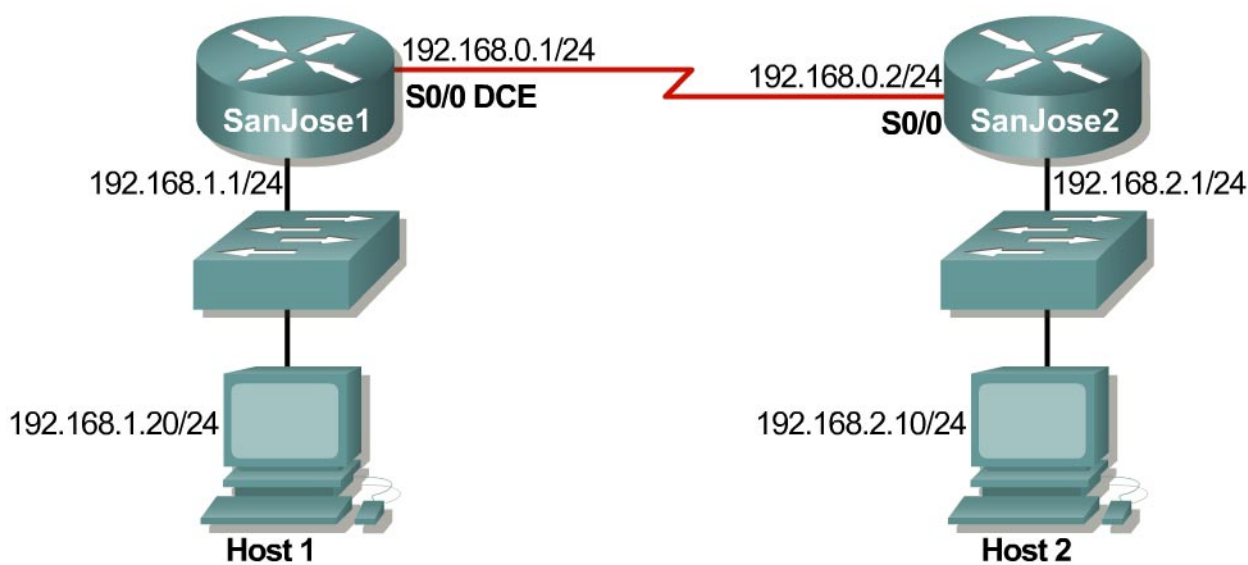


Práctica de laboratorio 7.1.9b Introducción al Fluke Protocol Inspector



Objetivo

Esta práctica de laboratorio es un tutorial que demuestra cómo usar el Fluke Networks Protocol Inspector para analizar el tráfico de red y las tramas de datos. Esta práctica de laboratorio demuestra las características principales de la herramienta que se puede incorporar a varias tareas de detección de fallas en las próximas prácticas de laboratorio.

Información básica / Preparación

El resultado de esta práctica de laboratorio es solamente representativa. El resultado varía según la cantidad de dispositivos que se agregan, direcciones MAC de dispositivos, nombres de host de dispositivos, a qué LAN se conecta, etc.

Esta práctica de presentación de Protocol Inspector resultará útil en las prácticas de laboratorio posteriores de detección de fallas, y también en el campo. Si bien el software Protocol Inspector (PI) es una parte importante del programa de la Academia, también es representativo de las características de otros productos disponibles en el mercado.

Opciones para llevar a cabo esta práctica.

- 1) Usar Protocol Inspector o Protocol Expert en una LAN pequeña controlada, configurada por el instructor en un entorno de laboratorio cerrado como se muestra en la figura anterior. El equipo mínimo debe incluir una estación de trabajo, un switch y un router.
- 2) Realizar las tareas en un entorno de mayor tamaño, como la red del aula o de la escuela para ver mayor variedad de equipos. Antes de intentar de usar PI o PE en la LAN de la escuela, consulte al instructor y el administrador de la red.

Por lo menos uno de los hosts debe tener el software Protocol Inspector instalado. Si la práctica se realiza en grupos de dos, ambas personas pueden ejecutar las tareas de la práctica de laboratorio si

se instala el software en las dos máquinas. Sin embargo, cada host puede presentar resultados ligeramente diferentes.

Paso 1 Configurar la red de laboratorio y conectar una estación de trabajo a la LAN de la escuela

Opción 1. Si se selecciona el entorno de laboratorio cerrado, realice el cableado del equipo como se muestra anteriormente y cargue los archivos de configuración en los routers correspondientes. Es posible que estos archivos estén precargados. En caso contrario, solicítelos al instructor. Estos archivos deben admitir el esquema de direccionamiento IP como se muestra en la figura anterior y la tabla siguiente.

Configure las estaciones de trabajo según las especificaciones que se muestran en la figura anterior y la tabla siguiente.

Host Nr. 1	Host Nr. 2
Dirección IP: 192.168.1.20	Dirección IP: 192.168.2.10
Máscara de subred: 255.255.255.0	Máscara de subred: 255.255.255.0
Gateway por defecto: 192.168.1.1	Gateway por defecto: 192.168.2.1

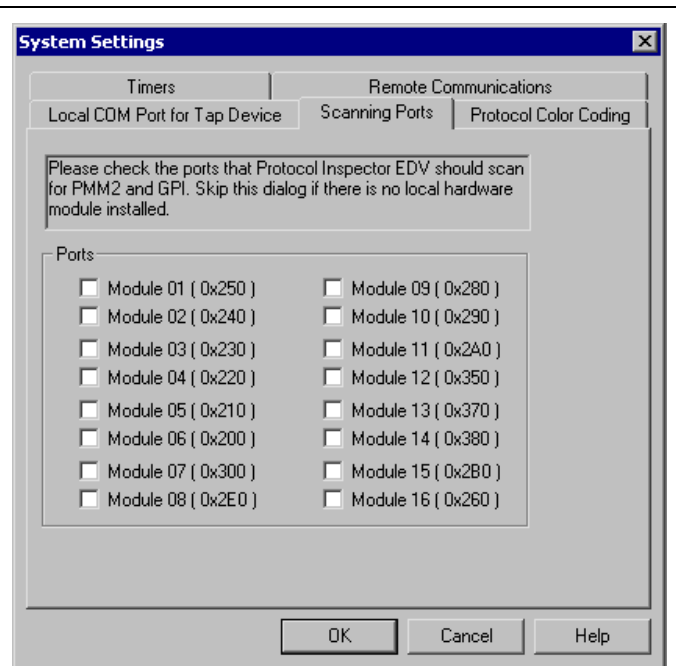
Opción 2. Si se selecciona la opción 2, conectarse a la LAN de la escuela, basta con conectar la estación de trabajo, con PI o PE instalados, directamente a un switch de un aula o un jack de datos conectados a la LAN de la escuela.

Paso 2 Iniciar el programa Protocol Inspector EDV

Desde el menú Inicio, abra el programa Fluke Protocol Inspector EDV.

Nota: La primera vez que se ejecuta el programa, aparece un mensaje que pregunta, **“Do you have any Fluke analyzer cards or Fluke taps in your local system?”** (¿Tiene tarjetas analizadoras Fluke o sensores Fluke en su sistema local?)

Si usa la versión educativa, haga clic en **No**. Si contesta que sí (Yes) o si aparece la siguiente pantalla, haga clic en **OK** sin seleccionar ningún puerto.

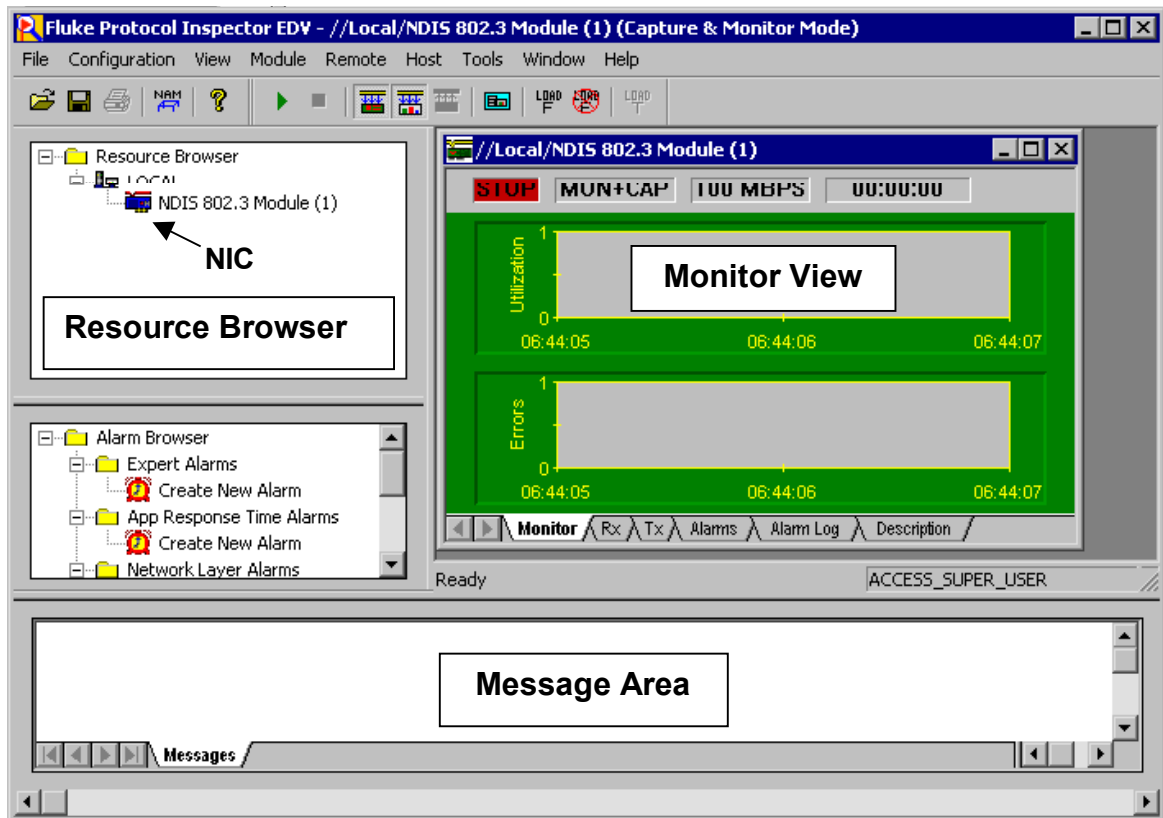


Hay cuatro vistas principales de Protocol Inspector, que incluyen lo siguiente:


- Vista resumida
- Vista detallada
- Vista de captura de búferes de captura
- Vista de captura de archivos de captura

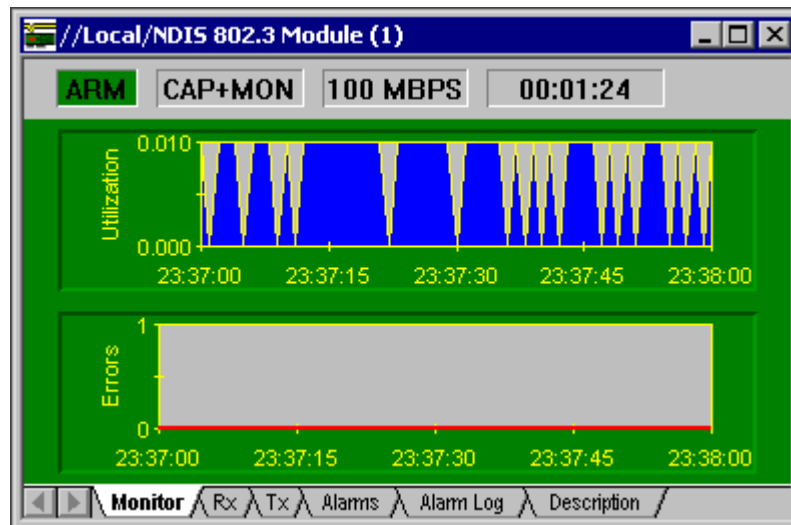
El programa se abre en **Summary View** (Vista resumida). Esta vista muestra varias ventanas que usa la herramienta. La ventana de **Resource Browser** (Navegador de recursos) en la esquina superior izquierda muestra el único dispositivo de monitoreo disponible, que es el Módulo NDIS 802.3 (NIC) del host. Si hubiera Monitores de Medios de Protocolo, se mostrarían con los dispositivos de host asociados. El **Alarm Browser** (Navegador de alarma) en el lado izquierdo y el **Message Area** (Área de mensajes) en la parte inferior se describirán más adelante.

La **Monitor View** (Vista de monitoreo), que es la ventana principal en la parte superior derecha, monitorea un recurso por ventana en una serie de opciones de vista. El ejemplo siguiente y probablemente la pantalla de inicio no muestran información en la ventana de la Vista de Monitoreo. **Stop** (Detener) en la esquina superior izquierda de la ventana de Vista de Monitoreo confirma que no se está realizando ningún monitoreo.



Paso 3 Inicio del proceso Monitoreo / Captura

Para iniciar el proceso de monitoreo/captura, use el botón Inicio  o Module | Start (Módulo | Inicio) desde el sistema de menús. El cuadro Utilization (Utilización) debe empezar a mostrar actividad, como en el gráfico siguiente:



La palabra **Arm** debe aparecer donde antes se veía **Stop**. Si se abre el menú **Module** (Módulo), observe que ahora **Stop** es una opción, mientras que **Start** aparece difuminado. No detenga el proceso aún. Reinicielo de nuevo si se detiene.

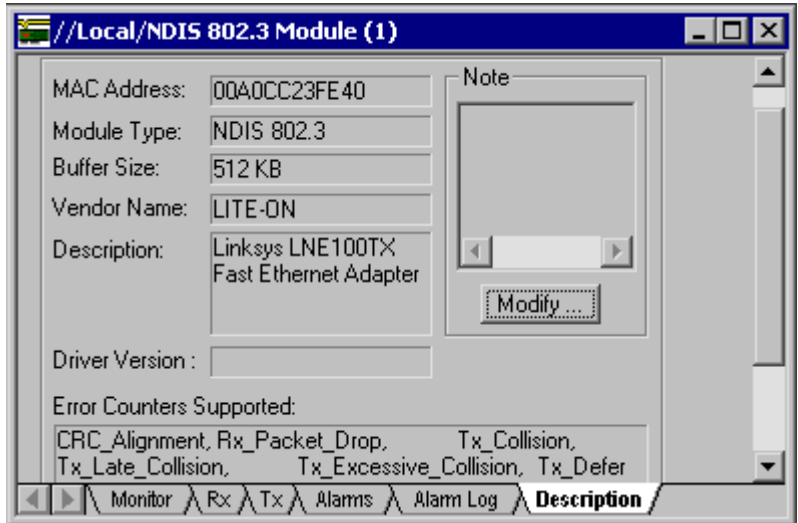
Las fichas en la parte inferior de la ventana muestran los datos resultantes en una variedad de formas. Haga clic en cada uno de ellos y observe los resultados. **Transmit (Tx)** (Transmitir), **Alarms** (Alarmas) y **Alarm Log** (Registro de alarmas) estarán en blanco. Lo siguiente son las tramas **Received (Rx)** (Recibidas), que indica que se están recibiendo tramas de **Broadcast y Multicast**, pero es posible que no muestren ningún **Unicast**.

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


Mediante la conexión de consola al router, haga ping al host controlador (192.168.1.10 ó 192.168.2.10) y observe que aparecen tramas de **Unicast**. Desafortunadamente, los errores que aparecen en la tercera columna no aparecen en la práctica de laboratorio, a menos que se agregue un generador de tráfico como el producto Fluke Networks OptiView.

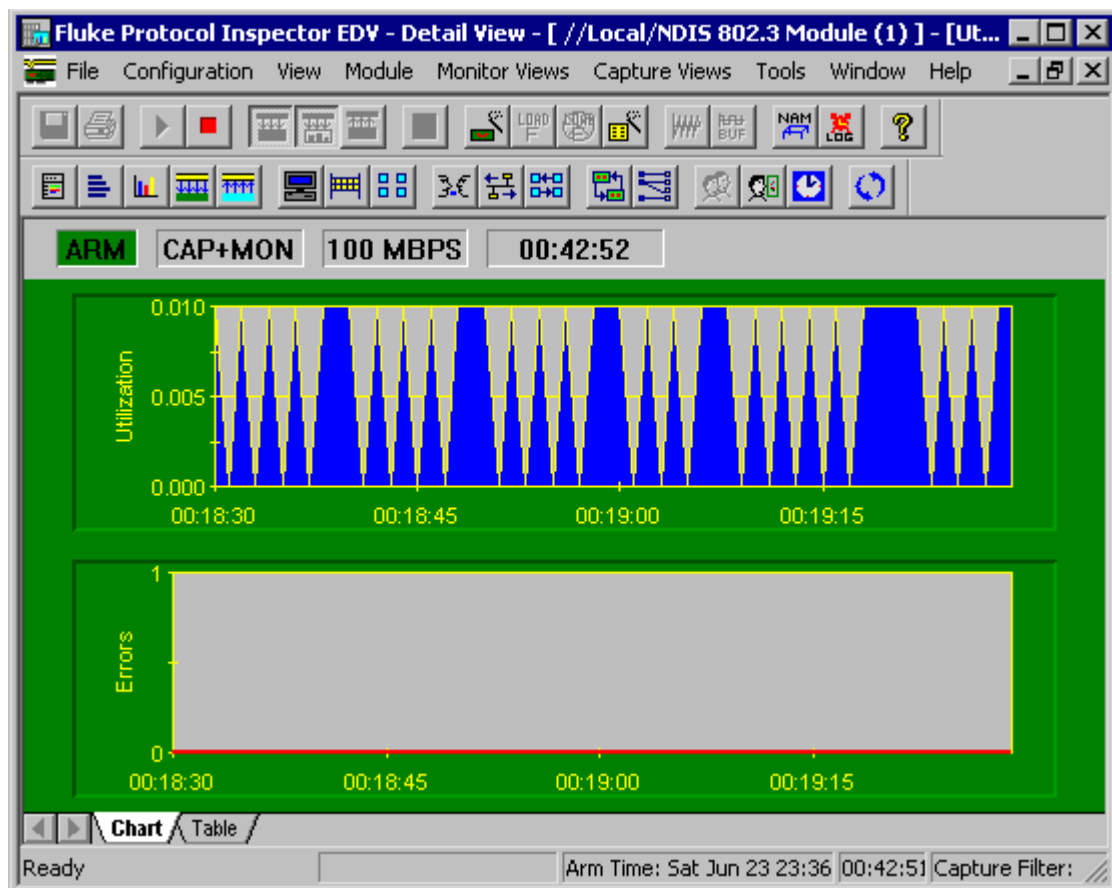
La ficha **Description** (Descripción) muestra la dirección MAC, fabricante y modelo de la NIC. Muestra también cuáles son los Contadores de Errores activados.

Tómese unos minutos para familiarizarse con las fichas y las funciones de desplazamiento de la ventana.



Paso 4 Ver los detalles

Para ir a la ventana de **Detail View** (Vista detallada) haga clic en el botón **Vista detallada**  en la barra de herramientas o haga doble clic en cualquier parte en el diagrama Monitor View (Vista de monitoreo). Esto abre otra ventana que debe tener un aspecto similar a lo siguiente, después de maximizar la ventana **Utilization / Errors Strip Chart (RX)** (Utilización / Diagrama de errores (RX)).





Nota: De ser necesario, active todas las barras de herramientas en el menú View (Ver).

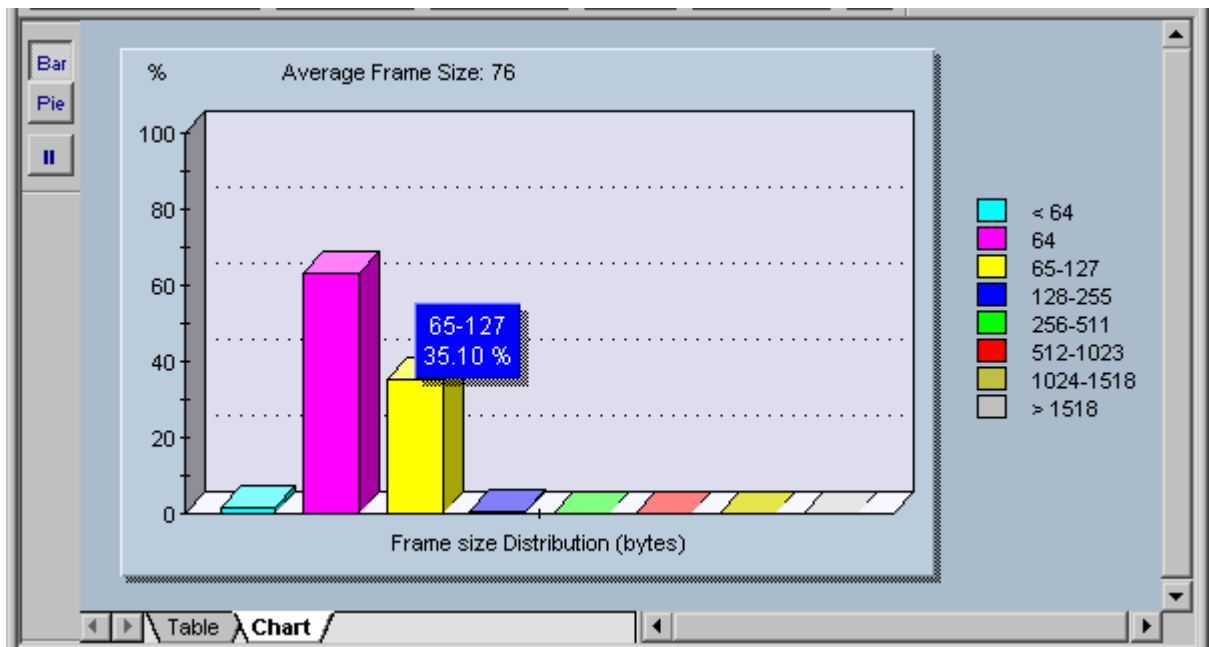
Al principio, el resultado del diagrama es el mismo de antes. Sin embargo, hay muchas más opciones de barra de herramientas y menús que las que se ven en la Vista Resumida. Antes de examinar estas funciones, verifique que las fichas **Chart** (Diagrama) y **Table** (Tabla) muestran la misma información que se vio anteriormente.


Al igual que todos los programas compatibles con Windows, al colocar el puntero del ratón sobre un botón, aparece una pantallita que identifica el propósito del botón. Al pasar el ratón sobre los botones, verá que algunos aparecen difuminados. Esto significa que esta función no es apropiada para la situación actual. En algunos casos, estas funciones no corresponden a la versión educativa.

Nota: Hay una vista completa de las barras de herramientas y lo que hacen en el Apéndice al final de esta práctica.

Haga clic en el botón **Estadísticas Mac**  para ver los datos de tabla de tramas de Rx en otro formato. El resultado debe ser obvio. Maximice la ventana resultante. Una información nueva es **Speed** (Velocidad), que muestra la velocidad de transmisión de la NIC.


Haga clic en el botón **Distribución del tamaño de trama**  para ver una distribución del tamaño de tramas recibidas por la NIC. Al colocar el puntero del ratón sobre cualquier barra, aparece un pequeño resumen como el que se ve a continuación. Maximice la ventana resultante.

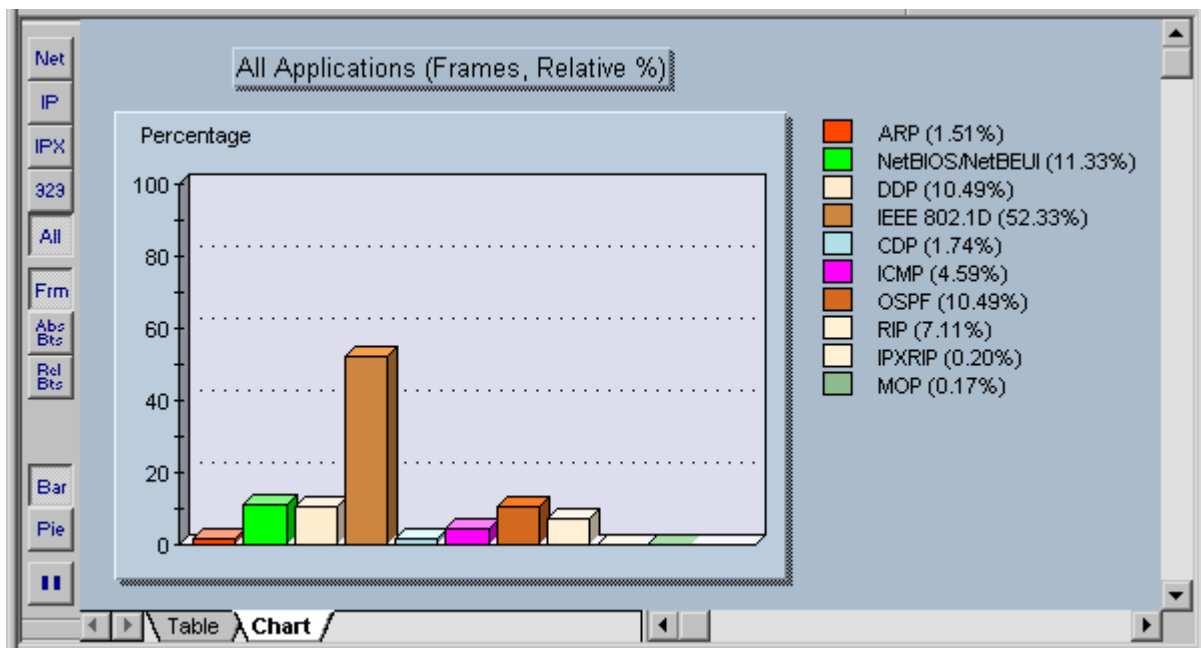


Vea que ocurre con los botones **Pie** (Diagrama de torta), **Bar** (Diagrama de barras) y **Pausa**  que aparecen en la esquina superior izquierda. Observe que **Pausa** interrumpe la captura, así que vuelva a hacer clic en él para reanudar la captura. Vea lo que muestran las fichas **Table** (Tabla) y **Chart** (Diagrama).


Con las configuraciones de muestra, el estudiante debe obtener principalmente tramas pequeñas, porque lo único que ocurre son las actualizaciones de enrutamiento. Pruebe las funciones extendidas de Ping en la conexión de Consola del router, y especifique 100 pings con un tamaño de paquete más grande.

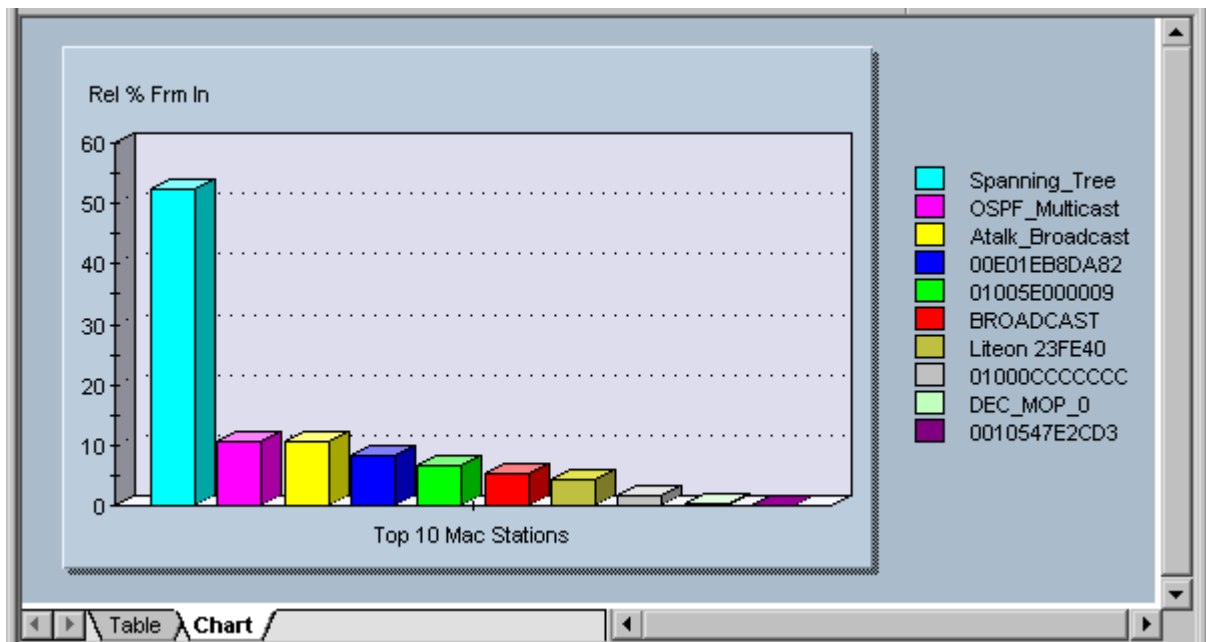
Si se maximiza cada nueva vista, se vuelve a la vista anterior con el menú Window (Ventana). El estudiante también puede acomodar las ventanas como mosaico con **Tile**. Pruebe las funciones del menú Window (Ventana) y luego cierre las vistas no deseadas.

Haga clic en el botón **Distribución de protocolo**  para ver una distribución de los protocolos recibidos por la NIC. Al colocar el puntero del ratón sobre cualquier barra aparece un pequeño panel de resumen. Maximice la ventana resultante.



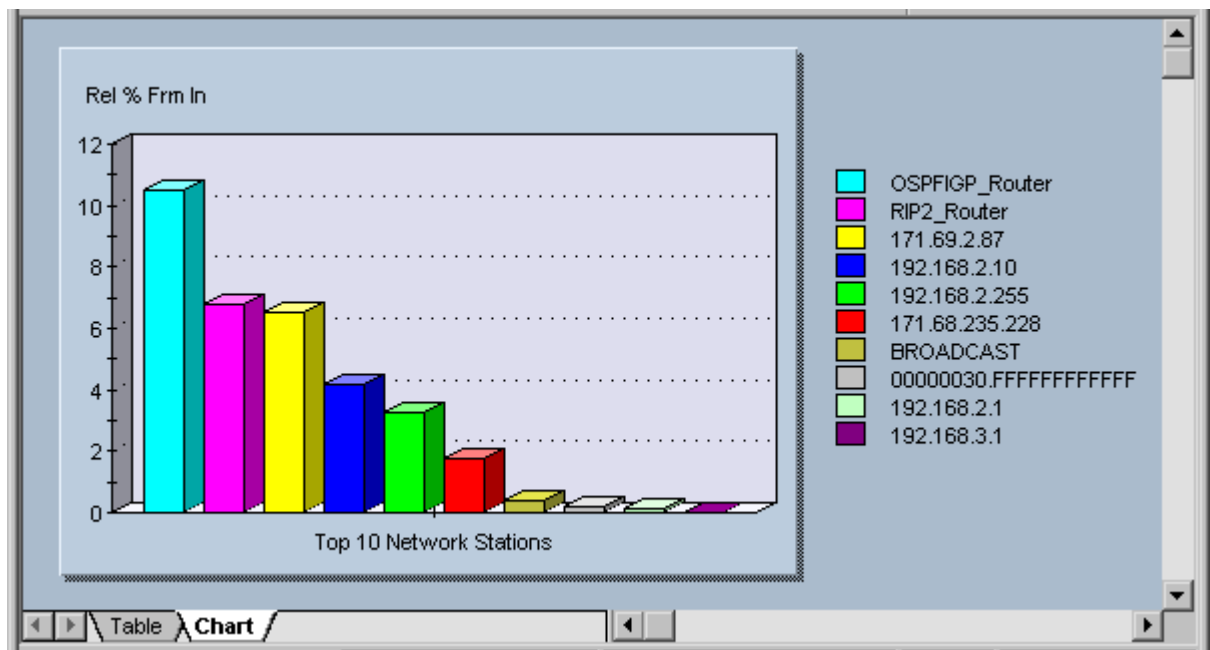
Vea lo que ocurre al accionar cada uno de los botones y fichas para ver los resultados. El botón **Net** (Red) muestra sólo protocolos de red. El botón **323** se refiere a los protocolos Voice over IP H323. Dependiendo de la versión de Protocol Expert o Inspector que se esté usando, este botón podría denominarse VoIP. Vea **Frm** (Trama), **Abs Bts** (Bytes absolutos) y **Rel Bts** (Bytes relativos) para ver los resultados. Recuerde que el botón **Pausa** interrumpe la captura.

Haga clic en el botón **Tabla de host**  para ver las estaciones MAC y el tráfico relacionado.



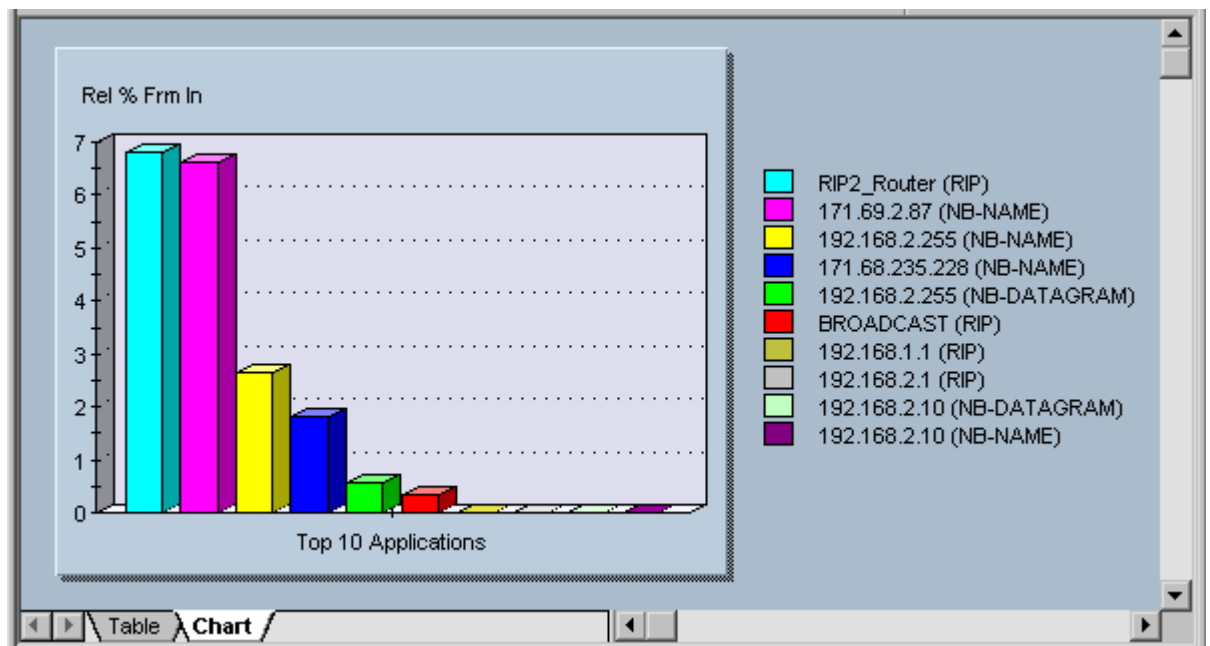
Observe el tráfico de Spanning Tree, AppleTalk y OSPF. Vea la ficha **Table** (Tabla) para ver los valores reales.




Haga clic en el botón **Tabla de host de capa de red**  para ver las estaciones de red (IP/IPX) y el tráfico relacionado.

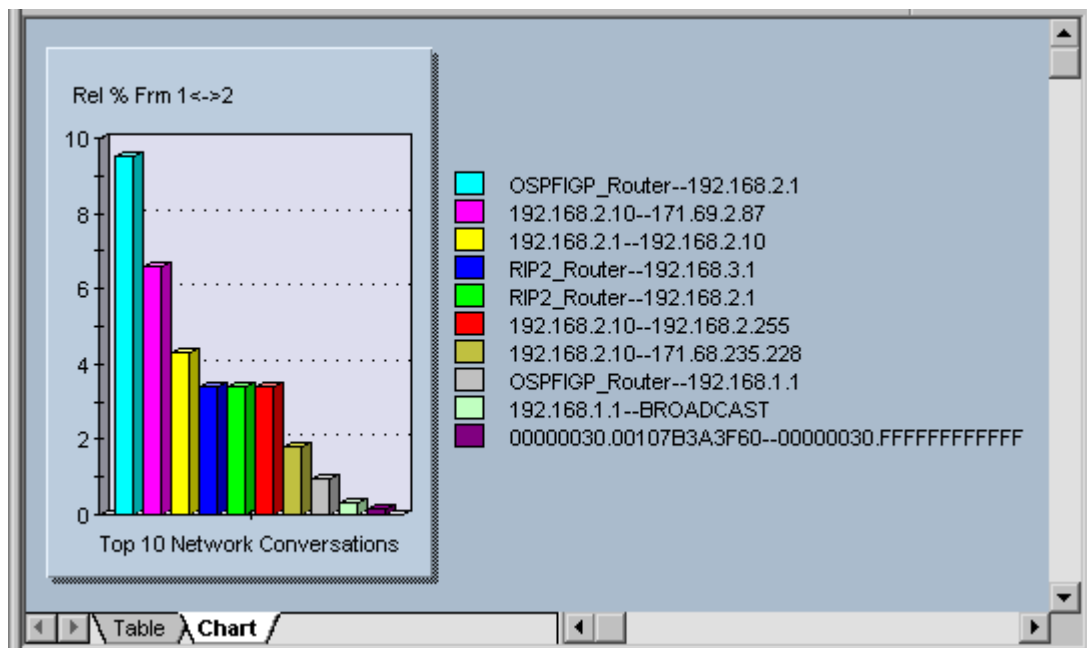



Cualquier ping y host adicional que se agreguen a la configuración afectarán las direcciones reales que aparecen a la derecha.

Haga clic en el botón **Tabla de host de capa de aplicación**  para ver el tráfico de estación de red por aplicación.




Pruebe lo que ocurre con los próximos tres botones   . Crean matrices host a host para conversaciones de la Capa de MAC, de red y de aplicación. Lo siguiente es un ejemplo de conversaciones de la Capa de Red (IP/IPX).




De los siguientes dos  botones, el primero es el botón de **VLAN** que muestra el tráfico de red en las VLAN. Esta muestra no usa VLAN. Recuerde este botón al detectar las fallas de las VLAN más adelante.

El segundo botón crea una matriz que compara las direcciones MAC y de estación de red con los nombres. En el ejemplo siguiente, la segunda fila contiene una estación de Novell.

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


El botón **Tabla de nombres**  abre la tabla de nombres actual para verla o editarla.


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

El botón **Vista experta**  muestra los síntomas expertos detectados. Estas estadísticas son la manera en que los PI tratan de mostrar problemas potenciales. Las opciones subrayadas abren ventanas detalladas adicionales si hay algún valor registrado. La muestra para esta práctica de laboratorio no muestra mucho, pero presenta las opciones para depurar ISL, HSRP y otros tipos de problemas que se verán en prácticas posteriores.

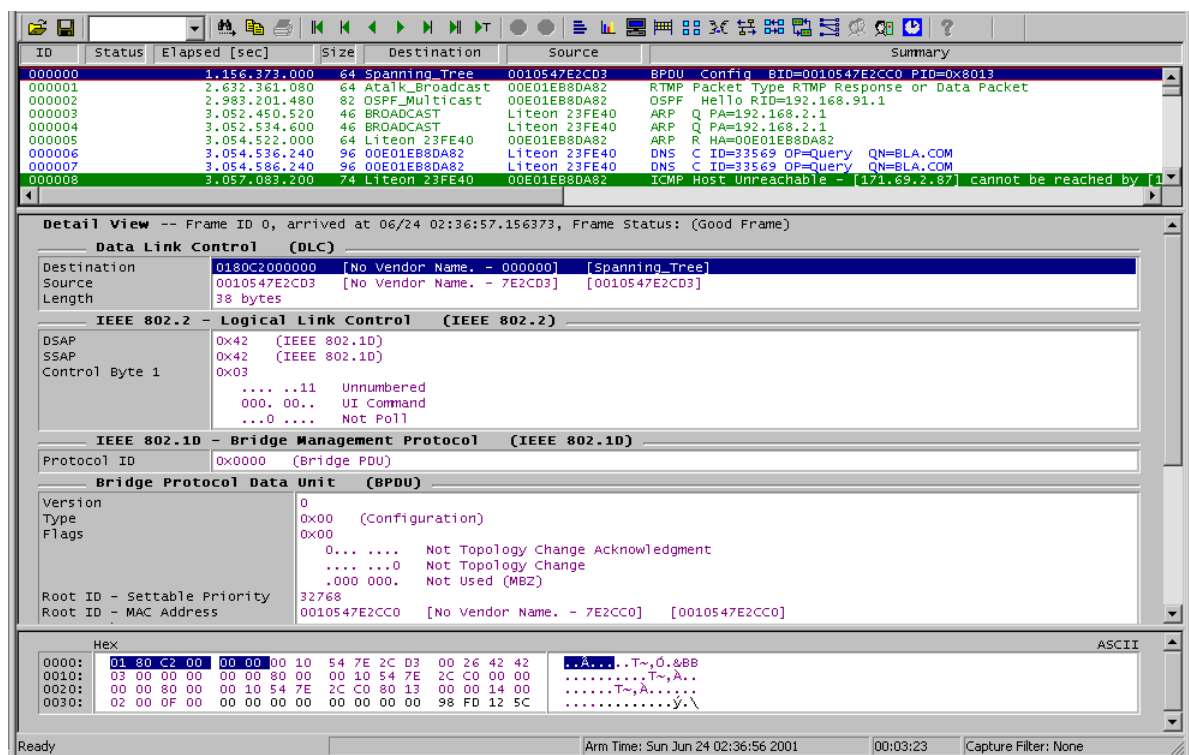
Expert Category	Value	Expert Category	Value
ICMP All Errors	368	Duplicate Network Address	0
ICMP Destination Unreachable	368	Unstable MST	0
ICMP Redirects	0	SAP Broadcast	0
Excessive Bootp	0	OSPF Broadcast	923
Excessive ARP	0	RIP Broadcast	25
NFS Retransmissions	0	ISL Illegal VLAN ID	0
TCP/M SYN Attack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

Paso 5 Detener el proceso de captura

Para detener la captura de tramas para ver tramas individuales use el botón **Detener**  o Module | Stop (Módulo | Detener) del menú.

Una vez que se haya detenido la captura, haga clic en el botón **Ver captura** . En la versión educativa, aparece una casilla de mensaje que indica que la captura se limita a 250 paquetes. Haga clic en OK.

La ventana resultante puede resultar algo abrumadora al principio. Maximice la ventana para ocultar cualquier otra ventana abierta en el fondo.



The screenshot displays the Wireshark interface with three main panes:

- Packet List:** Shows a list of captured packets. The selected packet is Frame 0, which is a BPDV Config packet.
- Detail View:** Shows the structure of the selected packet. It includes the Data Link Control (DLC) and IEEE 802.2 Logical Link Control (LLC) protocols. The IEEE 802.2 protocol is expanded, showing the Bridge Management Protocol (BPDV) and the Bridge Protocol Data Unit (BPDV).
- Raw Data:** Shows the raw packet data in hexadecimal and ASCII format.

Al ver los resultados, observe que hay tres ventanas horizontales abiertas. La ventana superior

muestra los paquetes capturados. La ventana del medio muestra los detalles del paquete seleccionado en la ventana superior, y la ventana inferior muestra los valores HEX del paquete.

Al colocar el puntero del ratón sobre los bordes de las tres ventanas, aparece un desplazador de línea o flecha de dos cabezas. Esto permite cambiar la distribución de espacio para cada ventana. Puede resultar conveniente agrandar la ventana del medio lo más posible, y dejar entre cinco y seis filas en cada una de las otras dos, como se muestra más arriba.

Mire los paquetes enumerados en la ventana superior. Se deben encontrar paquetes DNS, ARP, RTMP y otros tipos de paquetes. Si se usa un switch, debe haber paquetes de CDP y Spanning Tree. Observe que cuando se seleccionan las filas en la ventana superior, cambia el contenido de las otras dos ventanas.

Seleccione la información en la ventana del medio, y observe que la vista HEX en la ventana inferior cambia para mostrar dónde se almacena esa información específica. En el ejemplo siguiente, seleccionar Source Address (IP) (Dirección origen) muestra los valores HEX del paquete.

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 D9 00 00 80 11 A7 77 C0 A8 02 0A AB 45 .N"Û....\$wA..«E
0020:	02 57 00 89 00 89 00 3A 99 97 83 21 01 00 00 01 .W.....!....

Observe también que el código de colores facilita la ubicación de la información de la ventana del medio en la ventana HEX. En el ejemplo siguiente, con un paquete DNS, los datos en la sección Data Link Control (DLC) (Control de enlace de datos) es púrpura, mientras que la sección de Internet Protocol (IP) (Protocolo Internet) es verde. Los valores correspondientes de HEX son de los mismos colores.

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 D9 00 00 80 11 A7 77 C0 A8 02 0A AB 45 .N"Û....\$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 45ECEMEBCOE
0040:	44 45 50 45 4E 43 41 43 41 43 41 43 41 43 41 43 DEPENCACACACAC
0050:	41 43 41 43 41 41 41 00 00 20 00 01 67 87 47 13 ACACAAA...g.G.

Observe en el ejemplo anterior que el **EtherType** es **0x0800**. Esto indica que es un paquete IP. Observe las direcciones MAC para los hosts Destination (Destino) y Source (Origen) así como los datos almacenados en la vista HEX.

En el mismo ejemplo la siguiente sección en la ventana del medio es la información de **User Datagram Protocol (UDP)** (Protocolo del datagrama del usuario), que incluye los números de puerto UDP.

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]

La estructura de la ventana del medio cambia para cada tipo de paquete.

Tómese unos minutos para seleccionar diferentes tipos de paquete en la ventana superior, y luego observe el resultado en las otras dos ventanas. Preste atención especial al EtherType, cualquier número de puerto, así como las direcciones de origen y destino, que incluyen la capa de MAC y de red. Debe haber paquetes RIP, OSPF y RTMP o AppleTalk en la captura. Asegúrese de que los datos importantes se puedan ubicar e interpretar. En la siguiente captura RIP, observe que este es un paquete RIP versión 2. La dirección de destino multicast es 224.0.0.9, y se pueden ver las entradas reales de la tabla de enrutamiento. ¿Cuál sería la dirección de destino multicast en la versión 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


Si hay paquetes CDP, determine la plataforma. Lo siguiente es de un switch Catalyst 1900.

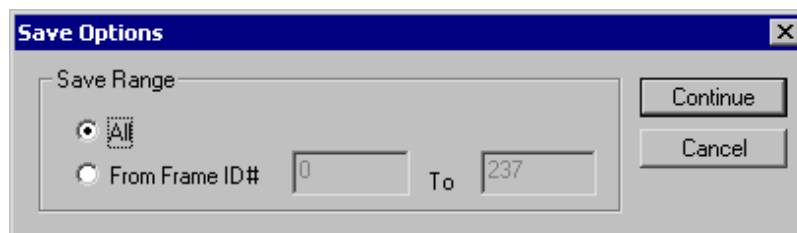
Variable Type	0x0006 (Platform)
Variable Length	14
Platform	cisco 1900

0020:	31 38 33 34 37 43 32 43 43 38 00 00 02 00 11 00	1034 E2CC0.....
0030:	00 00 01 01 01 CC 00 04 C0 A8 01 64 00 03 00 06i..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

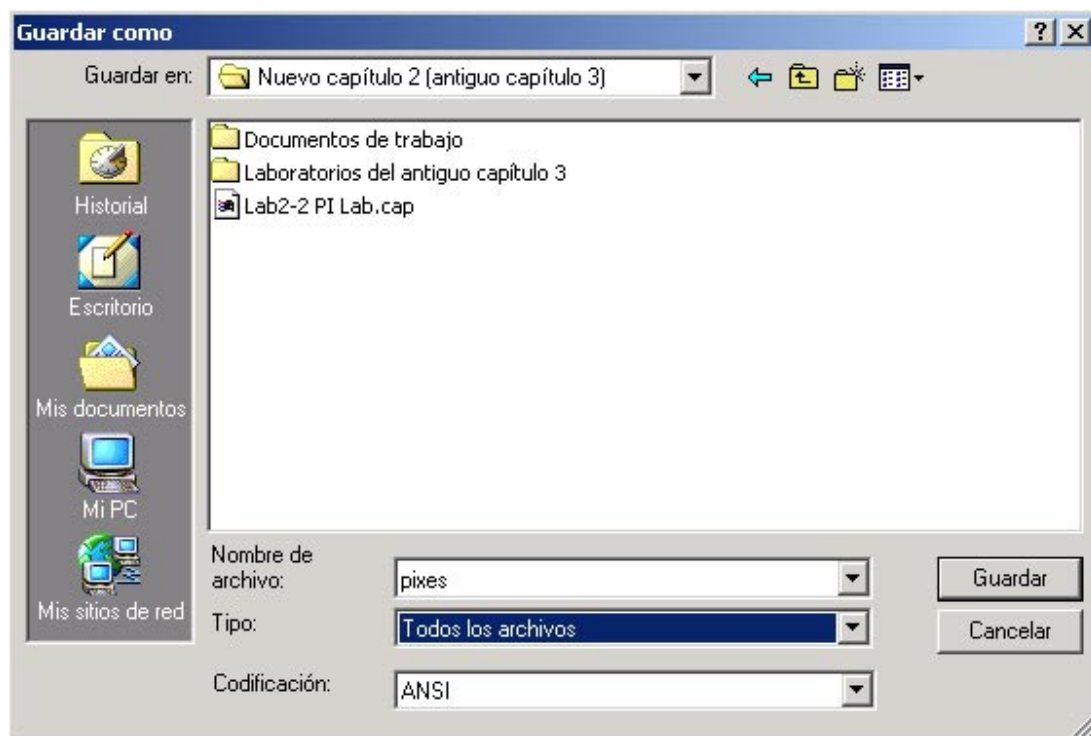
Siga probando hasta conocer bien las herramientas.


Paso 6 Guardar los datos capturados

Para guardar los datos capturados, use el botón **Guardar captura**  o seleccione File | Save Capture (Archivo | Guardar captura) del sistema de menús. Dependiendo de la versión de Protocol Expert o Inspector que se esté usando, el menú Archivo puede ofrecer la opción Save Current Sección (Guardar Sección Actual), en lugar de Save Capture (Guardar Captura). Acepte la opción **All** (Todos) con el botón **Continue** (Continuar). El estudiante puede guardar una serie de tramas capturadas con esta ventana.



Use un nombre de archivo apropiado y guarde el archivo en el disco correspondiente. Si aparece la extensión CAP cuando se abre esta ventana, asegúrese de no borrarla al escribir el nombre.



Use el botón **Abrir archivo de captura**  y abra el archivo llamado Lab3-2 PI Lab.cap. Si no está disponible, abra el archivo que acaba de guardar.


El estudiante ahora usa **Capture View of Capture Files** (Vista de captura de archivos de captura). No hay diferencia en las herramientas, pero la barra de título en la parte superior de la pantalla indica que se está viendo un archivo, y no una captura en la memoria.

Paso 7 Examinar las tramas

Seleccione una trama en la ventana superior y vea lo que ocurre al presionar los botones



Las flechas solas sirven para desplazarse una trama hacia arriba o hacia abajo. La flecha con una sola línea va a la parte inferior o superior de la ventana actual, mientras que la flecha con dos líneas representa la parte inferior o superior de toda la lista. La flecha con la T también se mueve a la parte superior de la lista.

Use los botones **Buscar**  para realizar búsquedas. Escriba texto, como por ejemplo “OSPF”, en el cuadro de lista. Haga clic en los binoculares, y con eso se va de una entrada OSPF a la siguiente.

Siga probando hasta conocer bien las herramientas.

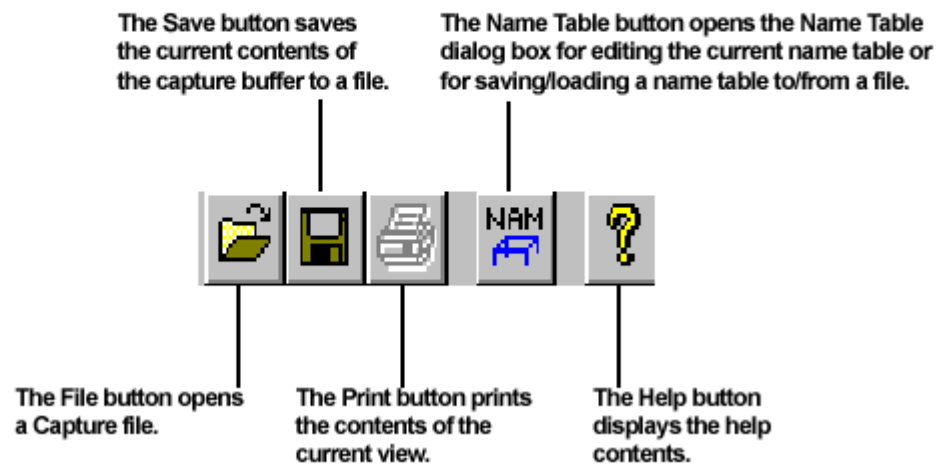
Reflexión

- ¿Cómo se puede usar esta herramienta en la detección de fallas?

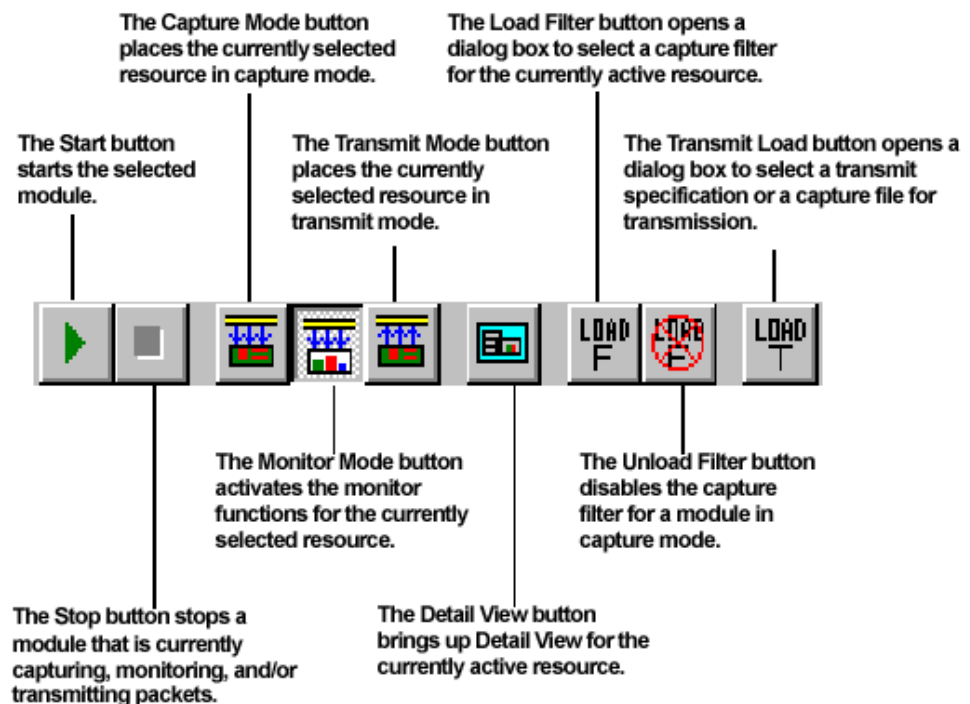
- ¿Se analiza todos los datos en la red?

- ¿Cuál es el impacto de estar conectado a un switch?

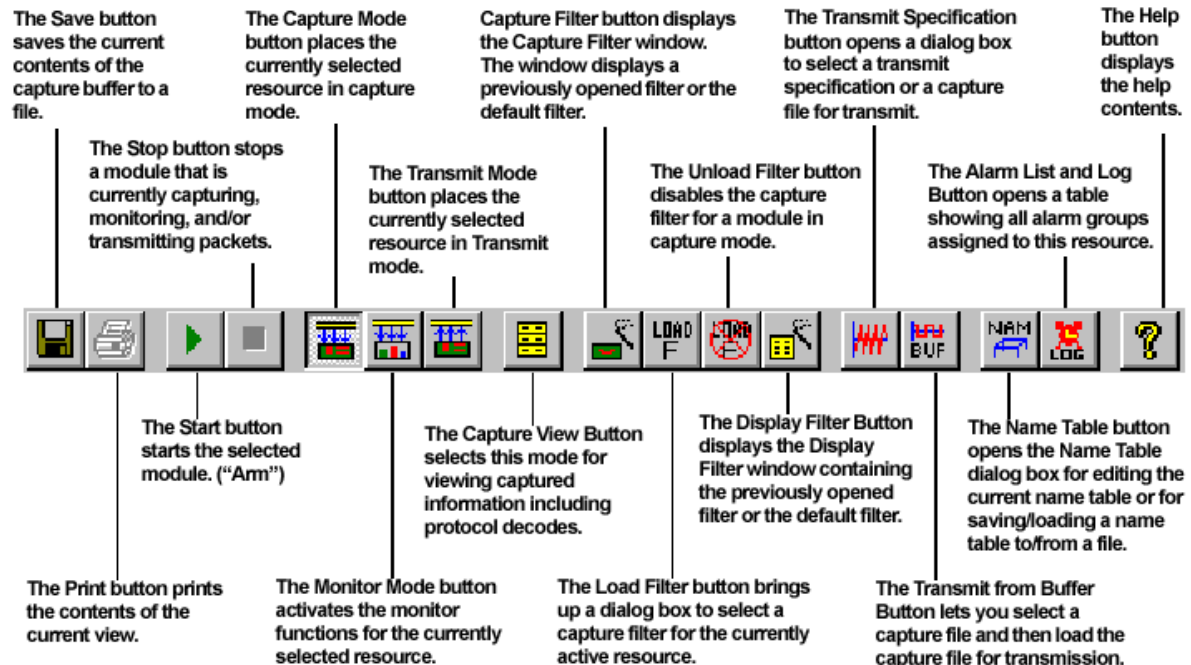
Protocol Inspector Toolbar



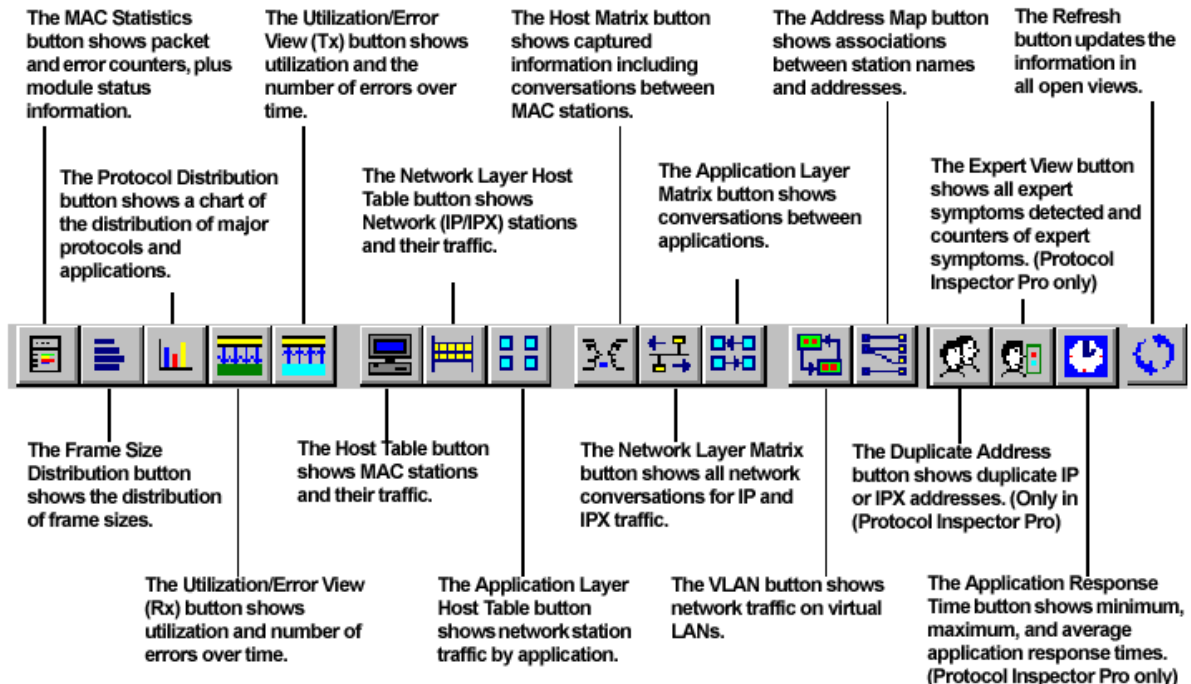
Module Toolbar (Summary View)



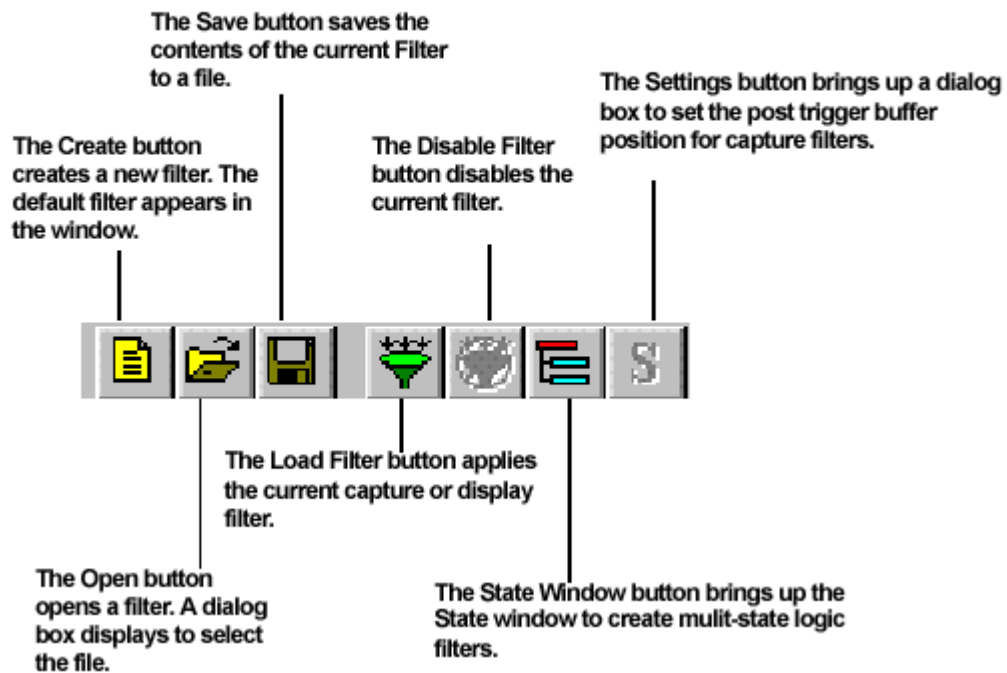
Detail View Toolbar



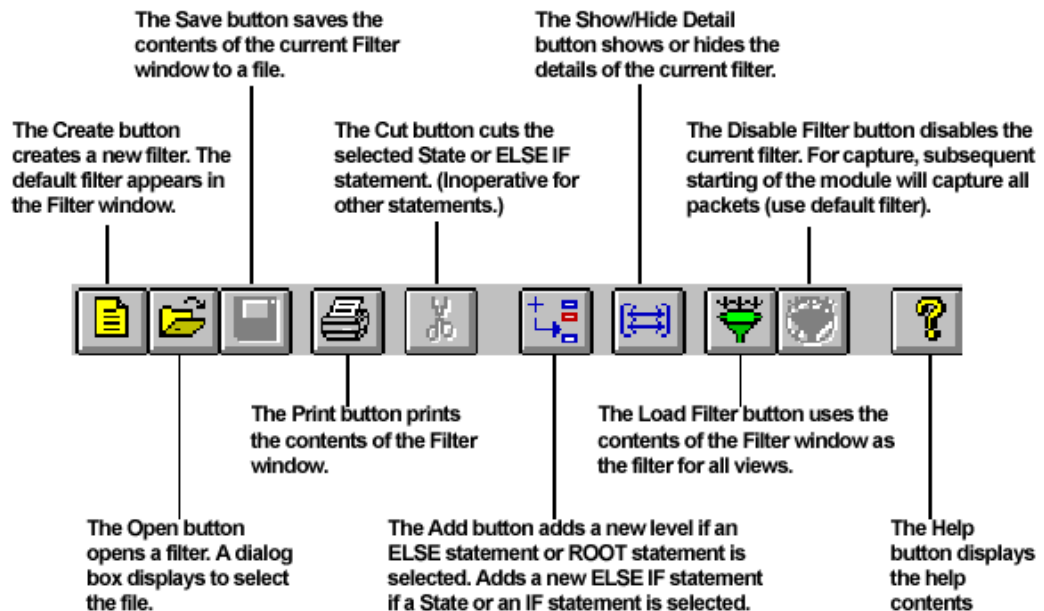
Data Views Toolbar (Note: Only some of these views are available with GMM cards)



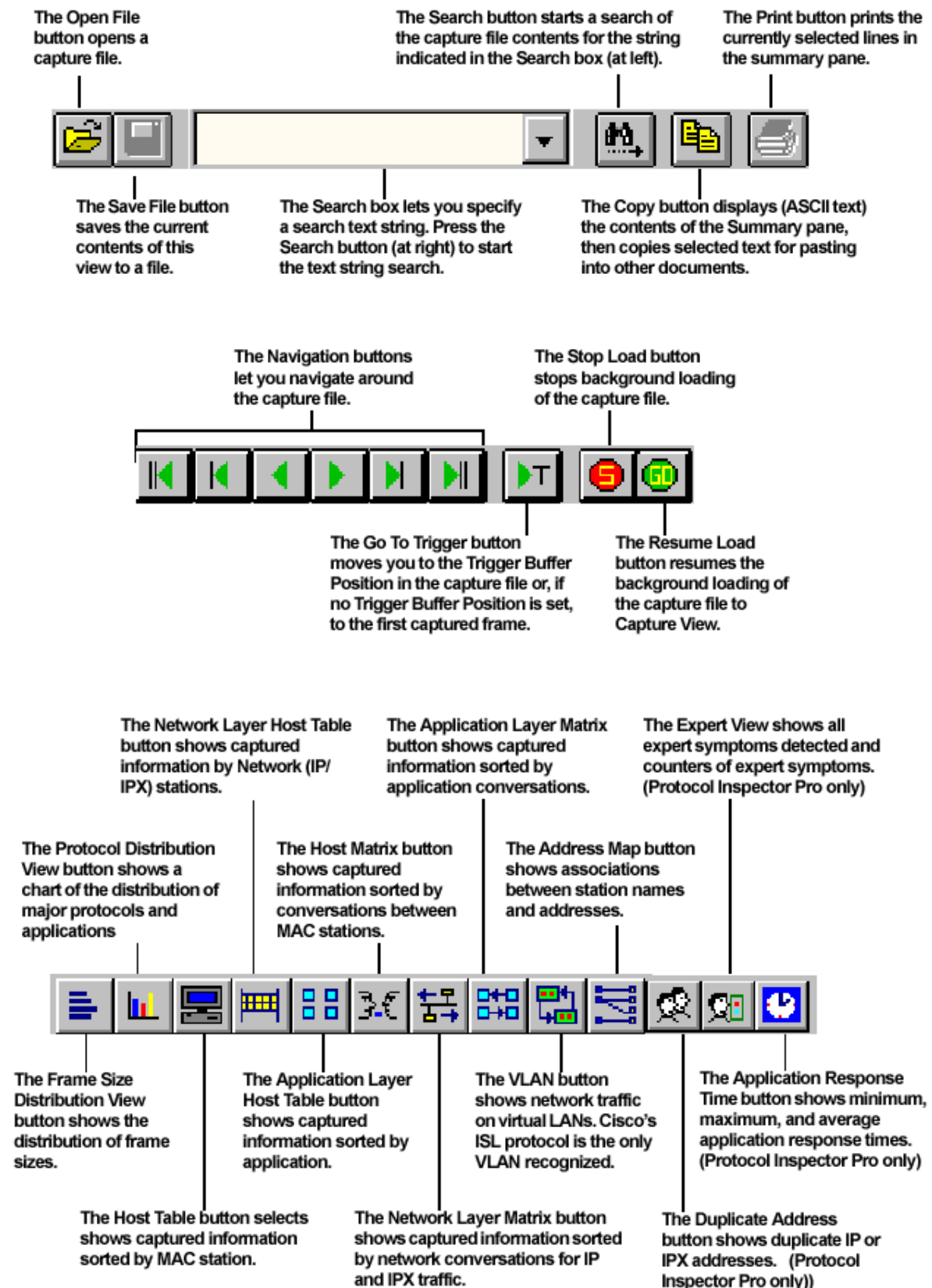
Create/Modify Filter Toolbar



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