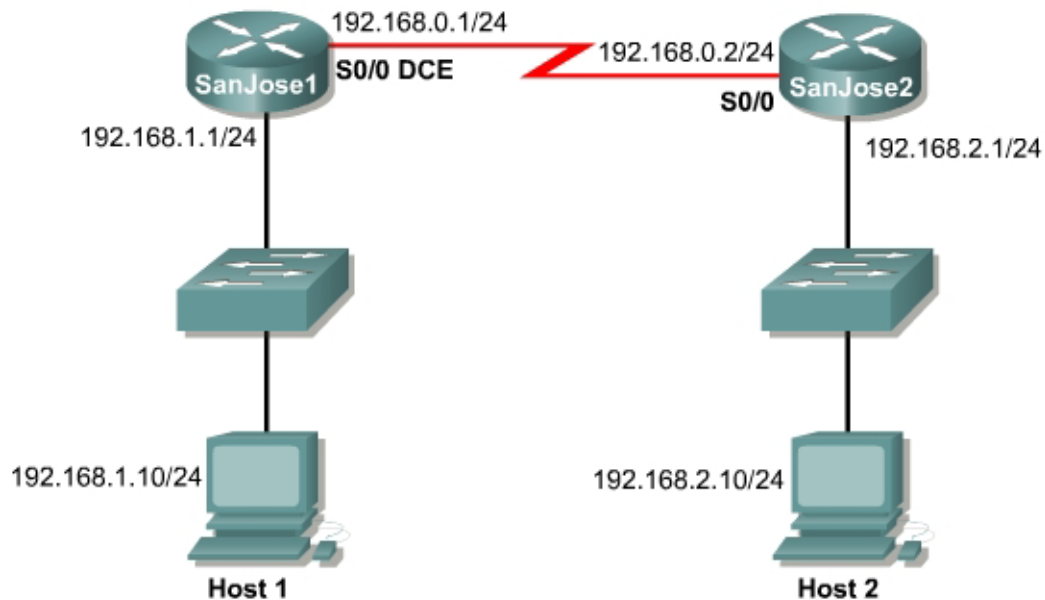


Lab 1.6.5 Introduction to Fluke Protocol Expert



Objective

This lab is a tutorial demonstrating how to use the Fluke Network OptiView Protocol Expert (PE) to analyze network traffic. In this lab, students will see the key features of the tool so that they can incorporate its use into various troubleshooting efforts.

The output in this lab is representative only. The output will vary depending on the number of devices in the network such as device MAC addresses and device host names.

Scenario

This lab introduces the Protocol Expert, which may be useful in later troubleshooting labs and in the field. The Protocol Expert software is a valuable part of the Academy program. It is also provides many of the same features as other products in the market.

If the software is installed on all classroom machines, each person can run the lab steps. However, each host may display slightly different results.

Step 1

Note: This is exactly the same lab configuration as the Network Inspector lab.

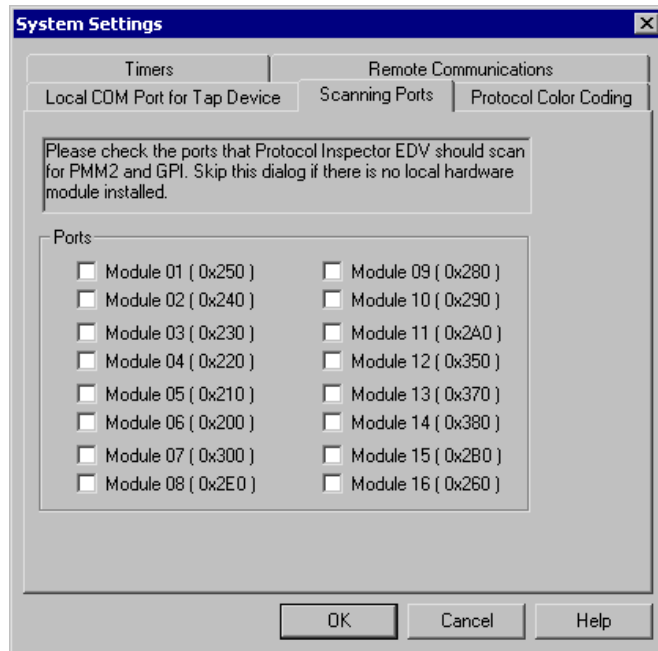
Cable and configure the devices as pictured in the network diagram. The switches pictured can be any Catalyst switches that are preferred. Be sure to use the default switch configurations on these switches. If necessary, erase the configuration files on the switches.

Step 2

From the **Start** menu, launch the OptiView Protocol Expert EDV program.

Note: The first time the program is run a message will appear that asks if the user has any Fluke analyzer cards or Fluke taps in the local system.

If the educational version is being used, click on **No**. If the answer is yes or if the following screen appears, click on **OK** without selecting any ports.

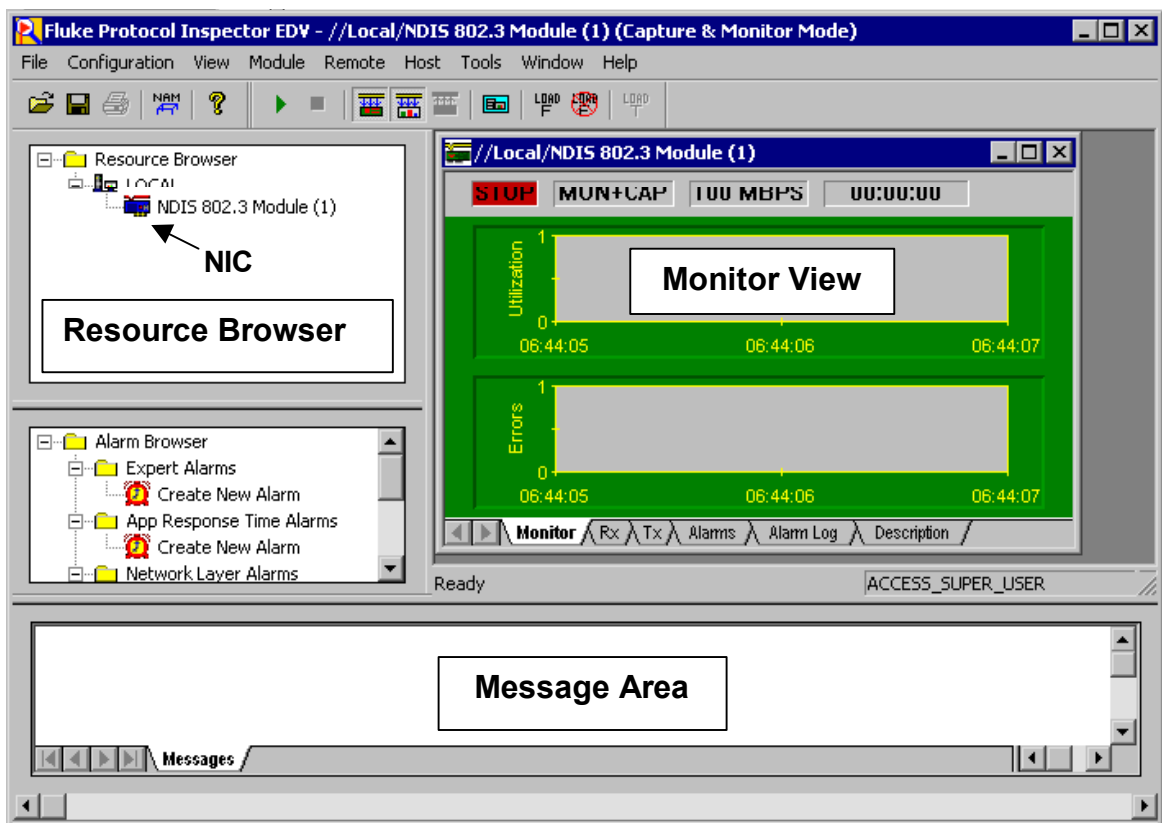


There are four main Protocol Expert views:


- Summary View
- Detail View
- Capture View of Capture Buffers
- Capture View of Capture Files

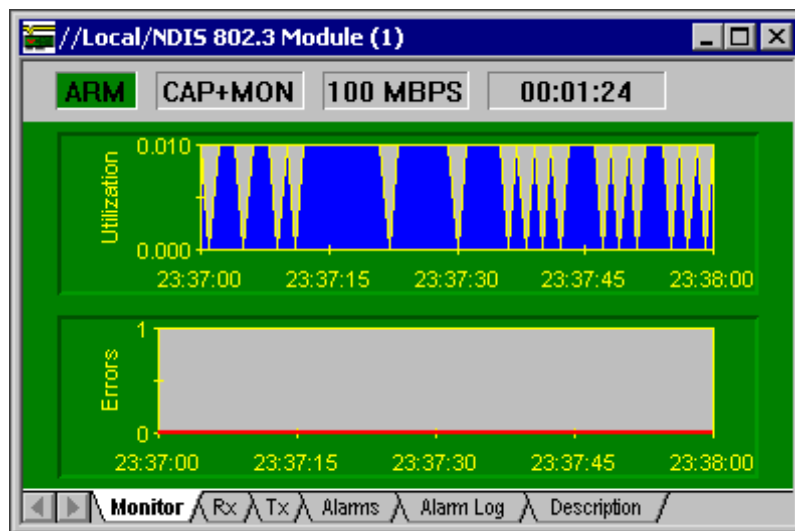
The program opens in the **Summary View**. This view shows several windows used by the tool. The **Resource Browser** window in the upper-left corner shows the only monitoring device available in this lab, which is the NDIS 802.3 Module NIC of the host. Any Protocol Media Monitors would be displayed with the associated host devices. The **Alarm Browser** on the left side and **Message Area** at the bottom will be covered later.

The **Monitor View**, which is the main window in the upper-right corner, monitors one resource per window in a variety of viewing options. The following example and the startup screen show no information in the **Monitor View** window. The **Stop** in the upper-left corner of the **Monitor View** window confirms that no monitoring is occurring.



Step 3

Use the **Start**  button or choose **Module > Start** from the menu system to begin the monitoring and capturing process. The **Utilization** chart should start showing activity as shown in the following figure.



The word **ARM** should appear where **Stop** had been before. The **Module** menu will show that **Stop** is now an option and **Start** has been muted. Do not stop the process yet and restart it if necessary.

The tabs at the bottom of the window show the resulting data in a variety of forms. Click on each tab and note the results. The **Tx** tab, which represents transmit, will be blank. The **Alarms** and **Alarm Log** will also be blank. The following figure shows the **Rx**, or received frames, which indicates that Broadcast and Multicast frames are being received. However, it may not show any Unicasts.

//Local/NDIS 802.3 Module (1)			
ARM		CAP+MON	
100 MBPS		00:08:27	
MAC Counters	Value	Errors	Value
Frames Captured	463	CRC Alignment	0
Frames Received	463	Undersize	N/A
Broadcast	100	Oversize	N/A
Multicast	363	Fragments	N/A
Unicast	0	Jabbers	N/A
Frames/Second	2	Collision Indication	N/A
Bytes Received	31,400	Packet Dropped	0
Utilization	0	Errors	0

Monitor Rx Tx Alarms Alarm Log Description

Use the console connection to the router to ping the monitoring host, which is 192.168.1.10 or 192.168.2.10. Unicast frames will appear. Dedicated hardware protocol analyzers such as Fluke Network OptiView can show a more complete picture of traffic on the network.

The **Description** tab reveals the MAC address, manufacturer, and model of the NIC. It also shows which Error Counters are on.

Take a few minutes to become familiar with the tabs and the scroll features of the window.

//Local/NDIS 802.3 Module (1)

MAC Address: 00A0CC23FE40

Module Type: NDIS 802.3

Buffer Size: 512 KB

Vendor Name: LITE-ON

Description: Linksys LNE100TX Fast Ethernet Adapter

Driver Version :

Note


Modify ...

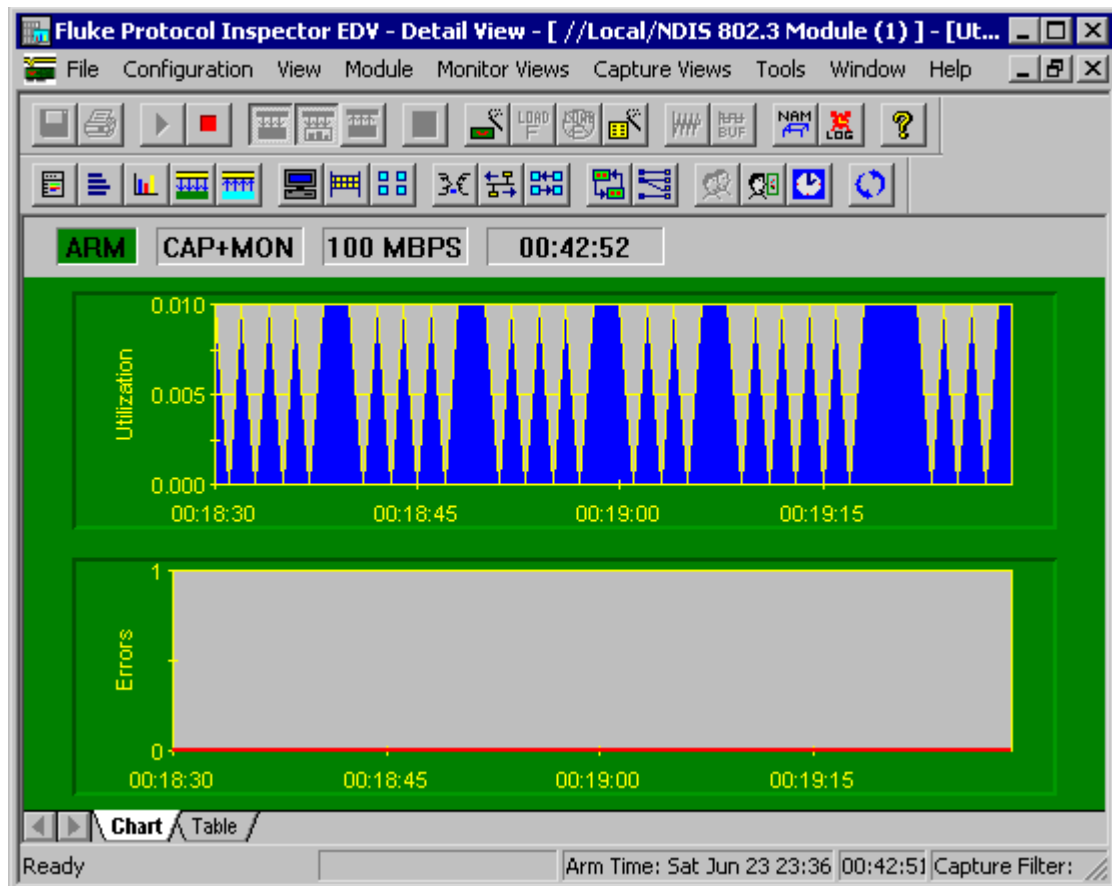
Error Counters Supported:

CRC_Alignment, Rx_Packet_Drop, Tx_Collision, Tx_Late_Collision, Tx_Excessive_Collision, Tx_Defer

Monitor Rx Tx Alarms Alarm Log **Description**

Step 4

Click on the **detail view**  button in the toolbar or double click anywhere on the **Monitor View** chart to access the **Detail View** window. This will open a second window that should resemble the following example after the **Utilization/Errors Strip Chart** or **RX** window has been maximized to fill the screen.




Note: If necessary, activate all toolbars on the **View** menu.


Initially, the chart output will be the same as before, but there are many more toolbar and menu options than in the **Summary View**. Confirm that the **Chart** and **Table** tabs still contain the same information.

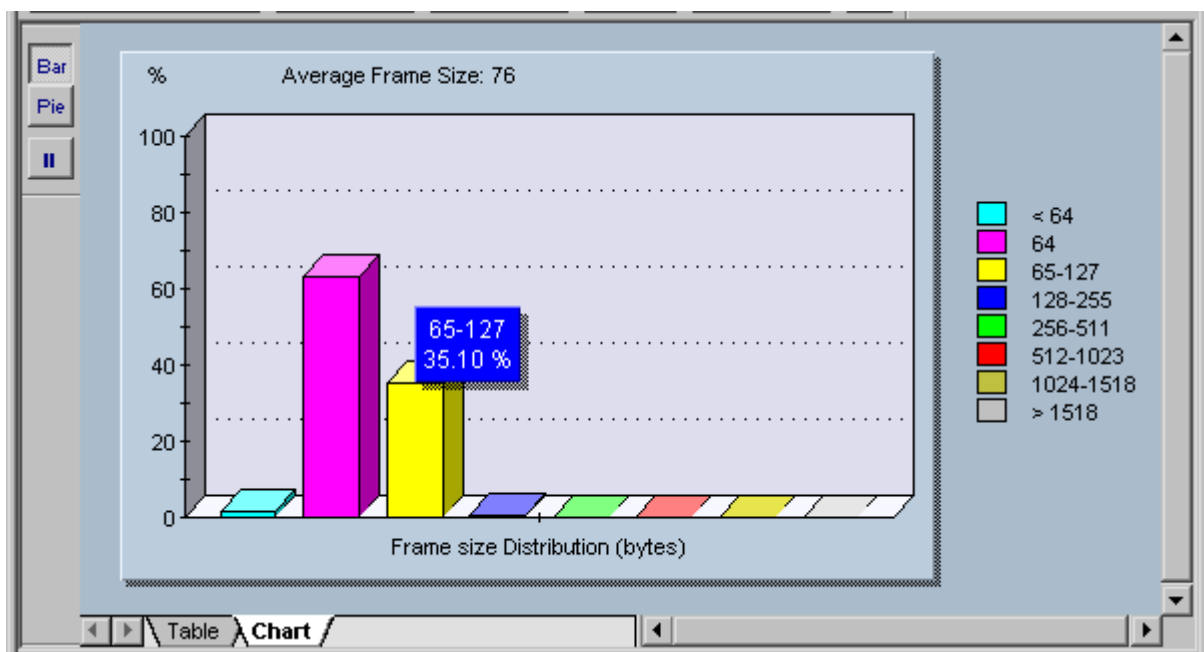
The **Detail View** window is covering the **Summary View** window from earlier. Use the taskbar to move between the windows.

Like all Windows-compliant programs, when the mouse is placed over a button, a screen tip will appear to identify the purpose of the button. Move the mouse over the buttons and notice that some of them are muted. This indicates that the feature is not appropriate under the current circumstances or it may not be supported on the educational version.

Note: A complete display of the toolbars and what they do is included in the Appendix at the end of this lab.

Click on the **Mac Statistics**  button to view the Rx frame table data in a different format. The result should be obvious. Maximize the resulting window. The one piece of new information is the **Speed**, which shows the NIC transmission rate.

Click on the **Frame Size Distribution**  button to see a distribution of the size of the frames being received by the NIC. When the mouse is placed over any bar, a small summary like the one in the following figure will appear. Maximize the resulting window.




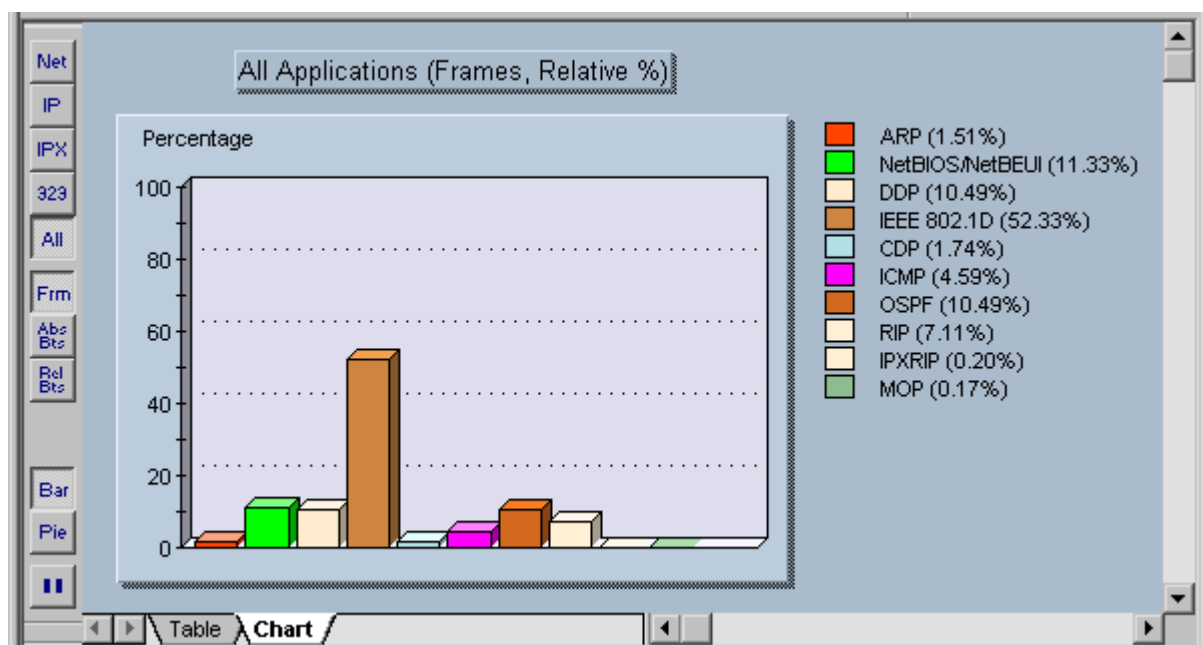
Try the **Pie**, **Bar**, and **Pause**  buttons in the upper-left corner.

Note: **Pause** stops the capture, so click on it again to resume the capture. Look at both the **Table** and **Chart** tab displays as well.


The sample configurations will mainly produce small frames since routing updates are occurring. Try using the extended ping feature from the router console connection and specify 100 pings with a larger packet size.

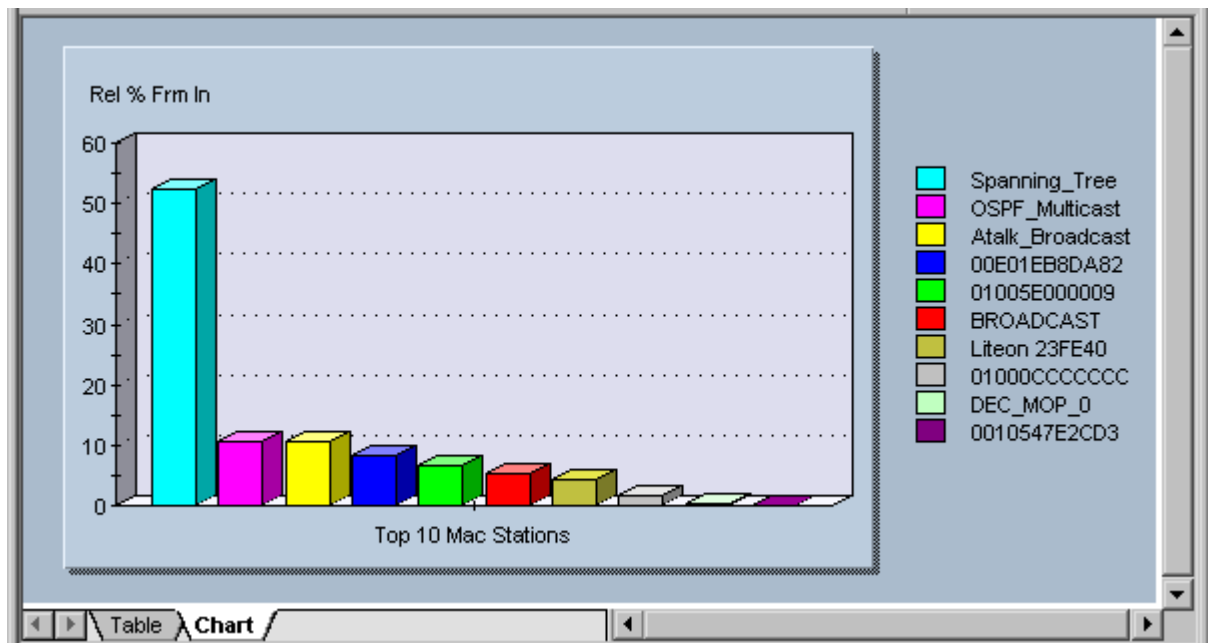
After maximizing each new display, use the **Window** menu to return to any previous view. Students can also **Tile** the windows. Experiment with the **Window** menu features and then close any unwanted views.

Click on the **Protocol Distribution**  button to see a distribution of the protocols being received by the NIC. Place the mouse over any bar to view a small summary panel. Maximize the resulting window.



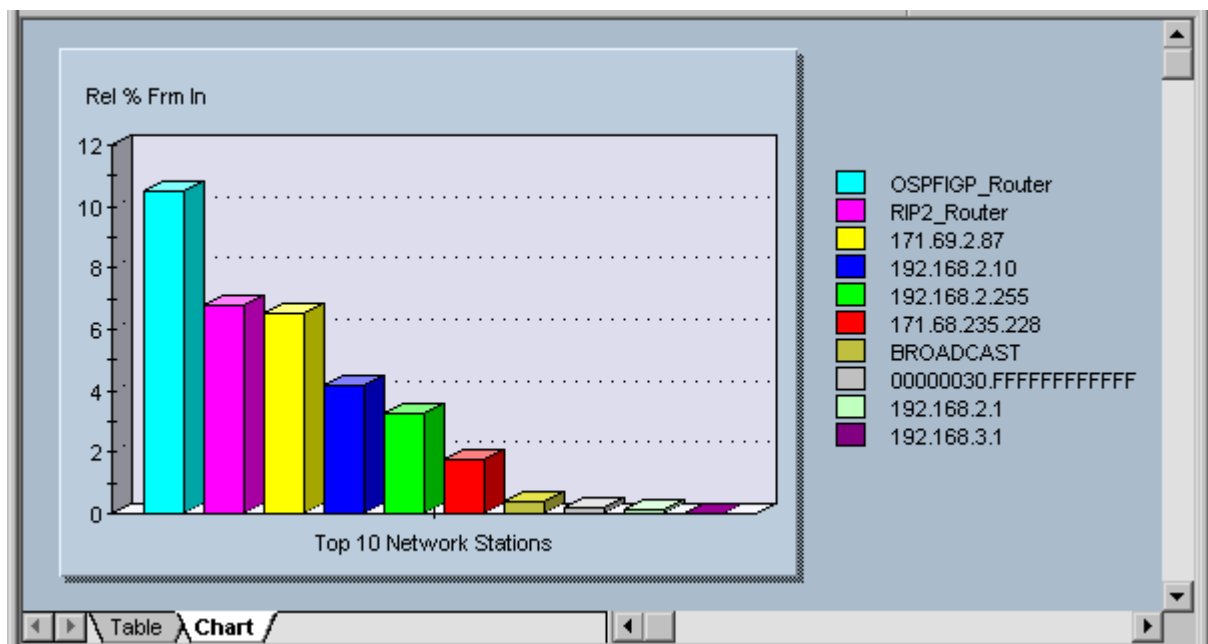
Try each of the buttons and tabs to see the results. The **Net** button shows only network protocols. The **323** button refers to the H323 Voice over IP protocols. Look at the frame (**Frm**), the absolute bytes (**Abs Bts**), and relative bytes (**Rel Bts**) to see the results. Remember that the **Pause** button stops the capture.

Click on the **Host Table**  button to see the MAC stations and related traffic.



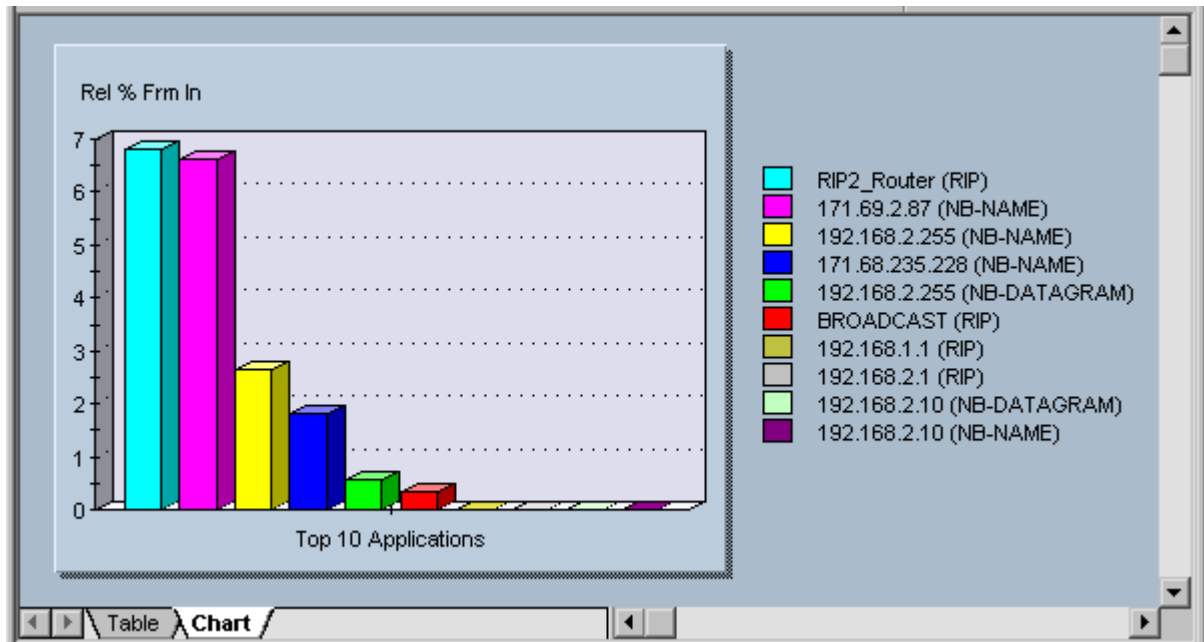
Notice in the preceding figure that Spanning Tree, AppleTalk, and OSPF traffic are present. The results will only include the protocols that are present on the network. Be sure to look at the **Table** tab to see the actual values.


Click on the **Network Layer Host Table**  button to see the network IP or IPX stations and related traffic.

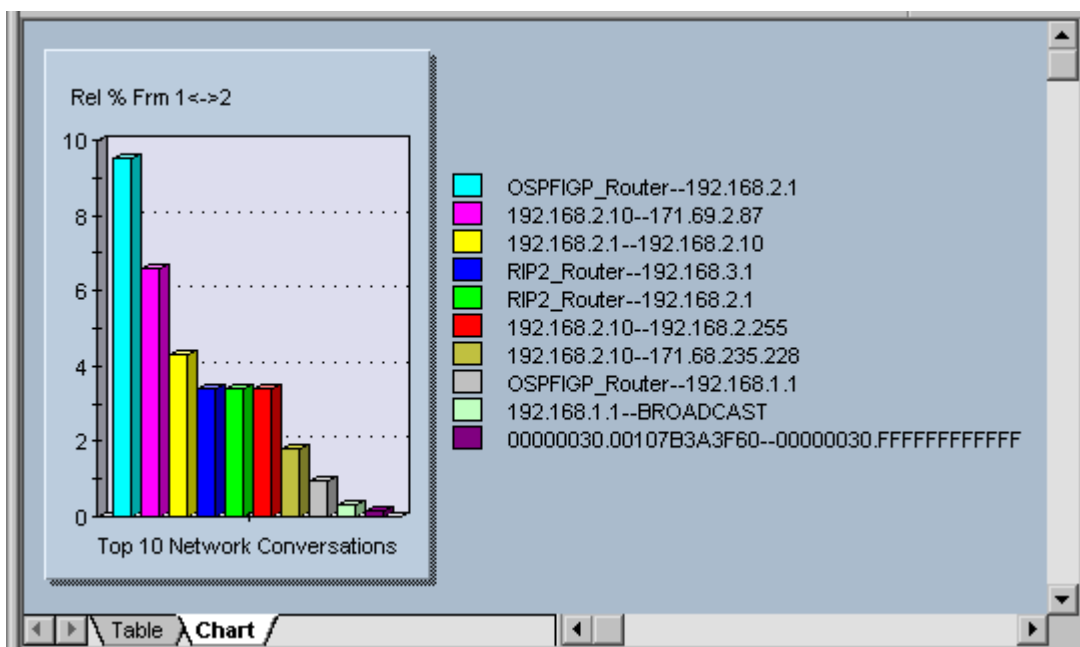



Any pings and any additional hosts that have been added to the configuration will impact the actual addresses that appear on the right.


Click on the **Application Layer Host Table**  button to see the network station traffic for each application.




Experiment with the next three  buttons. They create host-to-host matrices for MAC, network layer, and application layer conversations. The following figure is an example of the network layer IP or IPX conversations.




The **VLAN** button  shows network traffic on VLANs. If this lab does not use VLANs, remember to try it in future VLAN labs.

The second button  creates a matrix that compares MAC and Network station addresses to names. In the following example, the second row is a Novell station.

MAC Station Name	MAC Station Address	Network Station Name	Network Station Address
00107B3A3F60	00107B3A3F60	192.168.1.1	192.168.1.1
00107B3A3F60	00107B3A3F60	00000030.00107B3A3F60	00000030.00107B3A3F60
Liteon 23FE40	00A0CC23FE40	192.168.2.10	192.168.2.10
00E01EB8DA82	00E01EB8DA82	192.168.2.1	192.168.2.1
00E01EB8DA82	00E01EB8DA82	192.168.3.1	192.168.3.1


The **Name Table**  button opens the current name table for viewing or editing.


NameTable Entries		
Protocol	Name	Address
MAC	HP_Probe	090009000001
MAC	OSPF_Multicast	01005E000005
IP	IP_Station1	206.132.32.2
IP	BROADCAST	255.255.255.255
IP	IP_Multicast	224.0.0.0
IP	DVMRP_Router	224.0.0.4
IP	OSPF_IGP_Router	224.0.0.5
IP	OSPF_IGP_Router_0	224.0.0.6

The **Expert View**  button shows the expert symptoms discovered. These statistics are used to identify potential problems. The underlined options bring up additional detail windows if any values are recorded. The sample for this lab will not show much. However, students should review the options for debugging ISL, HSRP, and other types of problems that may be seen in later labs.

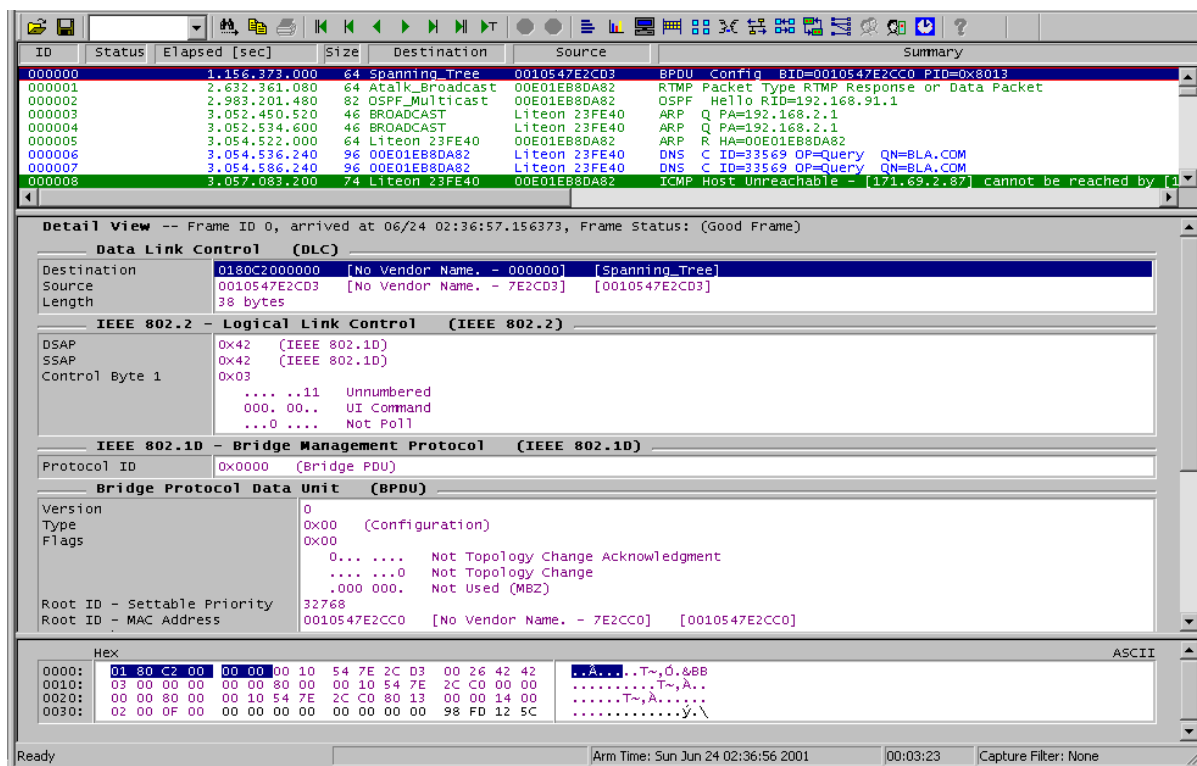
Expert Category	Value	Expert Category	Value
ICMP All Errors	368	<u>Duplicate Network Address</u>	0
ICMP Destination Unreachable	368	Unstable MST	0
ICMP Redirects	0	SAP Broadcast	0
Excessive Bootp	0	OSPF Broadcast	923
Excessive ARP	0	RIP Broadcast	25
<u>NFS Retransmissions</u>	0	ISL Illegal VLAN ID	0
TCP/IP SYN Attack	0	ISL BPDU/CDP Packets	0
TCP/IP RST Packets	0	<u>IP Time to Live Expiring</u>	0
<u>TCP/IP Retransmissions</u>	0	<u>IP Checksum Errors</u>	0
<u>TCP/IP Zero Window</u>	0	<u>Illegal Network Source Address</u>	0
<u>TCP/IP Long Acks</u>	0	Illegal MAC Source Address	0
<u>TCP/IP Frozen Window</u>	0	Total MAC Stations	11
Network Overload	0	Broadcast/Multicast Storm	0
<u>Non Responsive Stations</u>	0	Physical Errors	0
		<u>HSRP Errors</u>	0
		<u>TCP Checksum Errors</u>	0

Step 5

Use the **Stop**  button or **Module > Stop** from the menu to stop the frame capture so that students can look at individual frames.

After the capture has been stopped, click on the **Capture View**  button. The education version will display a message box that says the capture is limited to 250 packets. Click on **OK**.

The resulting window looks complicated at first. Maximize the window.



Looking over the results, note that there are three horizontal windows open. The top window lists the captured packets. The middle window shows the details of the selected packet in the top window, and the bottom window shows the HEX values for the packet.

When the mouse is positioned over the borders between the three windows, a line mover or two-headed arrow should appear, which can be used to change the distribution of space to each window. Students should make the middle window as large as possible and leave five to six rows in each of the other two, as shown in the figure.

Look over the packets that are listed in the top window. This should include DNS, ARP, and RTMP packets. When a switch is used, CDP and Spanning Tree packets should be displayed. Notice that when rows in the top window are selected, the contents of the other two windows will change.

When information in the middle window is selected, the HEX display in the bottom window will change to show where the specific information is stored. In the following example, when the Source Address or IP is selected, the HEX values from the packet will be displayed.

Checksum	0xA777 (Correct)
Source Address	192.168.2.10
Destination Address	171.69.2.87
	[58 bytes of data]

Hex	
0000:	00 E0 1E B8 DA 82 00 A0 CC 23 FE 40 08 00 45 00 .à.Ú..i#p@..E.
0010:	00 4E 22 09 00 00 80 11 A7 77 C0 A8 02 0A AB 45 .N"Ú....\$wA..«E
0020:	02 57 00 89 00 89 00 3A 99 97 83 21 01 00 00 01 .W.....!....

The color coding makes it easier to locate information from the middle window in the HEX window. In the following example with a DNS packet, the data in the Data Link Control (DLC) section of the middle window is purple while the Internet Protocol (IP) section is green. The corresponding HEX values are the same colors.

000005	3.054.522.000	64	Liteon 23FE40	00E01EB8DA82	ARP R HA=0C
000006	3.054.536.240	96	00E01EB8DA82	Liteon 23FE40	DNS C ID=33
000007	3.054.586.240	96	00E01EB8DA82	Liteon 23FE40	DNS C ID=33

Data Link Control (DLC)	
Destination	00E01EB8DA82 [No Vendor Name. - B8DA82] [00E01EB8DA82]
Source	00A0CC23FE40 [LITE-ON COMMUNICATIONS, INC. - 23FE40] [Liteon
EtherType	0x0800 (Internet Protocol (IP))

Internet Protocol (IP)	
Version/Header Length	0x45 0100 Version 4 0101 20 bytes - Header Length
Type of Service	0x00

Hex	
0000:	00 E0 1E B8 DA 82 00 A0 CC 23 FE 40 08 00 45 00 .à.Ú..i#p@..E.
0010:	00 4E 22 09 00 00 80 11 A7 77 C0 A8 02 0A AB 45 .N"Ú....\$wA..«E
0020:	02 57 00 89 00 89 00 3A 99 97 83 21 01 00 00 01 .W.....!....
0030:	00 00 00 00 00 00 20 45 43 45 40 45 42 43 4F 45 ECMEBCOE
0040:	44 45 50 45 4E 43 41 43 41 43 41 43 41 43 41 43 DEPENCACACACACAC
0050:	41 43 41 43 41 41 41 00 00 20 00 01 67 87 47 13 ACACAAA.. ..g.G.

Notice in the preceding figure the EtherType is 0x0800, which indicates that it is an IP packet. The MAC addresses for both the Destination and Source hosts and where that data is stored in the HEX display can be seen.

In the same example, the section in the middle window is the User Datagram Protocol (UDP), which contains information such as the UDP port numbers.

User Datagram Protocol (UDP)	
Source Port	137 (NETBIOS Name Service)
Destination Port	137 (NETBIOS Name Service)
Length	58 bytes
Checksum	0x9997 (Correct)
	[50 bytes of data]

The structure of the middle window is different for each type of packet.

Select different packet types in the top window and look over the resulting display in the other two windows. Pay attention to the EtherType, port numbers, and source and destination addresses. These can be both MAC and network layers addresses. RIP, OSPF, and AppleTalk RTMP packets may also be seen in the capture. Students should be able to find and interpret the important data. The following RIP capture shows that this is a RIP version 2 packet. This version has a multicast

destination address of 224.0.0.9 and the actual route table entries can be seen. Students should find the multicast destination address in version 1.

Source Address	192.168.3.1
Destination Address	224.0.0.9 [RIP2_Router] [72 bytes of data]
User Datagram Protocol (UDP)	
Source Port	520 (Routing Information Protocol)
Destination Port	520 (Routing Information Protocol)
Length	72 bytes
Checksum	0x6192 (Correct) [64 bytes of data]
Routing Information Protocol	
Command	2 (Routing Response)
Version	2 (RIP2)
Unused	0 0
Routing Info	Addr Family: 2 (IP), Route Tag: 0, Addr:192.168.0.0, Subnet Mask:255.255.255.0, Next Hop:0.0.0.0, Metric:1
Routing Info	Addr Family: 2 (IP), Route Tag: 0, Addr:192.168.90.0, Subnet Mask:255.255.255.0, Next Hop:0.0.0.0, Metric:1
Routing Info	Addr Family: 2 (IP), Route Tag: 0, Addr:192.168.91.0, Subnet Mask:255.255.255.0, Next Hop:0.0.0.0, Metric:1


If there are any CDP packets, determine the platform. The following figure is from a Catalyst 1900 switch.

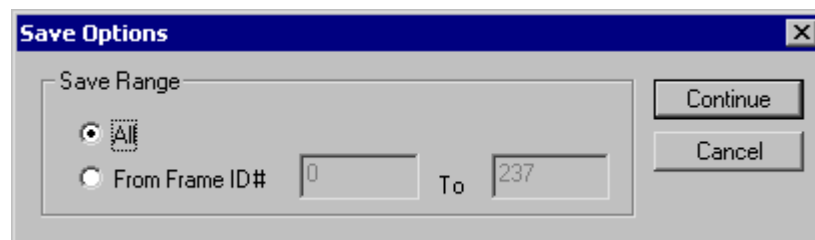
Variable Type	0x0006 (Platform)
Variable Length	14
Platform	cisco 1900

0020:	31 30 33 34 37 43 32 43 43 30 00 00 02 00 11 00	10 47 E2 C8
0030:	00 00 01 01 01 CC 00 04 C0 A8 01 64 00 03 00 06 i . . A . d . . .
0040:	31 39 00 04 00 08 00 00 00 0A 00 05 00 09 56 38	19 V8
0050:	2E 30 30 00 06 00 0E 63 69 73 63 6F 20 31 39 30	. 00 cisco 190
0060:	30 8A 8B 60 39	0 . . . 9

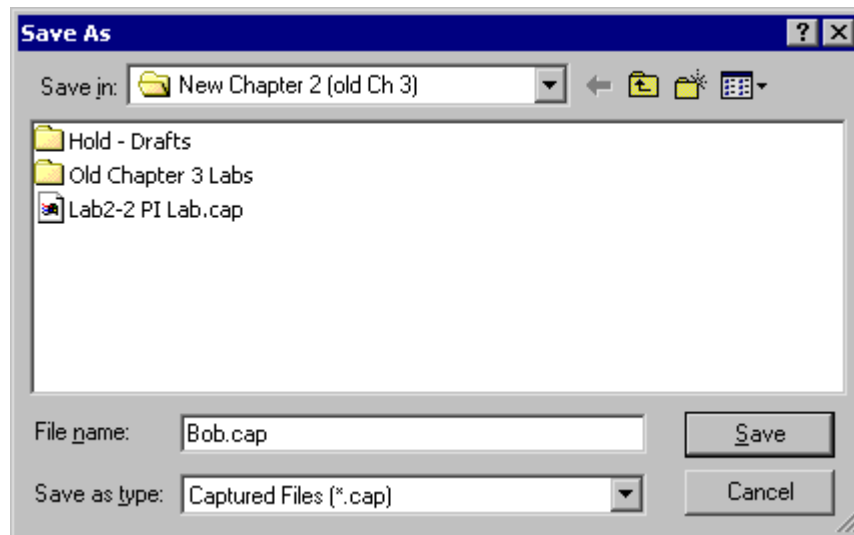
Experiment until the tools are familiar.

Step 6

Use the **Save Capture**  button or choose **File > Save Capture** from the menu system to save the captured data,. Use the **Continue** button to accept the **All** option. A range of captured frames can be saved with this window.




Use a first name or anything that could be recognized as a name and store the file on the data floppy disk. If the CAP extension is showing when this window opens, then make sure it is there after typing the name.




Use the **Open Capture File**  button to open the file that was just saved.

The **Capture View of Capture Files** is now being used. The tools are the same but the title bar at the top of the screen indicates that a file is being viewed instead of a capture in memory.

Step 7

Select a frame in the top window and try the  buttons. The basic arrows will move up or down one frame. The arrow with the single line will move to the top or bottom of the current window. The arrow with two lines will move to the top or bottom of the entire list. The arrow with the T also moves to the top of the list.

Use the **Search**  buttons to perform searches. Type text like OSPF in the list box. Then click on the binoculars to move from one OSPF entry to the next.

Experiment until the tools are familiar.

Reflection

How might this tool be used in troubleshooting?

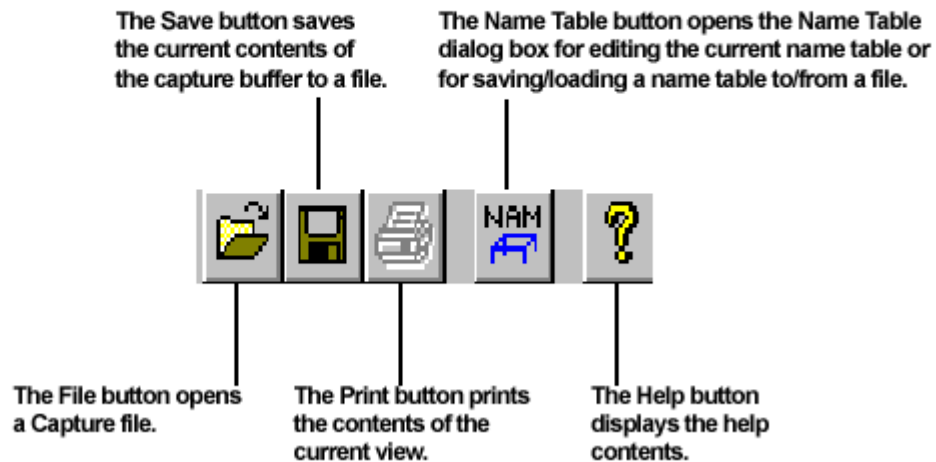
Is all of the data on the network being analyzed?

What is the impact of being connected to a switch?

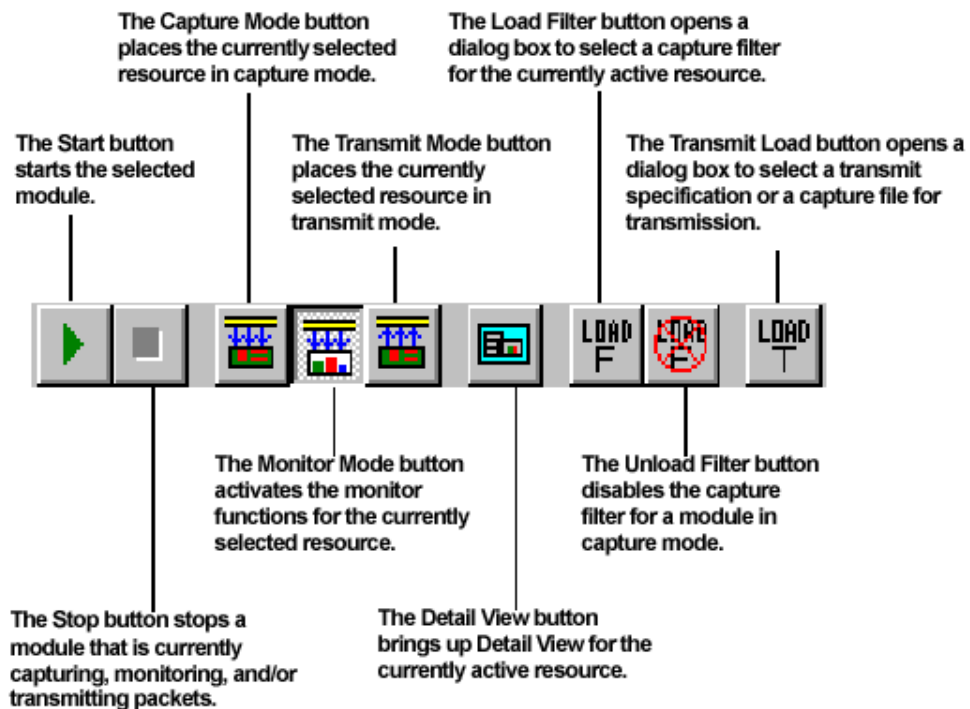
Students have only been receiving broadcast traffic and unicasts for the monitor host. In a later lab, students will learn how to mirror ports to direct a copy of any data to the protocol analyzer.

Appendix: Toolbars

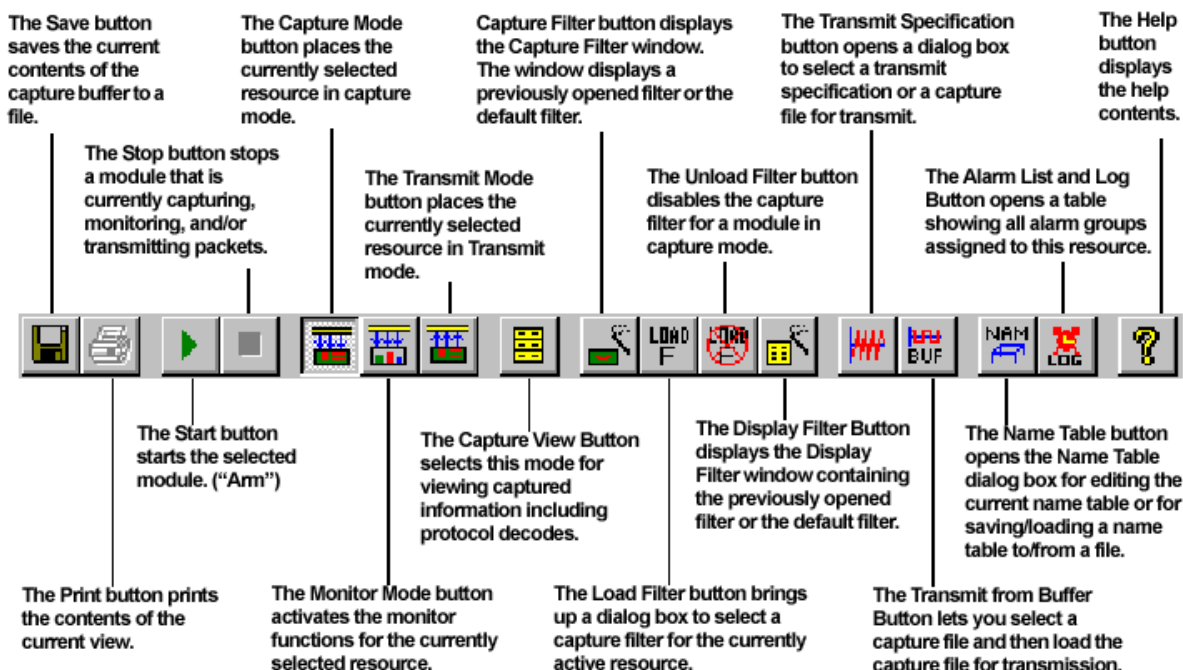
Protocol Inspector Toolbar



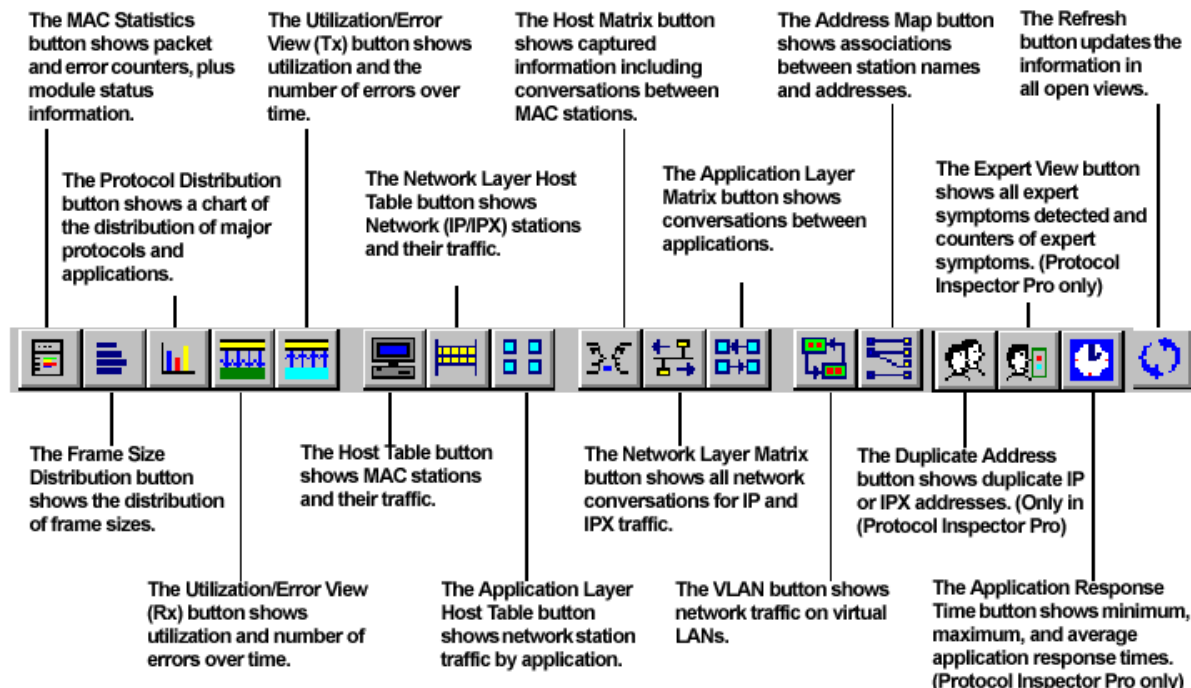
Module Toolbar (Summary View)



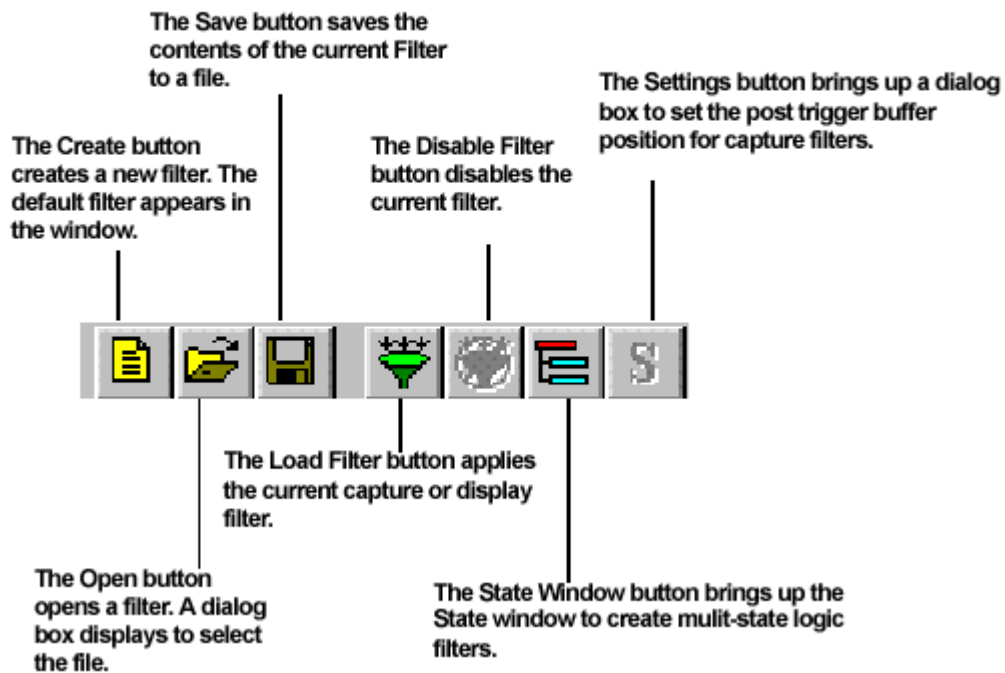
Detail View Toolbar



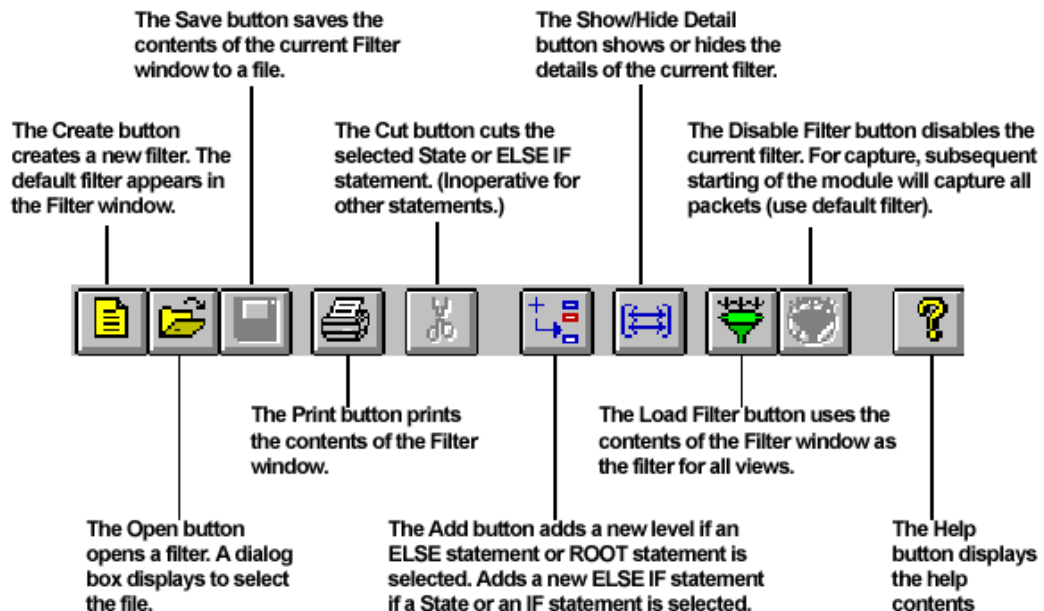
Data Views Toolbar (Note: Only some of these views are available with GMM cards)



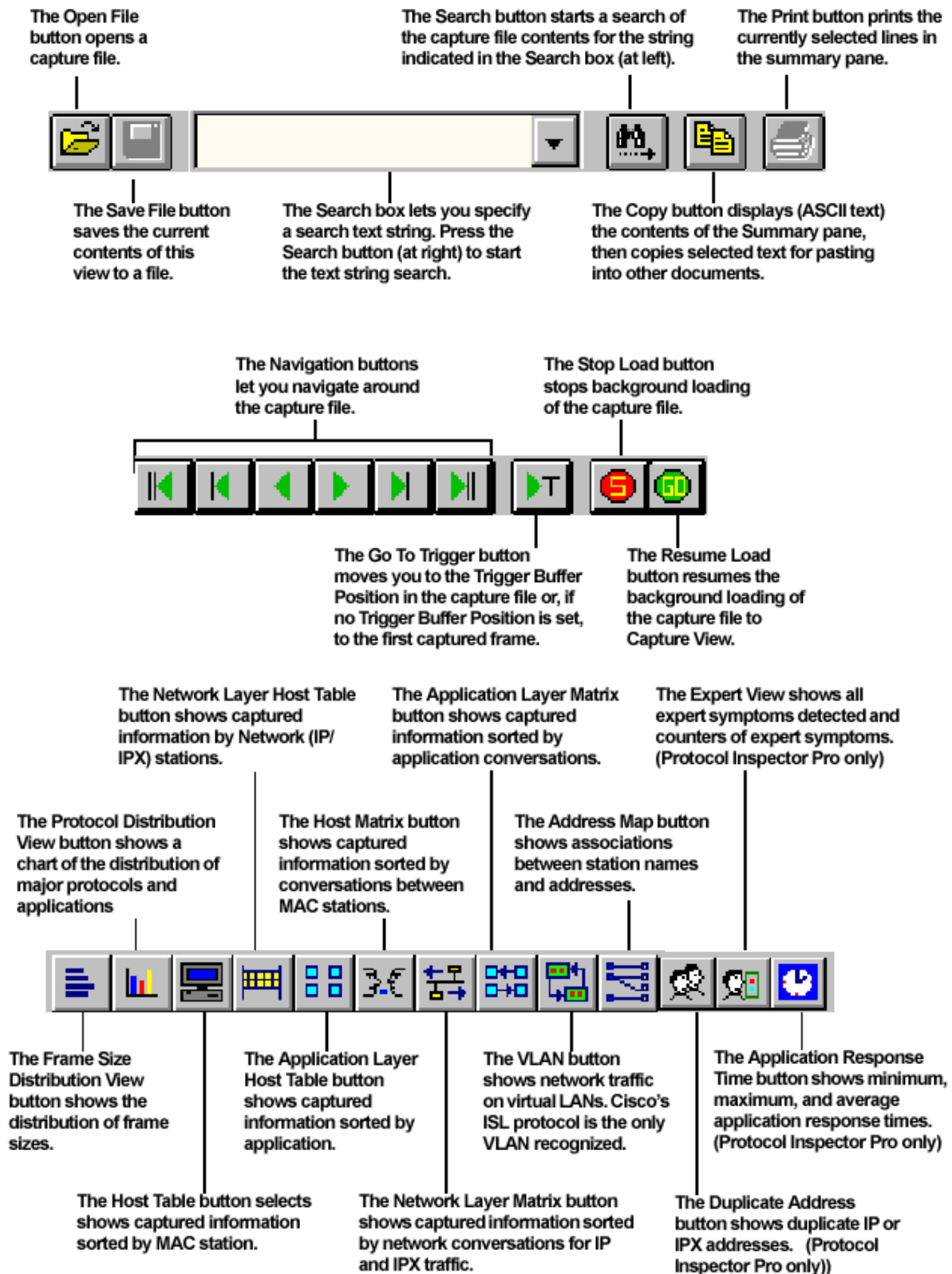
Create/Modify Filter Toolbar



State Toolbar



Capture View Toolbar



Function Keys

Function keys perform different operations within different Protocol Inspector views.

Function Key	Summary View	Detail View
F1	Help	Help
F2	System Settings	Capture View Display Options
F3	Module Settings	Module Settings
F4	Module Monitor View Preferences	Create Display Filter
F5	Connect to Remote	Create Capture Filter
F6	Load Capture Filter	Load Capture Filter
F7	Open Capture File	Expert Summary View
F8	Save Capture	Save Capture
F9	Go to Detail View	Capture View
F10	Start/Stop	Start/Stop
F11	N/A	N/A
F12	N/A	N/A

Other Keyboard Shortcuts...

Key Combination	Action
Alt + F4	Close Window
Ctrl + O	Open
Ctrl + S	Save
Ctrl + T	Start Module
Ctrl + P	Stop Module