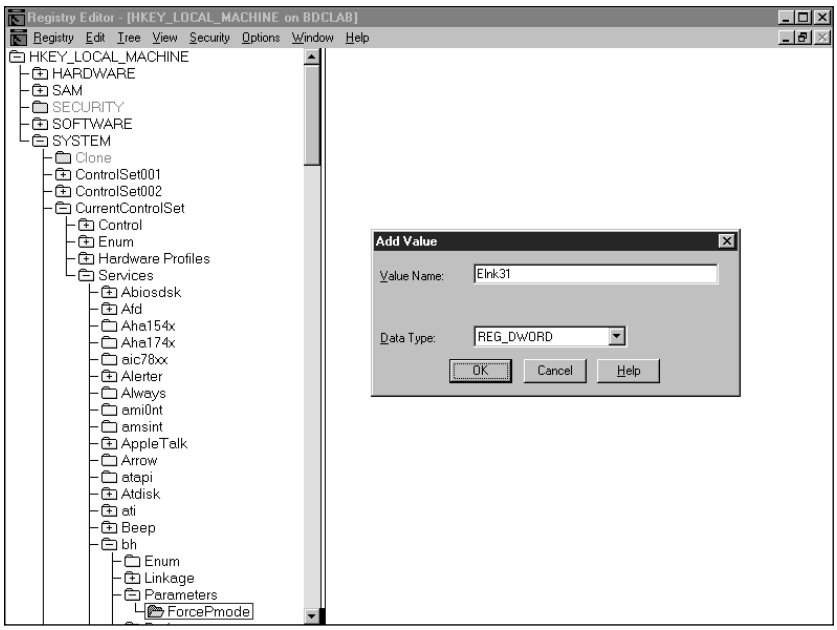


FIGURE 23-7 **Adding a value to the Network Monitor Registry settings**

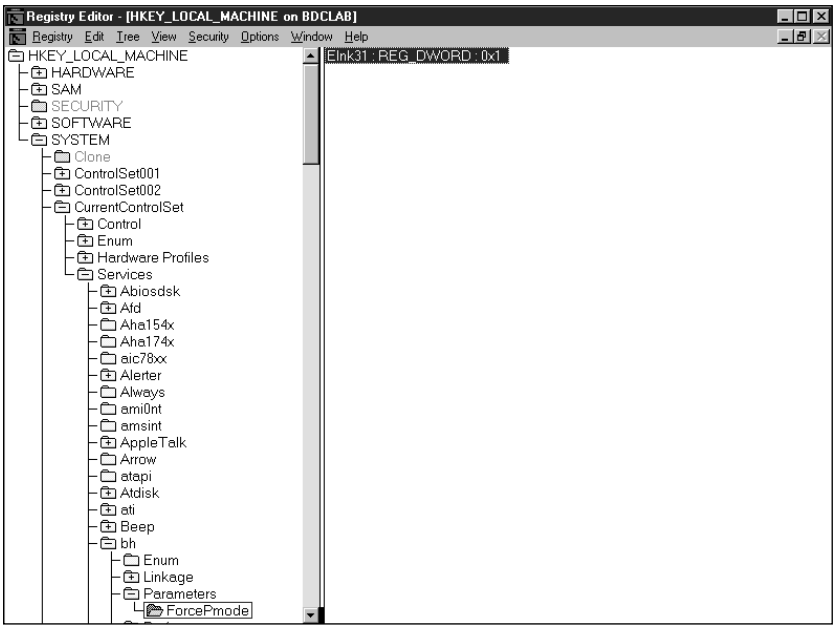


FIGURE 23-8 **Network Monitor configured to use promiscuous mode**

Capturing Packets

Network Monitor does *not* produce any statistics or other useful data until a capture is performed.

During a *capture,* Network Monitor receives packets transmitted on the local network segment and stores these packets either in memory or in a capture file. Capture files can be used for later analysis. The process of capturing doesn't interfere with packets reaching their intended destinations on the network.

If you are doing capacity planning or troubleshooting network access problems, you should consider performing a capture during a time of peak network activity. To troubleshoot other problems, you should perform a capture during the time when those problems most often occur.

To perform a capture, you must manually start and stop a capture in Network Monitor.

Three ways exist to *start* a capture in Network Monitor:

- Selecting Capture ≫ Start
- Pressing F10
- Clicking the Start Capture icon on the toolbar (this icon appears as a single right arrow, much like a play button on a CD or cassette tape player)

Once started, capturing continues until you stop the process.

There are three ways to *stop* a capture in Network Monitor:

- Selecting Capture ≫ Stop
- Pressing F11
- Clicking the Stop Capture icon on the toolbar (this icon appears as a single small square, much like a stop button on a CD or cassette tape player)

During the capture process, statistics in the four Network Monitor panes are updated continuously. You can view these statistics as they change to get a general impression of how the network is being used.

If you don't want to view statistics during the capture process, select Capture ≫ Dedicated Capture Mode before you begin the capture process. Selecting the *Dedicated Capture Mode* can save processor time on a computer that performs multiple server functions on the network. After you select the Dedicated Capture Mode, start the capture as you normally would. During the capture period, the Network Monitor dialog box will be minimized, and the Dedicated Mode dialog box will be displayed, as shown in Figure 23-9. Notice the only statistic displayed is the total number of frames captured, and that you can stop and pause the capture by using this dialog box.

When you stop a Dedicated Mode capture, all statistics are immediately updated and displayed in the four panes of the Network Monitor Capture Window dialog box.

Because a large number of packet statistics may be displayed in the Network Monitor Capture Window dialog box, you might want to use a capture filter to limit the type of network packets that will be captured by Network Monitor.

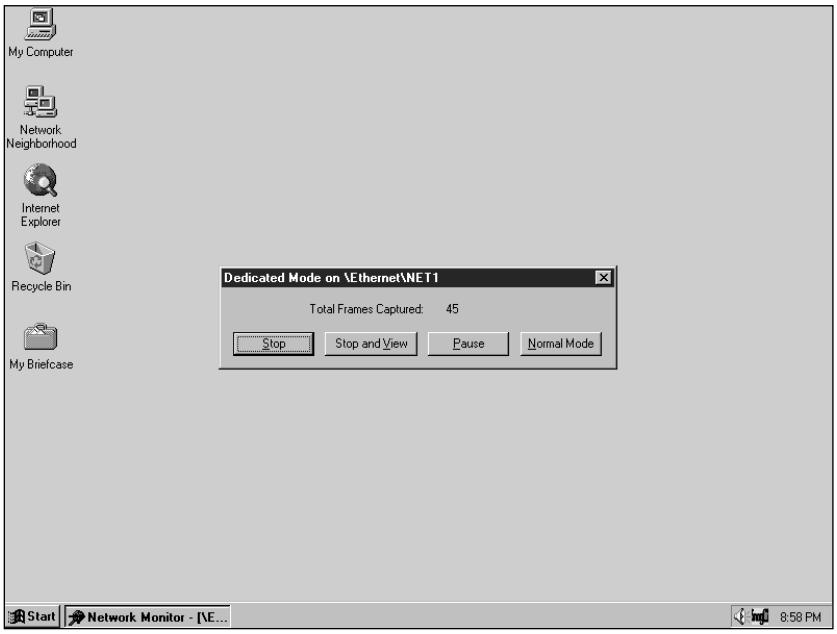


FIGURE 23-9 **Network Monitor performing a capture in Dedicated Mode**

Configuring a capture filter

By default, Network Monitor's *capture filter* is configured to capture *all* packets addressed to or sent by the Windows NT Server computer. However, you can specify which packets transmitted on the network segment will be captured by configuring a capture filter.

You can configure a capture filter so that:

- Only packets using certain protocols are (or are not) captured
- Only packets to or from specified computers or network devices are (or are not) captured
- Only packets containing specific byte patterns are captured
- Any combination of the previous

TO CONFIGURE A CAPTURE FILTER, FOLLOW THESE STEPS:

1. In Network Monitor, select Capture ≫ Filter. (Or press F8, or click the Edit Capture Filter icon in the toolbar—this icon appears as a funnel.)

2. The Capture Filter dialog box appears, as shown in Figure 23-10. Notice the default capture filter is displayed.

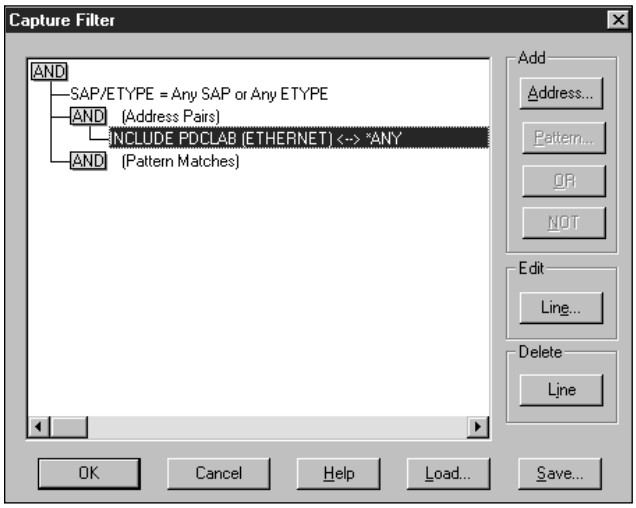


FIGURE 23-10 Default capture filter settings

3. To configure a capture filter to capture packets by protocol, double-click `SAP/ETYPE = Any SAP or Any ETYPE` in the Capture Filter dialog box.
4. The Capture Filter SAPs and ETYPEs dialog box appears, as shown in Figure 23-11.

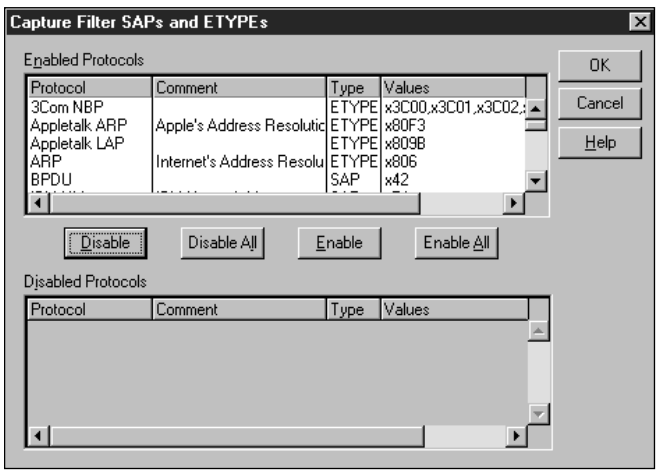


FIGURE 23-11 Configuring packets to be captured by protocol

Highlight the protocol(s) you want to exclude in the Enabled Protocols list box. Click the Disable command button.

Or, you can click the Disable All command button to exclude all protocols, and then highlight the protocol(s) you want to include in the Disabled Protocols list box. Then click the Enable command button.

Click OK.

5. To configure a capture filter to capture packets by their associated computer name or network address, highlight (Address Pairs) in the Capture Filter dialog box. Click the Address command button in the Add section of the dialog box.
6. The Address Expression dialog box appears, as shown in Figure 23-12. Note the Station 1 and Station 2 list boxes.

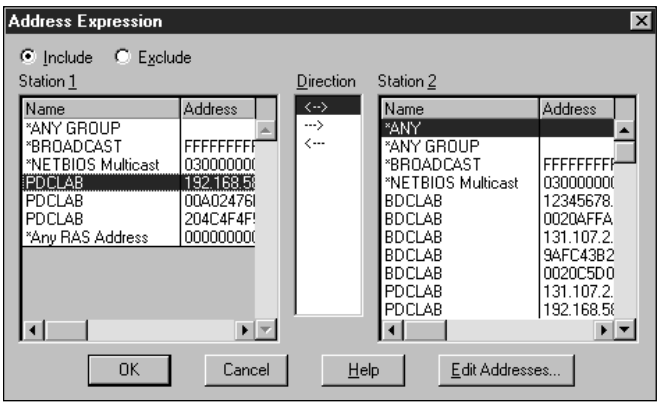


FIGURE 23-12 Configuring packets to be captured by network address or computer name

First, select the radio button next to Include or Exclude at the top of the Address Expression dialog box, depending on whether you want to capture or exclude from capturing packets associated with a particular pair of computer names or network addresses.

Then select a computer name or network address from the Station 1 list box. Then, select a direction arrow in the Direction list box to indicate whether the computer name or network address highlighted in the Station 1 list box is the packets' source address (--->), destination address (<---), or can be either (<-->).

Finally, select a computer name or network address from the Station 2 list box. Click OK.

The new address appears in the Capture Filter dialog box. Network Monitor enables you to configure up to three address pairs in a single capture filter.

7. If you have configured Network Monitor to use promiscuous mode, and you want to configure a capture filter to capture all packets transmitted on the local network segment, highlight INCLUDE computer_name [Ethernet] <--> *ANY in the Capture Filter dialog box, and then click the Line command button in the Delete section of this dialog box. This will instruct Network Monitor not to filter by computer name or network address, but to instead capture all packets.

   Figure 23-13 shows the resulting Capture Filter dialog box after this configuration is made. Compare this figure to Figure 23-10. Notice the capture filter in Figure 23-13 no longer restricts capturing by computer name or network address, because the INCLUDE *computer_name* [Ethernet] <--> *ANY entry under (Address Pairs) has been removed.

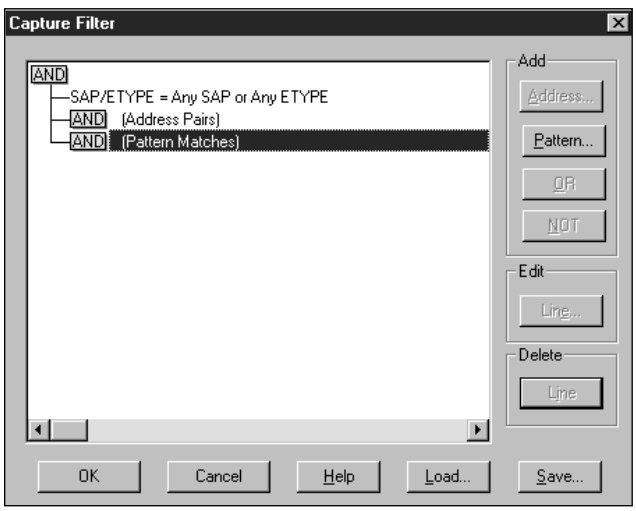


FIGURE 23-13 Configuring Network Monitor to capture all packets transmitted on the local network segment

8. To configure a capture filter to capture packets by a specific byte pattern contained in those packets, highlight (Pattern Matches) in the Capture Filter dialog box and click the Pattern command button in the Add section of the dialog box.
9. The Pattern Match dialog box appears, as shown in Figure 23-14. Configure the Offset (in hex) and Pattern text boxes. Click OK.

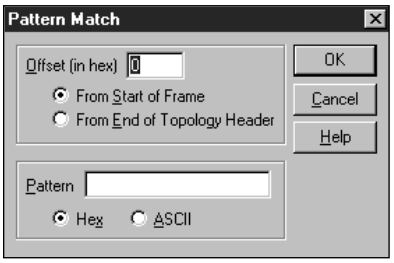


FIGURE 23-14 **Configuring packets to be captured by byte pattern**

note Configuring a capture filter by byte pattern is normally only done by advanced users of Network Monitor. Detailed knowledge of packet construction is required to configure a pattern match filter.

10. The Capture Filter dialog box reappears. Click OK.

Saving Captured Data

After you finish performing a capture, you can save the captured data to a file for later analysis if you like. To save captured data to a file, select File ➪ Save As in the Network Monitor main dialog box.

Also, when you exit Network Monitor, the Save File dialog box appears, prompting you to save captured data to a file at that time if you haven't previously done so.

To view the saved file at a later time, select File ➪ Open in the Network Monitor main dialog box, and then select the file you saved from the Open File dialog box.

Using Network Monitor To View Captured Packets

Captured packets are of no use until you view them and interpret the statistics and information displayed.

You can use two primary dialog boxes to view captured data in Network Monitor: the Capture Window dialog box, and the Capture Summary dialog box. The view you choose depends on the type of information you seek.

The *Capture Window* dialog box (the Network Monitor main dialog box) displays general network activity statistics. This dialog box is useful for determining current network utilization, the type and number of packets being sent over the network, and which computers are generating (or receiving) the most network traffic. These statistics can be used for troubleshooting, for trend analysis, and for capacity planning purposes.

The *Capture Summary* dialog box displays a listing of all packets captured, and enables individual packet contents to be viewed and analyzed. This dialog box is used for capacity planning and troubleshooting. For example, you can use this dialog box to establish a baseline of the amount of network traffic that maintains browser information on a network segment or subnet. This baseline can help with capacity planning your network.

Capacity planning is discussed in more detail in Chapter 24.

In addition to being useful for capacity planning, the Capture Summary dialog box can be useful when troubleshooting protocol and network adapter driver problems.

The following sections explain how to view and interpret captured data by using the Capture Window and Capture Summary dialog boxes.

Using the Capture Window Dialog Box

The Capture Window dialog box is the Network Monitor main dialog box, and is shown in Figure 23-15. As previously mentioned, this dialog box has four panes: the Graph pane, the Total Stats pane, the Session Stats pane, and the Station Stats pane.

The following sections explain how to use the Capture Window dialog box in Network Monitor to perform some of the most common network analysis tasks on captured data.

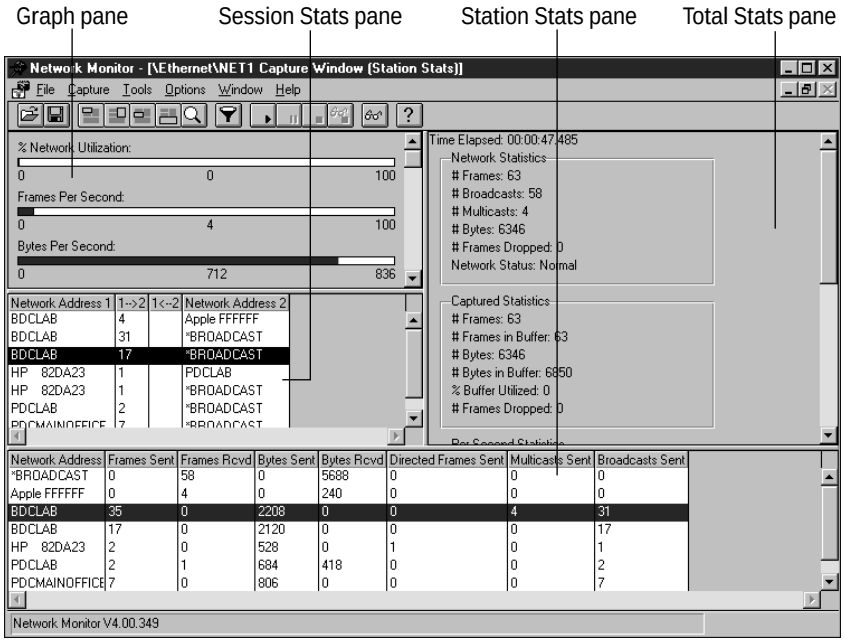


FIGURE 23-15 **The Network Monitor Capture Window dialog box**

Determining current network utilization

One way to determine the current utilization of a network segment is to start a capture in Network Monitor, and then watch the **%** Network Utilization bar graph in the Graph pane *during the entire capture period*. This graph displays only the most recent one-second's worth of network activity, so you must view it during the entire capture period to get a feel for overall network utilization. A high number on the graph (any number consistently over 50%) may indicate too many computers are on the segment being analyzed.

Another way to determine the overall utilization of a network segment during the entire capture period is to view the Network Statistics section in the Total Stats pane *after* the capture is completed. You can derive a great deal of information from the statistics displayed. For example, you can determine the average number of bytes transmitted per second by dividing the number of bytes shown by the number of seconds shown in the Time Elapsed statistic at the top of the Total Stats pane. If the average number of bytes per second is greater than 50 percent of the segment's total capacity (an Ethernet 10BaseT segment, for example,

has a maximum capacity of 10Mbps or 1,250,000 bytes per second), this may indicate too many computers are on the segment being analyzed.

Replacing network addresses with computer names

Sometimes analysis of data is simplified when you can easily identify the computer whose statistics are displayed in Network Monitor.

To view computers by their computer names instead of their network (MAC) addresses, first select Capture ➪ Find All Names in the Network Monitor Capture Window dialog box, as shown in Figure 23-16.

FIGURE 23-16 Finding NetBIOS names (computer names) in the captured data

A Find All Names dialog box appears, indicating how many NetBIOS (computer names) were found in the captured data. Click OK to replace the network addresses in the Session Stats and Station Stats panes with computer names.

note **Not *all* network addresses are replaced with computer names—only the network addresses whose associated computer names were transmitted and captured during the capture period will be replaced.**

Sorting columns to determine which computer is generating the most network traffic

You can sort any of the columns in the Session Stats and Station Stats panes to determine which computer is sending (or receiving) the most of a specific type of network traffic.

note **Sorting a column only produces a list of those computers whose packets were captured during the capture period. If you filtered the capture, some Network Monitor statistics, particularly the statistics in the Session Stats and Station Stats panes, are complete *only* for those computers, protocols, and byte patterns you specified for capture.**

Also, if you are *not* using Network Monitor in promiscuous mode, your capture data will *not* include all packets sent on the network segment.

For example, you can sort the Frames Sent column in the Station Stats pane to determine which computer on the network segment sent the most packets during the capture period. Similarly, you can sort the Broadcasts Sent column in the Station Stats pane to determine which computer sent the most broadcasts during the capture period. You can also sort the Frames Received column in the Station Stats pane to determine which computer received the most packets during the capture period. All the other columns can be sorted, as well, to determine which computer was responsible for generating the most bytes sent, most directed frames sent, most multicasts sent, and so forth.

To sort a column, right-click the column header (for example, Frames Sent). Select Sort Column from the menu that appears, as shown in Figure 23-17.

Network Monitor sorts the column in descending order, with the largest number appearing at the top of the column.

Using the Capture Summary Dialog Box

To access the Capture Summary dialog box select Capture ➪ Display Captured Data from the Network Monitor Capture Window (main dialog box).

The Network Monitor Capture Summary dialog box appears, as shown in Figure 23-18. Notice the dialog box lists, by frame number, all the packets captured by Network Monitor during the capture period.

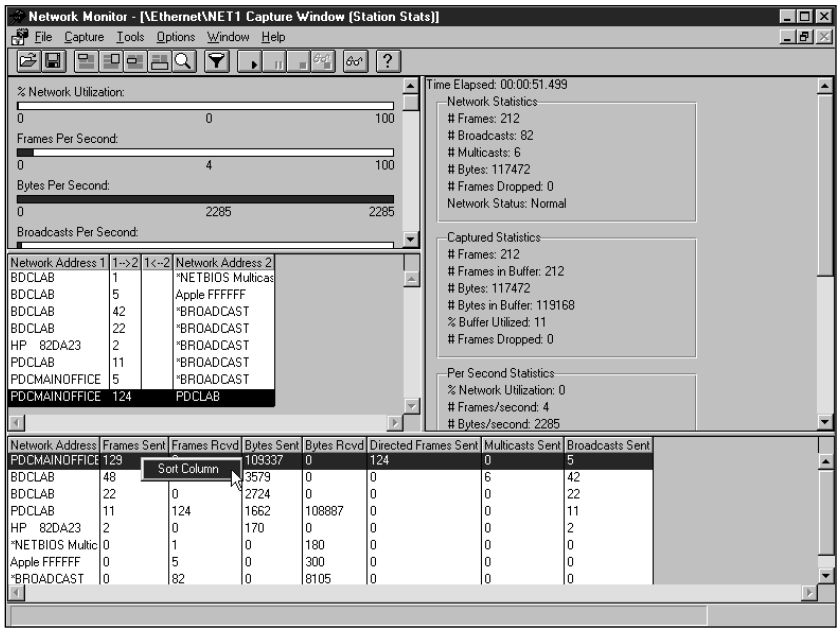


FIGURE 23-17 **Sorting a column in Network Monitor**

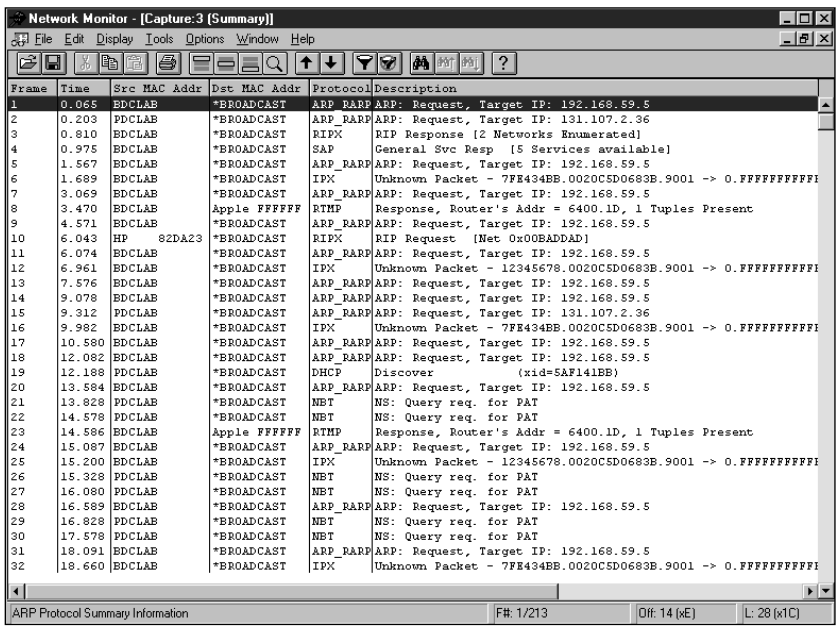


FIGURE 23-18 **The Capture Summary dialog box**

You can double-click any frame listed in this dialog box to obtain detailed information about the contents of that packet. Figure 23-19 shows the packet details view. Notice that middle pane in the dialog box shows protocol decode information, and the bottom pane shows, in hexadecimal, the entire contents of the packet.

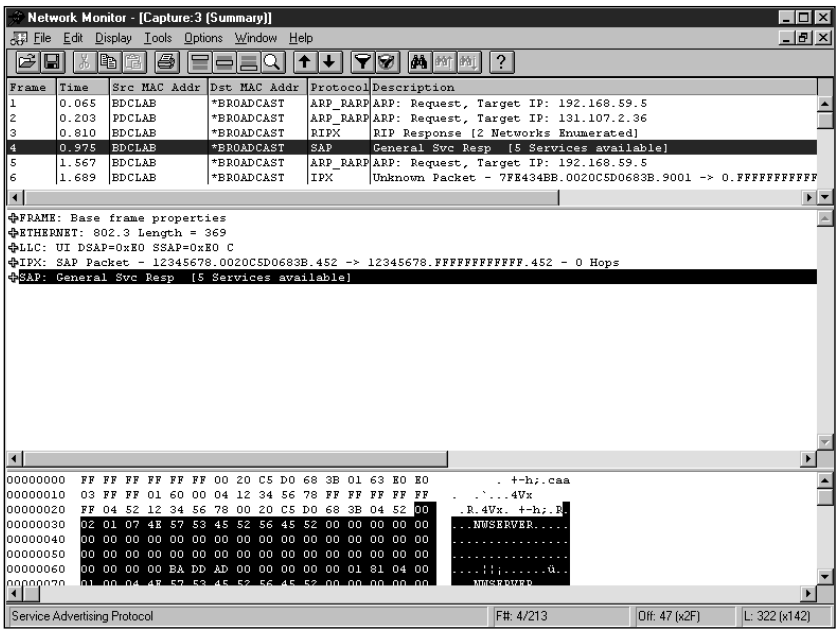


FIGURE 23-19 Viewing packet detail in the Capture Summary dialog box

Because a large number of packets may be displayed in the Capture Summary dialog box, you might want to use a display filter to limit the number of captured packets displayed.

Configuring a display filter

By default, Network Monitor's *display filter* is configured to display *all* packets captured in the Capture Summary dialog box. You can specify which captured packets will be displayed in this dialog box, however, by configuring a display filter.

You can configure a display filter so that:

- Only packets using certain protocols are (or are not) displayed
- Only packets to or from specified computers or network devices are (or are not) displayed

- Only packets containing specific byte patterns are displayed
- Any combination of the previous

For example, if you want to view all network packets containing browser information, you can configure a display filter so only packets containing the Browser protocol are displayed.

Likewise, if you are troubleshooting an IP address assignment problem, and your network uses DHCP to assign IP addresses, you can configure a display filter so only packets containing the DHCP protocol are displayed.

TO CONFIGURE A DISPLAY FILTER, FOLLOW THESE STEPS:

1. In the Network Monitor Capture Summary dialog box, select Display ➪ Filter. (Or press F8.)
2. The Display Filter dialog box appears, as shown in Figure 23-20. Notice the default settings. Configure the display filter as desired. Click OK.

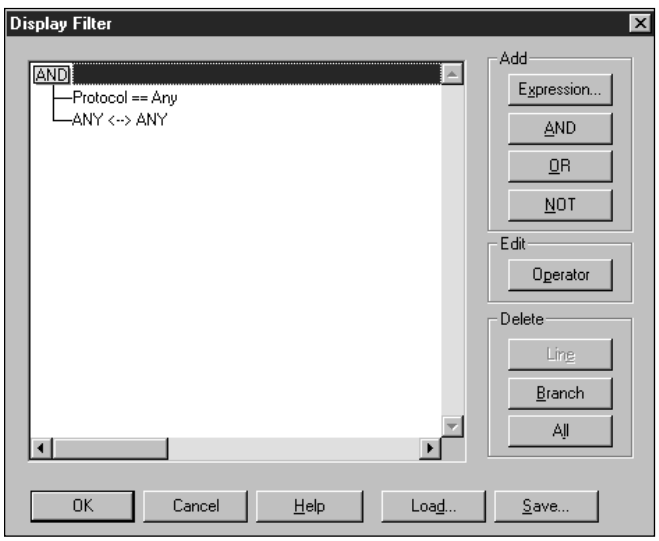


FIGURE 23-20 **Default display filter settings**

note Configuring a display filter is similar to configuring a capture filter. (The steps for configuring a capture filter are presented earlier in this chapter.)

Key Point Summary

Chapter 23 explored Network Monitor, a Windows NT Server administrative tool that enables you to capture, view, and analyze network packets. This packet analysis tool is useful in troubleshooting network problems and protocol problems. It can also be used to determine current network utilization, for trend analysis, and for network capacity planning.

- The version of Network Monitor that ships with Windows NT Server 4.0 is designed to capture only packets addressed to, or sent from, the Windows NT Server computer running Network Monitor. A more robust version of Network Monitor ships with Microsoft Systems Management Server. The main difference between the two versions in the ability of each product to use the promiscuous mode of the computer's network adapter: The NT Server 4.0 version, by default, *can't* be used in promiscuous mode; the Systems Management Server version, by default, *is* used in promiscuous mode.
- *Promiscuous* refers to a network adapter's ability to receive packets not addressed to that network adapter. A *non-promiscuous* network adapter can only receive packets addressed to that network adapter. A *promiscuous* network adapter can receive any packet transmitted on the local network segment.
- Network Monitor consists of two parts: the *Network Monitor Tools*, and the *Network Monitor Agent*. Both parts are installed together by using the Network application in Control Panel. Network Monitor requires a network adapter that uses an NDIS 4.0 driver.
- To access Network Monitor, from the Windows NT Server desktop, Select Start ➪ Programs ➪ Administrative Tools (Common) ➪ Network Monitor.
- The Network Monitor main dialog box is called the *Capture Window*, which contains four panes: the Graph pane, the Total Stats pane, the Session Stats pane, and the Station Stats pane.
- By default, the version of Network Monitor that ships with Windows NT Server 4.0 uses a special mode of the NDIS 4.0 driver, called "local capture only." Some NDIS 4.0 drivers don't correctly implement the "local capture only" mode. These drivers can capture packets sent *to* the Windows NT

Server computer, but *not* the packets sent *by* the Windows NT Server computer. To remedy this situation and to enable Network Monitor to capture packets both sent to and sent by the Windows NT Server computer, the Registry must be edited to configure Network Monitor to use the promiscuous mode of the NDIS 4.0 driver.

- A by-product of forcing Network Monitor to use promiscuous mode is Network Monitor can then capture *all* packets transmitted on the local network segment (instead of only packets addressed to or from the Windows NT Server computer on which Network Monitor is running).
- Network Monitor does *not* produce any statistics or other useful data until a capture is performed. During a capture, Network Monitor receives packets transmitted on the local network segment and stores these packets either in memory or in a capture file. Capture files can be used for later analysis. The process of capturing doesn't interfere with packets reaching their intended destinations on the network.
- To perform a capture, you must manually start and stop a capture in Network Monitor. You can either choose to view statistics in the Network Monitor Capture Window dialog box as they are gathered, or you can select the *Dedicated Capture Mode to not* view data while it is gathered and to ease processor load during the capture process.
- By default, Network Monitor's capture filter is configured to capture *all* packets addressed to or sent by the Windows NT Server computer. However, you can configure a capture filter to specify which packets transmitted on the network segment will be captured.
  - You can configure a *capture filte*r so that:
    - Only packets using certain protocols are (or are not) captured
    - Only packets to or from specified computers or network devices are (or are not) captured
    - Only packets containing specific byte patterns are captured
    - Any combination of the previous.
- After you finish performing a capture, you can save the captured data to a file for later analysis if you like.
- Two primary dialog boxes in Network Monitor are used to view captured data: the Capture Window dialog box, and the Capture Summary dialog box.

- The *Capture Window* dialog box (the Network Monitor main dialog box) displays general network activity statistics in its four panes. In addition to being able to determine current network utilization in this dialog box, you can replace network addresses with NetBIOS (computer names); this will make it easier to identify the computer whose statistics you are analyzing. You can also sort columns to determine which computer is sending (or receiving) the most of a specific type of network traffic.
- The *Capture Summary* dialog box displays a listing of all packets captured, and enables individual packet contents to be viewed and analyzed. This dialog box is useful for both capacity planning and troubleshooting. To access this dialog box, from the Network Monitor Capture Window (main dialog box) select Capture ≫ Display Captured Data.
- By default, Network Monitor's display filter is configured to display *all* packets that are captured in the Capture Summary dialog box. However, you can configure a display filter to specify which captured packets will be displayed in this dialog box.
- You can configure a display filter so that:
  - Only packets using certain protocols are (or are not) displayed
  - Only packets to or from specified computers or network devices are (or are not) displayed
  - Only packets containing specific byte patterns are displayed
  - Any combination of the previous
- To configure a display filter, in the Network Monitor Capture Summary dialog box, select Display ≫ Filter, or press F8. Configuring a display filter is similar to configuring a capture filter.

Applying What You've Learned

Now it's time to regroup, review, and apply what you've learned in this chapter.

The following Instant Assessment questions bring to mind key facts and concepts.

The hands-on lab exercise will reinforce what you've learned and give you an opportunity to practice some of the tasks tested by the Enterprise exam.

Instant Assessment

1. Which Windows NT packet analysis tool is useful for troubleshooting network problems and protocol problems; and also for determining current network utilization, trend analysis, and network capacity planning?
2. Define the term *promiscuous* as it refers to a network adapter.
3. Which two parts make up Network Monitor?
4. You want to install Network Monitor on your Windows NT Server computer. This computer already has the Network Monitor Agent installed. What must you do before you can install Network Monitor?
5. What hardware is specifically required to use Network Monitor?
6. How can you access Network Monitor from the NT Server desktop?
7. List the four panes found in the Network Monitor Capture Window dialog box.
8. Which special mode of the NDIS 4.0 driver does the Windows NT version of Network Monitor use, by default?
9. What must be performed *before* statistics can be displayed in Network Monitor?
10. By default, which packets are captured by Network Monitor?
11. What can you do if you want to specify or restrict the type of packets Network Monitor captures?
12. When configuring a capture filter, what types of criteria can you specify Network Monitor use to determine whether packets will be included in or excluded from capturing?
13. When can you save captured data to a file?
14. Which two dialog boxes in Network Monitor are the primary dialog boxes used to *view* captured packets?
15. You want to determine current network utilization. What are two ways you can do this by using Network Monitor?
16. How do you sort a column in the Capture Window dialog box?

17. You use Network Monitor to perform a capture and you are currently viewing the captured packets in the Capture Summary dialog box. You decide you *only* want to view packets containing the IPX protocol. What should you do to accomplish this?

T/F

18. Network Monitor is a Windows NT tool that ships with *both* Windows NT Workstation and Windows NT Server. _____

19. By default, the Windows NT version of Network Monitor is *not* used in promiscuous mode. _____

For answers to the Instant Assessment questions see Appendix D.

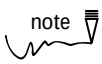
Hands-on Lab Exercise

The following hands-on lab exercise provides you with an opportunity to apply the knowledge you've gained in this chapter about Network Monitor.

Lab 23.36 *Installing and using Network Monitor*

Enterprise

The purpose of this hands-on lab exercise is to provide you with the experience of installing and using Network Monitor on a Windows NT Server computer.



***This lab is optional* because it requires that a network adapter be installed in your Windows NT Server computer. Also, if you have a second computer that is network-connected to your first computer, you can use this computer in Part 2 of this lab.**

This lab consists of two parts:

Part 1: Installing Network Monitor

Part 2: Using Network Monitor

Begin this lab by booting your computer to Windows NT Server. Log on as Administrator. Place your Windows NT Server compact disc in your computer's CD-ROM drive.

Complete the following steps carefully.

Part 1: Installing Network Monitor

In this section, you install Network Monitor on your Windows NT Server computer. Then you edit the Registry to force the network adapter in your computer to operate in promiscuous mode.

1. Select Start ➢ Settings ➢ Control Panel.
2. In the Control Panel dialog box, double-click the Network icon.
3. In the Network dialog box, click the Services tab.
4. On the Services tab, highlight Network Monitor Agent in the Network Services list box. Click the Remove command button.
5. A warning dialog box appears. Click the Yes command button to continue. Windows NT removes Network Monitor Agent.
6. On the Services tab, click the Add command button.
7. In the Select Network Service dialog box, highlight Network Monitor Tools and Agent. Click OK.
8. A Windows NT Setup dialog box appears. Ensure the correct path to your Windows NT Server source files (usually the `I386` folder on your Windows NT Server compact disc) is listed in the text box. Edit this text box if necessary. Click the Continue command button.
9. Windows NT copies source files and installs Network Monitor Tools and Agent.
10. The Network dialog box reappears. Click the Close command button.
11. Windows NT performs various bindings operations.
12. A Network Settings Change dialog box appears. Click the No command button.
13. Close Control Panel.
14. Select Start ➢ Run.
15. The Run dialog box appears. Type **regedt32** in the Open drop-down list box. Click OK.
16. The Registry Editor dialog box appears. Select Windows ➢ HKEY_LOCAL_MACHINE on Local Machine.
17. Double-click the + sign next to `SYSTEM`. Double-click the + sign next to `CurrentControlSet`. Double-click the + sign next to `Services`. Double-click the + sign next to `bh`. Highlight the `Linkage` folder.
18. Find the Bind value (located in the right-hand part of the dialog box). In the space provided, write the entry for the Bind value that directly follows the *first* \Device\ portion of the entry. (For example, Elnk31.).

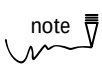
    _____

19. Highlight the `Parameters` folder.
20. Select Edit ➪ Add Key.
21. The Add Key dialog box appears. Type **ForcePmode** in the Key Name text box. Leave the Class text box blank. Click OK.
22. The Registry Editor dialog box reappears. Click the ForcePmode folder.
23. Select Edit ➪ Add Value.
24. The Add Value dialog box appears. In the Value Name text box, type the value you wrote in Step 18. For example, elnk31. In the Data Type drop-down list box, select REG_DWORD. Click OK.
25. The DWORD Editor dialog box appears. In the Data text box, type **1**. (Don't type the period at the end.) Click OK.
26. The Registry Editor dialog box reappears. Close the Registry Editor.
27. Select Start ➪ Shut Down.
28. In the Shut Down Windows dialog box, click the radio button next to "Restart the computer". Click the Yes command button.
29. Reboot your computer to Windows NT Server. Log on as Administrator.

Continue to Part 2.

Part 2: Using Network Monitor

In this section you use Network Monitor on your Windows NT Server computer to capture and view packets.



If you have a second computer and it is network-connected to your first computer, boot both computers before you do this part of the lab. (Boot the first [primary] computer to Windows NT Server, and boot the second computer to Windows NT Workstation.)

If you don't have a second computer, you can still do this part of the lab, but you won't be able to capture as much data.

1. Select Start ➪ Programs ➪ Administrative Tools (Common) ➪ Network Monitor.
2. The Network Monitor dialog box appears. Maximize this dialog box. Also maximize the Capture Window (Station Stats) within the Network Monitor dialog box.
3. Select Capture ➪ Filter.
4. A Capture Filter dialog box appears. Click OK.

5. The Capture Filter dialog box appears. Highlight the entry *under* AND (Address Pairs). Click the Line command button in the Delete section of this dialog box. (This allows Network Monitor to capture all packets transmitted on the local network segment.) Click OK.
6. The Network Monitor dialog box reappears. Select Capture ➢ Start to start capturing packets.
7. Wait approximately 1-2 minutes to allow Network Monitor time to capture data. While this process is taking place, notice the % Network Utilization, Frames Per Second, and Bytes Per Second bar graphs in the Network Monitor dialog box.
8. Select Capture ➢ Stop to stop capturing packets.
9. Select Capture ➢ Find All Names.
10. A Find All Names dialog box appears. Click OK.
11. To determine which computer is sending the most packets on the network segment, right-click Frames Sent (the Frames Sent column header) in the bottom section of the Network Monitor dialog box. Select Sort Column from the menu that appears. The computer on the network segment that sent the most packets during the capture period should appear at the top of the list in this section of the dialog box.
12. Right-click each of the other column headers (Frames Rcvd, Bytes Sent, Bytes Rcvd, Directed Frames Sent, Multicasts Sent, and Broadcasts Sent) and sort each column, one at a time. Notice the results of each sort.
13. Select Capture ➢ Display Captured Data.
14. The Capture (Summary) dialog box appears. Select Display ➢ Filter.
15. The Display Filter dialog box appears. Double-click Protocol == Any.
16. The Expression dialog box appears. Notice you can filter the display of captured packets by address, by protocol, or by protocol property. Click OK.
17. The Display Filter dialog box reappears. Click OK.
18. The Capture (Summary) dialog box reappears. Double-click any packet displayed in this dialog box to view its details. Do this several times.
19. When you are finished viewing packet details, exit Network Monitor.
20. A Save File dialog box appears. Click the No command button.
21. A Save Address Database dialog box appears. Click the No command button.