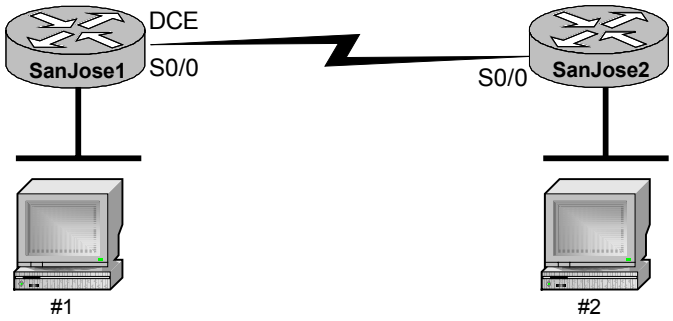
Lab 7.1.9b Introduction to Fluke Protocol Inspector



Objective

This lab is a tutorial demonstrating how to use the Fluke Networks Protocol Inspector to analyze network traffic and data frames. This lab will demonstrate key features of the tool that can be incorporated into various troubleshooting efforts in the remaining labs.

Background / Preparation

The output in this lab is representative only. Output will vary depending on the number of devices added, device MAC addresses, device hostnames, which LAN is joined, and so on.

This lab introducing Protocol Inspector will be useful in later troubleshooting labs as well as in the field. While the Protocol Inspector (PI) software is a valuable part of the Academy program, it is also representative of features available on other products in the market.

Note: The configuration files used for this lab are available from the instructor. They will be used for other labs, so please do not change any configuration settings. The configuration contains several components for testing purposes and is not intended to represent a good production configuration.

At least one of the hosts must have the Protocol Inspector software installed. If the lab is done in pairs, having the software installed on both machines means that each person can run the lab steps. However, each host may display slightly different results.

Step 1 Cable the lab as shown in the diagram

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

Load the configuration files Lab3-SanJose1Config.txt and Lab3-SanJose2Config.txt into the appropriate routers. These files are available from the instructor.

Configure the workstations as follows, which is the same as the NI lab:

Host #1	**Host #2**
IP Address: 192.168.1.10	IP Address: 192.168.2.10

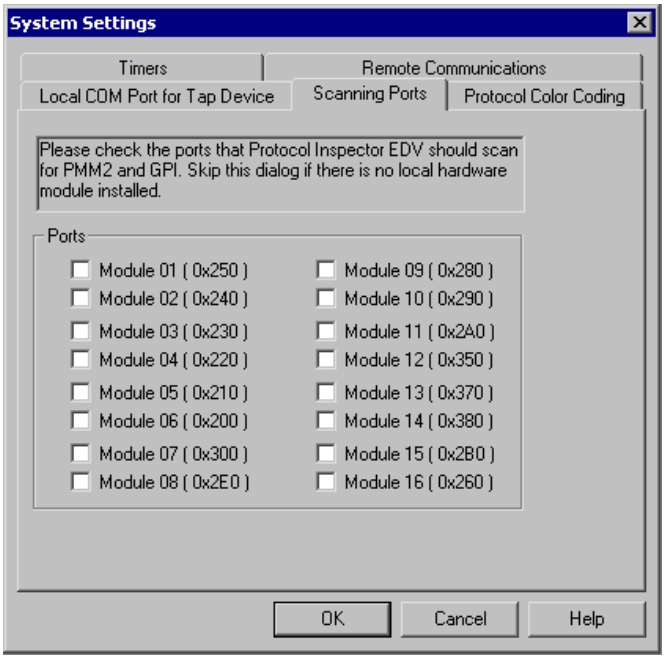
Subnet mask: 255.255.255.0	Subnet mask: 255.255.255.0
Default Gateway: 192.168.1.1	Default Gateway: 192.168.2.1

Step 2 Start Protocol Inspector EDV program

From the Start menu, launch the Fluke Protocol Inspector EDV program.

Note: The first time the program is run, a message will appear that asks, **"Do you have any Fluke analyzer cards or Fluke taps in your local system?"**

If using the educational version, click on **No**. If answering yes or if the following screen appears, just click on **OK** without selecting any ports.

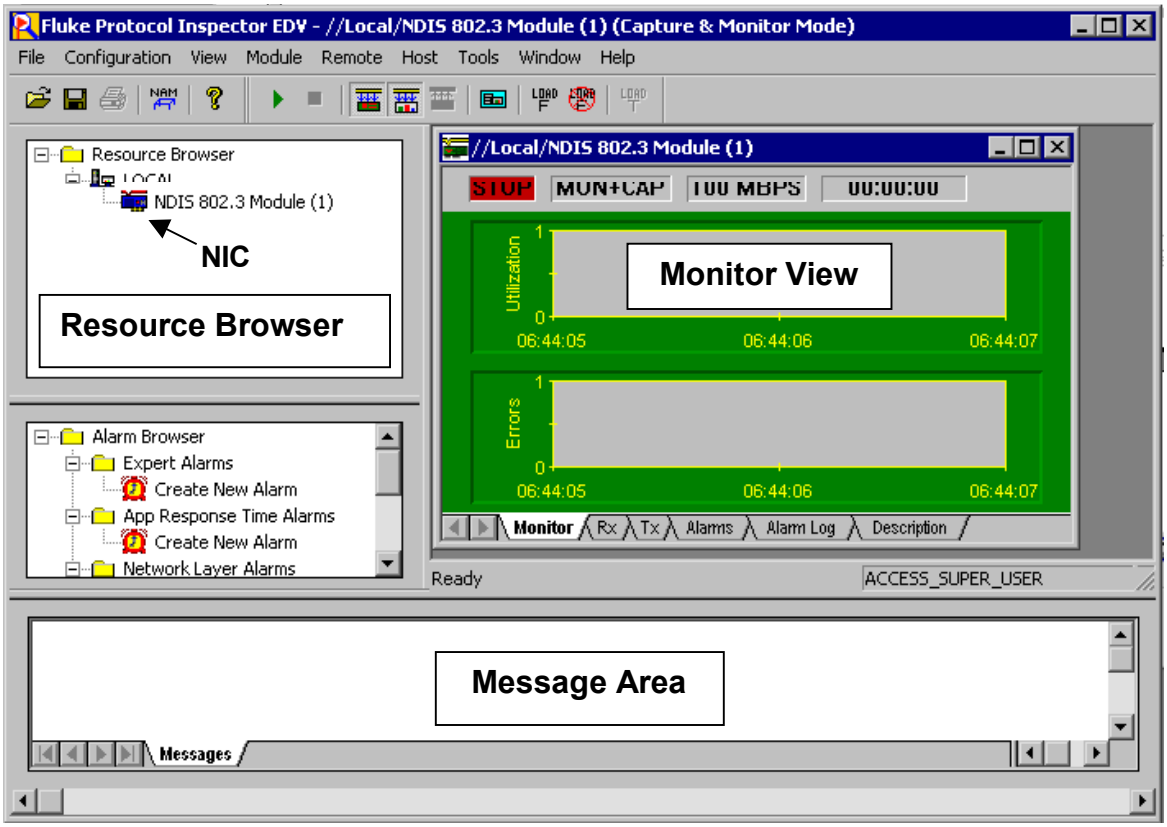


There are four main Protocol Inspector views, which include the following:

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

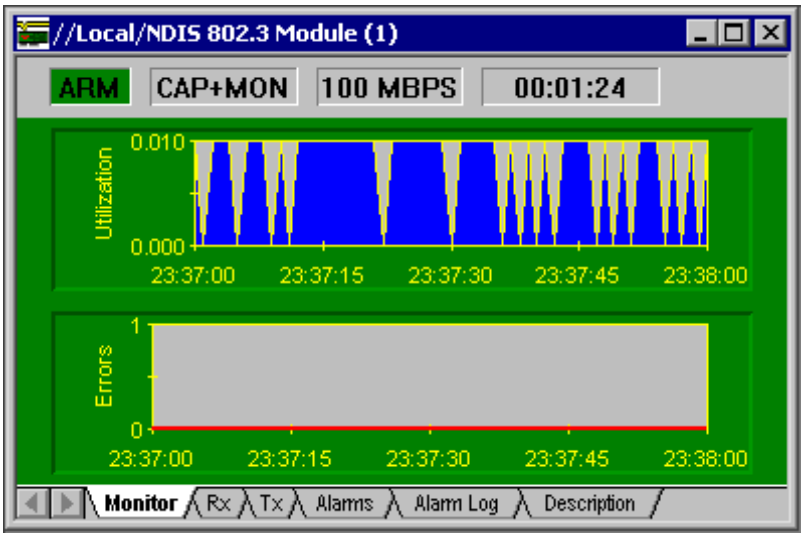
The program opens in the **Summary View**. This view shows several windows used by the tool. The **Resource Browser** window in the upper left corner shows the only monitoring device that is available, which is the NDIS 802.3 Module (NIC) of the host. If there were Protocol Media Monitors, they would 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 in the main window on the upper right, monitors one resource per window in a variety of viewing options. The example below and probably 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 Start the Monitor / Capture process

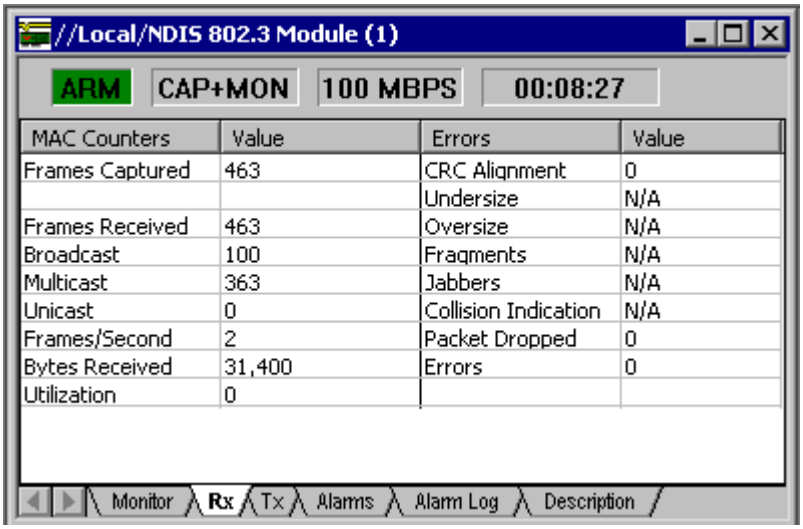
To start the monitoring/capturing process, use the Start button or Module | Start from the menu system. The Utilization chart should start showing activity like the graphic below:



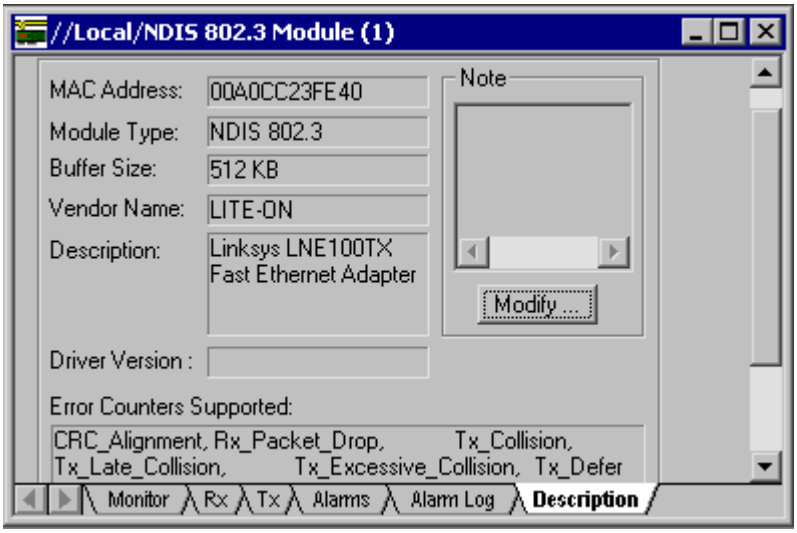
The word **Arm** should appear where **Stop** had been before. If opening the **Module** menu, notice that **Stop** is now an option while **Start** is muted. Do not stop the process yet. Restart it again if it is stopped.

The tabs at the bottom of the window show the resulting data in a variety of forms. Click on each and note the result. **Transmit** (**Tx**), **Alarms,** and **Alarm Log** will be blank. The following is the **Received**

(**Rx**) frames, which indicates that **Broadcast** and **Multicast** frames are being received, but they may not show any **Unicasts**.

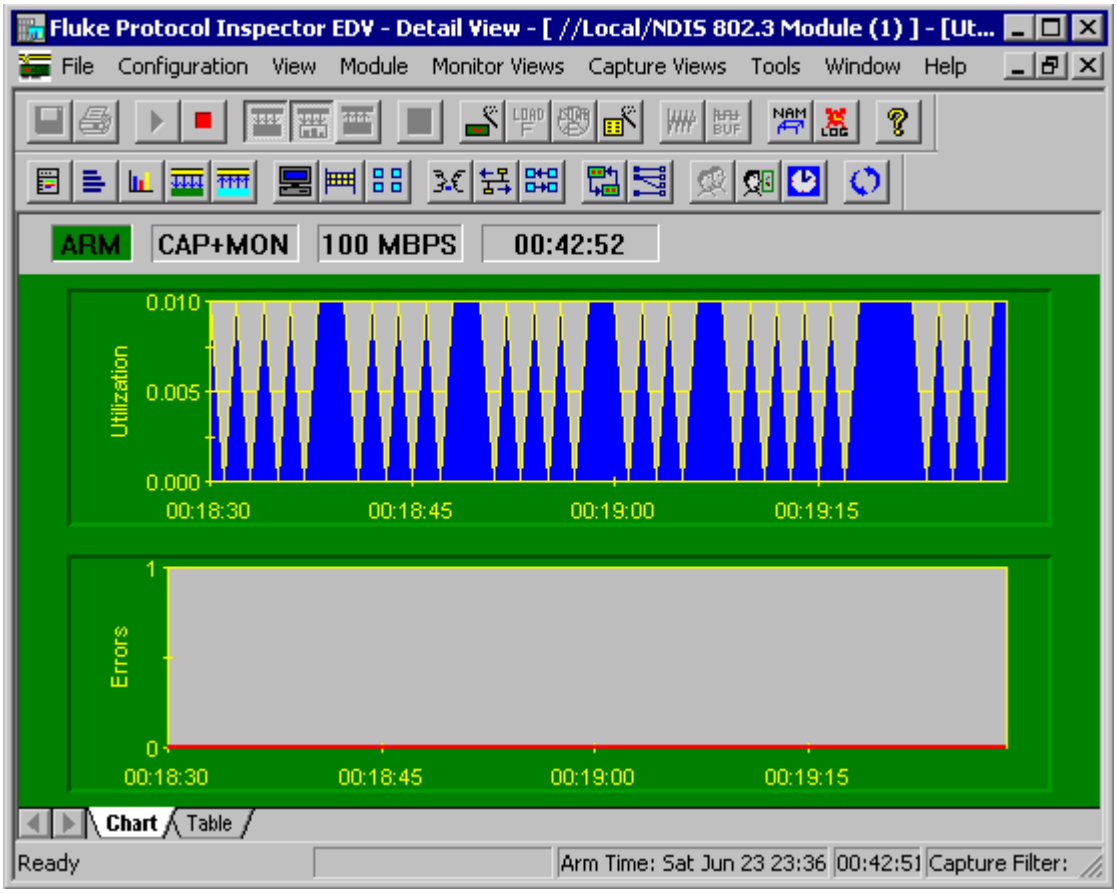


Using the console connection to the router, ping the monitoring host (192.168.1.10 or 192.168.2.10), and notice that **Unicast** frames appear. Unfortunately, the errors shown in the third column will not appear in the lab exercise unless a traffic generator like the Fluke Networks OptiView product has been added.

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.	

Step 4 View Details

To go to the **Detail View** window click on the **Detail View**  button in the toolbar or double click anywhere on the Monitor View chart. This will open a second window that should look something like the following, after maximizing the **Utilization / Errors Strip Chart (RX)** window.



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

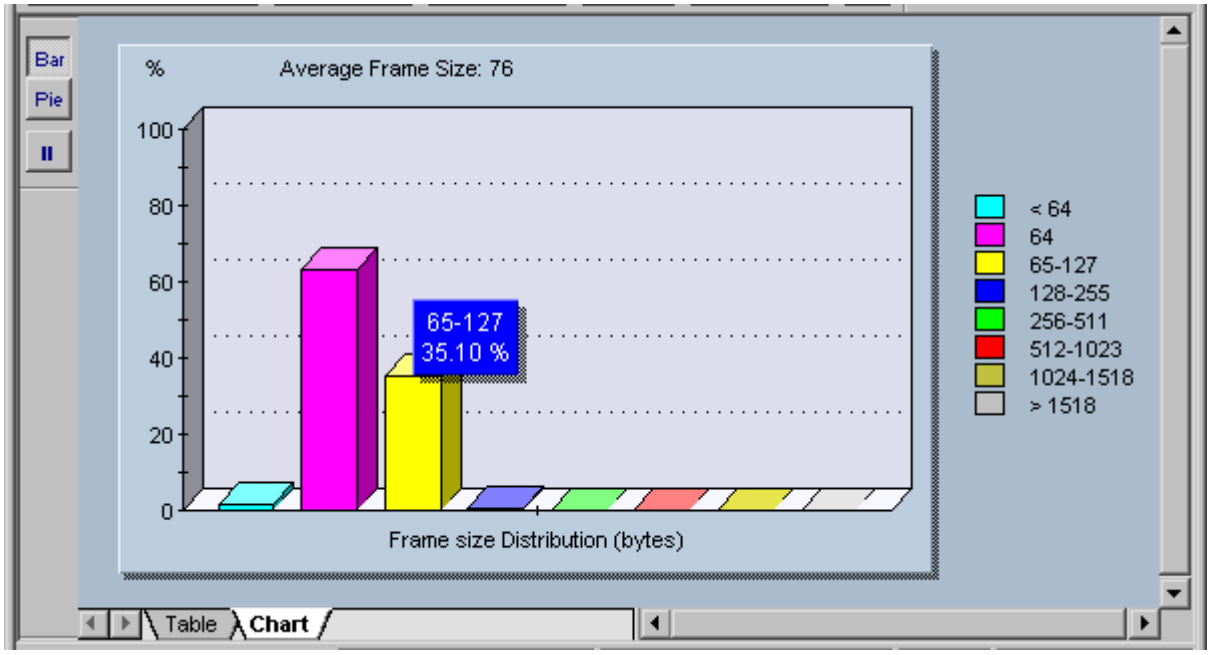
Initially, the chart output is the same as before. However, there are many more toolbar and menu options than in the Summary View. Before looking at these features, confirm that the **Chart** and **Table** tabs show the same information that was seen earlier.

Like all Windows compliant programs, placing the mouse over a button brings up a screen tip briefly identifying the purpose of the button. As the mouse moves over the buttons, notice that some are muted. This means that the feature is not appropriate under the current circumstances. In some cases, it is not supported in the educational version.

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

Click on the **Mac Statistics** button to see the Rx frame table data displayed in another 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 frames being received by the NIC. Placing the mouse over any bar will display a small summary like the one shown below. Maximize the resulting window.

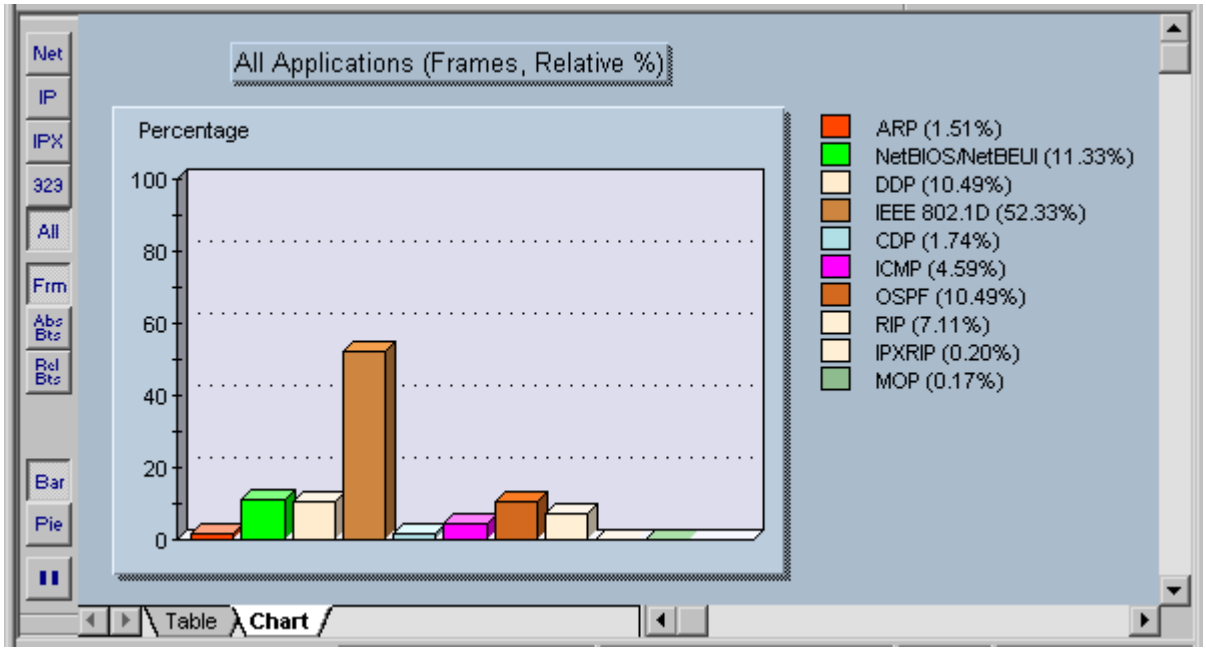


Try the **Pie**, **Bar**, and **Pause** buttons in the upper-left corner. Note that the **Pause** stops the capture, so click on it again to resume the capture. Look at both the **Table** and **Chart** tab displays as well.

With the sample configurations, the student should be getting mainly small frames, because the only thing happening is routing updates. Try using the extended Ping feature from the router Console connection, and specify 100 pings with a larger packet size.

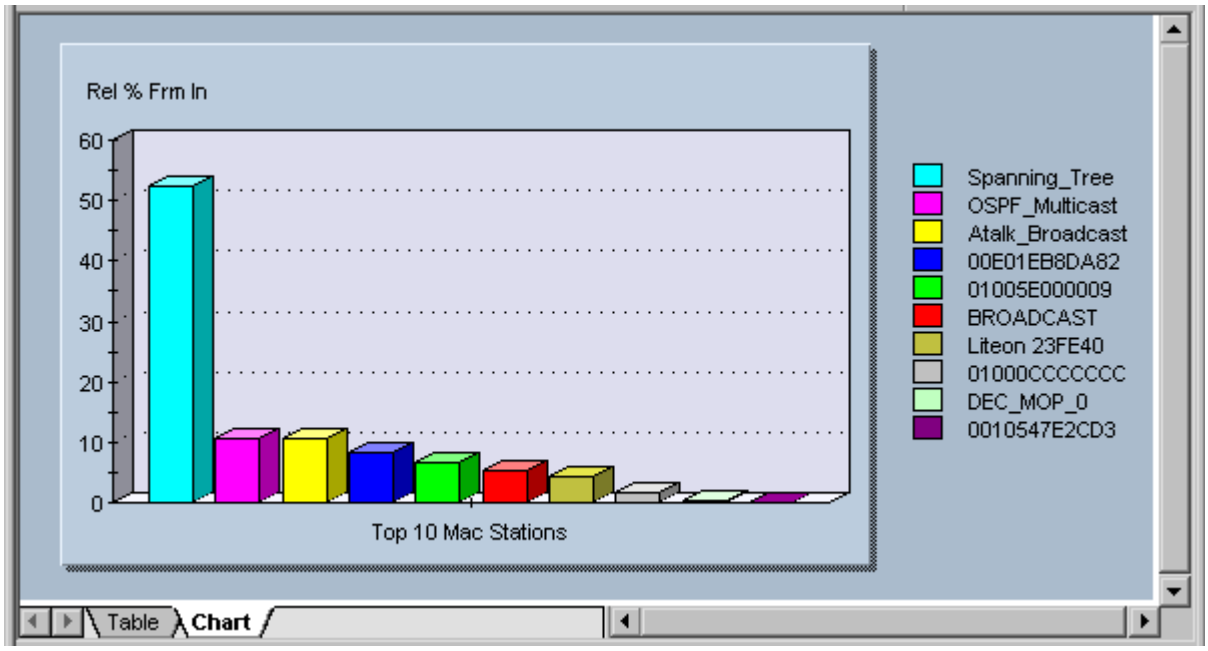
If maximizing each new display, return to any previous view by using the Window menu. The student can also **Tile** the windows. Experiment with the Window menu features and then close any unwanted views.

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



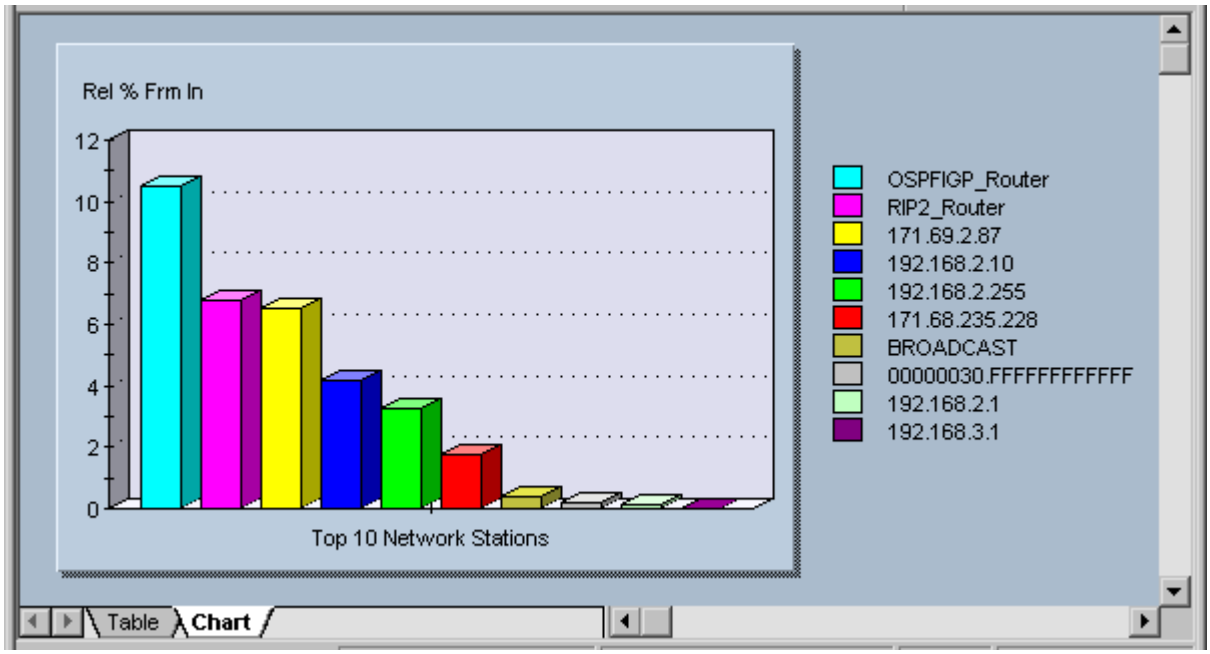
Try each of the buttons and tabs to see the results. The **Net** button shows only network protocols. The **323** button refers to the H323 Voiceover IP protocols. Look at the **Frm** (frame) and the **Abs Bts** (absolute bytes) and **Rel Bts** (relative bytes) to see the results. Remember that the **Pause**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

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



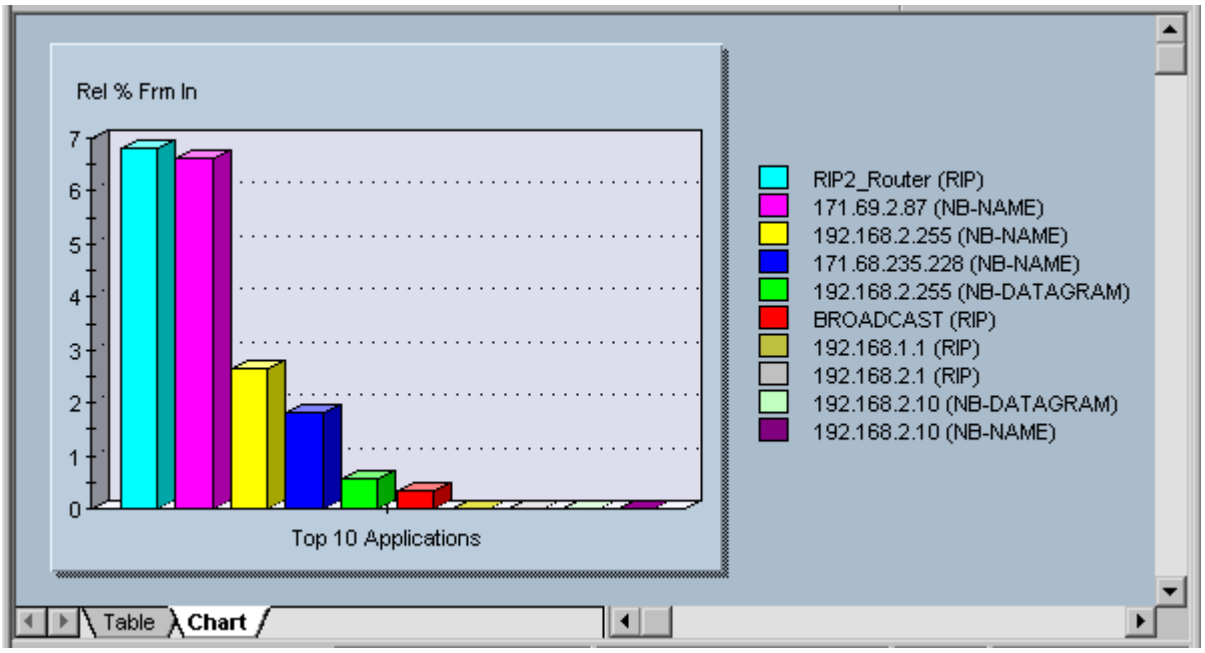
Notice the Spanning Tree, AppleTalk, and OSPF traffic. Be sure to look at the **Table** tab to see the actual values.

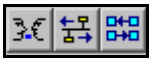
Click on the **Network Layer Host Table** button to see the network (IP/IPX) stations and related traffic.

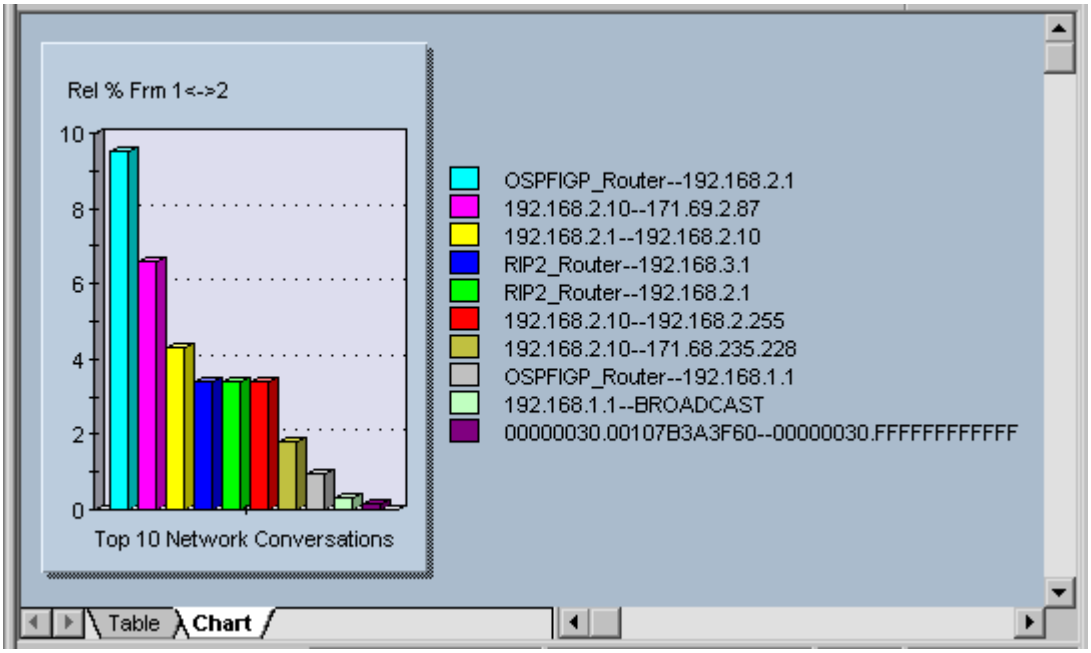


Any pings and any additional hosts that might have added to the configuration will impact the actual addresses that appear on the right.

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



Experiment with the next three  buttons. They create host-to-host matrices for MAC, Network, and Application layer conversations. The following is an example of the Network Layer (IP/IPX) conversations.



Of the next two  buttons, the first is the **VLAN** button that shows network traffic on VLANs. This sample does not use VLANs. Remember this button when troubleshooting VLANs later.

The second button creates a matrix comparing 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	OSPFIGP_Router	224.0.0.5
IP	OSPFIGP_Router_0	224.0.0.6

The **Expert View**  button shows the expert symptoms discovered. These statistics are how the PIs try to point out potential problems. The underlined options bring up additional detail windows if there are any values recorded. The sample for this lab will not show much, but it will look over the options for debugging ISL, HSRP, and other types of problems that will be seen in later labs.

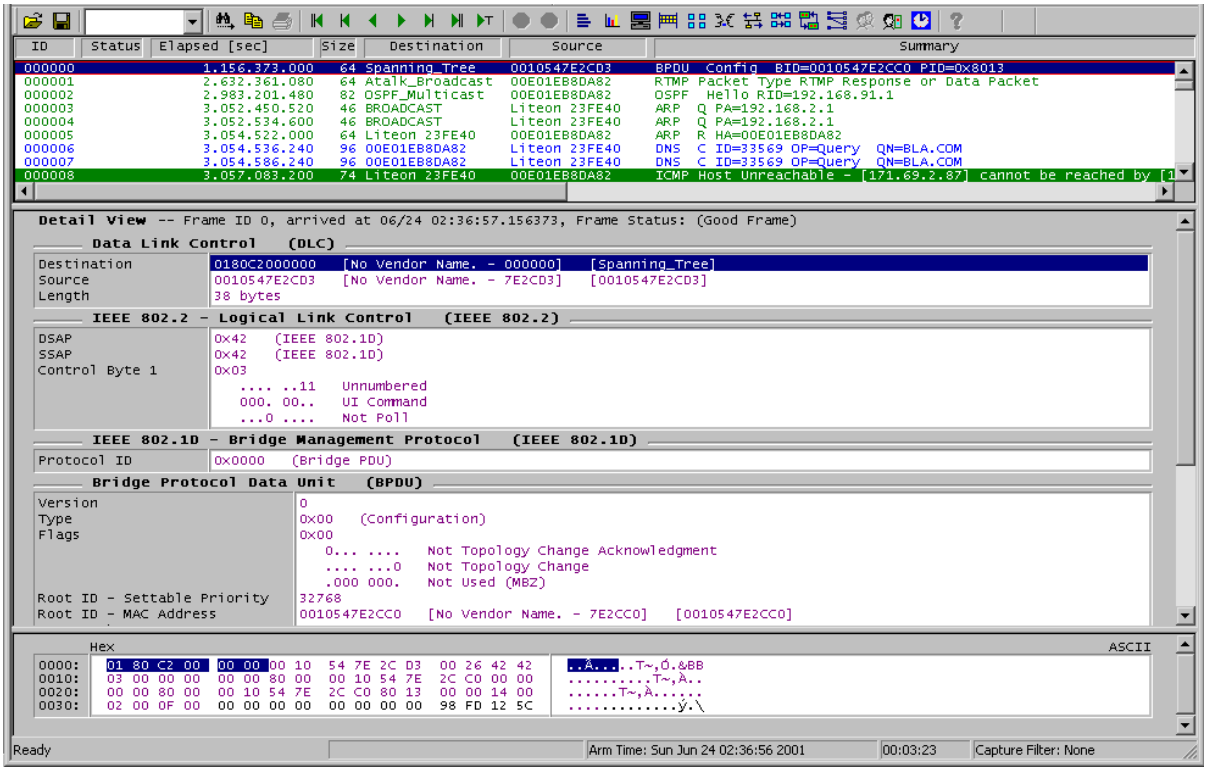
Expert Category	Value	Expert Category	Value
ICMP All Errors	368	Duplicate Network Address	0
ICMP Destination Unreachable	368	Unstable MST	0
ICMP Redirects	0	SAP Broadcast	0
Excessive Bootp	0	OSPF Broadcast	923
Excessive ARP	0	RIP Broadcast	25
NFS Retransmissions	0	ISL Illegal VLAN ID	0
TCP/IP SYN Attack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

Step 5 Stop the capture process

To stop the frame capture to look at individual frames use the **Stop**  button or Module | Stop from the menu.

Once the capture has been stopped, click on the **Capture View** button. With the education version, a message box appears announcing that the capture is limited to 250 packets. Just click OK.

The resulting window can be a little overwhelming at first. Maximize the window to hide any other windows open in the background.

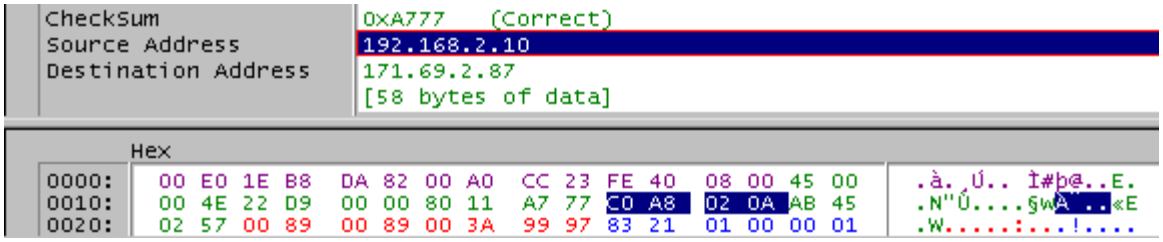


In looking over the results, note that there are actually three horizontal windows open. The top window lists the captured packets. The middle window shows the detail of the selected packet in the top window, and the bottom window shows the HEX values for the packet.

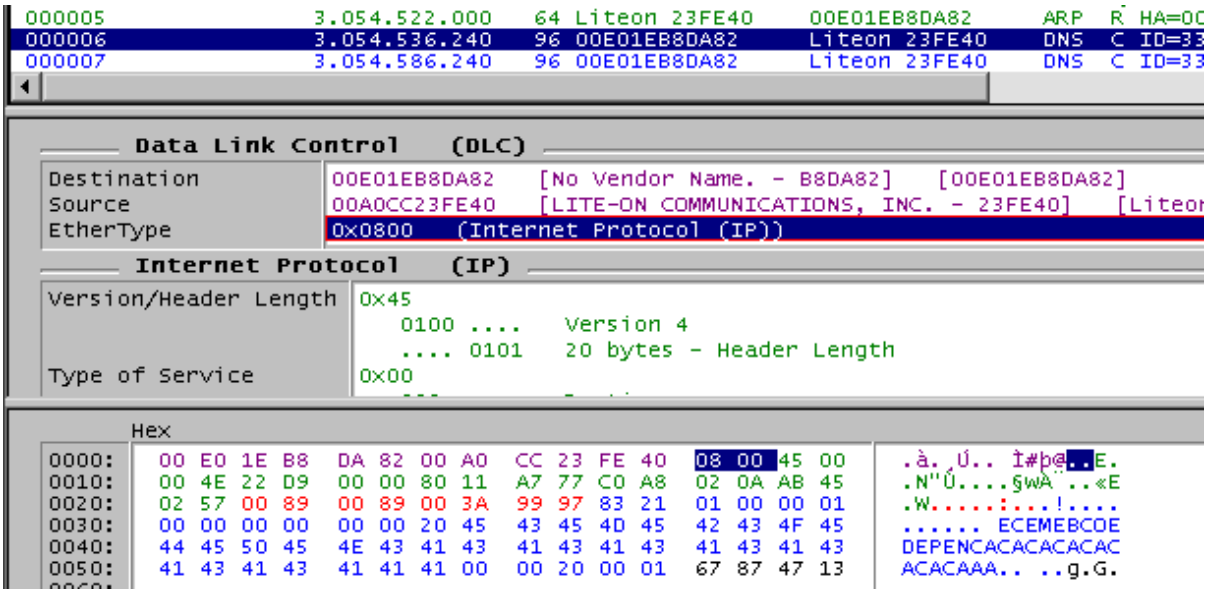
By positioning the mouse over the borders among the three windows, a line mover or two-headed arrow will appear. This allows the distribution of space for each window to be changed. It may be advantageous to make the middle window as large as possible and leave five to six rows in each of the other two, as shown above.

Look over the packets listed in the top window. DNS, ARP, RTMP, and other types of packets should be found. If using a switch, there should be CDP and Spanning Tree packets. Notice that as rows are selected in the top window, the contents of the other two windows change.

Select information in the middle window, and notice that the HEX display in the bottom window changes to show where that specific information is stored. In the following example, selecting the Source Address (IP) shows HEX values from the packet.

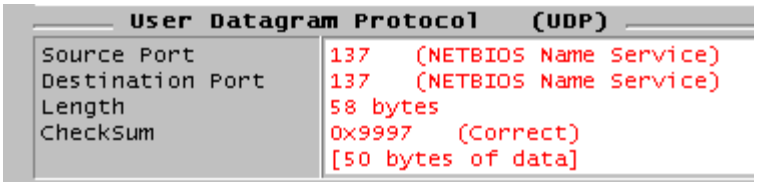


Note also the color coding makes it easier to locate information from the middle window in the HEX window. In the following example with a DNS packet, the data in the Data Link Control (DLC) section of middle window is purple, while the Internet Protocol (IP) section is green. The corresponding HEX values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



Notice in the above example the **EtherType** is **0x0800**. This indicates that it is an IP packet. Notice the MAC addresses for both the Destination and Source hosts as well as where that data is stored in the HEX display.

In the same example, the next section in the middle window is the **User Datagram Protocol (UDP)** information, which includes the UDP port numbers.



The structure of the middle window changes for each type of packet.

Take a few minutes to select different packet types in the top window, and then look over the resulting display in the other two windows. Pay particular attention to the EtherType, any port numbers, as well as source and destination addresses, which include both MAC and network layer. There should be RIP, OSPF, and RTMP or AppleTalk packets in the capture. Make sure that the important data can be located and interpreted. In the following RIP capture, notice that this is a RIP version 2 packet. The multicast destination address is 224.0.0.9,and that the actual route table entries can be seen. What would the multicast destination address be 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, figure out the platform. The following is from a Catalyst 1900 switch.

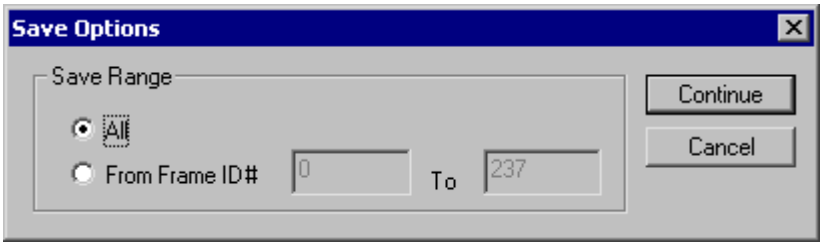
```
Variable Type           0x0006 (Platform)
Variable Length         14
Platform                cisco 1900

0030:  00 00 01 01  01 CC 00 04  C0 A8 01 64  00 03 00 06   .....Ì..À¨.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
```

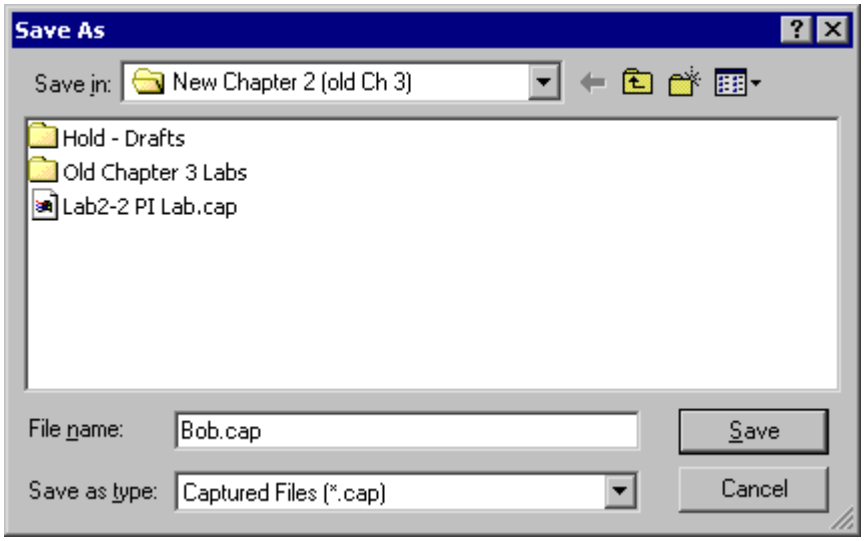
Experiment until comfortable with the tools.

Step 6 Save the captured data

To save captured data, use the **Save Capture**  button or choose File | Save Capture from the menu system. Accept the **All** option by using the **Continue** button. The student can save just a range of captured frames with this window.



Use a proper file name and store the file on the appropriate disk. If the CAP extension is showing when this window opens, make sure it remains after typing the name.



Use the **Open Capture File** button and open the file called Lab3-2 PI Lab.cap. If it is not available, then open the file that was just saved.

The student is now using the **Capture View of Capture Files**. There is no difference in tools, but the title bar at the top of the screen indicates that a file is being viewed rather than a capture in memory.

Step 7 Examine frames

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

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

Experiment until comfortable with the tools.

Reflection

a. How might this tool be used in troubleshooting?

_____

b. Is all of the data on the network being analyzed?

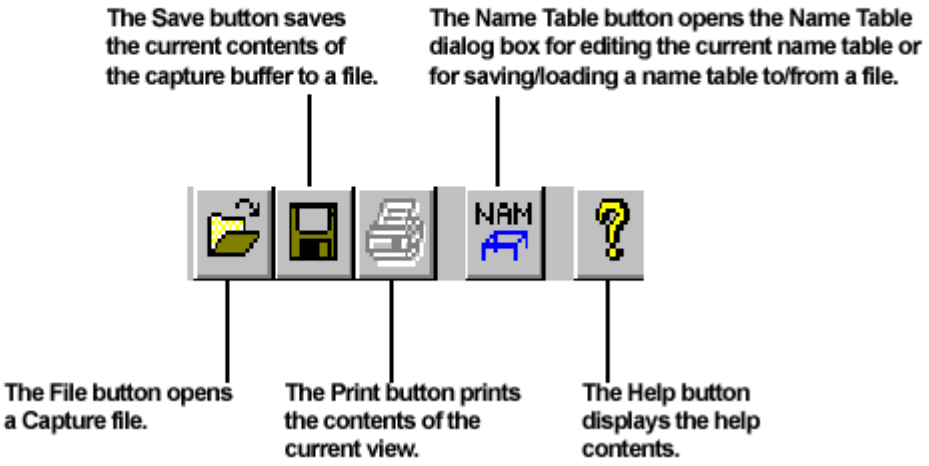
_____

c. What is the impact of being connected to a switch?

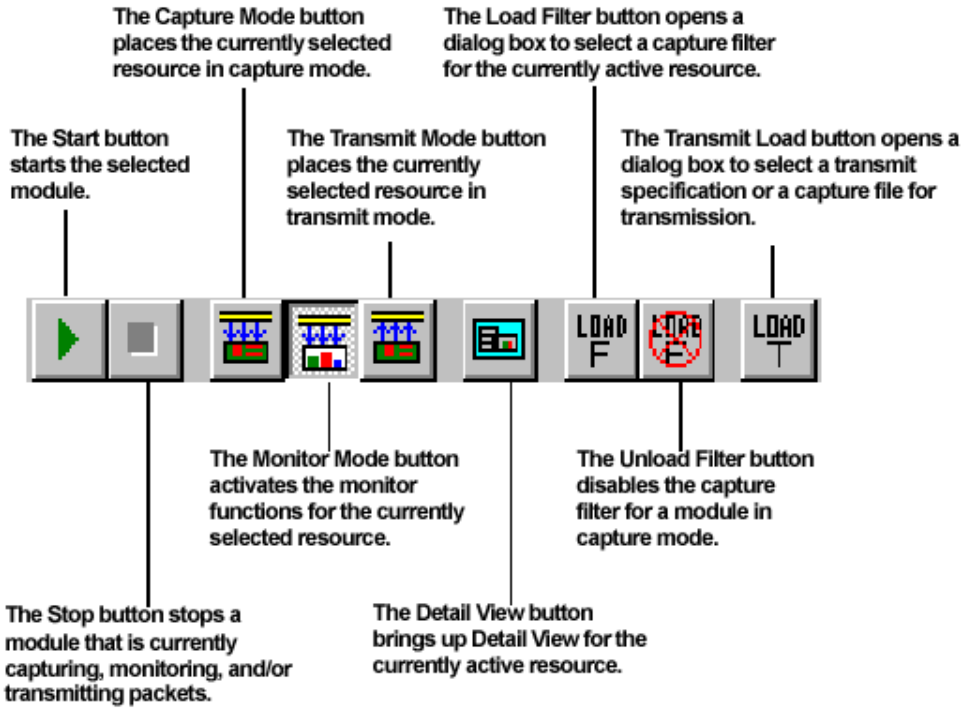
_____

Appendix: Toolbars

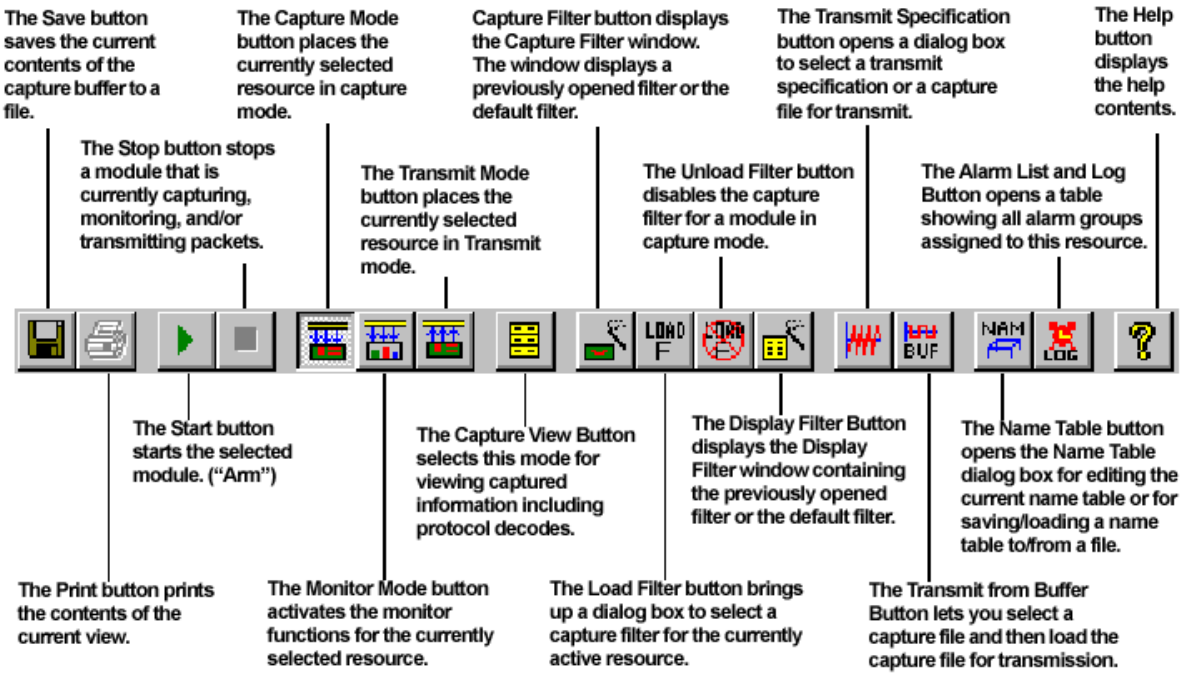
Protocol Inspector Toolbar



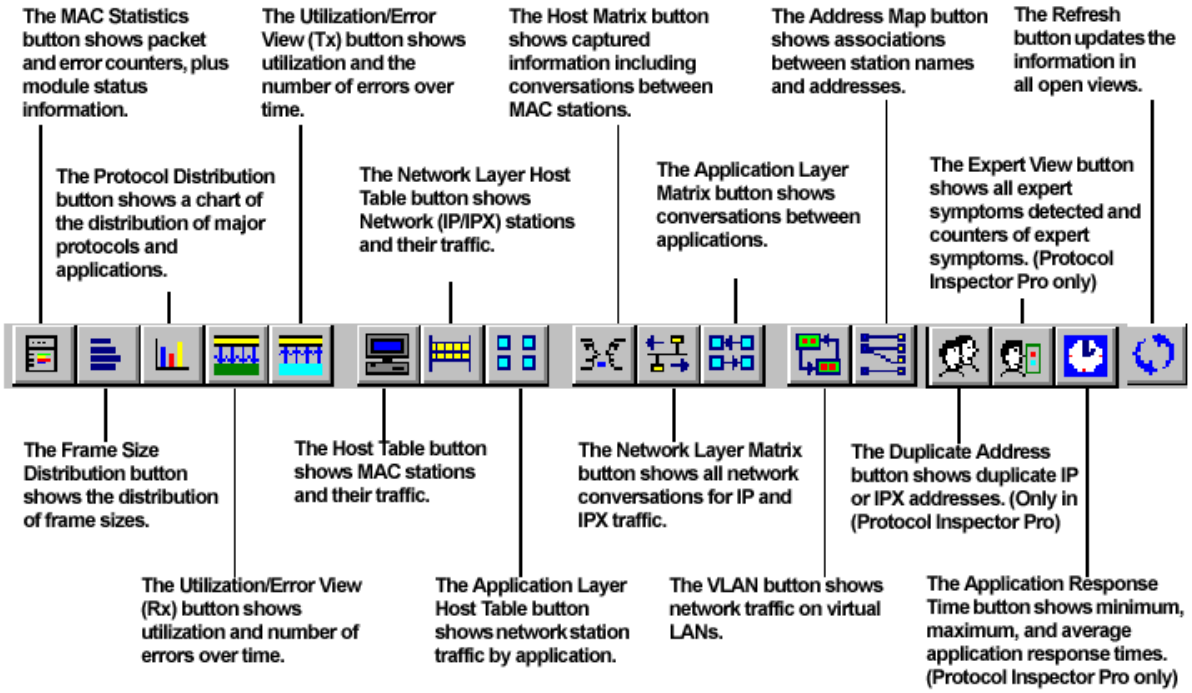
Module Toolbar (Summary View)



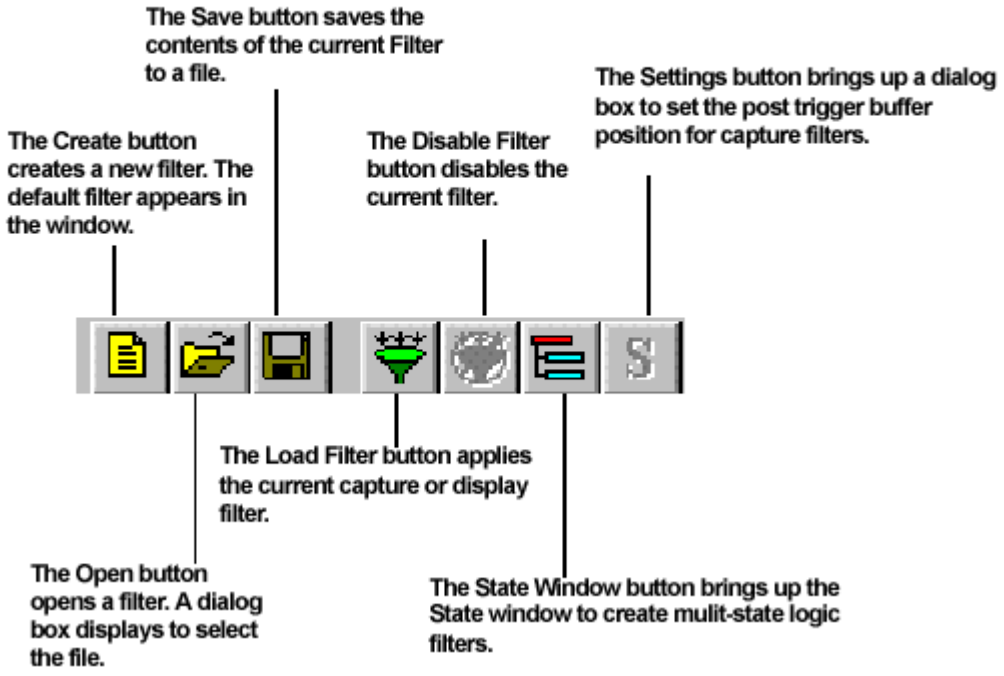
Detail View Toolbar



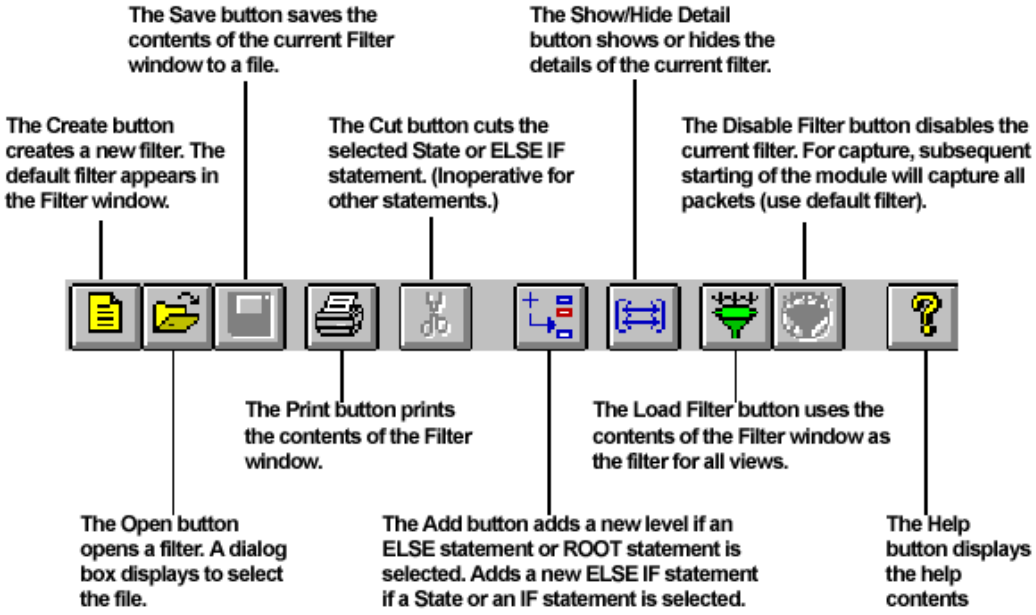
Data Views Toolbar (Note: Only some of these views are available with GMM cards)



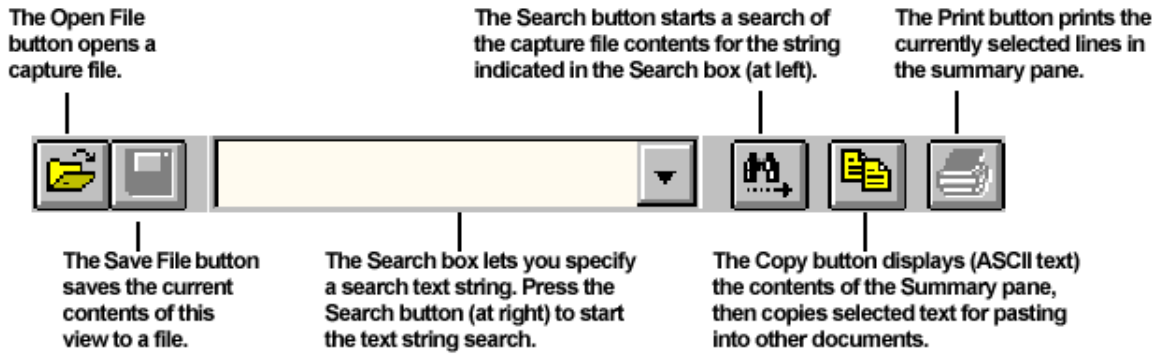
Create/Modify Filter Toolbar

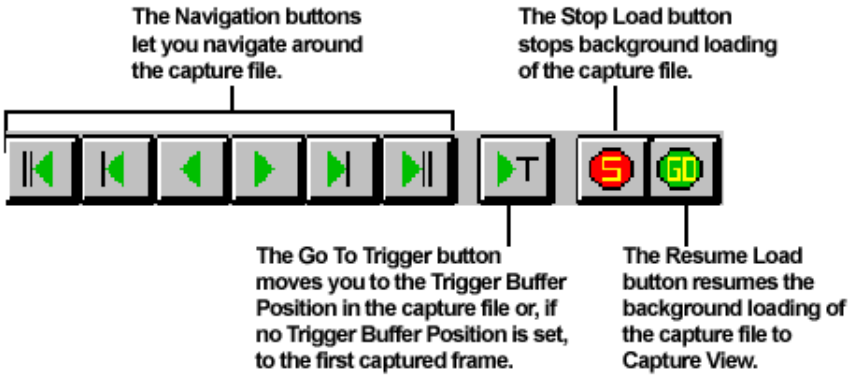


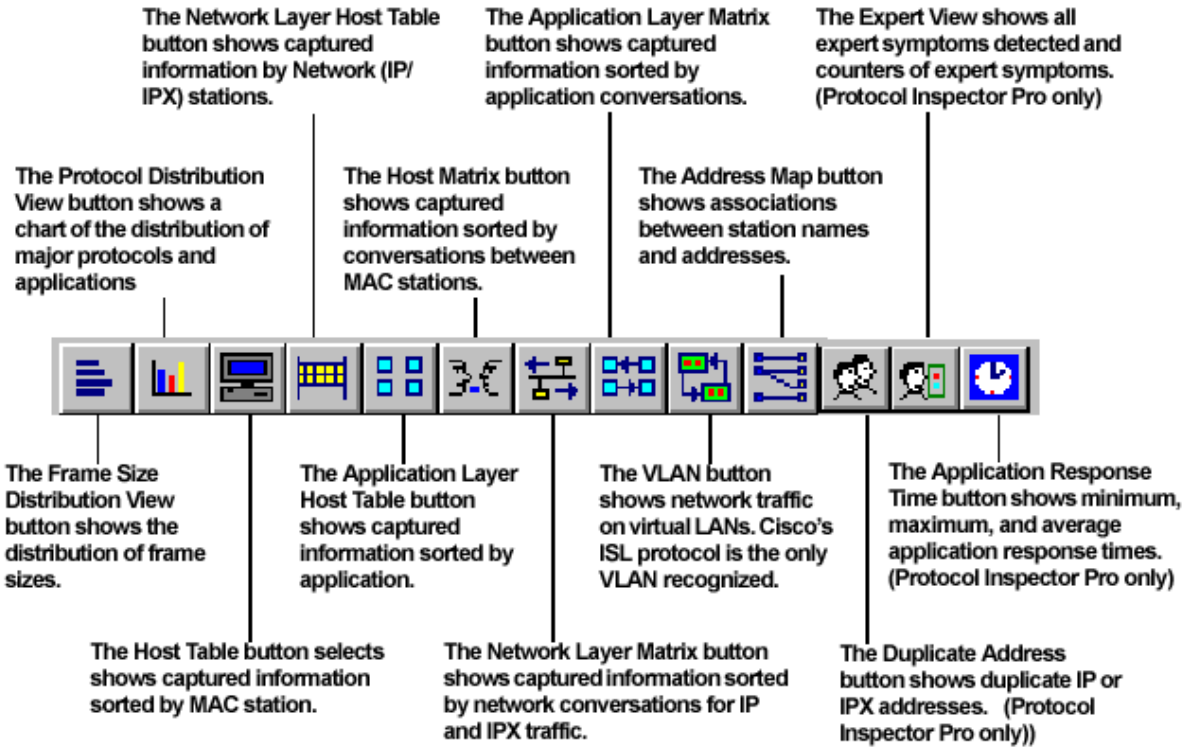
State Toolbar



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