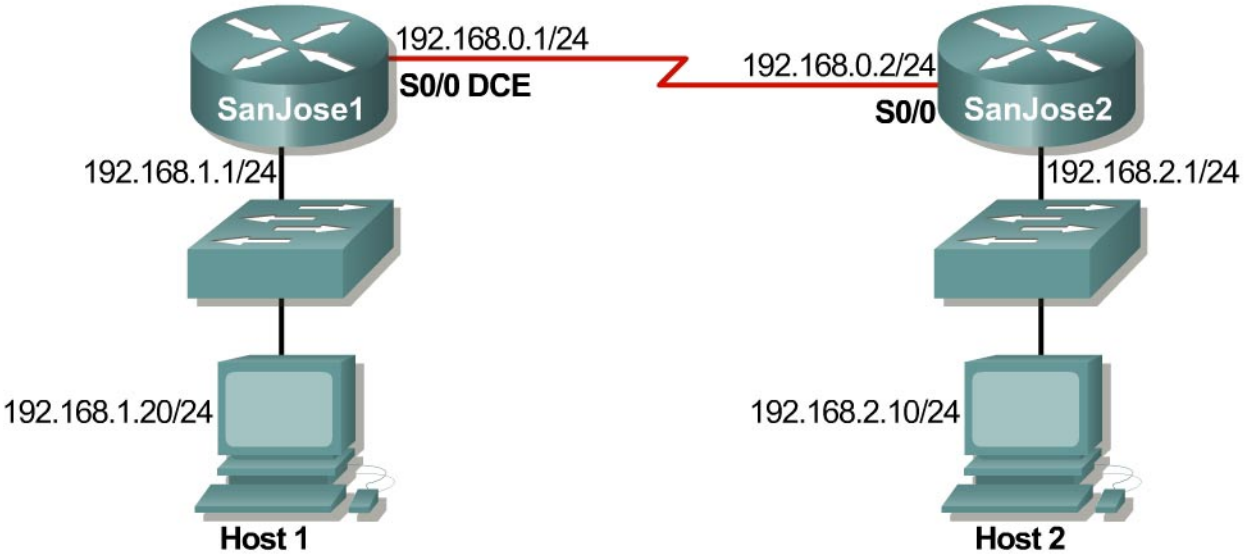
TP 7.1.9b Introduction à Fluke Protocol Inspector



Objectif

Ce TP explique comment utiliser Fluke Networks Protocol Inspector pour analyser le trafic réseau et les trames de données. Il présente les fonctionnalités clés de l'outil, qui pourront être utilisées lors de divers travaux de dépannage dans les TP restants.

Données de base / Préparation

Les informations contenues dans ce TP sont fournies à titre d'exemple uniquement. Les résultats peuvent en effet varier, selon le nombre d'équipements ajoutés, selon les adresses MAC des équipements et leur nom d'hôte, selon le réseau LAN étudié, etc.

Ce TP introduisant le logiciel Protocol Inspector se révélera utile lorsque vous traiterez les prochains TP de dépannage, ainsi que sur le terrain. Si le logiciel Network Inspector constitue un élément important du programme Cisco Networking Academy Program, il donne également un aperçu des fonctionnalités que peuvent posséder les autres produits sur le marché.

Pour réaliser ce TP, deux choix vous sont proposés:

1) L'utilisation de Protocol Inspector ou de Protocol Expert dans un petit réseau LAN contrôlé, configuré par le professeur dans un environnement de TP fermé, tel qu'illustré dans le schéma ci-dessus. L'équipement minimal requis consiste en une station de travail, un commutateur et un routeur.

2) La réalisation des étapes du TP dans un environnement plus grand tel que le réseau de la salle de classe ou de l'école pour plus de diversité. Avant de lancer Protocol Inspector (PI)

ou Protocol Expert (PE) sur le réseau LAN de l'école, consultez le professeur et l'administrateur réseau.

Le logiciel Protocol Inspector doit être installé sur au moins un des hôtes. Si ce TP s'effectue en binômes, l'installation du logiciel sur les deux postes permettra à chacun des étudiants d'effectuer lui-même les différents exercices. Il se peut toutefois que les hôtes affichent des résultats légèrement différents.

Étape 1 Configurez le TP ou connectez une station de travail au réseau LAN de l'école.

Option 1. Si vous avez choisi un environnement de TP fermé, connectez l'équipement comme indiqué ci-dessus et chargez les fichiers de configuration dans les routeurs appropriés. Ces fichiers sont peut-être préchargés. Dans le cas contraire, demandez-les à votre professeur. Ces fichiers doivent prendre en charge le système d'adressage IP comme illustré dans le schéma ci-dessus et dans le tableau ci-après.

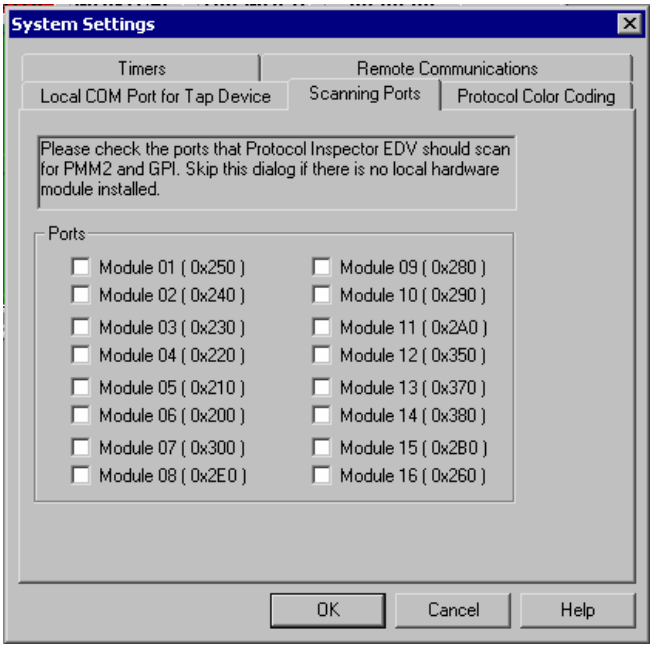
Configurez les stations de travail selon les indications fournies dans l'illustration ci-dessus et dans le tableau suivant.

Hôte n°1	**Hôte n°2**
Adresse IP: 192.168.1.20	Adresse IP: 192.168.2.10
Masque de sous-réseau: 255.255.255.0	Masque de sous-réseau: 255.255.255.0
Passerelle par défaut: 192.168.1.1	Passerelle par défaut: 192.168.2.1

Option 2. Si vous avez choisi la deuxième option (connexion au réseau LAN de l'école), reliez la station de travail sur laquelle est installé Protocol Inspector ou Protocol Expert directement au commutateur d'une salle de classe ou à une prise de données connectés au réseau LAN de l'école.

Étape 2 Lancez le programme Protocol Inspector Version éducative.

À partir du menu Démarrer, lancez le programme Fluke Protocol Inspector Version éducative.

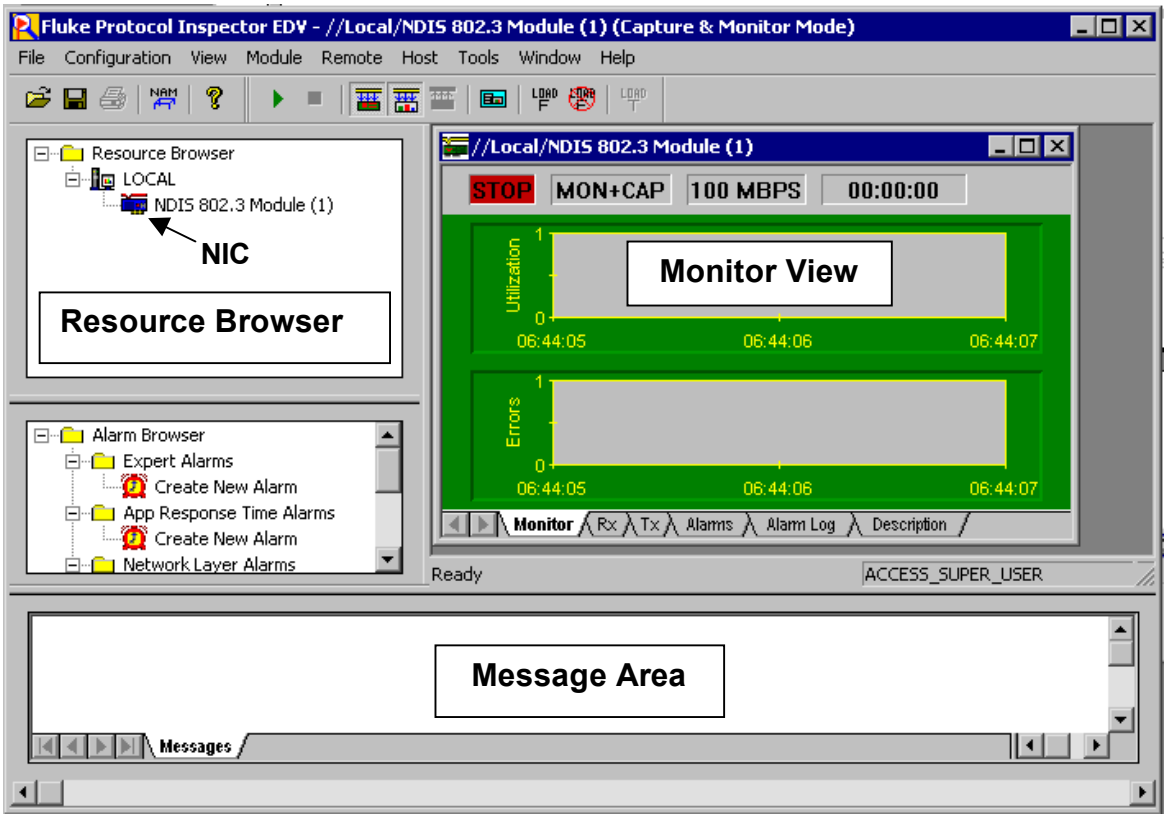
Remarque: Lors de la première exécution du programme, le message suivant apparaît: « **Do you have any Fluke analyzer cards or Fluke taps in your local system?** » Si vous utilisez la version éducative, cliquez sur **No**. Si vous répondez oui ou si l'écran suivant apparaît, cliquez sur **OK** sans sélectionner de ports.	

Il existe quatre vues principales dans Protocol Inspector:

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

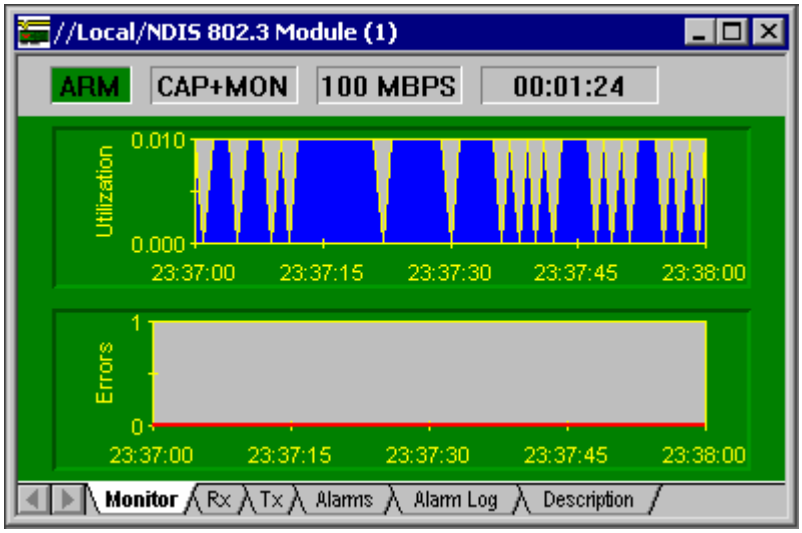
Le programme s'ouvre sur la fenêtre **Summary View**. Cette vue présente différentes fenêtres utilisées par l'outil. La fenêtre **Resource Browser**, située dans le coin supérieur gauche, présente la seule unité de surveillance disponible, à savoir le module NDIS 802.3 (carte réseau) de l'hôte. Lorsque des unités de surveillance de supports de protocole sont disponibles, elles figurent à cet emplacement avec les équipements hôtes associés. La fenêtre **Alarm Browser**, dans la partie gauche, et la fenêtre **Message Area**, en bas, seront traitées un peu plus loin.

La fenêtre **Monitor View**, qui constitue la fenêtre principale (en haut à droite), surveille une ressource par fenêtre avec plusieurs options d'affichage. L'exemple ci-dessous, et probablement l'écran de démarrage, indique qu'aucune information n'est affichée dans la fenêtre de surveillance. L'indication **Stop**, apparaissant dans le coin supérieur gauche de la fenêtre, confirme l'absence de surveillance.



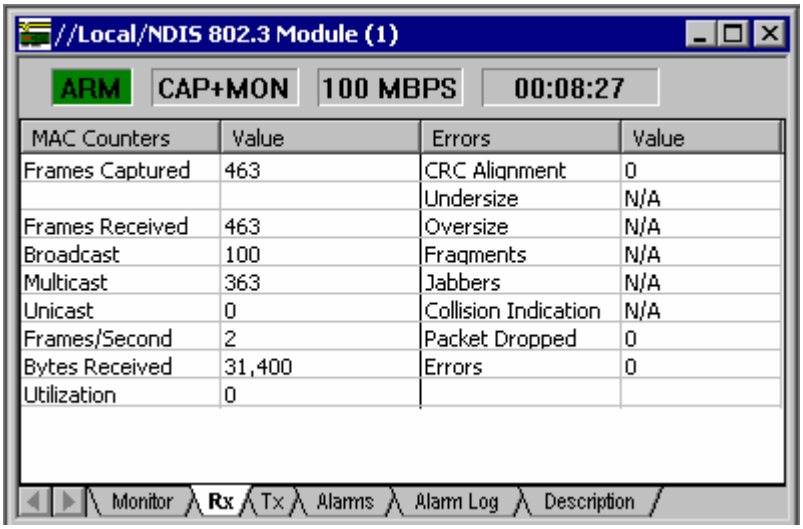
Étape 3 Lancez le processus de surveillance/capture.

Pour lancer le processus de surveillance/capture, utilisez le bouton **Start** ou cliquez sur le menu Module | Start. Le tableau d'utilisation doit commencer à afficher les activités comme dans le graphique suivant.



Le terme **Arm** doit apparaître là où figurait précédemment l'indication **Stop**. Si vous ouvrez le menu **Module**, vous remarquerez que **Stop** est devenu une option, alors que **Start** est désactivé. N'arrêtez pas le processus tout de suite. Redémarrez-le s'il est arrêté.

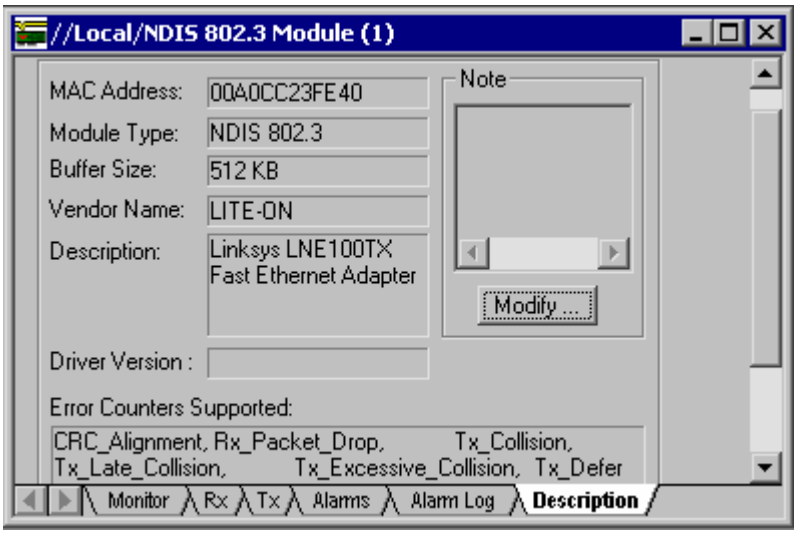
Les onglets en bas de la fenêtre affichent les données sous différentes formes. Cliquez sur chacun d'eux et observez le résultat. Les vues **Transmit** (**Tx**), **Alarms** et **Alarm Log** sont vides. Les trames **Received** (**Rx**) ci-dessous indiquent que les trames de **Broadcast** et de **Multicast** sont en cours de réception, mais qu'il risque de n'y avoir aucune trame **Unicast**.



À l'aide d'une connexion console au routeur, envoyez une requête ping à l'hôte de surveillance (192.168.1.20 ou 192.168.2.10) et remarquez l'apparition de trames **Unicast**. Malheureusement, les erreurs signalées dans la troisième colonne n'apparaissent pas dans cet exercice de TP, à moins qu'un générateur de trafic tel que le produit Fluke Networks OptiView n'ait été ajouté.

L'onglet de **Description** comporte des informations telles que l'adresse MAC, le nom du fabriquant et le modèle de la carte réseau. Il indique également les compteurs d'erreurs pris en charge.

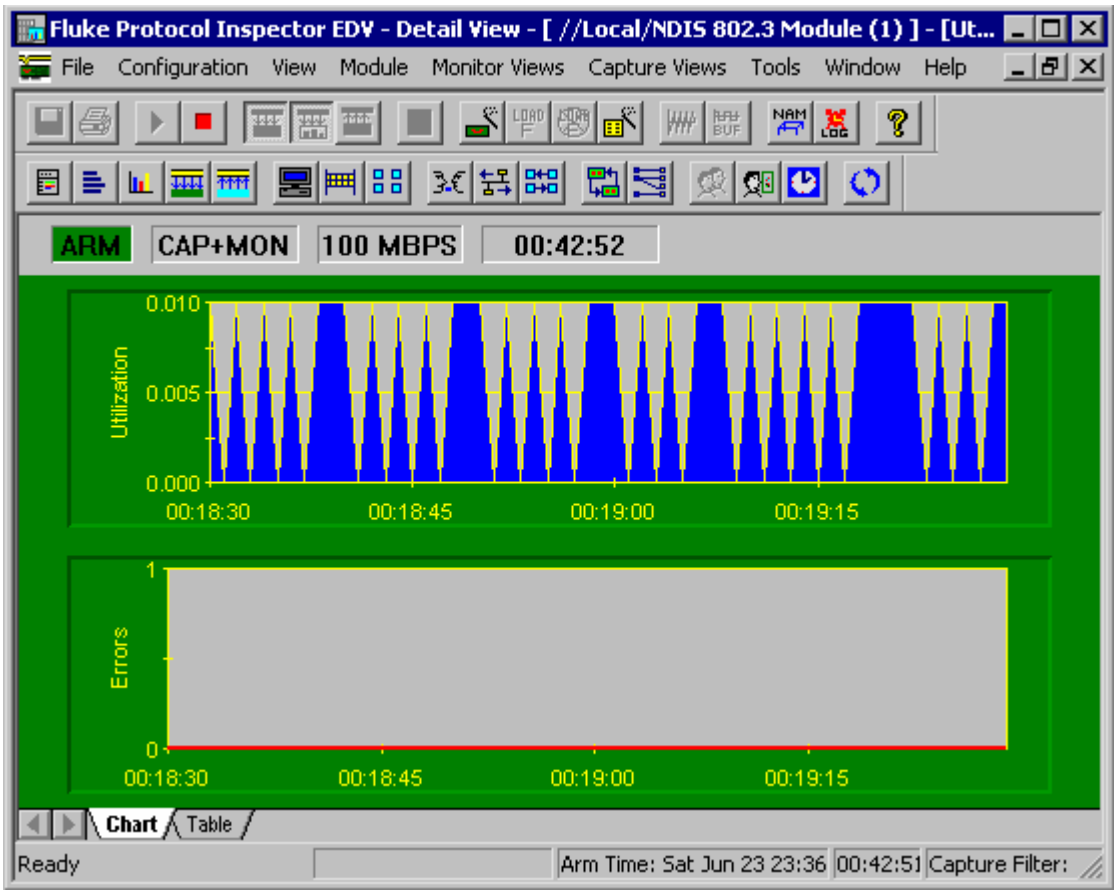
Prenez quelques minutes pour vous familiariser avec les onglets et les fonctions de défilement de la fenêtre.



Étape 4 Affichez les détails.

Pour accéder à la fenêtre **Detail View**, cliquez sur le bouton correspondant  dans la barre d'outils ou double-cliquez n'importe où dans le tableau de la vue de surveillance. Cette opération permet d'ouvrir une deuxième fenêtre qui devrait ressembler à celle illustrée ci-dessous, lorsque

vous aurez agrandi la fenêtre **Utilization / Errors Strip Chart (RX)**.



Remarque: si nécessaire, activez toutes les barres d'outils sur le menu d'affichage.

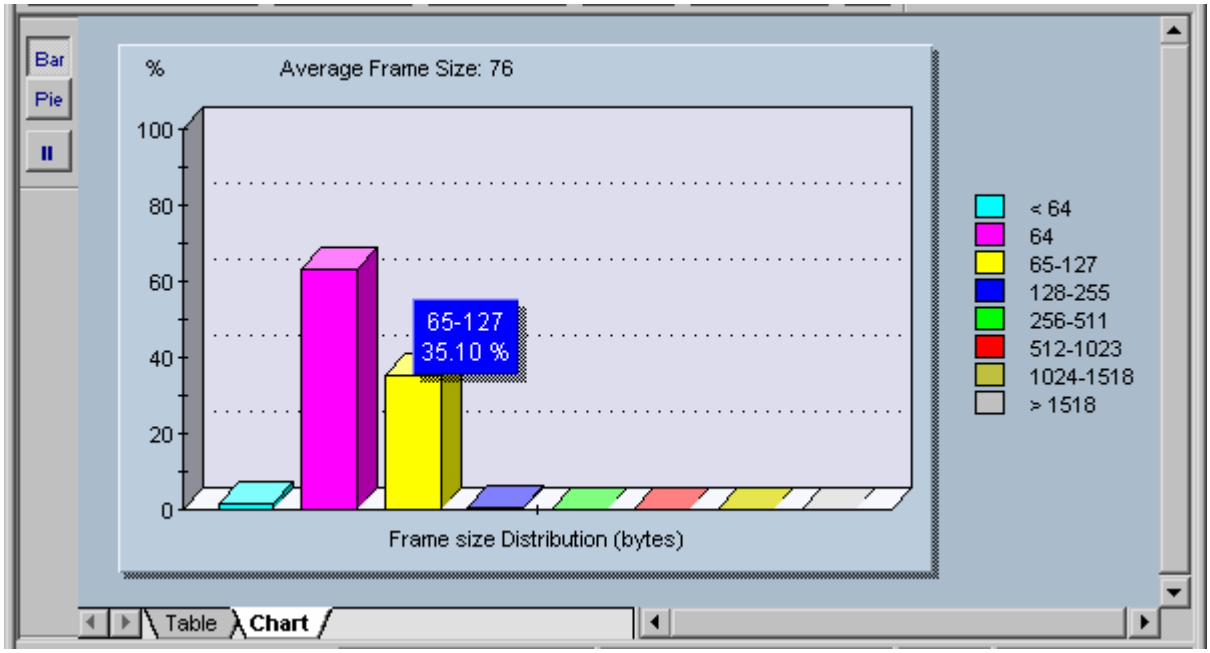
À première vue, les données du tableau sont les mêmes que précédemment. Néanmoins, cette vue comporte beaucoup plus de barre d'outils et d'options de menu que la vue récapitulative. Avant d'examiner ces fonctions, assurez-vous que les onglets **Chart** et **Table** comportent les mêmes informations que celles affichées précédemment.

Comme dans tous les programmes compatibles avec Windows, un renseignement sur la fonction d'un bouton apparaît lorsque vous placez la souris dessus. Notez que certains de ces boutons sont grisés et qu'aucune information n'apparaît si vous positionnez le curseur dessus. Cela signifie que la fonction correspondante ne peut être utilisée dans les circonstances actuelles. Dans certains cas, la version éducative ne la prend pas en charge.

Remarque: dans l'annexe qui se trouve à la fin de ce TP, vous trouverez l'affichage complet des barres d'outils, ainsi que leurs fonctions.

Cliquez sur le bouton  **Mac Statistics** pour faire apparaître les données du tableau des trames Rx sous un autre format. La différence est flagrante. Agrandissez la fenêtre qui apparaît. Le nouvel élément d'information **Speed** indique le débit de transmission de la carte réseau.

Cliquez sur le bouton  **Frame Size Distribution** pour afficher la répartition par taille des trames reçues par la carte réseau. Si vous placez le curseur sur une barre quelconque, un résumé comme celui illustré ci-dessous apparaît. Agrandissez la fenêtre.

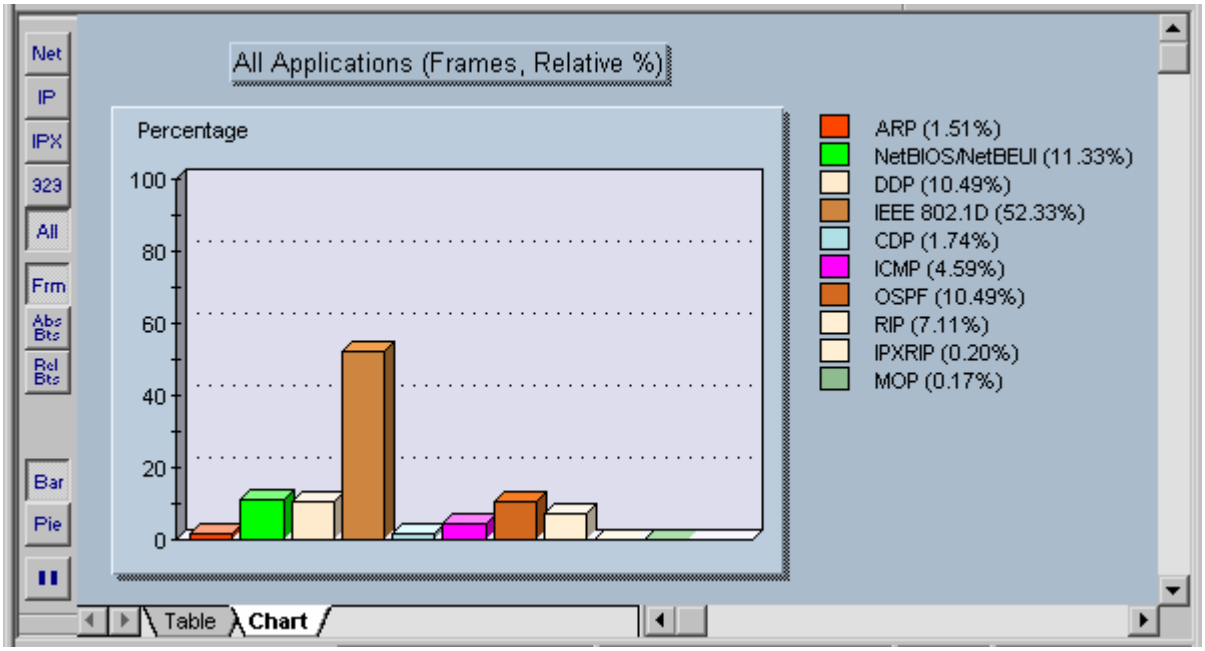


Cliquez sur les boutons **Pie**, **Bar** et **Pause** dans le coin supérieur gauche. Le bouton **Pause** arrête la capture. Pour recommencer la capture, cliquez dessus une nouvelle fois. Examinez l'affichage des onglets **Table** et **Chart**.

Avec les exemples de configuration, l'étudiant devrait principalement recevoir de petites trames, car seules les mises à jour de routage sont en cours. Essayez d'utiliser la fonction ping étendue à partir d'une connexion console avec le routeur et spécifiez 100 requêtes ping avec une taille de paquet supérieure.

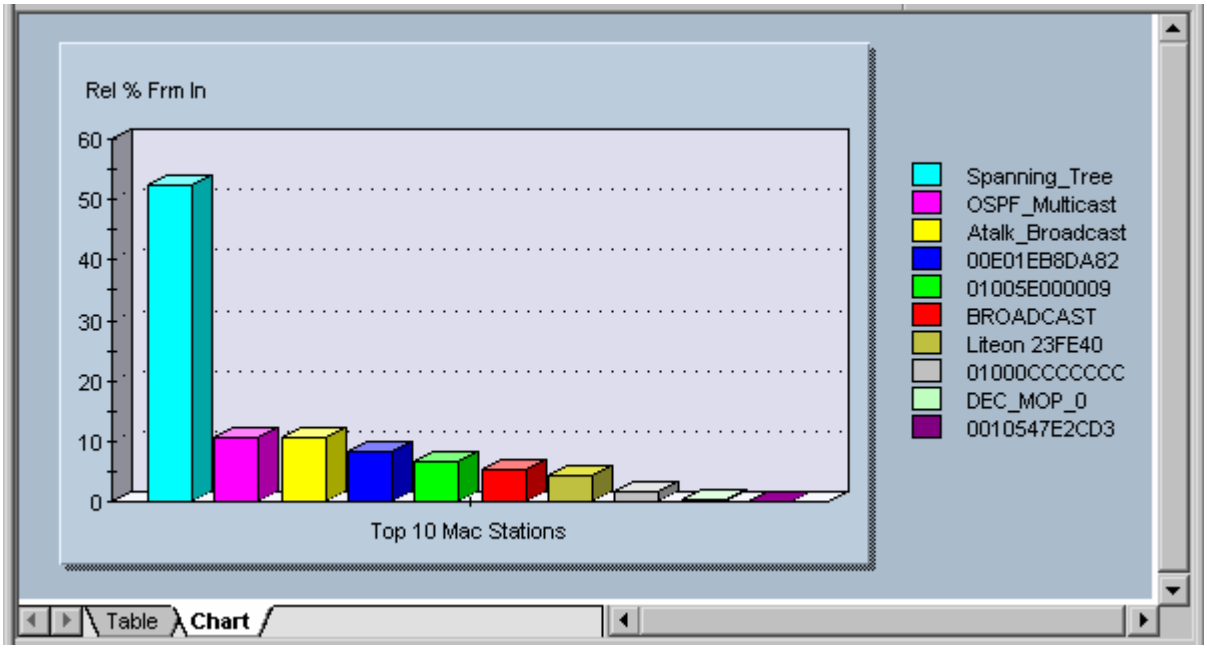
Si vous agrandissez chaque nouvel affichage, vous pouvez revenir à l'une des vues précédentes à l'aide du menu Window. L'étudiant peut également afficher les fenêtres en mosaïque. Familiarisez-vous avec les fonctions du menu Window, puis fermez les vues non souhaitées.

Cliquez sur le bouton **Protocol Distribution** pour afficher la répartition des protocoles reçus par la carte réseau. Si vous placez le curseur sur l'une des barres, un petit panneau récapitulatif apparaît. Agrandissez la fenêtre qui apparaît.



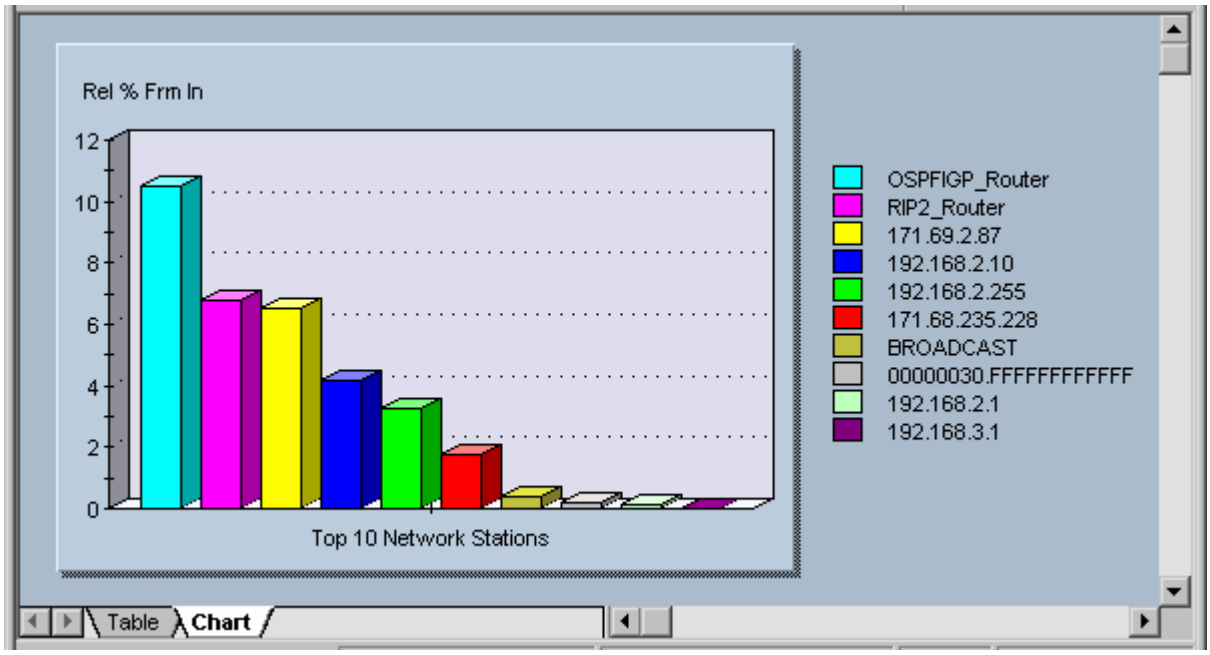
Cliquez sur chacun des boutons et des onglets et observez les différences. Le bouton **Net** affiche uniquement les protocoles réseau. Le bouton **323** fait référence aux protocoles H323 de voix sur IP. Selon la version de Protocol Expert ou de Protocol Inspector utilisée, ce bouton peut être appelé VoIP. Testez les boutons **Frm** (trame), **Abs Bts** (octets absolus) et **Rel Bts** (octets relatifs) pour voir les différences. Rappelez-vous que le bouton **Pause** arrête la capture.

Cliquez sur le bouton  **Host Table** pour afficher les stations MAC et le trafic associé.



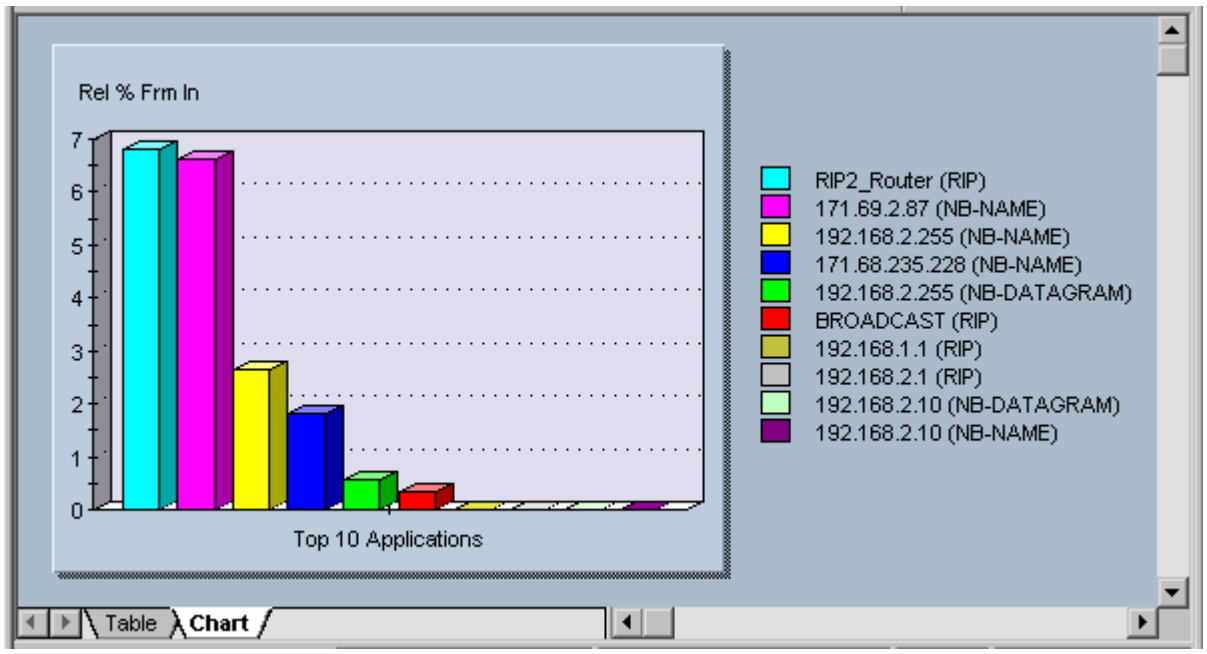
Observez le trafic OSPF, Apple Talk et Spanning Tree. Veillez à utiliser l'onglet **Table** pour consulter les valeurs réelles.

Cliquez sur le bouton  **Network Layer Host Table** pour afficher les stations réseau (IP/IPX) et le trafic associé.



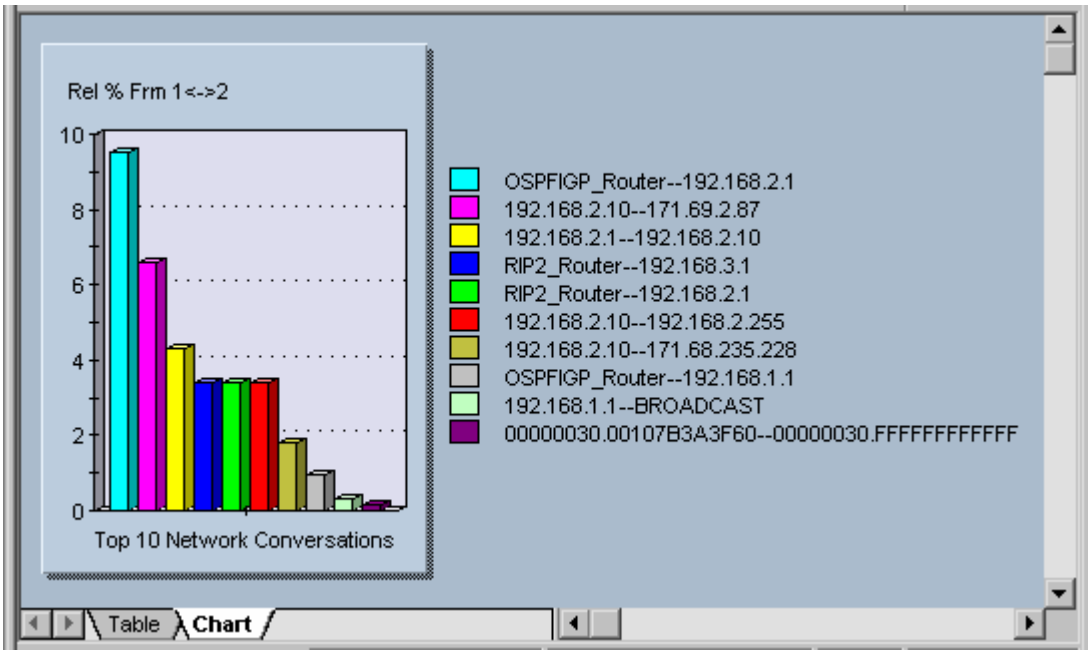
Les requêtes ping ou les hôtes supplémentaires ajoutés à la configuration ont une incidence sur les adresses qui apparaissent sur la droite.

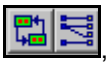
Cliquez sur le bouton  **Application Layer Host Table** pour afficher le trafic des stations du réseau par application.



Familiarisez-vous avec les trois boutons suivants  . Ils créent des matrices hôte-hôte pour les conversations de la couche application, MAC et réseau. L'exemple ci-dessous illustre les

conversations de la couche réseau (IP/IPX).



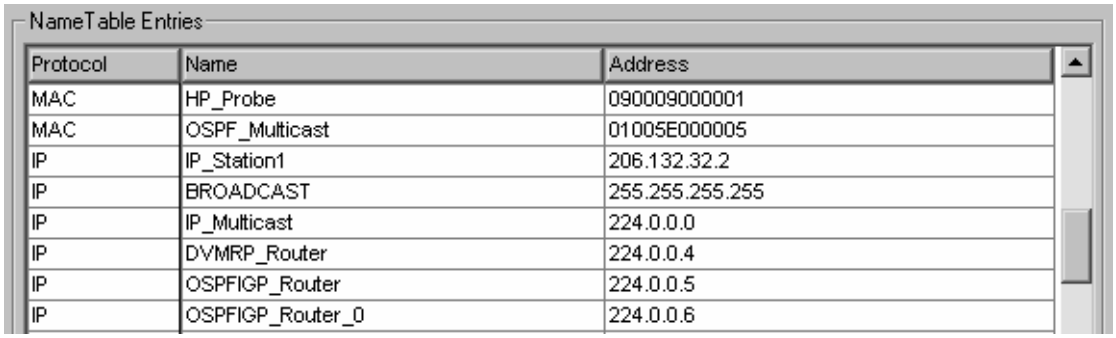
Parmi les deux boutons suivants  , le premier, **VLAN**, présente le trafic des réseaux LAN virtuels. Cet exemple n'utilise pas ce type de réseau. Souvenez-vous de l'existence de ce bouton lors des opérations de dépannage des réseaux LAN virtuels, abordées ultérieurement.

Le deuxième bouton crée une matrice comparant les adresses et les noms des stations MAC et réseau. Dans l'exemple suivant, la deuxième ligne correspond à une station 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

Le bouton 

Name Table permet d'ouvrir la table de noms actuelle afin de la consulter ou de la modifier.



Le bouton  **Expert View** permet d'afficher les symptômes découverts par l'expert. Ces statistiques indiquent de quelle manière les PI tentent de relever les problèmes éventuels. Les options soulignées indiquent qu'il est possible d'afficher d'autres fenêtres contenant plus de détails, si des valeurs sont enregistrées. L'exemple de ce TP ne fournit pas beaucoup de renseignements, mais il aborde les solutions de débogage ISL, HSRP et d'autres types de problèmes qui seront traités dans les prochains TP.

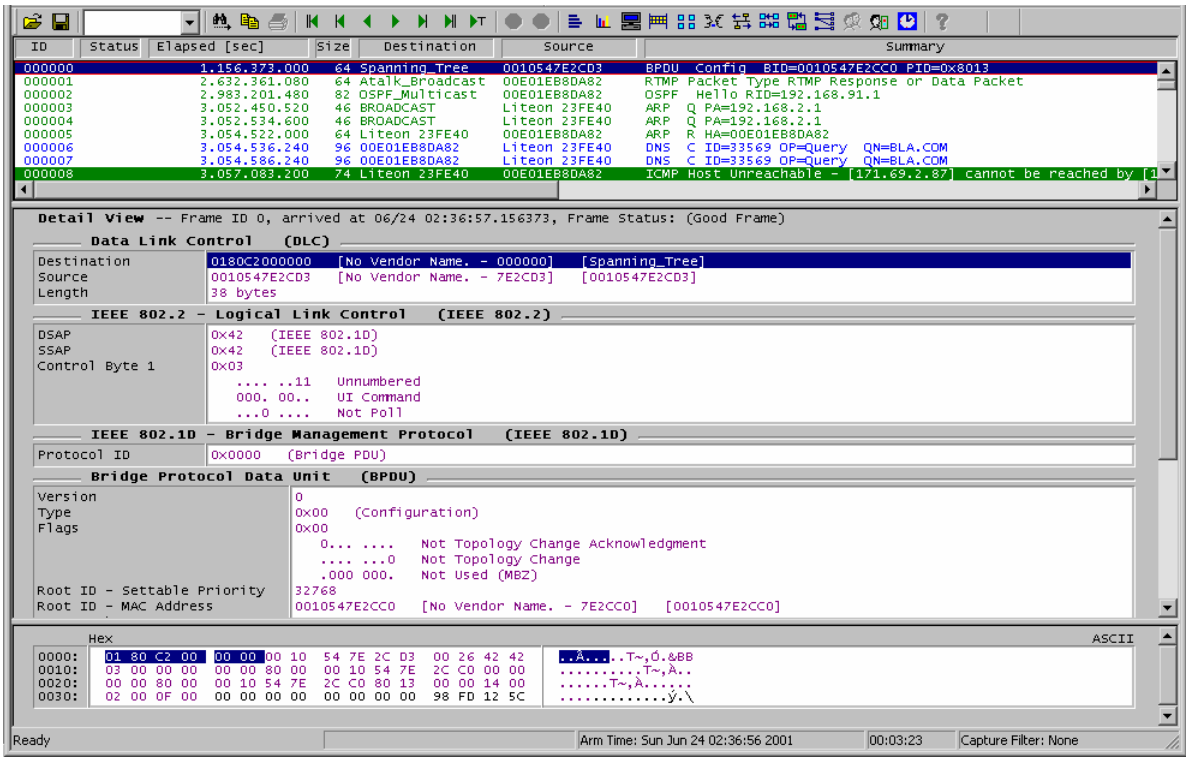
Expert Category	Value	Expert Category	Value
ICMP All Errors	368	Duplicate Network Address	0
ICMP Destination Unreachable	368	Unstable MST	0
ICMP Redirects	0	SAP Broadcast	0
Excessive Bootp	0	OSPF Broadcast	923
Excessive ARP	0	RIP Broadcast	25
NFS Retransmissions	0	ISL Illegal VLAN ID	0
TCP/IP SYN Attack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

Étape 5 Arrêtez le processus de capture.

Pour arrêter la capture de trames afin de vous intéresser à des trames individuelles, utilisez le bouton  **Stop** ou cliquez sur Module | Arrêter.

Une fois la capture arrêtée, cliquez sur le bouton  **Capture View**. Dans la version éducative, un message apparaît, annonçant que la capture est limitée à 250 paquets. Cliquez sur OK.

La fenêtre qui apparaît peut sembler à première vue un peu trop dense. Agrandissez-la pour masquer les autres fenêtres ouvertes en arrière-plan.

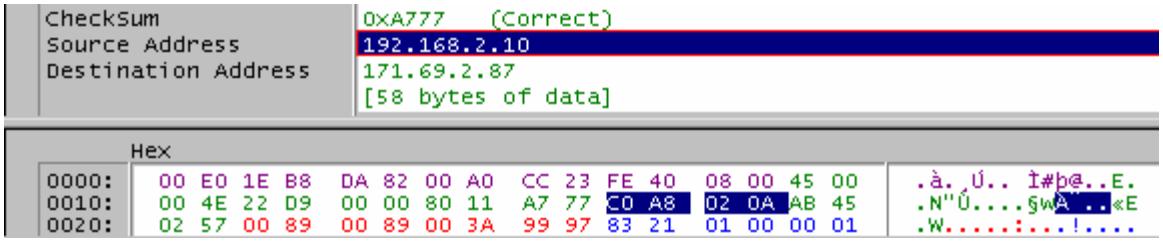


En étudiant les résultats, vous pouvez constater qu'il y a en réalité trois fenêtres horizontales. La fenêtre située en haut répertorie les paquets capturés. Celle du milieu fournit des détails sur le paquet sélectionné dans la fenêtre du haut, tandis que celle du bas présente les valeurs HEX de ce paquet.

En positionnant le curseur sur les lignes horizontales des contours de ces fenêtres, un curseur de déplacement de ligne ou une flèche à double sens apparaît. Cela vous permet de modifier la répartition de l'espace dédié à chacune des fenêtres. Il peut être judicieux d'élargir autant que possible la fenêtre du milieu et de laisser cinq à six rangées dans chacune des deux autres fenêtres, comme illustré ci-dessus.

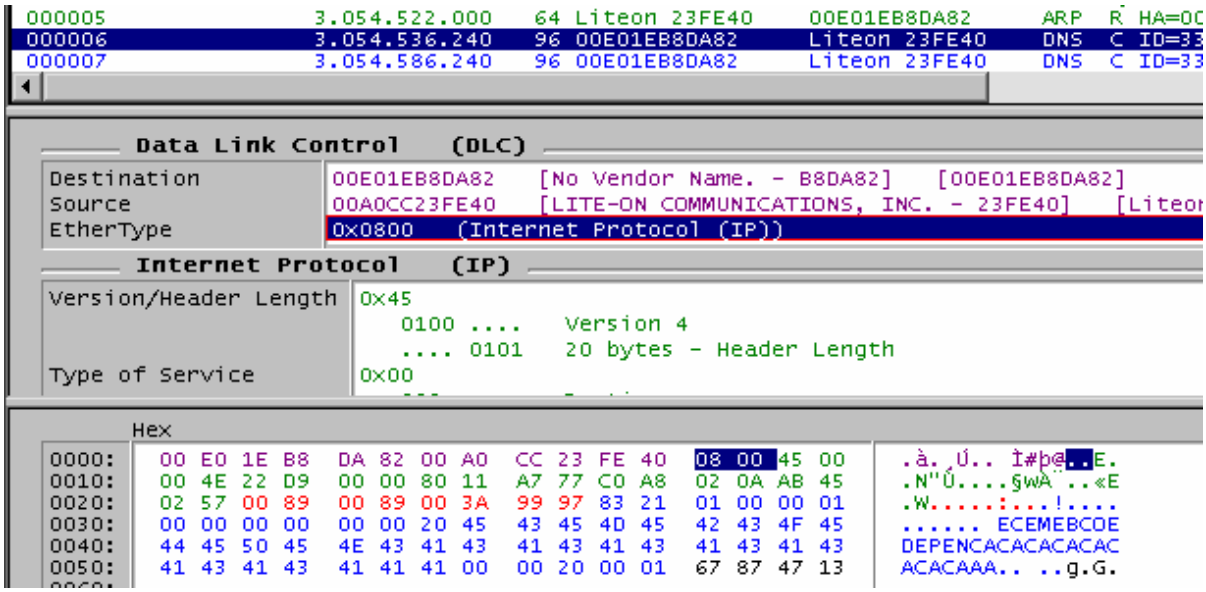
Examinez les paquets répertoriés dans la fenêtre du haut. Vous devriez y trouver des paquets DNS, ARP, RTMP et autres. Si vous utilisez un commutateur, des paquets CDP et Spanning Tree doivent y être représentés. Lorsque vous sélectionnez des lignes dans la fenêtre du haut, observez les modifications que cette opération implique sur le contenu des deux autres fenêtres.

Sélectionnez une information dans la fenêtre du milieu et observez la modification de l'affichage HEX dans la fenêtre du bas, qui indique alors l'emplacement de stockage de cette information. Dans l'exemple suivant, lorsque vous sélectionnez l'adresse source (IP), les valeurs HEX du paquet apparaissent.



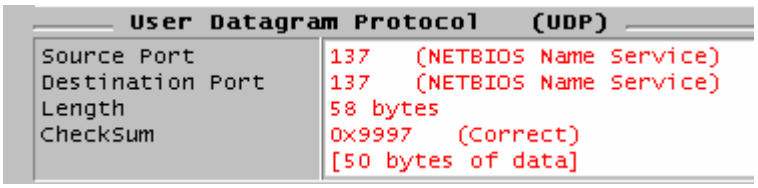
Vous constaterez que les codes de couleur permettent de repérer plus aisément les informations de la fenêtre du milieu dans la fenêtre HEX. Dans l'exemple suivant, portant sur un paquet DNS, les

données de la section DLC (*Data Link Control*) de la fenêtre du milieu apparaissent en mauve, tandis que celles de la section du protocole IP sont affichées en vert. Les valeurs HEX correspondantes sont de la même couleur.



Dans l'exemple ci-dessus, le champ **EtherType** indique **0x0800**. Cela signifie qu'il s'agit d'un paquet IP. Observez les adresses MAC des hôtes source et de destination, ainsi que l'emplacement de ces données dans l'affichage HEX.

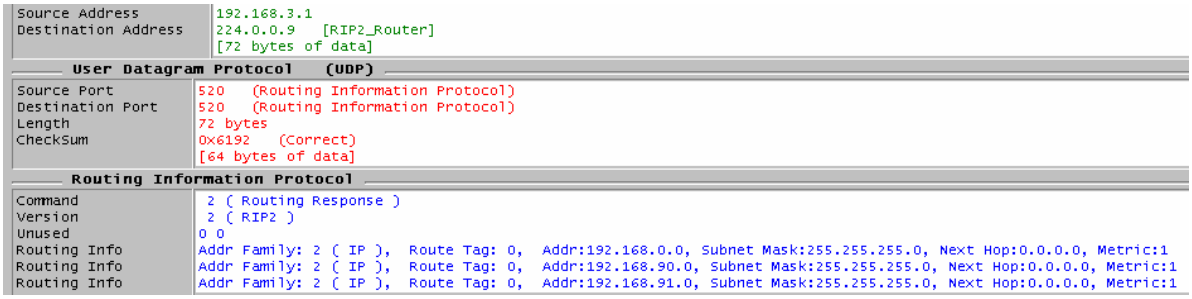
Dans le même exemple, la section suivante de la fenêtre du milieu contient les informations liées au **protocole de datagramme utilisateur (UDP)**, avec les numéros de port UDP.



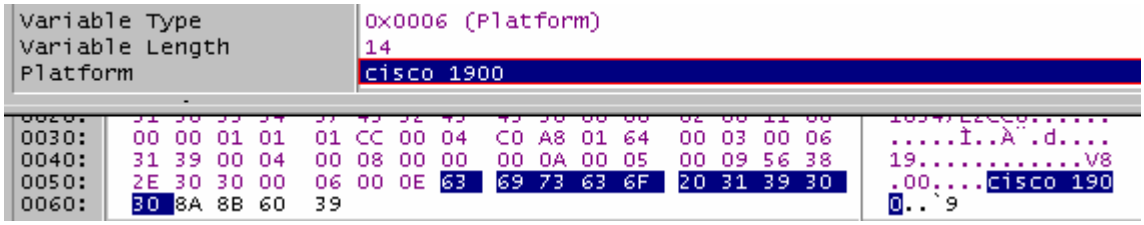
La structure de la fenêtre du milieu change en fonction du type de paquet.

Prenez quelques minutes pour sélectionner les différents types de paquets dans la fenêtre du haut, puis examinez ensuite l'affichage correspondant dans les deux autres fenêtres. Soyez particulièrement attentif au champ EtherType, aux numéros de port, ainsi qu'aux adresses d'origine et de destination des couches réseau et MAC. La capture doit contenir des paquets RIP, OSPF et RTMP ou AppleTalk. Assurez-vous que les données importantes peuvent être localisées et interprétées. Dans la capture RIP suivante, vous pouvez constater qu'il s'agit d'un paquet RIP version 2. L'adresse de destination multicast est 224.0.0.9 et les entrées actuelles de la table de routage sont visibles. Quelle serait l'adresse de destination multicast dans la version 1?

_____



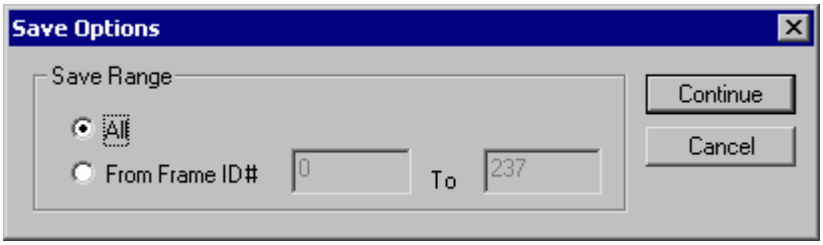
S'il y a des paquets CDP, identifiez la plate-forme. La capture suivante provient d'un commutateur Catalyst 1900.



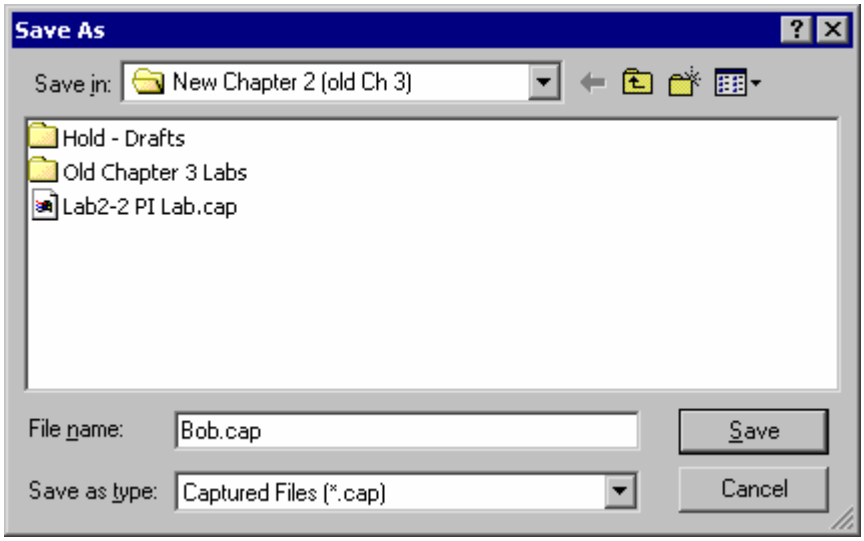
Familiarisez-vous avec les différents outils.

Étape 6 Enregistrez les données capturées.

Pour enregistrer les données capturées, utilisez le bouton  **Save Capture** ou cliquez sur le menu File | Save Capture. Selon la version de Protocol Expert ou de Protocol Inspector, le menu File propose d'enregistrer la section actuelle plutôt que d'enregistrer la capture. Acceptez l'option **All** en cliquant sur le bouton **Continue**. Dans cette fenêtre, l'étudiant a également la possibilité de n'enregistrer qu'une plage de trames capturées.



Utilisez un nom de fichier approprié et enregistrez le fichier sur le disque qui convient. Si l'extension CAP apparaît lorsque cette fenêtre s'ouvre, assurez-vous qu'elle est conservée lorsque vous indiquez le nom.



Utilisez le bouton  **Open Capture File** et ouvrez le fichier appelé Lab 3-2 PI Lab.cap. S'il n'est pas disponible, ouvrez celui qui vient d'être enregistré.

L'étudiant utilise à présent l'outil **Capture View of Capture Files**. Il n'y a pas de différence entre les outils mais la barre de titre, située en haut de l'écran, indique qu'un fichier est consulté plutôt qu'une capture de la mémoire.

Étape 7 Examinez les trames

Sélectionnez une trame dans la fenêtre du haut et faites des manipulations avec les boutons  . Les boutons correspondant aux flèches (sans autre symbole) permettent de déplacer une trame vers le haut ou vers le bas. Les flèches avec un seul trait permettent d'atteindre le haut ou le bas de la fenêtre actuelle, tandis que les flèches à deux traits permettent d'atteindre le haut ou le bas de toute la liste. La flèche avec un T permet également d'atteindre le haut de la liste.

Utilisez les boutons 

Search pour effectuer des recherches. Entrez du texte, par exemple OSPF, dans la zone de liste. Cliquez ensuite sur les jumelles pour passer d'une entrée OSPF à une autre.

Entraînez-vous pour vous familiariser avec ces outils.

Réflexion

a. Comment utiliser cet outil lors de la résolution de problèmes

_____

b. Est-ce que toutes les données du réseau sont analysées?

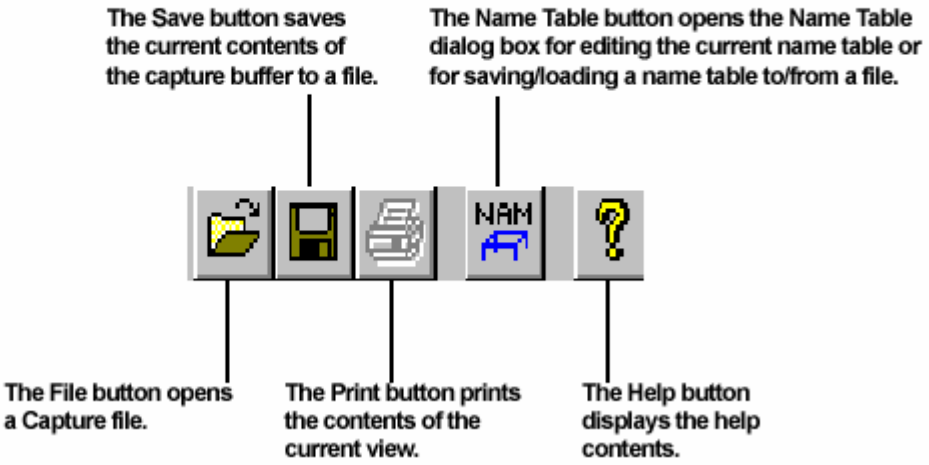
_____

c. Quelle est l'incidence d'une connexion à un commutateur?

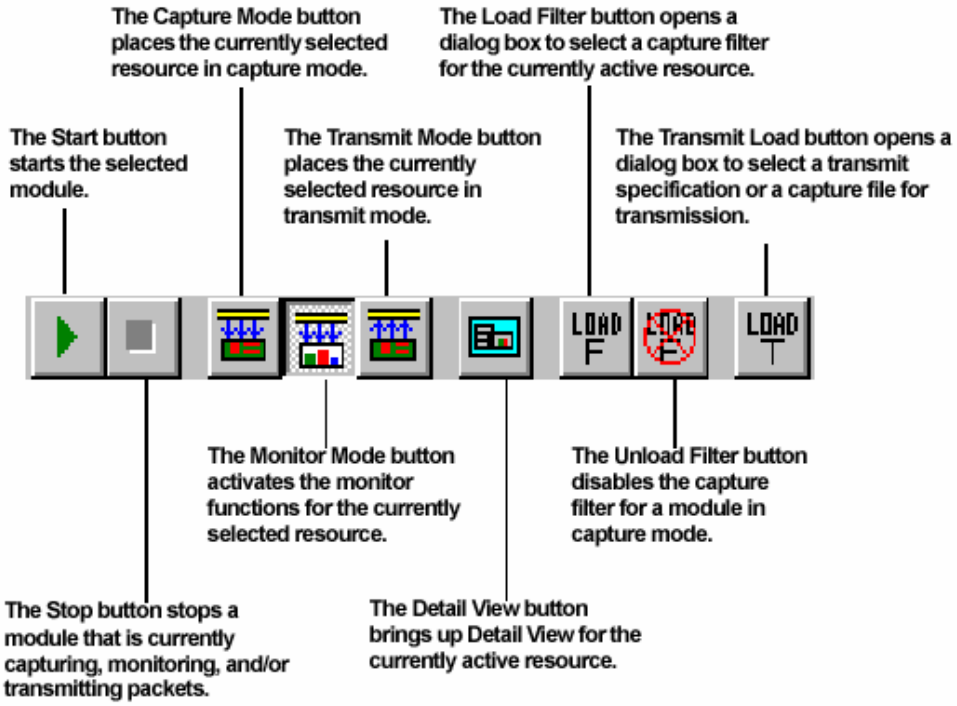
_____

Annexe: Barres d'outils de Protocol Inspector

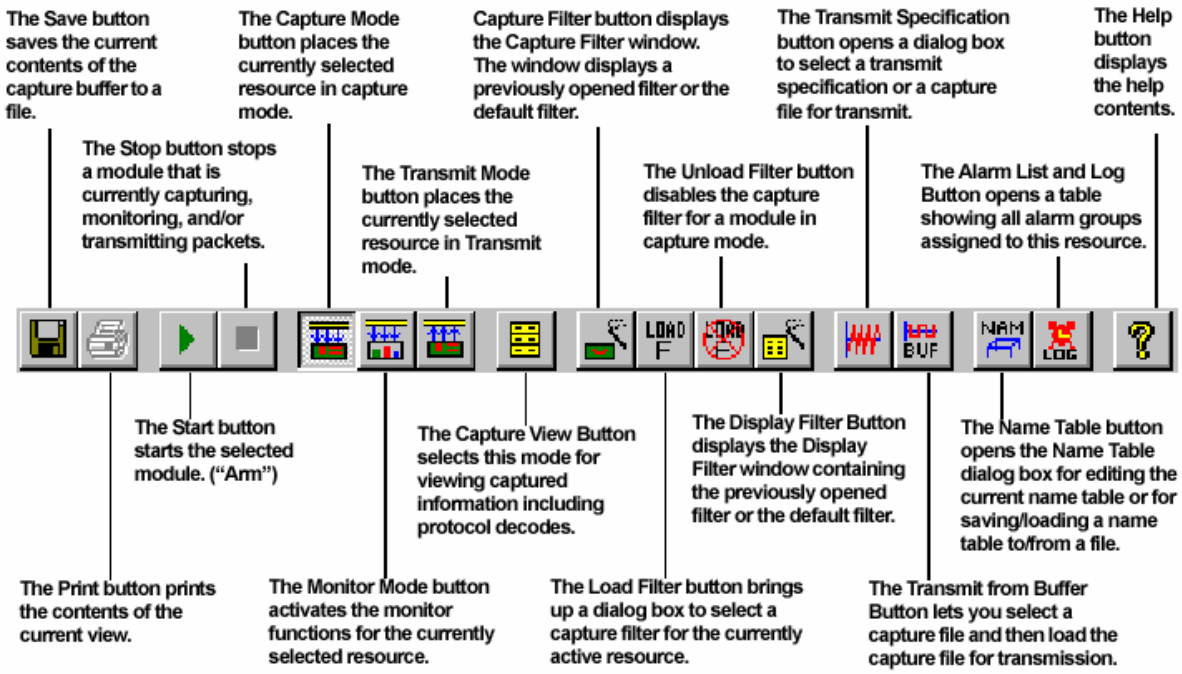
Protocol Inspector Toolbar



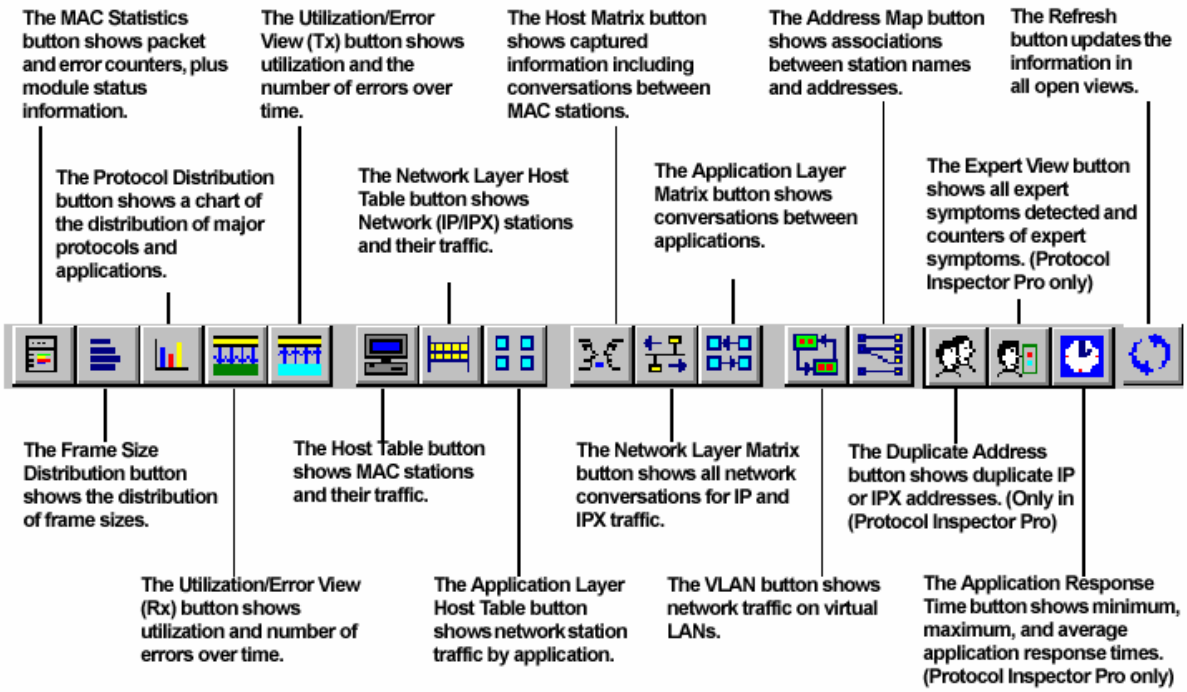
Module Toolbar (Summary View)



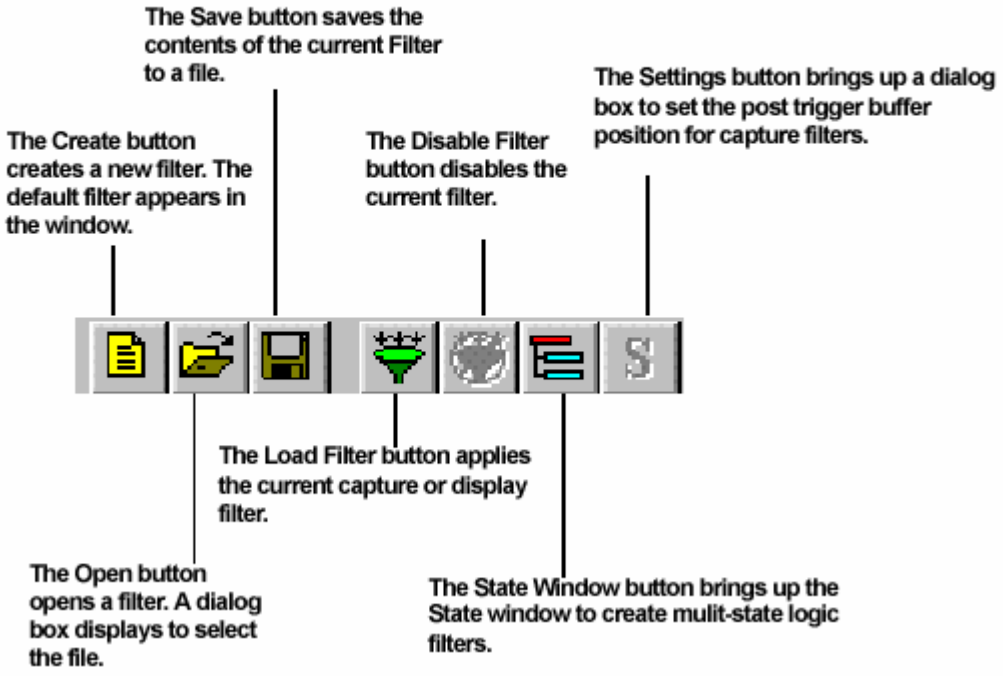
Detail View Toolbar



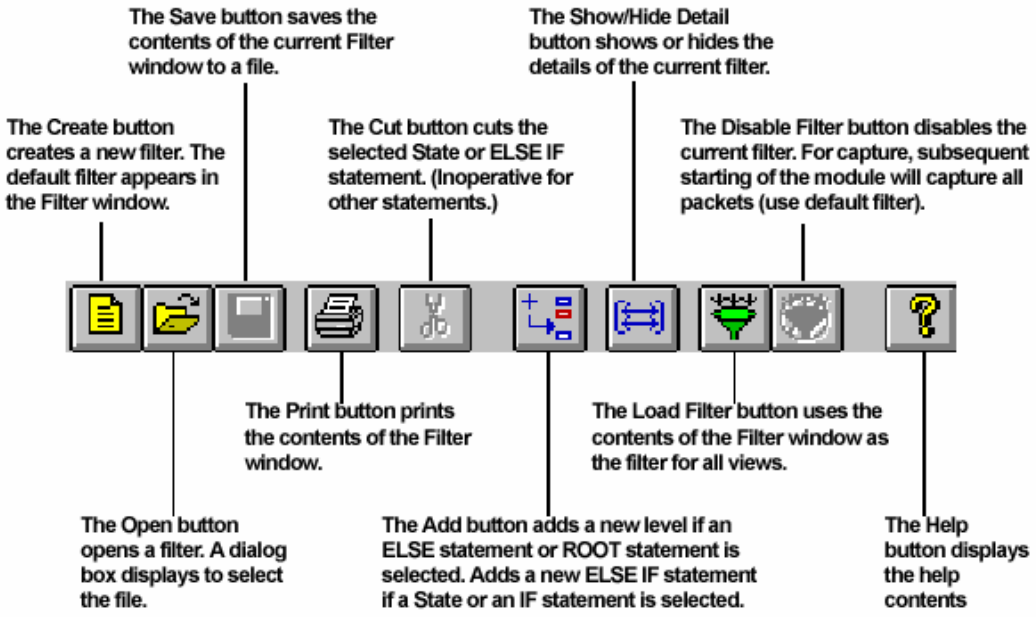
Data Views Toolbar (Note: Only some of these views are available with GMM cards)



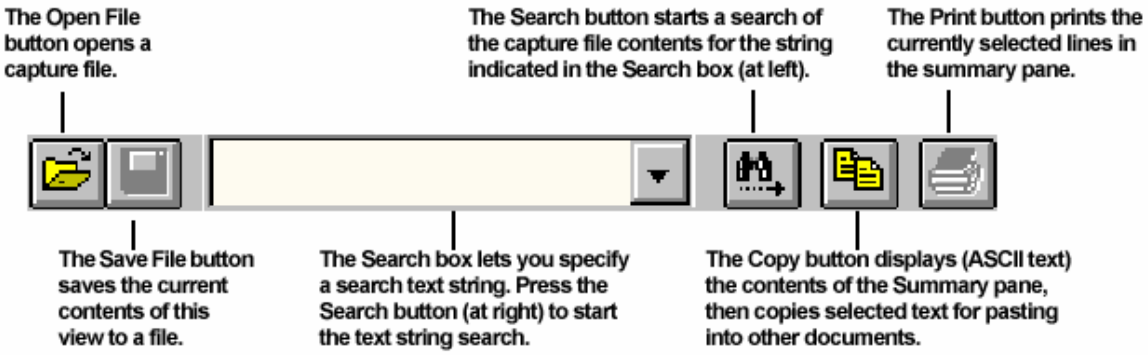
Create/Modify Filter Toolbar

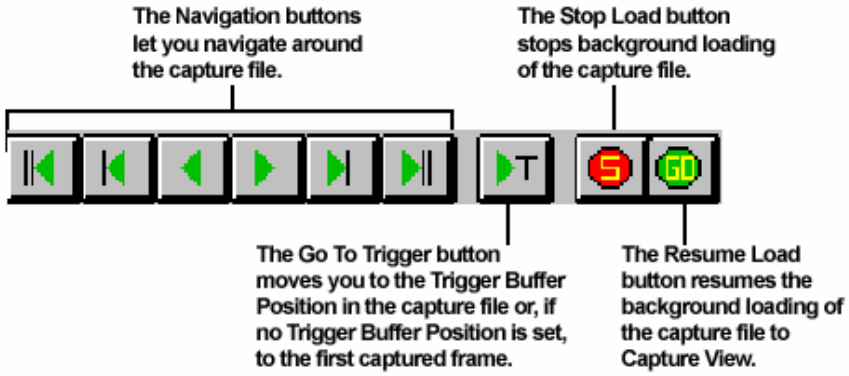


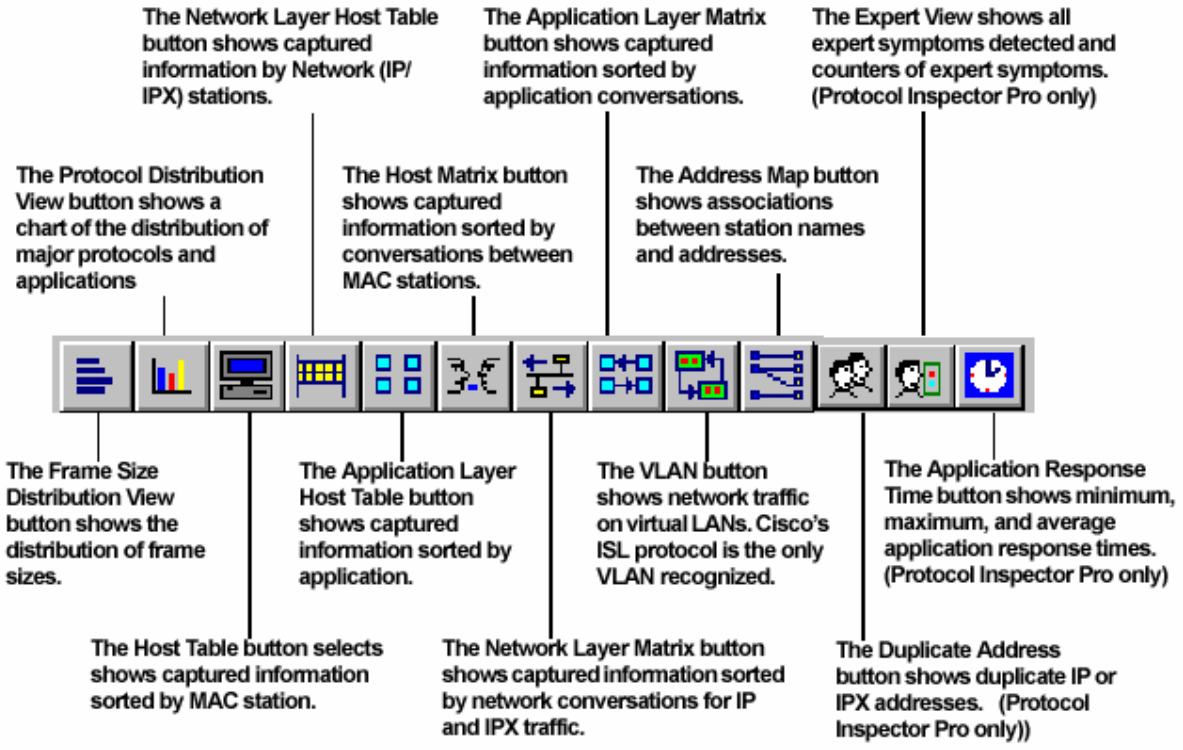
State Toolbar



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