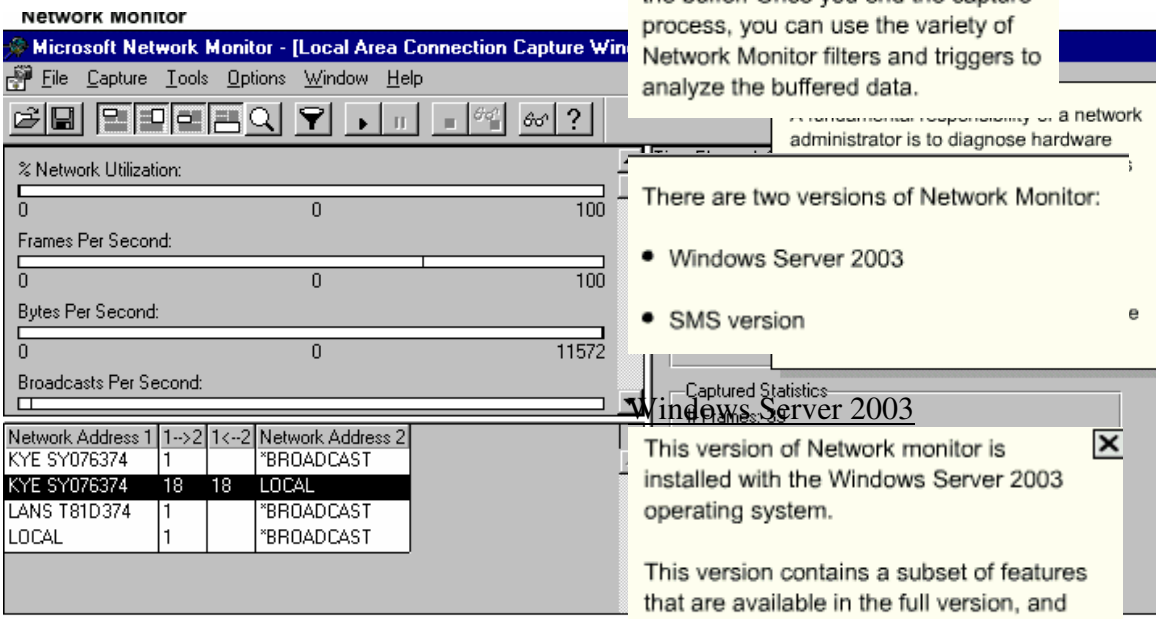
Monitoring Network traffic Section one

This topic covers the following points:

1. Network Monitor
2. Working with network captures
3. Configuring capture filters
4. Configuring display filters
5. Configuring triggers and parsers

Network Monitor uses an amount of RAM as its capture buffer.

When you instruct Network Monitor to start capturing frames to and from a computer, it copies any frame of data seen on the Network Interface Card (NIC) of that computer, and places it in the buffer. Once you end the capture process, you can use the variety of Network Monitor filters and triggers to analyze the buffered data.



a network administrator is to diagnose hardware

There are two versions of Network Monitor:

- Windows Server 2003
- SMS version

Windows Server 2003

This version of Network monitor is installed with the Windows Server 2003 operating system.

This version contains a subset of features that are available in the full version, and only allows you to capture traffic sent to or from the machine it is installed on.

Network Monitor is a network analyzer that captures frames of raw data that are transmitted and received on a computer. It also displays filtered frames and edits captured frames.

Once these frames have been captured, Network Monitor decodes them, and provides information about the frame, such as the

- type of packet
- source and destination address
- data contained in packet

SMS version

The SMS version of Network Monitor is part of the Microsoft Systems Management Server (SMS) product.

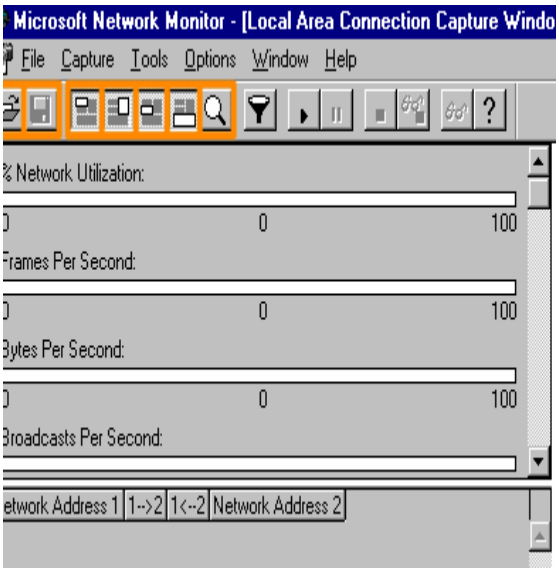
This version allows you to capture data from remote machines and also to capture all network traffic on a network segment using promiscuous mode.

Question

What are the functions of the Network Monitor shipped with Windows Server 2003?

1. Captures raw network traffic to and from the machine on which it's installed
2. Captures traffic from remote machines
3. Provides filters
4. Provides statistical data

Network Monitor captures raw network traffic and provides statistical data and filters.



Suppose you are the systems administrator for a global haulage company called Interswift. The company has offices in New York, and Seattle and Chicago, with a European branch in London. You work in the Interswift headquarters in New York.

The Interswift company network has been experiencing network connectivity problems. Some staff in the Sales department have not been able to access the Sales server. You have already installed Network Monitor on the server to diagnose the problem.

Select **Start - Administrative Tools - Network Monitor** to open the monitor.

The Network Monitor toolbar has buttons that you use to open and save capture files, and toggle the various viewing panes.

Capture button

You click the **Open Capture File** button to open and view a capture (.cap) file.

File Savae As button

You click the **File Save As** button to save captured data in a file so you can view in Network Monitor at a later time. You can also save a capture or display filter that yo have set up, and save frame data to a text file, which you can later print.

Toggle button

You click the **Toggle Graph Pane** button to toggle the Graph pane on and off.

Toggle Total Statistics Pane button

You click the **Toggle Total Statistics Pane** button to toggle the Toggle Total Statistics Pane on and off.

Toggle Session Statistics Pane

You click the **Toggle Session Statistics Pane** button to toggle the Toggle Session Statistics on and off.

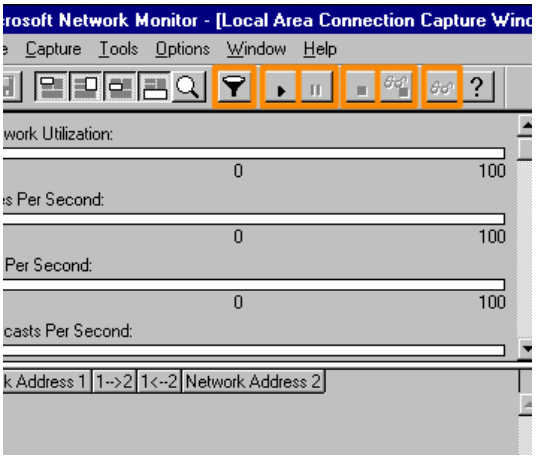
Toggle Station Statistics

You click the **Toggle Station Statistics Pane** button to toggle the Toggle Station Statistics Pane on and off.

Zoom button

You click the **Zoom Pane** button to obtain a larger view of the pane.

You use the remaining buttons in the Network Monitor toolbar to edit capture filters, to start, pause, and stop captures, and to view the captured data.



Edit capture filter

You click the **Edit Capture Filter** button to specify the protocols for Network Monitor to capture while your capture filter runs.

SAP or ETYPE protocols can be filtered in the capture filter.

Start Capture

You click the **Start Capture** button to start capturing network data frames.

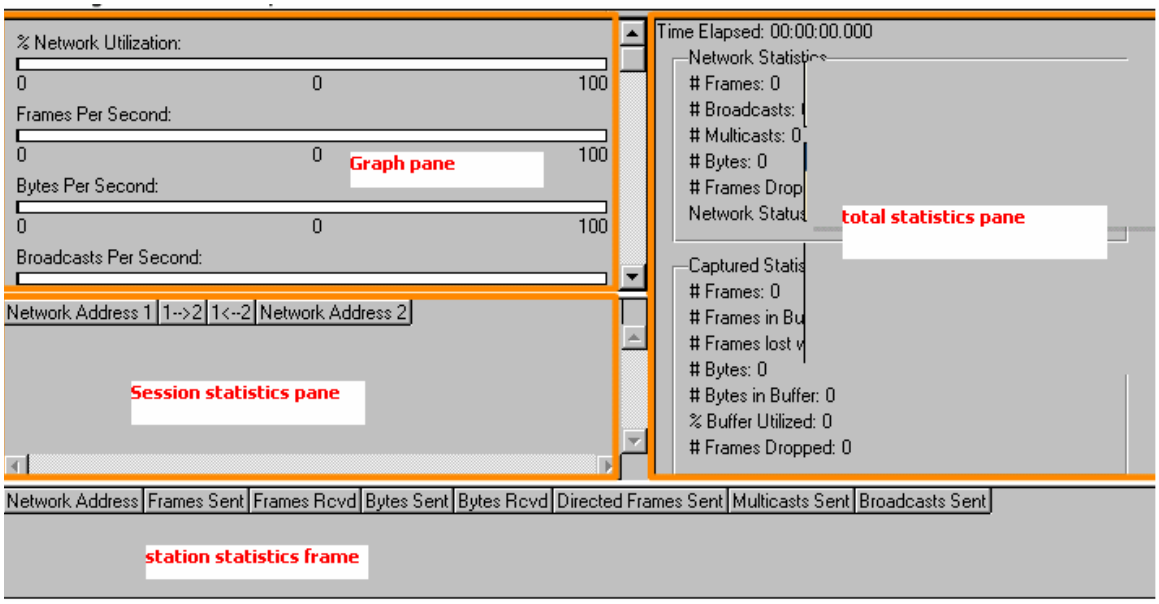
Pause Continue button

You click the **Pause/Continue Capture** button once to pause the capturing process and then you click it again to continue capturing network data frames.

Stop Capture button

You click the **Stop Capture** button to stop capturing network data frames.

Network Monitor is comprised of four panes:



Graph Pane

The Graph pane is on the upper-left corner of Network Monitor. It displays the current total capture statistics from the accumulated data in the form of bar graphs.

Station statistics

The Station Statistics frame is at the bottom of Network Monitor, and displays information about the computer's activity on the network.

Session statistics pane

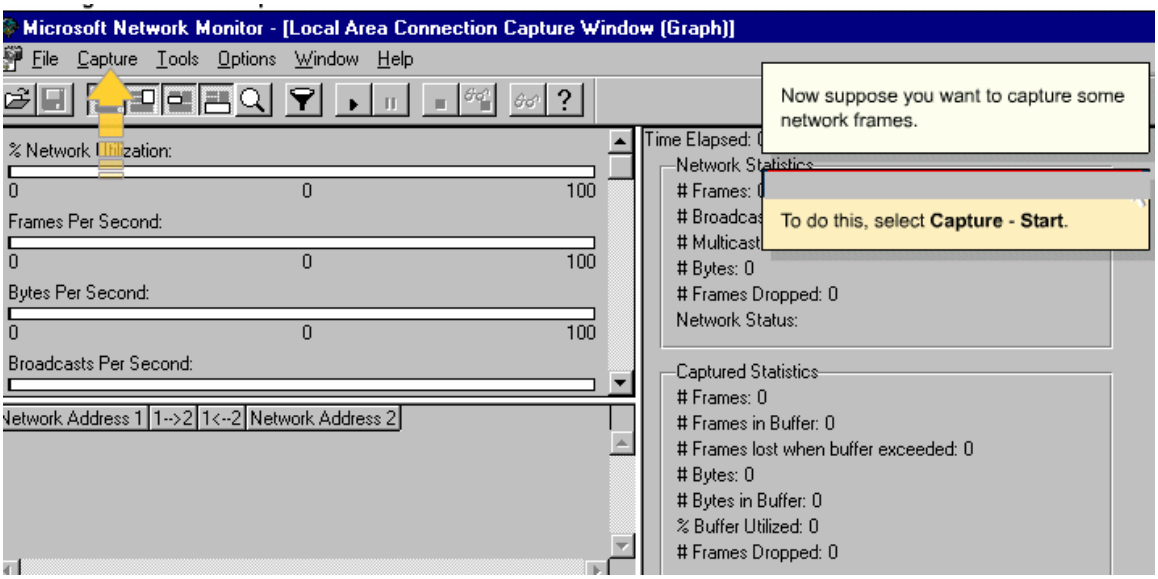
The Session Statistics pane is on the left-hand side of Network Monitor beneath the Graph pane. It displays the information collected about captured connections during the current capture session.

Source addresses, destination address, and amounts of data exchanged are displayed. This pane is continuously updated during the capture process.

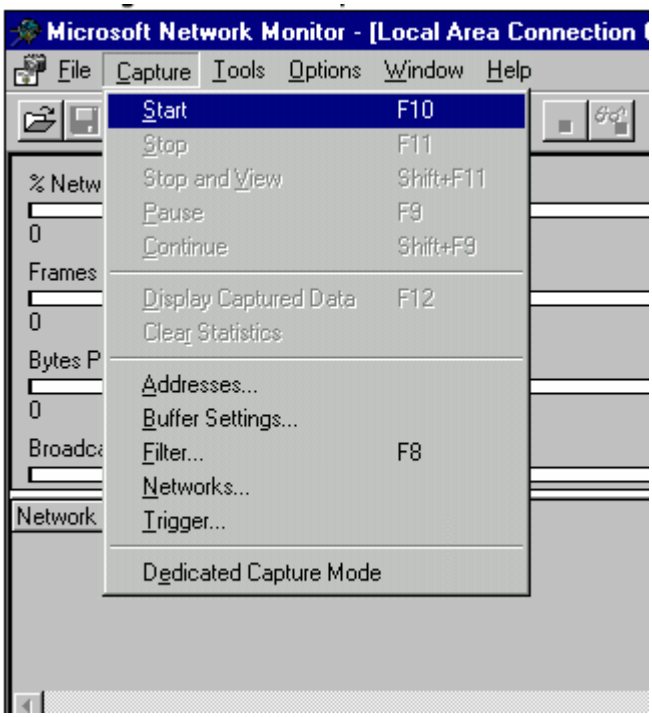
Total statistics pane

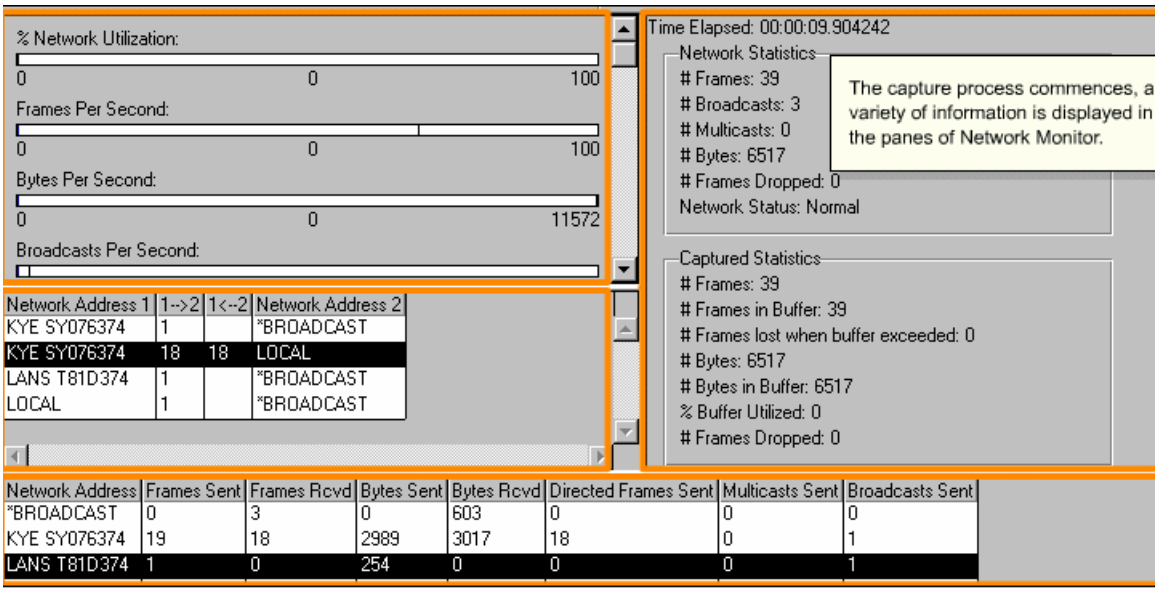
The Total Statistics pane is on the right-hand side of Network Monitor. It displays a summary of inbound and outbound traffic on the computer.

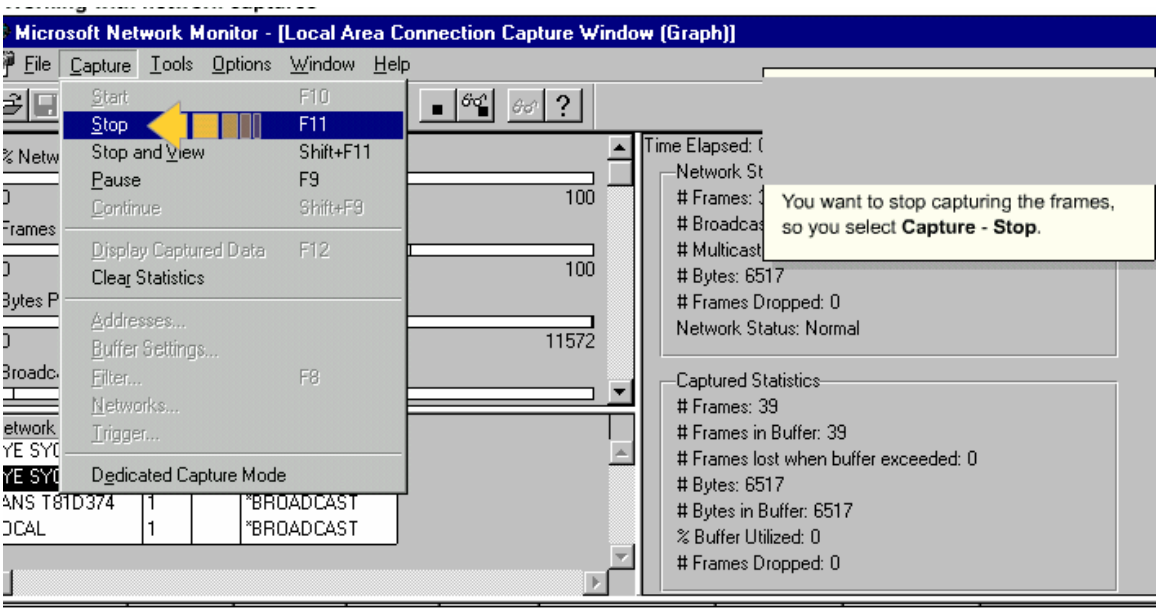
Statistics shown include number of unicast, broadcast, and multicast frames, and the amount of data contained in the buffer. This pane is continuously updated during the capture process.



Monitoring Network traffic Section one

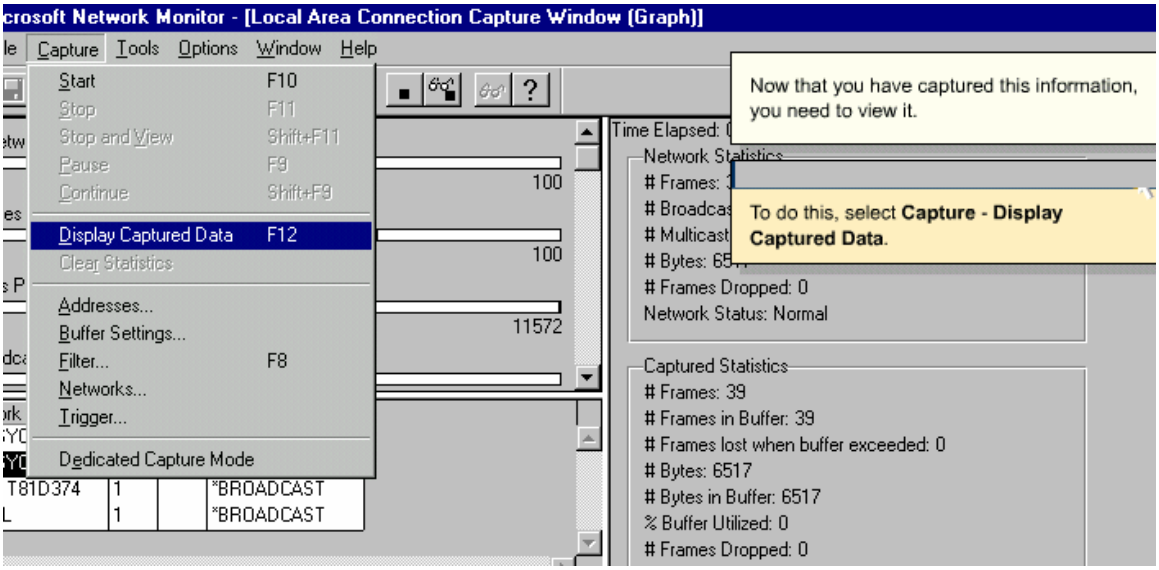






Note

To stop the capture process, you can also press the **Stop Capture** button or press **F11**.



Microsoft Network Monitor - [Capture: 6 (Summary)]

File Edit Display Tools Options Window Help

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
1	3.515055	KYE SY03A95B	*BROADCAST	ARP_RARP	ARP: Request, T
2	3.615199	KYE SY03A95B	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 192.168.1.201
3	7.791204	KYE SY03A95B	LOCAL	UDP	Src Port: Network Time Protocol (123);
4	7.801218	LOCAL	KYE SY03A95B	UDP	Src Port: Network Time Protocol (123);
5	20.259132	LANS T81D374	LOCAL	SMB	C echo, Repeat 1 times
6	20.259132	LOCAL	LAN:		e # = 1
7	20.369290	LANS T81D374	LOC.		A...., len: 0, seq:2
8	22.732688	KYE SY076374	LOC.		rk Time Protocol (123);
9	22.732688	LOCAL	KYE		rk Time Protocol (123);
10	37.734260	LOCAL	KYE		: call 0x40 opnum
11	37.734260	KYE SY076374	LOC.		e: call 0x40 conte
12	37.734260	KYE SY076374	LOC		call 0x44 opnum
13	37.764303	LOCAL	KYE SY076374	MSRPC	c/o RPC Response: call 0x44 conte
14	37.854432	LOCAL	KYE SY076374	TCP	Control Bits: .A...., len: 0, seq:4
15	37.884476	KYE SY076374	LOCAL	TCP	Control Bits: .A...., len: 0, seq:3
16	40.708536	LANS T81D374	LOCAL	UDP	Src Port: Network Time Protocol (123);
17	40.718551	LOCAL	LANS T81D374	UDP	Src Port: Network Time Protocol (123);
18	44.343764	KYE SY03A95B	*BROADCAST	BROWSER	Get Backup List Request [0x09]

The Frame Viewer window displays all the captured frames, and provides statistical information about each frame – its source and destination address, network type, time of capture, and protocol in use.

To see the full contents of an individual frame, you double-click it.

In this case, you double-click the first frame.

Microsoft Network Monitor - [Capture: 6 (Summary)]

File Edit Display Tools Options Window Help

The full contents of an individual frame are displayed in three panes.

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
1	3.515055	KYE SY03A95B	*BROADCAST	ARP_RARP	ARP: Reques
2	3.615199	KYE SY03A95B	*BROADCAST	ARP_RARP	ARP: Reques
3	7.791204	KYE SY03A95B	LOCAL	UDP	Sr
4	7.801218	LOCAL	KYE SY03A95B	UDP	Sr
5	20.259132	LANS T81D374	LOCAL	SMB	C
6	20.259132	LOCAL	LANS T81D374	SMB	R

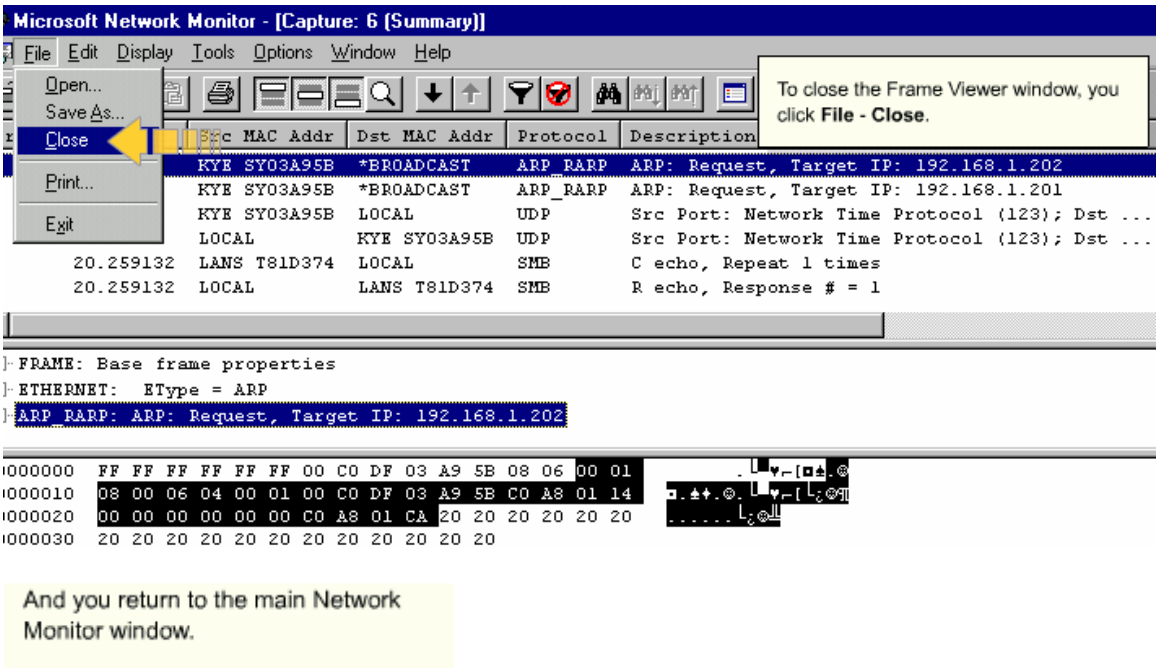
The Summary Pane displays the list of all captured frames. You can use a filter on this list to isolate certain frames.

```
FRAME: Base frame properties
ETHERNET:  EType = ARP
ARP_RARP: ARP: Request, Target IP: 192.168.1.202
```

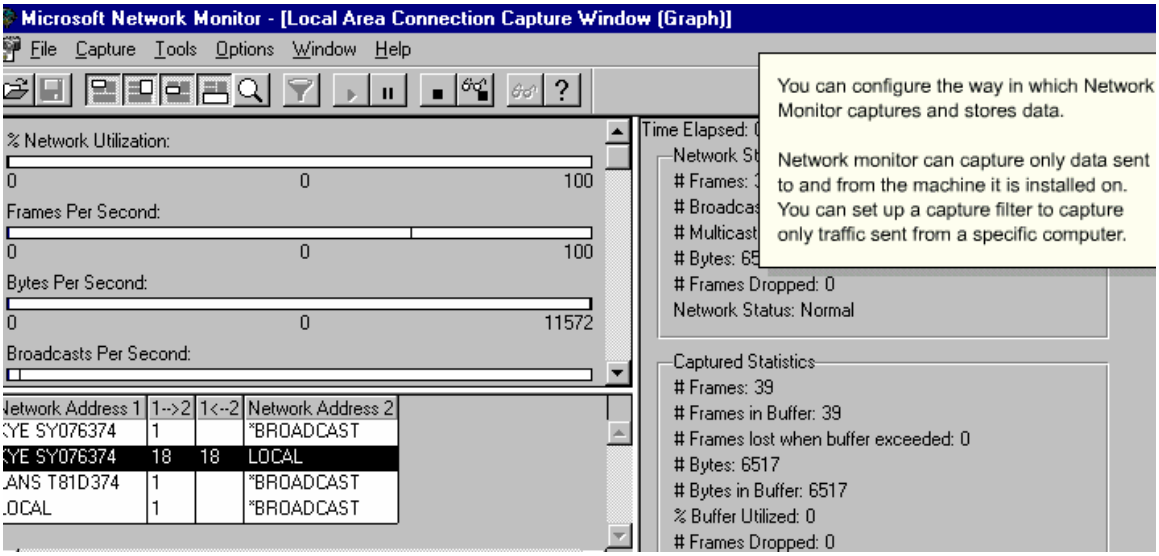
The Detail Pane shows information about the frame that is currently selected in the Summary Pane.

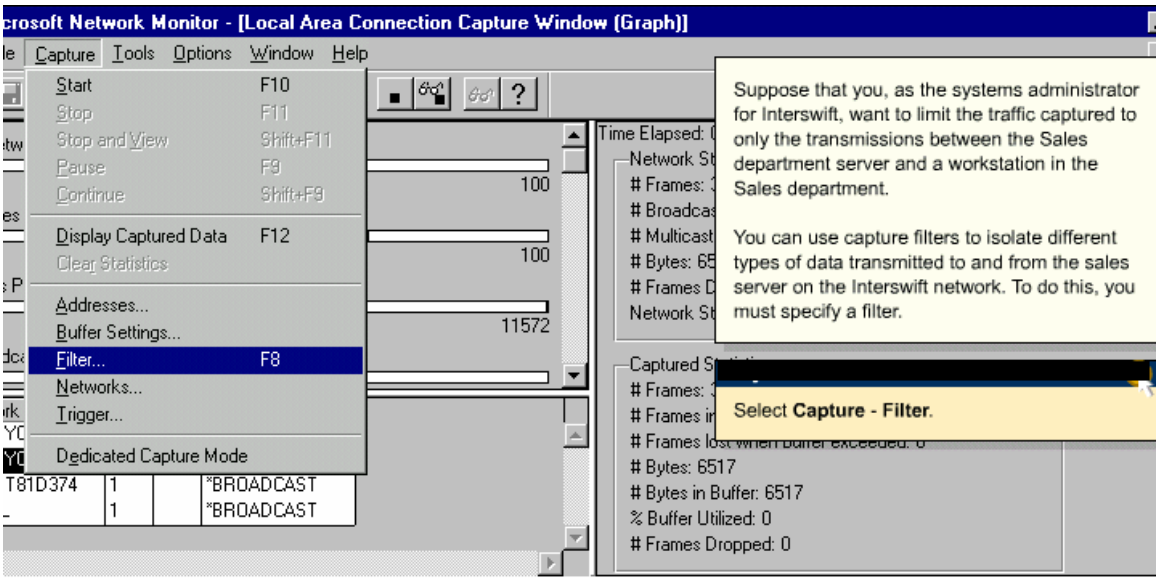
```
00000000  FF FF FF FF FF FF 00 C0 DF 03 A9 5B 08 06 00 0
00000010  08 00 06 04 00 01 00 C0 DF 03 A9 5B C0 A8 01 1
00000020  00 00 00 00 00 00 C0 A8 01 CA 20 20 20 20 20 2
00000030  20 20 20 20 20 20 20 20 20 20 20 20
```

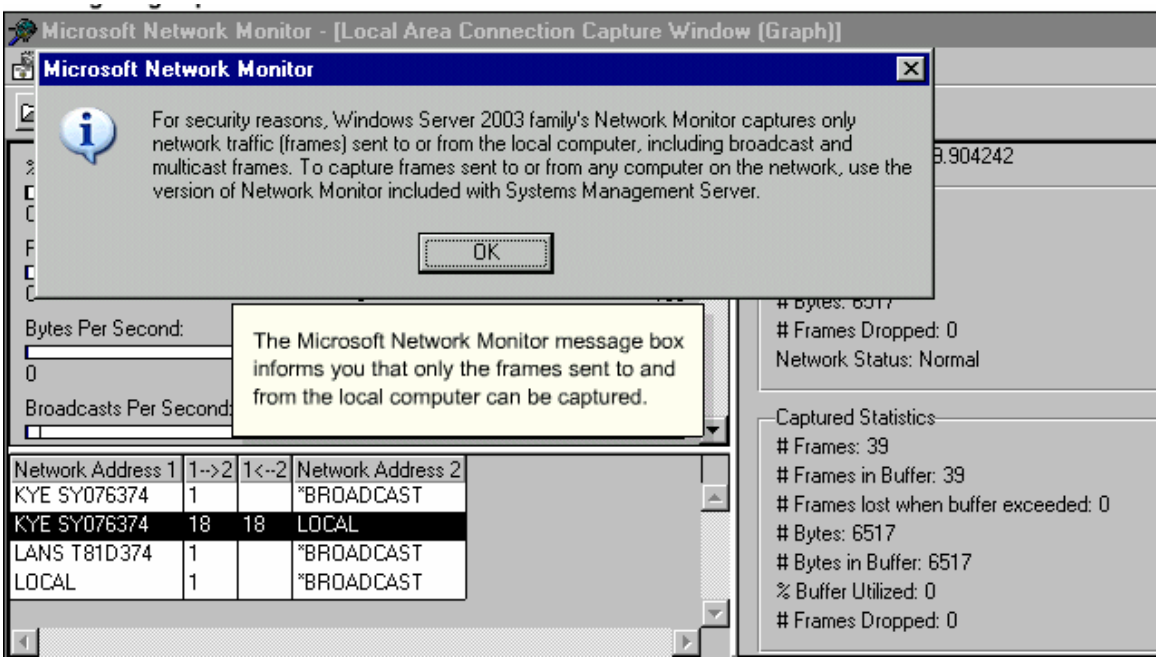
The Hexadecimal Pane contains two views – the actual data expressed in hexadecimal format, and the alphanumeric ASCII version of the frame.



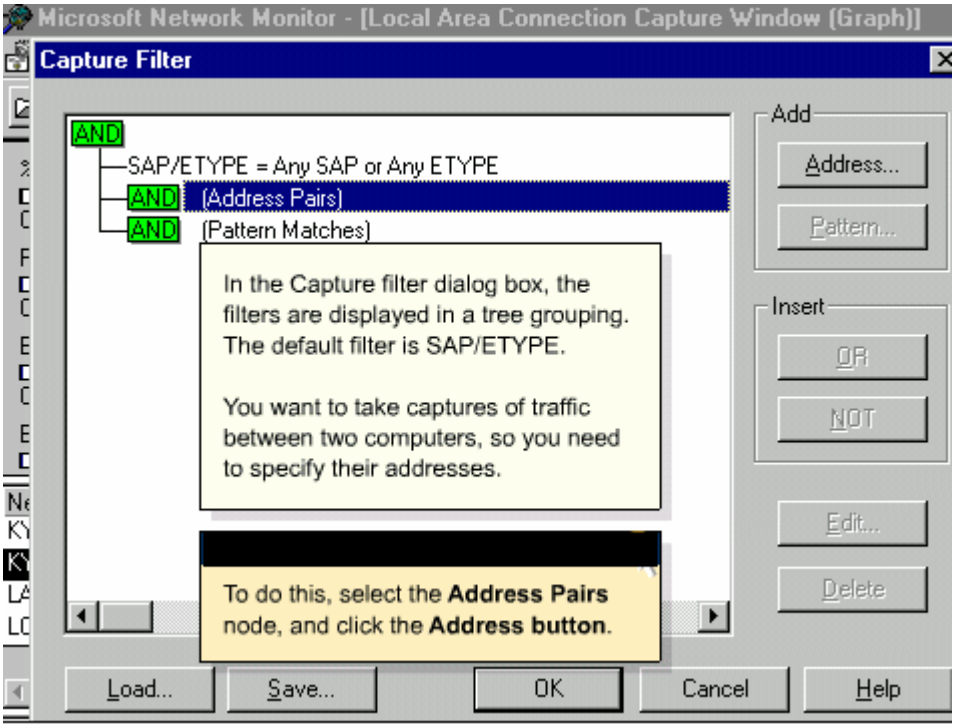
And you return to the main Network Monitor window.

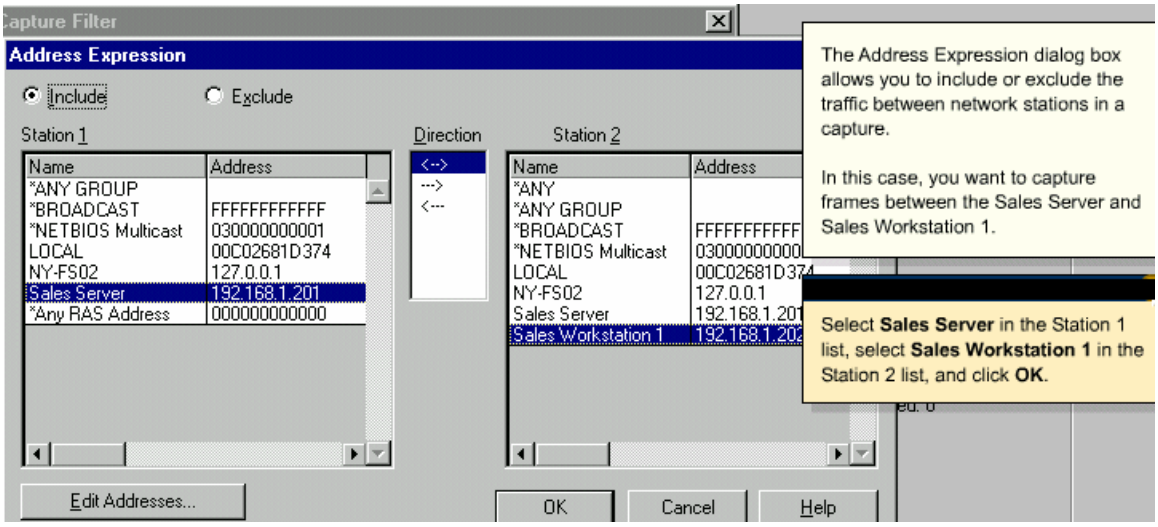


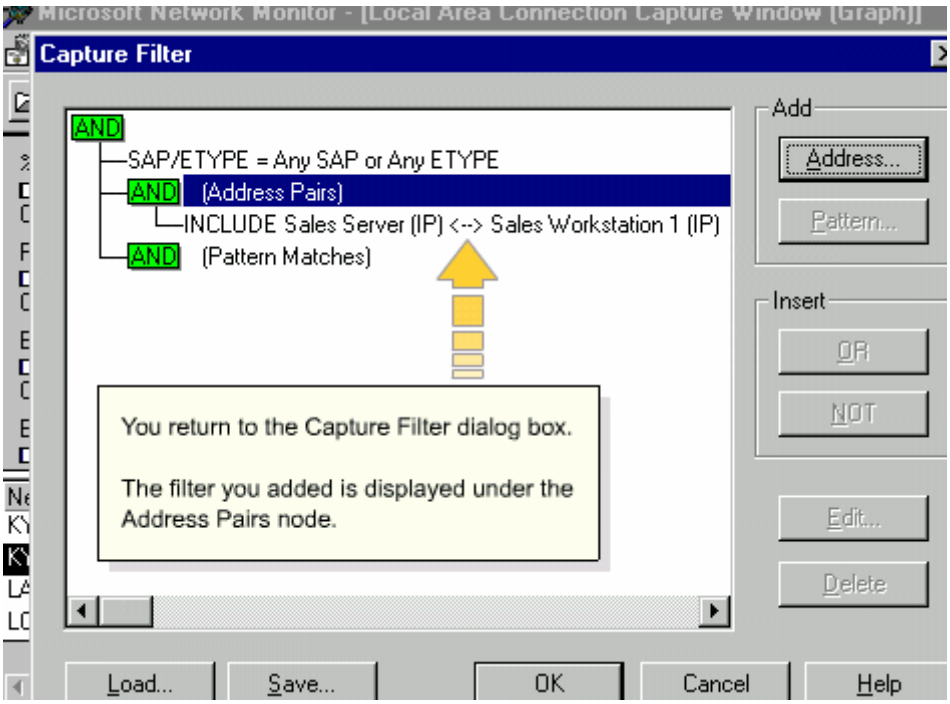




You click OK to close the message.


Microsoft Network Monitor - [Local Area Connection Capture Window (Graph)]
Capture Filter
AND
SAP/ETYPE = Any SAP or Any ETYPE
AND (Address Pairs)
AND (Pattern Matches)
In the Capture filter dialog box, the filters are displayed in a tree grouping. The default filter is SAP/ETYPE.
You want to take captures of traffic between two computers, so you need to specify their addresses.
To do this, select the Address Pairs node, and click the Address button.
Add
Address...
Pattern...
Insert
OR
NOT
Edit...
Delete
Load...
Save...
OK
Cancel
Help


Capture Filter
Address Expression
Include
Exclude
Station 1
Direction
Station 2
Name
Address
*ANY GROUP
*BROADCAST
*NETBIOS Multicast
LOCAL
NY-FS02
Sales Server
*Any RAS Address
Sales Workstation 1
The Address Expression dialog box allows you to include or exclude the traffic between network stations in a capture.
In this case, you want to capture frames between the Sales Server and Sales Workstation 1.
Select Sales Server in the Station 1 list, select Sales Workstation 1 in the Station 2 list, and click OK.
Edit Addresses...
OK
Cancel
Help



To confirm the addition you click OK

You are returned to the Network Monitor Window.

SkillCheck

Suppose you are the systems administrator for Interswift. You are experiencing some network connectivity problems between an Interswift (NY-FS01) DC, and a server in the New York domain (NY-FS02).

You have opened Network Monitor to see if you can diagnose the problem, and have accessed the Capture Filter dialog box.

To set up a filter that captures frames between NY-FS01, and NY-FS02, you select the **Address Pairs** node in the Capture Filter dialog box, and click the **Address** button in the Add section. In the Add Expression dialog box, you select **NY-FS01** in the Station 1 list, and select **NY-FS02** in the Station 2 list. Finally, you click **OK** twice.

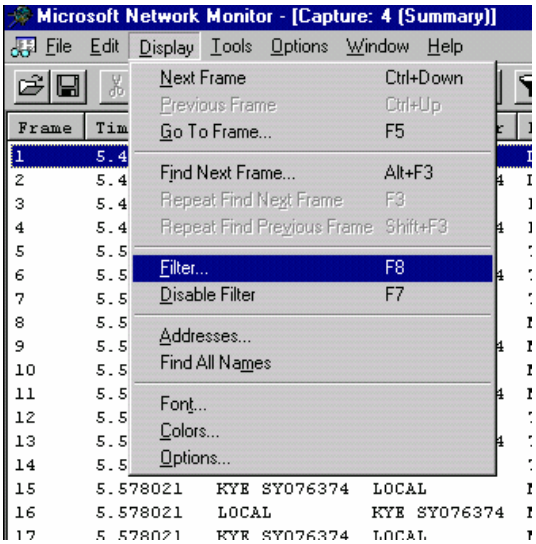
In addition to filtering which data to capture, you can also filter the information displayed in the viewing pane.

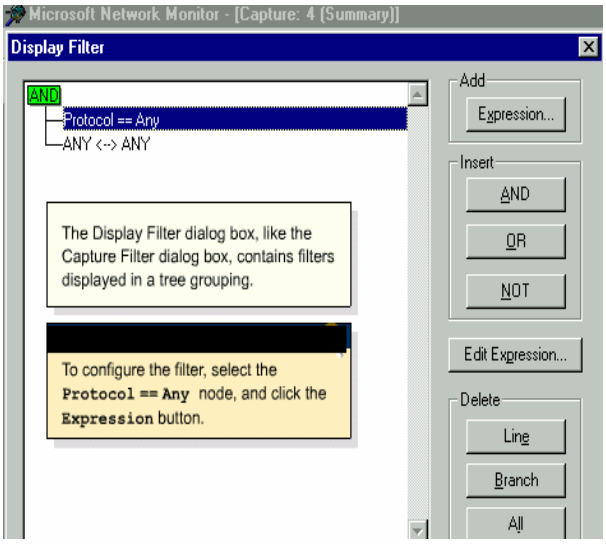
You use display filters to filter captured data. Like capture filters, they isolate specific types of information, but unlike capture filters, they filter data that has already been captured.

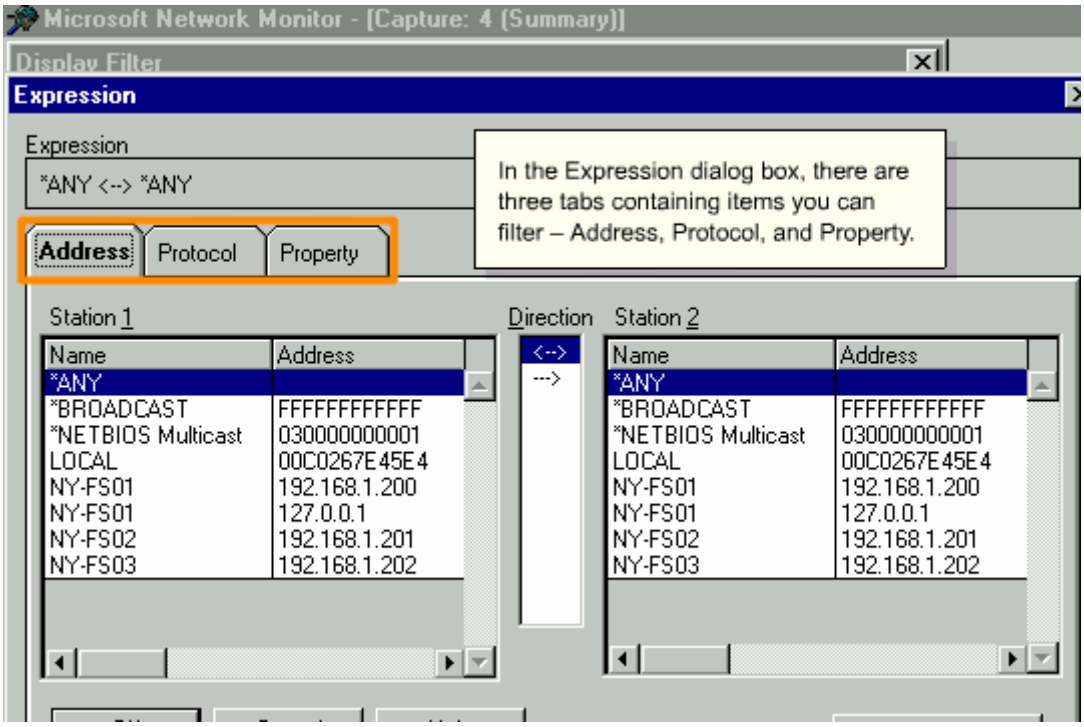
Suppose that you are trying to diagnose a problem between a user's workstation and a web server. You have captured traffic between the workstation and the server for the period of time the user was attempting to access a web page on the server.

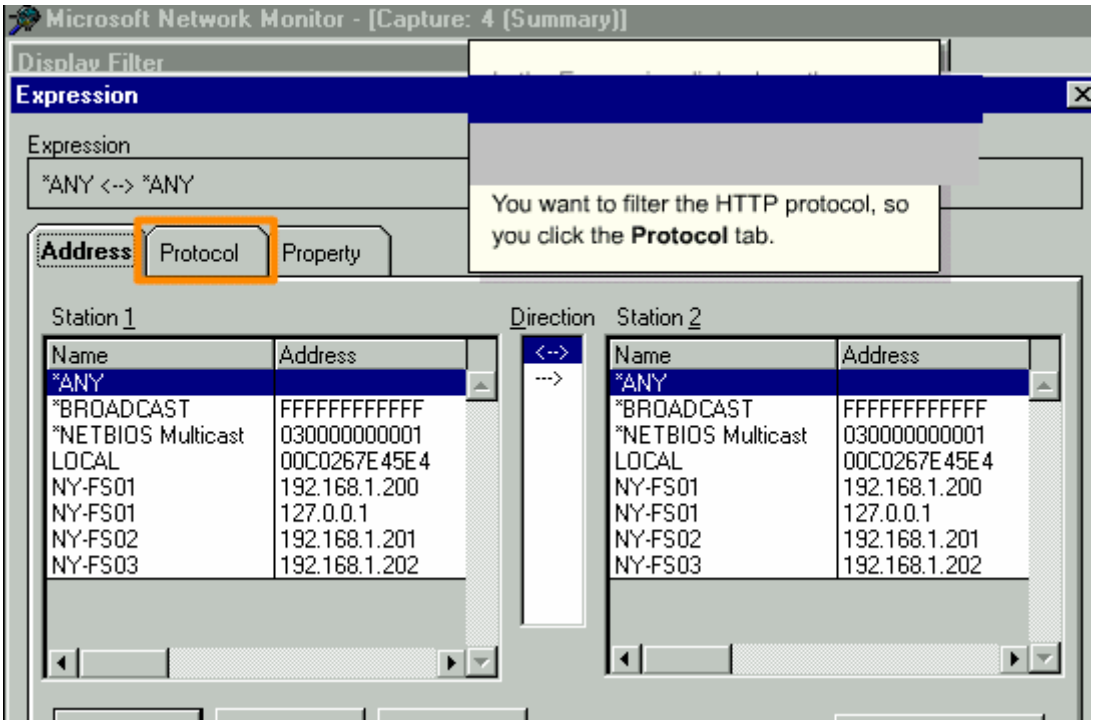
You want to filter the captured data so that only data relevant to web browsing is shown.

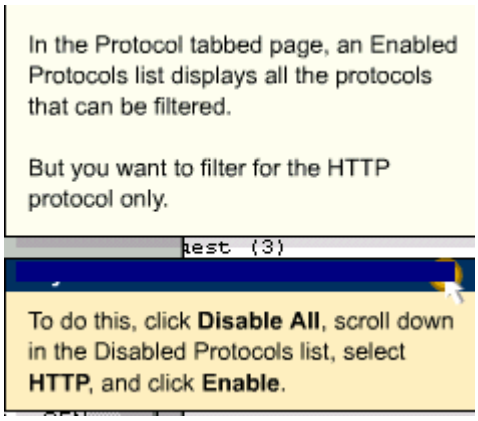
To configure a display filter, select **Display - Filter**.

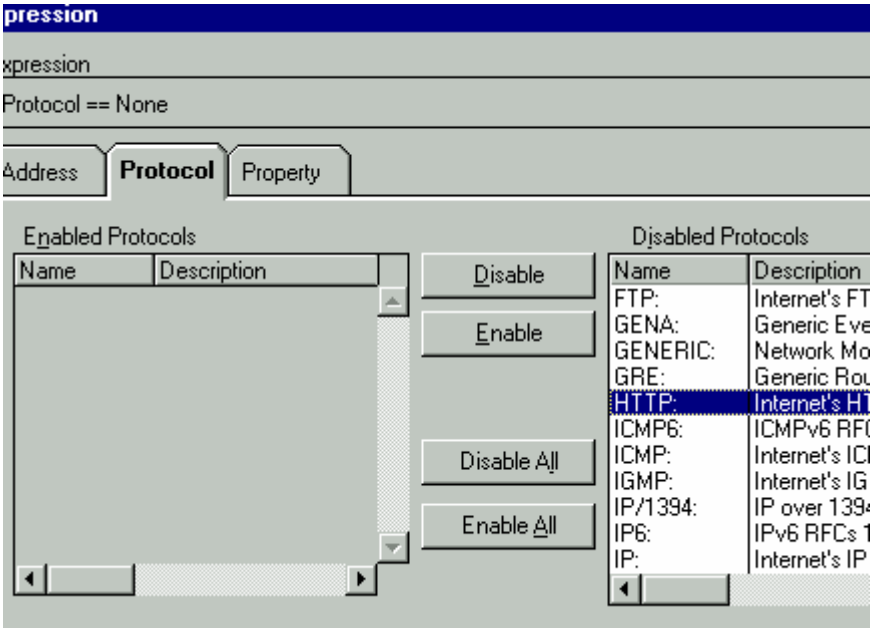

Microsoft Network Monitor - [Capture: 4 (Summary)]
File Edit Display Tools Options Window Help
Next Frame Ctrl+Down
Previous Frame Ctrl+Up
Go To Frame... F5
Find Next Frame... Alt+F3
Repeat Find Next Frame F3
Repeat Find Previous Frame Shift+F3
Filter... F8
Disable Filter F7
Addresses...
Find All Names
Font...
Colors...
Options...

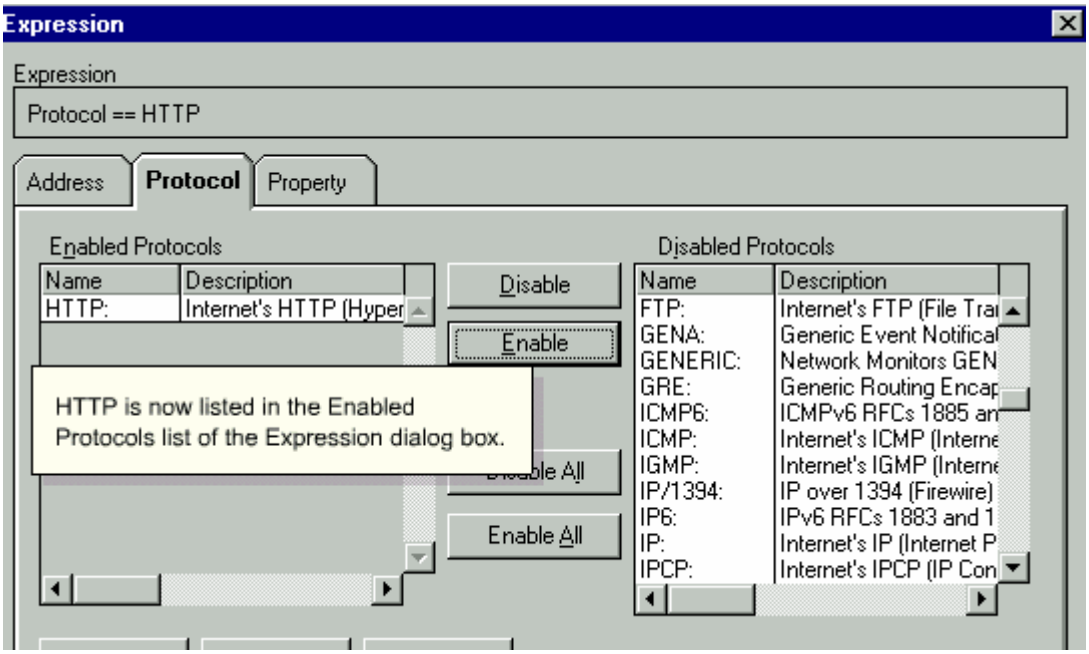

Microsoft Network Monitor - [Capture: 4 (Summary)]
Display Filter
AND
Protocol == Any
ANY <--> ANY
The Display Filter dialog box, like the Capture Filter dialog box, contains filters displayed in a tree grouping.
To configure the filter, select the Protocol == Any node, and click the Expression button.
Add
Expression...
Insert
AND
OR
NOT
Edit Expression...
Delete
Line
Branch
All

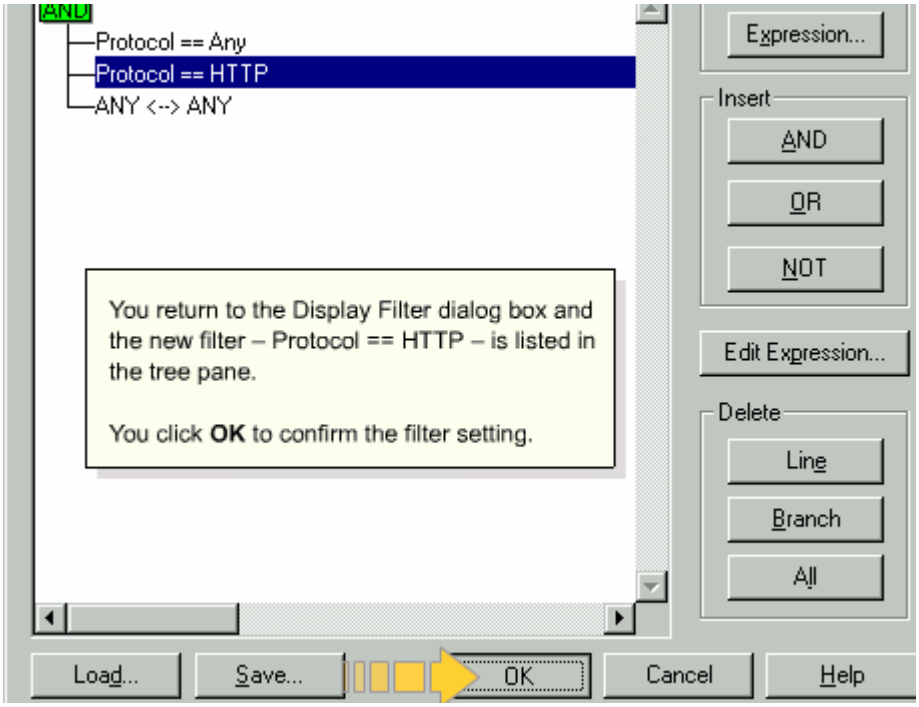

Microsoft Network Monitor - [Capture: 4 (Summary)]
Display Filter
Expression
Expression
*ANY <--> *ANY
In the Expression dialog box, there are three tabs containing items you can filter – Address, Protocol, and Property.
Address
Protocol
Property
Station 1
Direction
Station 2
Name Address
*ANY
*BROADCAST FFFFFFFFFFFF
*NETBIOS Multicast 030000000001
LOCAL 00C0267E45E4
NY-FS01 192.168.1.200
NY-FS01 127.0.0.1
NY-FS02 192.168.1.201
NY-FS03 192.168.1.202
<-->
-->

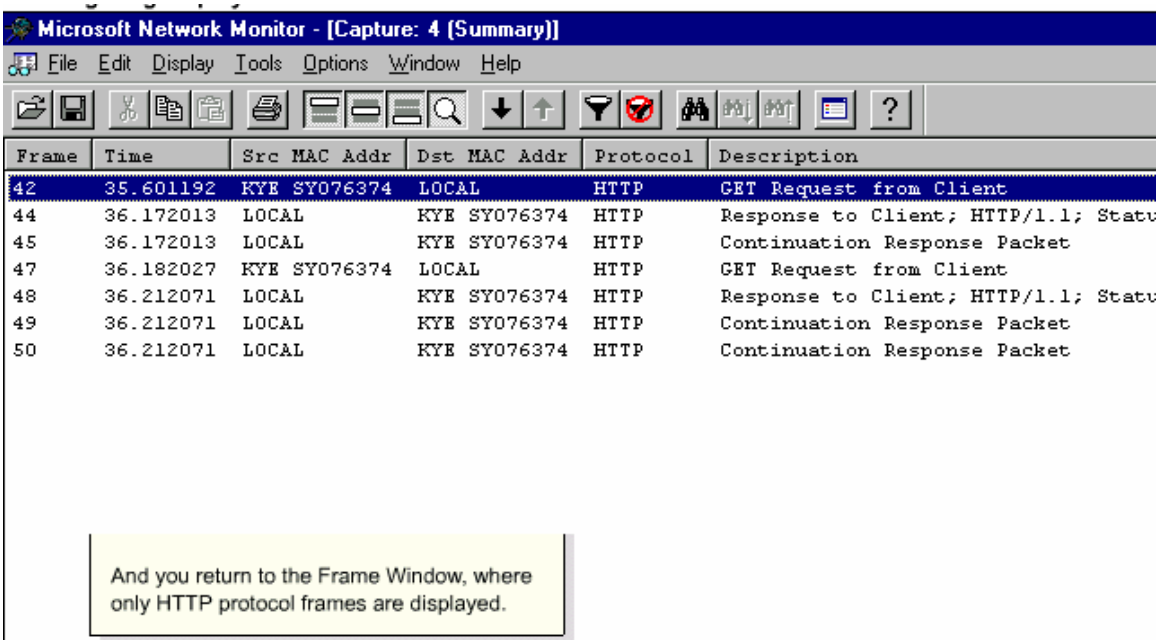

Microsoft Network Monitor - [Capture: 4 (Summary)]
Display Filter
Expression
Expression
*ANY <--> *ANY
You want to filter the HTTP protocol, so you click the **Protocol** tab.
Address
Protocol
Property
Station 1
Direction
Station 2
Name
Address
*ANY
*BROADCAST FFFFFFFFFFFF
*NETBIOS Multicast 030000000001
LOCAL 00C0267E45E4
NY-FS01 192.168.1.200
NY-FS01 127.0.0.1
NY-FS02 192.168.1.201
NY-FS03 192.168.1.202
<-->
-->

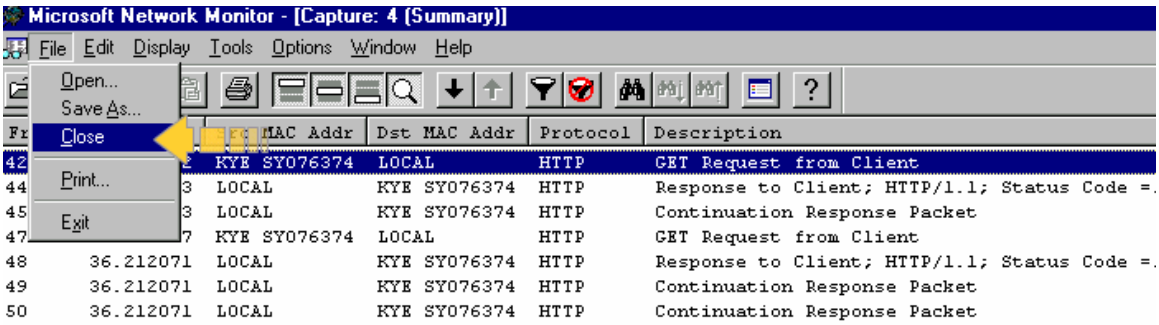

In the Protocol tabbed page, an Enabled Protocols list displays all the protocols that can be filtered.
But you want to filter for the HTTP protocol only.
To do this, click **Disable All**, scroll down in the Disabled Protocols list, select **HTTP**, and click **Enable**.


pression
xpression
Protocol == None
Address
Protocol
Property
Enabled Protocols
Name
Description
Disable
Enable
Disable All
Enable All
Disabled Protocols
Name
Description
FTP:
GENA:
GENERIC:
GRE:
HTTP:
ICMP6:
ICMP:
IGMP:
IP/1394:
IP6:
IP:

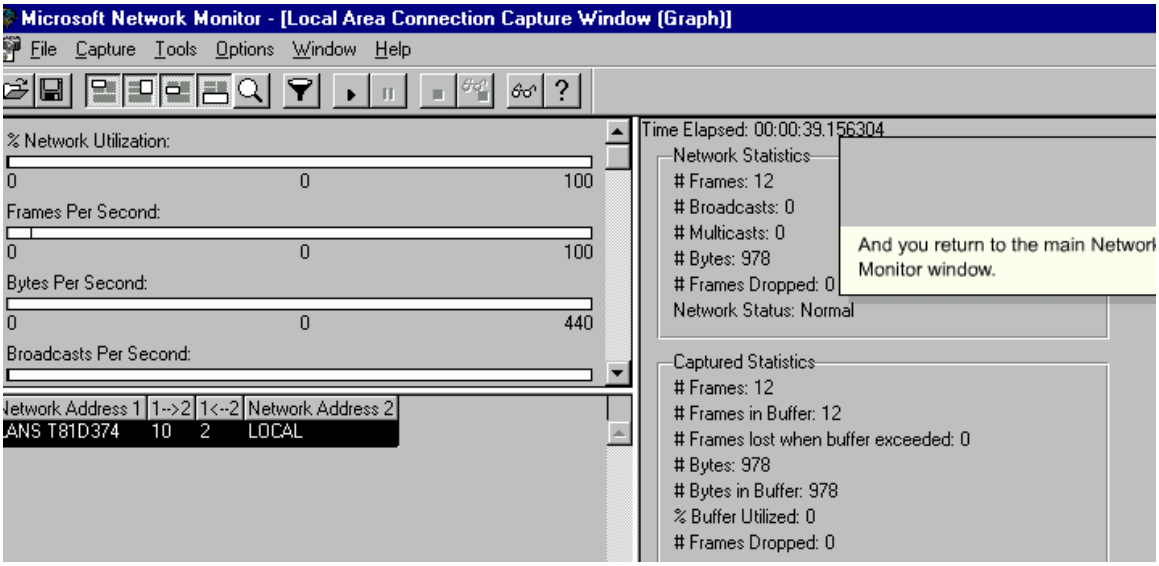

Expression
Expression
Protocol == HTTP
Address
Protocol
Property
Enabled Protocols
Name
Description
HTTP:
Internet's HTTP (Hyper
Disable
Enable
Enable All
HTTP is now listed in the Enabled Protocols list of the Expression dialog box.
Disabled Protocols
Name
Description
FTP:
GENA:
GENERIC:
GRE:
ICMP6:
ICMP:
IGMP:
IP/1394:
IP6:
IP:
IPCP:


AND
Protocol == Any
Protocol == HTTP
ANY <--> ANY
Expression...
Insert
AND
OR
NOT
Edit Expression...
Delete
Line
Branch
All
You return to the Display Filter dialog box and the new filter – Protocol == HTTP – is listed in the tree pane.
You click OK to confirm the filter setting.
Load...
Save...
OK
Cancel
Help


Microsoft Network Monitor - [Capture: 4 (Summary)]
File Edit Display Tools Options Window Help
Frame Time Src MAC Addr Dst MAC Addr Protocol Description
42 35.601192 KYE SY076374 LOCAL HTTP GET Request from Client
44 36.172013 LOCAL KYE SY076374 HTTP Response to Client; HTTP/1.1; Statu
45 36.172013 LOCAL KYE SY076374 HTTP Continuation Response Packet
47 36.182027 KYE SY076374 LOCAL HTTP GET Request from Client
48 36.212071 LOCAL KYE SY076374 HTTP Response to Client; HTTP/1.1; Statu
49 36.212071 LOCAL KYE SY076374 HTTP Continuation Response Packet
50 36.212071 LOCAL KYE SY076374 HTTP Continuation Response Packet
And you return to the Frame Window, where only HTTP protocol frames are displayed.



To close the Frame viewer window, you click **File - Close**.



And you return to the main Network Monitor window.

SkillCheck

Suppose you are the administrator for Interswift. You have been experiencing some connectivity-based problems in your network, and you want to isolate some network traffic to diagnose the problem.

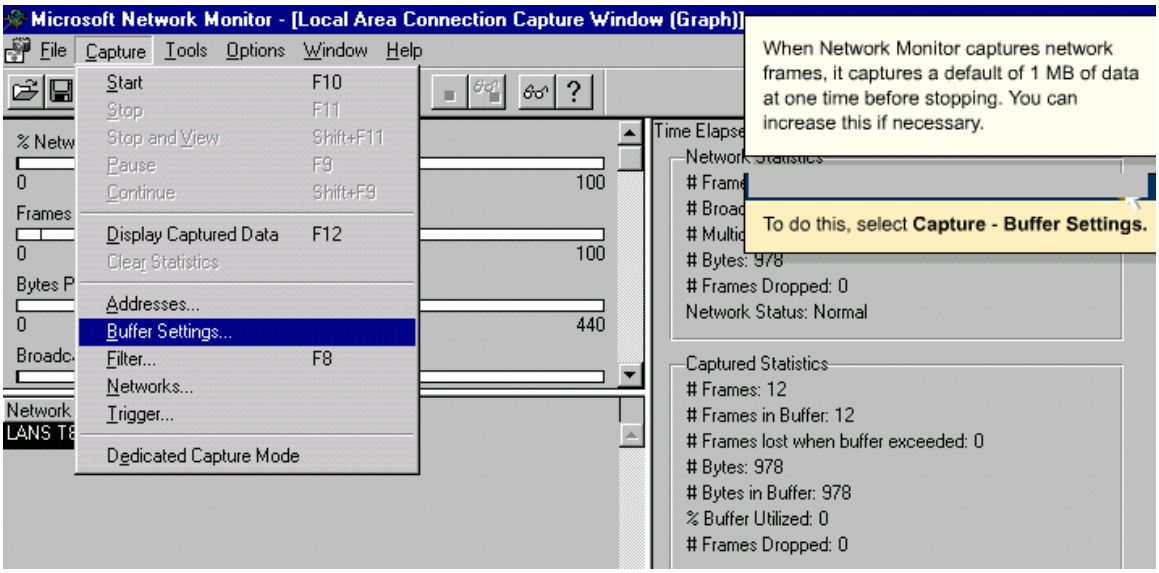
To do this, you must specify a capture filter.

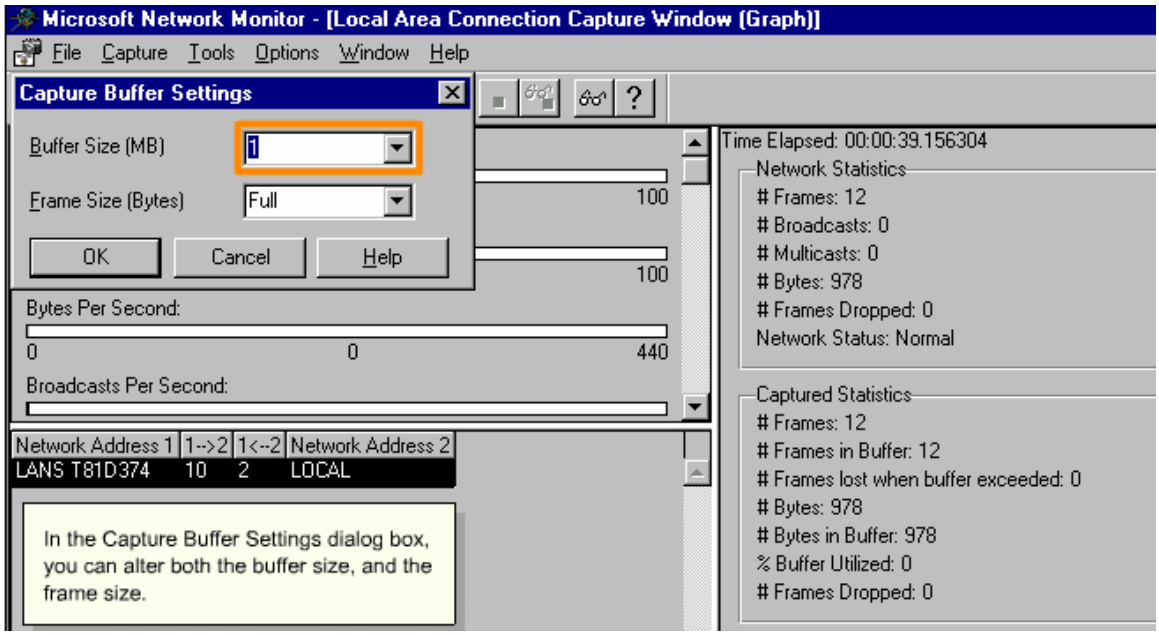
You select **Capture - Filter** in Network Monitor to specify a capture filter.

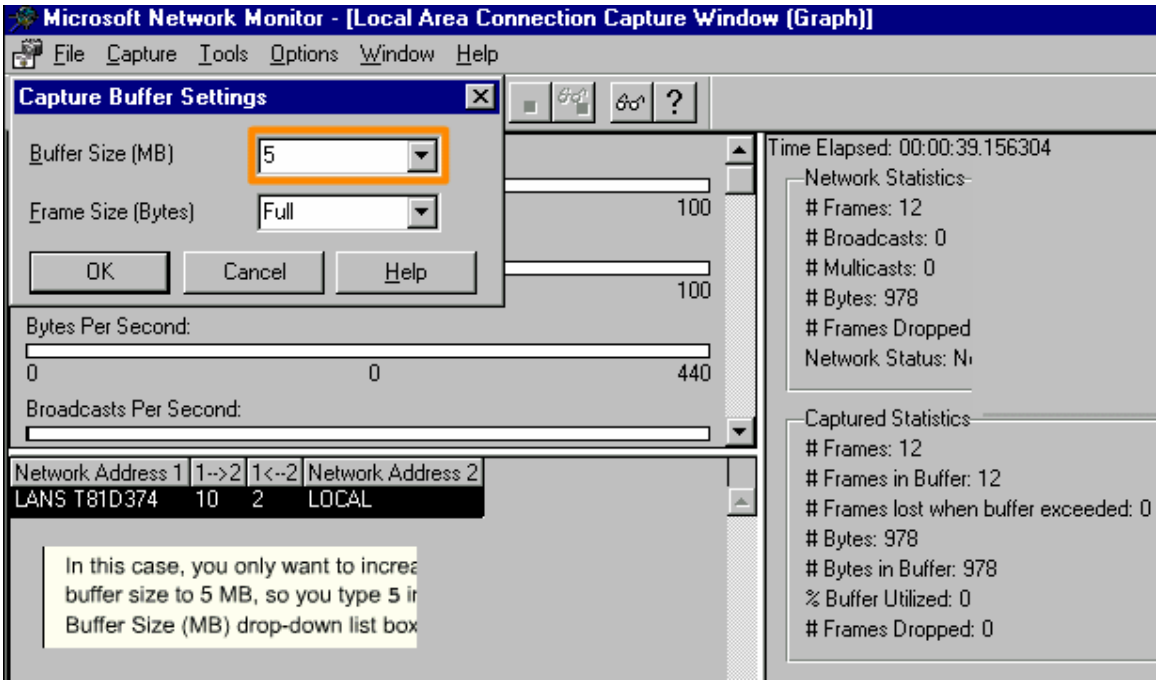
SkillCheck

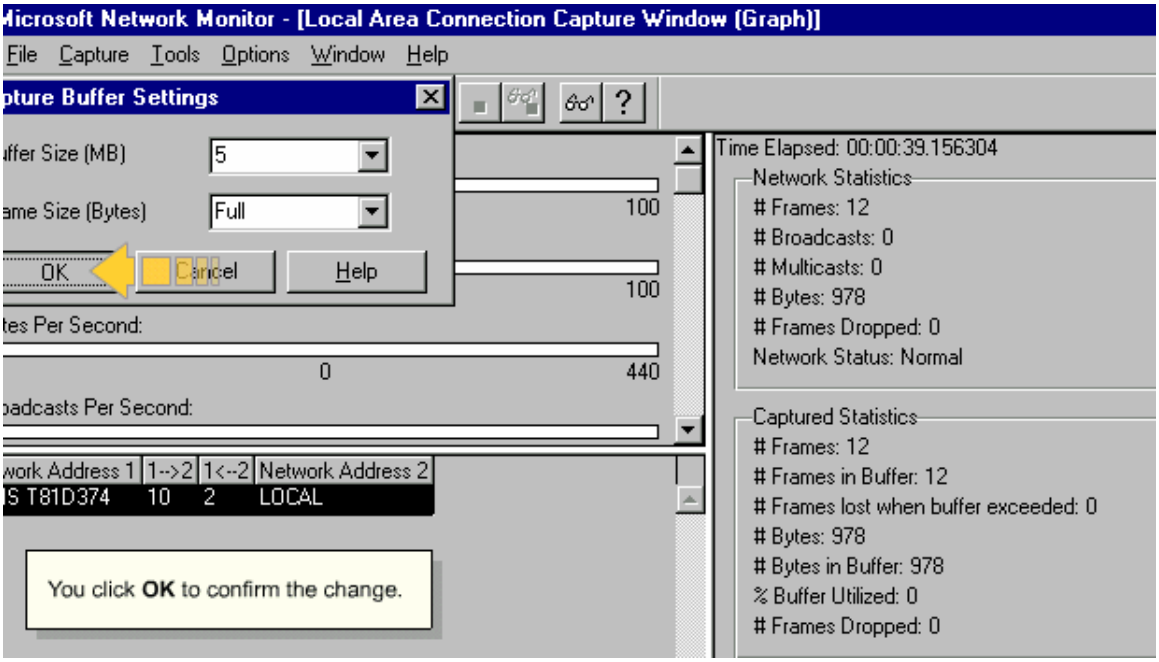
Suppose a department in Interswift's New York headquarters has not been able to access the local web server. You have configured a filter that captures frames sent between the web server and a workstation in the department. You have captured some frames, and now want to filter them to display only ones using HTTP. You have already accessed the Display Filter dialog box.

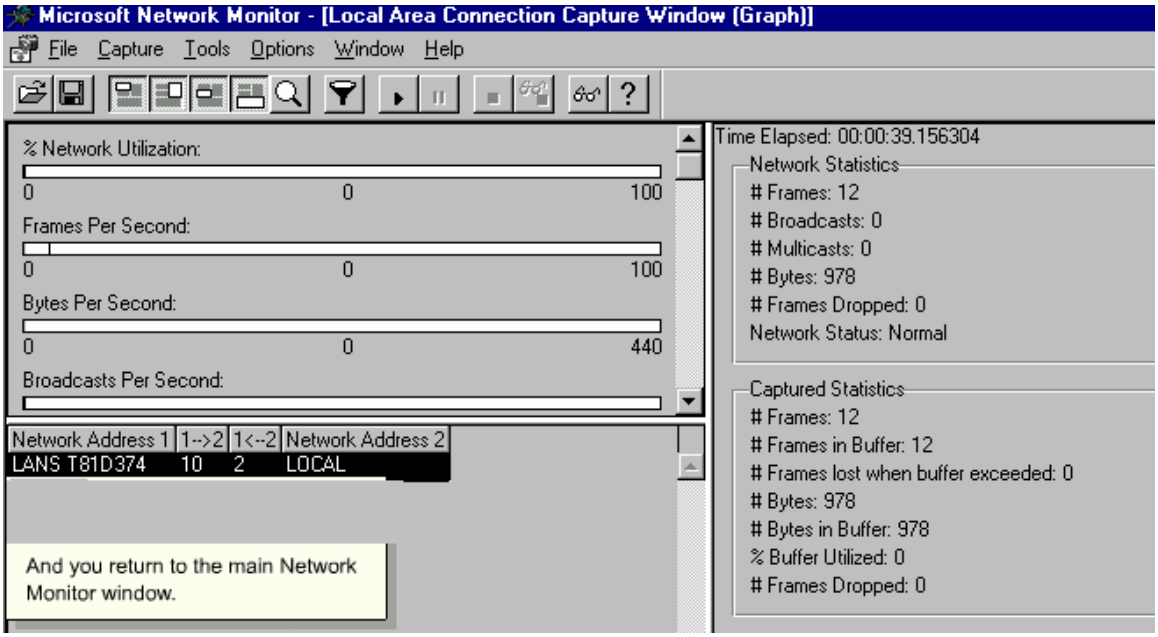
To filter and display only the frames using HTTP protocol, you select the **Protocol == Any** node in the Display Filter dialog box, and click **Expression**. In the Expression dialog box, you select the **Protocol** tab. You click **Disable All**, then select **HTTP** in the Disabled Protocols list, and click **Enable**. Then click **OK** twice.


Microsoft Network Monitor - [Local Area Connection Capture Window (Graph)]
File Capture Tools Options Window Help
Start F10
Stop F11
Stop and View Shift+F11
Pause F9
Continue Shift+F9
Display Captured Data F12
Clear Statistics
Addresses...
Buffer Settings...
Filter... F8
Networks...
Trigger...
Dedicated Capture Mode
When Network Monitor captures network frames, it captures a default of 1 MB of data at one time before stopping. You can increase this if necessary.
To do this, select Capture - Buffer Settings.
Frames Dropped: 0
Network Status: Normal
Captured Statistics
Frames: 12
Frames in Buffer: 12
Frames lost when buffer exceeded: 0
Bytes: 978
Bytes in Buffer: 978
% Buffer Utilized: 0
# Frames Dropped: 0


Microsoft Network Monitor - [Local Area Connection Capture Window (Graph)]
File Capture Tools Options Window Help
Capture Buffer Settings
Buffer Size (MB) 1
Frame Size (Bytes) Full
OK Cancel Help
Bytes Per Second:
Broadcasts Per Second:
Network Address 1 1-->2 1<--2 Network Address 2
LANS T81D374 10 2 LOCAL
In the Capture Buffer Settings dialog box, you can alter both the buffer size, and the frame size.
Time Elapsed: 00:00:39.156304
Network Statistics
Frames: 12
Broadcasts: 0
Multicasts: 0
Bytes: 978
Frames Dropped: 0
Network Status: Normal
Captured Statistics
Frames: 12
Frames in Buffer: 12
Frames lost when buffer exceeded: 0
Bytes: 978
Bytes in Buffer: 978
% Buffer Utilized: 0
# Frames Dropped: 0


Microsoft Network Monitor - [Local Area Connection Capture Window (Graph)]
File Capture Tools Options Window Help
Capture Buffer Settings
Buffer Size (MB)
5
Frame Size (Bytes)
Full
OK
Cancel
Help
100
100
Bytes Per Second:
0
0
440
Broadcasts Per Second:
Network Address 1 1-->2 1<--2 Network Address 2
LANS T81D374 10 2 LOCAL
In this case, you only want to increa
buffer size to 5 MB, so you type 5 i
Buffer Size (MB) drop-down list box
Time Elapsed: 00:00:39.156304
Network Statistics
Frames: 12
Broadcasts: 0
Multicasts: 0
Bytes: 978
Frames Dropped
Network Status: N
Captured Statistics
Frames: 12
Frames in Buffer: 12
Frames lost when buffer exceeded: 0
Bytes: 978
Bytes in Buffer: 978
% Buffer Utilized: 0
# Frames Dropped: 0


icrosoft Network Monitor - [Local Area Connection Capture Window (Graph)]
File Capture Tools Options Window Help
pture Buffer Settings
ffer Size (MB)
5
ame Size (Bytes)
Full
OK
Cancel
Help
100
100
tes Per Second:
0
440
adcasts Per Second:
work Address 1 1-->2 1<--2 Network Address 2
S T81D374 10 2 LOCAL
You click OK to confirm the change.
Time Elapsed: 00:00:39.156304
Network Statistics
Frames: 12
Broadcasts: 0
Multicasts: 0
Bytes: 978
Frames Dropped: 0
Network Status: Normal
Captured Statistics
Frames: 12
Frames in Buffer: 12
Frames lost when buffer exceeded: 0
Bytes: 978
Bytes in Buffer: 978
% Buffer Utilized: 0
# Frames Dropped: 0



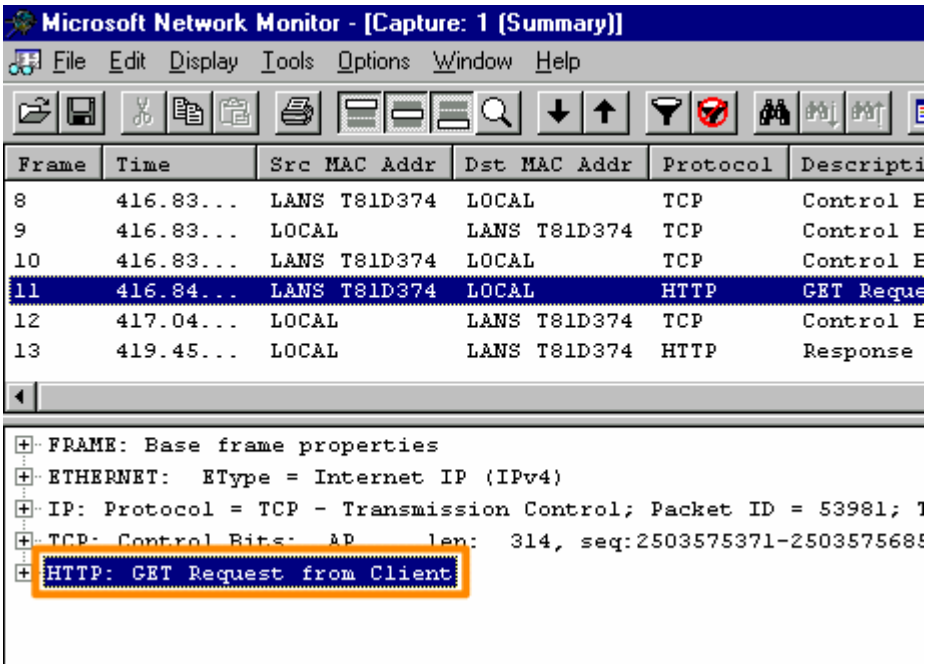
If you create capture triggers, Network Monitor can respond to events on your network. You can set triggers to alert you or to stop capturing when the buffer space has filled to a certain level.

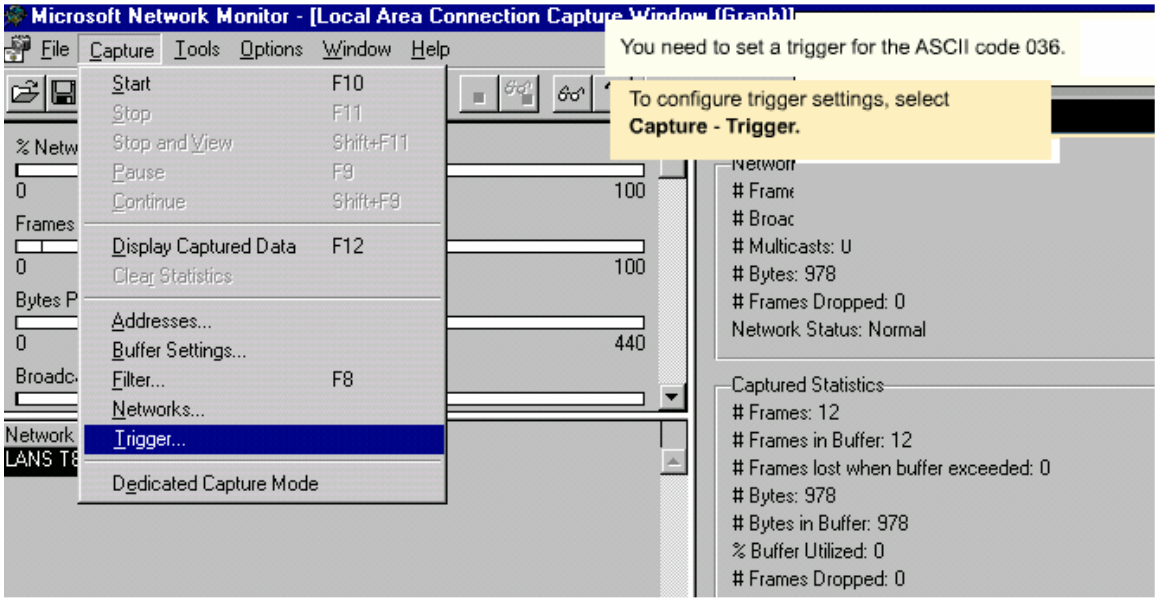
You can also set a trigger to stop capturing when a certain sequence of characters appears in the network frames received.

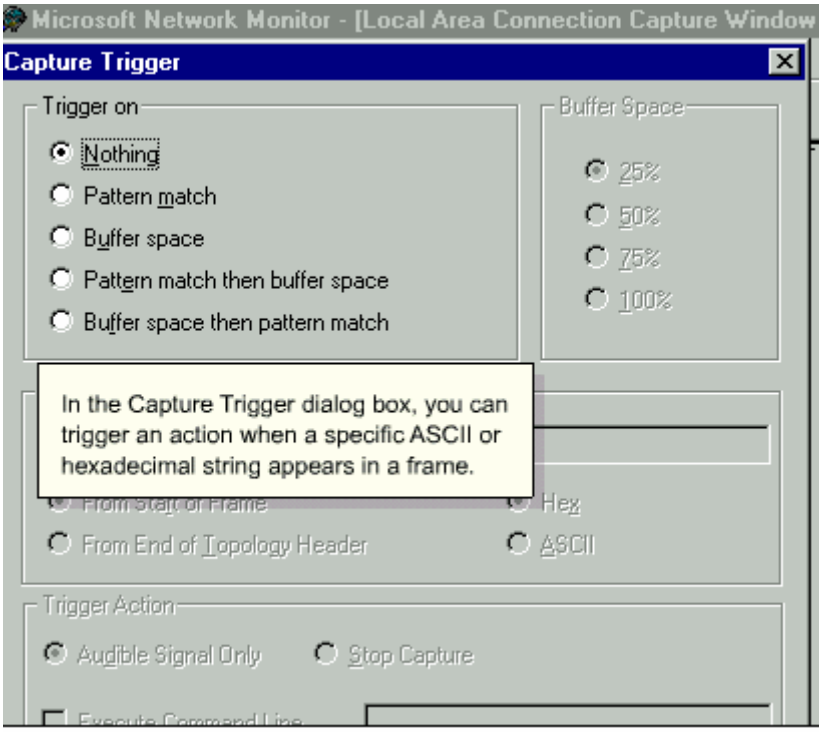
Suppose you are the systems administrator of Interswift. You are trying to resolve a problem with access to a local web server, and you wish to be notified when a user requests a web page from the server.

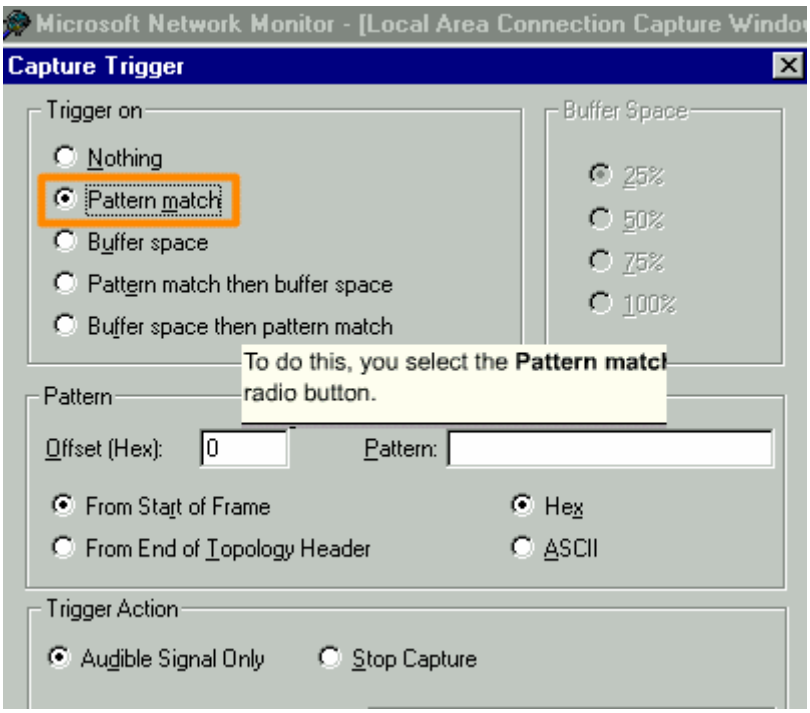
When a browser contacts a web server for a web page, it sends a HTTP GET command to the web server requesting the page. So, you need to set up a trigger to execute a command that alerts you when the GET text string is sent on the network.

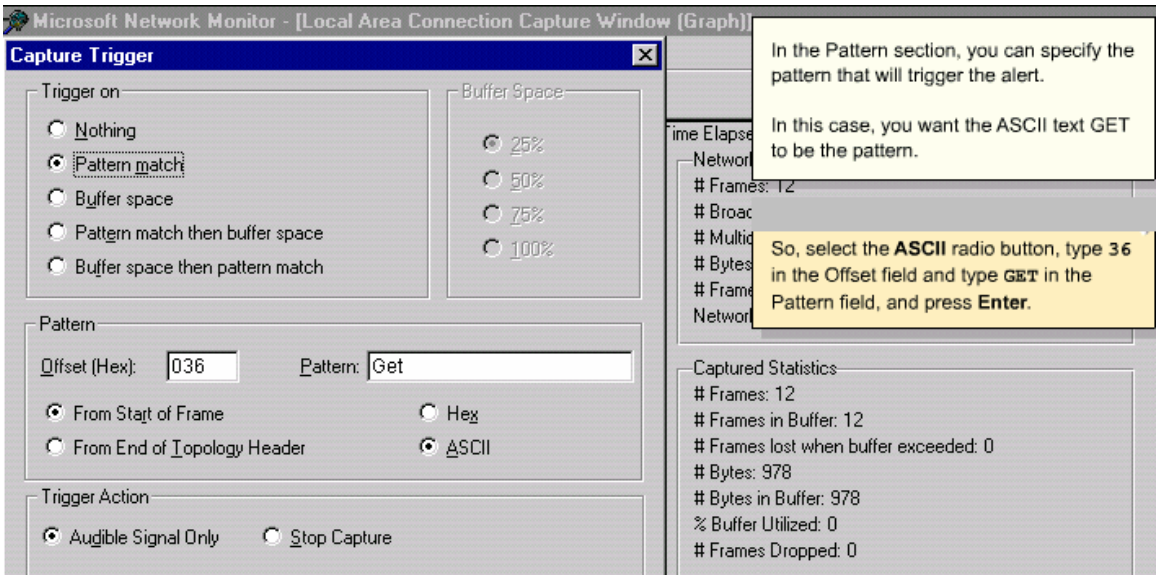
To determine the sequence of ASCII characters you need to set the trigger for, you examine a previously captured packet that was sent to the web server in the HEX detail pane of the capture. The ASCII text GET appears at offset 036.


Microsoft Network Monitor - [Capture: 1 (Summary)]
File Edit Display Tools Options Window Help
Frame Time Src MAC Addr Dst MAC Addr Protocol Descripti
8 416.83... LANS T81D374 LOCAL TCP Control E
9 416.83... LOCAL LANS T81D374 TCP Control E
10 416.83... LANS T81D374 LOCAL TCP Control E
11 416.84... LANS T81D374 LOCAL HTTP GET Reque
12 417.04... LOCAL LANS T81D374 TCP Control E
13 419.45... LOCAL LANS T81D374 HTTP Response
FRAME: Base frame properties
ETHERNET: EType = Internet IP (IPv4)
IP: Protocol = TCP - Transmission Control; Packet ID = 53981;
TCP: Control Bits: AP len: 314, seq:2503575371-2503575685
HTTP: GET Request from Client


Microsoft Network Monitor - [Local Area Connection Capture Window (Graph)]
File Capture Tools Options Window Help
You need to set a trigger for the ASCII code 036.
To configure trigger settings, select Capture - Trigger.
Start F10
Stop F11
Stop and View Shift+F11
Pause F9
Continue Shift+F9
Display Captured Data F12
Clear Statistics
Addresses...
Buffer Settings...
Filter... F8
Networks...
Trigger...
Dedicated Capture Mode
Frames: 12
Frames in Buffer: 12
Frames lost when buffer exceeded: 0
Bytes: 978
Bytes in Buffer: 978
% Buffer Utilized: 0
# Frames Dropped: 0
Network Status: Normal
Captured Statistics


Microsoft Network Monitor - [Local Area Connection Capture Window
Capture Trigger
Trigger on
Nothing
Pattern match
Buffer space
Pattern match then buffer space
Buffer space then pattern match
Buffer Space
25%
50%
75%
100%
In the Capture Trigger dialog box, you can trigger an action when a specific ASCII or hexadecimal string appears in a frame.
From End of Topology Header
Hex
ASCII
Trigger Action
Audible Signal Only
Stop Capture

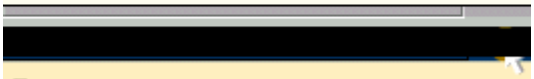

Microsoft Network Monitor - [Local Area Connection Capture Windo
Capture Trigger
Trigger on
Nothing
Pattern match
Buffer space
Pattern match then buffer space
Buffer space then pattern match
Buffer Space
25%
50%
75%
100%
To do this, you select the Pattern matc
radio button.
Pattern
Offset (Hex):
0
Pattern:
From Start of Frame
Hex
From End of Topology Header
ASCII
Trigger Action
Audible Signal Only
Stop Capture



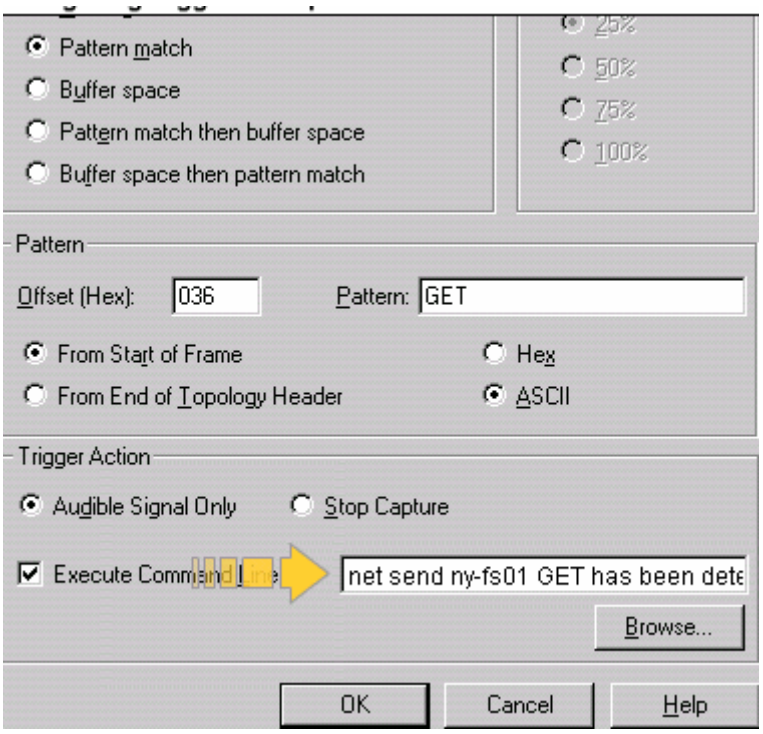
In the Trigger Action section, you can choose what type of action will take place if the pattern is found. You can choose an audible signal to stop the capture, or to execute a command.

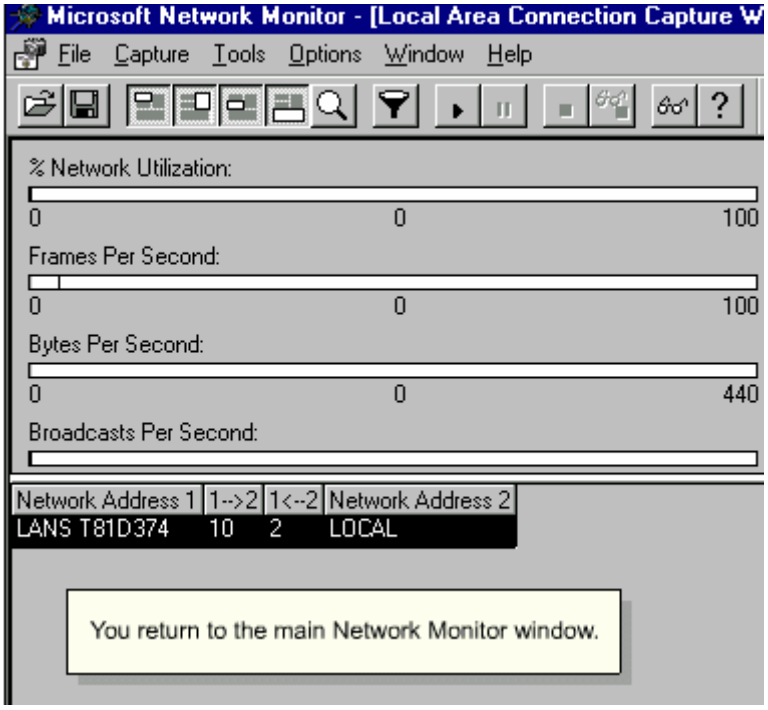
In this case, you want to execute the **net send** command, so you select the **Execute Command Line** checkbox.

Now you can type the **net send** command that will alert you when GET is found in a frame.

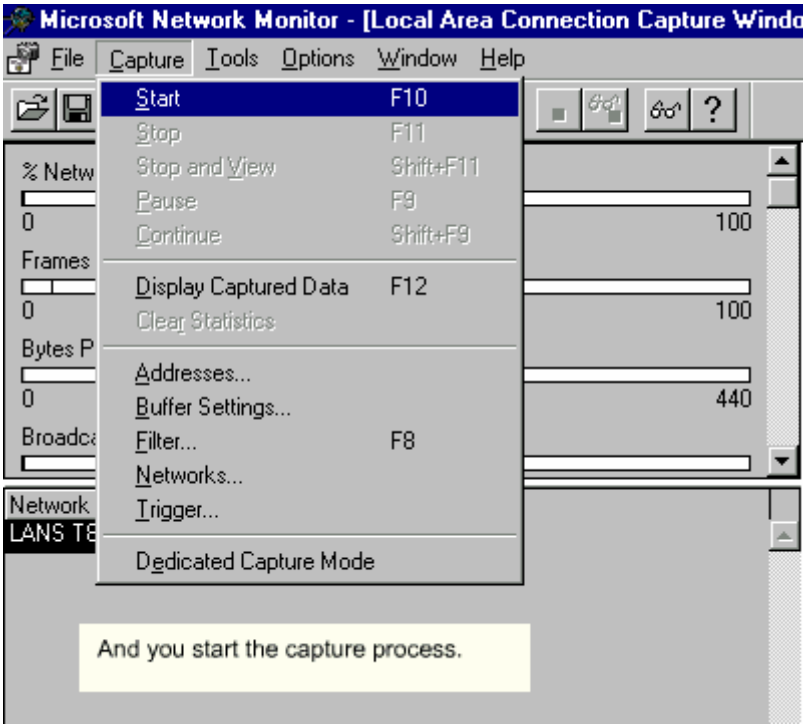


Type **net send ny-fs01 GET has been detected in captured data**, and click **OK.**

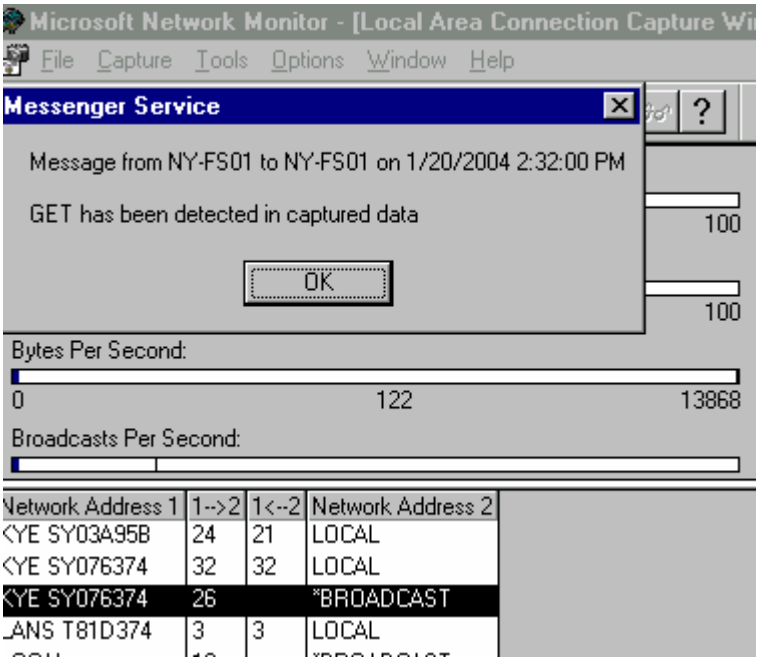

Pattern match
Buffer space
Pattern match then buffer space
Buffer space then pattern match
25%
50%
75%
100%
Pattern
Offset (Hex): 036
Pattern: GET
From Start of Frame
From End of Topology Header
Hex
ASCII
Trigger Action
Audible Signal Only
Stop Capture
Execute Command Line
net send ny-fs01 GET has been dete
Browse...
OK
Cancel
Help

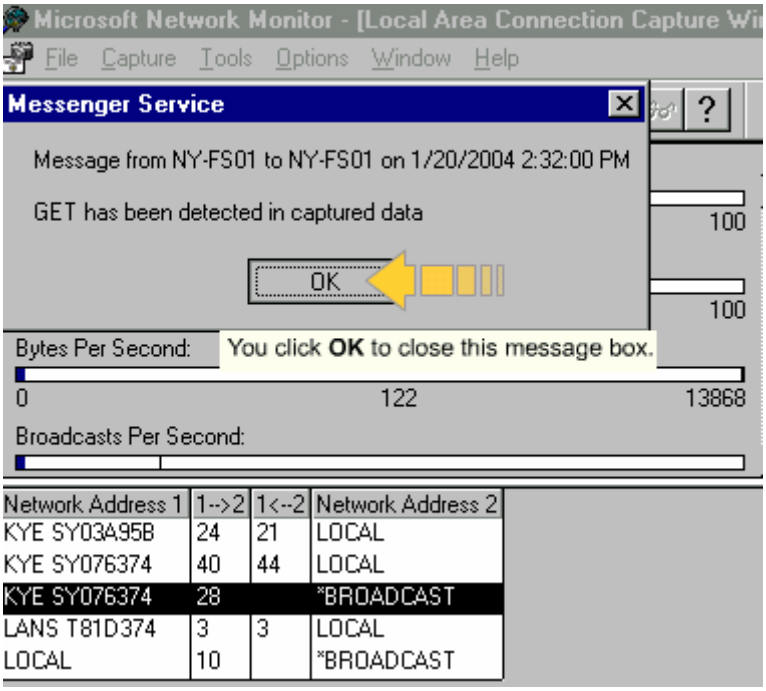

Microsoft Network Monitor - [Local Area Connection Capture W
File Capture Tools Options Window Help
% Network Utilization:
0 0 100
Frames Per Second:
0 0 100
Bytes Per Second:
0 0 440
Broadcasts Per Second:
Network Address 1 1-->2 1<--2 Network Address 2
LANS T81D374 10 2 LOCAL
You return to the main Network Monitor window.

Monitoring Network traffic Section one



Once the word GET is discovered in any frame, a message box is displayed indicating that GET has been detected in the captured data.





SkillCheck

Suppose you are troubleshooting access problems to a business web server. You want to set a trigger command that stops the capture when a certain web page is requested from the web server. You know from a previous capture that the HTTP response packet for this page contains the text "Interswift Sales" at offset 390.

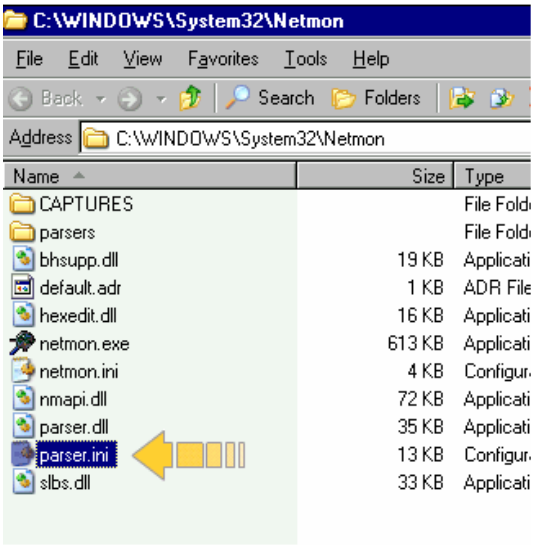
You have already accessed the Capture Trigger dialog box, and selected the **Pattern match** radio button.

To stop the capture when a web page containing the text "Interswift Sales" at offset 390 is requested from the web server, you select the **ASCII** radio button in the Pattern section.
You then type **390** in the Offset (Hex) field, type **Interswift Sales** in the Pattern field, select the **Stop Capture** radio button, and finally click **OK**.

A parser is a program or algorithm that reads, analyzes, and describes a frame and its contents.

For the Network Monitor, a parser is the DLL file that reads, analyzes, and describes messages from different protocols. Each protocol that Network Monitor supports has a corresponding parser. Network Monitor ships with approximately 30 parsers that are stored in the Windows\System32\Netmon\Parsers folder.

The 30 parsers can interpret over 110 protocols. You can add additional parsers for new protocols when they become available by placing the DLL in the Parsers folder and editing the parser.ini file.



Suppose you are the administrator for Interswift. Your company uses a customized protocol for communication with a specialized database. The development group has sent you a DLL. You want Network Monitor to parse this new protocol.

You've already placed the DLL in Windows\System32\Netmon\Parsers and have navigated to the parser.ini file, which is stored by default in Windows\System32\Netmon.

To open the parser.ini file, double-click it.

parser.ini - Notepad

File Edit Format View Help

```
;=============================================================
;   Bloodhound parser/protocol initialization file.
;=============================================================

[PARSERS]
    FRAME.DLL    = 0: FRAME
    MAC.DLL      = 0: ETHERNET, TOKENRING, FDDI, TMAC, SMT, ATM, IP/1394
    LLC.DLL      = 0: LLC, RPL, SNAP, BPDU
    NETBIOS.DLL  = 0: NETBIOS
    SMB.DLL      = 0: SMB
    XNS.DLL      = 0: XNS
    IPX.DLL      = 0: IPX, SAP, RIPX, NMPI, NBIPX, SPX, NWDP, NSP, NDR
    TCPIP.DLL    = 0: IP, ARP_RARP, ICMP, ESP, AH, ISAKMP, IGMP, UDP, NBT, TCP, DNS, FTP, RI
DHCP, RPC, NFS, OSPF, HTTP, FINGER, LPR, RADIUS, IP6, ICMP6

    NCP.DLL      = 0: NCP
    ATALK.DLL    = 0: LAP, AARP, DDP, RTMP, NBP, ATP, PAP, ASP, ZIP, AFP, ADSP
    BONE.DLL     = 0: BONE
    MSRPC.DLL    = 0: MSRPC, SSP
    BROWSER.DLL  = 0: BROWSER
    NETLOGON.DLL= 0: NETLOGON
    PPP.DLL      = 0: PPP, LCP, EAP, PPPPAP, PPPCHAP, IPXCP, IPCP, NBFCP, CBCP, CCP, PPTP, G
PPPML, IPXWAN, EAPOL
```

The parser.ini file contains the list of all the parsers and their associated details.

parser.ini - Notepad

File Edit Format View Help

To add the new customized protocol, which is called CUSTOM.DLL, you type CUSTOM.DLL=0: CUSTOM in between [PARSERS] and FRAME.DLL.

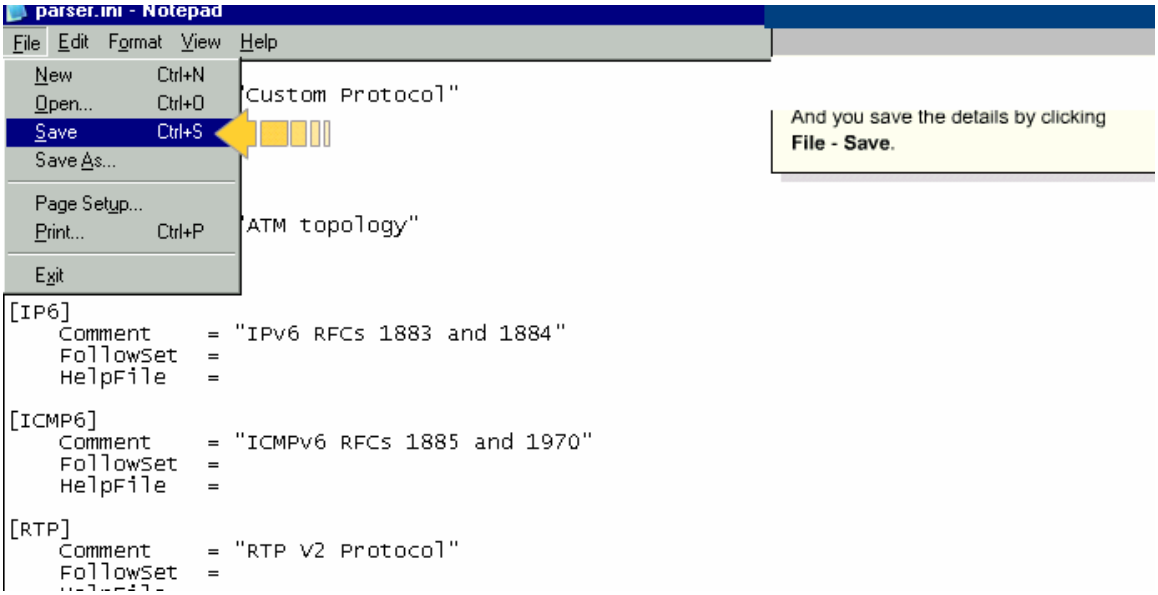
```
;==========================================================
;   Bloodhound parser/protocol initialization file.
;==========================================================

[PARSERS]
    CUSTOM.DLL   = 0: CUSTOM
    FRAME.DLL    = 0: FRAME
    MAC.DLL      = 0: ETHERNET, TOKENRING, FDDI, TMAC, SMT, ATM, IP/1394
    LLC.DLL      = 0: LLC, RPL, SNAP, BPDU
    NETBIOS.DLL  = 0: NETBIOS
    SMB.DLL      = 0: SMB
    XNS.DLL      = 0: XNS
    IPX.DLL      = 0: IPX, SAP, RIPX, NMPI, NBIPX, SPX, NWDP, NSP, NDR
    TCPIP.DLL    = 0: IP, ARP_RARP, ICMP, ESP, AH, ISAKMP, IGMP, UDP, NBT, TCP, DNS, FTP,
DHCP, RPC, NFS, OSPF, HTTP, FINGER, LPR, RADIUS, IP6, ICMP6

    NCP.DLL      = 0: NCP
    ATALK.DLL    = 0: LAP, AARP, DDP, RTMP, NBP, ATP, PAP, ASP, ZIP, AFP, ADSP
    BONE.DLL     = 0: BONE
    MSRPC.DLL    = 0: MSRPC, SSP
    BROWSER.DLL  = 0: BROWSER
    NETLOGON.DLL= 0: NETLOGON
    PPP.DLL      = 0: PPP, LCP, EAP, PPPPAP, PPPCHAP, IPXCP, IPCP, NBFCP, CBCP, CCP, PPTP
PPPML, IPXWAN, EAPOL
```

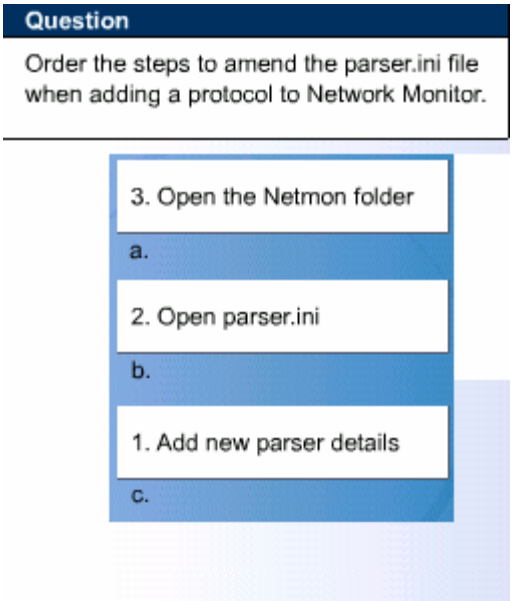
parser.ini - Notepad

File Edit Format View Help

You scroll down the file to the point above [ATM] and type the three lines onscreen.

```
[CUSTOM]
    Comment     = "Custom Protocol"
    FollowSet   =
    HelpFile    =

[ATM]
    Comment     = "ATM topology"
    FollowSet   =
    HelpFile    =

[IP6]
    Comment     = "IPv6 RFCs 1883 and 1884"
    FollowSet   =
    HelpFile    =

[ICMP6]
    Comment     = "ICMPv6 RFCs 1885 and 1970"
    FollowSet   =
    HelpFile    =

[RTP]
    Comment     = "RTP V2 Protocol"
```


parser.ini - Notepad
File Edit Format View Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Page Setup...
Print... Ctrl+P
Exit
"Custom Protocol"
"ATM topology"
[IP6]
Comment = "IPv6 RFCs 1883 and 1884"
FollowSet =
HelpFile =
[ICMP6]
Comment = "ICMPv6 RFCs 1885 and 1970"
FollowSet =
HelpFile =
[RTP]
Comment = "RTP V2 Protocol"
FollowSet =
And you save the details by clicking File - Save.


Question
Order the steps to amend the parser.ini file when adding a protocol to Network Monitor.
3. Open the Netmon folder
a.
2. Open parser.ini
b.
1. Add new parser details
c.

Summary

Network Monitor is a network analyzer that captures frames of raw data that are transmitted through a network. Network Monitor displays and captures filtered frames and edits captured frames.

Network Monitor contains numerous buttons you use to analyze captured frames, and there are four panes that display statistics about captured frames. Information about individual frames is displayed in three panes – Summary, Detail, and Hexadecimal.

You can configure the way in which Network Monitor captures and stores data. You use capture filters to capture only traffic sent from a certain source, using a certain protocol, or containing a specific pattern.

Summary

Once you have captured data, you can use display filters to filter the information displayed in the viewing pane. When Network Monitor captures network frames, it captures a default of 1 MB of data at one time before stopping. You can increase this if necessary.

Network Monitor can respond to events on your network if you create capture triggers. Triggers allow you to specify an action that occurs once a certain pattern is found in any of the captured frames. A parser is a program or algorithm that reads, analyzes, and describes a frame and its contents. Network Monitor uses parsers to read and interpret different protocol types.

This topic covers the following points:

1. Exercise overview
2. Task 1: Capturing data
3. Task 2: Filtering captured data
4. Task 3: Viewing captured data

Exercise

In this exercise, you're required to perform a network capture, and filter and view the captured frames.

This involves the following tasks:

- creating a filter to capture network data
- filtering the captured data to isolate specific information
- using different views to examine the filtered data

Staff in Interswift's New York marketing department have experienced trouble connecting to the local web server. You have installed Network Monitor on the server to begin diagnosing the problem.

You want to use the capture filters feature of Network Monitor to isolate different types of data transmitted between the web server and one of the marketing workstations on the Interswift network.

Task 1 of 3

Create a capture filter that intercepts the data transmitted between the web server and Marketing Workstation 3.

Steps

1. Select **Capture - Filter**
2. Click **OK**
3. Select the **Address Pairs** node and click **Address**
4. Select **Web Server** from the Station 1 list, and select **Marketing Workstation 3** from the Station 2 list, and click **OK**
5. Click **OK**

Task 2 of 3

Filter the captured data so that only data relevant to web browsing is shown.

Steps

1. Select **Display - Filter**
2. Select **Protocol == Any**, and click **Expression**
3. Select **Protocol**
4. Click **Disable All**
5. Scroll down, select **HTTP**, and click **Enable**
6. Click **OK** twice

The Interswift network has been experiencing more network connectivity problems. Users are complaining that they cannot access their files on network servers. You are at one of those servers now, and want to diagnose the problem.

You have installed Network Monitor on the server and have started the capture.

Task 3 of 3

Stop the capture and view the accumulated data. Change the view so you can view all listed frames, all protocol information for each frame, and the hexadecimal format of each frame.

Steps

1. Select **Capture - Stop**
2. Select **Capture - Display Captured Data**
3. Click **Toggle Detail** Pane
4. Click **Toggle Hex** Pane