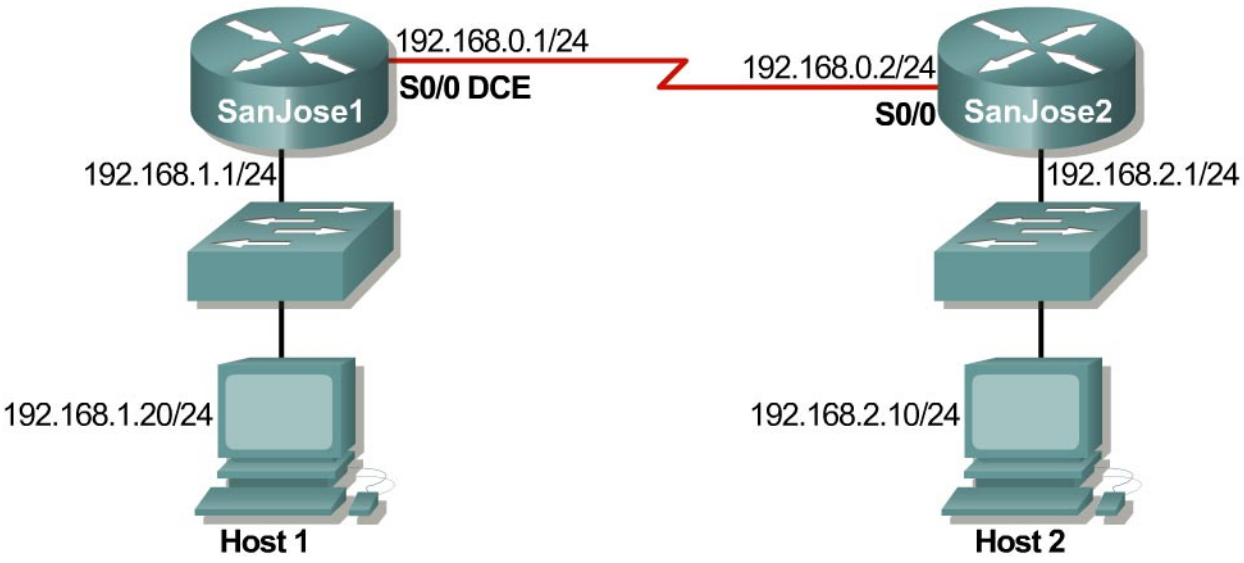
Ćwiczenie 7.1.9b Wprowadzenie do programu Fluke Protocol Inspector



Cele

To ćwiczenie ma na celu zapoznanie się z programem Protocol Inspector firmy Fluke Networks, służącym do analizy ruchu sieciowego i ramek danych. W tym ćwiczeniu zostaną przedstawione podstawowe funkcje programu, które mogą być bardzo przydatne podczas rozwiązywania problemów w pozostałych ćwiczeniach

Wprowadzenie i przygotowanie

Wyniki przedstawione w tej instrukcji są wyłącznie przykładowe. Uzyskane rzeczywiste wyniki będą się różnić w zależności od liczby dodanych urządzeń, ich adresów MAC, nazw hostów podłączonej sieci LAN, itd.

Przedstawiony w tym ćwiczeniu program Protocol Inspector będzie przydatny w kolejnych ćwiczeniach dotyczących rozwiązywania problemów, a także w rzeczywistych sytuacjach. Oprogramowanie Protocol Inspector (PI) jest cennym uzupełnieniem programu nauczania Akademii. Prezentuje przy tym typowe funkcje dostępne w innych produktach znajdujących się na rynku.

Wskazówki dotyczące przeprowadzenia tego ćwiczenia.

1) Użyj programu Protocol Inspector lub Protocol Expert w małej, kontrolowanej sieci LAN, która została skonfigurowana przez instruktora w zamkniętym środowisku laboratoryjnym w sposób pokazany na powyższym rysunku. Minimalna konfiguracja powinna składać się ze stacji roboczej, przełącznika i routera.

2) Aby zapoznać się z innymi, bardziej zróżnicowanymi sytuacjami, wykonaj opisane czynności w większym środowisku, takim jak sieć klasowa lub szkolna. Przed próbą uruchomienia programu PI lub PE w szkolnej sieci LAN uzyskaj zgodę instruktora i administratora sieci.

Przynajmniej na jednym hoście musi być zainstalowany program Protocol Inspector. Jeśli ćwiczenie wykonywane jest w parach, zainstalowanie programu na obu komputerach powoduje, że każda osoba może samodzielnie wykonywać wszystkie czynności opisane w tej instrukcji. Wyniki wyświetlane dla każdego hosta mogą się jednak nieco różnić.

Krok 1 Konfigurowanie sieci wydzielonej lub podłączenie stacji roboczej do szkolnej sieci LAN

Opcja 1. Jeśli wybrane jest zamknięte środowisko laboratoryjne, podłącz sprzęt w sposób pokazany powyżej i załaduj pliki konfiguracyjne na odpowiednie routery. Te pliki mogą być już załadowane na routerach. W przeciwnym wypadku uzyskaj je od instruktora. Ustawienia zawarte w plikach powinny być zgodne ze schematem adresowania IP przedstawionym na powyższym rysunku i w poniższej tabeli.

Skonfiguruj stacje robocze zgodnie ze specyfikacjami podanymi w poniższej tabeli.

Host nr 1	**Host nr 2**
Adres IP: 192.168.1.20	Adres IP: 192.168.2.10
Maska podsieci: 255.255.255.0	Maska podsieci: 255.255.255.0
Domyślna brama: 192.168.1.1	Domyślna brama: 192.168.2.1

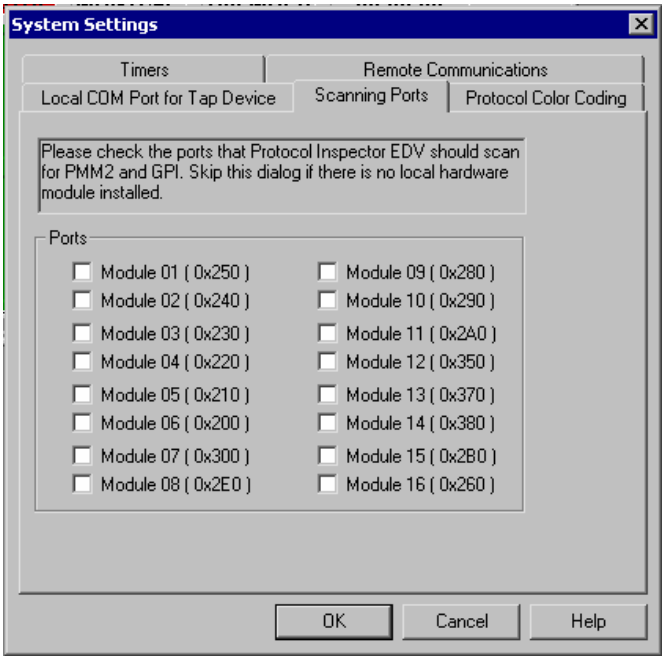
Opcja 2. W przypadku wyboru opcji 2, podłączenia do szkolnej sieci LAN, podłącz po prostu stację roboczą, na której zainstalowano program PI lub PE, bezpośrednio do znajdującego się w klasie przełącznika lub do gniazdka szkolnej sieci LAN.

Krok 2 Uruchomienie programu Protocol Inspector EDV

Z menu Start uruchom program Fluke Protocol Inspector EDV.

Uwaga: Po pierwszym uruchomieniu programu zostanie wyświetlony komunikat **„Do you have any Fluke analyzer cards or Fluke taps in your local system?" („Czy w lokalnym systemie znajdują się jakiekolwiek karty analizatora Fluke lub sondy Fluke?")**

Jeśli korzystasz z wersji edukacyjnej, wybierz opcję **No (Nie)**. Jeśli udzielisz pozytywnej odpowiedzi lub jeśli zostanie wyświetlony ekran przedstawiony obok, kliknij przycisk **OK** bez wybierania jakichkolwiek portów.

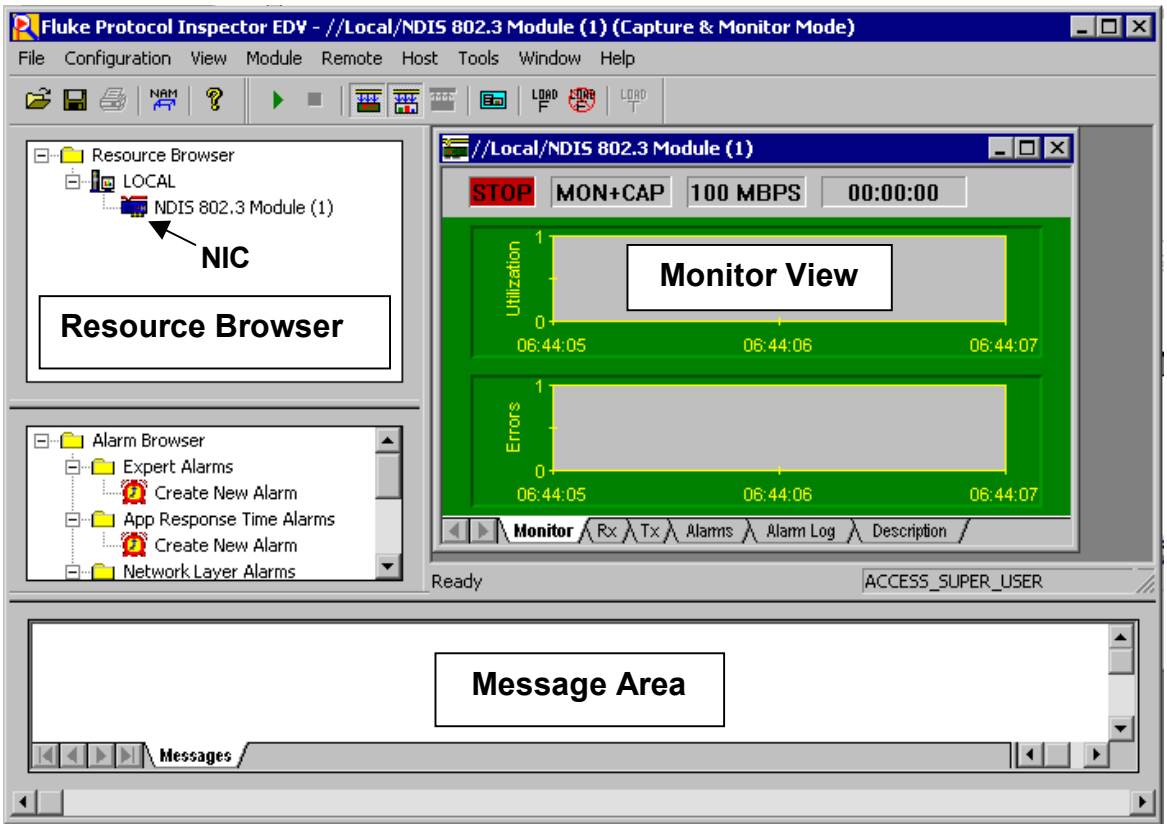


W programie Protocol dostępne są cztery główne widoki:

- Summary View (Widok podsumowania),
- Detail View (Widok szczegółów),
- Capture View of Capture Buffers (Widok przechwytywania buforów przechwytywania),
- Capture View of Capture Files (Widok przechwytywania plików przechwytywania).

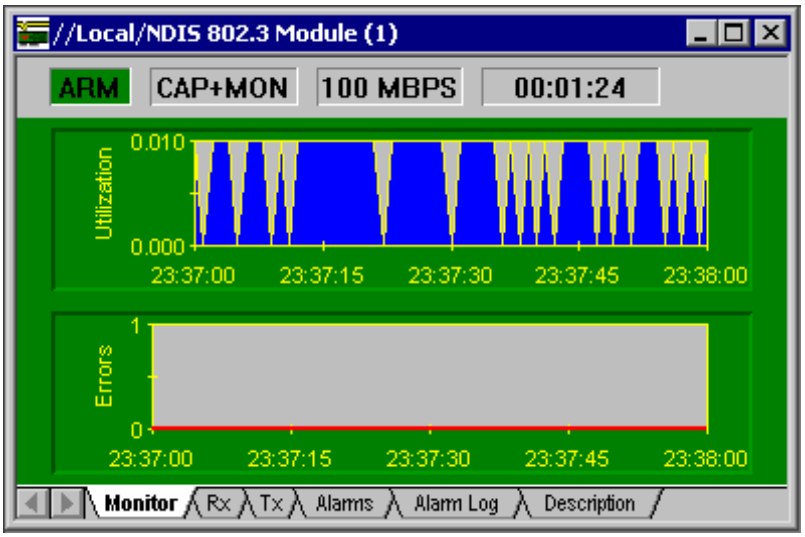
Przy otwarciu programu wyświetlany jest widok **Summary View (Widok podsumowania)**. W widoku tym dostępnych jest kilka okien. Okno **Resource Browser (Przeglądarka zasobów)** w lewym górnym rogu przedstawia jedyne dostępne urządzenie monitorujące, którym jest moduł NDIS 802.3 (karta sieciowa) hosta. Gdyby dostępne były monitory Protocol Media Monitors (Monitory medium protokołu), zostałyby wyświetlone wraz z przypisanymi im urządzeniami hosta. Okna **Alarm Browser (Przeglądarka alarmów)** znajdujące się po lewej stronie i **Message Area (Obszar komunikatów)** umieszczone poniżej zostaną omówione później.

Widok **Monitor View (Widok monitora)**, który jest wyświetlany w prawej górnej części okna głównego, służy do monitorowania każdego zasobu w oddzielnym oknie, przy użyciu różnych wybranych opcji wyświetlania. W poniższym przykładzie i prawdopodobnie na ekranie startowym w oknie Monitor View (Widok monitora) nie są wyświetlane żadne informacje. Napis **Stop** w lewym górnym rogu okna Monitor View (Widok monitora) oznacza, że monitorowanie jest wyłączone.



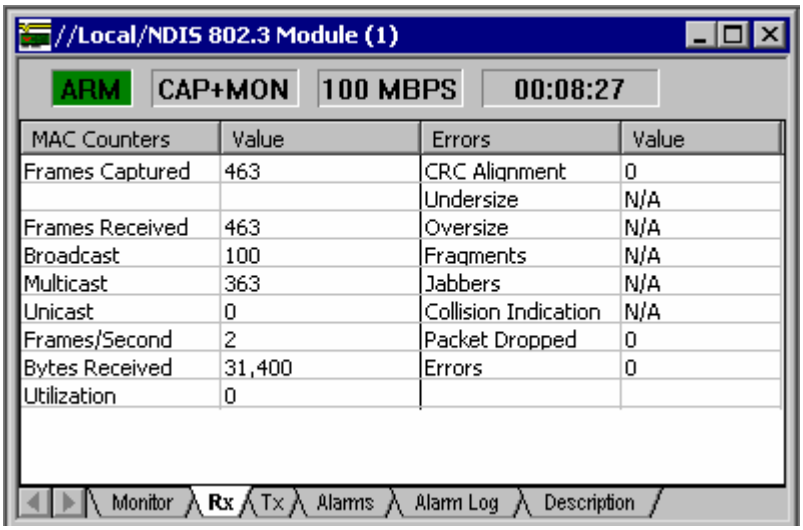
Krok 3 Uruchomienie procesu monitorowania/przechwytywania

Aby rozpocząć proces monitorowania/przechwytywania, użyj przycisku Start  lub z menu Module (Moduł) wybierz opcję Start. Powinno to spowodować rozpoczęcie wyświetlania aktywności na wykresie Utilization (Wykorzystanie) w sposób przedstawiony na poniższym rysunku.

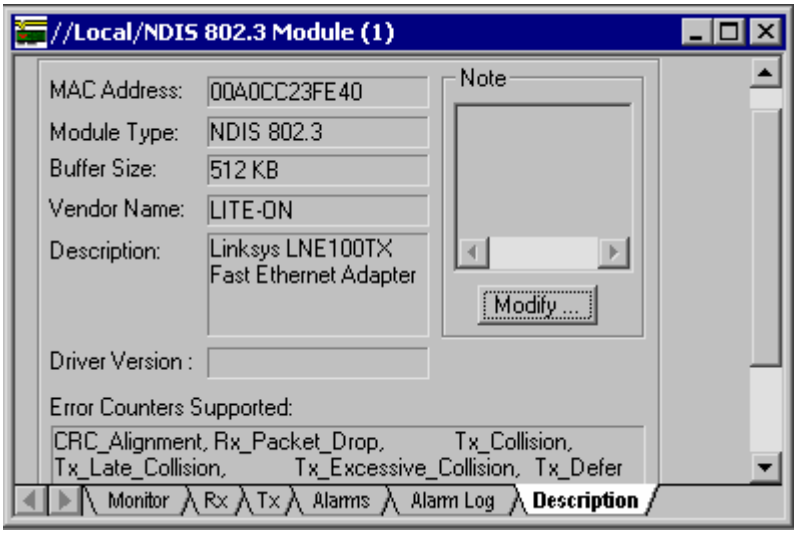


Tam, gdzie wcześniej było wyświetlane słowo **Stop**, powinno zostać wyświetlone słowo **ARM**. Zauważ, iż po otwarciu menu **Module (Moduł)** dostępna jest opcja **Stop**, a opcja **Start** stała się niedostępna. Nie przerywaj procesu monitorowania. Jeśli uległ przerwaniu, uruchom go ponownie.

Zakładki dostępne w dolnej części okna przedstawiają dane wynikowe wyświetlane w różnych formularzach. Kliknij każdą z nich, aby obejrzeć wyniki. Karty **Transmitted (Tx) (Wysłano)**, **Alarms (Alarmy)** i **Alarm Log (Rejestr alarmów)** będą puste. Na przedstawionej poniżej karcie **Received (Rx) (Odebrano)** widać, że zarejestrowano jedynie ramki rozgłoszeniowe **(Broadcast)** oraz ramki wysłane w trybie multiemisji **(Multicast)**, nie odebrano zaś żadnych ramek wysłanych w trybie emisji pojedynczej **(Unicast)**.

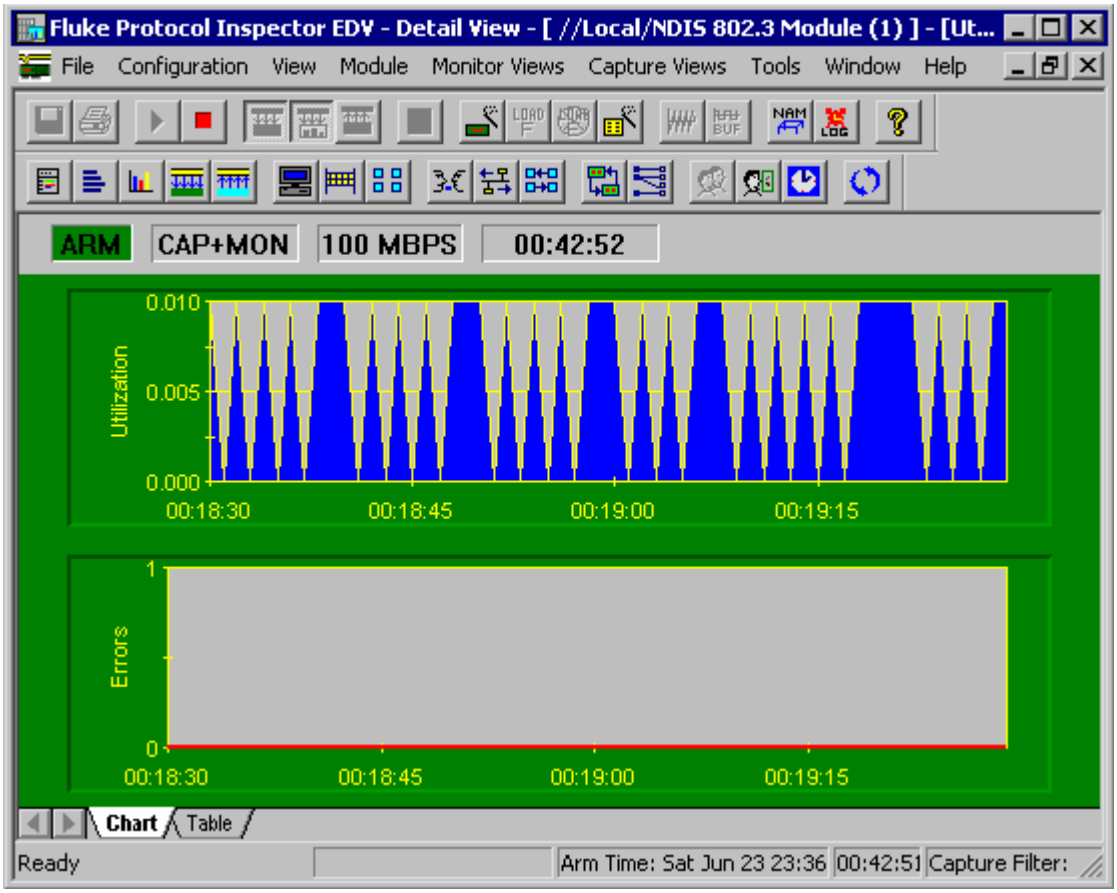


Wykorzystując konsolowe połączenie z routerem, użyj polecenia ping wobec monitorowanego hosta (192.168.1.20 lub 192.168.2.10). Zwróć uwagę, że zostaną wyświetlone ramki **Unicast**. Niestety, błędy wyświetlane w trzeciej kolumnie nie pojawią się w trakcie ćwiczenia, chyba że zostanie dodany generator ruchu, taki jak Fluke Networks OptiView.

Zakładka **Description (Opis)** pokazuje adres MAC, producenta oraz model karty sieciowej. Wskazuje również, które liczniki błędów są włączone. Poświęć kilka minut na zaznajomienie się z zakładkami i funkcjami przewijania okna.	

Krok 4 Wyświetlenie szczegółów

Aby przejść do okna **Detail View (Widok szczegółów)**, kliknij przycisk **Detail View** **(Widok szczegółów)** na pasku narzędzi lub kliknij dwukrotnie dowolne miejsce wykresu Monitor View (Widok monitora). Spowoduje to otwarcie drugiego okna, które, po zmaksymalizowaniu okna **Utilization / Errors Strip Chart (RX) (Wykres wykorzystania/błędów RX)**, powinno wyglądać tak jak poniższe.



Uwaga: Jeśli jest to konieczne, uaktywnij wszystkie paski narzędzi w menu View (Widok).

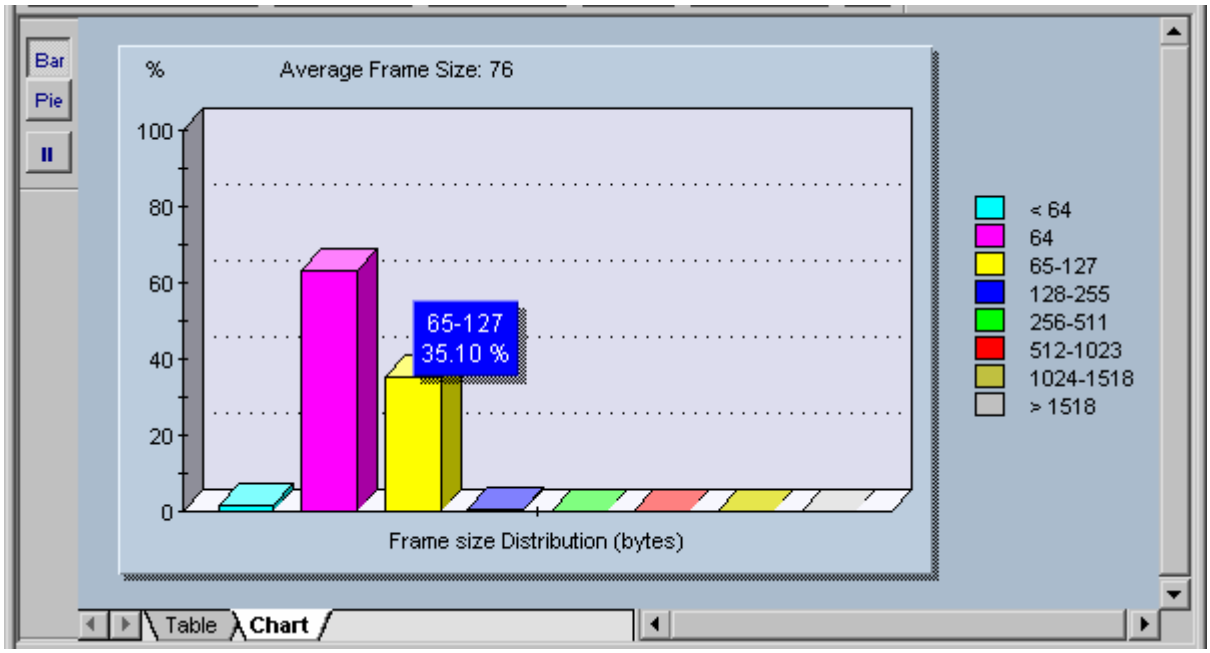
Wykres wygląda tak samo jak w widoku Summary View (Widok podsumowania), jednak w tym przypadku dostępnych jest więcej opcji na pasku narzędzi i w menu. Zanim przyjrzysz się tym funkcjom sprawdź, czy zakładki **Chart (Wykres)** i **Table (Tabela)** pokazują te same informacje, co wcześniej.

Podobnie jak w innych programach zgodnych z systemem Windows, umieszczenie kursora myszy na przycisku powoduje wyświetlenie wskazówki ekranowej z krótkim opisem funkcji przycisku. Przesuwając myszą nad przyciskami, zwróć uwagę, że niektóre z nich są nieaktywne. Oznacza to, że w danej sytuacji funkcja nie ma zastosowania. W przypadku wersji edukacyjnej programu może to również w niektórych przypadkach oznaczać, że taka funkcja nie jest obsługiwana.

Uwaga: W dodatku umieszczonym na końcu tego ćwiczenia znajdują się rysunki wszystkich pasków narzędzi oraz ich opis.

Kliknij przycisk **Mac Statistics** **(Statystyki adresów MAC)**, aby wyświetlić tabelę danych ramek odebranych (Rx) w innym formacie. Znaczenie wyświetlanych wyników powinno być oczywiste. Zmaksymalizuj wyświetlone okno. Nową wyświetlaną informacją jest pole **Speed (Szybkość)**, które przedstawia szybkość transmisji karty sieciowej.

Kliknij przycisk **Frame Size Distribution** **(Rozkład wielkości ramek)**, aby wyświetlić rozkład wielkości ramek odbieranych przez kartę sieciową. Umieszczenie kursora myszy na pasku spowoduje wyświetlenie krótkiego podsumowania, takiego jak przedstawione na poniższym rysunku. Zmaksymalizuj wyświetlone okno.



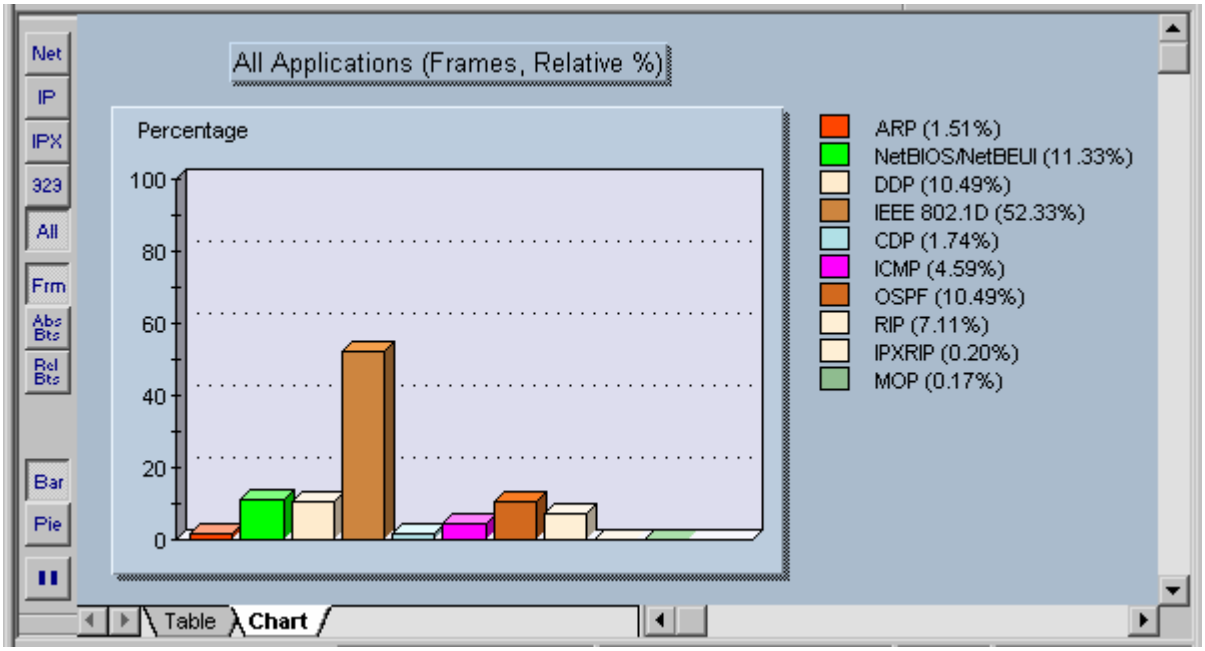
Spróbuj użyć przycisków **Pie (Wykres kołowy)**, **Bar (Wykres słupkowy)** i **Pause** **(Pauza),** znajdujących się w lewym górnym rogu. Zauważ, że przycisk **Pause (Pauza)** powoduje zatrzymanie przechwytywania, zatem naciśnij go ponownie, aby wznowić przechwytywanie. Obejrzyj zarówno zakładki **Table (Tabela)**, jak i **Chart (Wykres)**.

W przykładowej konfiguracji powinny być odbierane wyłącznie krótkie ramki, ponieważ jedynymi procesami, jakie są wykonywane, są aktualizacje routingu. Łącząc się z routerem poprzez port konsoli, przećwicz stosowanie rozszerzonej funkcji ping przez wysłanie 100 długich pakietów.

Jeśli każdy nowy ekran jest maksymalizowany, możesz wrócić do poprzedniego widoku, używając opcji Window (Okno) z menu programu. Możesz również rozłożyć okna przy użyciu opcji **Tile (Rozłóż sąsiadująco)**. Poeksperymentuj z menu Window (Okno) i zamknij wszystkie niepotrzebne

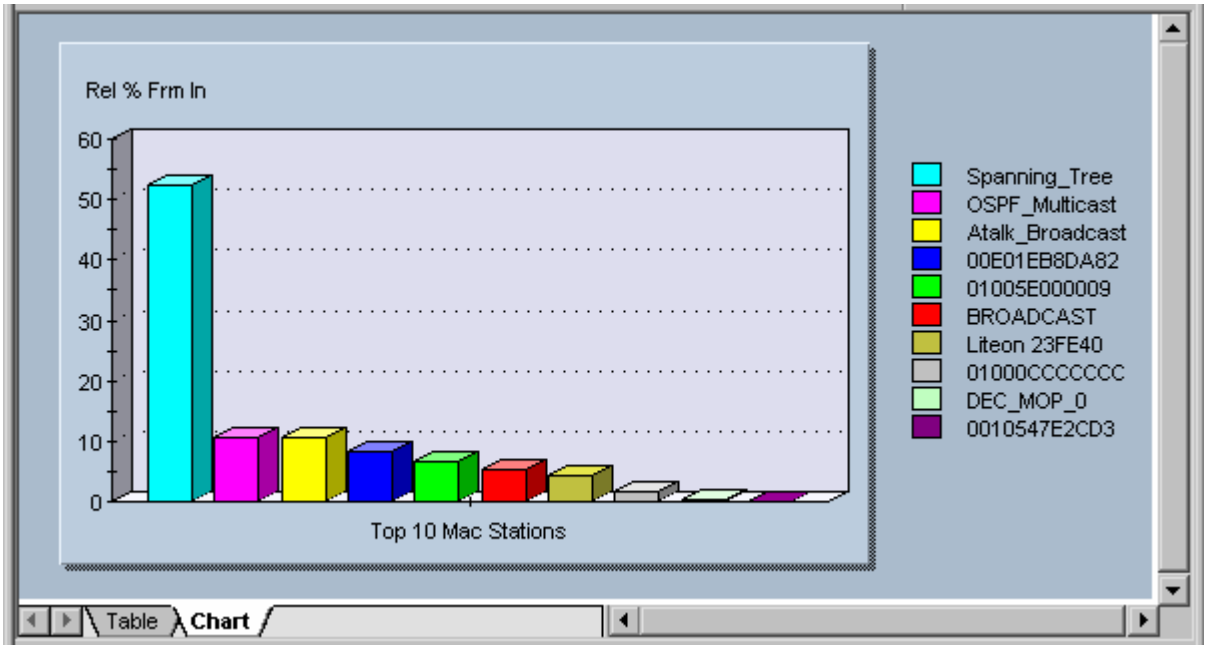
widoki.

Kliknij przycisk **Protocol Distribution** **(Rozkład protokołów)**, aby wyświetlić rozkład protokołów odebranych przez kartę sieciową. Umieszczenie kursora myszy na pasku spowoduje wyświetlenie małego panelu podsumowania. Zmaksymalizuj wyświetlone okno.



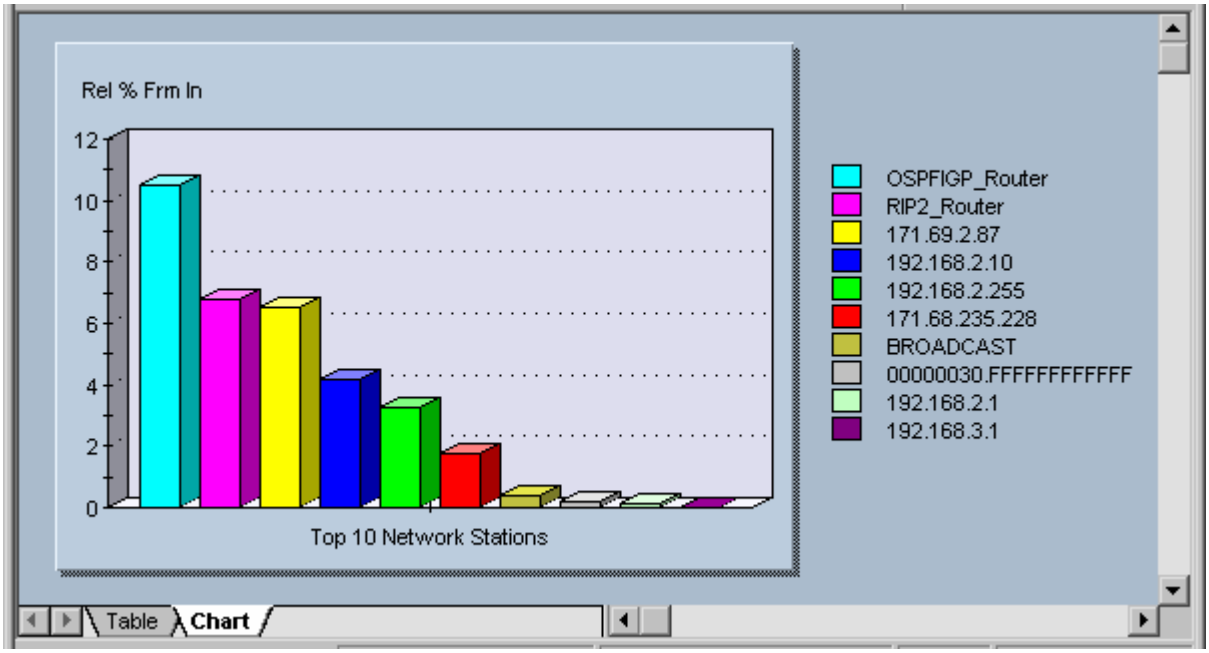
Wypróbuj inne przyciski i inne zakładki, aby zobaczyć wyświetlane wyniki. Po kliknięciu przycisku **Net (Sieć)** zostaną wyświetlone wyłącznie protokoły sieciowe. Przycisk **323** odnosi się do protokołów H323 Voiceover IP (VoIP). Jednakże w zależności od wersji używanego programu, przycisk ten może być opisany również jako VoIP. Aby wyświetlić wyniki, kliknij przyciski **Frm (Ramka)**, **Abs Bts (Bezwzględna liczba bajtów)** i **Rel Bts (Względna liczba bajtów)**. Pamiętaj, że przycisk **Pause (Pauza)** powoduje zatrzymanie przechwytywania.

Kliknij przycisk **Host Table** **(Tabela hosta)**, aby wyświetlić urządzenia z adresami MAC oraz związany z nimi ruch.



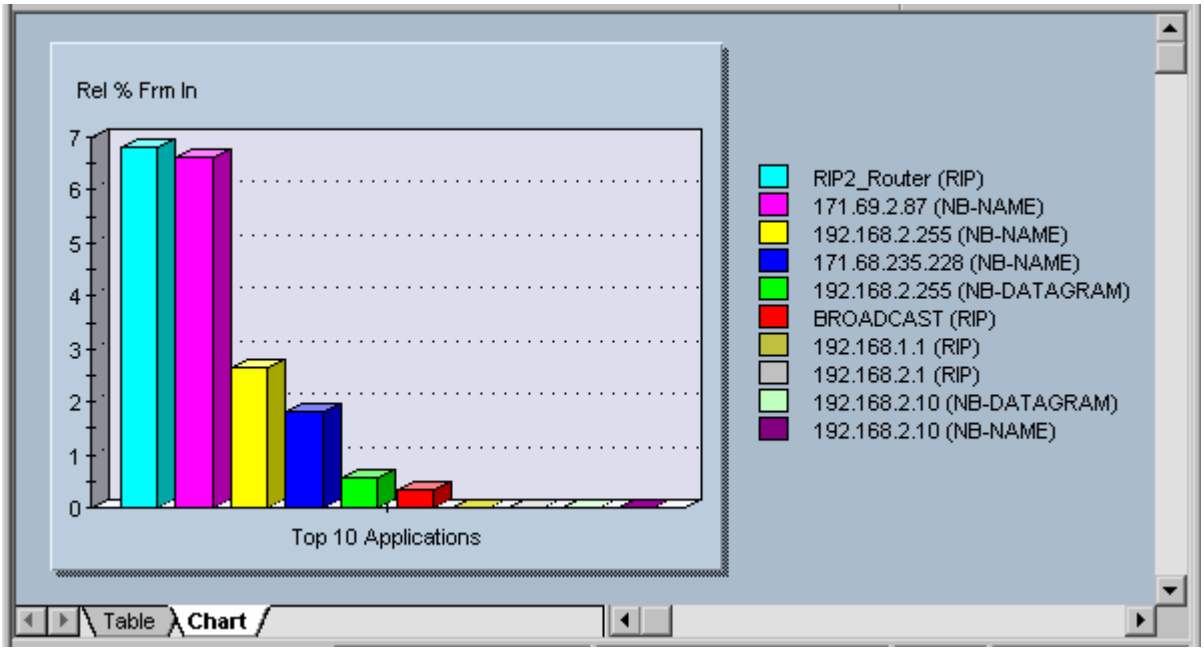
Zwróć uwagę na ruch Spanning Tree, AppleTalk i OSPF. Pamiętaj, aby wyświetlić zakładkę **Table (Tabela)** w celu obejrzenia bieżących wartości.

Kliknij przycisk **Network Layer Host Table**  **(Tabela hostów warstwy sieciowej)**, aby wyświetlić urządzenia sieciowe (IP/IPX) i związany z nimi ruch.

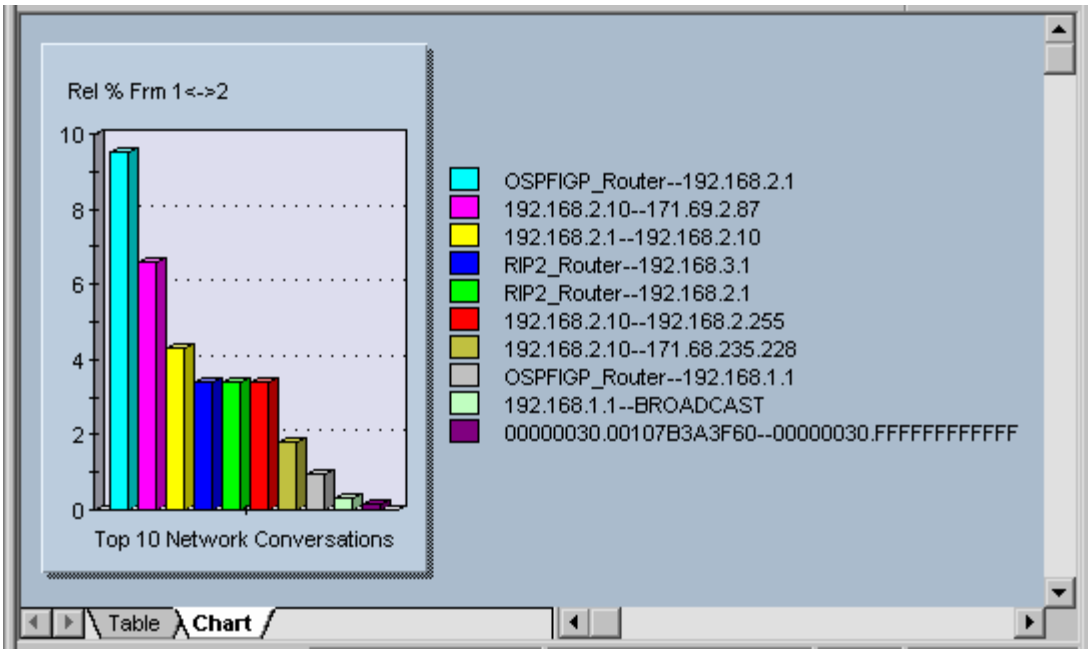


Wszelkie pakiety ping oraz hosty, które zostały dodane do bieżącej konfiguracji, będą miały wpływ na adresy, które zostaną pokazane po prawej stronie.

Kliknij przycisk **Application Layer Host Table**  **(Tabela hostów warstwy aplikacji)**, aby wyświetlić ruch pomiędzy urządzeniami sieciowymi uporządkowany według aplikacji.



Poeksperymentuj z kolejnymi trzema przyciskami  . Służą one do tworzenia macierzy opisujących konwersacje dla par host-host w warstwach MAC, sieci i aplikacji. Poniżej przedstawiony jest przykład konwersacji w warstwie sieciowej (IP/IPX).

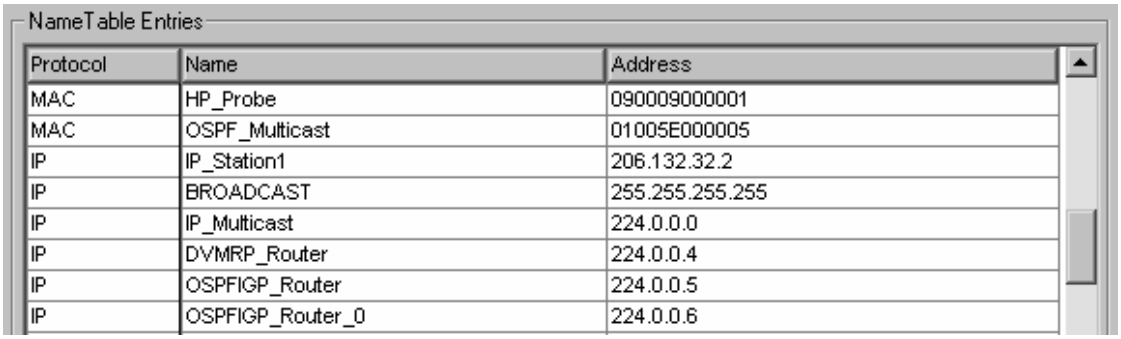


Kolejne dwa przyciski to  . Przy użyciu pierwszego z nich, przycisku **VLAN** wyświetlany jest ruch sieciowy w sieciach VLAN. W tym przykładzie sieci VLAN nie są używane. Pamiętaj o tym przycisku podczas późniejszego rozwiązywania problemów występujących w sieciach VLAN.

Za pomocą drugiego przycisku można utworzyć macierz wiążącą adresy MAC i adresy sieciowe stacji z nazwami. W poniższym przykładzie drugi wiersz dotyczy stacji sieci 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

Przycisk **Name Table**  **(Tabela nazw)** służy do otwierania bieżącej tabeli nazw w celu jej odczytu lub edycji.



Za pomocą przycisku **Expert View**  **(Widok eksperta)** przedstawiane są wykryte objawy, które mogą mieć znaczenie dla eksperta. Programy PI używają tych statystyk, aby wskazać potencjalne problemy. Podkreślone opcje umożliwiają wyświetlenie dodatkowego okna zawierającego dodatkowe szczegóły, jeśli zarejestrowane zostały jakiekolwiek wartości. Konfiguracja w tym ćwiczeniu nie zawiera wiele takich informacji. Pozwala natomiast zbadać opcje debugowania ISL, HSRP oraz inne typy problemów, które pojawią się w późniejszych ćwiczeniach.

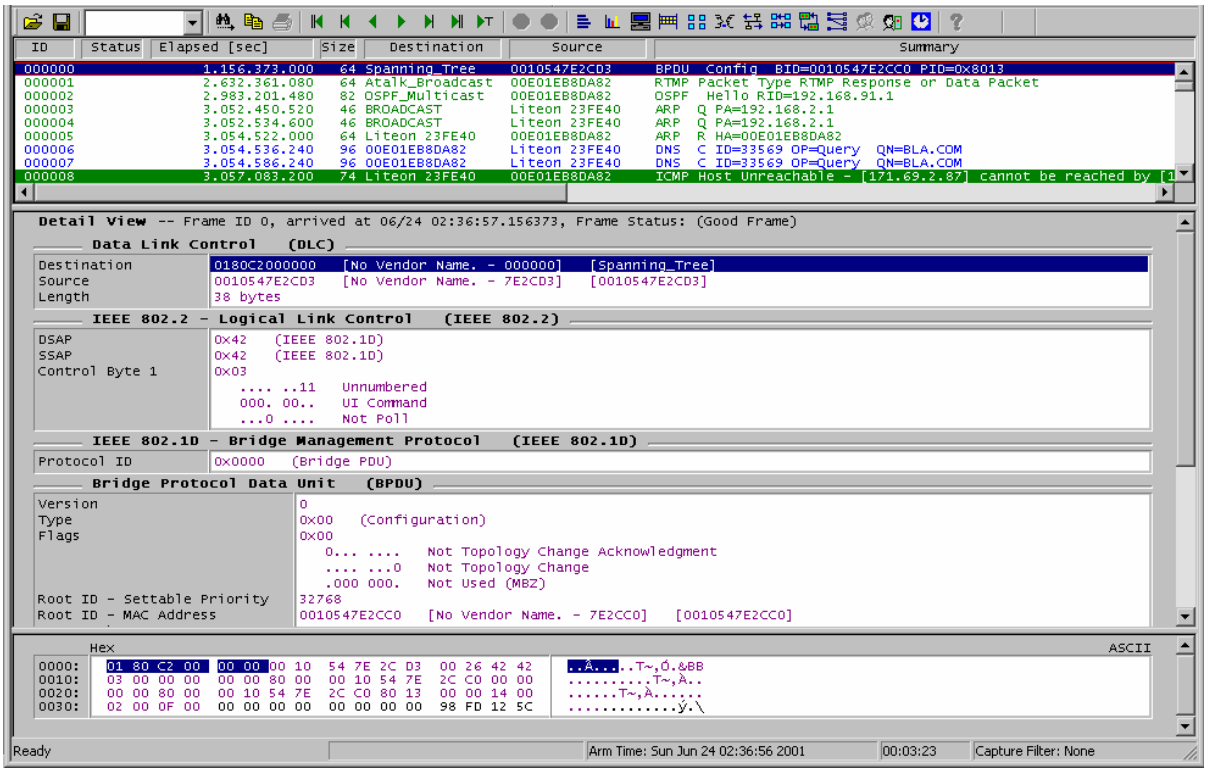
Expert Category	Value	Expert Category	Value
ICMP All Errors	368	Duplicate Network Address	0
ICMP Destination Unreachable	368	Unstable MST	0
ICMP Redirects	0	SAP Broadcast	0
Excessive Bootp	0	OSPF Broadcast	923
Excessive ARP	0	RIP Broadcast	25
NFS Retransmissions	0	ISL Illegal VLAN ID	0
TCP/IP SYN Attack	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

Krok 5 Zatrzymanie procesu przechwytywania

Aby zatrzymać przechwytywanie ramek i przyjrzeć się poszczególnym ramkom, użyj przycisku **Stop**  **(Zatrzymaj)** lub z menu Module (Moduł) wybierz polecenie Stop (Zatrzymaj).

Po zatrzymaniu przechwytywania kliknij przycisk **Capture View**  **(Wyświetlenie przechwytywania)**. W tej wersji edukacyjnej zostanie wyświetlone okno informujące, że przechwytywanie jest ograniczone do 250 pakietów. W takim przypadku kliknij przycisk OK.

Wyświetlone okno może na pierwszy rzut oka wydawać się przeładowane informacjami. Zmaksymalizuj je, aby ukryć wszystkie inne okna otwarte w tle.

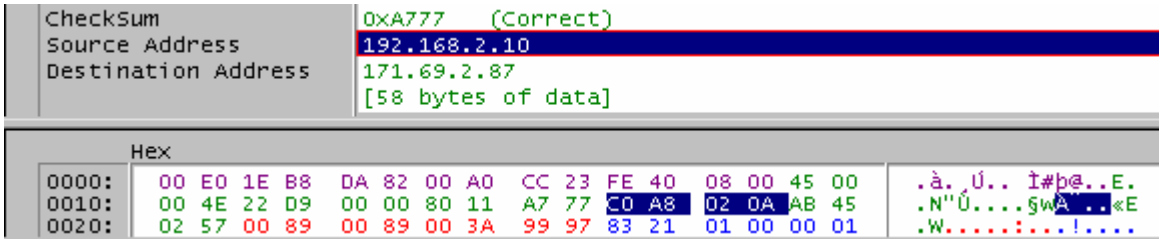


Przeglądając wyniki, zwróć uwagę, że otwarte są trzy okna rozmieszczone w pionie. Okno górne przedstawia listę przechwyconych pakietów. Okno środkowe przedstawia szczegółowe informacje o pakiecie wybranym w oknie górnym, a okno dolne przedstawia wartości szesnastkowe tego pakietu.

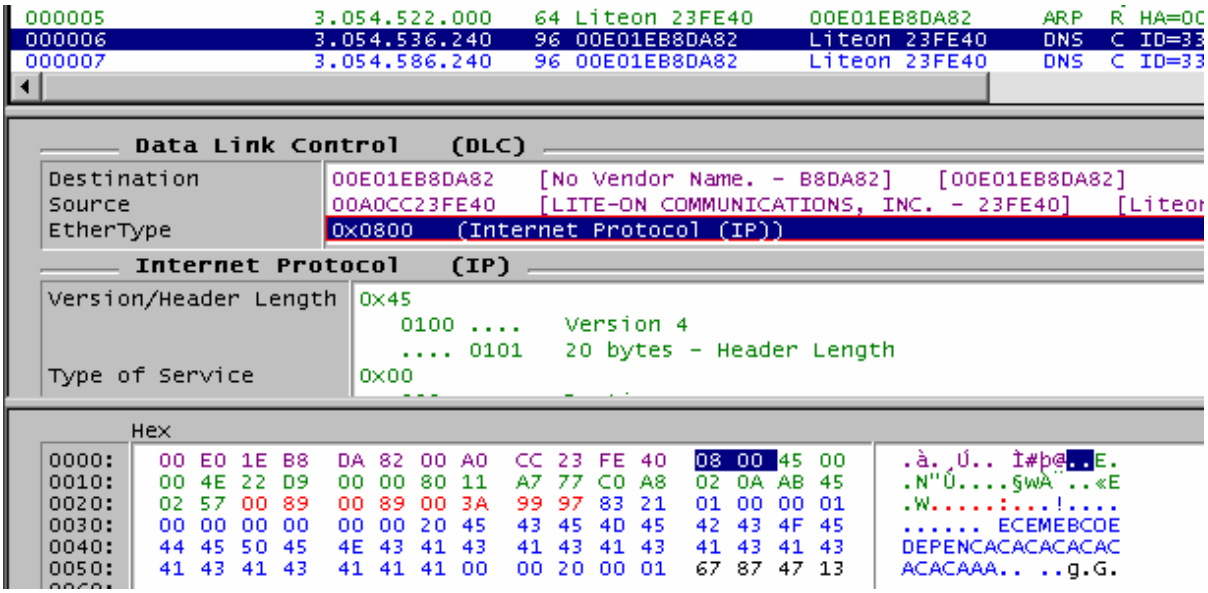
Po umieszczeniu myszy na granicy okien kursor zmieni się w ikonę przesuwania linii (dwustronną strzałkę). Umożliwia to zmianę obszaru zajmowanego przez poszczególne okna. Warto maksymalnie powiększyć okno środkowe i pozostawić pięć lub sześć wierszy w pozostałych oknach, tak jak w powyższym przykładzie.

Przejrzyj pakiety znajdujące się w oknie górnym. Powinny w nim znajdować się pakiety DNS, ARP, RTMP oraz pakiety innych typów. W przypadku stosowania przełącznika powinny znajdować się tam pakiety CDP i Spanning Tree. Zwróć uwagę, że wybranie wiersza w górnym oknie powoduje zmianę zawartości dwóch pozostałych okien.

Zaznacz dane w oknie środkowym i zwróć uwagę, że zmianie uległy dane wyświetlane w dolnym oknie (format szesnastkowy), wskazując miejsce, w którym przechowywane są zaznaczone dane. W tym przykładzie wybranie pozycji Source Address (IP) (Adres źródłowy IP) spowoduje wyświetlenie wartości szesnastkowych zawartych w pakiecie.

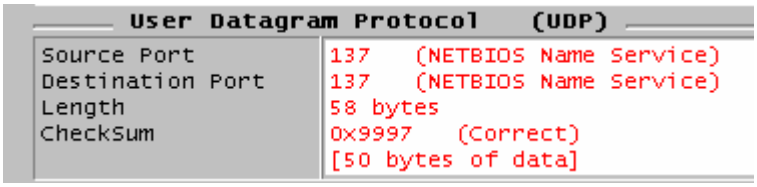


Zwróć również uwagę, że kolory ułatwiają zlokalizowanie informacji z okna środkowego w oknie danych szesnastkowych. W poniższym przykładzie prezentującym pakiet DNS dane w sekcji Data Link Control (DLC) (Kontrola łącza danych - DLC) w oknie środkowym są fioletowe, a sekcja Internet Protocol (IP) (Protokół IP) jest zielona. Odpowiednie wartości szesnastkowe mają ten sam kolor.



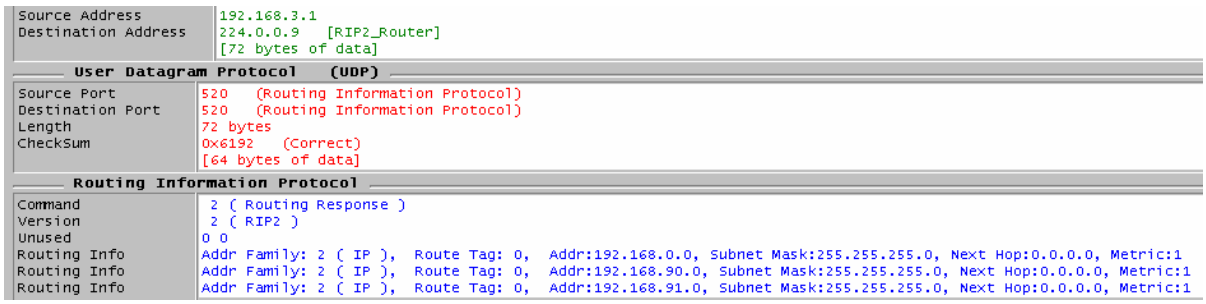
Zwróć uwagę, że w powyższym przykładzie wartość pola **EtherType** wynosi **0x0800**. Oznacza to, że jest to pakiet IP. Zwróć uwagę na adresy MAC hosta docelowego i źródłowego oraz na miejsce przechowywania danych znajdujących się w oknie zawierającym dane szesnastkowe.

Kolejną sekcją środkowego okna jest w tym przykładzie **User Datagram Protocol (UDP) (Protokół UDP)**, zawierający numery portów UDP.

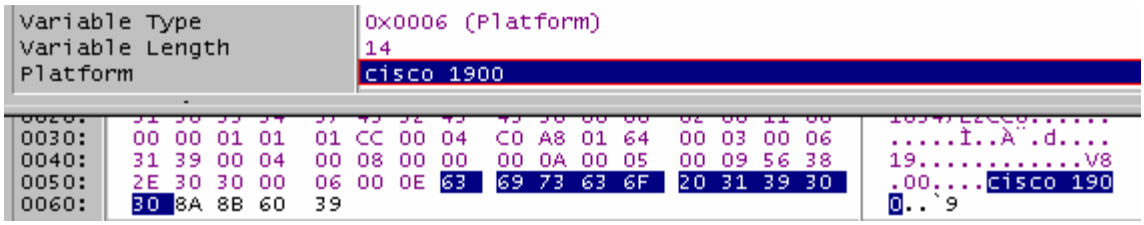


Struktura środkowego okna zmienia się w zależności od typu pakietu.

Poświęć kilka minut na wybieranie różnych typów pakietów w górnym oknie i przejrzenie informacji wyświetlanych w pozostałych dwóch oknach. Zwróć szczególną uwagę na typ EtherType i numery portów, a także adresy źródłowe i docelowe, które zawarte są zarówno w warstwie MAC, jak i w warstwie sieciowej. Powinny zostać przechwycone pakiety RIP, OSPF, RTMP oraz AppleTalk. Upewnij się, że można zlokalizować i zinterpretować istotne dane. Zwróć uwagę, że poniższe przechwycone pakiety RIP są w wersji 2. Adresem docelowym multiemisji jest 224.0.0.9 i widoczne są wpisy w bieżącej tablicy routingu. Jaki byłby adres multiemisji w wersji 1? _____



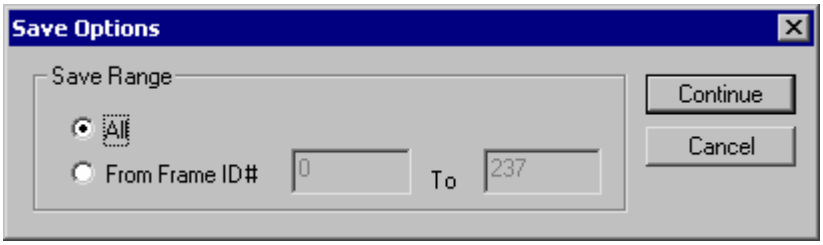
Jeśli są dostępne jakiekolwiek pakiety CDP, spróbuj uzyskać informacje o platformie. Poniższe dane pochodzą z przełącznika Catalyst 1900.



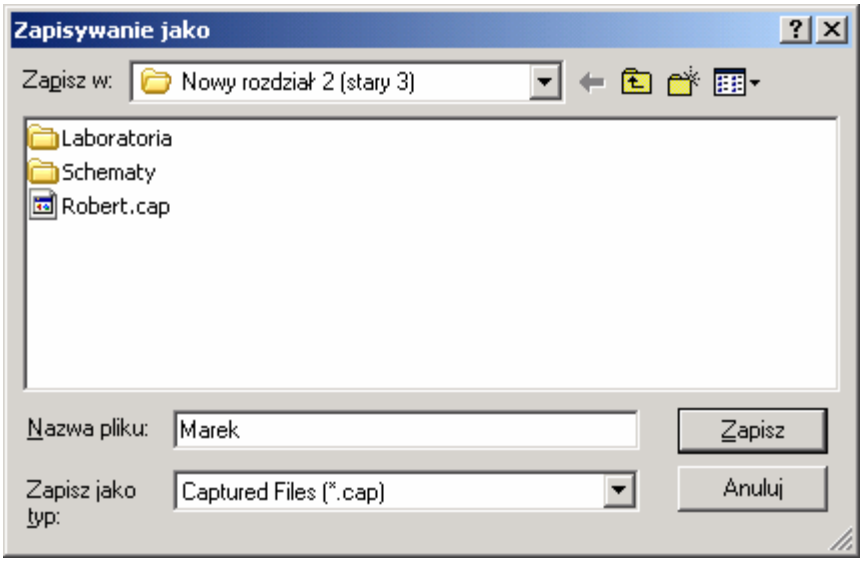
Eksperymentuj tak długo, aż używanie narzędzi nie będzie ci sprawiać problemów.

Krok 6 Zapisanie przechwyconych danych

Aby zapisać przechwycone dane, użyj przycisku **Save Capture** **(Zapisz przechwycone dane)** lub z menu File (Plik) wybierz polecenie Save Capture (Zapisz przechwycone dane). W zależności od używanej wersji programu w menu File (Plik) opcja Save Capture (Zapisz przechwycone dane) może zostać zastąpiona przez „Save Current Section” (Zapisz aktualnie przeglądaną sekcję). Zaakceptuj opcję **All (Wszystkie)** przy użyciu przycisku **Continue (Kontynuuj)**. Uczestnik kursu może w tym oknie wybrać zakres przechwyconych ramek, które mają zostać zapisane.



Podaj odpowiednią nazwę pliku i zapisz plik na wybranym dysku. Jeśli po otwarciu okna wyświetlane jest rozszerzenie CAP, upewnij się, że będzie ono również wyświetlane po wpisaniu nazwy.



Użyj przycisku **Open Capture File** **(Otwórz plik przechwytywania)** i otwórz plik o nazwie Lab3-2 PI Lab.cap. Jeśli plik ten nie jest dostępny, otwórz plik, który został zapisany.

Użyj teraz funkcji **Capture View of Capture Files (Widok przechwytywania plików przechwytywania)**. Dostępne są te same narzędzia, ale pasek tytułu w górnej części ekranu wskazuje, że wyświetlane są dane z pliku, a nie dane przechwytywania znajdujące się w pamięci.

Krok 7 Badanie ramek

Wybierz ramkę w górnym oknie i użyj przycisków  . Strzałki powodują przesunięcie ramek o jedną w górę lub w dół. Za pomocą strzałki z pojedynczą linią można przejść do góry lub na dół bieżącego okna, a za pomocą strzałki z dwoma liniami można przejść do początku lub na koniec całej listy. Strzałka z literą T również służy do przejścia na początek listy.

Użyj przycisku **Search** 

(Wyszukiwanie), aby wykonać wyszukiwanie. W polu listy wpisz tekst OSPF. Następnie kliknij ikonę lornetki, co spowoduje przejście od jednego wpisu OSPF do drugiego.

Eksperymentuj tak długo, aż używanie narzędzi nie będzie ci sprawiać problemów.

Do przemyślenia

a. W jaki sposób narzędzie to może być przydatne do rozwiązywania problemów?

_____

b. Czy wszystkie dane w sieci są analizowane?

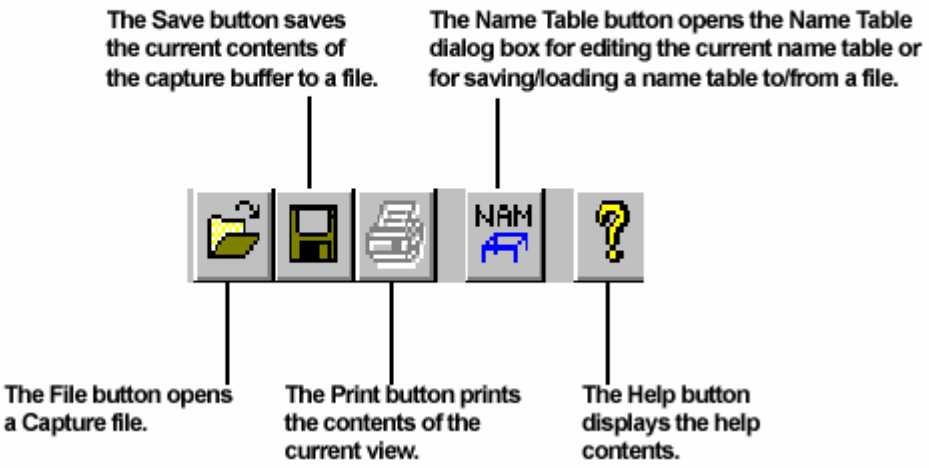
_____

c. Jaki wpływ ma podłączenie do przełącznika?

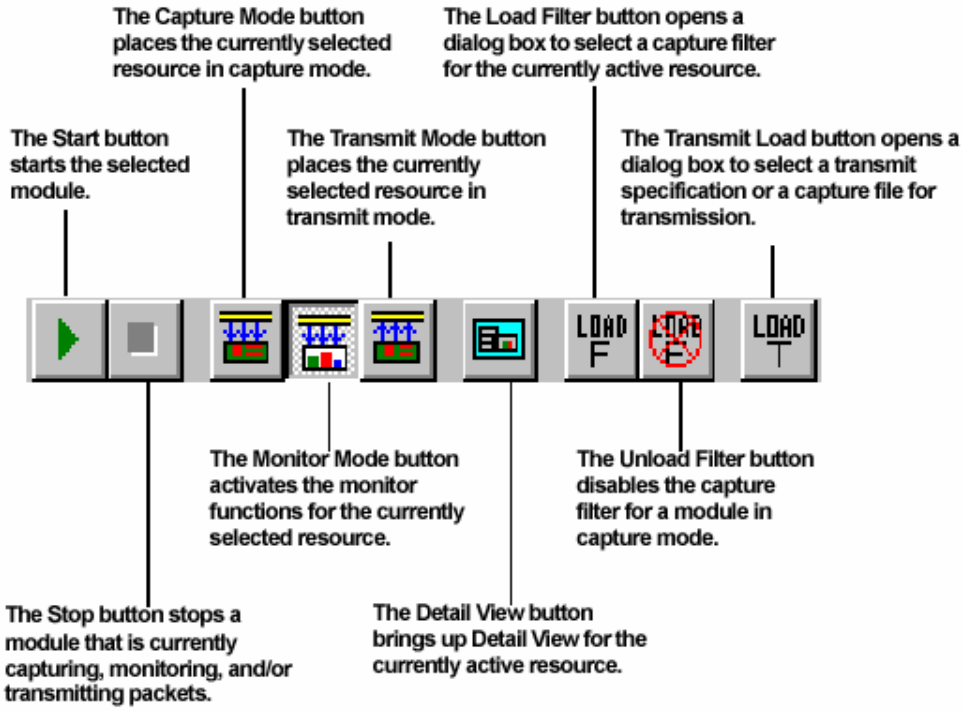
_____

Dodatek: Paski narzędzi programu PI

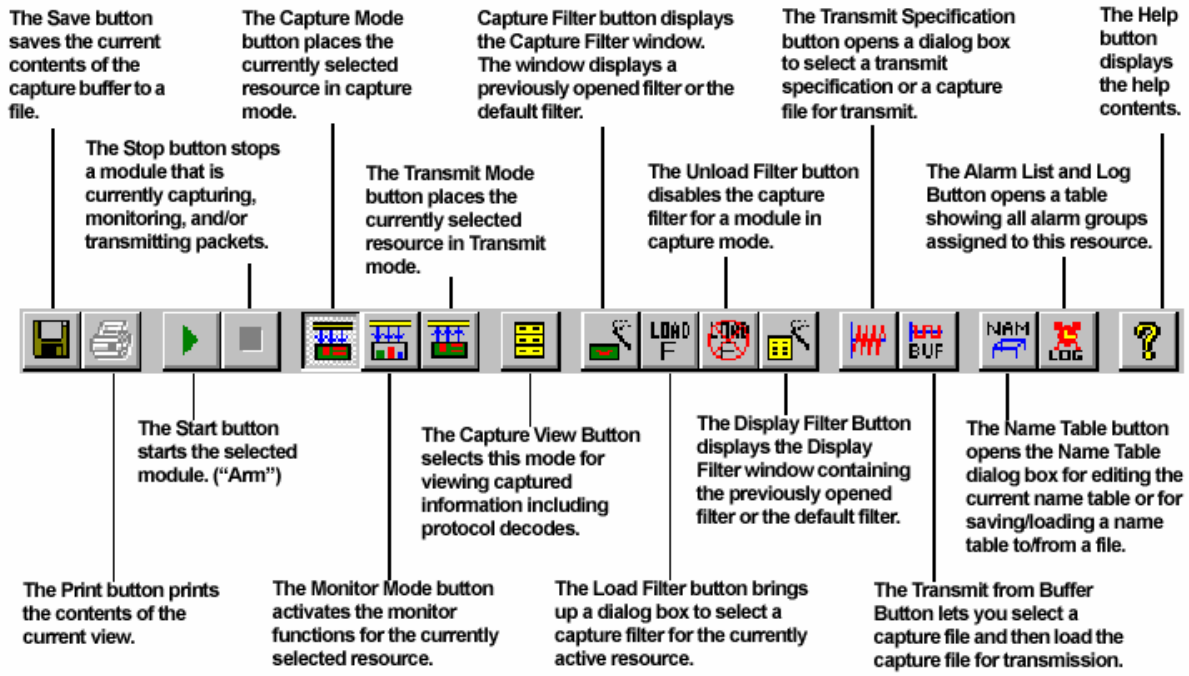
Protocol Inspector Toolbar



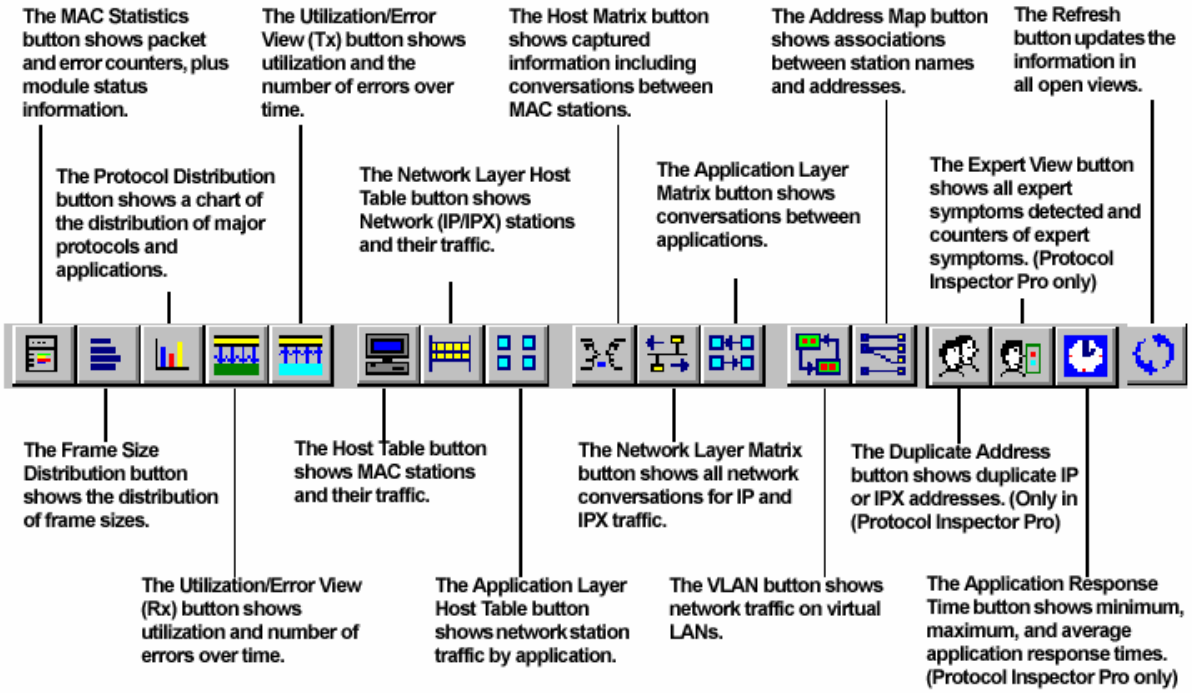
Module Toolbar (Summary View)



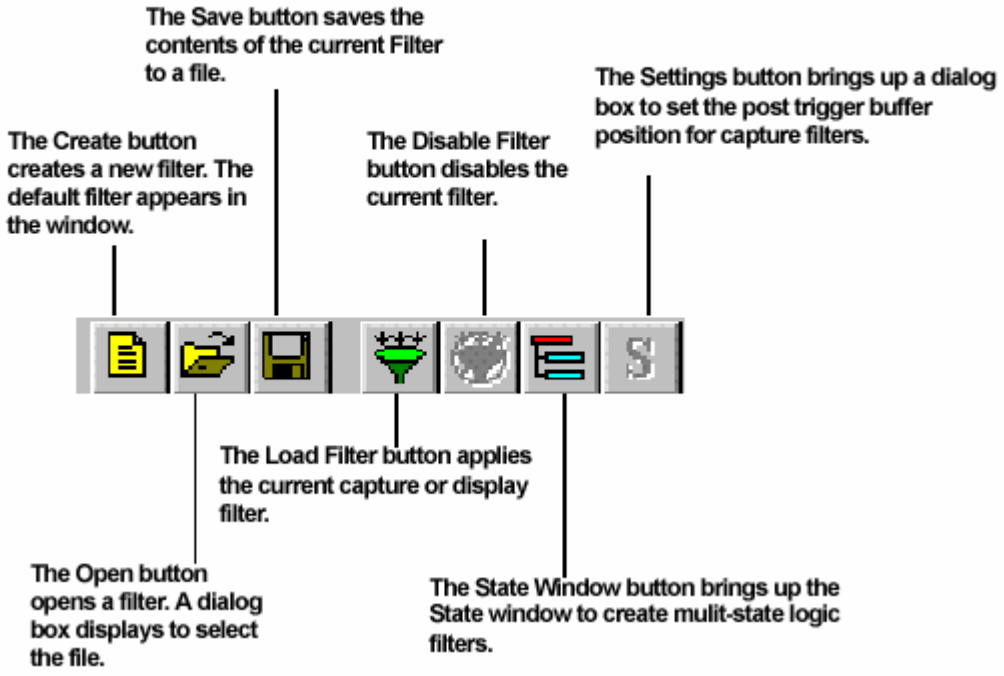
Detail View Toolbar



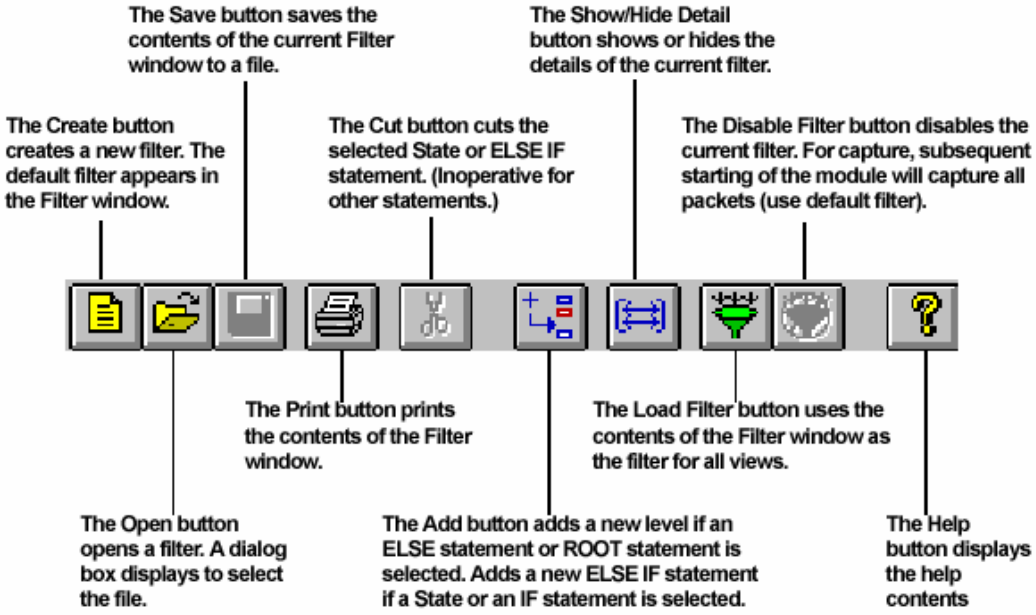
Data Views Toolbar (Note: Only some of these views are available with GMM cards)



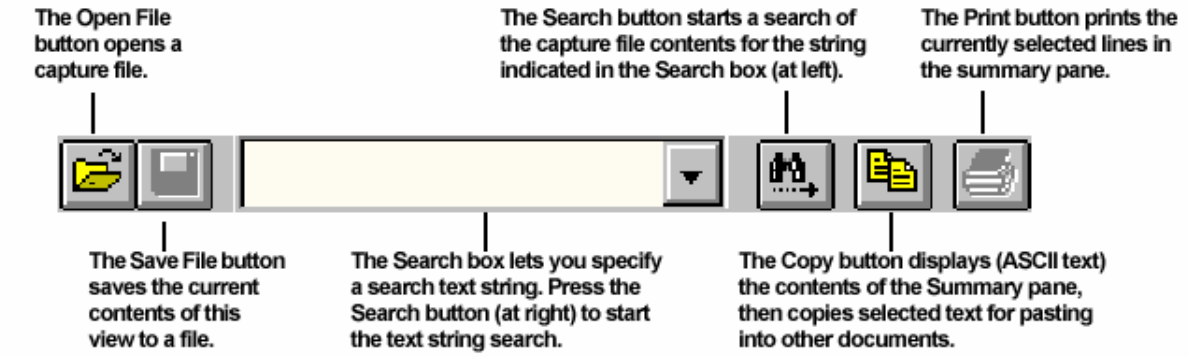
Create/Modify Filter Toolbar

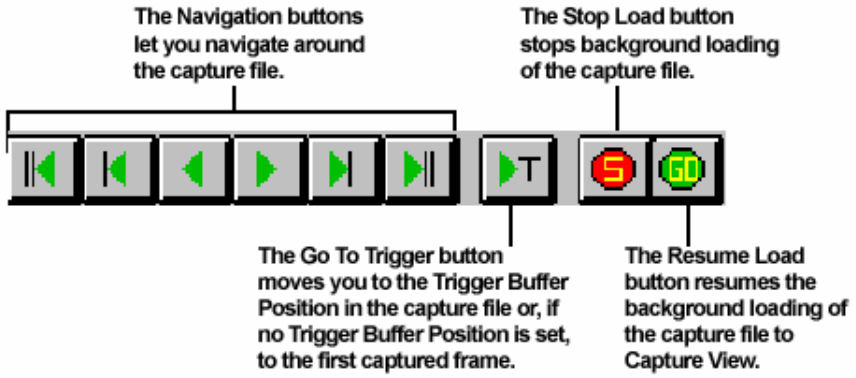


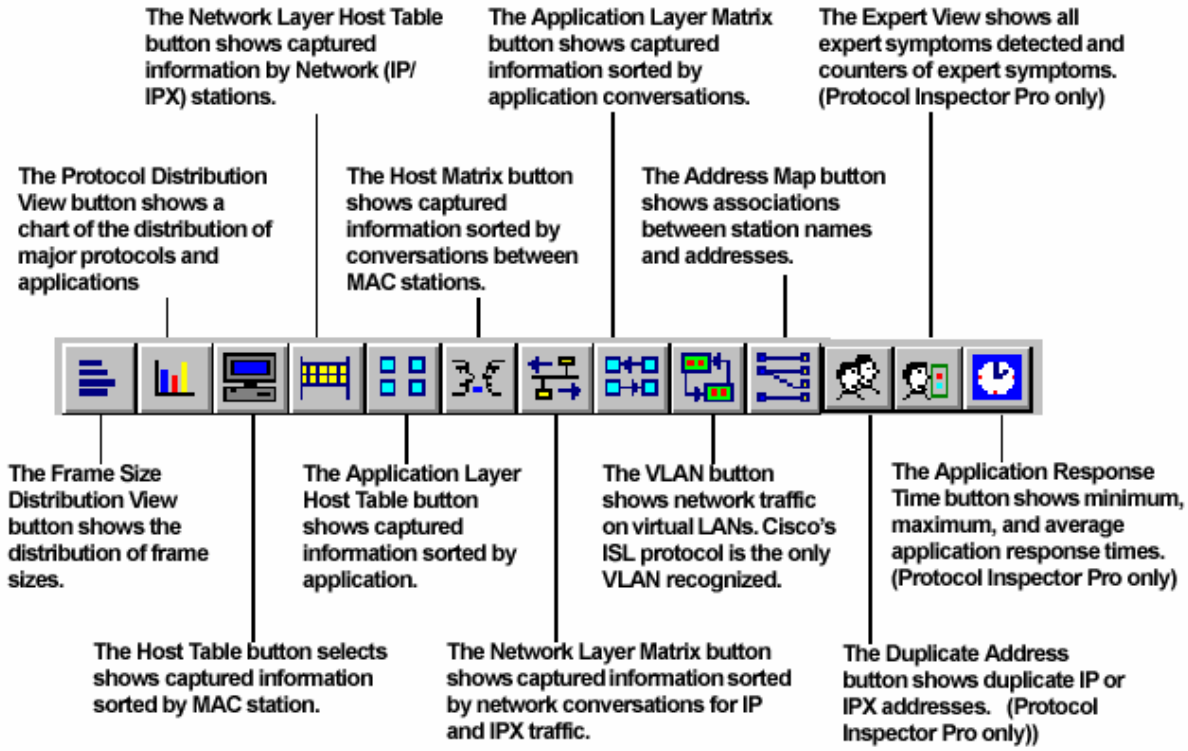
State Toolbar



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

