



Version 1.2
User's Guide

DISCLAIMER

ASTECC, Inc. provides this documentation "as is" without warranty of any kind, including, but not limited to, any express or implied merchantability or fitness for a particular purpose.

This documentation is subject to change by ASTEC, Inc. without notice while ASTEC, Inc. has taken all care to ensure this documentation complete and accurate, in no event shall ASTEC, Inc. be liable for errors that may be included in this documentation. Nor, in no event shall ASTEC, Inc. be liable for any direct, indirect, special, incidental, or consequential damages arising out of the offering, function, and use of this documentation.

ASTECC Eyes on the net version 1.2

User's Guide

Manual Version 1.201

Copyright © 2000 - 2003 ASTEC, Inc. All rights reserved.

Last revised: July 1, 2003.

No part of this documentation may be reproduced, stored in retrieval system, or transmitted in any form or by any means, electronic, graphic or mechanical, including photocopying, video recording, taping, or otherwise, without prior written permission of ASTEC, Inc.

Trademarks

ASTECC is a registered servicemark and trademark of ASTEC, Inc. in Japan.

ASTECC Eyes on the net is a trademark of ASTEC, Inc.

ASTECC, Inc. is a subsidiary of ASTEC, Inc.

Windows is a registered trademark of Microsoft Corporation.

Windows NT is a trademark of Microsoft Corporation.

All other product names and company names referenced herein are trademarks or registered trademarks of their respective companies.

ASTECC, Inc.

Itohpia Koishikawaumezu Bldg. 1-3-11 Koishikawa, Bunkyo-ku, Tokyo 112-0002, Japan

TEL: +81-3-5804-1853 FAX: +81-3-5804-1854

Contents

Introduction

About this Manual	1
Typographical Conventions	2

Chapter 1 Install ASTEC Eyes

Confirming the Runtime Environment	3
Installation	5
Overview of Installation	5
Installing Product Edition	5
Installing Evaluation Edition	6
License Registration	6
Invoking ASTEC Eyes	8
Invoking ASTEC Eyes	8
Invoking and Installing a Remote Module as a Windows' Service	8
Uninstallation	10
Uninstalling ASTEC Eyes	10
Uninstalling a Remote Module	10
Protocols Supported by ASTEC Eyes	12
About Product Support	16

Chapter 2 New features in ASTEC Eyes version 1.2

New Features	18
Remote Watching	18

Reporting Expert Events	18
Continuous Capture	19
Enhanced and Improved Features	20
Filters	20
Improvement of User Interface	21
Other Improvements	22
Addition of Supported Protocols	22
Chapter 3 Getting Started with ASTEC Eyes	
Invoking ASTEC Eyes	25
Displaying Network Traffic	28
Selecting a Network Interface	28
Starting Monitoring	30
Displaying Charts	31
Using a Popup Menu on the Monitor Window	34
Displaying the Traffic Breakdown	35
Configuring a Decode Hint	42
Changing the Display Format of the Monitor Window	48
Analyzing Network Packets	52
Capturing Packets	52
Decoding Captured Data	53
Screening Data to Be Displayed	56
Using the Stream View	60
Searching Decoded Results	64
Organizing Windows	66
Using Workspaces	66
Saving a Configuration	70

Using a Remote Module	71
Exiting ASTEC Eyes	73
Chapter 4 Functional Description	
Preparation before Using the Functions	75
Main Window of ASTEC Eyes	75
Selecting an Interface	78
Monitoring	80
Selecting the Target Interface for Monitoring	80
Starting or Pausing Monitoring	80
Opening a Monitor Window	81
Changing the Display Format of the Monitor Window	84
Selecting a Graph Item	86
Using the Popup Menu on the Monitor Window	87
Monitoring Required Data Only	91
MAC and IP Address Tables	91
Saving Monitoring Information	93
Capturing	95
Selecting the Target Network Interface for Capture	95
Starting Capture	95
Pausing Capture	96
Discarding Captured Data	96
Appending Data in the Capture Buffer	96
Saving Captured Data into a File	97
Using the Start Capture Trigger	98
Using the Pause Capture Trigger	98
Capturing Data of Interest Only	99

Continuous Capture	99
Decoding	103
Decoding Data in the Capture Buffer	103
Decoding Data Saved in a File	103
The Decode View	105
Saving Decoded Data into a File	107
Using the Stream View	107
Using Toolbars of the Decode View and the Stream View	110
Key Binds on the Decode View and the Stream View	112
Searching the Decode View or the Stream View for Text	113
Selecting Data Displayed in the Decode or Stream View	113
Displaying Statistics of Decoded Data	121
Decoding Divided Data	122
Saving the Decoded Results	124
Copying the Decoded Results	127
Error in Decoding Data	128
Logging	129
Configuring Logging	129
Displaying Logs	132
Displaying Information on the Network Interface Card	136
Remote Watching	137
Connecting to Remote Modules	137
Actions on a Remote Module	139
Actions on Remote Module Interfaces	142
Reporting Expert Events	146
Configuring Expert Events	147
Displaying Reported Events	149

Configuring Options 151

 Configuring Capture Options 152

 Configuring Decode Hints 153

 Configuring Host Name Preference 156

 Configuring Monitor Options 159

 Configuring Charts Default Options 160

 Configuring Other Options 162

 Saving a Configuration 164

Miscellaneous Functions 167

 Workspace 167

 Window Operation 171

 Filter Editor 172

 Searching Host Names 189

 Editing an Address Book 193

 Printing 204

Index

Introduction

ASTECC Eyes on the net is a network analyzer for measuring network traffic, and collecting and analyzing network packets. By using ASTEC Eyes on the net (hereafter, referred to as ASTEC Eyes), you can prevent network troubles and obtain the information to resolve problems.

About this Manual

This manual describes the following subjects in ASTEC Eyes version 1.2:

- How to install the software
- A tutorial
- Details on each function

Typographical Conventions

This manual uses the following typographical conventions.

Typeface or Symbol **Meaning**

`computer text` Enter text from the keyboard as specified. For example, the instruction

Enter 192.168.0.1.

literally means to input “192.168.0.1”. This font is also used to describe file names, folder names, and values.

italic text

A placeholder you replace with your actual value. For example,

Double-click `SETUP.exe` under *savedir*.

means that you replace part of *savedir* with an actual directory name.

emphasis Emphasizes **emphasis**.

<**Key**> Indicates that you press the corresponding key on the keyboard.

<**Modifier-Key**> Indicates that you press <**Key**> while holding down <**Modifier**>.

Where necessary, remarks like the following example will be shown.



Some types of monitor windows may not display bar or pie charts.



Chapter 1

Install ASTEC Eyes

This chapter describes how to install ASTEC Eyes. First, it describes the runtime environment and then the installation procedure in detail.

Confirming the Runtime Environment

Before starting installation, you should confirm your runtime environment. To install and execute ASTEC Eyes, you need the following environment:

- OS
ASTEC Eyes supports the following operating systems.
 - Windows 98 English Version
 - Windows Me English Version
 - Windows NT 4.0 English Version
with SP3 or later and Internet Explorer 4.01 SP1 or later installed.
 - Windows 2000 English Version
 - Windows XP English Version

The Remote Module of ASTEC Eyes supports the following operating systems.

- Windows NT 4.0 English Version
with SP3 or later and Internet Explorer 4.01 SP1 or later installed.
- Windows 2000 English Version
- Windows XP English Version

- **Computer Type**
ASTEC Eyes supports PC/AT compatible machines with an Intel x86 running any of the above mentioned operating systems.

- **Network Interface Cards**
ASTEC Eyes uses one or more Ethernet network interface cards that are supported by the operating system.
Make sure the followings:
 - At least one network interface card is installed.
 - The TCP/IP protocol is installed.

- Pentium 133 MHz processor or higher (recommended)

- 64 MB or more memory (recommended)

- A monitor capable of displaying 800 × 600 High Color (65536 colors)

- A hard disk with 10 MB or more free space



ASTEC Eyes version 1.2 does not support 16 and 256 color display.



From version 1.2, ASTEC Eyes supports plug and play for network interface cards.

Installation

Overview of Installation

To install ASTEC Eyes onto Windows NT 4.0, Windows 2000, or Windows XP, you need Administrator privileges.

You can install ASTEC Eyes from the following drives.

- CD-ROM drive
- Network drive

If your PC (Personal Computer) does not have a CD-ROM drive, you can install ASTEC Eyes from another PC's CD-ROM drive as a network drive.

After the installation, you need to register the license key.

Installing Product Edition

First, insert the CD into the CD-ROM drive. If you are going to install from a network drive, connect to the drive into which you inserted the CD.

Start the setup program either by following:

- Double-clicking `SETUP.exe` in the CD-ROM or the network drive in Explorer, or
- Executing the program specifying its file name:
 1. From the **Start** menu, choose **R**un.
 2. Enter the following text into the **O**pen box.

Case	String to be entered
If you install from CD-ROM (D:)	D:\SETUP.exe
If you install from network drive (N:)	N:\SETUP.exe

3. Click the **OK** button.

Once the setup program has started, go through the installation procedure following the instructions displayed on the screen. You will be prompted to select either entire ASTEC Eyes or its Remote Module only for installation.

Typically, you want to select entire ASTEC Eyes. If you purchased a license of the Remote Module and want to install it, select Remote Module.

Installing Evaluation Edition

Start the setup program using either of the following:

- Double-click the downloaded `EYES_EVL.exe` in Explorer.
- Execute the program by specifying its file name.
 1. From the **Start** menu, choose **R**un.
 2. If you saved the evaluation copy in the *TEMP* directory of the C drive, enter the following text into the **O**pen box.

```
C:\TEMP\EYES_EVL.exe
```

3. Click the **OK** button.

Once the setup program has started, go through the installation procedure by following the instructions displayed on the screen.

License Registration

Please register your name as user of the software through the website;

```
http://www.asteceyes.com/ENGLISH/REGISTRATION/
```

or fill the license information in the Product Registration Form in README.txt file and send it to ASTEC by E-mail (support@asteceyes.com).

We will then send you the registration information and the license key by **E-mail**.

After receiving the E-mail, you can register the license key.

License Key Registration for Stand-Alone and Evaluation Editions

1. Save the `eyes_license.txt` file attached to the E-mail in an appropriate directory. Here, we assume it to be *savedir*.
2. From the **Start** menu, choose **R**un, enter the following text into the **O**pen box,

```
regedit savedir\eyes_license.txt
```

and click the **OK** button.

3. With Windows 98, Windows Me, Windows 2000, and Windows XP, a dialog box similar to Figure 1-1 will appear. Click the Yes button.

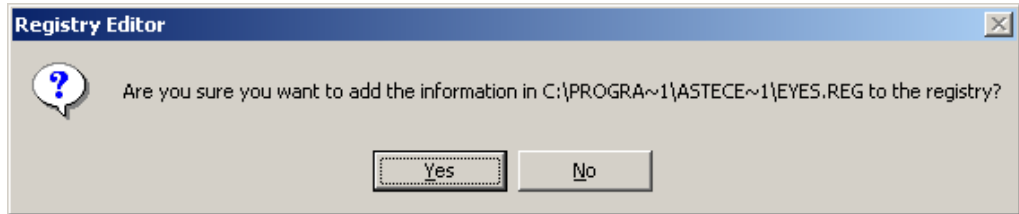


Figure 1-1 Registry Editor dialog box

The license key will be added into the registry.

This completes the whole registration process for the stand-alone license.

Network License Key Registration

This section is only for those customers who purchased a Remote Module.

In order to run a Remote Module, you must register **the same** license key on the PC that invokes ASTEC Eyes, and **all of the PCs you want to install the Remote Module**. If the license keys for ASTEC Eyes and its Remote Module differ, you cannot connect ASTEC Eyes to the Remote Module.

The registration procedure for network licensing is identical to that of stand-alone licensing.

Invoking ASTEC Eyes

Invoking ASTEC Eyes

To invoke ASTEC Eyes, open the **Start** menu and choose **Programs** (for Windows XP, **All Programs**), **ASTEC Eyes**, and **ASTEC Eyes**.



If you are using Windows NT 4.0, Windows 2000, or Windows XP, you need Administrator privileges.

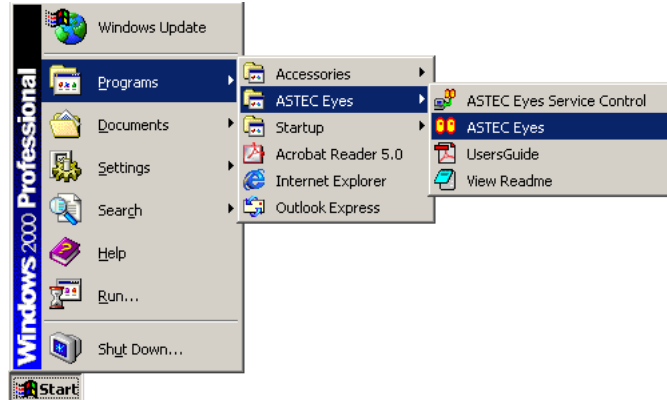


Figure 1-2 Invoking ASTEC Eyes from the **Start** menu

Invoking and Installing a Remote Module as a Windows' Service

To invoke the Remote Module, open the **Start** menu and choose **Programs** (for Windows XP, **All Programs**), **ASTEC Eyes**, and **ASTEC Eyes Service Control**.

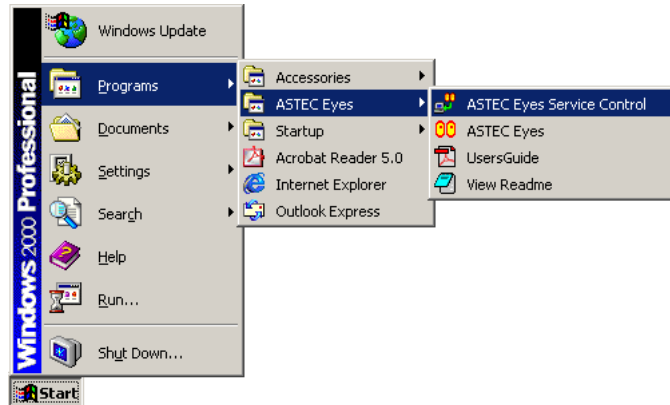


Figure 1-3 Invoking ASTEC Eyes Service Control from the **Start** menu



In order to invoke a Remote Module, you need Administrator privileges. The Remote Module of ASTEC Eyes version 1.2 does not support Windows 98 and Windows Me.

A window similar to the following figure will appear.

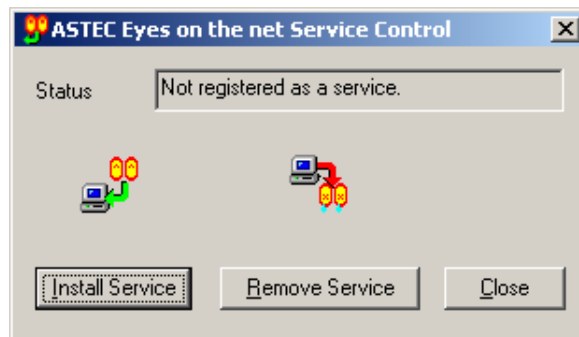


Figure 1-4 ASTEC Eyes on the net Service Control

Click the **I**nstall Service button.

Make sure that **S**tatus has been changed to "Monitoring".

Click the **C**lose button to close the window.

Uninstallation

If you are writing a log file, you must stop the logging **before uninstalling ASTEC Eyes**. To do so, go through the following steps:

1. Invoke ASTEC Eyes.
2. To stop the logging of the Remote Module, connect ASTEC Eyes to the host the Remote Module is running on.
3. In the Interface Selector window, click on the icon or label of the host making the log with the right mouse button.
The popup menu for the host will appear.
4. Choose **Properties** from the popup menu.
The **Host Properties** dialog box will appear.
5. Click on the **Log** tab in the **Host Properties** dialog box.
The **Log** page will be shown.
6. Clear the **Output** check box in the **Log** region.
7. Click the **OK** button to close the dialog box.
8. Exit ASTEC Eyes.

Uninstalling ASTEC Eyes

The steps to uninstall ASTEC Eyes are:

1. Open the **Start** menu and choose **Settings**, and **Control Panel**.
For Windows XP, open the **Start** menu and choose **Control Panel**.
2. Double-click the **Add/Remove Programs** icon (for Windows XP, the **Add or Remove Programs** icon) in the Control Panel.
3. Select **ASTEC Eyes on the net**, and click the **Add/Remove** button (for Windows 2000 and Windows XP, the **Change/Remove** button).

Uninstalling a Remote Module

To uninstall a Remote Module, first stop the service, open the **Start** menu, and choose **Programs** (for Windows XP, **All Programs**), **ASTEC Eyes**, and **ASTEC Eyes Service Control**.

A window similar to the following figure will appear.

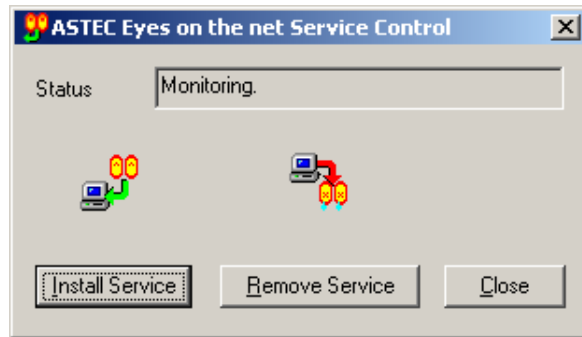


Figure 1-5 ASTEC Eyes on the net Service Control

Click the **R**emove Service button.

Make sure that **S**tatus has been changed to “Not registered as a service”.

Click the **C**lose button to close the window.

After removing the service, uninstall the Remote Module by **A**dd/**R**emove Programs (for Windows XP, **A**dd or **R**emove Programs) in the Control Panel. The steps are as follows:

1. Open the **S**tart menu and choose **S**ettings, and **C**ontrol Panel.
For Windows XP, open the **S**tart menu and choose **C**ontrol Panel.
2. Double-click the **A**dd/**R**emove Programs icon (for Windows XP, the **A**dd or **R**emove Programs icon) in the Control Panel.
3. Select **A**STEC **E**yes **o**n **t**he **n**et, and click the **A**dd/**R**emove button (for Windows 2000 and Windows XP, the **C**hange/**R**emove button).

Protocols Supported by ASTEC Eyes

The protocols that ASTEC Eyes version 1.2 supports are listed below.

- AARP (AppleTalk Address Resolution Protocol)
- ACL3 (ACL network protocol version 3)
- AEP (AppleTalk Echo Protocol)
- AFP (AppleTalk Filing Protocol)
- ARP (Address Resolution Protocol)
- ASP (AppleTalk Session Protocol)
- ATP (AppleTalk Transaction Protocol)
- BB (Big Brother Protocol)
- BPDU (Bridge Protocol Data Unit)
- CDP (Cisco Discovery Protocol)
- CIFSP (SMB) (Common Internet File System Protocol)
- CVSPSERVER (CVS PSERVER)
- DCE RPC (DCE Remote Procedure Call Protocol)
- DDP (AppleTalk Datagram Delivery Protocol)
- DHCP (Dynamic Host Configuration Protocol)
- DLC (Data Link Control)
- DNS (The Domain Name System)
- DSI (Data Stream Interface (for AFP over TCP))
- ECHO (Echo Protocol)
- EYESP (ASTEC Eyes Protocol)
- FINGER (Finger Protocol)
- FTP (File Transfer Protocol)
- H323GATESTAT (H323 Call Signalling Protocol)
- H323HOSTCALL (H323 RAS Message Protocol)
- HTTP (Hypertext Transfer Protocol)
- HTTPS (HTTP Protocol over TLS/SSL)
- ICMP (Internet Control Message Protocol)
- ICMPv6 (Internet Control Message Protocol for IPv6)

- IDENT (Identification Protocol)
- IGMP (Internet Group Management Protocol)
- IMAP4 (Internet Message Access Protocol (Version 4))
- IPX (Internetwork Packet Exchange)
- IPv4 (Internet Protocol Version 4)
- IPv6 (Internet Protocol Version 6)
- ISO-TP0 (ISO Transport Class 0 Protocol)
- LDAP (Lightweight Directory Access Protocol)
- LLC (Logical Link Control (IEEE 802.2))
- LPDP (Line Printer Daemon Protocol)
- MOUNTP (Mount Protocol Version 1)
- MOUNTP3 (Mount Protocol Version 3)
- NBP (AppleTalk Name Binding Protocol)
- NCP (NetWare Core Protocol)
- NFS v2 (NFS Version 2 Protocol)
- NFS v3 (NFS Version 3 Protocol)
- NetBIOS-DGM (NetBIOS Datagram Service)
- NetBIOS-DM (NetBIOS Diagnostic and Monitoring)
- NetBIOS-NM (NetBIOS Name Management)
- NetBIOS-NS (NetBIOS Name Service)
- NetBIOS-SM (NetBIOS Session Management)
- NetBIOS-UD (NetBIOS User Datagram)
- NetBIOS-SSN (NetBIOS Session Service)
- NICNAME (Who Is Protocol)
- NIS (Network Information Service Version 2)
- NLM (Network Lock Manager Protocol)
- NMPI (Name Management Protocol on IPX)
- NNTP (Network News Transfer Protocol)
- NTALK (Ntalk Protocol)
- NTP (Network Time Protocol (Version 3))
- NWDP (Netware WatchDog Protocol)

- NWNB (Novell NetBIOS)
- OSPF (Open Shortest Path First Protocol)
- POP3 (Post Office Protocol (Version 3))
- PORTMAPPER (Binding Protocols Version 2 for ONC RPC Version 2)
- RADIUS (Remote Authentication Dial In User Service)
- RADIUS-ACC (Remote Authentication Dial In User Service Accounting)
- RARP (Reverse Address Resolution Protocol)
- REXEC (Remote Execution Protocol)
- RIP (Routing Information Protocol)
- RIPX (Routing Information Protocol for IPX)
- RIPng (Routing Information Protocol for IPv6)
- RLOGIN (BSD Rlogin)
- RPCBIND3 (Binding Protocols Version 3 for ONC RPC Version 2)
- RSH (Remote Shell Protocol)
- RTMP (AppleTalk Routing Table Maintenance Protocol)
- RTP (Transport Protocol for Real Time Application)
- SAP (Service Advertising Protocol)
- SMTP (Simple Mail Transfer Protocol)
- SNMP (Simple Network Management Protocol)
- SOCKS (SOCKS Protocol)
- SSH (SSH Remote Login Protocol)
- SUNRPC (Sun Remote Procedure Call, Version 2)
- SVRLOC (Service Location Protocol)
- SYSLOG (System Log Protocol)
- TALK (Talk Protocol)
- TCP (Transmission Control Protocol)
- TELNET (TELNET Protocol)
- TFTP (Trivial File Transfer Protocol)
- TSP (Time Synchronization Protocol)
- UDP (User Datagram Protocol)
- VARP (VINES Address Resolution Protocol)

- VIP (VINES Internet Protocol)
- VLAN (Virtual Bridged Local Area Network Protocol (IEEE 802.1Q))
- WHO (WHO Protocol)
- WNN6 (Wnn6 Protocol)
- X (X Protocol)
- XDMCP (X Display Manager Control Protocol)
- XFSP (X Font Service Protocol)
- ZIP (AppleTalk Zone Information Protocol)



For CVSPSERVER and NICNAME, only monitoring is available.



For the protocols not supported by ASTEC Eyes, “Unknown (TCP/UCP) Protocol” will be used for the protocol name.

“Unknown TCP Protocol” indicates the traffic of unsupported application protocols above the TCP layer.

“Unknown UDP Protocol” indicates the traffic of unsupported application protocols above the UDP layer.

“Unknown Protocol” indicates the traffic of those packets whose value in the protocol field of the IP header has not been registered in ASTEC Eyes.

About Product Support

If you have any questions, please contact our support section listed below by fax or E-mail.

FAX: +81-3-5804-1856

E-mail: support@asteceyes.com


Chapter **2**

New Features in ASTEC Eyes version 1.2

This chapter describes new features and improvements in ASTEC Eyes version 1.2.

New Features

In ASTEC Eyes version 1.2, the following new features have been added:

- Remote watching
- Reporting expert events
- Continuous capture

A description of each feature follows.

Remote Watching

ASTEC Eyes version 1.0 could monitor only the networks local to the PC with ASTEC Eyes installed.

ASTEC Eyes version 1.2 can now monitor remote networks using **Remote Modules** installed into remote PCs.

A Remote Module can collect the same information as ASTEC Eyes can. You can monitor the information collected by more than one Remote Module from your local PC. Conversely, you can also monitor the information collected by one Remote Module from more than one PC.

To enable those functions, you only need to install a Remote Module into a PC in each local network and to connect ASTEC Eyes to the Remote Module interactively using a popup menu.

The ASTEC Eyes also has the Remote Module functionality. It is therefore possible to connect ASTEC Eyes to other ASTEC Eyes installed on other PCs as Remote Modules.

Reporting Expert Events

This is the feature to monitor and detect symptoms of network troubles and issue notification messages. ASTEC Eyes can identify the following network events:

- Continuous high traffic
- Duplicate IP addresses
- Frequent TCP retransmissions
- TCP buffers full for a long time (frozen window)

- Late acknowledgements in TCP transmission (late ack)

If any abnormality is observed, the messages will be displayed in the event viewer window.

Continuous Capture

In the previous version, captured data were preserved in the internal buffer of ASTEC Eyes. For that reason, it was impossible to capture data continuously for a long period.

The new version can also store captured data directly on to a disk.

Enhanced and Improved Features

This section describes improvements and enhancements of features in ASTEC Eyes version 1.2.

Filters

Enhancement of Convenience Filter

The interactive convenience filter, which characterizes ASTEC Eyes, has been enhanced and made easier to use.

When analyzing network data and displaying the results, the convenience filter allows the user to screen packets or records easily by interactive operations, without specifying logical expressions.

The “convenience filter” in ASTEC Eyes version 1.0 has been renamed “caption filter”. A new filter named “header attribute filter” has been added. In ASTEC Eyes version 1.2, the caption filter and header attribute filter are generically called the convenience filters.

With the former “convenience filter”, you selected from the values to be matched in the pull-down menu for each column of the decode or stream view.

In addition, you can use string values more conveniently using the new caption filter:

- Displaying those packets or records matching one of the specified strings.
- Displaying those packets or records that do not match any of the specified strings.
- Displaying packets or records specified a range of the value.

The new **header attribute filter** selects the packets by the attributes, which may not be shown in the Summary pane. As shown below, the attribute used here are those used to classify the monitored traffic.

- MAC layer source address
- MAC layer destination address
- MAC layer host pair
- MAC layer protocol
- IP layer source address

- IP layer destination address
- IP layer host pair
- IP layer protocol

As with the former “convenience filter”, you can apply filters to multiple columns and combine them with logical AND operation. In addition, you can use the logical OR operation by the **(Enable Check Marks)** of the new convenience filter.

Filter Editor

To use the display filter, capture filter, and monitor filter effectively, you want to define logical expressions. Editing logical expressions is far easier, with the new and enhanced filter editor, which has the following characteristics:

- You can now set conditions by choosing from the list of candidate values, without typing those values.
- You can now copy, paste, drag and drop for logical expressions shown as tree.

New Monitor Filter

The monitor filter for screening the monitored information has also been renewed.

In the former versions, monitor filters were applied when collecting statistics. In this version, the filters are applied when displaying statistics. Consequently, statistics are not lost when the filters are applied. Thus, you can specify different filter conditions on the same statistics, and analyze the traffic from various viewpoints.

Improvement of User Interface

The following improvements have been made to the user interface:

- Even if many items are shown in the legend, the chart and the legend are both kept visible.
The legend area no longer grows too large and hides the chart.
- Now you can bind a workspace to a particular network interface.
If you select the workspace bound to an interface, the interface will also be selected.
- You can now display the statistics of the captured data in the same way as those of the monitored traffic are shown. By clicking a button on the toolbar of the decode view, you can show the statistics of the decoded captured data as a chart or a table.

- Finding host names during monitoring has been added.
- You can now edit the user defined name for a host with the editor of ASTEC Eyes.
- You can now write the result of decoding into a text file, as shown in the decode or stream view (CSV format is also supported).

Other Improvements

- Support for tcpdump and snoop data
The capture files of tcpdump and snoop, tools frequently used on UNIX, can now be loaded and decoded.
- Faster decoding
The decoding process of captured data has been made faster. Compared to the previous version, the time required for decoding packet data was decreased by half, and the time for displaying the stream view to one third.
- Decoding the divided data
Because of the memory limitations, with former versions it was difficult to decode data stored in a very large file. With the new version, you can decode data in a large file created by tools other than ASTEC Eyes (for example, tcpdump), by dividing it into smaller parts. You can specify the range of the file to be decoded by time or packet header attributes.
- Plug and play for network interface cards is now supported.

Addition of Supported Protocols

The following protocols are now monitored and decoded:

- BB (Big Brother Protocol)
- CDP (Cisco Discovery Protocol)
- DCE RPC (DCE Remote Procedure Call Protocol)
- FINGER (Finger Protocol)
- H263 (Video Coding for Low Bit Rate Communication)
- H323GATESTAT (H323 Call Signalling Protocol)
- H323HOSTCALL (H323 RAS Message Protocol)
- HTTPS (HTTP Protocol over TLS/SSL)
- ICMPv6 (Internet Control Message Protocol for IPv6)

- IDENT (Identification Protocol)
- IPv6 (Internet Protocol Version 6)
- ISO-TP0 (ISO Transport Class 0 Protocol)
- LDAP (Lightweight Directory Access Protocol)
- NICNAME (Who Is Protocol)
- NLM (Network Lock Manager Protocol)
- NTALK (Ntalk Protocol)
- OSPF (Open Shortest Path First Protocol)
- RADIUS (Remote Authentication Dial In User Service)
- RADIUS-ACC (Remote Authentication Dial In User Service Accounting)
- RIPng (Routing Information Protocol for IPv6)
- RTMP (AppleTalk Routing Table Maintenance Protocol)
- RTP (Transport Protocol for Real Time Application)
- SSH (SSH Remote Login Protocol)
- SYSLOG (System Log Protocol)
- TALK (Talk Protocol)
- VARP (VINES Address Resolution Protocol)
- VIP (VINES Internet Protocol)
- VLAN (Virtual Bridged Local Area Network Protocol (IEEE 802.1Q))
- WNN6 (Wnn6 Protocol)
- X224TPDU (X.224 Connection-mode Transport Service Protocol)



For NICNAME, only monitoring is available.


Chapter 3

Getting Started with ASTEC Eyes

ASTEC Eyes is the tool for monitoring network status to prevent network troubles, and obtaining the information to resolve network problem. For that, it has functionalities to monitor networks and collect/analyze packets flowing in there.

This chapter is a tutorial on the basic functions of ASTEC Eyes.

Invoking ASTEC Eyes

First, let's invoke ASTEC Eyes.

To invoke ASTEC Eyes, open the **Start** menu and choose **Programs**, **ASTEC Eyes**, and **ASTEC Eyes**. For Windows XP, open the **Start** menu and choose **All Programs**, **ASTEC Eyes**, and **ASTEC Eyes**.



If you are running the software on Windows NT 4.0, Windows 2000, or Windows XP, you need Administrator privileges.

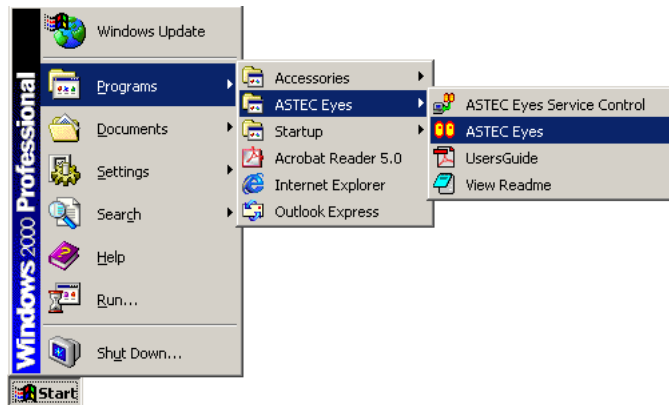


Figure 3-1 Invoking ASTEC Eyes from **Start** menu

When ASTEC Eyes is up, a window similar to the following figure will appear on the screen.

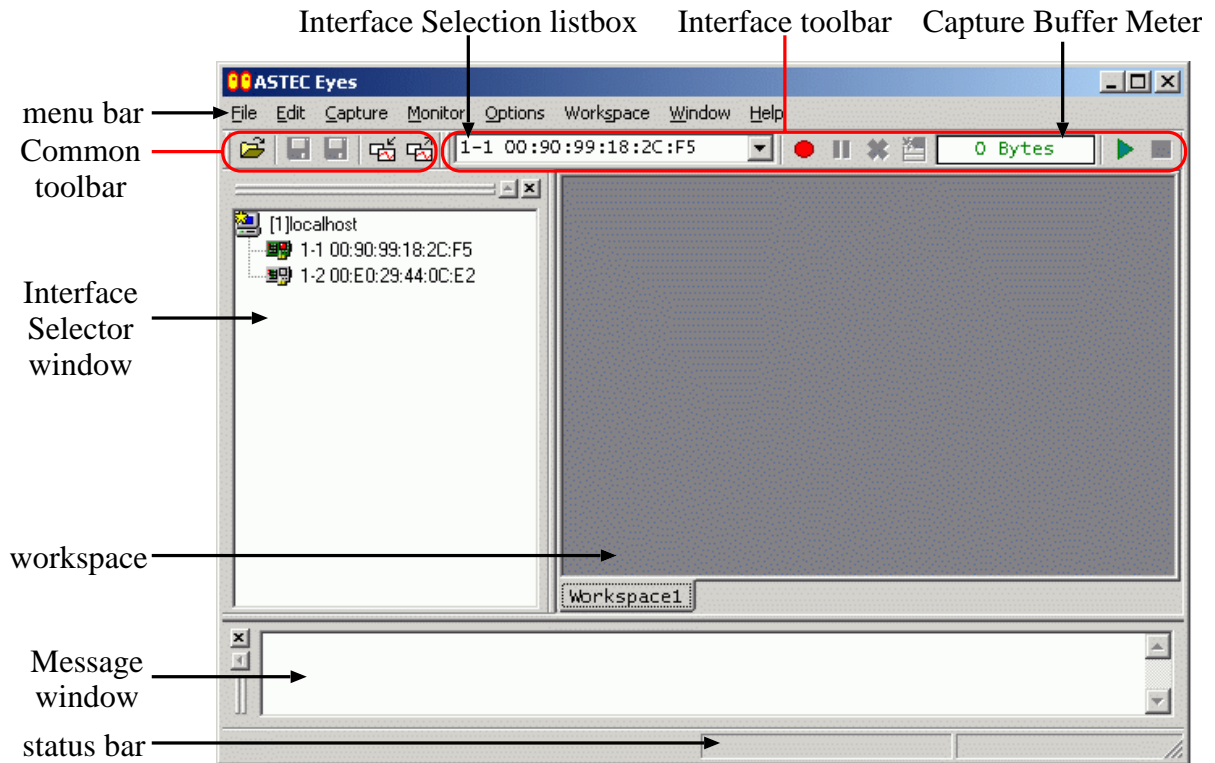


Figure 3-2 Main window

The Main window of ASTEC Eyes is composed of the following components.

- menu bar
- Common toolbar
- Interface toolbar
- workspaces
- Interface Selector window
- Message window
- status bar

You can make visible or invisible the Common toolbar, Interface toolbar, the Interface Selector window, the Message window, and the status bar using the **Options** menu. The Message window is not visible by default.

Windows other than dialog boxes, such as the Monitor window for displaying network traffic statistics and the decode view for the decoded and analyzed network data, will appear in a workspace. You can create more than one workspace. By adding or deleting workspaces and moving windows among workspaces, you can organize the entire screen so that it is meaningful and easier to see.

For more information about the Main window, see “Main Window of ASTEC Eyes” on page 75.

For more information about the workspaces, see “Workspace” on page 167.

Displaying Network Traffic

Traffic means the data volume that flows through a network. In order to detect unusual events as they occur, it is important that you understand your network traffic in its ordinary state.

To display network traffic, you use **monitoring**. Select the network interface to be monitored before you start monitoring.

Selecting a Network Interface

If multiple network interface cards (NIC) are installed in your PC, you need to select the network interface to be monitored.



To select the network interface, you use the Interface Selector window. In the Interface Selector window, the host and network interface cards installed in each host are displayed. The icon for a selected interface is  (green) and the icon for a non-selected interface is  (gray).

Figure 3-3 shows that the localhost (the PC with ASTEC Eyes installed) has two interface cards installed.

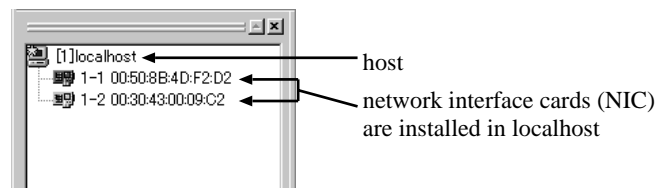




Figure 3-3 Interface Selector window

When the  mark is overlaid with the icon of a host or an interface, it means that it is not available.

Click on the icon or label for the interface you want to display the traffic. Make sure that the icon changes from  (gray) to  (green).



You can also select a network interface by using the Interface Selection listbox () in the Main window.

Changing the Interface Label

Next, let's change the label of the interface to the one easier to understand. The label for an interface includes a MAC address by default. Generally, it is not easy to remember a MAC address. It may be more convenient if you change the label of the interface to one that is easier, since it will be used at various places, such as in the title of the Monitor window.

Double-click on the icon or label of the interface displayed in the Interface Selector window. The **Interface Properties** dialog box will appear as shown in Figure 3-4.

In the dialog box, in addition to the label, other information about the network interface card such as MAC address, maximum frame size, link speed, vendor ID, etc. is displayed.

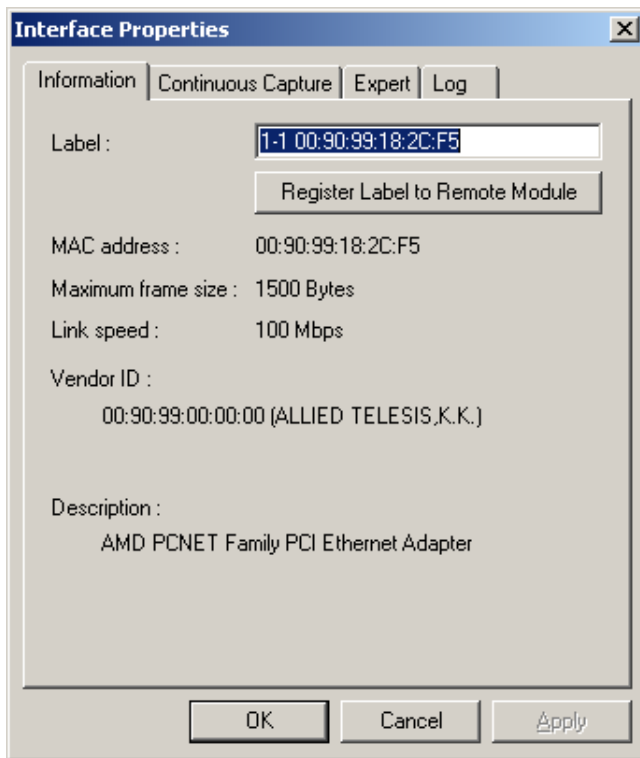


Figure 3-4 **Interface Properties** dialog box

Enter “Example interface” into the Label input field, and click the **OK** button. Make sure that the label displayed in the Interface Selector window has been changed.



From ASTEC Eyes version 1.2, a new feature has been added for watching the remote networks using Remote Modules on remote PCs. If you connect ASTEC Eyes to a PC with the Remote Module installed, its host name and the network interfaces will appear in the Interface Selector window. For a complete discussion of remote watching, see “Remote Watching” on page 137.

Starting Monitoring

To display the network traffic, use monitoring. With this feature, you can measure the network traffic, as well as displaying and analyzing various statistics.

To start monitoring, click the **Start Monitor** button () on the Interface toolbar.

Nothing is shown right away. You need to choose the traffic charts to be displayed.

Displaying Charts

ASTEY Eyes can display MAC (Media Access Control) and IP (Internet Protocol) layer traffic.

Let's try to see the IP layer entire traffic first and then traffic by protocol.

First, choose **6 IP Traffic** from the **Monitor** menu on the menu bar of the Main window.

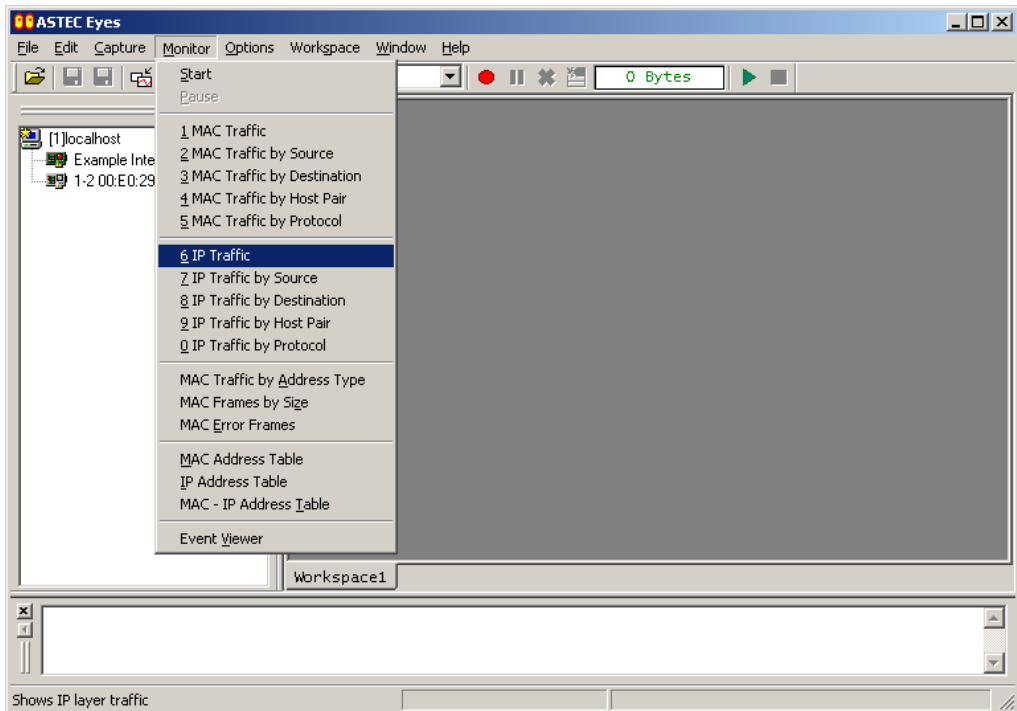


Figure 3-5 Choosing IP Traffic

The Monitor window of “IP Traffic” will appear as shown in Figure 3-6. A line chart showing the history of last five minutes is displayed.

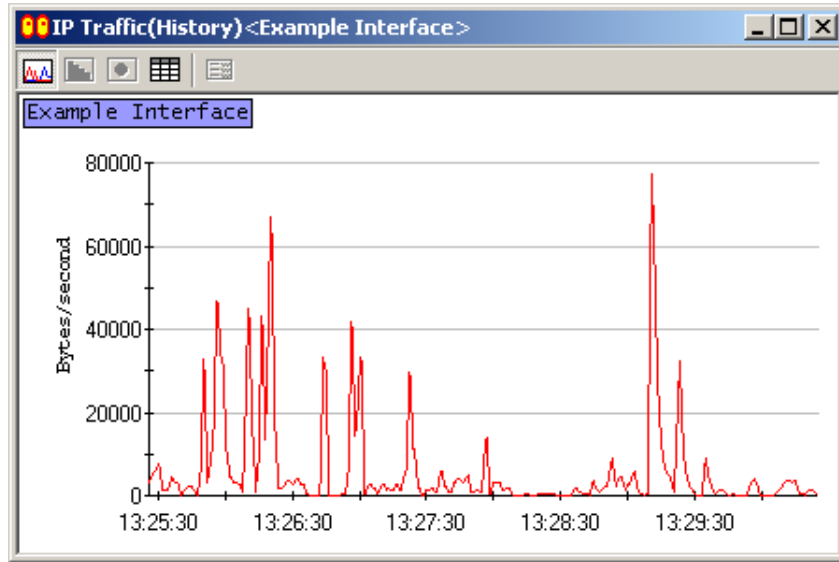


Figure 3-6 Monitor window of “IP Traffic”

Next, let's display the Monitor window of "IP Traffic by Protocol". Choose **0 IP Traffic by Protocol** from the **Monitor** menu on the menu bar of the Main window.

This time, the Monitor window of "IP Traffic by Protocol" will appear as shown in Figure 3-7. A line chart showing the IP layer traffic classified by protocol is displayed.

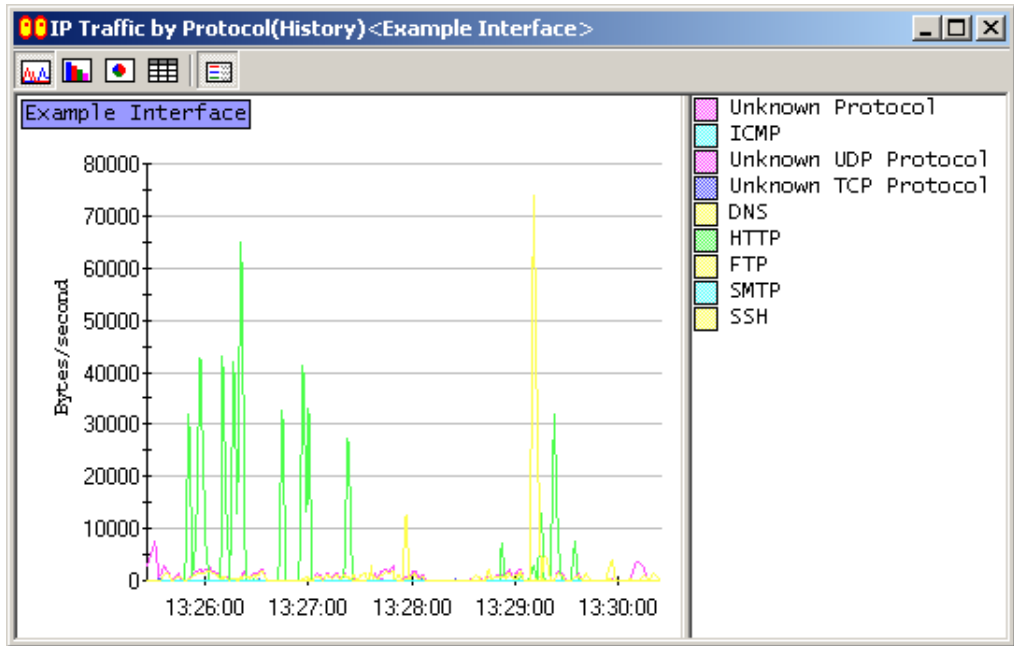


Figure 3-7 Monitor window of "IP Traffic by Protocol"

In these charts in the Monitor window, the traffic is measured and displayed in bytes (octets) per second by default.



The newly opened Monitor window displays the traffic of the currently selected network interface. ASTEC Eyes can monitor the traffic of multiple network interfaces at the same time. If you want to monitor another network interface, select the network interface, start monitoring, and then display the charts.



A Monitor window displays a line chart by default. Depending upon the type of Monitor window, you can choose from bar chart, pie chart, and detailed table format. For more information, see “Changing the Display Format of the Monitor Window” on page 48.



For a complete discussion of the type of Monitor window, see “Opening a Monitor Window” on page 82.

Using a Popup Menu on the Monitor Window

ASTEC Eyes provides popup menus for interactively displaying the information you need. Let’s try a popup menu. Click on the Monitor window of “IP Traffic by Protocol” with the right mouse button. A popup menu will appear as shown in Figure 3-8.

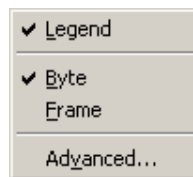


Figure 3-8 Popup menu when line chart is displayed

If you choose **Frame**, the chart is configured to show the traffic measured in number of Ethernet frames per second, as shown in Figure 3-9.

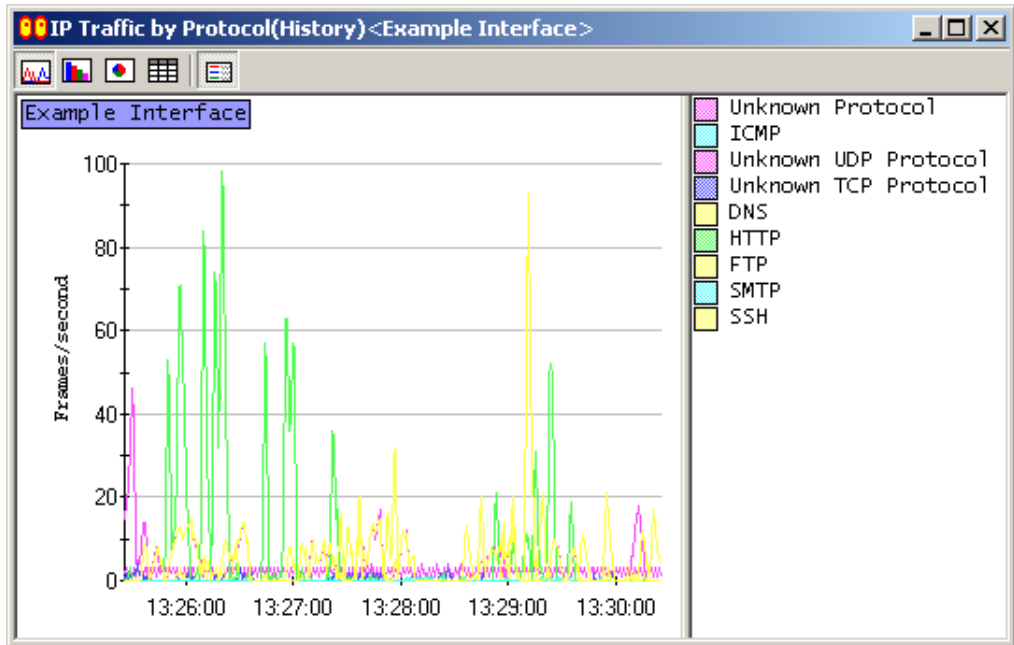


Figure 3-9 Monitor window measured in number of frames per second

To revert to the chart in bytes per second, display the popup menu again and choose **Byte**.

Choosing **Legend** toggles the state of the legend between shown and hidden.



The items of the popup menu on the Monitor window differ depending on the type of Monitor window and the format of the data shown. For further information, see “Using the Popup Menu on the Monitor Window” on page 87.

Displaying the Traffic Breakdown

When you look at a chart showing the traffic by protocol, you might want to see the breakdown to know what host pairs are involved. Conversely, when you look at a chart showing the traffic by host pair, you might want to see the breakdown to know what protocols are used.

ASTEC Eyes allows the user to display the traffic breakdown easily and interactively

using a popup menu.

Here, let's select a Graph Item from the Monitor window of "IP Traffic by Protocol", and see what host pairs are involved. A Graph Item is the element of a line chart, bar chart, or pie chart.

Selecting a Graph Item

To display the breakdown of the traffic, first select a Graph Item.

You can select a Graph Item in two ways:

- Click on the Graph Item in the chart directly with the left mouse button.
- Show the legend, and click on the item corresponding to the Graph Item.



To select the Graph Item of a line chart, it is recommended to click around the vertices rather than clicking on the line segments.



The selected item in the legend can be changed using the up or down arrow keys (<↑>, <↓>). This key operation also selects the corresponding Graph Item.



ASTEC Eyes version 1.2 allows only one Graph Item to be selected at a time .

When you select a Graph Item, its name will be shown in the status bar of the Main window. If you select a Graph Item directly in the chart, the tooltip showing the Graph Item name will also appear. If you move the mouse, it will disappear.

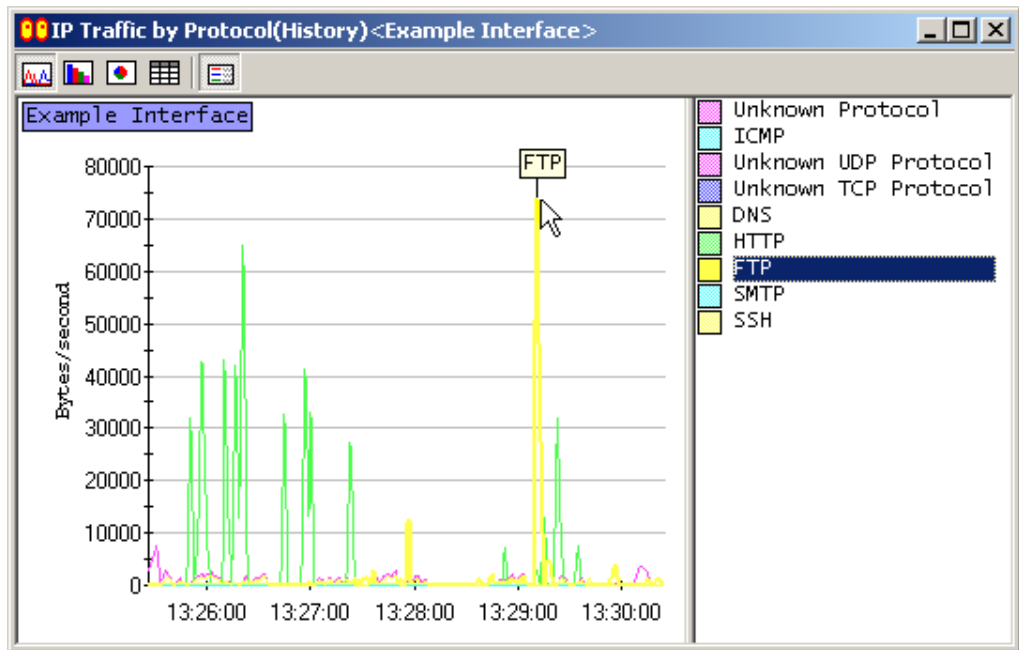


Figure 3-10 Status of chart when FTP selected

Displaying the Breakdown of a Graph Item

You can display a popup menu as shown in Figure 3-11, using right click on the Monitor window, with a Graph Item selected. Note it has more items than the one in Figure 3-8.

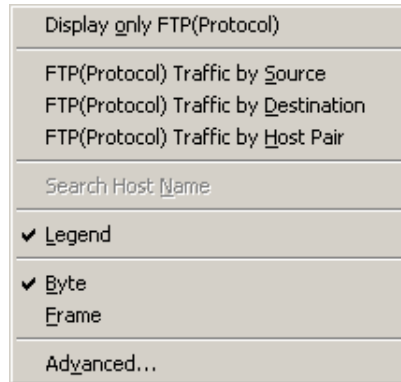


Figure 3-11 Popup menu when a Graph Item is selected

Choose **FTP(protocol) Traffic by Host Pair** as an example. You will see that the chart is switched to the one for the FTP traffic by host pair, as shown in Figure 3-12.

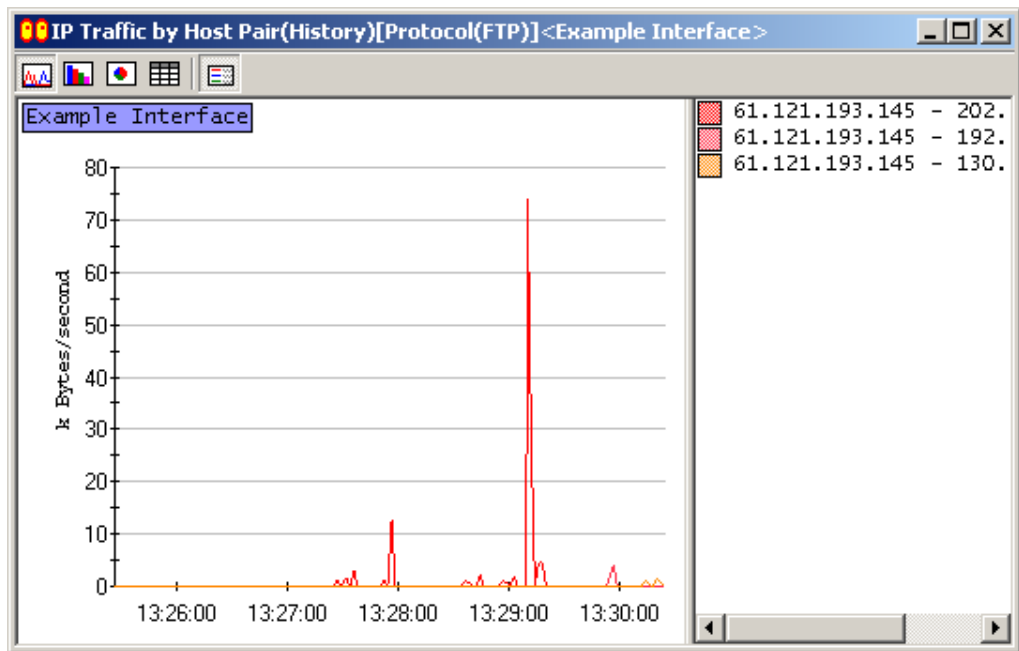


Figure 3-12 Breakdown of traffic by host pair for selected FTP protocol

Searching Host Names Corresponding to an IP Address

If you look at the legend in Figure 3-12, you will notice that IP addresses are used to identify the hosts. You might want to use host names rather than IP addresses.

ASTEY Eyes can search DNS (Domain Name System), NetBIOS (NetBIOS over TCP/UDP, NBT), and NIS (Network Information Service) names corresponding to an IP address.

Choose **Search Host Name...** from the **File** menu on the menu bar of the Main window. The **Searching for Host Name** dialog box will appear, as shown in Figure 3-13.

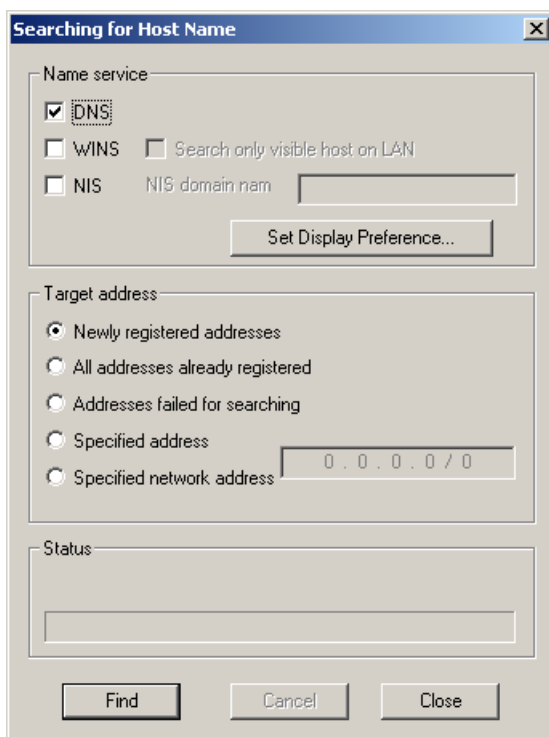


Figure 3-13 Searching for Host Name dialog box

Specify the name services to query host names in the **Name service** region. You can specify **DNS**, **WINS** (Windows Internet Naming Service, NetBIOS name service on IP), and **NIS**.

If you select NIS, you need to enter its domain name as well. If you do not know it, please ask your system administrator.



You can specify more than one name service.

In this example, we are specifying DNS and WINS.

Specify the type of addresses to be searched in the **Target address** region. In this example, select “Newly registered addresses”.

Click the **Search** button to start the search. Figure 3-14 shows the **Searching for Host Name** dialog box while the search is in progress.

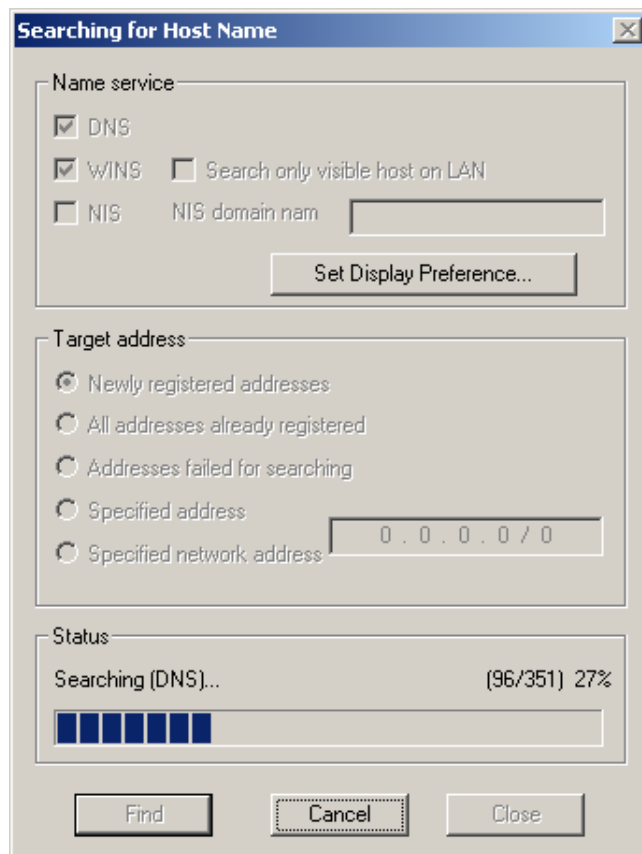


Figure 3-14 Searching for Host Name dialog box while the search is in progress

If you want to stop the search, click the **Cancel** button.

If the host names are found, the content of the legend changes as shown in Figure 3-15. Compare it to Figure 3-12 to see what has been changed.

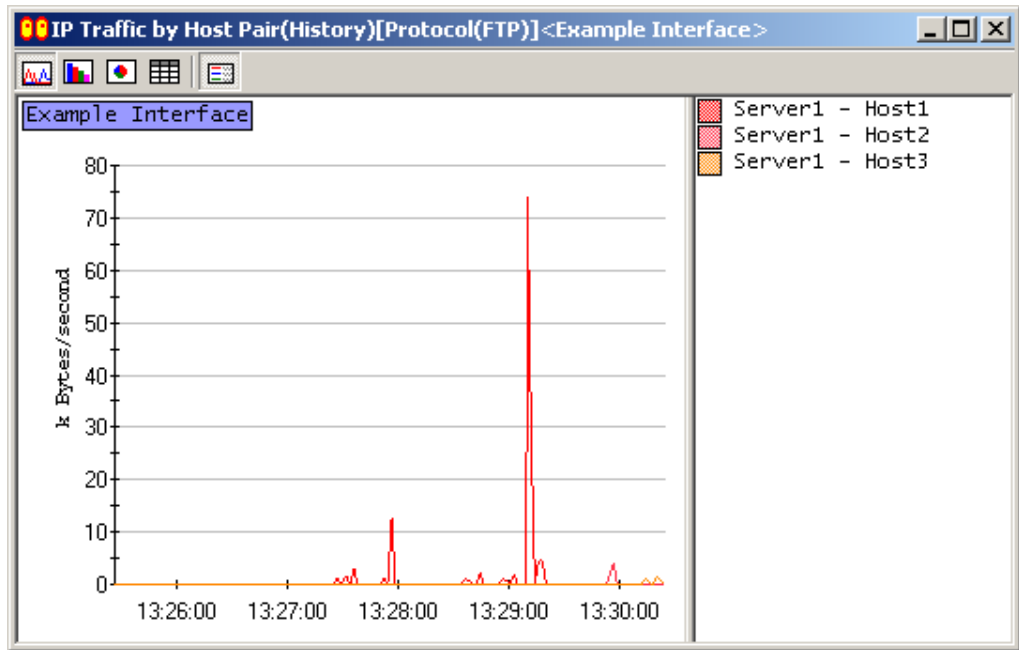


Figure 3-15 Monitor window for “IP Traffic by Host Pair” with hosts shown by name



If you search using the **Searching for Host Name** dialog box, ASTEC Eyes will actively transmit packets into the network. Therefore, network traffic increases.

When the search process ends, click the **C**lose button to close the **Searching for Host Name** dialog box.



From the chart of Figure 3-15, you can further display the breakdown of “traffic of specific host pair that uses FTP protocol”, by selecting Graph Item. You will get the breakdown by source or destination, which effectively shows the direction of the FTP traffic between the pair.

Reverting to the Previous Chart

We will revert to the previous “IP Traffic by Protocol” chart.

Click on the chart showing the breakdown with the right mouse button. A popup menu will appear, which contains a menu item named **Revert**. If you choose this item, the chart will revert to the previous “IP Traffic by Protocol” (see Figure 3-7).

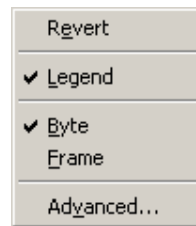


Figure 3-16 Popup menu containing menu item **Revert**

Configuring a Decode Hint

In the Monitor window of “IP Traffic by Protocol”, sometimes the Graph Item labeled “Unknown TCP Protocol”, “Unknown UDP Protocol”, or “Unknown Protocol” appears (see Figure 3-9). These labels are used when ASTEC Eyes cannot identify the protocol because its port number is different from the standard one (well-known port), e.g., when a proxy server is used, or ephemeral port number is used.

You can specify the appropriate protocol labels by configuring the decode hint. Decode hints are also required to decode the captured data correctly. For more information about decoding the captured data, see “Analyzing Network Packets” on page 52.

Choose **C**onfigure... from the **O**ptions menu on the menu bar of the Main window, and the **C**onfigure Options dialog box will appear as shown in Figure 3-17.

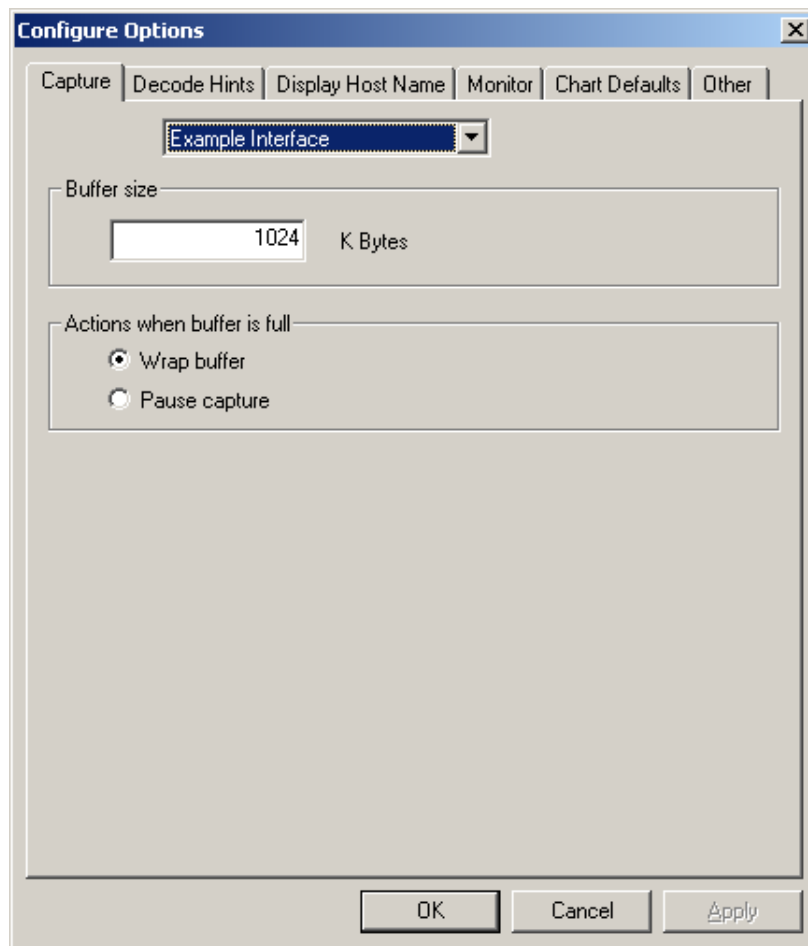


Figure 3-17 **C**onfigure Options dialog box showing the **C**apture page

Select the **Decode Hints** tab.

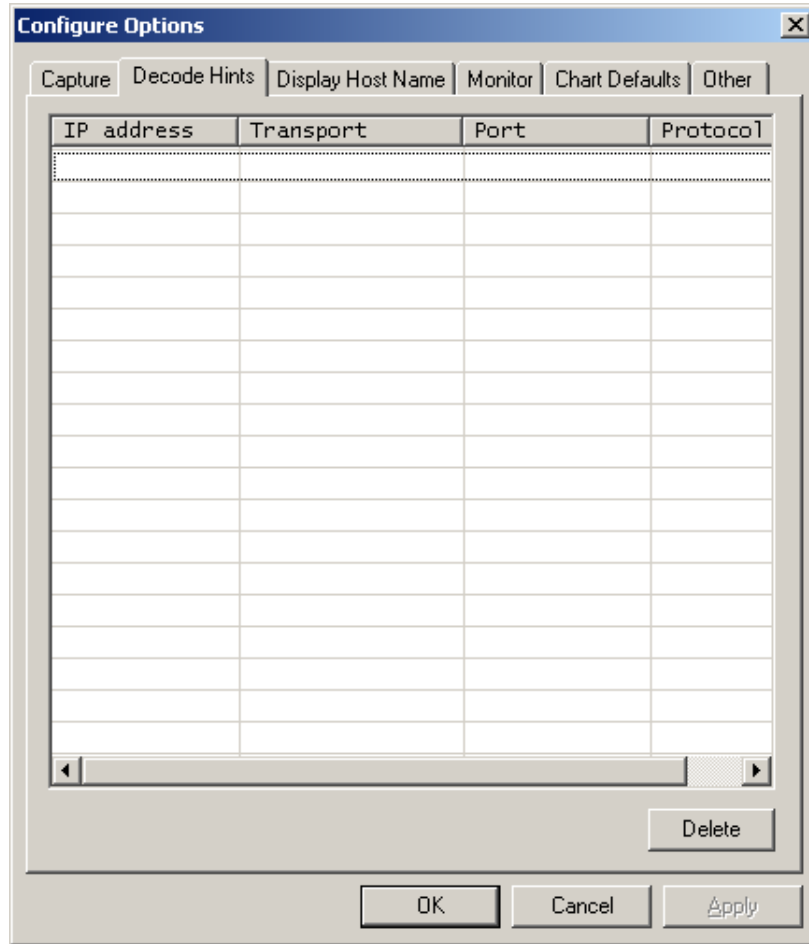


Figure 3-18 **Configure Options** dialog box showing the **Decode Hints** page

As an example, let's assume that a proxy server for HTTP protocol is running on the host with IP address 192.168.0.1, and the port number used is 8080 for TCP.

1. Select the first row by clicking on it.
The row will be highlighted in dark blue.
2. First, you want to specify the source or destination address used for the protocol. Click on the **IP Address** cell in the selected row, and a combo box to specify the IP address will appear, as shown in Figure 3-19. You can use “Any” if you do not want to specify any particular address.

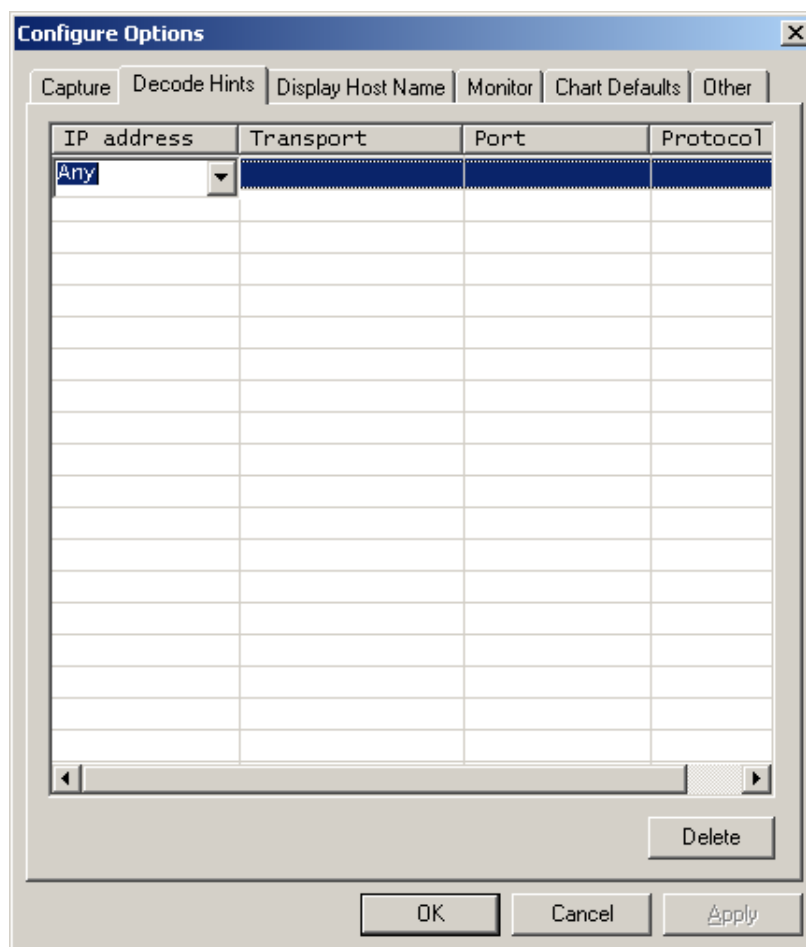


Figure 3-19 Entering a decode hint (IP address)

3. Type 192.168.0.1.
4. Next, you want to select the transport protocol. Click on the **Transport** cell or press the <TAB> key, and a drop down list will appear.
5. Select **TCP**, as shown in Figure 3-20.

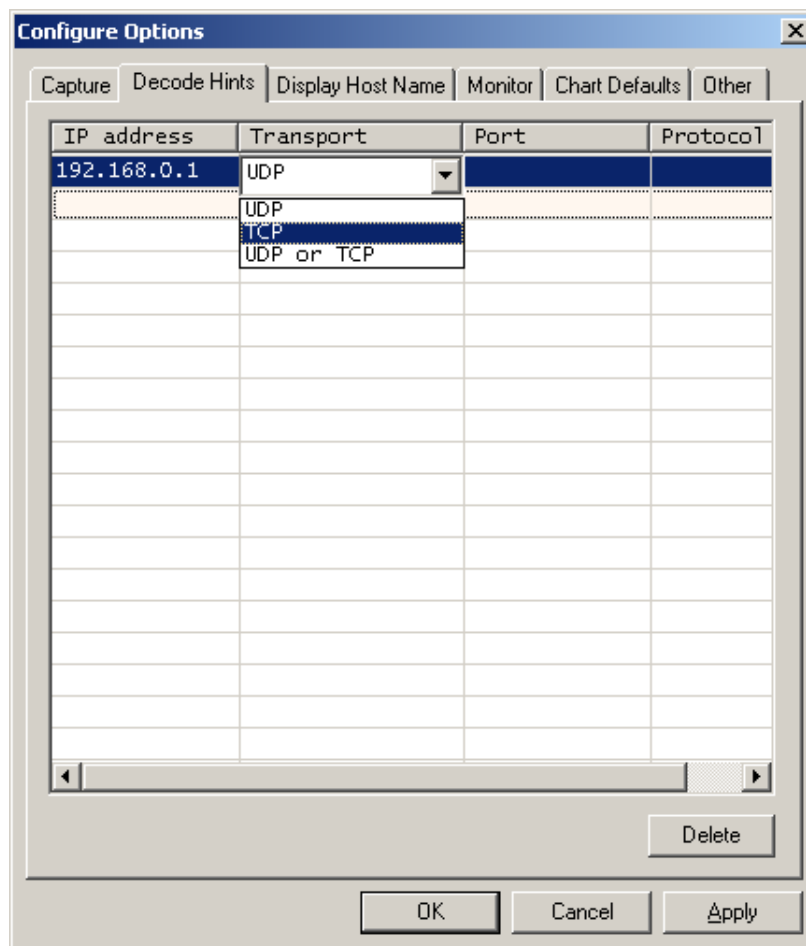


Figure 3-20 Entering a decode hint (transport)

6. Then you want to choose the port used by the protocol. Click on the **Port** cell or press the <TAB> key.
7. Enter 8080.
8. Lastly, you want to specify the protocol itself. Click on the **Protocol** cell or press the <TAB> key, and a combo box will appear.
9. Select **HTTP**, as shown in Figure 3-21.

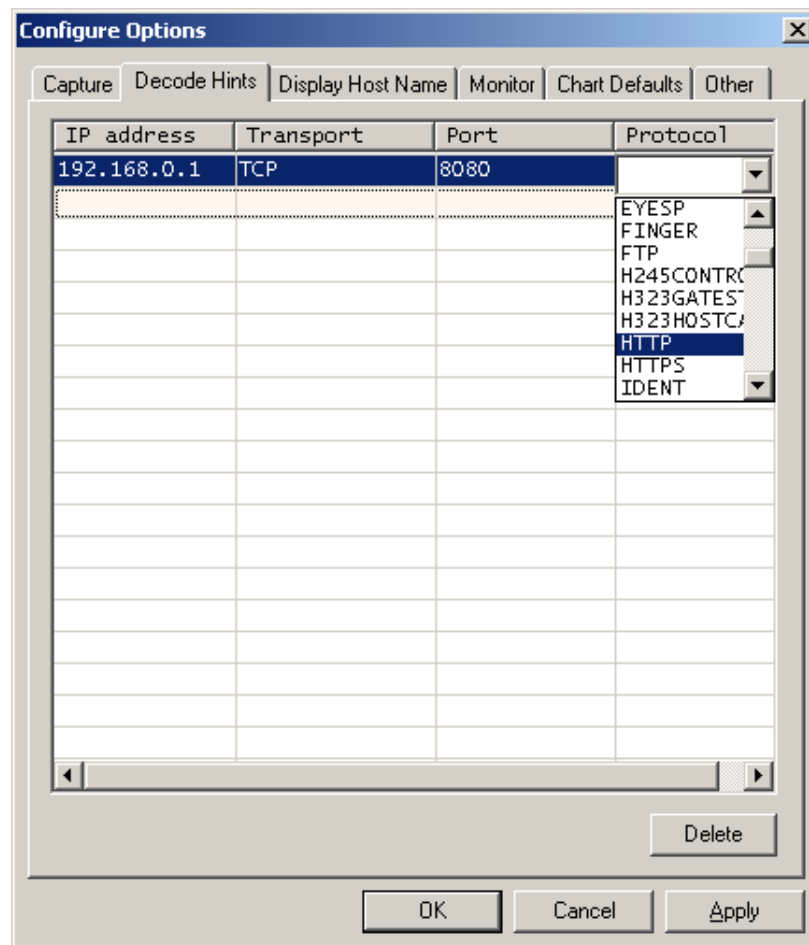


Figure 3-21 Entering a decode hint (protocol)

Now you have finished configuring the decode hints. Click the **OK** button to close the **Configure Options** dialog box.

After configuring a Decode Hint properly, note that the label “Unknown TCP Protocol” is no longer shown, as shown in Figure 3-22.

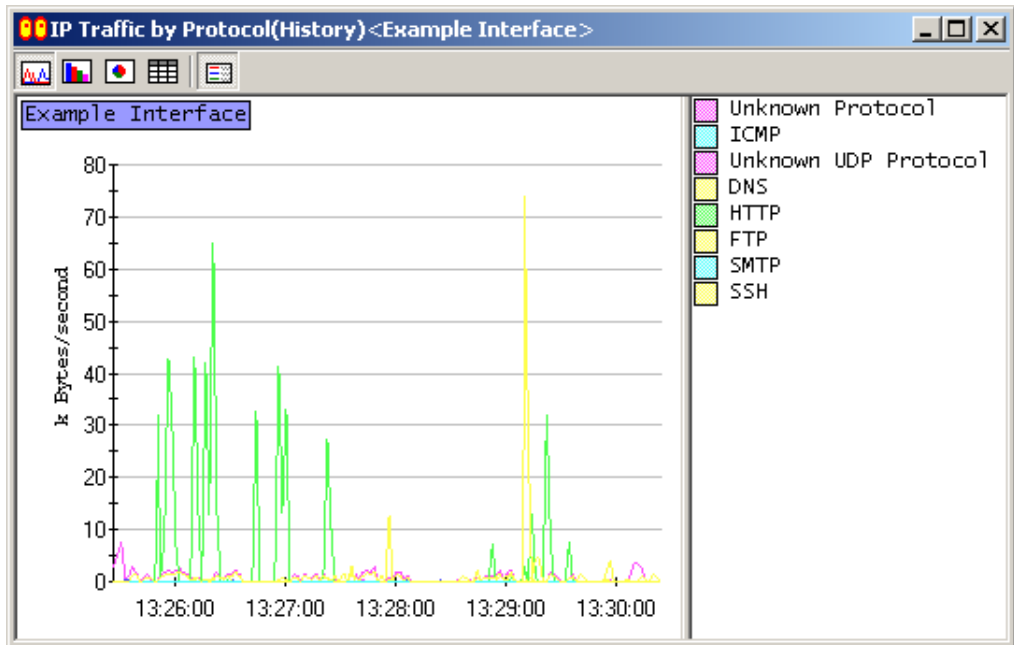


Figure 3-22 “IP Traffic by Protocol” after configuring a decode hint

Changing the Display Format of the Monitor Window

Hitherto, we used line charts as examples. You can display data in the bar or pie chart, or detailed table format, all of which may not be available depending on the type of the statistics you are displaying now. You might want to change the display format depending on how you want to monitor the network.

To change the display format, use the toolbar in the Monitor window.

Let's click the **Bar Chart (Total)** button (📊) on the toolbar. The display format will be changed to a bar chart. This chart shows the accumulated traffic for each protocol.

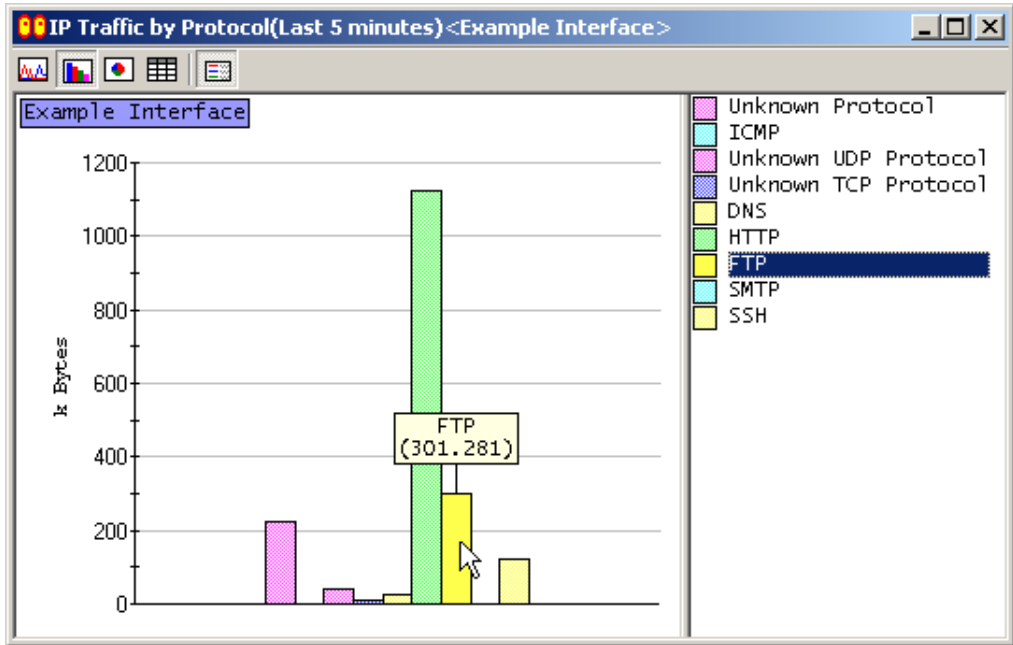


Figure 3-23 Display in bar chart format

You can select a Graph Item as with the line chart. If you select a Graph Item directly in the chart, a tooltip will pop up. With the bar chart, the name of the Graph Item and the number of bytes or frames will be shown, too.

Let's click the **Pie Chart (Distribution)** button (📊) on the toolbar. The display format will be changed to a pie chart. This chart shows the traffic distribution by protocol.

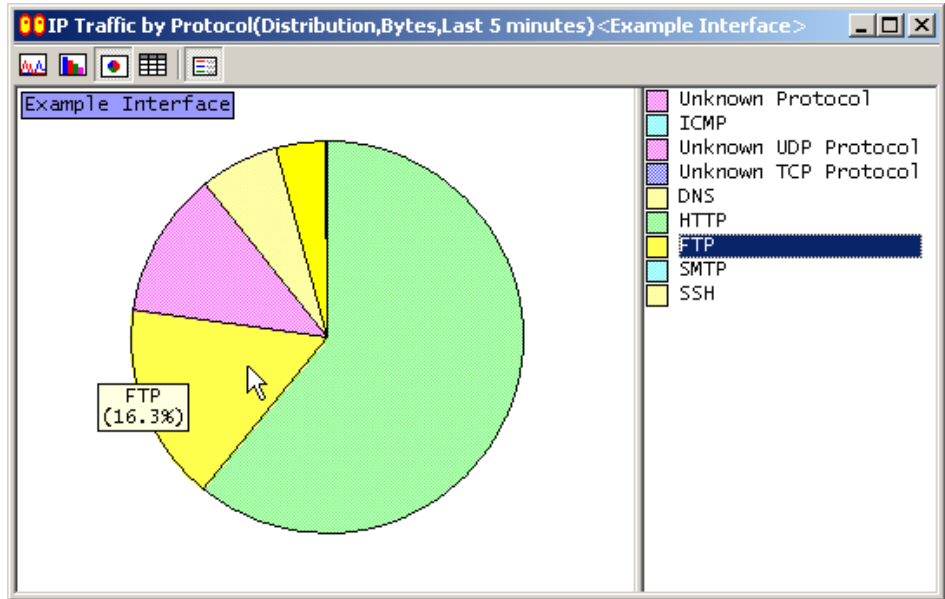


Figure 3-24 Display in pie chart format

You can select a Graph Item as with the line and bar charts. If you select a Graph Item directly in the chart, a tooltip will pop up. With the pie chart, the name of the Graph Item and the share of each protocol in the total volume will be shown.

Let's click the **Table (Detail)** button (☰) on the toolbar. The display format will be changed to a table. A row in the table corresponds to a Graph Item. This table contains the data for all the protocols since ASTEC Eyes were invoked. Therefore, the data for the Graph Items with no activities within last five minutes and eliminated from the line chart will be shown, too.

Protocol	k Bytes/second(aver...	k Bytes>Last 5 mi...	k Bytes(Total)
NetBIOS-NS	0.000	0.000	0.288
BB	0.000	0.000	0.192
NTP	0.000	0.000	0.564
NFS	0.000	0.000	0.064
IDENT	0.000	0.000	1.084
ICMP	0.000	0.148	0.148
SMTP	0.004	1.152	17.637
Unknown TCP Protocol	0.029	8.779	68.565
DNS	0.078	23.336	62.363
Unknown UDP Protocol	0.142	42.702	186.318
FTP	1.004	301.281	334.768
SSH	0.403	121.050	267.488
Unknown Protocol	0.750	225.066	1428.624
HTTP	3.744	1123.069	2270.987

Figure 3-25 Display in table format

You can easily search for text and find a target Graph Item within the table.

Let's press the <Ctrl-F> key. The **Find** dialog box will appear. Enter HTTP into the "Find what" input field, and click the **Find Next** button.

If data for HTTP protocol exists in the table, the corresponding row will be selected.

Analyzing Network Packets

In order to investigate the network, in addition to monitoring traffic, sometimes it is necessary to analyze the contents of the data (packets) that are actually flowing in the network.

To do this, first you need to copy the packets flowing in the network into the buffer of ASTEC Eyes. This operation is called **capture**. The buffer packets are copied into is called the **capture buffer**.

Second, you need to analyze the captured data based on all the supported protocols and display it. This operation is called **decoding** packets.

Capturing Packets

Let's capture packets.

Click the **Start Capture** button (●) on the Interface toolbar.

Capturing packets starts. The **Start Capture** button (●) turns gray and disabled, while the **Pause Capture** button (||) turns blue and enabled.

Let's look at the Capture Buffer Meter. The Capture Buffer Meter indicates the status of the capture buffer. As data are copied into the buffer, the bar that indicates the ratio of the captured data to the buffer size stretches forward to the right. The Capture Buffer Meter also shows the number of bytes copied into the buffer (353 K Bytes).

After copying some packets, click the **Pause Capture** button (||) on the Interface toolbar.

Capturing packets pauses. The **Start Capture** button (●) turns red and enabled, while the **Pause Capture** button (||) turns gray and disabled.




If your PC has more than one network interface, capturing packets is done for the currently selected network interface. If you want to capture packets on another network interface, first select the interface, and then click the **Start Capture** button (●).

For further information about selecting the network interface, see "Selecting a Network Interface" on page 28.

Saving Captured Data


Saving captured data allows the user to decode and view the data afterwards.

Let's save the captured data. Click the **Save Capture Buffer** button () on the Common toolbar in the Main window. The **Save As** dialog box will appear. Specify the filename and save the data.



The captured data is saved in the uncompressed Sniffer format compressed by "bzip2" (file extension .ebz) by default. You can also save it without compressing. For details on "bzip2", refer to <http://sources.redhat.com/bzip2/>.

Decoding Captured Data

Click the **New Decode View** button () on the Interface toolbar in the Main window.

The data in the capture buffer are decoded, and the decode view appears displaying the result, as shown in Figure 3-26.

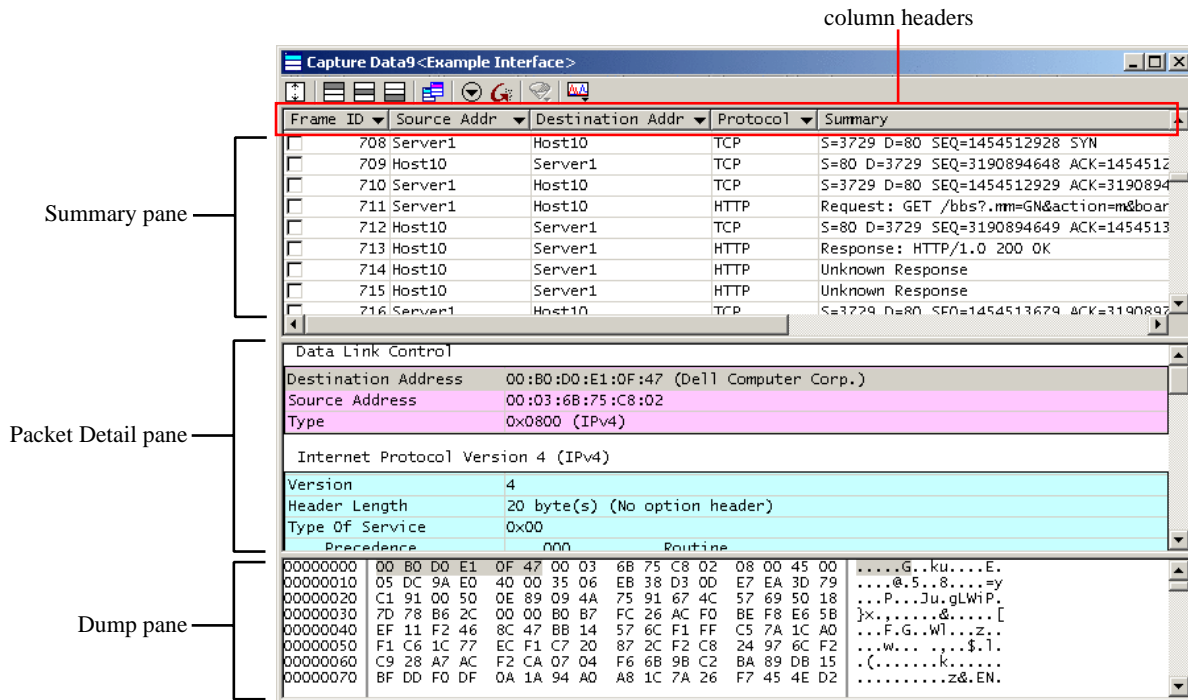

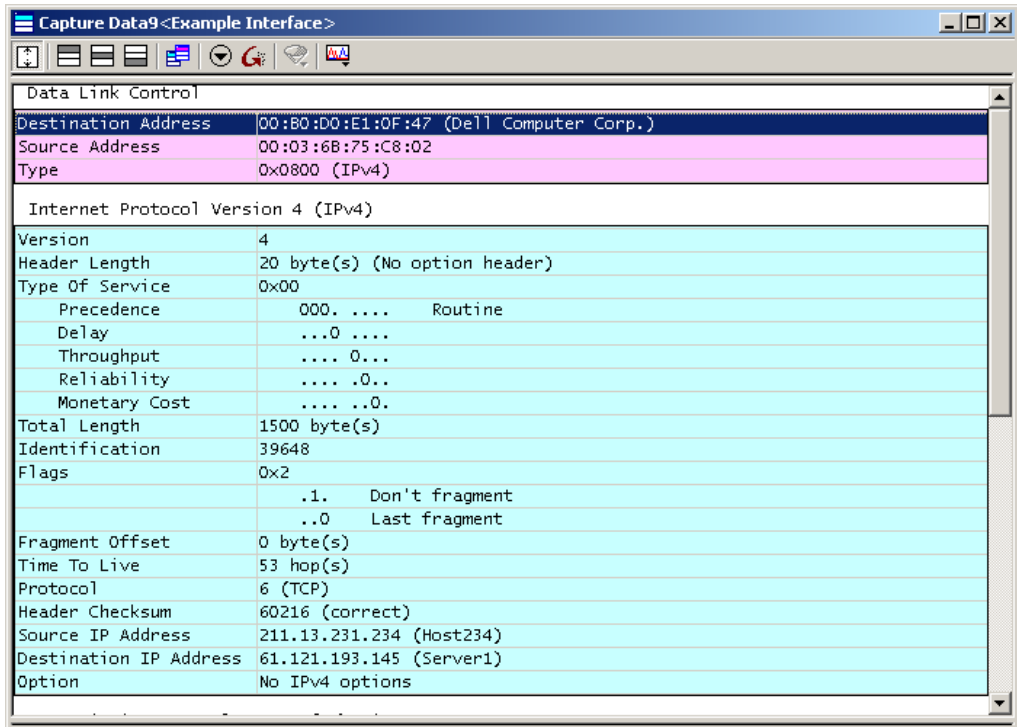


Figure 3-26 Decode view

The decode view is divided into three panes: the Summary pane, Packet Detail pane, and Dump pane. In the Summary pane, the summaries of the packets are shown. In the Packet Detail pane, the analysis of each packet is displayed. In the Dump pane, the packet data are displayed in a hexadecimal format. A row in the Summary pane corresponds to one packet.

Let's click on the Packet Detail pane. The focus will be set to the Packet Detail pane. Click the **Expand** button () on the toolbar. The Packet Detail pane will be enlarged to cover the entire decode view, as shown in Figure 3-27.




Data Link Control	
Destination Address	00:B0:D0:E1:0F:47 (Dell Computer Corp.)
Source Address	00:03:6B:75:C8:02
Type	0x0800 (IPv4)
Internet Protocol Version 4 (IPv4)	
Version	4
Header Length	20 byte(s) (No option header)
Type Of Service	0x00
Precedence	000. Routine
Delay	...0
Throughput 0...
Reliability0..
Monetary Cost0.
Total Length	1500 byte(s)
Identification	39648
Flags	0x2
	.1. Don't fragment
	..0 Last fragment
Fragment Offset	0 byte(s)
Time To Live	53 hop(s)
Protocol	6 (TCP)
Header Checksum	60216 (correct)
Source IP Address	211.13.231.234 (Host234)
Destination IP Address	61.121.193.145 (Server1)
Option	No IPv4 options

Figure 3-27 Decode view with decode result

Let's review the displayed contents by using the scroll bar with the mouse or pressing the arrow keys (<↑>, <↓>) and the page scroll keys (<Page Up>, <Page Down>).

For each protocol layer, the field names defined by the protocol are displayed on the left-hand side of the pane, and their values on the right-hand side.

To show the Summary and Dump pane again, press the **Expand** button () once again.



For the meaning of each field and the value, see appropriate documentation such as RFCs defining the protocol.

Screening Data to Be Displayed

Many packets are displayed in the decode view. ASTEC Eyes provides filters to narrow the packets being displayed so that you can easily reach the packets of interest.

First, let's try to display only the HTTP protocol by using the **caption filter**.

Click on the column header labeled "Protocol". A menu will appear as shown in Figure 3-28. Choose **HTTP**.

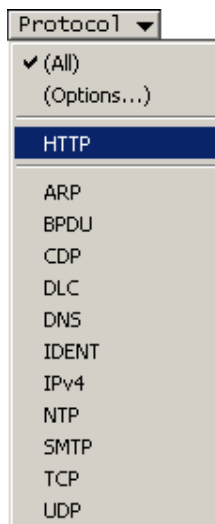


Figure 3-28 Caption filter menu

The contents of the decode view will change as shown in Figure 3-29.

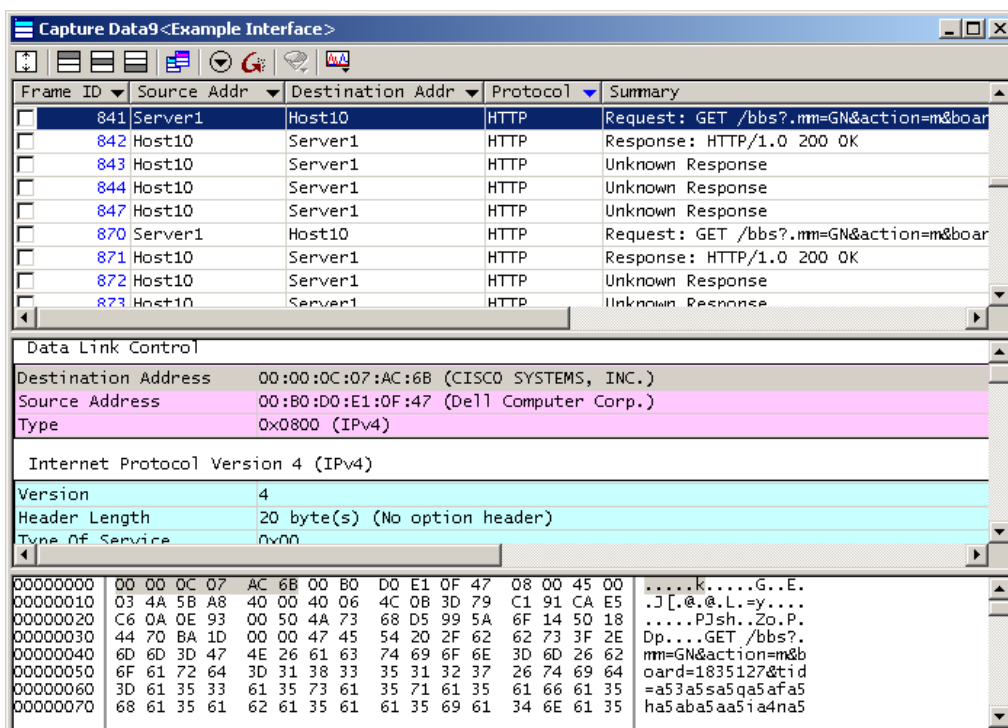


Figure 3-29 Decode view displaying packets of HTTP protocol only

To revert to the previous view showing all the packets, click on the “Protocol” column header again. The **caption filter** menu will appear. Choose **(All)** from the menu. All the packets will be shown again.

Next, let’s use the **header attribute filter**. As with monitoring, the header attribute filter classifies packets based on various attributes and screens them to be displayed.

Click the **Header Attribute Filter** button (☿) on the toolbar of the decode view. A menu will appear as shown below.

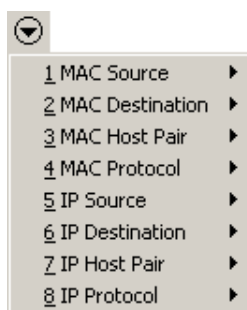


Figure 3-30 Header attribute filter menu

Each menu item in this menu leads to a submenu. Choose **Server1-Host10** from the submenu of **7 IP Host Pair** menu item.

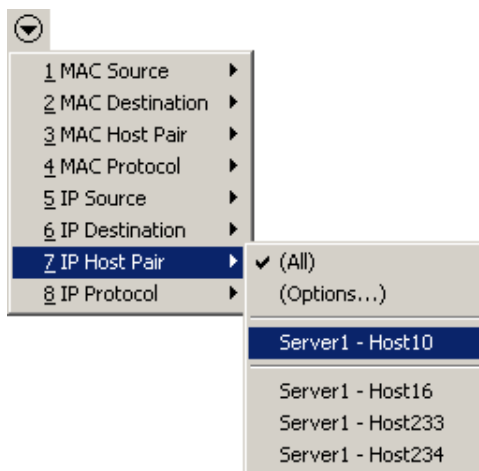


Figure 3-31 Selecting IP Host Pair

Now the decode view displays only IP layer packets that were transmitted between Server1 and Host10, as shown in Figure 3-32.

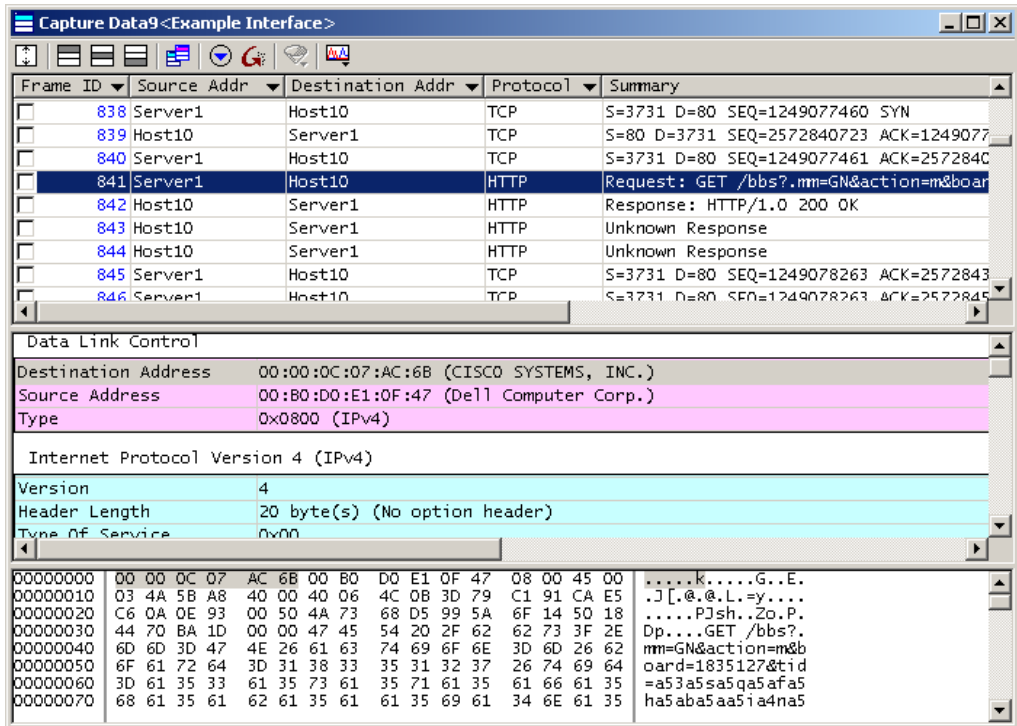


Figure 3-32 Decode view for a specific host pair only, limited by header attribute filter

To revert to the previous view showing all the packets as before, click the **Discard Filter** button (🗑️) in the decode view. All the packets will be shown again.



The **Discard Filter** button (🗑️) releases all the caption and header attribute filters set.

The caption filters and the header attribute filters are generically called **convenience filters**. In addition to these filters, you can use display filters in the decode view. A display filter is used to set complex conditions for screening packets. You need to define logical expressions for display filters. For further information, see “Filter Editor” on page 172.



You can also configure filters to capture desired packets, which are called **capture filters**. For further information, see “Filter Editor” on page 172.

Using the Stream View

In Figure 3-33, the Summary column for Frame ID 37 reads “Unknown Response”. This data is the continued data from Frame ID 36. Because the record of the HTTP protocol was split into two packets, the second packet cannot be decoded correctly. In TCP application protocols, it often happens that a record is split and transmitted in several packets.

The screenshot shows a network analysis tool interface with a packet capture list and a detailed decode view for frame 37.

Frame ID	Source Addr	Destination Addr	Protocol	Summary
34	Host10	Server1	HTTP	Request: GET /ENGLISH/VER1_2/introduc
35	Server1	Host10	TCP	S=80 D=1744 SEQ=268385890 ACK=5371402
36	Server1	Host10	HTTP	Response: HTTP/1.1 200 OK
37	Server1	Host10	HTTP	Unknown Response
38	Host10	Server1	TCP	S=1744 D=80 SEQ=537140203 ACK=2683888
39	Server1	Host10	HTTP	Unknown Response
40	Server1	Host10	HTTP	Unknown Response
41	Host10	Server1	TCP	S=1744 D=80 SFO=537140203 ACK=2683917

Data Link Control		
Destination Address	00:90:99:18:2C:F5 (ALLIED TELEESIS,K.K.)	
Source Address	00:04:6E:60:80:10	
Type	0x0800 (IPv4)	

Internet Protocol Version 4 (IPv4)		
Version	4	
Header Length	20 byte(s) (No option header)	
Type Of Service	0x00	
Precedence	000.	Routine
Delay	...0	

00000000	00 90 99 18 2C F5 00 04 6E 60 80 10 08 00 45 00n....E.
00000010	05 DC 69 76 40 00 3F 06 5D 6A AC 10 0A 22 AC 10	..iv@?.jj....
00000020	0C F9 00 50 06 00 0F FF 3E 62 20 04 1B EB 50 10	...P....>b...P.
00000030	60 F4 DD EE 00 00 48 54 54 50 2F 31 2E 31 20 32HTTP/1.1 2
00000040	30 30 20 4F 4B 0D 0A 44 61 74 65 3A 20 46 72 69	00 OK..Date: Fri
00000050	2C 20 30 35 20 4F 63 74 20 32 30 30 31 20 30 37	, 05 Oct 2001 07
00000060	3A 30 38 3A 33 31 20 47 4D 54 0D 0A 53 65 72 76	:08:31 GMT..Serv

Figure 3-33 Decode view

In such cases, the stream view that reassembles the virtual TCP stream will be handy. Click the **Stream View** button (📄) on the toolbar of the decode view. The stream view will appear as shown in Figure 3-34.

Stream ID	Address 1	Port 1	Direction	Address 2	Port 2	Protocol	Summary
0	Server3	57319	←	Host10	6000	X	Event: LeaveNotify
0	Server3	57319	→	Host10	6000	X	Request: ImageText8
0	Server3	57319	→	Host10	6000	X	Request: PolyLine
1	Host10	1744	→	Server1	80	HTTP	Request: GET /ENGLISH/V
1	Host10	1744	←	Server1	80	HTTP	Response: HTTP/1.1 200
1	Host10	1744	←	Server1	80	HTTP	Request: GET /ENGLISH/V
1	Host10	1744	←	Server1	80	HTTP	Response: HTTP/1.1 304
1	Host10	1744	→	Server1	80	HTTP	Request: GET /ENGLISH/V

Hypertext Transfer Protocol (HTTP 1.1)	
Response	HTTP/1.1 200 OK
Date	Fri, 05 Oct 2001 07:08:31 GMT
Server	Apache/1.3.20 (Unix)
Last-Modified	Fri, 05 Oct 2001 06:14:17 GMT
ETag	"54af01-1e41-3bbd4fb9"
Accept-Ranges	bytes
Content-Length	7745
Keep-Alive	timeout=15, max=100
Connection	Keep-Alive
Content-Type	text/html

00000000	48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 48 0D	HTTP/1.1 200 OK.
00000010	0A 44 61 74 65 3A 20 46 72 69 2C 20 30 35 20 4F	.Date: Fri, 05 O
00000020	63 74 20 32 30 30 31 20 30 37 3A 30 38 3A 33 31	ct 2001 07:08:31
00000030	20 47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 41 70	GMT..Server: Ap
00000040	61 63 68 65 2F 31 2E 33 2E 32 30 20 28 55 6E 69	ache/1.3.20 (Uni
00000050	78 29 0D 0A 4C 61 73 74 2D 4D 6F 64 69 66 69 65	x)..Last-Modifie
00000060	64 3A 20 46 72 69 2C 20 30 35 20 4F 63 74 20 32	d: Fri, 05 Oct 2

Figure 3-34 Stream view

As with the decode view, you can use the caption filter in the stream view. Let's click on the "Protocol" column header and choose **HTTP** from the menu that will appear. The contents of the stream view will change as shown in Figure 3-35.

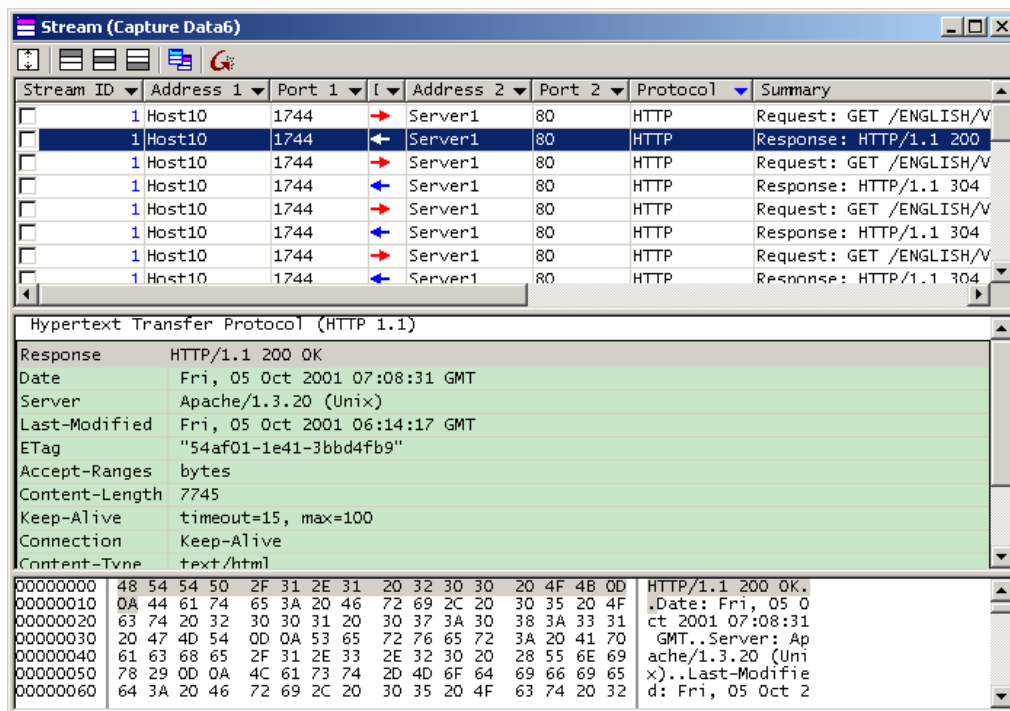


Figure 3-35 Stream view displaying the HTTP protocol packets only

In Figure 3-35, a row in the Summary pane corresponds to a record of the HTTP protocol.

Let's click on a row with Stream ID 1 in the stream view. The corresponding packets in the decode view will be highlighted in green, as shown in Figure 3-36.

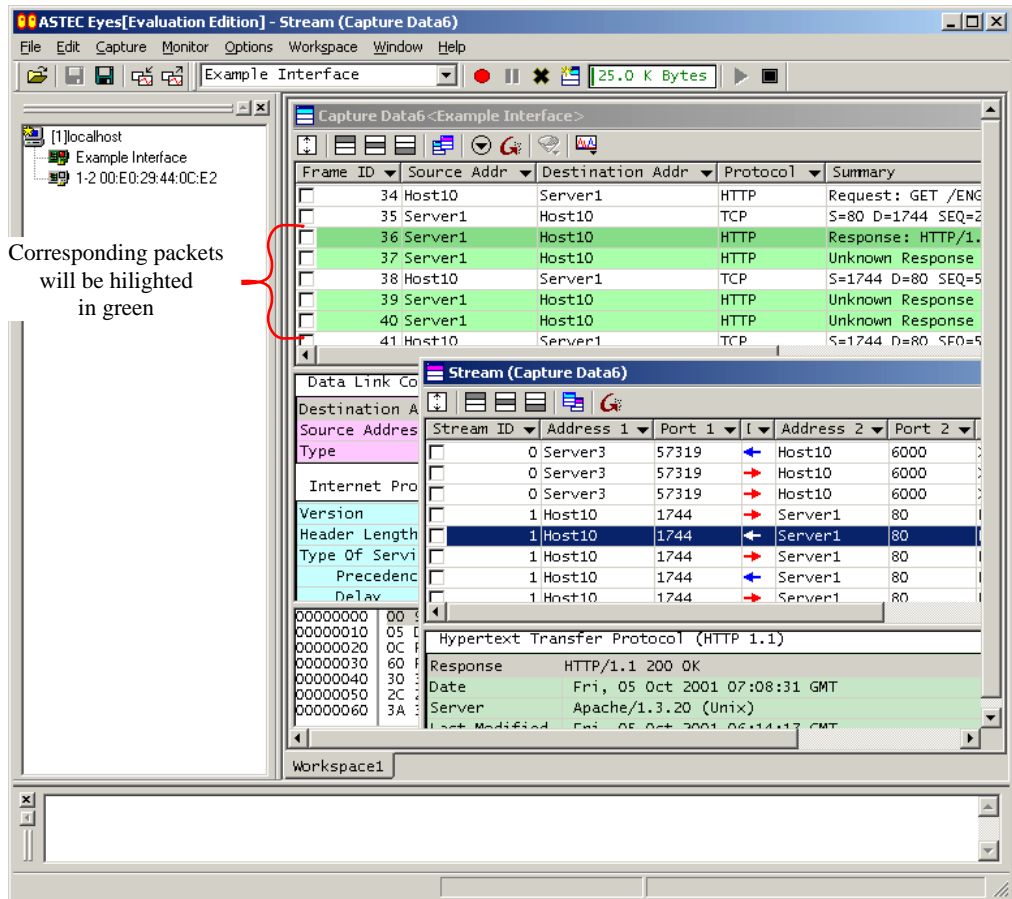


Figure 3-36 Mapping between a stream view record and decode view packets

In the stream view, there is no record with “Unknown Response” in the Summary column. Owing to TCP virtual stream reassembly, the data are analyzed properly.

Searching Decoded Results

You can search the decode and stream view for certain text. It can be done in the Summary, Packet Detail, or Dump pane respectively.

Here, let's search the Summary pane of the decode view for a specific packet. Set the focus to the Summary pane by clicking on it, and choose **F**ind... from the **E**dit menu on the menu bar of the Main window or press the <Ctrl-F> key. The **F**ind dialog box will appear as shown in Figure 3-37. Enter the text you want to find (here, `astec`), and click the **F**ind Next button.

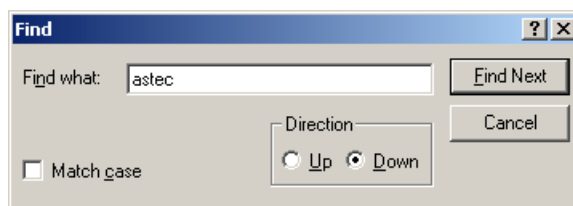


Figure 3-37 Find dialog box

Figure 3-38 shows the decode view displaying the result of the search. Note that the row found has been selected.

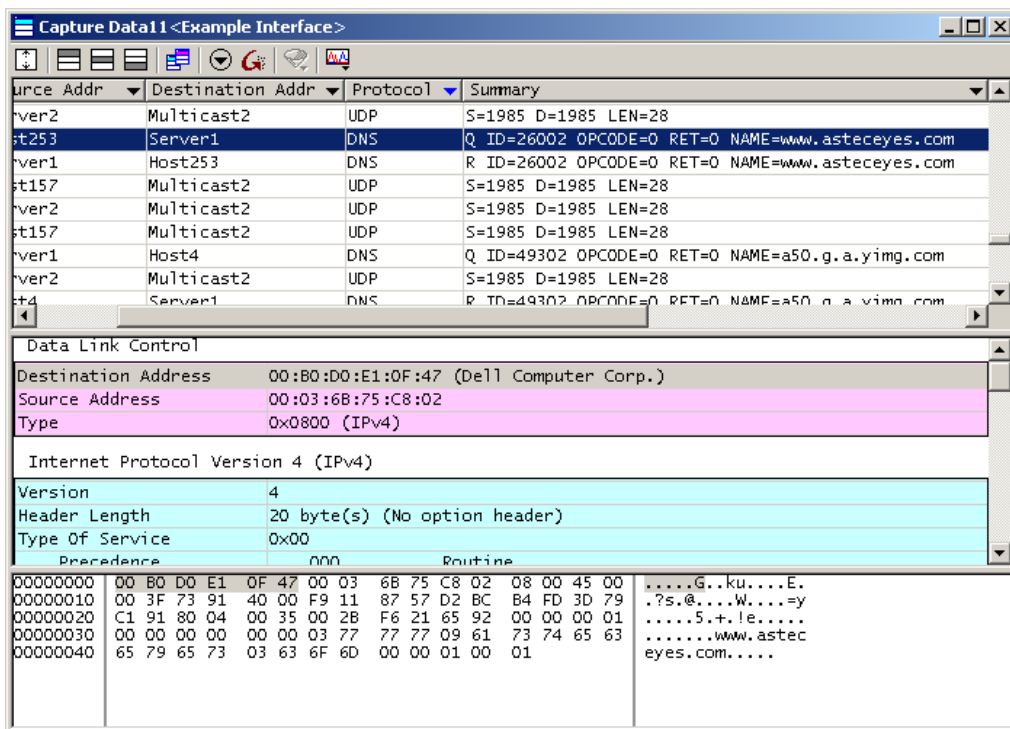


Figure 3-38 Decode view after the search

Organizing Windows

Getting through this tutorial so far, you will feel that ASTEC Eyes is clumsy, with many windows crowded in one workspace. Let's assume that we want to compare the two Monitor windows for "IP Traffic" and for "IP Traffic by Protocol" by placing these two side by side.

Using Workspaces

To make a comparison effectively, you can close all the windows other than those to be compared. However, there is a more convenient alternative to create a new workspace and move there only those windows of your interest.

First, click on the title bar of the Monitor window for "IP Traffic" with the right mouse button. A popup menu will appear as shown in Figure 3-39.

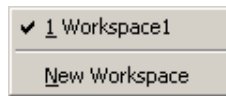


Figure 3-39 Popup menu for moving windows to another workspace

Choose **New Workspace** from the menu. A new workspace named **Workspace2** will be created in the Main window. The Monitor window for "IP Traffic" will then disappear from Workspace1.

Click on the tab of **Workspace2**. There you will find the Monitor window for "IP Traffic" alone, as shown in Figure 3-40.

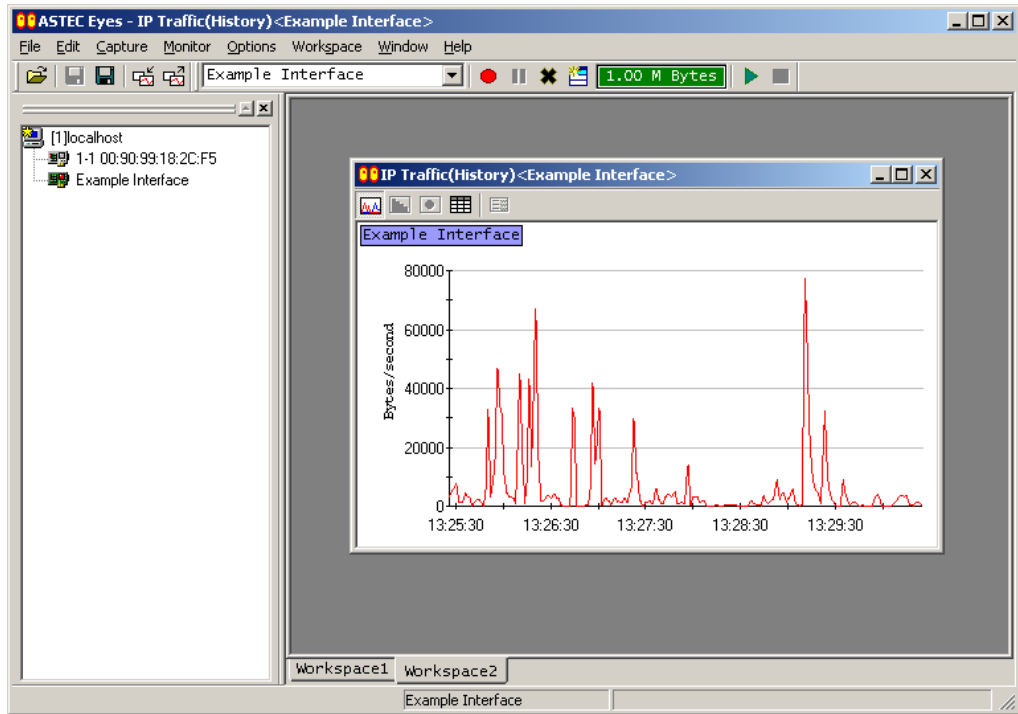


Figure 3-40 Monitor window for “IP Traffic” moved to the new workspace

Next, return to **Workspace1** by clicking on the tab. Then click on the title bar of the Monitor window for “IP Traffic by Protocol” with the right mouse button. As **Workspace2** already exists, a popup menu will appear as shown in Figure 3-41.

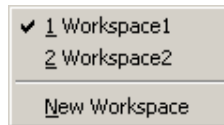


Figure 3-41 Popup menu for selecting workspaces

This time, choose **2 Workspace2**.

The Monitor window for “IP Traffic by Protocol” will be moved to the **Workspace2** and disappear from the current workspace. Click on the tab of **Workspace2** to show **Workspace2**.

You will find the two Monitor windows; one for “IP Traffic” and the other for “IP Traffic by Protocol”. To make it easier to compare them, choose **Tile Horizontally** from the **Window** menu on the menu bar of the Main window. ASTEC Eyes will look like in Figure 3-42 below.

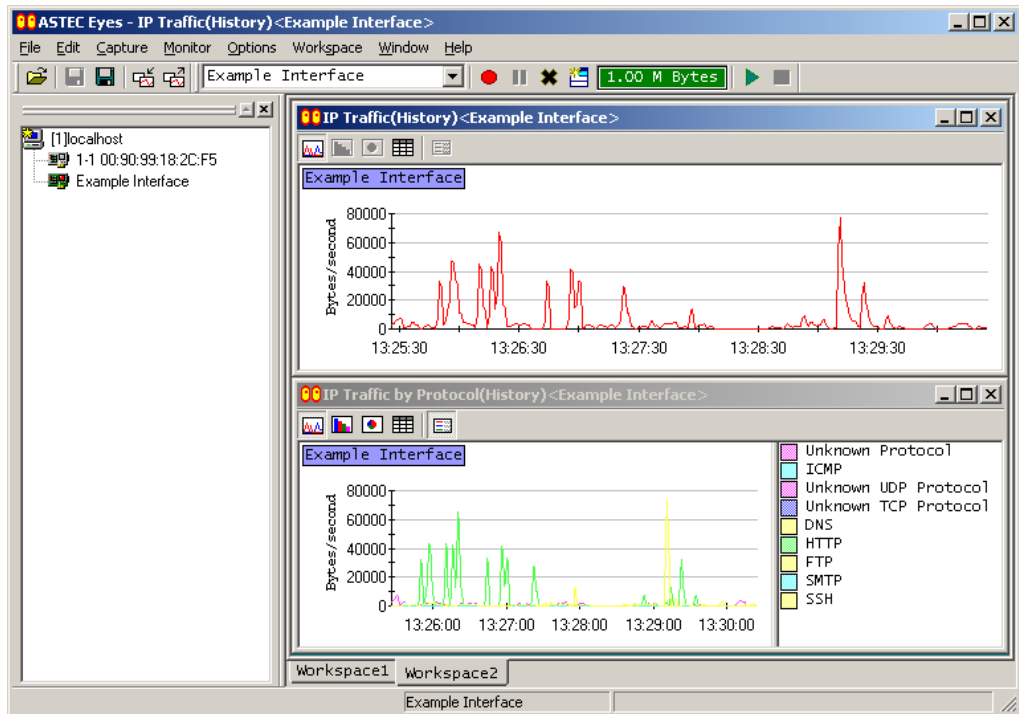


Figure 3-42 “IP Traffic” and “IP Traffic by Protocol” tiled horizontally

Changing the Properties of a Workspace

You may want to change the workspace name on its tab into a more meaningful one.

Let's change the workspace name.

Click on the tab of **Workspace2** with the right mouse button. A popup menu will appear. Choose **Properties** from the popup menu.

The **Workspace Properties** dialog box will appear as shown in Figure 3-43.

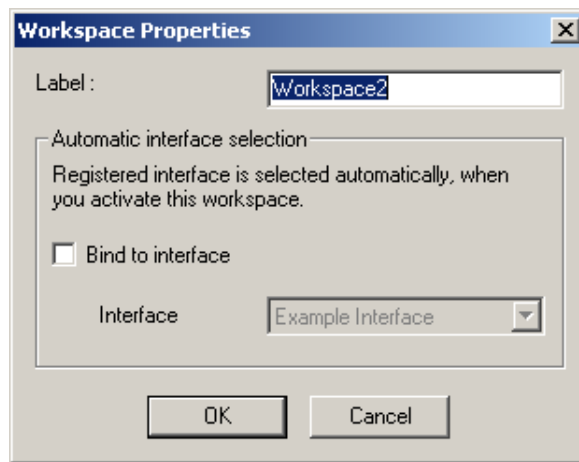


Figure 3-43 **Workspace Properties** dialog box


Type a new name into the input field to the right of the Label, and click the **OK** button.

For the complete discussion of the properties of the Workspace, see “Changing Workspace Properties” on page 169.

Saving a Configuration

With the ASTEC Eyes, it is easy to save and restore a particular configuration. You can save the configuration of the workspaces and the geometry of the Monitor windows. When you invoke ASTEC Eyes again, you can restore the previous configuration you saved before just by loading the configuration file.

The decode hints are also saved at the same time. Therefore, so long as the IP addresses and port numbers remain the same, you need not reconfigure the decode hints.

To save the configuration, click the **Save Configuration** button  on the Common toolbar in the Main window, or choose **Save Configuration...** from the **Options** menu on the menu bar of the Main window. For the complete discussion on saving the configuration, see “Saving a Configuration” on page 164.

Using a Remote Module

From ASTEC Eyes version 1.2, a new type of remote watching capability has been added. This feature enables the user to watch remote networks in the same way as you monitor the local network your PC is connected to. You can use the feature **just by connecting** ASTEC Eyes on the local PC to a remote PC with a Remote Module installed.

To connect ASTEC Eyes to the Remote Module, you use the Interface Selector window.

Click on an open space in the Interface Selector window with the right mouse button. Make sure you do not click on the icons and labels of the hosts or interfaces. Choose **Connect Remote...** from the popup menu.

The **Connect** dialog box will appear as shown in Figure 3-44.

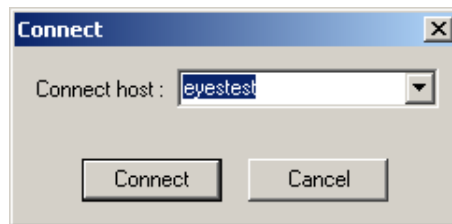


Figure 3-44 **Connect** dialog box

Fill the **Connect Host** input field, and click the **Connect** button.

For a “Connect Host” name, specify a host name that the local PC can recognize such as a NetBIOS name, a DNS name, an IP address, and so on.

The host you have specified and its interfaces will appear in the Interface Selector window.

Now all the functions of ASTEC Eyes described so far are available for the network interfaces of the remote PCs.



For the complete discussion of installing a Remote Module into a remote PC, see “Installation” on page 5. Also, for the complete discussion on invoking the Remote Module, see “Invoking and Installing a Remote Module as a Windows’ Service” on page 8.



For further information about remote watching, see “Remote Watching” on page 137.

Exiting ASTEC Eyes

After completing your work, exit ASTEC Eyes. To do so, choose **Exit...** from the **File** menu on the menu bar of the Main window.

This completes “Getting Invoked with ASTEC Eyes”.

ASTEC Eyes has more functions not covered in this tutorial. These functions are listed below. See Chapter 4 “Functional Description” for details.

- Logging for long-term trend observation
See “Logging” on page 129.
- Saving the chart
See “Saving Monitoring Information” on page 93.
- Detailed configurations for charts
See “Configuring Charts Default Options” on page 160.
- Reporting expert events
See “Reporting Expert Events” on page 146.



Chapter 4

Functional Description

This chapter details each function of ASTEC Eyes.

ASTEC Eyes has the following major functions:

- Monitoring
- Capturing
- Decoding
- Logging
- Remote watching
- Reporting expert events

The Remote Module has the functions of monitoring, capturing, logging, and reporting expert events. With the Remote Modules installed on remote PCs, you can watch remote networks in the same way as you monitor the local network your PC is connected.

Hereafter, we will discuss the preparation for using those functions, then investigate each function in detail, and finally present the configuration options and other miscellaneous functions.

Preparation before Using the Functions

Main Window of ASTEC Eyes

Figure 4-1 shows the Main window of ASTEC Eyes. The Main window has a menu bar, the Common toolbar, the Interface toolbar, a status bar, workspaces, the Interface Selector window, and the Message window.

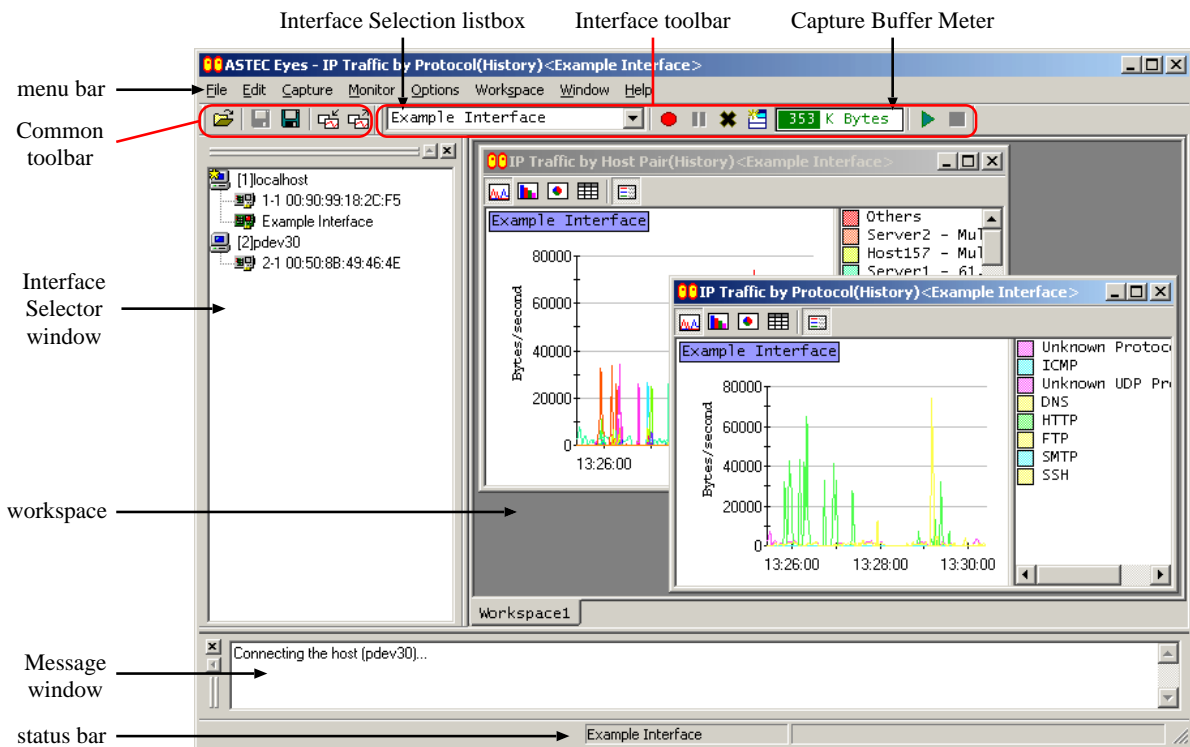


Figure 4-1 Main window

You can configure the Common toolbar, the Interface toolbar, the status bar, the Message window, and the Interface Selector window to be visible or invisible.






Common Toolbar and Interface Toolbar

Many of the windows of ASTEC Eyes, including the Main window, provide toolbars for your convenience. The Main window has two toolbars: the Common toolbar and the Interface toolbar.

The Common toolbar is for operations independent of interfaces.







The Interface toolbar is to manipulate the selected interface.

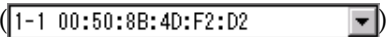
The following table shows the buttons on the Common toolbar in the Main window.

Button	Icon	Function
Open		Loads and decodes the captured data saved in a file, and shows the decode view.
Save Decoded Packets		Saves the captured data currently decoded.
Save Capture Buffer		Saves the data in the capture buffer.
Load Configuration		Loads the configuration.
Save Configuration		Saves the configuration.

You can hide the Common toolbar. Select **Show Toolbar** from the **Options** menu on the menu bar of the Main window, to make the Common toolbar visible or invisible.

The following table shows the buttons on the Interface toolbar in the Main window.

Button	Icon	Function
Start Capture		Starts capture.
Pause Capture		Pauses capture.
Discard Capture Data		Discards the data in the capture buffer.
New Decode View		Decodes the data in the capture buffer and shows the decode view.
Start Monitor		Starts monitoring.
Pause Monitor		Pauses monitoring.

The Interface toolbar in the Main window has a drop down list () for selecting the target interface, too. This is called the **Interface Selection listbox**.

You can hide the Interface toolbar. Select **Show Interface Toolbar** from the **Options** menu on the menu bar in the Main window, to make the Interface toolbar visible or

invisible.

Status Bar

The status bar of the Main window displays the status of ASTEC Eyes, and the name of the Graph Item selected in the Monitor window. Select **Show Status Bar** from the **Options** menu on the menu bar of the Main window, to make the status bar visible or invisible.

Message Window

The Message window displays important messages from ASTEC Eyes. For example, if the decode of a packet fails, it prints the frame ID and protocol name of the associated packet.

To set the focus to the Message window, click on the Message window with the left mouse button or press the <Alt-2> key.

If you click on the Message window with the right mouse button, a popup menu will appear as shown in Figure 4-2.

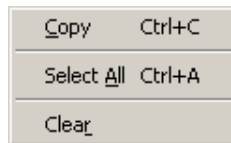


Figure 4-2 Popup menu for the Message window

Copy First, select the text in the Message window, then open the popup menu, and choose this menu item. The selected text is copied to the clipboard.

Select All Selects all the messages shown in the Message window.


Clear Deletes all the messages shown in the Message window.

Interface Selector Window

The Interface Selector window has various functions including selecting an interface, connecting to a Remote Module, manipulating an interface, and so forth.

To set the focus to the Interface Selector window, click on the Interface Selector window with the left mouse button or press the <Alt-1> key.

The selected interface is represented by the icon  (green), and the unselected interface is represented by the icon  (gray).

If you click on the icon or label of the interface, it will be selected and its icon will change to the **Selected Interface** icon ().

Immediately after invoking ASTEC Eyes, the Interface Selector window shows only the interface directly connected to the PC running ASTEC Eyes (localhost).

For the complete discussion of using the Remote Module and manipulating the interface of a remote PC, see “Remote Watching” on page 137.

Workspace

When you open windows in ASTEC Eyes, new windows, except for dialog boxes, will appear in the currently selected workspace. You can create multiple workspaces and move windows from one workspace to another. The workspace is a useful tool for categorizing and organizing the windows.

To set the focus to the workspace, click on with the left mouse button or press the <Alt-0> key.

For further information, see “Workspace” on page 167.

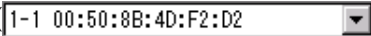
Selecting an Interface

In this section, “interface” refers to a network interface card installed in the PC.

If multiple network interface cards are installed in the PC, you need to select the target interface before you start monitoring or capturing.

From ASTEC Eyes version 1.2, you can watch remote networks by installing Remote Modules into remote PCs. If you have the Remote Modules installed, you can select the remote interfaces as well as the local interfaces.

You can select the interface in three ways:

- Click on the Interface Selection listbox () in the Main window, and choose the desired interface from the list.
- Click on the interface shown in the Interface Selector window with the left mouse button.
- Set the focus to the Interface Selector window by pressing the <Alt-1> key, select the desired interface by pressing the <↑> or <↓> key, and then press the <Enter> key.

ASTECS Eyes can monitor or capture the multiple interfaces simultaneously. You can select another interface and start monitoring or capturing it.

Monitoring

You can monitor the network traffic, measuring the flow of the packets through the network and viewing the statistics. You can classify the traffic by the source addresses, the destination addresses, the host pairs, and the protocols. In addition, you can visualize the statistics of the traffic in chart or table.

You can view various address tables: the MAC address table, the IP address table, and the MAC address - IP address table.

This section investigates monitoring in depth. In this chapter, the statistical data on the traffic are sometimes referred to as “monitor data” or simply “data”.


Selecting the Target Interface for Monitoring

You can start and pause monitoring each network interface independently. You need to select the target interface before you start monitoring.

For a complete discussion on selecting an interface, see “Selecting an Interface” on page 78.

Starting or Pausing Monitoring

You can start monitoring by any of the three ways shown below:

- Click the **Start Monitor** button () on the Interface toolbar in the Main window, after selecting the target interface.
- Choose **Start** from the **Monitor** menu on the menu bar in the Main window, after selecting the target interface.
- Click on the target interface in the Interface Selector window with the right mouse button. A popup menu will appear as shown in Figure 4-3.

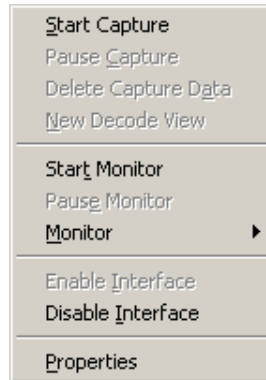


Figure 4-3 Popup menu for interface specific operation

Choose **Start Monitor** from the menu.



A Monitor window displaying statistics does not appear by just starting monitoring. For more information, see “Opening a Monitor window” below.

There are three ways to pause monitoring:

- Click the **Pause Monitor** button (■) on the Interface toolbar in the Main window, after selecting the target interface.
- Choose **Pause** from the **Monitor** menu on the menu bar in the Main window, after selecting the target interface.
- Click on the target interface in the Interface Selector window with the right mouse button. A popup menu will appear. Choose **Pause Monitor** from the popup menu (see Figure 4-3).

Opening a Monitor Window

You need to open Monitor windows, to view the statistics. There are two ways to open a Monitor window:

- Choose the statistics of your interest from the **Monitor** menu on the menu bar in the Main window, after selecting the target interface.
- Click on the target interface in the Interface Selector window with the right mouse button. A popup menu will appear. Choose **Monitor** from the popup menu. The

submenu will appear as shown in Figure 4-4.

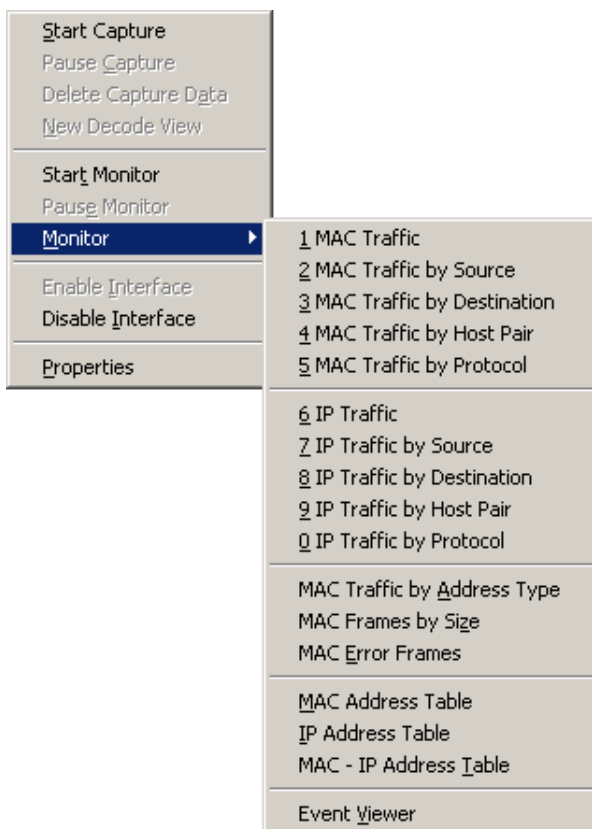


Figure 4-4 Popup menu and the **Monitor** submenu

Choose the statistics of your interest.

A Monitor window will appear in the active workspace. The title of the Monitor window indicates the name of the interface in purple. The legend for Graph Items is shown by default.

ASTEC Eyes version 1.2 provides Monitor windows for the following thirteen types of statistics:

MAC Traffic

Displays the total traffic measured in packets or bytes at the MAC

(Media Access Control) layer.

MAC Traffic by Source

Displays the traffic classified by the source addresses at the MAC layer.

MAC Traffic by Destination

Displays the traffic classified by the destination addresses at the MAC layer.

MAC Traffic by Host Pair

Displays the traffic classified by the combinations of the source and the destination addresses (the host pairs) at the MAC layer.

MAC Traffic by Protocol

Displays the traffic classified by the protocols at the MAC layer.

IP Traffic

Displays the total traffic measured at the IP (Internet Protocol) layer.

IP Traffic by Source

Displays the traffic classified by the source addresses at the IP layer.

IP Traffic by Destination

Displays the traffic classified by the destination addresses at the IP layer.

IP Traffic by Host Pair

Displays the traffic classified by the combinations of the source and the destination addresses (the host pairs) at the IP layer.

IP Traffic by Protocol

Displays the traffic classified by the protocols at the IP layer.

MAC Traffic by Address Type

Displays the traffic classified by the address types (unicast, multi-cast, or broadcast) at the MAC layer.

MAC Frames by Size


Displays the traffic classified by the frame size ranges at the MAC layer.


MAC Error Frames


Displays the statistical data of error packets. The traffic is classified by the types of errors.


Changing the Display Format of the Monitor Window

The Monitor window displays the statistics of the traffic in line chart format by default. You can choose how the statistics are shown in bar chart, pie chart, or detailed table.

Click the **Line Chart (History)** button () on the toolbar of each Monitor window, to use the line chart.

Click the **Bar Chart (Total)** button () on the toolbar of each Monitor window, to use the bar chart.

Click the **Pie Chart (Distribution)** button () on the toolbar of each Monitor window, to use the pie chart.

Click the **Table (Detail)** button () on the toolbar of each Monitor window, to use the table format.

The line chart shows the fluctuation of the traffic over time by the line segments. The bar chart shows the traffic by the bar's height. The pie chart shows the distribution of the traffic by the sectors. Each one of the lines, bars, and sectors, which represents a statistical element such as the traffic of a certain protocol, is referred to as a **Graph Item**.



The bar chart and pie chart for "MAC Traffic" or "IP Traffic" are not available in the Monitor window.



The legend is shown on the right-hand side of the Monitor window by default, but can be made invisible to give more room for the chart. For further information, see "Popup Menu on the Monitor Window When No Graph Item Is Selected" on page 88.

The Number of Graph Items Displayed in the Monitor Window

There are two types of the line and bar charts, different in the statistics they are displaying. One type displays all Graph Items while the other displays only some higher-volume Graph Items in the traffic.

All Graph Items are displayed for the following statistics:

- MAC Traffic by Protocol
- IP Traffic by Protocol
- MAC Frames by Size
- MAC Traffic by Address Type
- MAC Error Frames

Only some higher-volume Graph Items are displayed for the following statistics:

- MAC Traffic by Source
- MAC Traffic by Destination
- MAC Traffic by Host Pair
- IP Traffic by Source
- IP Traffic by Destination
- IP Traffic by Host Pair

In the **bar chart**, “TopN” is appended to the title of the Monitor window displaying only some higher-volume Graph Items. The number of the Graph Items to be displayed may be selected by the user. The default value is 10, and it can be altered through the popup menu and **Configure Options** dialog box.

In the **pie chart**, the number of the Graph Items to be displayed depends on the value specified through the popup menu or the **Configure Options** dialog box. The default value is 10.

The number of frames (packets) and octets flowing through the network are counted, and the statistical data are generated every one second. In the **line chart**, the Graph Items that were in top N at any time of the period covered by the data, are displayed individually. Those Graph Items that were never in top N for the period covered by the data, are aggregated into the Graph Item “Others”. The user may choose not to use the Graph Item “Others”, and to display all the Graph Items.



You can set the number of the Graph Items displayed in the TopN charts by using the **Configure Options** dialog box.

For further information, see “Configuring Charts Default Options” on page 160 and “Popup Menu on the Monitor Window When No Graph Item Is Selected” on page 88.

Table Format

In the table format, each row corresponds to a Graph Item. A table contains all the Graph Items since ASTEC Eyes or its Remote Module was invoked. That is, the data for the Graph Items with no activities within the monitoring period and thus eliminated from the line chart will be shown, too. The table has columns such as the type of traffic, the total number of octets and frames during a certain period, and the accumulated number of octets and frames since ASTEC Eyes or its Remote Module was invoked. Clicking on the header of each column sorts the rows according to the cell values of the column.

If you want to find a specific Graph Item, you can search for text. To search for text, choose **Find...** from the **Edit** menu on the menu bar of the Main window, or press the **<Ctrl-F>** key. The **Find** dialog box will appear. Enter the text you want to search and click the **OK** button or press the **<Enter>** key.

Saving the Display Format of the Monitor Window

You can save in a configuration file such information as the type of traffic you are watching, the display format, the geometry, and displaying the legend, or not. For more information, see “Saving a Configuration” on page 164.

Selecting a Graph Item

You can select a Graph Item of the chart shown in the Monitor window by clicking on it with the left mouse button.

The selected Graph Item will be highlighted and the tooltip for it will appear. When the legend is visible, the corresponding item in the legend is also highlighted.

The name of the selected Graph Item is displayed in the tooltip and the status bar of the Main window. For bar charts, the total number of octets or frames is also displayed. For pie charts, the name and the share are displayed, too.



To select the Graph Item of a line chart, it is recommended to click around the vertices rather than clicking on the line segments.



For a complete discussion of the status bar of the Main window, see “Status Bar” on page 77.

Selecting a Graph Item Using the Legend

If it is not easy to select the Graph Item in the chart, you can select the Graph Item by clicking on the corresponding item in the legend.

You can also select an item in the legend by using the keyboard. The description of the key bind follows:

<↑> and <↓>

The selected item in the legend can be changed using these keys. The corresponding Graph Item will be selected.

<Ctrl-Space>


When a legend item and the corresponding Graph Item are selected, their selection will be cleared. When they are not selected, they will be selected.



You can select a Graph Item using the keyboard even when the legend is not shown.

Selecting a Graph Item Using the Table

You can select a Graph Item using the table.

If it is not easy to select the Graph Item in the chart, you can also use the table. First, you need to show the data in the table format by clicking the **Table (Detail)** button  on the toolbar of the Monitor window. After selecting the row for the desired Graph Item, revert to the previous chart. You will notice that the desired Graph Item is selected in the chart, too.



When there are many Graph Items, searching for the text is recommended.

Using the Popup Menu on the Monitor Window

You can display a popup menu using right click on the Monitor window with a chart displayed. The menu items may differ depending on the chart and whether the Graph Item is selected or not. Using the popup menu, you can change the unit used in the chart or show the breakdown of the Graph Item.

Popup Menu on the Monitor Window When No Graph Item Is Selected

Figure 4-5 shows the popup menu for the line chart.

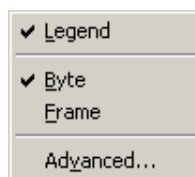


Figure 4-5 Popup menu for the line chart

<u>L</u>egend	Shows the legend if it is not displayed. Hides the legend if it is displayed.
<u>B</u>yte	Displays the traffic in octets.
<u>F</u>rame	Displays the traffic in frames.
<u>U</u>tilization	Available only for the Monitor window of “MAC layer traffic”. The utilization is how much traffic is actually flowing compared with the upper limit of the media. Displays the traffic in percentage.
<u>A</u>dvanced...	Opens the Advanced dialog box. The contents of the dialog box are the same as those of Chart Defaults page in Configure Options dialog box. However, the values set here are applied only to the Monitor window the popup menu was invoked for. For further information, see “Configuring Charts Default Options” on page 160.



You can make the legend shown or hidden by clicking the **Legend** button () on the toolbar of the Monitor window.

Figure 4-6 shows the popup menu of a bar and pie chart.

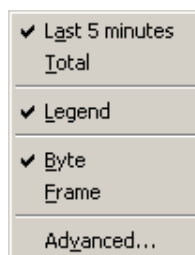


Figure 4-6 Popup menu for the bar and pie chart

Last *T* minutes Displays the traffic in octets or frames during the last *T* minutes. *T* is the monitoring period, which can be set through options for monitoring. For more information, see “Configuring Monitor Options” on page 159.

Total Displays traffic in octets or frames since ASTEC Eyes or its Remote Module was invoked.

Other menu items are the same as those in the popup menu for the line chart.

Popup Menu on the Monitor Window When a Graph Item Is Selected

When a Graph Item is selected, the menu items for displaying its **breakdown** are added. The menu items added may differ according to the type of the Monitor window, the selected Graph Item, and display format of the Monitor window.

As an example, Figure 4-7 shows the popup menu when the Graph Item of the IP address 111.22.111.222 was selected in the Monitor window for “IP Traffic by Source”.

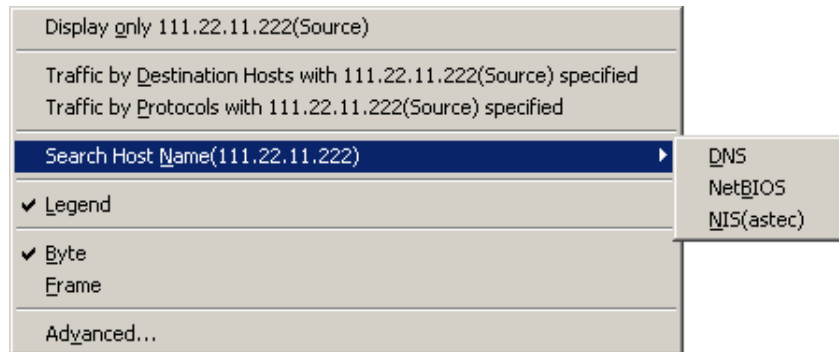


Figure 4-7 Popup menu of a Monitor window when a Graph Item is selected

Display only 111.22.11.222 (Source)

Displays only the selected Graph Item “111.22.11.222”. This menu item is added for the line chart only.

111.22.11.222 (Source) Traffic by Destination

Displays the statistics of packets from the selected host 111.22.11.222, classified by the receiving host.

111.22.11.222 (Source) Traffic by Protocol

Displays the statistics of packets from the selected host 111.22.11.222, classified by protocol.

Search Host Name (111.22.11.222)

This menu item has a submenu listing name services. Between the parentheses of the submenu item NIS, the NIS domain name specified through the **Searching for Host Name** dialog box is shown. If you have not specified the domain name, “Unspecified” is shown, and you cannot choose this menu item.

If you choose an item from the submenu, host names will be searched using the selected name service. If they are found, the host names will be used instead of the IP addresses in tooltips, legends, and tables.

The rest of the menu items are those in the popup menu when no Graph Item is selected.

Even with the Monitor window displaying item breakdown, you can use the popup menu pretty much in the same way. You can also display the further breakdown of the Graph Item by selecting from the popup menu. To revert to the previous chart, choose **Revert**. The **Revert** menu item will appear only in the popup menu on the Monitor window displaying the breakdown of a certain item.

You can open a new Monitor window for the breakdown, choosing the menu item for the breakdown while holding down the <Shift> key. There will be no **Revert** menu item in the popup menu for the new Monitor window.

Monitoring Required Data Only

Sometimes you want to monitor only a certain portion of the entire traffic, which can be determined by specific conditions. In this case, you can filter the packets to be monitored, using the monitor filter.

With ASTEC Eyes version 1.0, only the statistics specified by the monitor filter were collected. With ASTEC Eyes version 1.2, all statistics are collected, but only those specified by the monitor filter will be displayed. As the original statistics are not lost, you can specify different filter conditions, and analyze the traffic from various viewpoints.

The filter editor is used to configure the monitor filter. To invoke the filter editor, choose **Filter Editor** from the **Edit** menu on the menu bar of the Main window. For further information, see "Filter Editor" on page 172.



There are no monitor filter conditions applicable to "MAC Frames by Size" nor "MAC Error Frames".

MAC and IP Address Tables

You can view MAC and IP address tables and their mapping tables.

To display the **MAC address table**, choose **MAC Address Table** from the **Monitor** menu on the menu bar of the Main window.

The table has three columns: the MAC Address, the Vendor Name, and the Host Name. In this table, all the MAC addresses collected are shown. In the Host Name column, host names obtained by capturing and decoding packets and defined by the user are both displayed.

To display the **IP address table**, choose **IP Address Table** from the **Monitor** menu on the menu bar of the Main window.

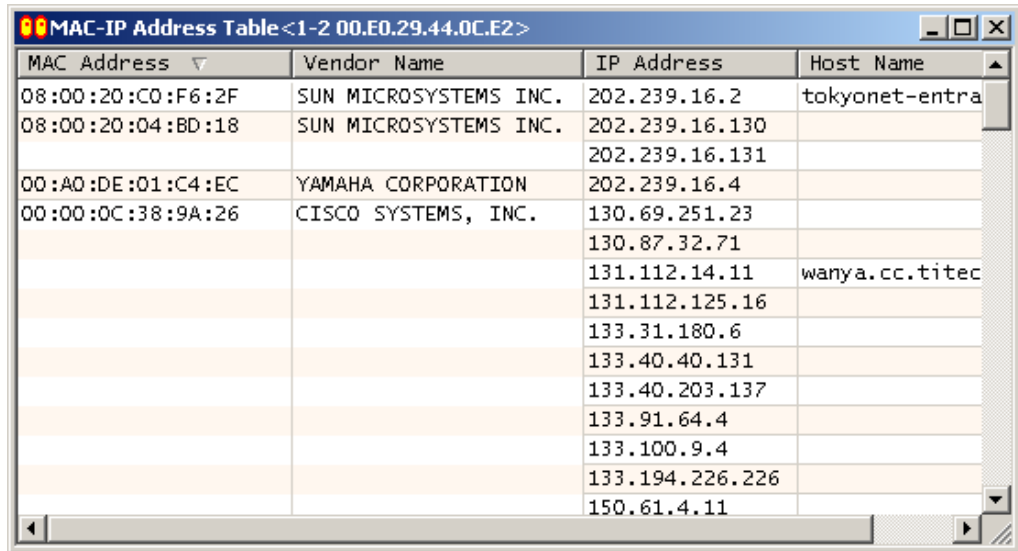
The table has two columns: the IP Address, and the Host Name. In this table, all the IP addresses collected are shown. The Host Name column contains the names:

- Found during monitoring,
- Recorded to the log file,
- Found by active search,
- Obtained by capturing and decoding packets, and
- Defined by the user.

To display the **MAC address and IP address mapping table**, choose **MAC - IP Address Table** from the **Monitor** menu on the menu bar of the Main window.

The table has the four columns: the MAC Address, the Vendor Name, the IP address, and the Host Name. This table includes only the MAC addresses of the nodes with their IP addresses assigned. The values for the Host Name column are taken from the IP address table.

By clicking on the column header of each table, the table will be sorted according to the contents of the column. Once you click, the table will be sorted in the ascending order. Click again, and the table will be sorted in the descending order this time. If more than one row has the same value for that column, the value is shown only in the uppermost row. For example, if there are multiple IP addresses corresponding to one MAC address, the table sorted by the MAC Address will look like Figure 4-8.



MAC Address	Vendor Name	IP Address	Host Name
08:00:20:C0:F6:2F	SUN MICROSYSTEMS INC.	202.239.16.2	tokyonet-entra
08:00:20:04:BD:18	SUN MICROSYSTEMS INC.	202.239.16.130	
		202.239.16.131	
00:A0:DE:01:C4:EC	YAMAHA CORPORATION	202.239.16.4	
00:00:0C:38:9A:26	CISCO SYSTEMS, INC.	130.69.251.23	
		130.87.32.71	
		131.112.14.11	wanya.cc.titec
		131.112.125.16	
		133.31.180.6	
		133.40.40.131	
		133.40.203.137	
		133.91.64.4	
		133.100.9.4	
		133.194.226.226	
		150.61.4.11	

Figure 4-8 The MAC - IP address table sorted by the MAC address



Before you start monitoring, nothing will be shown in any of the tables, IP address, MAC address, or MAC - IP address.



Each network interface has its own tables, IP address, MAC address, and MAC - IP address, separate from those for the other interfaces.

Saving Monitoring Information

The information collected during monitoring and displayed in the Monitor window is collectively called **monitoring information**. It includes statistics, IP addresses, and MAC addresses.

The monitoring information can be saved into a file, or copied and pasted into other applications (Microsoft Word, Microsoft Excel, Word Pad, Notepad, and so forth).

When saving the information, you can choose the file format. The supported formats are:

- CSV (Comma Separated Values) format (*.csv),

- the bitmap format (*.bmp),
- the metafile format (*.wmf), and
- the enhanced metafile format (*.emf).

When you use copy and paste, the format will be selected by the receiving application. Some applications allow the user to select the format of the data to be pasted. With Microsoft Word and Excel, you can paste the chart displayed in the Monitor window as bitmap for visual effect, or you can paste the underlying data as text or in CSV format.

You can save the monitoring information into a file:

1. Activate the Monitor window you want to save.
2. Choose **Save Monitor...** from the **F**ile menu on the menu bar of the Main window.

You can copy and paste the monitoring information into another application:

1. Activate the Monitor window you want to copy.
2. Choose **C**opy from the **E**dit menu on the menu bar of the Main window, or press the <Ctrl-C> key.
3. Open or activate the target application.
4. Press the <Ctrl-V> key.

Data in the Monitor window will be pasted into the target application. If it is Microsoft Word or Excel, you can choose **Paste Special** from the **E**dit menu on the menu bar.



The monitoring information to be saved or copied will differ slightly, depending on the display format of the Monitor window.

For example, when the top 10 items are displayed in the source bar chart, only their statistics will be saved or copied.

Capturing

You can copy the packets flowing through the network into the buffer of ASTEC Eyes to analyze them in detail. This operation is called **capture**, and the buffer is called the **capture buffer**.


Selecting the Target Network Interface for Capture

Capture is done for each network interface individually. In addition, each network interface has its own capture buffer. Therefore, you need to select the target interface before you start any capture-related operations.



For a complete discussion of selecting the network interface, see “Selecting an Interface” on page 78.

Starting Capture

There are three ways to start capture:

- Click the **Start Capture** button () on the Interface toolbar in the Main window after selecting the target interface.
- Choose **Start** from the **Capture** menu on the menu bar of the Main window after selecting the target interface.
- Click on the target interface in the Interface Selector window with the right mouse button. A popup menu will appear. Choose **Start Capture** from the popup menu (see Figure 4-3).

As packets are copied into the capture buffer, the bar of the Capture Buffer Meter stretches to the right, indicating the number of bytes copied into the buffer. The length of the bar indicates how much in the buffer is already used. As the captured data increases, the Capture Buffer Meter is updated.


If you configure to pause capture when the capture buffer is full, the bar and the number of bytes in the Capture Buffer Meter are shown in blue (). If you configure to wrap around when the capture buffer is full, they are shown in green ().



For further information on configuring the capture behavior at buffer full, see “Configuring Capture Options” on page 152.


Pausing Capture

There are three ways to pause capture:

- Click the **Pause Capture** button () on the Interface toolbar in the Main window after selecting the target interface.
- Choose **Pause** from the **Capture** menu on the menu bar of the Main window after selecting the target interface.
- Click on the target interface in the Interface Selector window with the right mouse button. A popup menu will appear. Choose **Pause Capture** from the popup menu (see Figure 4-3).

Discarding Captured Data

There are three ways to discard the captured data:

- Click the **Discard Capture Data** button () on the Interface toolbar in the Main window after selecting the target interface.
- Choose **Discard Capture Data** from the **Capture** menu on the menu bar of the Main window after selecting the target interface.
- Click on the target interface in the Interface Selector window with the right mouse button. A popup menu will appear. Choose **Discard Capture Data** from the popup menu (see Figure 4-3).

Appending Data in the Capture Buffer

If you resume capture without discarding the data in the buffer, the newly captured data will be appended to the data already in the capture buffer.

If you resume capture when the capture buffer is full, the behavior depends on the configuration. With **Wrap around**, the buffer is overwritten. With **Pause capture**, an **ASTEC Eyes** dialog box appears as shown in Figure 4-9. Discard the captured data before you resume capture.

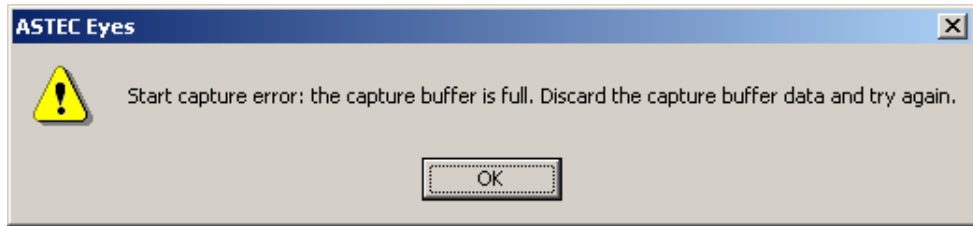


Figure 4-9 Dialog box that appears when capture buffer is full



For further information on configuring the capture behavior at buffer full, see “Configuring Capture Options” on page 152.

Saving Captured Data into a File

You can save the captured data into a file, so that you can analyze the data later. There are two ways to save the captured data into a file:

- Click the **Save Capture Buffer** button (📁) on the Common toolbar in the Main window.
- Choose **Save Capture Buffer** from the **F**ile menu on the menu bar of the Main window.



The captured data is saved in the uncompressed Sniffer format compressed by “bzip2” (file extension `.ebz`) by default. You can also save it without compressing. For details on “bzip2”, refer to <http://sources.redhat.com/bzip2/>.



ASTEC Eyes can read compressed Sniffer format (file extension `.enc`) and the Microsoft Network Monitor format (file extension `.cap`), “tcpdump” format, and “snoop” format. However you cannot save the data in these formats.

Using the Start Capture Trigger

You can configure to start capture, triggered by a specific packet on the network.

The logical expression defining this trigger is called the **start capture trigger**.

Use the filter editor, to configure the start capture trigger. To invoke the filter editor, choose **Filter Editor** from the **Edit** menu on the menu bar of the Main window. You can edit the start capture trigger of the target interface with this filter. For further information, see “Filter Editor” on page 172.

Start capture after you configure the start capture trigger. As long as the logical expression remains false, capture will not start, and “Waiting” is displayed in the Capture Buffer Meter. When the logical expression becomes true, capture will start, and the number of bytes copied into the capture buffer will be displayed instead of “Waiting”.



The packet triggering the start is also captured.

Using the Pause Capture Trigger

You can also configure to pause capture, triggered by a specific packet on the network.

The logical expression defining this trigger is called the **pause capture trigger**.

Use the filter editor to configure the pause capture trigger. To invoke the filter editor, choose **Filter Editor** from the **Edit** menu on the menu bar of the Main window. You can edit the pause capture trigger of the target interface with this filter editor. For more information, see “Filter Editor” on page 172.

Start capture after you configure the pause capture trigger. As long as the logical expression remains false, the capture continues, and the Capture Buffer Meter is updated as the captured data increases. When the logical expression becomes true, capture will pause automatically.



The packet triggering the pause is also captured.

Capturing Data of Interest Only

If you capture packets of a backbone network where various packets flow in a large volume, you might end up with many unwanted packets in the capture buffer. Furthermore you might fail to capture the data you want, as the size of the capture buffer is limited. To cope with such a situation, you can use the capture filter to collect only the packets of interest.

Use the filter editor to configure the capture filter. Choose **Filter Editor** from the **Edit** menu on the menu bar of the Main window. With this filter editor, you can edit the capture filter of the target interface. For further information, see “Filter Editor” on page 172.



Continuous Capture




A new function called the “continuous capture” has been added to ASTEC Eyes version 1.2. It is to capture packets continuously and save the captured data directly into files. The capture filter, the start capture trigger, and the pause capture trigger, which are available for “normal” capture storing the data into the capture buffer, are not available for continuous capture. In continuous capture, **all** packets flowing through the network connected to the specified network interface card are captured.

You can use this function as follows:

1. You need to have configuration privileges. First, make sure that you have these privileges.

In the Interface Selector window, check the status of the icon for the host that has the interface at which you want to capture packets.

The **host with privileges** icon  means you have these privileges. The **host** icon  means you do not have these privileges.

If the host is represented by the **host** icon , click on the icon or its label with the right mouse button. A popup menu will appear. Choose **Get Privilege** from the popup menu. Make sure that the **host** icon  has been changed to the **host with privileges** icon .

For a complete discussion of configuring privileges, see “Actions on a Remote Module” on page 140.

2. Click on the host icon or its label in the Interface Selector window with the right mouse button.

The popup menu for the host will appear.

3. Choose **Properties** from the popup menu.
The **Host Properties** dialog box will appear.
4. Click on the **Continuous Capture** tab in the **Host Properties** dialog box.
The **Continuous Capture** page will be shown in the **Host Properties** dialog box, as shown in Figure 4-10.

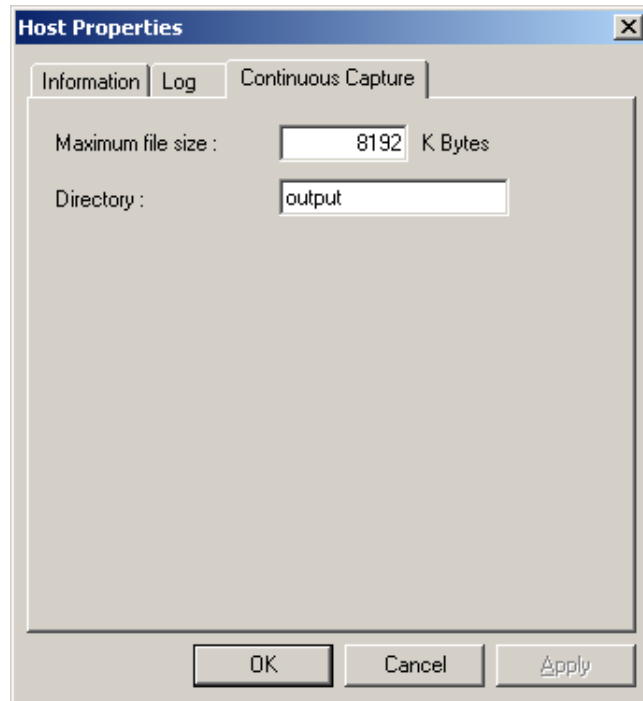


Figure 4-10 The **Host Properties** dialog box showing the **Continuous Capture** page

5. Specify maximum file size and directory.
Enter the upper limit of the file size in the **Maximum file size** field. If the size of the output file exceeds the specified upper limit, a new file will be created.
Enter the directory name, in the **Directory** field. This directory is where the output files will be placed. The directory should be a subdirectory of the directory ASTEC Eyes or the Remote Module is installed. So, specify the directory as relative path of the directory ASTEC Eyes or the Remote Module is installed. If this directory is not existed yet, you need to create it by yourself.
6. Click the **OK** button to close the **Host Properties** dialog box.

7. In the Interface Selector window, click on the interface icon or its label for the interface you want to run continuous capture.
The **Interface Properties** dialog box will appear.
8. Click on the **Continuous Capture** tab.
The **Continuous Capture** page will be shown in the **Interface Properties** dialog box, as shown in Figure 4-11.

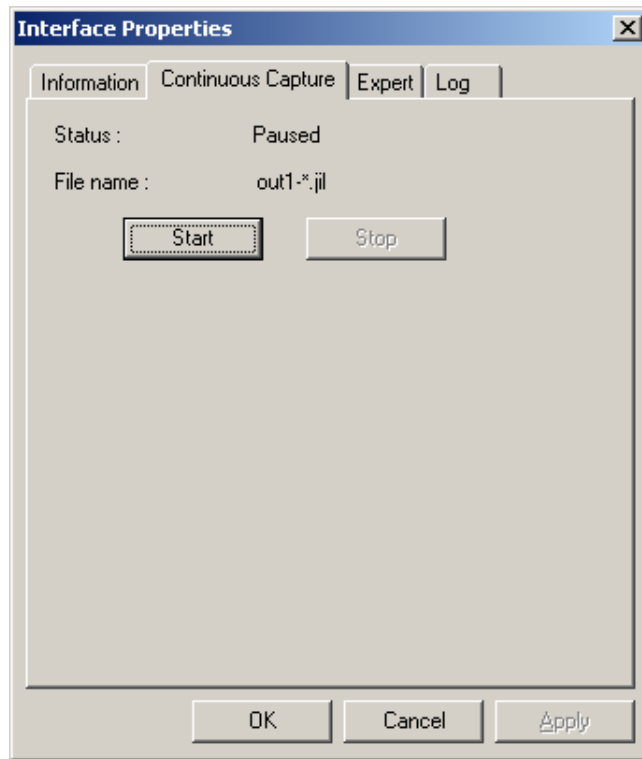


Figure 4-11 The **Interface Properties** dialog box with the **Continuous Capture** page shown

The **Status** is indicated as “Paused”.

9. Click the **Start** button.

The **Status** will be changed to “Output” and the capture for the interface will start.

A file for storing the captured data is created under the directory specified in the **Continuous Capture** page of the **Host Properties** dialog box.

Its extension is `.jil`, and its filename is the one shown in the **File name** field with * replaced by the sequence number starting from 1.

To stop the captured data into the file, click the **Stop** button. The **Status** will be changed to "Paused".



It is recommended that you stop continuous capture at an appropriate time. Otherwise, the free hard disk space of the PC with ASTEC Eyes or the Remote Module running will decrease.

If the free hard disk space becomes about less than 80M bytes, the writing of the captured data is automatically stopped.

As with files with the extension `.enc` and `.ebz`, the captured data written into a file can be analyzed by using decoding.

Decoding


You can analyze the data in the capture buffer or saved in a file. Analyzing data is called **decoding**.

ASTEC Eyes analyzes packets one by one to figure out what kind of protocols they contain, interprets them based on the protocols used, and shows the result in the **decode view**.

For upper layer protocols above TCP, ASTEC Eyes reassembles the TCP virtual streams and analyzes them. This result is shown in the **stream view**.

Decoding Data in the Capture Buffer


Select the target interface before decoding the captured data in the buffer, as a capture buffer is allocated to each interface. You can create the decode view by any of the following three ways:

- Click the **New Decode View** button  on the Interface toolbar in the Main window.
- Choose **New Decode View** from the **Capture** menu on the menu bar of the Main window.
- Click on the target interface in the Interface Selector window with the right mouse button. A popup menu will appear. Choose **New Decode View** from the popup menu.

The data in the capture buffer are analyzed and the decode view will appear showing the results.

Decoding Data Saved in a File

There are the following five ways to open a file and decode the data in it:

- Click the **Open** button  on the Common toolbar in the Main window. The **Open** dialog box will appear. Specify the file to be decoded.
- Choose **Open...** from the **File** menu on the menu bar of the Main window. The **Open** dialog box will appear. Specify the file to be decoded.
- Press the <Ctrl-O> key. The **Open** dialog box will appear. Specify the file to be decoded.

- Drag the icon of the file to be decoded from the Windows Explorer, and drop it in the Main window of ASTEC Eyes.
- Double-click on the icon of the file to be decoded in the Windows Explorer. This is effective only for files with the extensions `.enc` or `.ebz`.

The data in the specified file will be analyzed and the decode view will appear showing the results.

You can decode the files of the following formats.

File Format	File Extension
Uncompressed Sniffer format	<code>.enc</code>
Compressed Sniffer format	<code>.enc</code>
<code>.enc</code> file compressed by "bzip2"	<code>.ebz</code> , <code>.enc.bz2</code>
Continuous capture output file	<code>.jil</code>
<code>.jil</code> file compressed by "bzip2"	<code>.jil.bz2</code>
Microsoft Network Monitor format	<code>.cap</code>
"tcpdump" format (libpcap version 2 or later)	not specified
"snoop" format	not specified



A file with an extension other than `.enc`, `.ebz`, `.enc.bz2`, `.jil`, `jil.bz2`, and `.cap` is treated as the "tcpdump" format or the "snoop" format.



You can open a file compressed by the "bzip2" program (file extension `.bz2`), except the one originally in the Microsoft Network Monitor format.



For an extremely large file, you can divide it into parts and decode each part separately. For more information, see "Decoding Divided Data" on page 122.

The Decode View

Figure 4-12 shows a decode view.

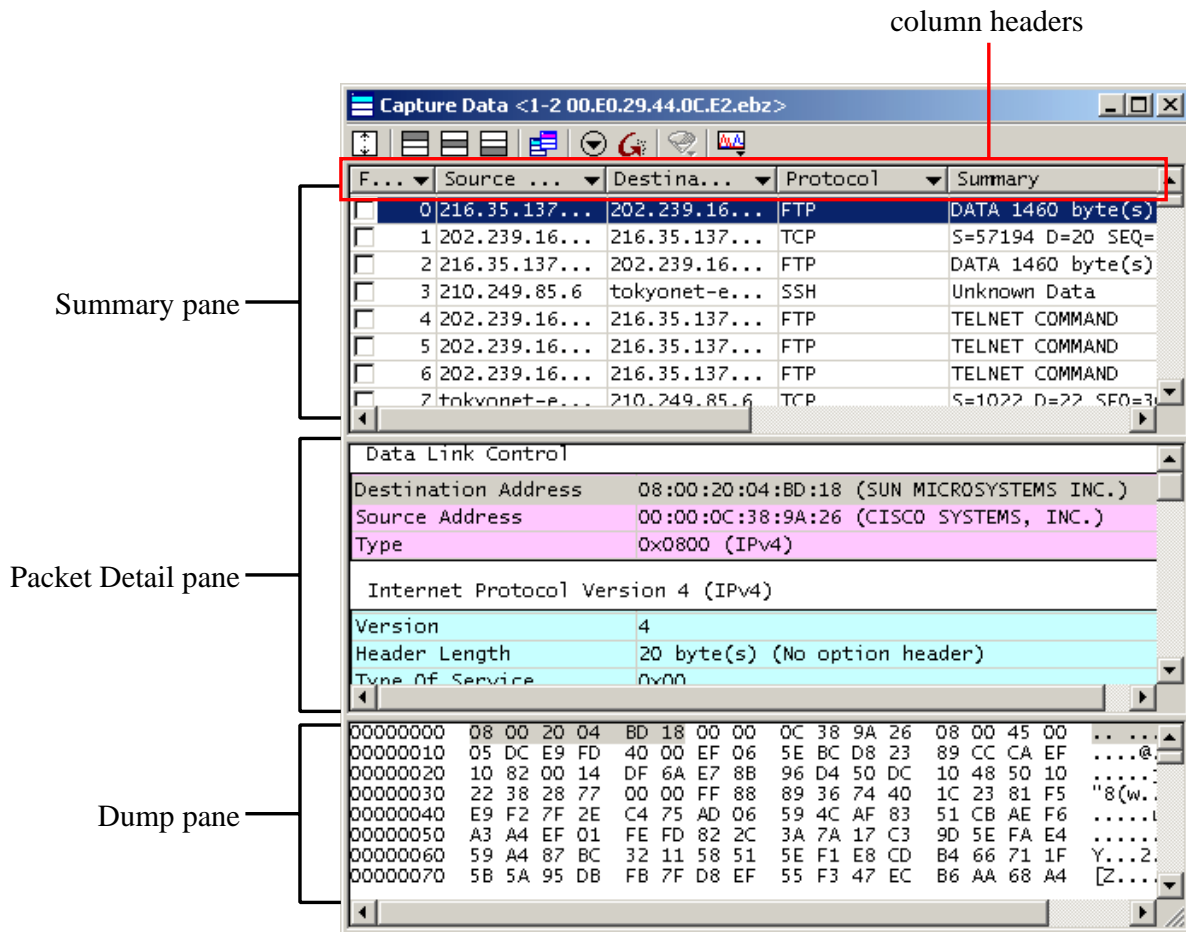


Figure 4-12 Decode view

The decode view has three major panes: the **Summary pane**, **Packet Detail pane**, and **Dump pane**. The Summary pane shows the packet summaries. A row in the Summary pane corresponds to one packet. The Packet Detail pane shows the analysis of the packet selected in the Summary pane. The Dump pane shows the hexadecimal dump of the packet content.

The Summary pane has the following columns:

Frame ID	The ID of the packets. IDs are sequence numbers starting from 0.
Source Addr, Destination Addr	The MAC address for the MAC layer protocol and the IP address for the IP layer protocol. If a host name for the address is known, it will be used instead of the address.
Protocol	The protocol name of the uppermost layer (the layer closest to the application).
Summary	The decode summary of the uppermost layer protocol.
Length	The length of the packet, not including the CRC field on the MAC layer.
Time	The time when the packet was captured.
Relative Time	The time elapsed from when the first packet with ID 0 was captured.
Delta Time	The time elapsed from when the last packet was captured.

To display the decode results, click on the row of your interest in the Summary pane. When you select the row in the Packet Detail pane, the corresponding part in the Dump pane will be shown in gray. Conversely, when you click on the Dump pane, the corresponding row in the Packet Detail pane will be shown in gray.




For the meaning of the fields and the values shown in the Packet Detail pane, refer to the documents defining protocols such as RFCs.



The decode view analyzes the packets one by one and shows the result. Therefore, it is not always possible to correctly analyze the packets containing the fragmented data. In such a case, use the stream view.

Saving Decoded Data into a File

There are two ways to save the decoded data:

- Click the **Save Decoded Packets** button () on the Common toolbar in the Main window.
- Choose **Save Decoded Packets...** from the **File** menu on the menu bar of the Main window.



Trying to close the decode view without saving the data will show an **ASTEC Eyes** dialog box, prompting you to save the data.



Trying to discard the data in the capture buffer which is not yet decoded will show an **ASTEC Eyes** dialog box, confirming you want to discard the data.

Using the Stream View

The stream view reassembles TCP virtual streams from the data shown in the decode view. You can view the protocol data above TCP in the stream view, decoded more precisely in most cases.

There are two ways to open the stream view:


- Click the **Stream View** button () in the decode view.
- Activate the decode view containing the data to be reassembled, and choose **Stream View** from the **Capture** menu on the menu bar of the Main window.

Figure 4-13 shows a stream view.

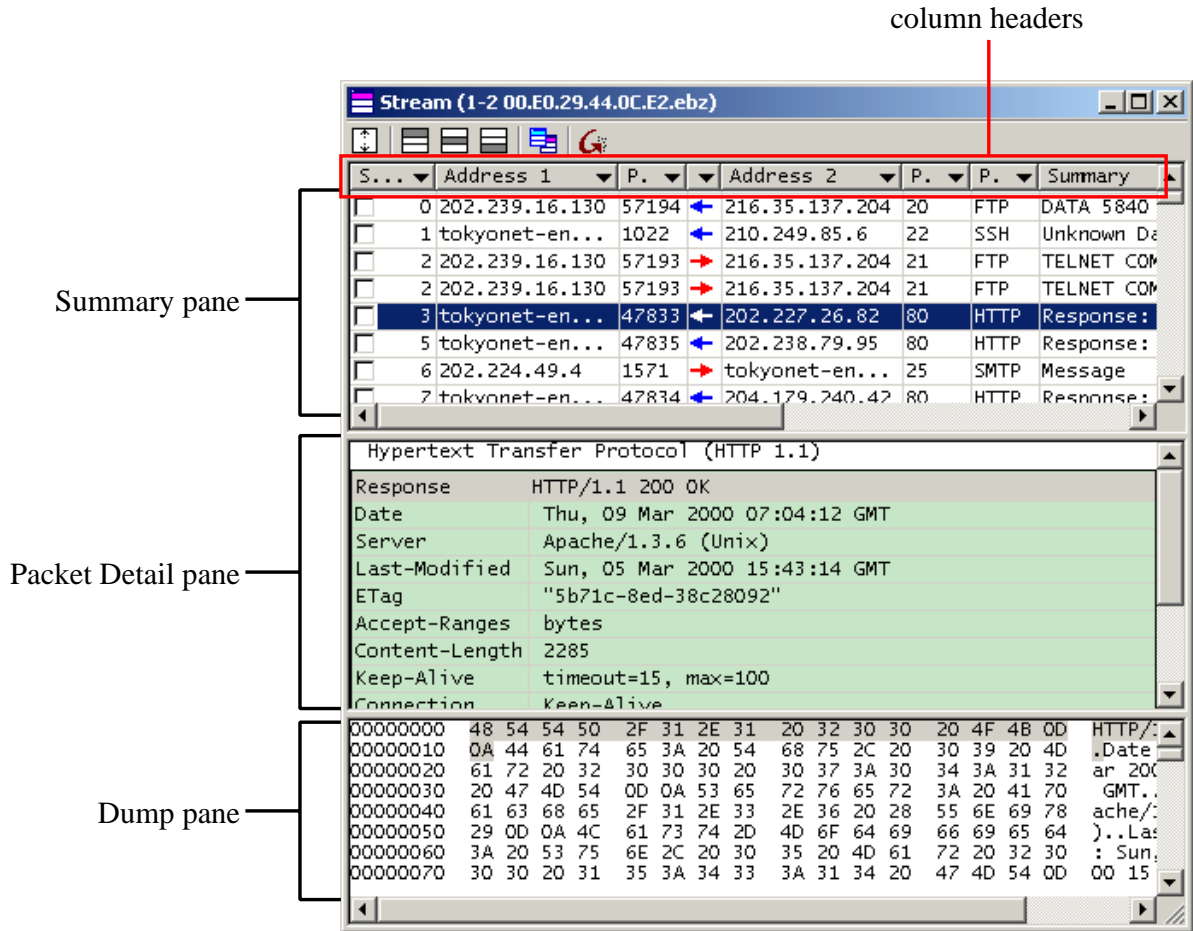


Figure 4-13 Stream view

As with the decode view, the stream view has three major panes: **Summary pane**, **Packet Detail pane**, and **Dump pane**.

A row in the Summary pane corresponds to an application layer record. The Packet Detail pane shows the analysis of the record of the selected row in the Summary pane. The Dump pane shows the hexadecimal dump of the record.

The Summary pane has the following columns:

Stream ID	The ID assigned to each TCP stream.
Address 1 Port 1 Address 2 Port 2	Addresses and port numbers of both ends of the stream.
Direction	The direction of the transmission indicated by an arrow (←, →).
Protocol	The protocol name of the uppermost layer (the layer closest to the application).
Summary	The summary of decode results of the uppermost layer protocol.
Length	The length of the record. The length of protocol headers below the application layer is excluded.
Time	The time when the first packet is captured among those that constitute the record.
Relative Time	The time elapsed from the first row occurrence to the current row occurrence.
Delta Time	The time elapsed from the previous row occurrence to the current row occurrence.

To display the decode results, click on a row in the Summary pane. If you select a row in the Packet Detail pane, the corresponding part in the Dump pane will be shown in gray. Conversely, if you click on the Dump pane, the corresponding row in the Packet Detail pane will be shown in gray.

If you select a record in the Summary pane of the stream view, the packets constituting the record are highlighted in green in the Summary pane of the decode view.

Displaying the Stream Containing a Specific Packet

If you want to extract a stream containing a certain packet:

1. Click on the row for the packet of your interest in the Summary pane of the decode view with the right mouse button.
A popup menu having only one item named **Show Stream View** will appear.

2. Choose **Show Stream View**.

If there is not the corresponding stream view yet, a new stream view with the only stream containing the packet in question will be created.

If the stream view is already created, it shows only the stream containing the packet in question.

In either case, the Stream IDs are shown in blue, which means a filter is applied.









If there is no stream containing the packet (for example, when the transport layer protocol is UDP), all the streams are shown. In this case, however, the Stream IDs are shown in black.







If you know which stream contains the packet, you can obtain the same result by using the caption filter, with which only the records of a specific stream ID will be shown.

Using Toolbars of the Decode View and the Stream View

The decode view and the stream view each comes with a toolbar for your convenience. This section describes the buttons on the toolbars of the decode view and the stream view.

- **Expand** button 
Clicking this button toggles between the following two status.
If all of the three panes, the Summary, Packet Detail, and Dump panes are displayed, the pane with the focus will be expanded to the full window size.
Conversely, if there is only one of them, all of the three panes will be displayed.
- **Summary** button 
Sets the focus to the Summary pane.
- **Packet Detail** button 
Sets the focus to the Packet Detail pane.
- **Dump** button 
Sets the focus to the Dump pane.
- **Stream View** button 
Exists only in the decode view. Activate the corresponding stream view.
- **Decode View** button 

Exists only in the stream view. Activate the corresponding decode view.

- **Header Attribute Filter** button Exists only in the decode view. Shows the menu for the header attribute filter. For further information, see “Header Attribute Filter” on page 119.
- **Discard Filter** button Discards all of the convenience filters currently applied.
- **Display Filter** button Exists only in the decode view. If you click this button, a menu will appear. It shows the names of the existing display filters.
If you choose a filter from the menu, a new decode view will appear. It shows only those packets, which meet the conditions specified in the filter. For more information, see “Display Filter” on page 121.
- **Display Statistics** button Exists only in the decode view. If you click this button, the statistics of the decoded data will be created and displayed as a chart or a table in Monitor windows as with the statistical data of the network traffic.

Key Binds on the Decode View and the Stream View

Key	Summary pane	Packet Detail pane	Dump pane
<TAB> <Shift-TAB>	Moves the focus on the decode view or the stream view among the Summary, Packet Detail, and Dump panes.		
<↑>	Moves the selected position one row up.		Moves toward a lower address.
<↓>	Moves the selected position one row down.		Moves toward a higher address.
<←> <→>	When a horizontal scroll bar is shown, scrolls left or right.		Works in the same way as <↑> and <↓> respectively.
<Alt-↑> <Alt-↓>	Effective only in the decode view. The packets that corresponds to the currently selected record in the stream view are highlighted in green in the Summary pane of the decode view. You can jump back and forth among the highlighted packet with these keys.		
<Page Up>	Moves the selected position one page up.		Moves the displayed area one page up.
<Page Down>	Moves the selected position one page down.		Moves the displayed area one page down.
<Home>	Selects the first row.		Locates the lowest address.
<End>	Selects the last row.		Locates the highest address.
<z>	If all of the three panes of the decode view or the stream view are displayed, the pane with the focus will be expanded to the full window size, and the remaining two panes will be hidden. Conversely, if only one pane is displayed, all of the three panes will be shown.		
<Ctrl-↑> <Ctrl-↓> <Ctrl-Home> <Ctrl-End>	To whichever pane the focus is set, these keys work as <↑>, <↓>, <Home>, and <End> keys in the Summary pane respectively. You can navigate among packets or records without setting the focus to the Summary pane.		
<Ctrl-C>	You can copy the content of the pane, which the focus is set to. The copied content can be pasted to other applications.		

Searching the Decode View or the Stream View for Text

You can search the decode view or the stream view for text independently in each pane (Summary, Packet Detail, or Dump pane).

It is recommended that you search in the Summary pane to find a specific packet.

You can search for text as follows:

1. Set the focus to the pane in which you want to find the text.
2. Choose **F**ind... from the **E**dit menu on the menu bar of the Main window, or press the <Ctrl-F> key.

The **F**ind dialog box will appear. Enter the text you want to search for, and click the **F**ind Next button.

Searching the Dump Pane for Text

The Dump pane is horizontally divided into three regions. The leftmost region is for displaying addresses of the data starting from 0, and is outside the scope of the search. The center region is for displaying the hexadecimal representation of the data. The rightmost region is for displaying the data as a sequence of characters. The latter two regions are within the scope of the search. That is, in the Dump pane, you can specify the text to be searched either using hexadecimal numbers or characters. For example, when searching for the text “Keep”, you can enter “Keep”, “4b656570”, or “4b 65 65 70” into the “Find what” input field of the **F**ind dialog box.



When you try to search for data that cannot be expressed by characters, enter the data in its hexadecimal representation instead.

Selecting Data Displayed in the Decode or Stream View

Sometimes it happens that the packets you want to see are scattered among the huge volume of data. In such a case, you might want to display only those packets of your interest. To do so, use filters.

There are two types of filters for screening packets or records: the **display filter** and the **convenience filter**. The display filter allows the user to display only those packets that meet the condition defined by a logical expression. On the other hand, the convenience filter does not require any logical expression. It allows the user to screen packets or

records easily through the GUI operations only. There are two types of convenience filters: the **caption filter** and the **header attribute filter**.

In the decode view, you can use all the three filters, the display filter, caption filter, and header attribute filter. In the stream view, you can only use the caption filter.

Caption Filter

The caption filter allows you to select from the values shown in the pull-down menu, for each column of the Summary pane of the decode or stream view. These values are the ones from each column and the filter will show only the rows with the selected value.

To use the caption filter, click on the column header in the Summary pane of the decode or stream view.

A menu will appear. Figure 4-14 shows the menu for the **Summary** column. Likewise, Figure 4-15 shows the menu for the **Frame ID** column.

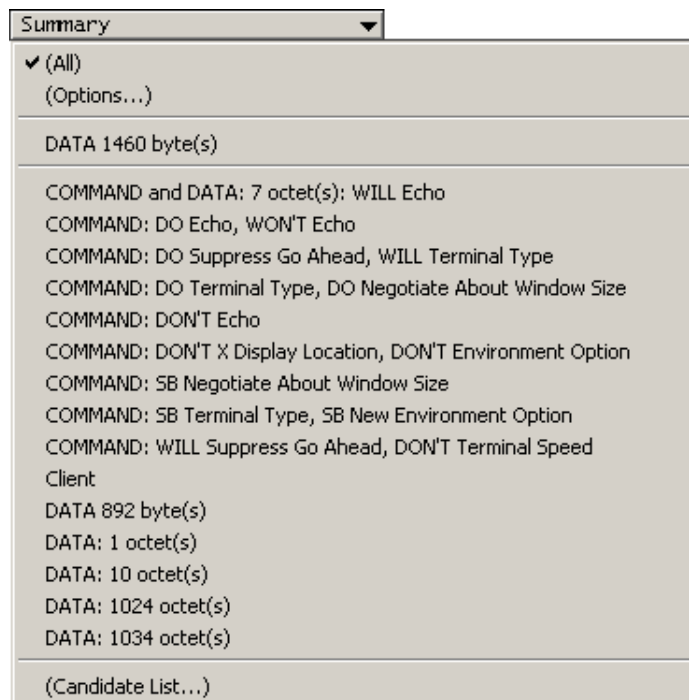


Figure 4-14 The caption filter menu for **Summary**

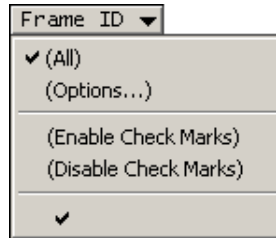


Figure 4-15 The caption filter menu for **Frame ID**

The menu is divided into several regions.

- Menu items **(All)** and **(Options...)** are in the uppermost region. Choosing **(All)** will cancel the caption filter and display all rows. Choosing **(Options...)** will show the **Option** dialog box.
- In the menu for **Frame ID** or **Stream ID**, **(Enable Check Marks)** and **(Disable Check Marks)** appears in the next region. With these items, you can select or clear the check box for all the rows currently shown in the decode or stream view.
- In the next region, the column value of the currently selected row in the Summary pane is placed.
- In the next region, all the distinct values of the column are listed.
- If there are too many items, a menu item **(Candidate List...)** is added.

If you choose an unparenthesized menu item with a column value, only the rows containing the value are displayed.

Choosing **(Options...)** will display the **Option** dialog box as shown in Figure 4-16.

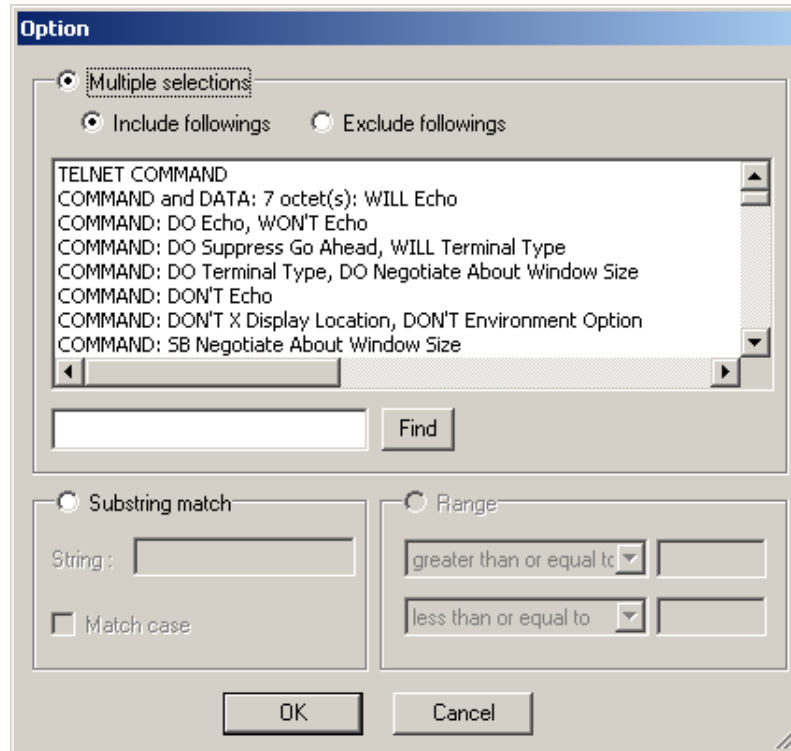


Figure 4-16 **Option** dialog box

With the **Option** dialog box, you can do the followings:

Multiple selections

Allows you to select multiple items and display only those rows whose column value matches one of the selected items. Also allows you to display only those rows that do not contain any of the selected items. You can search the list of items for text.

Substring match

Allows you to type text and display only those rows that include the specified text in the column value.

This operation is not available in the **Option** dialog box invoked from **Frame ID**, **Stream ID**, and **Length**.

Range This operation is available in the **Option** dialog box invoked from **Frame ID**, **Stream ID**, and **Length**. Allows you to specify the range of the values that qualify rows to be displayed.

Choosing (**Candidate List...**) will display the **Candidate List** dialog box as shown in Figure 4-17.

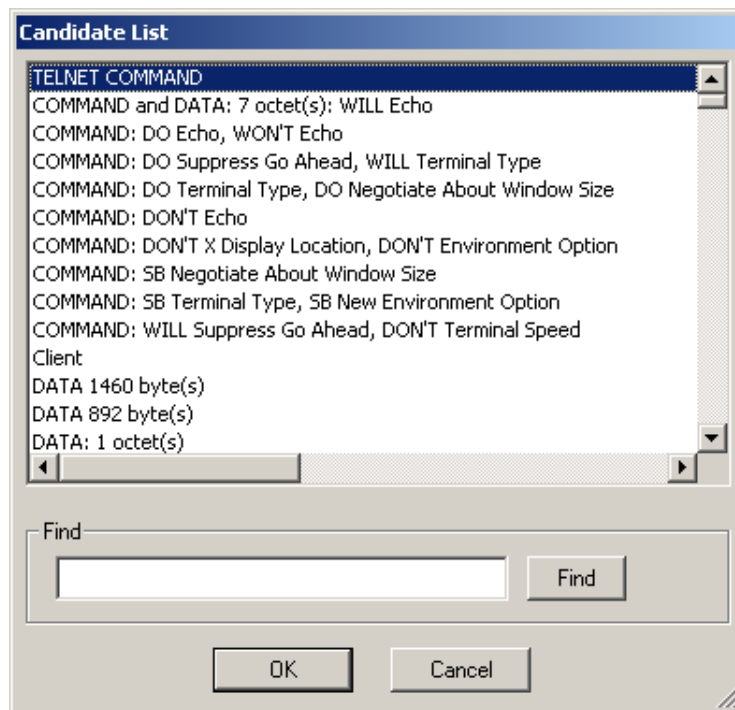


Figure 4-17 Candidate List dialog box

This dialog box allows the user to search the listed values for text. It is convenient when there are too many menu items to search from.

▼ mark is placed to the right of each column header if the caption filter is available for the column. In the decode view, you can use caption filter for the following columns:

- **Frame ID**
- **Source Addr**
- **Destination Addr**

- **Protocol**
- **Summary**
- **Length**

In the stream view, you can use the caption filter for the following columns:

- **Stream ID**
- **Address 1**
- **Port 1**
- **Direction**
- **Address 2**
- **Port 2**
- **Protocol**
- **Summary**
- **Length**

When the caption filter is used, the color of the ▼ mark and the numbers in the **Frame ID** or **Stream ID** column turn blue to indicate that a filter is applied.



If some errors occur at decode time, red check boxes will be added to the popup menu for the **Frame ID** or **Stream ID** column.



You need not click the ▼ mark in order to use the caption filter. Wherever you click on the column header, its popup menu will appear.

Choosing (**Enable Check Marks**) from the menu for the **Frame ID** or **Stream ID** column header, will make the check boxes of all the displayed rows be selected. In addition, ✓ will be added to the menu on the **Frame ID** or **Stream ID** column. If you choose (**Disable Check Marks**), the check boxes of all the displayed rows will be cleared.



You can select or clear the check box not only by clicking on it with the left mouse button, but also by selecting a row with the arrow keys (<↑>, <↓>) and pressing the <Space> key.

Using check marks, you can aggregate the results of multiple filtering.

As an example, the procedure for displaying only the packets whose source or destination is host *111.111.111.111*, is shown as below:

1. Click on the column header **Source Addr**, and choose *111.111.111.111* from the popup menu.
2. Click on the column header **Frame ID**, and choose **(Enable Check Marks)** from the popup menu.
3. Click on the column header **Source Addr**, and choose **(All)** from the popup menu.
4. Click on the column header **Destination Addr**, and choose *111.111.111.111* from the popup menu.
5. Click on the column header **Frame ID**, and choose **(Enable Check Marks)** from the popup menu.
6. Click on the column header **Destination Addr**, and choose **(All)** from the popup menu.
7. Click on the column header **Frame ID**, and choose ✓ from the popup menu.

Header Attribute Filter

The Monitor window displays traffic based upon various attributes of the packet headers. You can also screen packets in the decode view based upon the attributes of packet headers . This function is called the **header attribute filter**.

To use the header attribute filter, click the **Header Attribute Filter** button (▼) on the toolbar of the decode view. A menu with the following items will appear:

- MAC Source
- MAC Destination
- MAC Host Pair
- MAC Protocol
- IP Source
- IP Destination
- IP Host Pair
- IP Protocol

Each of these menu items leads to a submenu, as shown in Figure 4-18.

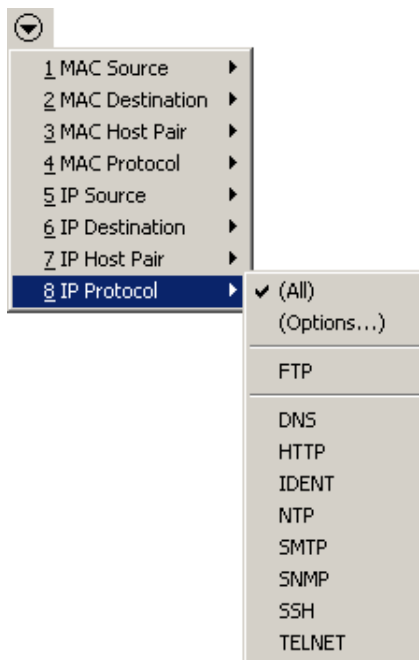


Figure 4-18 A cascaded menus for header attribute filter

This submenu is organized in the same way as the menu of the caption filter. If you choose an unparenthesized menu item for a value type of the header attribute, only the rows containing the selected value type will be displayed.

Choosing **(Options...)** will display the **Option** dialog box. Choosing **(Candidate List...)** will display the **Candidate List** dialog box. For more information, see “Caption Filter” on page 114.


When you apply the header attribute filter, the color of the **Header Attribute Filter** button (▼) and text in the **Frame ID** column turns blue to indicate that a filter is applied.



As with monitoring, the value of the IP layer protocol in the header attribute filter is determined based on the information from the IP, UDP, and TCP headers only. Therefore it might differ from the protocol column value of the decode view that shows the uppermost layer protocol.

Discarding the Configuration of Convenience Filter


By combining convenience filters (caption filter and header attribute filter), you can set complex conditions. To discard a condition, choose **(All)** from the menu you set the condition with.

If you want to discard all of the applied filters at once, click the **Discard Filter** button () on the toolbar of the decode or stream view.

Display Filter

If you want to configure complex conditions that cannot be set by the convenience filter, use the display filter.

You can use the filter editor to configure the display filter. To invoke the filter editor, choose **Filter Editor** from the **Edit** menu on the menu bar of the Main window. For more information, see “Filter Editor” on page 172.

To apply the configured display filter to the decode view, click the **Display Filter** button () on the toolbar of the decode view. A menu will appear. The menu lists the names of the display filters. Choose the name of the filter you want to apply from that menu. Then, a new decode view will appear showing only the packets matching the logical expressions specified in the filter. In this decode view, numbers in the **Frame ID** column will be shown in red.



You cannot use a display filter in the stream view. Create it from the decode view to which the display filter is applied.


Saving Packets Currently Shown on the Decode View

Sometimes we want to save only the packets extracted by the convenience filter or display filter into a file.

In such a case, activate the decode view, and choose **Save Visible Packets...** from the **File** menu on the menu bar of the Main window.

Displaying Statistics of Decoded Data

You can display the statistics of the decoded data in a chart or a table of the Monitor window, just as the statistical data collected from the network.

Click the **Display Statistics** button () on the toolbar of the decode view. A menu

similar to Figure 4-19 will appear.

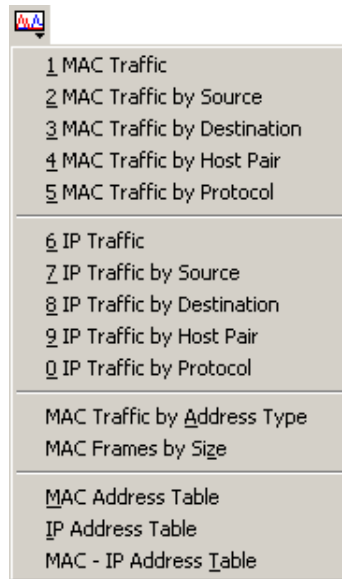


Figure 4-19 Menu for displaying statistics of decoded data

Choosing a menu item will display the corresponding Monitor window or address table.

The data name will be shown in reddish purple as the title of the Monitor window.

You can manipulate this type of Monitor window in the same way as a normal Monitor window that displays traffic statistics.

For example, you can change one display format to another, view the breakdown of the selected Graph Item, and use a popup menu. Basically you can do the same operations as with a normal Monitor window. The exception, however, is that **utilization** in the popup menu of “MAC Traffic” is grayed out and no menu item exists for “MAC Error Frames”.

Decoding Divided Data

A capture file created by tools other than ASTEC Eyes such as “tcpdump” or “snoop” could grow very large. In addition, from ASTEC Eyes version 1.2, you can store the

captured data directly into a file without using the capture buffer, which is called continuous capture. When you use it, there is also a high possibility that a very large capture file will be created.

The larger the file grows, the longer it takes for ASTEC Eyes to decode it and the more memory is required. Therefore it is more convenient to divide the large capture file.

To decode a part of a file, specify the decode range using the **Open with Filter** dialog box, and then decode it.

The procedure is as follows:

1. Choose **Open with Filter...** from the **File** menu on the menu bar of the Main window. The **Open** dialog box will appear.
2. Specify the file name in the **Open** dialog box. The **Open with Filter** dialog box will appear as shown in Figure 4-20.

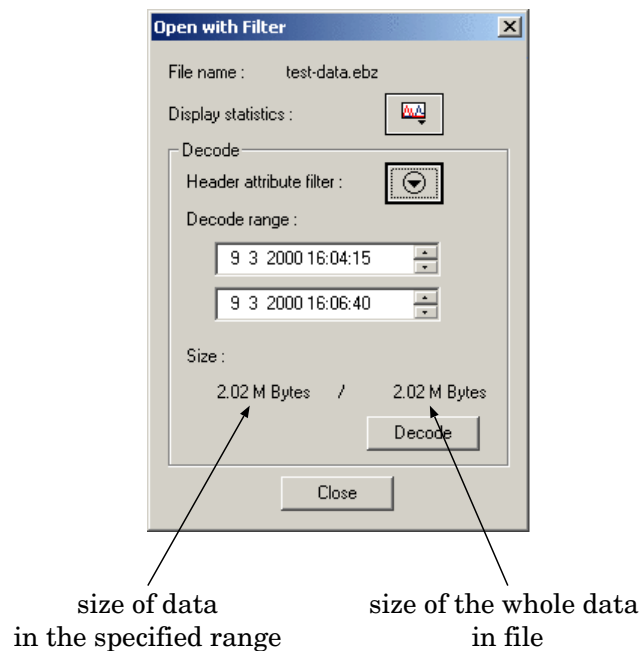







Figure 4-20 **Open with Filter** dialog box

The **Size** shown is not the size of the specified file, but the amount of memory used to load it into ASTEC Eyes.

3. Click the **Display Statistics** button .
The same menu will appear as with the **Display Statistics** button  in the decode view (see Figure 4-19). If you choose the menu item, the corresponding Monitor window or address table will appear.
This operation is not mandatory, but statistics displayed in the Monitor window are a good reference for determining the decode range.
4. Specify the decode range.
Enter the start time of the decode in the upper field and the end time in the lower field. By default, the start time and end time of the whole capture file are set to the upper and lower fields respectively. Specify them by their year, month, day, hour, minute, and second.
As you enter those values, the size of data to be decoded changes dynamically.
5. If you want to limit the packets to be decoded based on the statistics, click the **Header Attribute Filter** button .
The same menu will appear as with the **Header Attribute Filter** button  in the decode view (see Figure 4-18).
You can further extract packets matching specific conditions. Choose the item from the submenu as you do in the decode view.
If you configure the header attribute filter, the color of the **Header Attribute Filter** button  turns blue.
6. Click the **Decode** button.

Only the packets within the specified time range will be decoded and the results shown in the decode view. Numbers in the **Frame ID** column of the decode view will be shown in red to indicate that a filter is applied.



You may change the order of steps 4 and 5. In addition, you can specify the decode range in either one of those two steps.

Saving the Decoded Results

With ASTEC Eyes, you can save the decode results in the decode or stream view into a text file. You can also copy it to the clipboard so that you can paste it into other applications, such as Microsoft Word, Microsoft Excel, WordPad, and Notepad.

The decode results in text format is handy when you want to look through them thoroughly or search through them with other applications.

Saving the Decoded Results into a File

To save the decode results into a file, first activate the associated decode or stream view, and then choose **Save Decoded Results...** from the **File** menu.

The **Save Decoded Results** dialog box will appear, as shown in Figure 4-21.

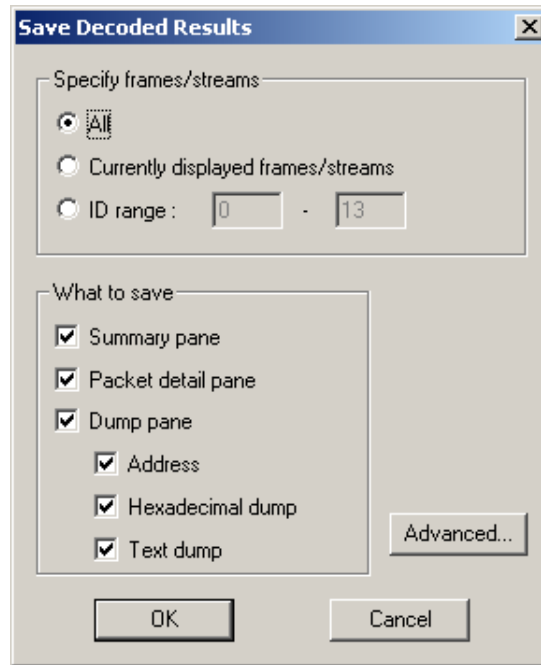


Figure 4-21 **Save Decoded Results** dialog box

Specify the range of the output in the **Specify frames/streams** region. When “**All**” is selected, the entire decode result will be saved regardless of all the filters applied. If you want to save the packets or records screened by the convenience or display filter, select “**Currently displayed frames/streams**”. You can specify the range by frame IDs or stream IDs by selecting “**ID range**”.

Specify the panes whose contents should be saved in the **What to save** region. All panes are selected by default. Clear the check boxes of the panes you do not need to save.

Clicking the **OK** button will display the **Save As** dialog box. Specify the file name.

Clicking the **Advanced...** button will display the **Output Format** dialog box as shown in Figure 4-22.

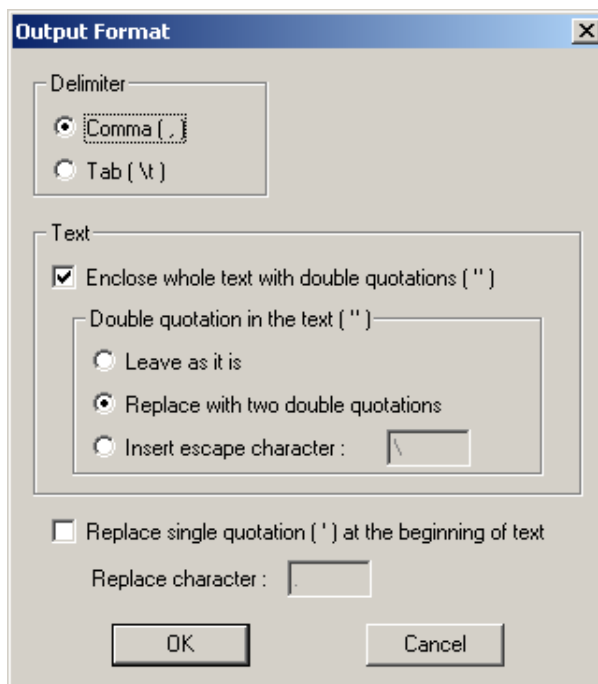


Figure 4-22 **Output Format** dialog box

You can specify the detailed format of the output file in this dialog box.

In the **Delimiter** region, specify the character to be used to as the delimiter between columns. You can select it either **“Comma (,)”** or **“Tab (\t)”**. **“Comma (,)”** is used by default.

In the **Text** region, specify whether or not to double-quote (") the values when writing out the results shown in the Packet Detail and Dump panes, or the following columns of the Summary pane:

- Source Addr
- Destination Addr
- Protocol
- Summary

- Time
- Address 1
- Address 2
- Direction

Values are double-quoted by default. If you do not want to use double quotations, clear the “**Enclose the text with double quotations (")**” check box. If you choose to use double quotations, you need to specify how to deal with double quotations included in the original values. There are following three options:

- Leave as it is (do nothing).
- Replace it with two double quotations in a row.
- Insert an escape character (for example, backslash (\)) before a double quotation.

Select an appropriate option depending on the way you deal with the output file and the tool you use.



If you load the output file into an application such as Microsoft Excel, the result may differ depending on whether each value is enclosed in double quotations or not. Unless you select “Replace with two double quotations”, there is a risk of misinterpretation of a double quotation as delimiter.

Furthermore, specify whether a single quotation (') at the beginning of the value should be replaced by another character or not. It is not replaced by default. If you choose to replace it, you also need to specify the replacement character.



In Microsoft Excel, the leading single quotation (') of a value is treated in a special way: it is kept but not displayed or deleted when the value is saved into a file. In order to prevent this from happening, you can replace it with another character.

Copying the Decoded Results

You can paste the decode result using the copy and paste function. The procedure is as follows:

1. Activate the decode view or the stream view, showing the decode result you want to copy.

2. Select the pane (Summary, Packet Detail, or Dump pane) you want to copy from by clicking on it or using the <TAB> key.
3. Choose **C**opy from the **E**dit menu on the menu bar of the Main window or press the <Ctrl-C> key.
4. Activate the application you want to paste the decode result into.
5. Paste the result into the target application. Typically you can do so by choosing **P**aste from the **E**dit menu or pressing the <Ctrl-V> key.
For applications such as Microsoft Word or Excel, you can choose **P**aste **S**pecial from the **E**dit menu.



You cannot copy the entire results by a single operation. Copy panes one by one.

Error in Decoding Data

If you try to decode data with an incorrect decode hint, or the data itself is erroneous, decoding might fail.

In such a case, the decode and stream views are shown in different way as usual to indicate that an error has occurred. In the decode view, the color of the check box for the packet that could not be decoded in the Summary pane is shown in red. Likewise, in the stream view, the color of the check box for the stream ID of the record with an error is shown in red.

In addition, a message including the frame ID or stream ID of the packet/record that could not be decoded and its protocol name are printed in the Message window of the Main window.

Shown below are messages indicating decode errors:

```
!!! DECODER EXCEPTION [frameid 2467] (0xE0000006 in EVAL_PACKET of FTP) !!!  
!!! DECODER EXCEPTION [frameid 2469] (0xE0000006 in EVAL_PACKET of FTP) !!!  
!!! DECODER EXCEPTION [frameid 2471] (0xE0000006 in EVAL_PACKET of FTP) !!!
```



When an error message is printed, you are recommended to save necessary data (configuration and capture buffer data) and exit ASTEC Eyes. If an error occurs with correct decode hints, please contact ASTEC Eyes support.

Logging

ASTEY Eyes can periodically output statistics of network traffic into a file. This function is called logging. The statistical data written into the file is called the **log**, and the file is called a **log file**.

You can use logging to investigate long-term traffic trends.

Logging is useful to know what time of the day or the week it is when the network traffic is the heaviest, or what protocol is most used during particular period.

Configuring Logging

Logging is disabled by default. You can enable the logging by the following steps:

1. In the Interface Selector window, click on the icon or label of the host for which you want to enable logging with the right mouse button. A popup menu will appear as shown in Figure 4-23.

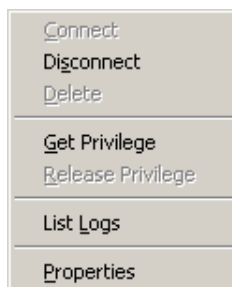


Figure 4-23 Popup menu for a host in the Interface Selector window

2. If you do not have configuration privileges, choose **Get Privilege** first. For details on configuration privileges, see “Actions on a Remote Module” on page 140.
3. Choose **Properties**. The **Host Properties** dialog box will appear.
4. Click on the **Log** tab. The **Log** page will be shown in the dialog box as shown in Figure 4-24.

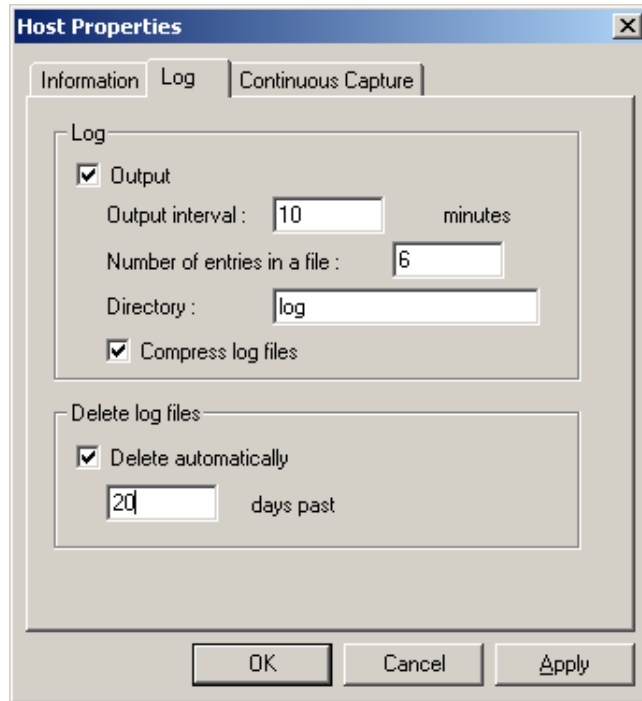


Figure 4-24 Host Properties dialog box showing the Log page

5. Select the “**Output**” check box.
6. Enter **Output interval**.
This is the interval between log outputs. Enter the number of minutes as the interval.
7. Enter **Number of entries in a file**.
Specify how many log entries are to be written into a file.
With ASTEC Eyes version 1.0, each log entry was written into a different file, and whenever the log entry was written all the statistical data were saved.
With ASTEC Eyes version 1.2, multiple log entries can be written into one file. The first log entry contains all the statistical data. From the second entry on, only the difference between the current and previous entries are saved for better performance.
8. Enter **Directory**.
Enter the directory where the log file is created as a relative path to the directory where ASTEC Eyes or the Remote Module is installed.

You need to create the directory by yourself. The directory needs to be under the directory where ASTEC Eyes or the Remote Module is installed.

9. If you want to save the log files with compression, select the “**Compress log files**” check box.

The log files will be compressed by “bzip2”.

10. If you want to delete old log files automatically, select the “**Delete automatically**” check box, and enter the number of days each file should be kept.

The files older than the specified number of the days will be automatically deleted.

11. Click the **OK** button or the **Apply** button.

The log output will start.

If you click the **OK** button, the dialog box will be closed.



Log information can only be displayed after all the entries in one log file are written. Therefore the larger the value for **Number of entries in a file**, the longer it will take before the log data can be displayed.



If you configure ASTEC Eyes to output log files, ASTEC Eyes continues to output them even after you exit the application.

By default, a log file is created for each network interface installed in the host configured to output a log. If you do not want to create a log file for a specific interface, configure it with **Interface Properties** dialog box.

The steps are as follows:

1. In the Interface Selector window, click on the icon or label of the interface for which you want to disable logging with the right mouse button.
2. Choose **Properties** from the popup menu for the interface.
The **Interface Properties** dialog box will appear.
3. Click on the **Log** tab.

The **Log** page will be shown in the **Interface Properties** dialog box as shown in Figure 4-25.

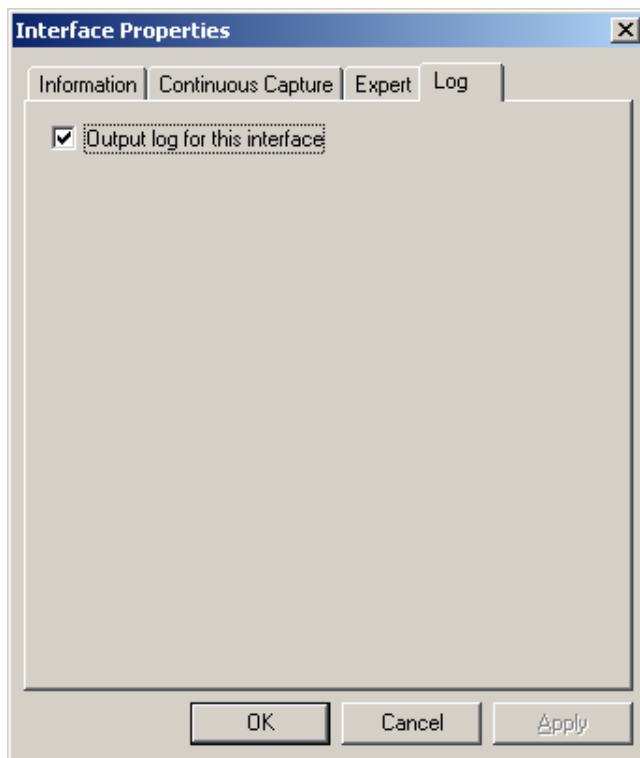


Figure 4-25 Interface Properties dialog box (log)

4. Clear the “Output log for this interface” check box.

Displaying Logs

Depending on the location where the log files are kept, the steps to display logs are slightly different.

If the log files are located under the directory ASTEC Eyes or the Remote Module is installed, the chart or table showing the log will be updated as the log is being written.

Displaying the log under the directory where ASTEC Eyes or the Remote Module is installed:

1. Click on the icon or label of the host with the right mouse button in the Interface Selector window.

A popup menu will appear as shown in Figure 4-23.

2. Choose **List Logs**.

The analysis of the log files, which are saved under the directory specified from the **Log** page of the **Host Properties** dialog box (see Figure 4-24), will start. While the log files are being analyzed, a dialog box showing the progress is displayed.

As soon as the analysis is done, the icon and label for the log will appear in the Interface Selector window, as shown in Figure 4-26.

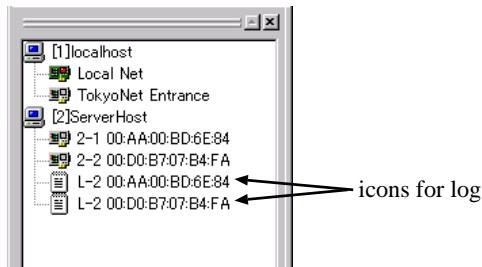


Figure 4-26 Interface selector window showing icons for log

The analyzed logs are classified by the network interfaces. An icon is displayed for each network interface in the Interface Selector window.

Displaying the log under the specified directory:

1. Choose **Open Log Directory...** from the **File** menu on the menu bar of the Main window.

The **Open Log Directory** dialog box will appear.

2. Specify the directory in the **Open Log Directory** dialog box.

In the Interface Selector window under the localhost, a folder and icons representing the directory and the log files respectively will appear as shown in Figure 4-27.

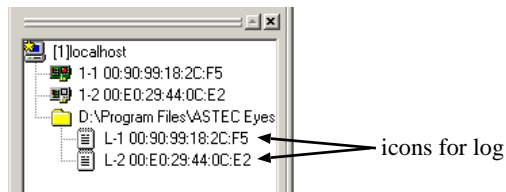


Figure 4-27 Interface selector window showing a folder and icons for a log

The following steps apply to both cases:

3. Click on the icon or label for the log file shown in the Interface Selector window with the right mouse button.
A popup menu will appear as shown in Figure 4-28.

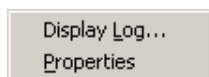


Figure 4-28 Popup menu for log

4. Choose **Display Log...**
The **Displaying Log** dialog box will appear as shown in Figure 4-29.

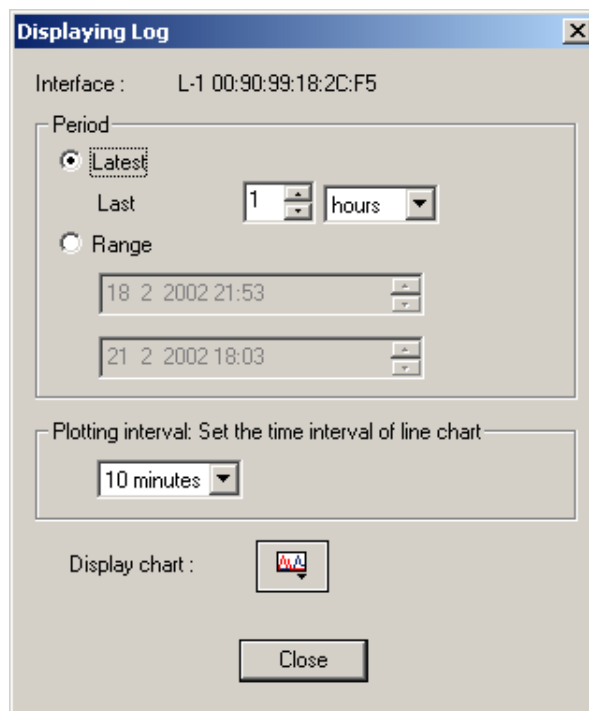


Figure 4-29 Displaying Log dialog box

5. Specify the period to be covered and the plotting interval in the **Displaying Log** dialog box.

Choose **Latest** or **Range** in the **Period** region. If you choose **Latest**, specify the duration.

If you choose **Range**, specify the start and end times. There are five subfields for year, month, day, hour, and minute in each time field. Clicking on one of the subfields will highlight the subfield in blue. Enter the value there.

The value can be increased or decreased by pressing the <↑> or <↓> key, or clicking buttons at the right edge of the time field.

In the **Plotting interval** region, choose an interval for plotting data for a line chart from the drop down list.

6. Click the **Display Chart** button .

A menu will appear showing the types of traffic as menu items. Choose the one you want to display in a chart. You can also display the list of IP or MAC addresses recorded in the log file.



If you display a log in a directory where ASTEC Eyes or the Remote Module is installed, all the log files in the directory are analyzed at once, regardless of whether the interface associated with the log is currently installed or not.



If you specify the directory to display the log, you can display the log file created by ASTEC Eyes version 1.0. In that case, however, it may take longer since the file needs to be converted from the old format.

Displaying Information on the Network Interface Card

Choosing **Properties** from the popup menu shown in Figure 4-28 will display the **Log Properties** dialog box as shown in Figure 4-30.

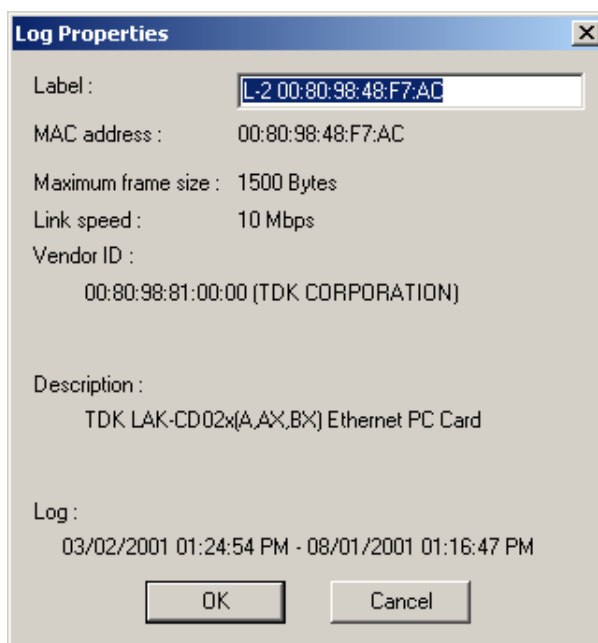


Figure 4-30 **Log Properties** dialog box

The information on the network interface card that collected the log data is shown in this dialog box. As with a network interface, you can change the label to make it easily identifiable.

Remote Watching

The Remote Module, available since ASTEC Eyes version 1.2, has the same functionalities as these of ASTEC Eyes: watching the network, collecting the statistics, capturing the packets and writing the logs.

You can monitor a remote network as you monitor the local network, through the Remote Module connected to ASTEC Eyes at hand.

ASTEC Eyes includes all the functionalities of a Remote Module. So you can connect local ASTEC Eyes to ASTEC Eyes installed on other PCs as Remote Modules.

When Remote Modules are connected, their interfaces, and their status are shown in the Interface Selector window. You can use Remote Modules and their interfaces primarily through the Interface Selector window.

Connecting to Remote Modules

To watch a remote network, first connect the local ASTEC Eyes to a Remote Module on the PC in the remote network. The steps are as follows:

1. Choose **Connect Remote...** from the **File** menu on the menu bar of the Main window.

OR

1. Click on an open space in the Interface Selector window with the right mouse button. A popup menu will appear as shown in Figure 4-31.

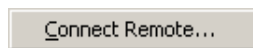


Figure 4-31 Popup menu in the Interface Selector window

Choose **C**onnect Remote....

2. The **Connect** dialog box will appear as shown in Figure 4-32.

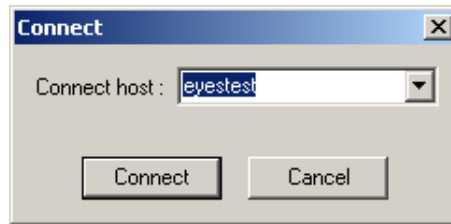


Figure 4-32 **Connect** dialog box

Enter the name of the host running a Remote Module or ASTEC Eyes into the **Connect host** field. You can also choose from drop down list of the host names known to ASTEC Eyes.

For a **Connect host** name, specify a host name the local PC can recognize such as a NetBIOS name, a DNS name, an IP address, and so forth.

3. Click the **Connect** button.

When the connection to the Remote Module on the specified host is established, the host name and its interface entries will appear in the Interface Selector window.



ASTEC Eyes connects to a Remote Module using port 8887 of TCP protocol.

If the specified host is not found, an **ASTEC Eyes** dialog box will appear as shown in Figure 4-33.

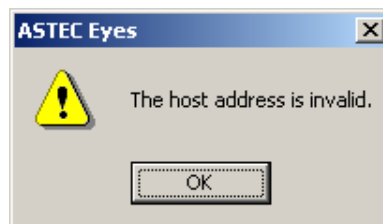


Figure 4-33 Dialog box shown when the host is not found

If a connection attempt to the Remote Module on the specified host fails, an **ASTEC Eyes** dialog box will appear as shown in Figure 4-34.

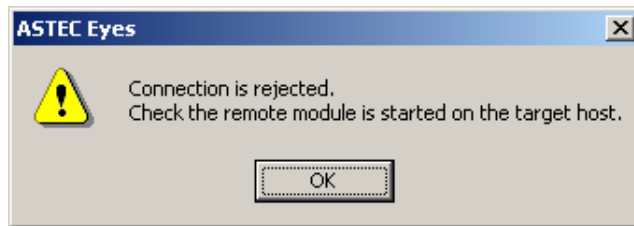


Figure 4-34 Dialog box shown when a connection attempt to the Remote Module fails

Actions on a Remote Module

To perform actions such as disconnecting from and reconnecting to a Remote Module, you can use a popup menu for the host in the Interface Selector window.

If you click on the icon or label of the host in the Interface Selector window with the right mouse button, a popup menu will appear as shown in Figure 4-35.

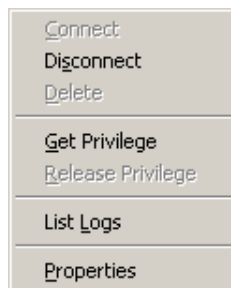


Figure 4-35 Popup menu for the host

By choosing a menu item, you can do the following actions for the host.

Connect

Reconnects to a disconnected Remote Module. When the connection is established, the **Cross Mark** icon (X) will disappear.

Disconnect

Disconnects from a Remote Module. Once disconnected, monitoring,

capturing, and displaying logs are unavailable. The **X** mark is overlaid with the icon of the host and its interfaces.

Delete


Deletes the entries of disconnected Remote Modules from the Interface Selector window.

Get Privilege

Obtains the privileges to configure the interface properties of the host.

You can obtain the privileges only when any other currently-running ASTEC Eyes has not yet obtained them.


For the `localhost`, ASTEC Eyes automatically tries to obtain the configuration privileges at startup time.

If the privileges are successfully obtained, the icon shown in the Interface Selector window changes to the **host with privileges** icon ().

For a complete discussion of interface properties, see “Interface Properties Dialog Box” on page 143.

Release Privilege

Releases the privileges of the network interface of a host so that other ASTEC Eyes can obtain them.

If you release the privileges, the icon shown in the Interface Selector window, changes to the **host** icon (.

List Logs

Analyzes the log files in the directory specified in the **Log** page of the **Host Properties** dialog box. For further information, see “Logging” on page 129.

Properties

Opens the **Host Properties** dialog box.

Host Properties Dialog Box

Choosing **Properties** from the popup menu of the host will display a **Host Properties** dialog box as shown in Figure 4-36.

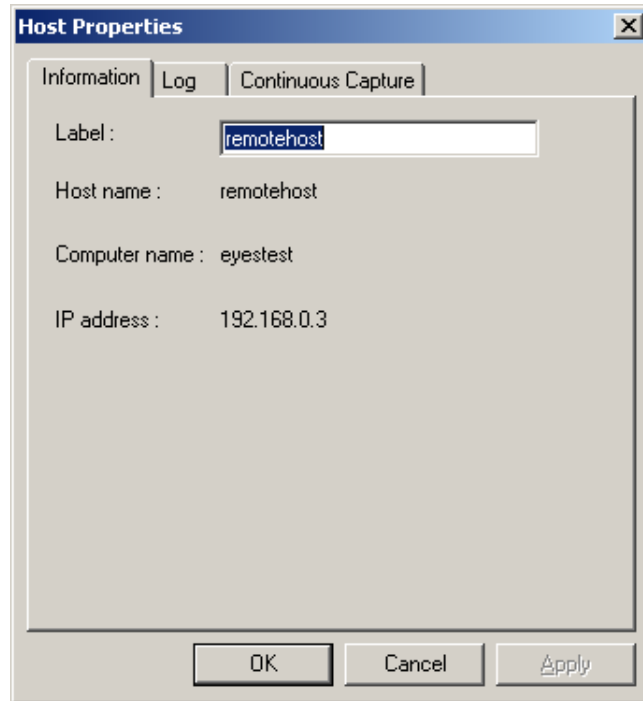


Figure 4-36 Host Properties dialog box

In this dialog box, you can configure the following host properties:

- **Information** page

The host name, the computer name, and the IP address are shown here. The host name is the one used for establishing the connection. The computer name is the one to identify Remote Module. You can specify a label for the host.

- **Log** page

Configure logging, such as whether or not to output the log, delete log files automatically, and so on. For a complete discussion of logging, see “Logging” on page 129.

- **Continuous Capture** page

Configure continuous capture, such as the maximum file size of the capture data, and the directory the file is saved. For a complete discussion of continuous capture, see “Continuous Capture” on page 99.

In the **Directory** field, enter the directory where the file is to be saved. Specify it

by the relative path to the directory in which ASTEC Eyes or the Remote Module is installed. You need to create the directory by yourself.

The directory needs to be a subdirectory of the directory where ASTEC Eyes or the Remote Module is installed.

Actions on Remote Module Interfaces

To perform actions on an interface associated with the Remote Module, use the popup menu for the interface in the Interface Selector window.

If you click on the icon or label of the interface in the Interface Selector window with the right mouse button, a popup menu will appear as shown in Figure 4-37.

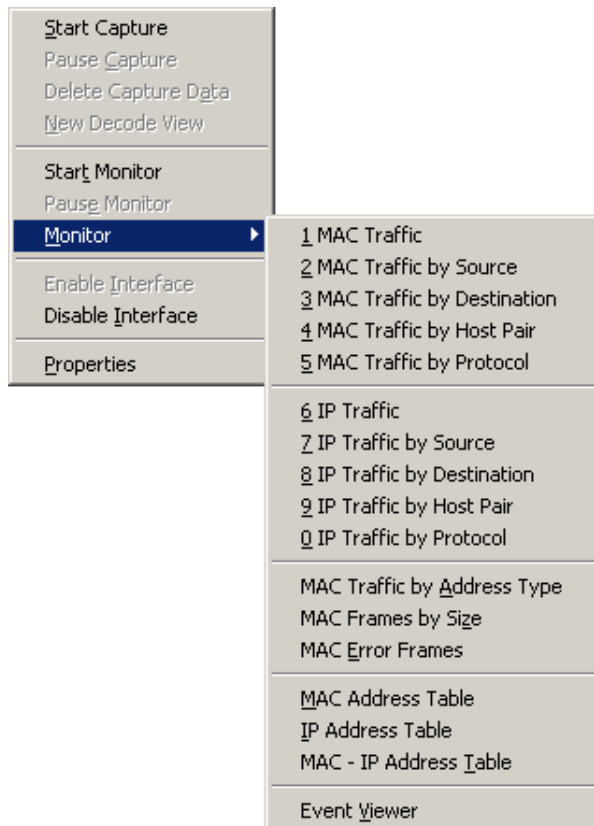


Figure 4-37 Popup menu for an interface in the Interface Selector window

By choosing a menu item, you can do the following actions on an interface:

Start Capture Starts capture.

Pause Capture Pauses capture.

Discard Capture Data

Discards captured data in the capture buffer.

New Decode View

Decodes the data in the capture buffer and shows the decode view.

Start Monitor Starts monitoring.

Pause Monitor Pauses monitoring.

Monitor

Opens the submenu with the same menu items as the **Monitor** menu on the menu bar of the Main window. Choosing an item from the submenu will display the corresponding Monitor window.

Enable Interface

Enables interfaces. You can choose this item only when you have the configuration privileges. For further information, see “Actions on a Remote Module” on page 140.

Disable Interface

Disables interfaces. You can choose this item only when you have the configuration privileges. For further information, see “Actions on a Remote Module” on page 140.

Properties

Opens the **Interface Properties** dialog box.

Interface Properties Dialog Box

Choosing **Properties** from the popup menu for the interface will display the **Interface Properties** dialog box as shown in Figure 4-38.

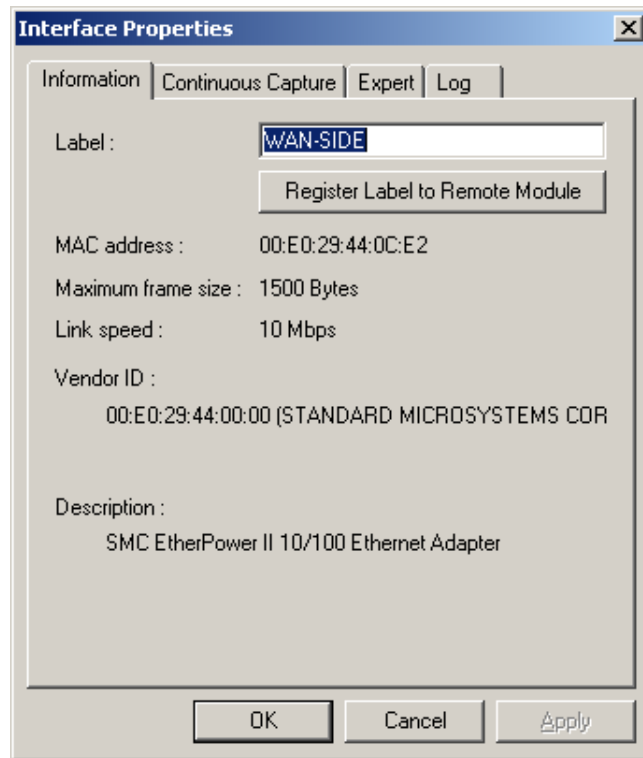


Figure 4-38 Interface Properties dialog box (information)

You can configure the interface properties in this dialog box, when you have the **configuration privileges**. To obtain the configuration privileges, use the popup menu for the host in the Interface Selector window. For more information, see "Actions on a Remote Module" on page 140.

- **Information** page

The information about the network interface card such as **MAC address**, **Maximum frame size**, **Link speed**, **Vendor ID**, and so forth is shown, here. You can specify a name to identify the host for your convenience in this page.

If you have the configuration privileges, you can register the label for the Remote Module so that the same name will be used when you invoke ASTEC Eyes again after exiting or connect ASTEC Eyes to the Remote Module again after disconnecting.

If you do not register the label by clicking the **Register Label to Remote Module** button, the label will not be kept after you disconnect from the Remote Module.

- **Continuous Capture** page

In this page, you can configure the options for capturing data continuously and saving it into files. For a complete discussion of saving the capture data into files, see “Continuous Capture” on page 99.

- **Expert** page

The symptoms of network trouble that can be detected by ASTEC Eyes are listed here. Select the symptoms you want to detect. For further information, see “Reporting Expert Events” on page 146.



This dialog box can be shown by double-clicking on the icon or label of the target interface in the Interface Selector window, too.



You do not need to have the configuration privileges to change the interface label temporarily.



ASTEC Eyes version 1.2 supports the plug and play of network interface cards. When a network interface card supporting plug and play is installed or uninstalled, ASTEC Eyes or the Remote Module automatically detects the change and updates the display in the Interface Selector window.

Reporting Expert Events

Symptoms of network trouble can be detected while monitoring.

ASTEY Eyes version 1.2 can report the following events:

- TCP flag NULL
Detects packets with all the bits in the flags field cleared.
- TCP flag MAX (Xmas scan)
Detects packets whose URG, ACK, PSH, RST, SYN, and FIN bits in the flags field are all set.
- TCP connection refused
Detects a RST packet in response to a SYN packet to establish a TCP connection.
- TCP connection reset
Detects a RST packet excluding TCP connection refused case.
- TCP SYN retransmission
Detects SYN packets with the same sequence number.
- TCP close retransmission
Detects the retransmission of FIN packets.
- TCP retransmission
Detects the retransmission of TCP packets in general.
- TCP window frozen
Detects that the window size has been smaller than 576 bytes for the specified period of time.
- TCP window overflow
Detects packets containing the data larger than the recipient's window.
- TCP long ack time
Detects an ACK packet not received within the specified period of time.
- TCP fragmented TCP data
Detects TCP packets are fragmented in the IP layer.
- TCP checksum error
Detects a packet with an incorrect checksum.
- TCP ack flag not set
Detects a packet with the ACK bit in the flags field cleared, excluding SYN packets transmitted first.

- UDP checksum error
Detects packets with an incorrect checksum.
- IP fragment timeout
Indicates that some IP fragments are not delivered within a certain time span.
- IP fragment error
Indicates an IP packet cannot be reassembled properly.
- IP wrong header
Detects packets with IP header length less than 20 bytes.
- Small IP length
Detects packets with IP header shorter than indicated in the header length field.
- IP header checksum error
Detects packets with an incorrect checksum.
- Invalid IP length
Detects IP packets shorter than indicated in the total length field.
- IP version mismatch
Detects packets with versions other than 4.
- Duplicate IP addresses
Detects an IP address assigned to more than one MAC address.
- MAC byte threshold over
Detects that the number of bytes per second measured at MAC layer has exceeded the specified threshold.

Configuring Expert Events

All the expert events are reported by default.

You can specify events you do not need to detect, and specify threshold values for “MAC byte threshold over”, “Long Ack Time”, and “Frozen Window Time”.

The configuration should be done for each interface. The steps to configure expert events are as follows:

1. Click on the icon or label of the target interface in the Interface Selector window with the right mouse button.
The popup menu for the interface will appear.
2. Choose **Properties** from the menu.
The **Interface Properties** dialog box will appear.

3. Click on the **Expert** tab.

The **Expert** page will be shown in the **Interface Properties** dialog box, as shown in Figure 4-39.

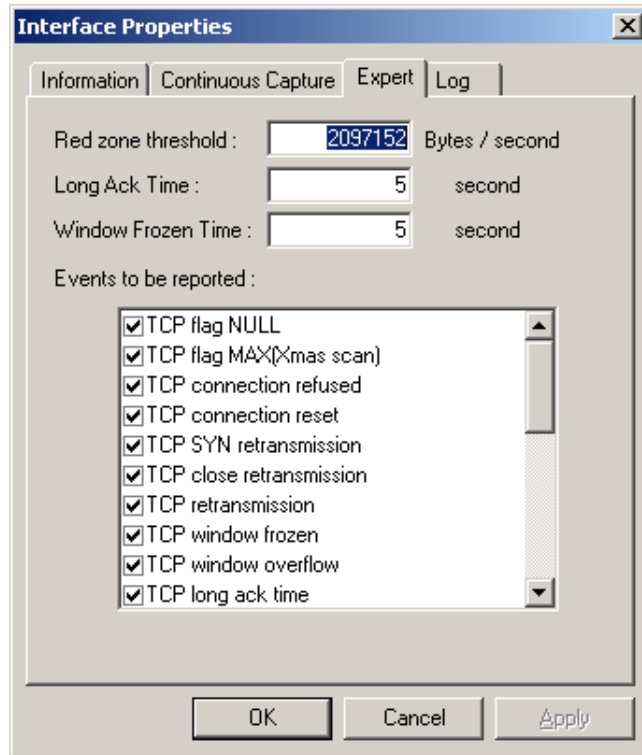


Figure 4-39 **Interface Properties** dialog box showing the **expert** page

4. In the “Events to be reported” scrolled window, select the events to be reported, and clear the events to be ignored.
 - Enter a value for the **Red zone threshold** when “MAC byte threshold over” is selected.
 - Enter a value for **Long ack time** when “TCP long ack time” is selected.
 - Enter a value for **Window frozen time** when “TCP window frozen” is selected.
5. Click the **OK** or **Apply** button.

Displaying Reported Events

The steps to display the detected expert events are as follows:

1. Select the target interface.
Use the Interface Selection listbox (1-1 00:50:8B:4D:F2:D2) or click on the icon or label of the interface in the Interface Selector window.
2. Choose **Event Viewer** from the **Monitor** menu on the menu bar of the Main window.

OR

1. Click on the icon or label of the interface in the Interface Selector window with the right mouse button.
The popup menu for the interface will appear.
2. Choose **Event Viewer** from the **Monitor** submenu in the popup menu. The Event Viewer window will appear as shown in Figure 4-40.

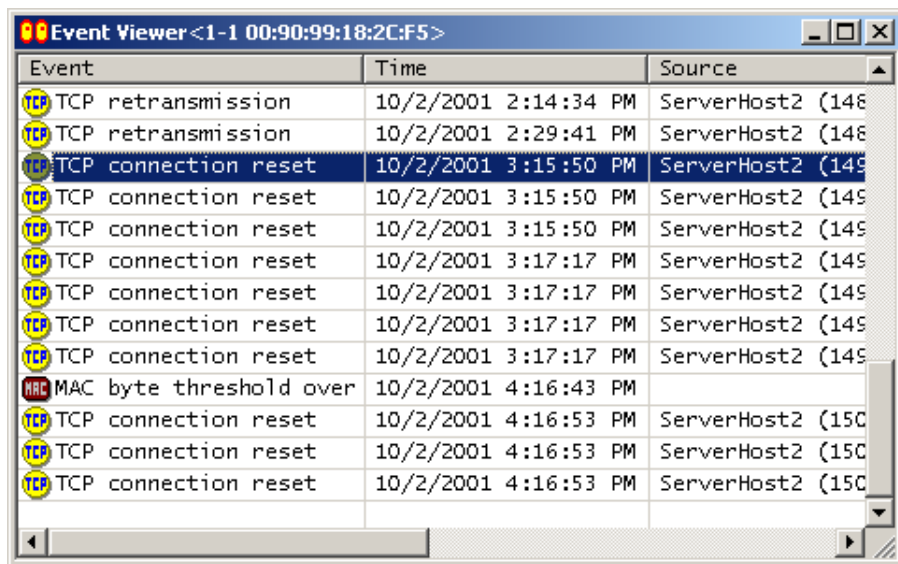





Figure 4-40 Event Viewer window

 denotes an MAC protocol related event.

 denotes an IP protocol related event.

 denotes a UDP protocol related event.

 denotes a TCP protocol related event.

The **Event** column shows the event type.

The **Time** column shows the time the events were detected.

The **Source** and **Destination** columns show the IP addresses of the host and UDP/TCP port number if applicable.

The **Information** column shows event type specific information as described in the table below if applicable.

Events	Information Displayed
TCP retransmission	The length of TCP data
TCP window frozen TCP long ack time	The last ACK time
TCP checksum error UDP checksum error	The incorrect checksum in the packet and its calculated and correct checksum
IP version mismatch	The version number in the packet
Small IP length	The header length in the IP header and the actual header length
Invalid IP length	The total length in the IP header and the actual packet length

Configuring Options

To configure options, choose **C**onfigure... from the **O**ptions menu on the menu bar of the Main window. The **C**onfigure **O**ptions dialog box will appear.

Configure **O**ptions dialog box contains the following six property pages:

- Capture
- Decode Hints
- Display Host Name
- Monitor
- Chart Defaults
- Other

Click on the tab for the property you want to configure, and the corresponding page will be shown. Make the changes as you need.

After making all the changes you want, click the **A**pply or **O**K button. All the changes you made will be applied at once. Clicking the **O**K button will close the **C**onfigure **O**ptions dialog box, too.



Depending on the operating system you are using, the look and feel of each page might differ slightly.



You can save the configuration into a file. For more information, see “Saving a Configuration” on page 164.

Configuring Capture Options

The page for configuring capture options is shown in Figure 4-41.

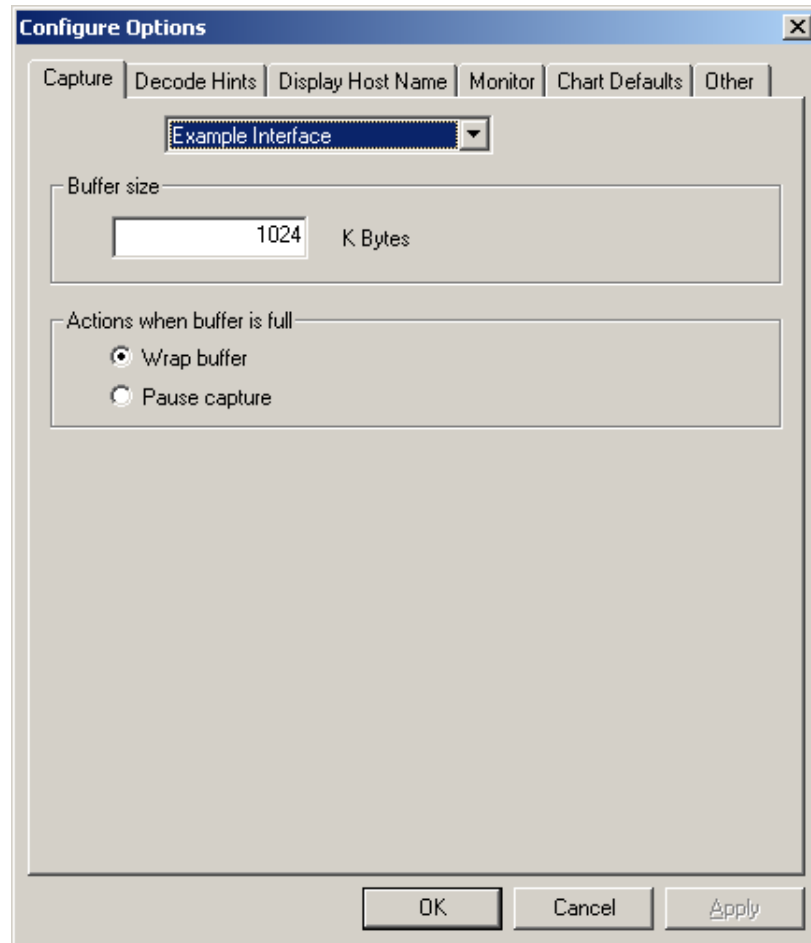


Figure 4-41 **Configure Options** dialog box (capture)

Capture options need to be configured for each interface. First, select a target interface from the drop down list. Then, specify the buffer size and the action when the buffer becomes full.

Buffer size Specifies the capture buffer size in K bytes (1024 bytes). The default size is 1024 K bytes.

Actions when buffer is full

Specifies the action to be taken when the buffer becomes full.

If **Wrap around** is selected, the buffer will be wrapped around; the oldest data will be discarded and the newly captured data will be copied into the buffer.

If **Pause capture** is selected, capture will be stopped automatically.



In ASTEC Eyes version 1.2, the minimum buffer size is 2K bytes, and the maximum is one fourth (1/4) of the physical memory of the PC with ASTEC Eyes or the Remote Module installed.

Configuring Decode Hints

ASTEC Eyes cannot always identify the protocols transmitted using the ports other than the standard ones (well-known ports), e.g., when a proxy server or an ephemeral port is used. ASTEC Eyes shows these protocols as “Unknown TCP Protocol” or “Unknown UDP Protocol” in the Monitor window. The capture data for such protocols cannot be analyzed correctly.

To cope with this situation, configure decode hints.



You can configure the decode hints only for the protocols above the TCP or UDP layer.

Click on the **Decode Hints** tab in the **Configure Options** dialog box.

The page for decode hints configuration is shown in Figure 4-42.

mouse or IP address cell, if the arrow keys are used, will have a white frame.

2. Click on the cell you want to enter the data. The cell will become ready for editing. If you are using the keyboard and there is no cell in edit mode, move the white frame to the cell using the <←> or <→> key, and then press the <F2> key. If there is a cell in edit mode, move the white frame to the cell you want to edit with the <TAB> or <Shift-TAB> key.
3. Enter the value.
4. Repeat steps 2 and 3 until you finish entering all the values.

The **IP Address** column has a combo box. In its drop down list, there is an item named **Any**. If you want to apply a decode hint to all the IP addresses, choose **Any**. If you want to apply it to a specific IP address, enter the IP address.

Choose one of **UDP**, **TCP**, or **UDP or TCP** from the drop down list for the **Transport** column.

Enter the port number to the **Port** column.

The **Protocol** column has a combo box. In its drop down list, application protocols supported by ASTEC Eyes version 1.2 are listed. Choose a protocol from the list, or type a protocol name that is not listed.

In the example shown in Figure 4-42, packets using TCP port 8080 of any host are decoded and displayed as HTTP protocol data.

You can delete a decode hint by the following steps:

1. Click on the decode hint row you want to delete, or select the row using the <↑> or <↓> key. The selected row will be highlighted in blue.
2. Click the **Delete** button or press the <Delete> key.

Sometimes both the source and destination ports are “well-known ports”. The protocol is judged by the direction in which the packet captured first was sent.

For example, suppose DNS packets are transmitted between TCP port 53 (DNS) and 1080 (SOCKS). If the packet captured first was sent from 1080 to 53, ASTEC Eyes decides that they are SOCKS packets.

You can avoid this by configuring decode hints.

In this example, it is appropriate to configure a decode hint so that a combination of a specific address, transport layer protocol TCP, and port 53 implies DNS.

On the other hand, a decode hint that implies a combination of a specific address, transport layer protocol TCP, and port 1080 implies DNS would be inappropriate.

Configuring Host Name Preference

You can use a host name instead of an IP address to identify a host in the IP layer Monitor window, the decode view, and the stream view. ASTEC Eyes searches for a host name for you using the name services: DNS, WINS, and NIS. You can also assign any name to an IP address for yourself.

ASTEC Eyes allows the user to use more than one name service simultaneously for searching. Therefore you want to specify the preference in the host names given by different name services.

Click on the **Display Host Name** tab of the **Configure Options** dialog box.

The page for configuring the use of host names is shown in Figure 4-43.

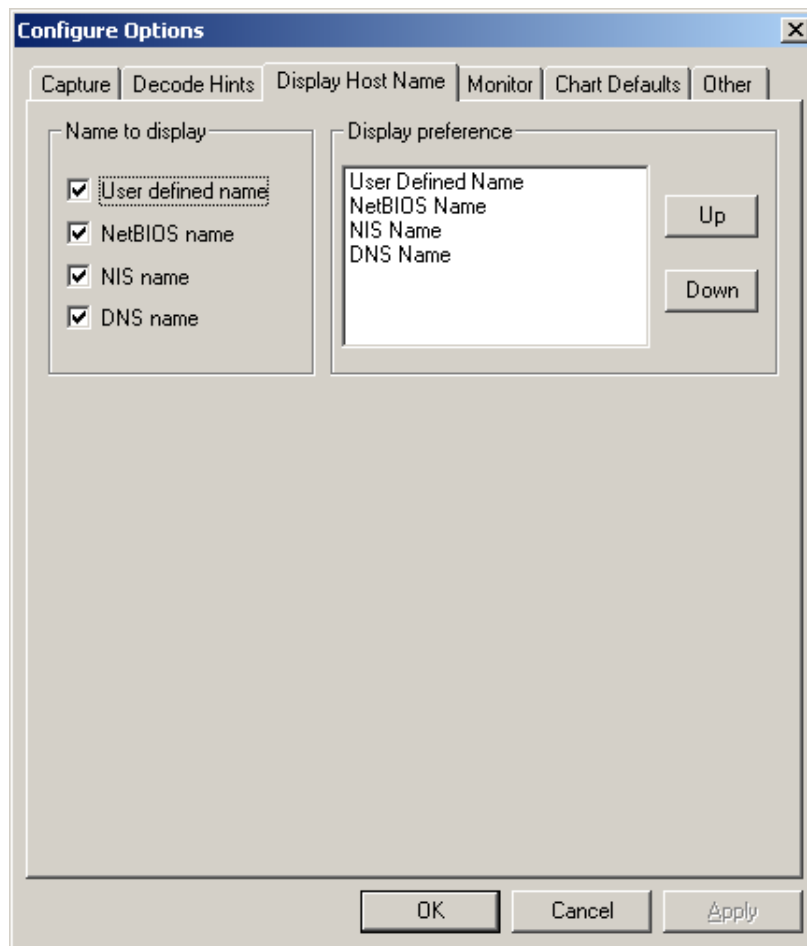


Figure 4-43 **Configure Options** dialog box (display host name)

Select the services you want to use in the **Name to display** region. Only selected name services appear in the **Display preference** region.

All name services are selected by default and the following default order of the preference is set:

1. User defined name
2. NetBIOS name
3. NIS name
4. DNS name

If you want to change the order of the preference in name services, select a name service in the **Display preference** region. Click the **Up** or **Down** button to raise or lower the position of the selected name service.



If you disable all the name services in the **Name to display** region, IP addresses will be used.



The **Configure Options** dialog box for host name preference can be opened from the **Searching for Host Name** dialog box and the edit window of the IP address book. For a complete discussion of the IP address book, see “Editing an Address Book” on page 193.



You can specify a **User defined name** in the address books. By editing the address books, you can assign a desired host name to an IP or MAC address. For more information, see “Editing an Address Book” on page 193.

Configuring Monitor Options

Click on the **Monitor** tab of the **Configure Options** dialog box.

The page for configuring monitor options is shown in Figure 4-44.

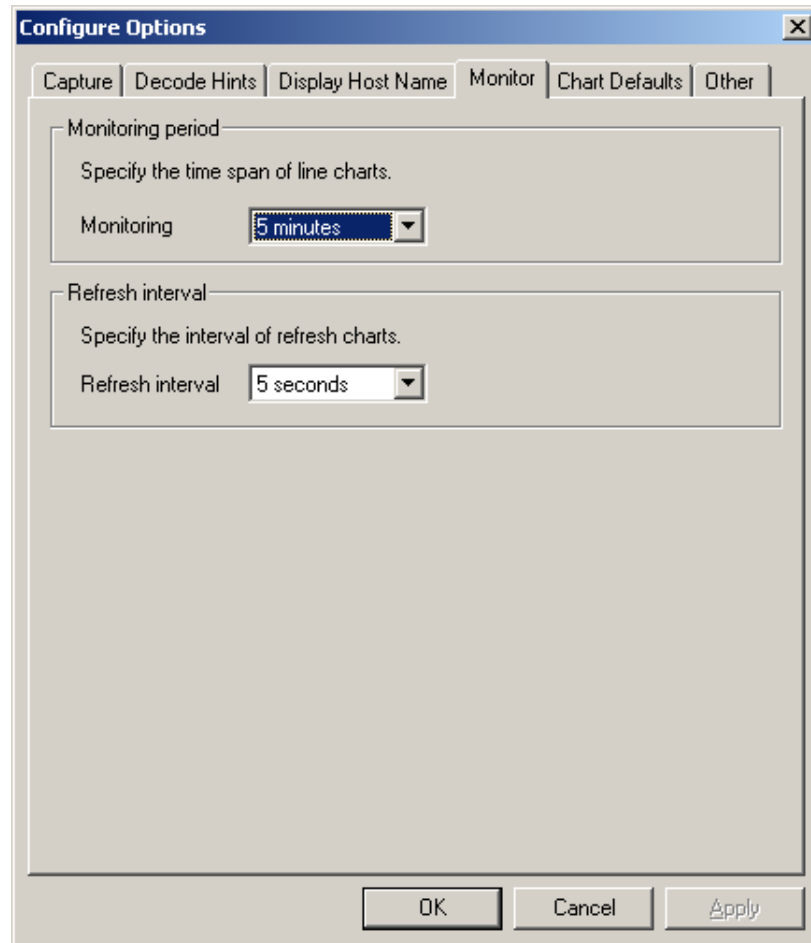


Figure 4-44 **Configure Options** dialog box (monitor)

Monitoring period specifies the time span in minutes for which the traffic information is displayed. The line charts are drawn for this monitoring period. The accumulating totals and the distributions of the traffic for the specified items during the specified

monitoring period are shown in bar and pie charts. The default value is 5 minutes.

Refresh interval specifies the intervals in seconds at which Monitor windows are refreshed with most recent data. The default value is 5 seconds.

Configuring Charts Default Options

Click on the **Chart Defaults** tab of the **Configure Options** dialog box.

The page for configuring the default setting of a chart is shown in Figure 4-45.

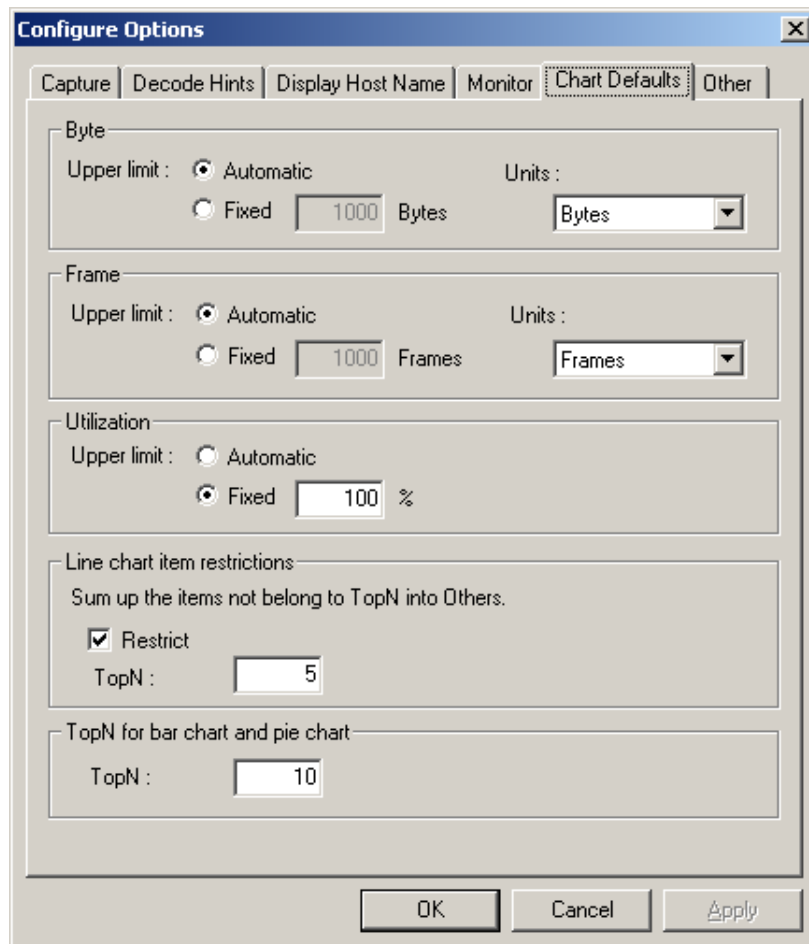


Figure 4-45 **Configure Options** dialog box (chart defaults)

The **Byte** and **Frame** regions specify the unit for the traffic volume or the y-axis of a chart, and whether the upper limit of the y-axis is fixed or not in a line or bar chart of the Monitor window. If you want to fix the upper limit, enter the value.

For example, if only one of the Graph Items has a very high volume, and you set the upper limit to **Automatic**, this Graph Item will be drawn with an appropriate scale. However, all the other Graph Items will be drawn congested around value zero, making the chart difficult to identify. To see the Graph Items with lower traffic with an appropriate scale, it might be better to select **Fixed** and specify the upper limit accordingly.

Choose a unit from the drop down list.

Utilization is peculiar to the Monitor window for “MAC Traffic”. As with Byte and Frame, specify whether the upper limit is fixed or not. If you choose to fix the upper limit, enter the value. By default, it is **Fixed** at 100%.

If the traffic is too little for the network bandwidth, e.g., lines in a line chart may stay around the value zero, and it may be difficult for you to read the values. In such a case, it might be better to select **Automatic**.

Line chart item restriction specifies whether you limit the number of Graph Items to be shown when you display a line chart.

ASTEY Eyes counts the number of frames/packets and octets flowing through the network, and generate the statistical data periodically (every one second by default). If you limit the maximum number of items, only the Graph Items that were in top N at least once during the time the data is collected will be displayed. Graph Items that have never in top N within the monitoring period are aggregated into the Graph Item “Others”. Select **Restrict** check box and enter the value of top N into **TopN** field to apply a limit. The default top N value is 5. If you do not apply the limit, all Graph Items will be displayed.



If there are a large number of Graph Items, it is recommended that you restrict the number of items to be displayed. If you try to display all of them, the drawing speed of chart might slow down as the usage of memory increases. In addition, the resulting chart might be crowded and difficult to identify.



You can specify the monitoring period the data covers in the Monitoring period field of the **Configure Options** dialog box. For details, see “Configuring Monitor Options” on page 159.

TopN for bar and pie charts specifies how many Graph Items from the top are to be displayed in a bar or pie chart of the Monitor window.

The top 10 items are displayed by default. For a pie chart, the Graph Items that do not fall into top N are aggregated.



The values specified here are applied to newly created Monitor windows. They have no effect on current existing Monitor windows. To change the display configuration of the existing Monitor window, use the popup menu of the Monitor window. For more information, see “Popup Menu on the Monitor Window When No Graph Item Is Selected” on page 88.

Configuring Other Options

Click on the **Other** tab of the **Configure Options** dialog box.

The page for configuring other options is shown in Figure 4-46.

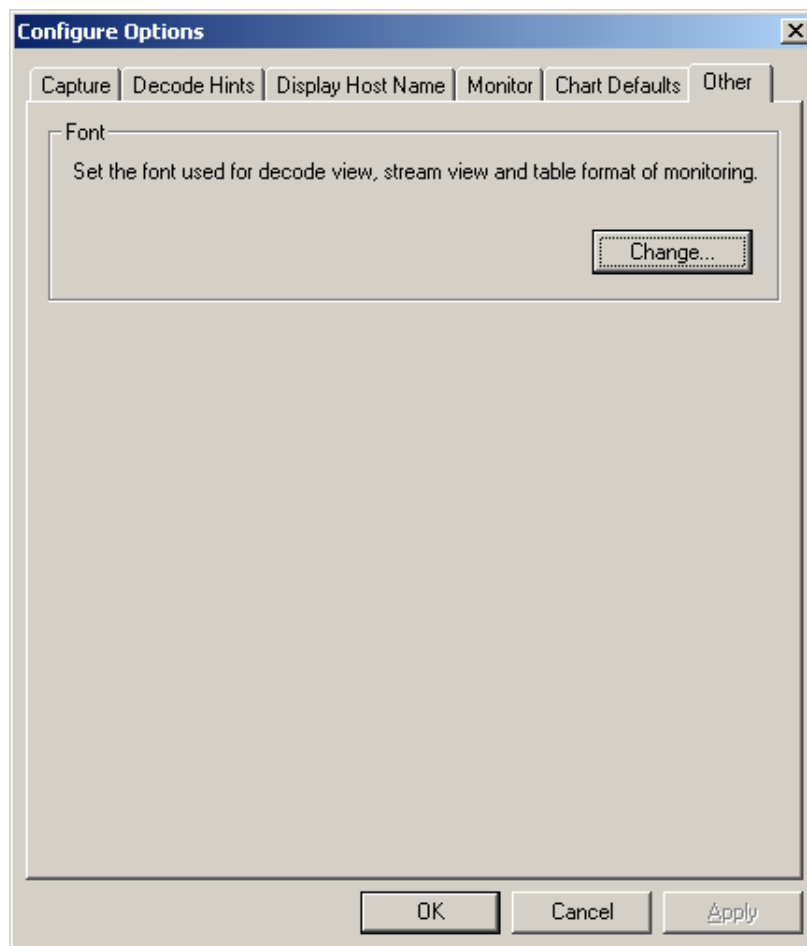


Figure 4-46 **Configure Options** dialog box (other)

You can change the font used in the decode view, the stream view, and the Monitor window in table format.

To change the font, click the **Change...** button. The **Font** dialog box will appear as shown in Figure 4-47.

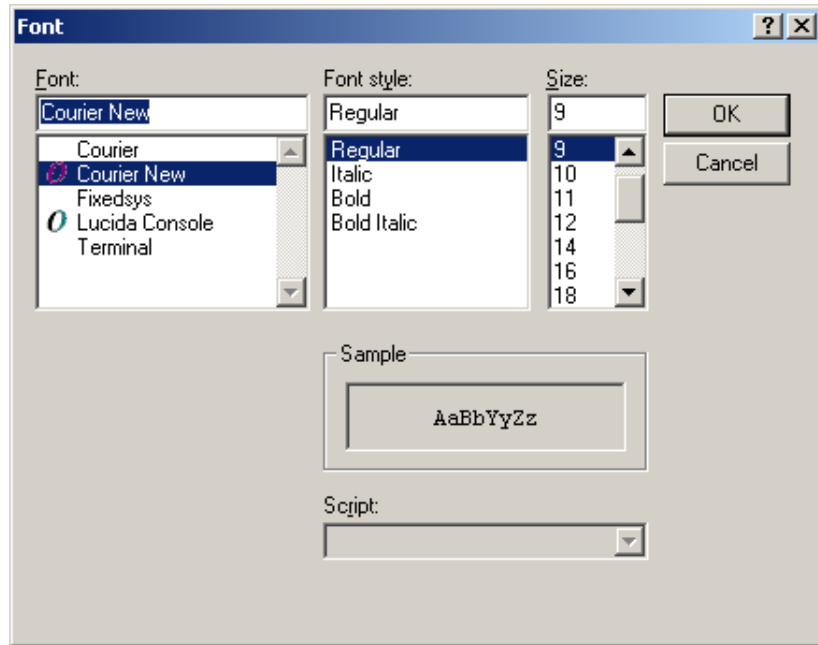


Figure 4-47 Font dialog box

Specify a font by choosing appropriate values from the font, style, and size lists. A sample font will be shown in the **Sample** region. Make sure it is suitable. To apply it, click the **OK** button.

The old font will be replaced with the new one in the decode view, the stream view, and the Monitor window in table format.

Saving a Configuration

There are two types of configuration information. One of them is saved into the registry automatically and the other is saved in a configuration file.


Information Saved in a Configuration File

By loading the saved configuration file when you invoke ASTEC Eyes again, you will have the same look and feel as before, and you need not reconfigure such items as decode hints.


You can save the following configuration information into a file.

- Workspace information
 - Organization and properties of workspaces
- Monitor window information
 - Type and display format of Monitor windows
 - Whether the legend is visible or invisible
 - Geometry information
- Configured options
 - Capture options
 - Decode hints
 - Host name preference
 - Monitor options
 - Default options for charts
 - Font information
- NIS domain name entered in the **Searching for Host Name** dialog box

There are two ways to save the configuration into a file:

- Click the **Save Configuration** button  on the Common toolbar in the Main window.
- Choose **S**ave Configuration... from the **O**ptions menu on the menu bar of the Main window.

There are two ways to load the configuration from a file:

- Click the **Load Configuration** button  on the Common toolbar in the Main window.
- Choose **L**oad Configuration... from the **O**ptions menu on the menu bar of the Main window.



The file extension for a saved configuration file is `.wsi`.

If you save the configuration into a file named `default-workspace.wsi` in the directory where `EYES.exe` is installed, ASTEC Eyes will load the configuration file during the startup automatically.



The configuration for a Remote Module is not saved in a file. Only the configuration for ASTEC Eyes can be saved.

Information Saved in the Registry

The following information is automatically saved in the registry and loaded automatically when ASTEC Eyes is invoked.

- History of connected hosts.
When you connect ASTEC Eyes to the Remote Module using the **Connect** dialog box, you can select a host from the connections history.
- The geometry of the Main window
- Whether the Message window is shown or hidden
- The geometry of the Interface Selector window

Miscellaneous Functions

Workspace

When you open windows in ASTEC Eyes, all the new windows except the dialog boxes appear in the currently selected workspace.

To set the focus to a workspace, click on the workspace with the left mouse button or press the <Alt-0> key.

You can create more than one workspace and move windows from one to another. Workspaces are useful for organizing windows.

In addition, you can bind an interface to a workspace, so that the interface will be automatically selected by activating the corresponding workspace.

This section describes how to manipulate workspaces.

Creating a Workspace

There are three ways to create a workspace:

- Choose **A**dd **W**orkspace from the **W**orkspace on the menu bar of the Main window.
- Click on an open space of the workspace with the right mouse button. A popup menu will appear as shown in Figure 4-48. Choose **A**dd **W**orkspace from this menu.

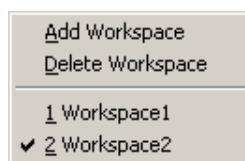


Figure 4-48 Popup menu for the workspace

- Click on the title bar of a window in a workspace with the right mouse button. A popup menu will appear as shown in Figure 4-49. Choose **N**ew **W**orkspace from this menu.

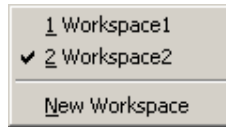


Figure 4-49 Popup menu on the title bar

When you create a workspace this way, the window you clicked will be moved into the newly created workspace.

When a new workspace is added, the corresponding tab is added at the bottom of the Main window. The menu item for the workspace is also added to the **Workspace** menu on the menu bar of the Main window.

Selecting a Workspace

There are four ways to select a workspace:

- Choose the menu item corresponding to the target workspace from the **Workspace** menu on the menu bar of the Main window.
- Click on the tab of the target workspace.
- Click on an open space of the workspace with the right mouse button. A popup menu will appear as shown in Figure 4-48. Choose the menu item corresponding to the target workspace.
- Use the <Ctrl-Alt-←> or <Ctrl-Alt-→> key. By pressing the <Ctrl-Alt-←> key, the previous workspace will be selected. By pressing the <Ctrl-Alt-→> key, the next workspace will be selected.
By pressing the <Ctrl-Alt-←> key on the first workspace, the last workspace will be selected. By pressing the <Ctrl-Alt-→> key on the last workspace, the first workspace will be selected.



The <Ctrl-PageUp> and <Ctrl-PageDown> keys work in the same way as the <Ctrl-Alt-←> and <Ctrl-Alt-→> keys respectively.

If you select a workspace bound to an interface, the interface will be selected as well.

Moving a Window to Another Workspace

To move a window into another workspace, click on the title bar of the window with the right mouse button. A popup menu will appear as shown in Figure 4-49. Currently existing workspaces will be listed on the menu. Choose the target workspace from the menu.

Changing Workspace Properties

The workspace has the following properties:

- **Workspace name**
You can assign a name to a workspace instead of the default name such as “Workspace 1” or “Workspace 2”.
- **Automatic selection of the interface**
If you bind a workspace to an interface, the corresponding interface will be automatically selected when you select the workspace.
For a complete discussion on selecting the interface, see “Selecting an Interface” on page 78.

To change the properties of a workspace, click on the tab of the target workspace with the right mouse button. A popup menu with the **Properties** item will appear. Choosing it will display the **Workspace Properties** dialog box as shown in Figure 4-50.

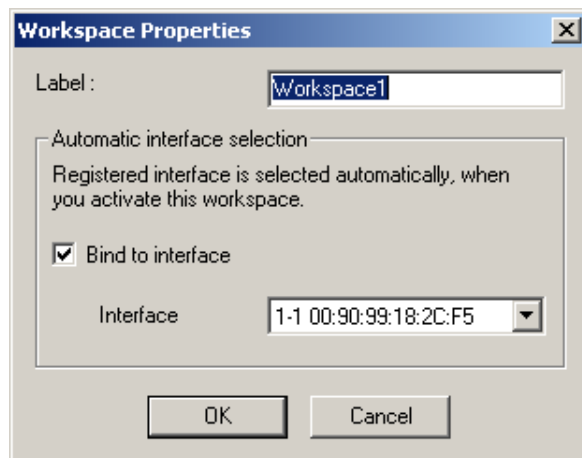


Figure 4-50 **Workspace Properties** dialog box

Enter a new name into the label field, and it will then appear on the tab of the workspace. If you want to bind a workspace to an interface, select the “**Bind to interface**” check box, and choose the desired interface from the drop down list.

Deleting a Workspace

There are two ways to delete a workspace:

- Select the workspace you want to delete, and choose **Delete Workspace** from the **Workspace** menu on the menu bar of the Main window.
- Click on an open space of the workspace with the right mouse button. The popup menu will appear as shown in Figure 4-48. Choose **Delete Workspace**.

If there are any windows placed in the target workspace, the **ASTEC Eyes** dialog box will show confirming you want to delete those windows together with the workspace. If you do not need them, click the **OK** button. The workspace and the windows in it will be deleted all at once. Otherwise, click the **Cancel** button to quit the operation. After moving those windows into another workspace, retry the operation.



You cannot delete the first (left most) workspace.



The workspace properties (the label and the automatic selection of the interface) including their existence can be saved into a configuration file. For details, see “Saving a Configuration” on page 164.

Window Operation

As you keep using ASTEC Eyes, a workspace will be messed up with many windows, like Monitor windows and decode views. Then, you can clean up the workspace so that it is more organized and easier to see.

To organize the windows in the workspace, use the **Window** menu on the menu bar of the Main window.

N**ew Window**

Creates a new window with the same contents as the active window.

C**ascade**

Stacks up windows so that the titles of all windows can be seen.

T**ile Horizontally** or **T**ile Vertically****

In the workspace currently selected, tiles the workspace with all the windows horizontally or vertically, changing their sizes accordingly so that no window will overlap one another.

A**rrange Icons**

Arranges the icons in the bottom part of the workspace.

In the **Window** menu on the menu bar of the Main window, the windows in the current workspace are listed as the menu items. Choosing the item from the menu will activate the corresponding window.



Sometimes an icon is hidden by another window and cannot be selected. In such a situation, you can choose the corresponding menu item from the **Window** menu on the menu bar of the Main window. It will be brought up to the front in the original size.

Filter Editor

In the filter editor, you can edit the conditions for the following filters:

- display filter** Filters the results of the analysis to be displayed in the decode view.
- monitor filter** Filters the data to be displayed in the Monitor window. The monitor filter applies to the following Monitor windows:
- MAC traffic
 - MAC traffic by source
 - MAC traffic by destination
 - MAC traffic by host pair
 - MAC traffic by protocol
 - IP traffic
 - IP traffic by source
 - IP traffic by destination
 - IP traffic by host pair
 - IP traffic by protocol
 - MAC traffic by address type
- capture filter** Filters the packets to be captured.
- start capture trigger** Specifies a condition used as a trigger for capture.
- pause capture trigger** Specifies a condition used as a pause trigger for capture.

To invoke the filter editor, choose **Filter Editor** from the **Edit** menu on the menu bar of the Main window. The filter editor window will appear as shown in Figure 4-51.

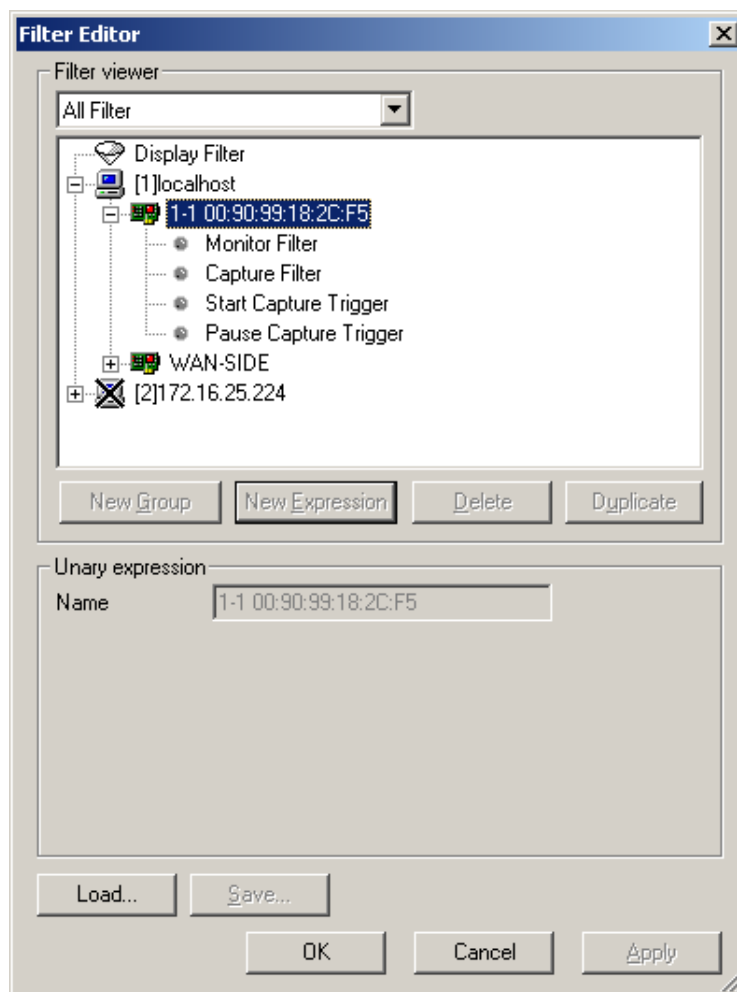


Figure 4-51 Filter Editor

Filter viewer region

Displays, as a tree, applicable hosts, their interfaces, filter types and their conditions as logical expressions. Select a filter or a logical expression to edit. You can use copy and paste, and drag and drop operations. You can also use popup menus. By using the drop down list in the upper left, you can restrict the display contents to a network interface or filter type.

Unary expression region

Specify individual conditions constituting the logical expression for the filter in the **Unary expression**¹ region. You can also change the name and condition of a condition group, and the name of a display filter have.

For a complete discussion on unary expression and condition group, see “Components of a Logical Expression”.

Load... and Save... buttons

Loads filters from a file and saves edited filters into a file.

Components of a Logical Expression

A logical expression is composed of two parts: **condition group** and **unary expression**. A unary expression is a minimum component of a logical expression. A condition group is logical expressions united by a logical operator, AND or OR. See Figure 4-52.

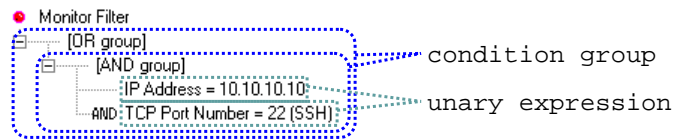


Figure 4-52 Logical expression and its component

A condition group determines how its component logical expressions are united. An **AND group** is the group whose component logical expressions are united by AND operator. An **OR group** is the group united by OR operator. Each component logical expression is either a unary expression or a condition group.

A unary expression is a simple logical expression without AND or OR operator. A unary expression may consist of a variable, a conditional operator, and a value. Or it may consist of the name of the condition and its value.

There are seventeen (17) types of unary expressions predefined by ASTEC Eyes. Depending on the filter type, all of the unary expression types may not be available. The table below describes the availabilities of the unary expression types to each filter type.

¹An expression without AND or OR operators.


	display filter	monitor filter	capture filter start capture trigger pause capture trigger
MAC Address	✓	✓	✓
Ethernet Encapsulation	✓		✓
Type Field of Ethernet Header	✓	✓	✓
Ethernet Address Type	✓	✓	✓
Ethernet Size	✓		✓
LLC Service Access Point	✓	✓	✓
IP Address	✓	✓	✓
IP Network Address	✓	✓	✓
Protocol Field of IP Header	✓	✓	✓
UDP Port Number	✓	✓	✓
TCP Port Number	✓	✓	✓
TCP Status			✓
Flags Field of TCP Header	✓		✓
Analyzed Packet Status			✓
Data Comparison	✓		✓
Start Capture Timer			Available for start capture trigger only
Pause Capture Timer			Available for pause capture trigger only

Constraints of Filter

Depending on the filter type, the following constraints apply:

- The filter names, other than that of the display filter, cannot be changed.
- You can define only one monitor filter, capture filter, start capture trigger, and pause capture trigger for each network interface.
- You can define up to 250 display filters. The display filter is independent of the interfaces and can be applied to any data captured or loaded from capture files.
- You can define up to 250 layers of condition groups in a display filter or a monitor filter.
- Logical expressions for the capture filter, start capture trigger, and pause capture trigger can have three layers of condition groups at most. The top layer must be an OR group and the second layer must be AND groups.

Starting to Edit Logical Expressions

The filter with no logical expression is denoted by a  (gray) icon. Start editing a logical expression by the following steps:

1. Click on the icon or label of the target filter.

When you select the display filter or monitor filter, the **New Group** and **New Expression** buttons in the **filter viewer** region will become sensitive. When you select the capture filter, start capture trigger, or pause capture trigger, only the **New Expression** button will become sensitive.
2. Click the **New Group** or **New Expression** button.

Click the **New Group** button if you need more than three layers of a logical expression, or click the **New Expression** button if you need up to three layers of a logical expression.

OR

1. Click on the target filter with the right mouse button.

A popup menu will appear.
2. Choose **New Group** or **New Expression** from the menu.

For the display filter or monitor filter, an OR group is created as the top layer of the logical expression. The type of the second layer logical expression depends upon which button you click.

Clicking the **New Group** button will create an AND group.




Clicking the **New Expression** button will create a unary expression.



For the capture filter, start capture trigger, and pause capture trigger, an OR group, an AND group, and a unary expression are created as the top, second, and third layer respectively.



The icon for the filter to which a logical expression is added will be changed to  (pink).

Editing a Logical Expression

To set the type, operator, and value of a unary expression, do the following:

1. Select the target unary expression in the **filter viewer** region.
The **Type**, **Operator**, and **Value** will become editable in the **unary expression** region.
2. Choose the type.
Choose the type of a unary expression from the drop down list in the **unary expression** region. Depending upon the selected type, radio buttons may appear.
3. Set the operator.
Choose the operator from the drop down list for **Operator** in the **unary expression** region. Depending upon the **Type**, items in the list may differ.
4. Set the value.
The values will differ according to the **Type**:

Label	Input values and methods
Value (Dec)	Enter the value as decimal numbers or use the Candidate... button.
Value (Hex)	Enter the value as hexadecimal numbers or use the Candidate... button.
Value (Candidate)	Use the Candidate... button.

Clicking the **Candidate...** button, a popup menu will appear. The menu shows **History**, **Known Values**, and **Predefined Values** as the menu items.

- Choose **History**, and a list of the formerly entered values will appear.
- Choose **Known Values**, and a list of the values found during monitoring and decoding the capture data will appear.
- Choose **Predefined Values**, and a list containing the values specific to each type will appear.

The values that can be set are described below in detail.

The following is a description of the types for unary expression and the values to be set.

- **MAC Address**
Sets the value of a MAC layer address.
Three radio buttons “**Src/Dst**”, “**Src**”, and “**Dst**” will appear.
Enter six octets of a MAC address as hexadecimal numbers.
- **Ethernet Encapsulation**
Specifies which standard Ethernet frame complies with: RFC 894 (without LLC header) or RFC 1042 (with LLC header).
You cannot enter a value for this. Click the **Candidate...** button, and choose RFC 894 or RFC 1042 from the list of **Predefined Values**.
- **Type Field of Ethernet Header**
Specifies the value for the type field of the Ethernet header.
Enter the value in hexadecimal, or click the **Candidate...** button and choose an appropriate value from the list of **Predefined Values**.
- **Ethernet Address Type**
Specifies an Ethernet address type. Valid values are multicast, broadcast, and unicast.
You cannot enter a value for this. Click the **Candidate...** button, and choose multicast, broadcast, or unicast from the list of **Predefined Values**.
- **Ethernet Size**
Specifies the size of the Ethernet frame.
Enter the size in octets as decimal numbers. The CRC field of Ethernet (4 octets) is not included.
- **LLC Service Access Point**
Specifies the values for the DSAP (Destination SAP) and the SSAP (Source SAP) fields of LLC (IEEE 802.2).
Three radio buttons “**Src/Dst**”, “**Src**”, and “**Dst**” will appear.
Enter the value for the DSAP or SSAP field in hexadecimal.
- **IP Address**
Specifies the value for an IP layer (IPv4) address.
Three radio buttons “**Src/Dst**”, “**Src**”, and “**Dst**” will appear.
Enter four octets of the IP address in decimal.
- **IP Network Address**
Specifies the value for an IP layer (IPv4) network address.
Three radio buttons “**Src/Dst**”, “**Src**”, and “**Dst**” will appear.

Enter four octets of the IP address and the number of significant bits for the subnet mask in decimal.

- **The Protocol Field of IP Header**

Specifies the value for the protocol field of the IP header (IPv4).
Two radio buttons “**Well-known**” and “**Unknown**” will appear.
When you select the “**Well-known**” radio button, enter the value in decimal, or click the **Candidate...** button and choose an appropriate item from the **Predefined Values**. If there are more than nine items in the list, an item named “**(Candidate List...)**” will appear. If there is not a desired value in the list, choose **(Candidate List...)**. The **Candidate List** dialog box will appear. Choose an appropriate item from the dialog box.
When you choose “**Unknown**”, you are not allowed to enter any value. You choose this when you want to filter packets containing types of values not recognized by ASTEC Eyes.
- **UDP Port Number and TCP Port Number**

Specify the values for UDP and TCP port number respectively.
For filters other than monitor filter, radio buttons “**Src/Dst**”, “**Src**”, “**Dst**”, and “**Unknown**” will appear.
For monitor filter, radio buttons “**Well-known**” and “**Unknown**” will appear.
Enter the value in decimal, or click the **Candidate...** button and choose the appropriate item from the **Predefined Values**. If there are more than nine items in the list, an item named “**(Candidate List...)**” will appear. If there is not a desired value in the list, choose **(Candidate List...)**. The **Candidate List** dialog box will appear. Choose an appropriate item from the dialog box. The **Candidate List** dialog box has the list of UDP or TCP port numbers for the protocols supported by ASTEC Eyes.
Choose “**Unknown**” for protocols neither supported by ASTEC Eyes nor registered in the decode hints.
- **TCP Status**

Specifies the TCP status (CLOSED, SYN_SENT, and so forth).
You cannot enter the value for this. Click the **Candidate...** button, and choose an appropriate item from the **Predefined Values**.
- **Flags Field of TCP Header**

Specifies the value for the flags in the TCP header.
You cannot enter the value for this. Instead, you can use the **Candidate...** button. Choosing **Predefined Values**, a list will appear showing the meaning of each bit (6 bits) of the flags field. If you want to change more than one bit, choose those bits one by one from the list. Each item in the list works as a toggle. Choosing **(Clear)**, all bits

are cleared.

- Analyzed Packet Status

Specifies the expert events caused by the packet.

You cannot enter a value for this. Instead, you can use the **Candidate...** button. Choosing **Predefined Values**, a list will appear showing the expert events that can be detected by ASTEC Eyes. Each item in the list works as a toggle. You can choose more than one item. Choosing **(Clear)** will clear all of the selected items at once.

- Data Comparison

Specifies the value to be compared to the data in packets.

Specifies the offset and the value used for comparison in hexadecimal. The offset is an octet value representing is the distance from the beginning of the packet. The value for comparison can be up to 32 octets long.

- Start Capture Timer

Specifies the time interval between the time a triggering packet is detected and the time the capture actually starts.

When you specify no condition about the triggering packet, the first packet is considered to be the triggering packet.

Enter hours, minutes, and seconds.

- Pause Capture Timer

Specifies the time interval between the time a triggering packet is detected and the time the capture actually pauses.

When you specify no condition about the triggering packet, the first packet is considered to be the triggering packet.

Enter hours, minutes, and seconds.



If you use an IP address as the type for a unary expression, the condition that the packet is using IP protocol is implicitly applied at the same time.

For example, a unary expression "IP Address = 192.168.0.1" is true for a packet using IP protocol with the IP address 192.168.0.1.

On the other hand, a unary expression "IP Address NOT= 192.168.0.1" is true for a packet that is not using IP protocol or a packet whose IP address is not 192.168.0.1.

If you want to define the expression that is true for an IP packet whose address is not 192.168.0.1, unite the unary expressions "Type Field of Ethernet Header = 0x0800 (IP version 4)" and "IP Address NOT= 192.168.0.1" with an AND operator.

Editing a Condition Group

You can edit the name and operator of a condition group.

1. Select the target group in the **filter viewer** region.
2. Change the name.
A group is named “AND group” or “OR group” by default. Enter the desired name.
3. Select an operator.
You can select AND or OR from the list.
If you use a default group name, it will be changed in accordance with the operator you have selected. If you change the operator of an OR group to AND, then the name will be changed to “AND group”.



The condition group operator at the first and second layer of a capture filter, start capture trigger, and pause capture trigger cannot be changed.

Changing the Name of a Display Filter

You can define up to 250 display filters, which are independent of network interfaces. They are named “Display Filter *N*” by default. You can change the name to the one easily identifiable.

When you select the target display filter in the **filter viewer** region, only the input field for the name will be shown. Enter the desired name there.

Adding a Logical Expression

The steps to add a logical expression as follows:

- Select a filter, a condition group, or a unary expression in the **filter viewer** region, and click the **New Group** or **New Expression** button.

OR

- Click on a filter, a condition group, or a unary expression in the **filter viewer** region with the right mouse button, and choose **New Group** or **New Expression** from the popup menu.

Choosing **New Group** will add a group. Choosing **New Expression** will add a unary expression.

The results are described below:

- The add operation for the display filter will create a new filter “Display Filter *N*” with the initial logical expression described in “Starting to Edit Logical Expressions” on page 176.
- The add operation for “Display Filter *N*” or the monitor filter will create an AND group or a unary expression under the OR group of top layer. The added group or unary expression will be joined to other expressions in the same layer with an OR operator.
- The add operation for capture filter, start capture trigger, or pause capture trigger will create an AND group with a unary expression under the OR group of top layer. The added group will be joined to other groups in the same layer with an OR operator.
- The add operation for a condition group of display or monitor filter will create an AND group or a unary expression under the condition group. The added group or unary expression will be united to other logical expressions in the same layer with the selected group operator.
- The add operation for an OR group of capture filter, start capture trigger, or pause capture trigger will create a new expression. The result will be the same as for the filter containing the OR group.
- The add operation for an AND group of capture filter, start capture trigger, or pause capture trigger will create a unary expression under the AND group. The added unary expression will be united to the other logical expressions in the same layer with the AND operator.
- The add operation for a unary expression will cause the same result as that for a condition group one layer above.



Only the **New Expression** button is available for capture filter, start capture trigger, and pause capture trigger. The **New Group** button is disabled for these filters.

Duplicating a Logical Expression

The steps to duplicate a logical expression as follows:

- Select the target logical expression in the **filter viewer** region, and click the **Duplicate** button.

OR

- Click on the target logical expression in the **filter viewer** region with the right mouse button, and choose **Duplicate** from the popup menu.

When you select a top layer condition group, all of the logical expressions under the selected group will be duplicated and placed under the selected group. When you select a condition group other than top layer one, the selected condition group and all of the lower layers will be duplicated and placed in the same layer. When you select a unary expression, it will be duplicated and placed in the same layer.

The duplicated logical expressions are united to the other expressions in the same layer by the group operator one layer above. A logical expression with no unary expression cannot be duplicated.

Deleting a Logical Expression

The Steps to delete a logical expression are as follows:

- Select the target logical expression in the **filter viewer** region, and click the **Delete** button.

OR

- Click on the target logical expression in the **filter viewer** region with the right mouse button, and choose **Delete** from the popup menu.

The selected logical expression will be deleted. If it includes more than one condition group, those groups and all of their lower layers will be deleted all together.

Deleting a filter, all the logical expressions defined for the filter will be deleted.

Using Copy and Paste

You can replicate a logical expression using copy and paste by the following steps:

1. In the **filter viewer** region, select the logical expression you want to copy, and press the <Ctrl-C> key.
2. Select one of the unary expressions in the layer you want to place the copied logical expression and press the <Ctrl-V> key. Alternatively, select a condition group under which you want to place the copied expression and press the <Ctrl-V> key.

OR

1. In the **filter viewer** region, click on the logical expression you want to copy with the right mouse button.
2. Choose **C**opy from the popup menu.
3. Click on one of the unary expressions in the layer you want to place the copied logical expression, or the condition group under which you want to place the copied expression, with the right mouse button.
4. Choose **P**aste from the popup menu.

The copy and paste works in the same way as the copied logical expression is added at the paste destination. For more information, see “Adding a Logical Expression” on page 181.

Using Drag and Drop

By using drag and drop, you can move or copy a logical expression.

The steps to move a logical expression are as follows:

1. In the **filter viewer** region, point to a logical expression you want to move with the mouse cursor, and press and hold down the left mouse button.
2. While holding down the left mouse button, drag the selected logical expression to one of the unary expressions in the layer you want to place it. Alternatively, drag it to a condition group under which you want to place it.
3. Release the left mouse button.

The effects are as follows:

- After you release the left mouse button on a unary expression, the dragged logical expression will be moved to the same layer as the pointed unary expression belongs to. The moved logical expression will be united to the other expressions in the same layer with the same logical operator.
- After you release the left mouse button with the mouse cursor on a condition group of the display or monitor filter, or on an AND condition group of capture filter, start capture trigger, or pause capture trigger, the dragged logical expression will be moved under the pointed condition group. If the group is not empty, the dragged expression will be united to the existing expressions by the group logical operator.
- After you release the left mouse button with the mouse cursor on an OR group of the capture filter, start capture trigger, or pause capture trigger, an AND group will be

created and the dragged logical expression will be moved under the newly created AND group. If the pointed OR group is not empty, the new AND group will be united to the existing groups with an OR operator.

- After you release the left mouse button with the mouse cursor on a filter, the result will be the same as the one of releasing the button with the mouse cursor on the logical expression in the uppermost layer.




If you drag and drop while holding down the <Ctrl> key, the logical expression will not be moved but copied.



Applying a Logical Expression

After you have finished editing, click the **OK** or **Apply** button. All of the modified filters will be applied at once.

If there is any invalid logical expression, an **ASTEC Eyes** dialog box will appear notifying you.

Any invalid logical expression is denoted by  (red). Correct or delete it, and click the **OK** or **Apply** button again.

A logical expression containing only logical operators but no unary expressions will be deleted.

When a filter is applied, the icon turns from  (pink) to  (green).

Clicking the **OK** button will close the filter editor.



The following are the examples of invalid logical expressions:

- The filter contains an unsupported type of unary expressions.
This may happen when a filter file created in ASTEC Eyes version 1.0 is loaded.
- The value of a unary expression is not set.
This happens when you do not complete editing a unary expression.

Temporarily Disabling a Logical Expression

You can disable a logical expression without deleting it. It is useful when you want to change the filter temporarily.

The steps to disable a logical expression are as follows:

1. In the **filter viewer** region, select a logical expression that you want to temporarily disable.
2. Clear the “**Enable this unary expression**” check box in the lower part of the **unary expression** region.

OR

- In the **filter viewer** region, click on a logical expression that you want to temporarily disable with the right mouse button, and choose **Disable** from the popup menu.

A  mark is displayed beside the selected logical expression and all the logical expressions below it.

Saving and Loading Filters

You can save filters in a file so that you can load and reuse them later.

To save filters in a file, click the **Save...** button. The **Save As** dialog box will appear as shown in Figure 4-53.

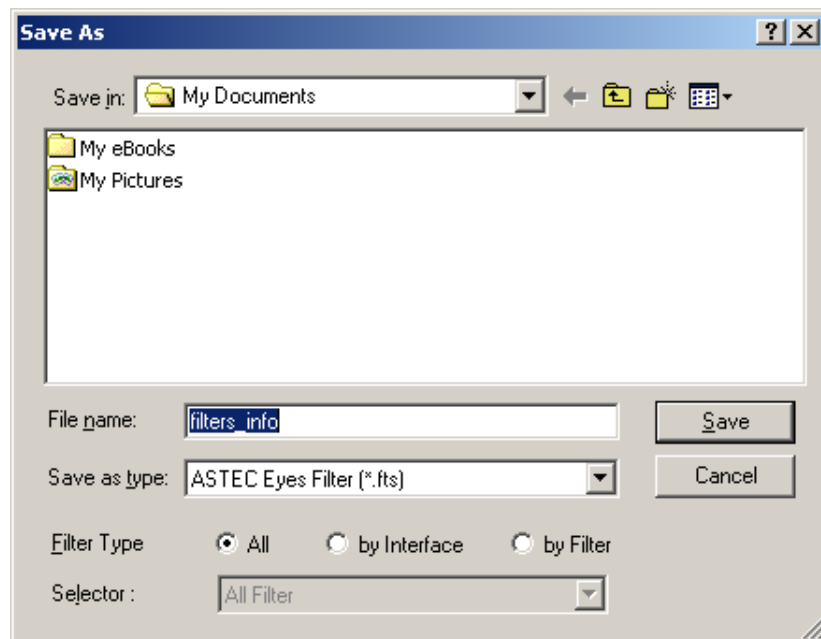


Figure 4-53 **Save As** dialog box for saving a filter

Specify the filters to save by the **Filter Type** radio buttons and the **Selector** list.

When the “**All**” radio button is selected, all filters in the filter editor will be saved into one file. In this case, the **Selector** list will be grayed out.

When the “**by Interface**” radio button is selected, you need to select a network interface from the **Selector** list. Only the filters for the selected network interface are saved into one file. Display filters are not saved.

When the “**by Filter**” radio button is selected, the edited filters will be shown in the **Selector** list. Only those that are selected from the list will be saved.

To load filters from a file, click the **Load...** button. The **Open** dialog box will appear. Specify the file name there.


The display filters included in the file will be added to the list of the existing display filters. The other types of filters will be loaded as is, if the filters of the same types and network interfaces are not in the filter editor. Otherwise, a dialog box will appear asking if they should be replaced with the corresponding filter in the file or not.

The extension of a saved filter file is `.fts`.



With ASTEC Eyes version 1.0, each filter type was saved in a separate file. ASTEC Eyes version 1.2 can load the filter files created by ASTEC Eyes version 1.0. If the display filters are loaded from a file (extension `.fls`), they are added to the list of display filters. If the other types of filters are loaded from a file (extension `.flt`), the **Specify Where to Load Filter** dialog box will appear.



When you load a filter file created by ASTEC Eyes version 1.0, that logical expressions not useful with the monitor or display filter of ASTEC Eyes version 1.2 might be included in the file. Such logical expressions are denoted by  (in red). Either correct or delete these logical expressions.

Popup Menu on the Filter Editor

The filter editor provides a popup menu for your convenience. From this menu, you can do the followings:

- Add a logical expression
- Duplicate a logical expression
- Delete a logical expression

- Enable or Disable a logical expression
- Copy a logical expression
- Paste a logical expression

Click on the target logical expression in the **filter viewer** region with the right mouse button to use the popup menu.

The popup menu will appear as shown in Figure 4-54.

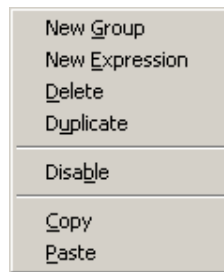


Figure 4-54 Popup Menu on filter editor

Choose an item from the popup menu.

New Group

Adds a condition group.

New Expression

Adds a unary expression.

Duplicate

Duplicates a logical expression. If the selected logical expression has subordinate layers, the selected logical expression and all its lower layers will be duplicated.

Delete

Deletes a logical expression. If the selected logical expression has subordinate layers, the selected logical expression and all its lower layers will be deleted.

Copy

Copies a logical expression into the internal buffer. If the selected logical expression has subordinate layers, the selected logical expression and all its lower layers will be copied.

Paste

Pastes a logical expression held in the internal buffer.

Disable and Enable

If the selected logical expression is disabled, a menu item labeled **Enable** will appear. It enables the logical expression.

If the selected logical expression is enabled, a menu item labeled **Disable** will appear. It disables the logical expression.

Searching Host Names

IP addresses are used to identify hosts in the Monitor windows for the IP layer, decode view, and stream view. However, host names are probably preferred in most occasions.

You can search for host names with ASTEC Eyes.

Using the Search for Host Name Dialog Box

Choose **Search Host Name...** from the **File** menu on the menu bar of the Main window. The **Searching for Host Name** dialog box will appear as shown in Figure 4-55.

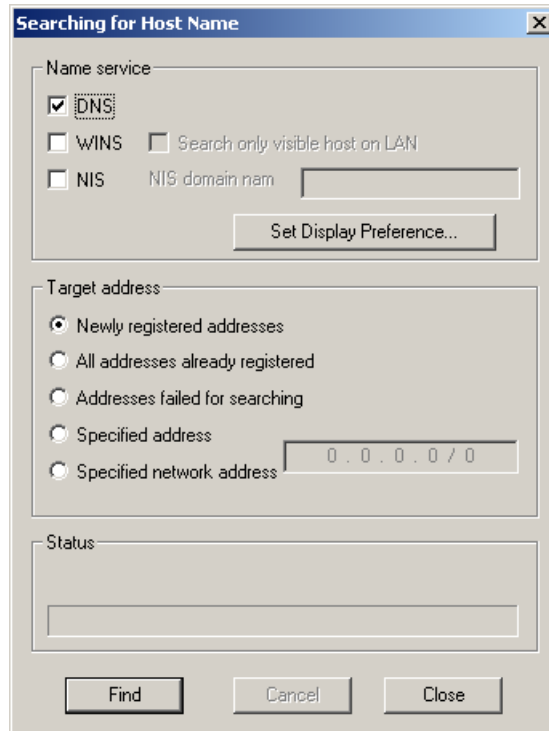


Figure 4-55 Searching for Host Name dialog box

The steps to search for the host names are as follows:

1. Select the name services to use in the **Name service** region.
ASTEC Eyes supports DNS, WINS, and NIS.
You need to specify a NIS domain name when NIS is selected.
Selecting WINS will enable the “**Search only visible host on LAN**” check box. When you select this check box, only the computers displayed below the “Entire Network” in “My Network Places” or “Network Neighborhood” will be searched.
2. Specify a range in the **Target address** region.
You can select one of the followings:
 - Newly registered addresses
Searches only newly found addresses. Addresses searched once will not be searched again.

- All addresses already registered
When this is selected, it may take very long to complete the search. To stop the search in the middle, click the **Cancel** button.
- Addresses failed for searching
Search only the addresses the search once failed for.
- Specified address
Enter an IP address or copy and paste it from the address book. The IP address being searched and the status of the search will be shown in Message window.
- Specified network address
Select this range when, of the addresses registered by now, you want to search those in a specific network segment. For example, to search the computers the upper 24 bits of whose IP addresses equal a specific value, enter something like *111.22.11.0/24*, the network address and the mask length.

3. Click the **Search** button.

While searching, the name service in use and the progress are displayed in the **Status** region. The host names found will be registered to the address book.

You can specify the preference among the name services, in case different host names are returned from different name servers.

To specify the preference, click the **Set Display Preference...** button in the **Name service** region. The **Configure Options** dialog box will appear. The dialog box includes only the **Display Host Name** tab of the options property sheet. For further information, see “Configuring Host Name Preference” on page 156.



The host names found are automatically registered and displayed in the address book in the following cases:

- While monitoring, DNS packets mapping IP addresses and host names are sent.
- Host names (DNS names) are found in the loaded log file.
- Decoded captured data containing the packets mapping IP addresses and host names.
- Loaded a file of address book data.



When you search for host names, ASTEC Eyes will generate name service packets. Therefore, the network traffic will increase.

Searching for the Host Names of a Graph Item in the Monitor Window

In the Monitor windows for “IP Traffic by Source”, “IP Traffic by Destination”, and “IP Traffic by Host Pair”, you can select a Graph Item and search for the corresponding host name by the following steps:

1. Select a Graph Item in the Monitor window, and click on the Monitor window with the right mouse button.

A popup menu will appear as shown below:

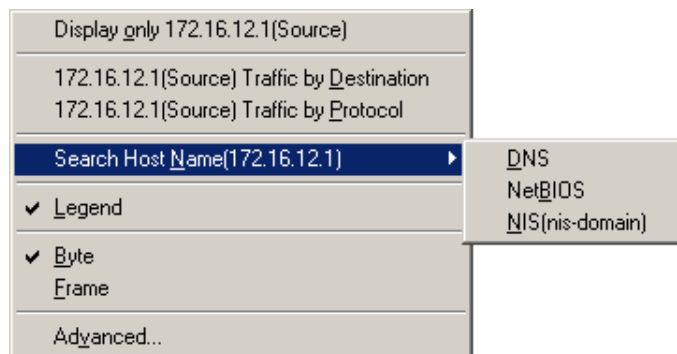


Figure 4-56 Popup Menu for searching the host names in the Monitor window

2. Choose **Search Host Name** from the popup menu.
A submenu listing the available name services will appear.
3. Choose the name service from the submenu.

The IP address being searched and the status will be shown in the Message window.

The host names found will be registered in the address book, and these names will be shown in the legend and tooltips of the Monitor windows.



If you did not specify a NIS domain name with the **Searching for Host Name** dialog box, a menu item for NIS in the popup menu will be grayed out.

Searching for Host Names with the IP Address Book

You can search for the host names for an IP address shown in the edit window of the IP address book.

This involves the following steps:

1. Click on the row you want to search for the host name for, with the right mouse button.

A popup menu will appear as show below:

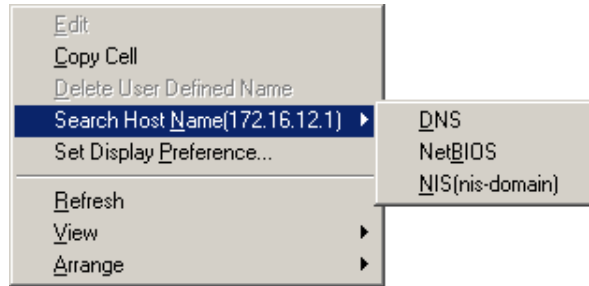


Figure 4-57 Popup Menu for searching the host names in the edit window of the IP address book

2. Choose **Search Host Name** from the popup menu.
A submenu listing the available name services will appear.
3. Choose the name service from the submenu.

The IP addresses being searched and the status will be shown in the Message window.

The host names found will be registered in the address book, and these names will be shown in the edit window of the IP address book.

Editing an Address Book

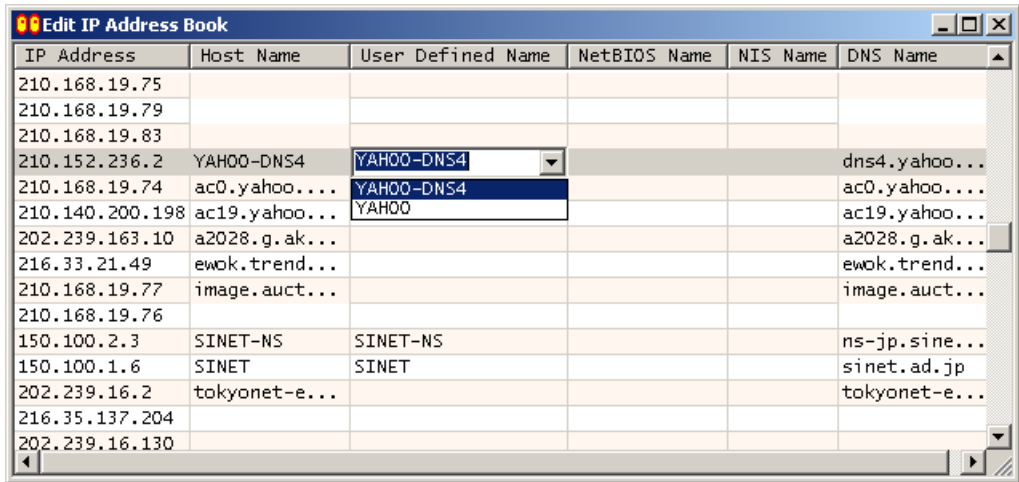
You can use a host name instead of an IP or MAC address to identify a host in the Monitor window, decode view, and stream view. With ASTEC Eyes, you can search for host names corresponding to an IP address, using the name services; DNS, WINS, and NIS. You can then use the host names found.

However, sometimes host names may not be found or you may want to use names easier to understand rather than actual host names. In such cases, you can edit the address book, giving arbitrary names to an IP or a MAC address.

There are two types of address books; one for the IP layer and the other for the MAC layer.

IP Address Book

To edit the IP address book, choose **IP Address Book** from the **Edit** menu on the menu bar of the Main window. The edit window of the IP address book will appear as shown in Figure 4-58.



IP Address	Host Name	User Defined Name	NetBIOS Name	NIS Name	DNS Name
210.168.19.75					
210.168.19.79					
210.168.19.83					
210.152.236.2	YAHOO-DNS4	YAHOO-DNS4			dns4.yahoo...
210.168.19.74	ac0.yahoo...	YAHOO-DNS4			ac0.yahoo...
210.140.200.198	ac19.yahoo...	YAHOO			ac19.yahoo...
202.239.163.10	a2028.g.ak...				a2028.g.ak...
216.33.21.49	ewok.trend...				ewok.trend...
210.168.19.77	image.auct...				image.auct...
210.168.19.76					
150.100.2.3	SINET-NS	SINET-NS			ns-jp.sine...
150.100.1.6	SINET	SINET			sinet.ad.jp
202.239.16.2	tokyonet-e...				tokyonet-e...
216.35.137.204					
202.239.16.130					

Figure 4-58 Edit window of the IP layer address book

The IP address book has six columns; IP Address, Host Name, User Defined Name, NetBIOS Name, NIS Name, and DNS Name. Clicking on the column header will sort the records in the book by the contents of this column.

The IP address book contains:

- Data found during monitoring,
- Data recorded in the log file,
- Data found by decoding captured data, and
- Data loaded from an address book file

In each of the **NetBIOS Name**, **NIS Name**, and **DNS Name** columns, host names returned by the corresponding name service are recorded.

You can enter arbitrary names in the **User Defined Name** column.

A name used as the host name is shown in the **Host Name** column. If you change the display preference of the host names, the name shown in this column will change. The

order of the columns to the right of the **Host Name** column is decided by the display preference of the host names. Suppose the preference is as follows:

1. User Defined Name
2. NetBIOS Name
3. NIS Name
4. DNS Name

Then, the order of these four columns will be User Defined Name, NetBIOS Name, NIS Name, and DNS Name from left to right.

If you specify a certain name service as unused, the corresponding column will not be shown.



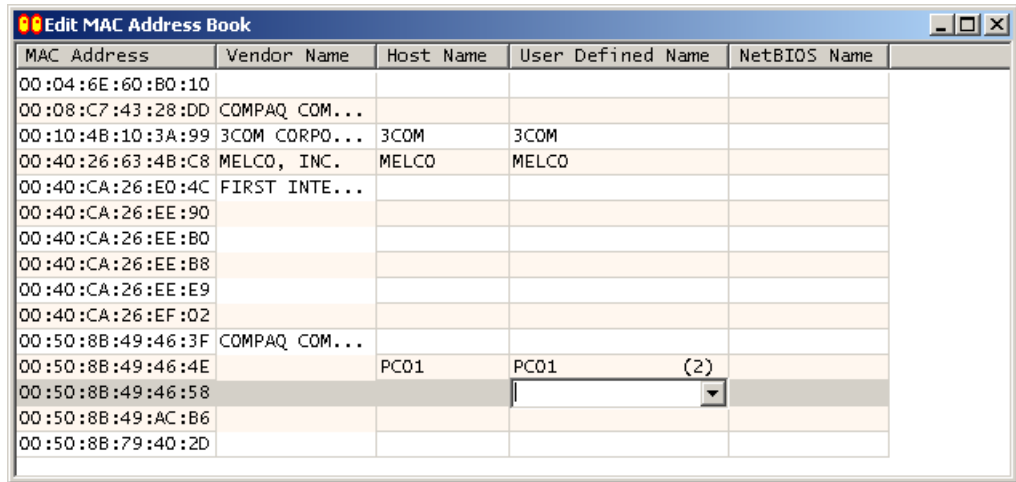
For a complete discussion of changing the display preference of the host names and disabling a particular name service, see “Configuring Host Name Preference” on page 156.



ASTEC Eyes has two address books; one is for IP layer and the other for MAC layer. There is no address book dedicated to an individual network interface. If you are monitoring multiple network interfaces, all the IP and MAC addresses found will be shown in the IP and MAC address book, respectively.

MAC Address Book

To open the MAC address book, choose **MAC Address Book** from the **Edit** menu on the menu bar of the Main window. The edit window of the MAC address book will appear as shown in Figure 4-59.



MAC Address	Vendor Name	Host Name	User Defined Name	NetBIOS Name
00:04:6E:60:B0:10				
00:08:C7:43:28:DD	COMPAQ COM...			
00:10:4B:10:3A:99	3COM CORPO...	3COM	3COM	
00:40:26:63:4B:C8	MELCO, INC.	MELCO	MELCO	
00:40:CA:26:E0:4C	FIRST INTE...			
00:40:CA:26:EE:90				
00:40:CA:26:EE:B0				
00:40:CA:26:EE:B8				
00:40:CA:26:EE:E9				
00:40:CA:26:EF:02				
00:50:8B:49:46:3F	COMPAQ COM...			
00:50:8B:49:46:4E		PC01	PC01 (2)	
00:50:8B:49:46:58				
00:50:8B:49:AC:B6				
00:50:8B:79:40:2D				

Figure 4-59 Edit window of the MAC address book

The MAC address book has five columns: MAC Address, Vendor Name, Host Name, User Defined Name, and NetBIOS Name. Clicking on the column header will sort the records in the book by the contents of this column.

The MAC address book contains:

- Data found by decoding captured data, and
- Data loaded from an address book file.

In the **Vendor Name** column, the vendor name obtained from the MAC address is shown.

You can enter arbitrary names in the **User Defined Name** column.

In the **NetBIOS Name** column, the NetBIOS names obtained by decoding captured data are shown.

In the **Host Name** column, a User Defined Name or a NetBIOS Name is shown. One of them will be adopted depending on the preference specified for selecting the host name. The order of the User Defined Name and NetBIOS Name columns is also dependent on the preference specified. If you disable the User Defined Name and/or NetBIOS Name upon specifying the preference, the corresponding column(s) will not be shown in the address book.

Entering User Defined Names

You can enter data into the User Defined Name column of the address book.

There are three ways to turn the column into the edit mode:

- Click on the target row with the left mouse button, or select the target row using the up and down arrow keys (<↑>, <↓>).
Click on the User Defined Name cell of the selected row again, or press the <F2> key.
- Double-click on the User Defined Name cell you want to edit.
- Click on the User Defined Name cell you want to edit with the right mouse button.
The popup menu will appear as shown below:

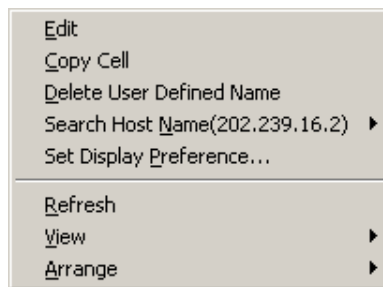


Figure 4-60 Popup menu on address book

Choose **E**dit from the popup menu.

When the cell is turned into the edit mode, a combo box will appear. Enter a name, and press the <Enter> key in the combo box.

You can enter more than one name by repeating the operation. If you enter more than one name, the number of the names entered will be shown on the right-hand side of the cell.

Deleting a User Defined Name

You can delete the User Defined Name by the following steps:

1. Turn the User Defined Name cell into the edit mode, and select the name you want to delete from the combo box.

2. Erase the name by pressing the <Delete> or <Backspace> key, and then press the <Enter> key.

OR

2. Click on the User Defined Name cell with the right mouse button.
A popup menu will appear as shown in Figure 4-60. Choose **Delete User Defined Name** from the popup menu.

Selecting a Name to Be Used from Candidates

In a name service, more than one name might be assigned to an IP address. In addition, more than one user defined name can be assigned to an IP or a MAC address. In such cases, the number of candidates will be shown in parentheses on the right-hand side of the cell. Among those names, you can choose the name to be used.

This involves the following steps:

1. Select the target row by clicking on it or using the up and down arrow keys (<↑>, <↓>).
2. Click on the cell containing the name you want to select.

OR

1. Click on the cell containing the name you want to select with the right mouse button.
A popup menu will appear as shown in Figure 4-60.
2. Choose **Edit** from the popup menu.

A drop down list will appear (or a combo box, for a user defined name). Choose a name then.

Changing the Display of an Address Book

An address book displays at most one name in each name service column by default. You can change the view of the address book to include the method the host name was obtained. You can also align the components of the IP addresses.

To change the display of the address book, click somewhere in the edit widow of the IP or MAC address book with the right mouse button. A popup menu will appear. Choose **View** from the popup menu. Then, a submenu will appear as shown in Figure 4-61.

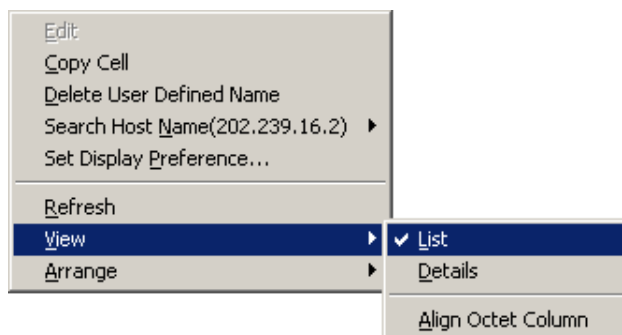


Figure 4-61 Popup menu whose “View” item is selected

Choose an item from the submenu. The display will change accordingly.

- **List**

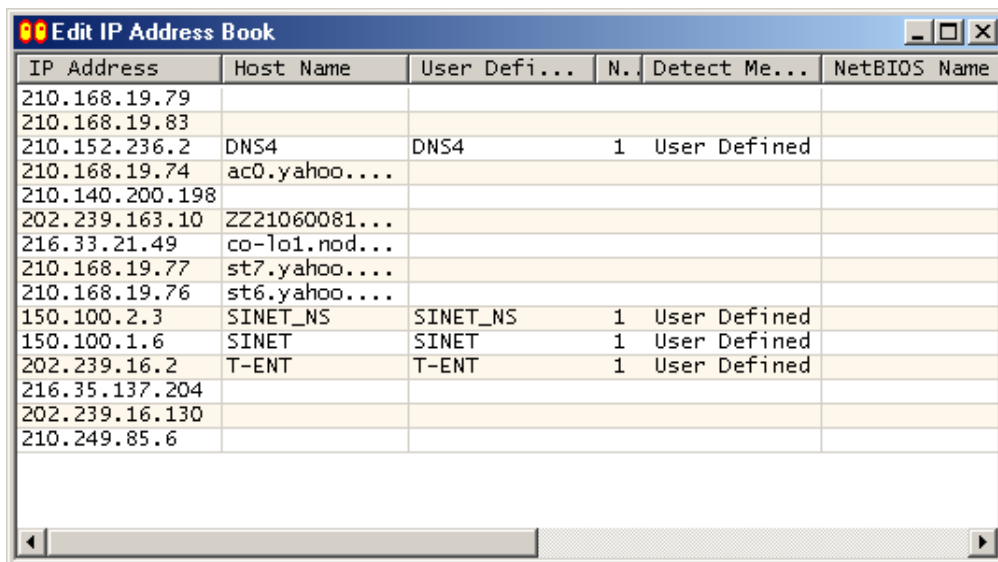
This is the default setting. If more than one host name are assigned, the number of candidates will be also shown.

- **Details**

For each name service, the columns to show the number of host names and the method they were obtained are added. One of the followings will be shown as the method.

Search	Found by the search of ASTEC Eyes
File	Loaded from an address book file
User Defined	Entered into the address book by the user
Decoder	Found while decoding captured data
Monitor	Found during monitoring
Log	Recorded in the log file

Figure 4-62 shows the edit window of the IP address book in detail display mode.



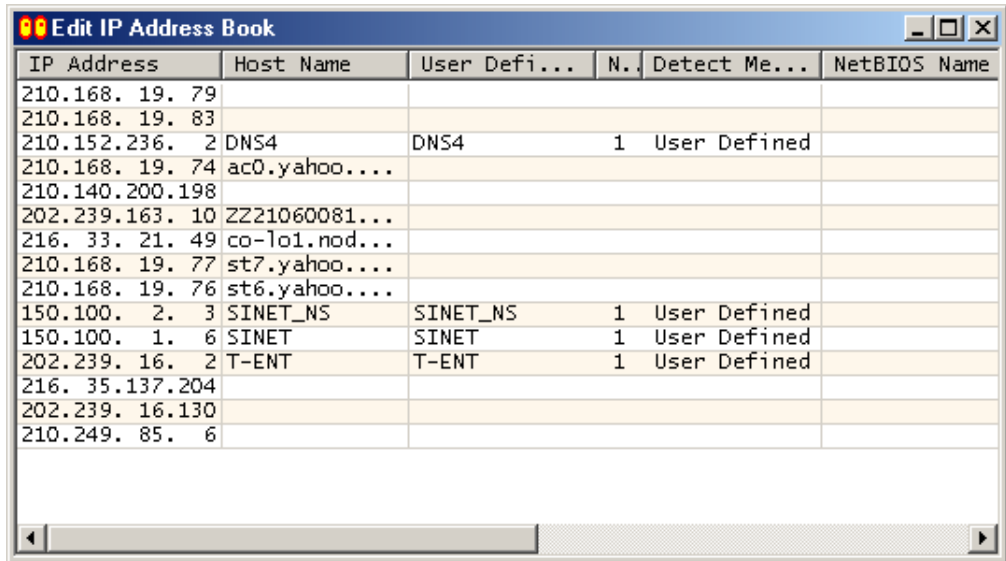
IP Address	Host Name	User Defi...	N.	Detect Me...	NetBIOS Name
210.168.19.79					
210.168.19.83					
210.152.236.2	DNS4	DNS4	1	User Defined	
210.168.19.74	ac0.yahoo....				
210.140.200.198					
202.239.163.10	ZZ21060081...				
216.33.21.49	co-1o1.nod...				
210.168.19.77	st7.yahoo....				
210.168.19.76	st6.yahoo....				
150.100.2.3	SINET_NS	SINET_NS	1	User Defined	
150.100.1.6	SINET	SINET	1	User Defined	
202.239.16.2	T-ENT	T-ENT	1	User Defined	
216.35.137.204					
202.239.16.130					
210.249.85.6					

Figure 4-62 Edit window of the IP address book in detail display mode

- **Align Dots**

This menu item exists only in the edit window of the IP address book.

If IP addresses are set to align dots, the dots will be vertically aligned and the digits will be right-adjusted as shown in Figure 4-63. IP addresses are left-adjusted by default.



IP Address	Host Name	User Defi...	N.	Detect Me...	NetBIOS Name
210.168. 19. 79					
210.168. 19. 83					
210.152.236. 2	DNS4	DNS4	1	User Defined	
210.168. 19. 74	ac0.yahoo....				
210.140.200.198					
202.239.163. 10	ZZ21060081...				
216. 33. 21. 49	co-1o1.nod...				
210.168. 19. 77	st7.yahoo....				
210.168. 19. 76	st6.yahoo....				
150.100. 2. 3	SINET_NS	SINET_NS	1	User Defined	
150.100. 1. 6	SINET	SINET	1	User Defined	
202.239. 16. 2	T-ENT	T-ENT	1	User Defined	
216. 35.137.204					
202.239. 16.130					
210.249. 85. 6					

Figure 4-63 Edit window of the IP address book in align dots display mode

The Popup Menu on an Address Book

If you click somewhere in the edit window of the IP or MAC address book with the right mouse button, a popup menu will appear as shown in Figure 4-64.

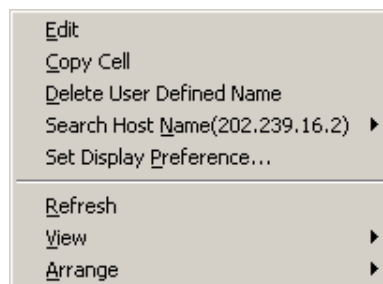


Figure 4-64 Popup Menu on Address Book

This popup menu will be slightly different depending on the position (the row and the cell) you click on. Some of the menu items may be grayed out in some situations.

- **Edit**

This menu item is enabled when you click on a User Defined Name cell or a cell with more than one name assigned.

Clicking on a User Defined Name cell will show a combo box. You can type the host name or choose one from the drop down list.

Clicking on a cell with more than one name assigned will show a list box. You can choose a host name from the list.
- **Copy Cell**

Copies the text of the cell you click on into the clipboard.
- **Delete User Defined Name**

This menu item is enabled when you click on a User Defined Name cell. The host name in the cell will be deleted.
- **Search Host Name**

This menu item is enabled when you click on an edit window of the IP address book. The **Search Host Name** will search for the host names of the IP address you click on. A submenu listing name services will appear. Choose the name service to be used for the search. The host names found will be registered in the address book.
- **Set Display Preference...**

The **Configure Options** dialog box will appear. It includes only the **Display Host Name** page. For more information, see “Configuring Host Name Preference” on page 156. The name service columns will be ordered according to the display preference setting.
- **Refresh**

Immediately updates information in the edit window of the IP or MAC address book.
- **View**

A submenu for changing the view will appear. The following menu items are included in the submenu.

<u>L</u>ist	Displays a host name only. If there are more than one host name, the number of candidates will be displayed on the right edge of a cell, too. This is the default setting.
<u>D</u>etails	Displays a host name, the number of the candidates, and the method the host names are obtained.

Align Dots

This item appears only when you click on the edit window of the

IP address book. The dots will be vertically aligned and the digits will be right-adjusted.

- **A**rrange

Shows a submenu. The columns of the address book are listed as menu items. Choosing an item in the submenu, rows in the table will be sorted by the contents of the selected column.



Even if you do not choose **R**efresh, the information shown in the edit windows of the IP and MAC address books will be updated periodically.

Searching an Address Book for Text

You can search the edit windows of the IP and MAC address books for text.

Choose **F**ind... from the **E**dit menu on the menu bar of the Main window, or press the <Ctrl-F> key.

The **F**ind dialog box will appear. Type the text you want to search, and click the **F**ind **N**ext button.

Saving and Loading Address Book Data in a File

You can save address book data (address and host name) into a file.

Choose **S**ave **A**ddress **B**ook... from the **F**ile menu on the menu bar of the Main window.

The **S**ave **A**s dialog box will appear. Enter a file name and save it.

Conversely, you can load the data saved in a file.

Loading address book data in advance, host names can be displayed in the Monitor windows for the IP layer, decode view, stream view, and so on, without a search.

Choose **L**oad **A**ddress **B**ook... from the **F**ile menu on the menu bar of the Main window.

The **O**pen dialog box will appear. Enter a file name in the dialog box.



If you save address book data as `default-address.txt` in the directory where the executable of ASTEC Eyes (`EYE.exe`) is located, then the next time you invoke ASTEC Eyes, the data will be automatically loaded.



If you assign the IP address for a computer dynamically, using DHCP for example, it is not guaranteed that the same IP address as before is assigned when you restart the computer. Therefore, the mapping of the IP address and the host name may differ from that in an address book file.

Printing

You can print the monitoring information of the Monitor window. You can also print the address information shown in the edit windows of the IP and MAC address books.

Choose **P**rint... from the **F**ile menu on the menu bar of the Main window.



When the focus is not on the Monitor window, **P**rint... is grayed out.

Index

Symbol

<Alt-0> 78, 167
<Alt-1> 77
<Alt-2> 77
<Ctrl-C> 94, 112, 128, 183
<Ctrl-End> 112
<Ctrl-F> 86, 113, 203
<Ctrl-Home> 112
<Ctrl-O> 103
<Ctrl-PageDown> 168
<Ctrl-PageUp> 168
<Ctrl-Space> 87
<Ctrl-V> 94, 128, 183
<End> 112
<F2> 155, 197
<Home> 112
<PageDown> 112
<PageUp> 112
<↑> 79, 87, 112, 135
<↓> 79, 87, 112, 135
<←> 112
<→> 112
<Alt-↑> 112
<Alt-↓> 112
<Ctrl-↑> 112
<Ctrl-↓> 112
<Ctrl-Alt-←> 168
<Ctrl-Alt-→> 168
<z> 112

A

Actions when buffer is full 96, 153
Address book
 editing 193
 loading 203
 printing 204
 saving 203
 searching text 203
Administrator privileges 5, 8, 25
Analysis
 captured data 52, 103
 traffic 30, 80
AND group (filter editor) 174, 181
Apply Display Filter 121
ASTEC Eyes
 evaluation edition 6
 exiting 73
 installation 5
 invoking 8, 25
 uninstallation 10

B

Bar chart 49, 84
Breakdown of traffic 35, 89
Buffer full
 capture buffer 96, 153
 dialog box 97
 TCP (window frozen) 18, 146
bzip2 53, 97, 104, 131

C

.cap (file extension) 97, 104
 Caption filter 20, 56, 114
 Capture 52, 95
 appending data 96
 buffer full 96
 discarding captured data 76, 96, 143
 saving captured data 53, 76, 97
 starting/pausing 52, 76, 95, 143
 Capture buffer 52, 95
 buffer full 96, 153
 buffer size 153
 Capture Buffer Meter 52, 75, 95, 98
 Capture filter 59, 99, 172, 175
 Capture option 152
 Pause capture 96, 153
 Wrap around 96, 153
 Changing
 display filter name 181
 display format 48, 84
 font 163
 interface label 29, 136
 workspace property 69, 169
 Chart
 displaying 31
 printing 204
 reverting to the previous chart 42, 91
 Chart defaults options 160
 Check mark
 disable 115, 118
 enable 21, 115, 118
 Common toolbar 26, 76
 Condition group 174, 181
 Configuration
 capture option 152
 chart defaults 88, 160

 decode hint 42, 153
 expert events 147
 font 163
 host name preference 156
 interface 29, 143
 loading 76, 165
 log 129
 monitor options 159
 saved in the registry 166
 saving 70, 76, 86, 164
 workspace 69, 169
 Configuration privilege 99, 140, 144
 Connecting to Remote Module 18, 71, 137
 Continuous capture 19, 99
 configuration 142, 145
 configuration privilege 99
 directory 100
 maximum file size 100
 starting/stopping 101
 Convenience filter 20, 59, 114
 discarding 111, 121
 Copy and paste
 address book 191
 decode data 127
 filter editor 183
 monitoring information 94

D

Decode data
 copy and paste 127
 saving 124
 Decode hint 42, 70, 128, 153
 Decode view 53, 54, 103, 105
 creating 76, 103
 Dump pane 54, 105
 key bind 112

- Packet Detail pane 54, 105
 - searching text 64, 113
 - Summary pane 54, 105
 - toolbar 110
 - Decoded data
 - saving 107
 - statistics 121
 - DECODER EXCEPTION 128
 - Decoding 52, 103
 - captured data 53, 103
 - divided data 22, 122
 - error 128
 - file 76, 103
 - default-address.txt 204
 - default-workspace.wsi 166
 - Deleting log file 131
 - Dialog box
 - Candidate List 117
 - Configure Options 43
 - Capture 43, 152
 - Chart Defaults 160
 - Decode Hints 44, 154
 - Display Host Name 157
 - Monitor 159
 - Other 163
 - Connect 71, 138
 - Displaying Log 134
 - Find 64, 86, 113, 203
 - Font 164
 - Host Properties 141
 - Continuous Capture 100
 - Log 130
 - Interface Properties 29
 - Continuous Capture 101
 - Expert 148
 - Information 144
 - Log 132
 - Log Properties 136
 - Open with Filter 123
 - Option 116
 - Output Format 126
 - Save Decoded Results 125
 - Searching for Host Name 39, 190
 - Workspace Properties 69, 169
 - Directory
 - continuous capture 100, 141
 - default-address.txt 204
 - default-workspace.wsi 166
 - log 131, 133
 - Discarding
 - captured data 96
 - convenience filter 111, 121
 - Display filter 114, 121, 172, 175
 - changing name 181
 - Display format 48, 84
 - Displaying
 - chart 31
 - expert event 149
 - host name 156
 - log 132, 135
 - Monitor window 32, 81
 - TopN Graph Items 85, 161
 - traffic 31
 - DNS 39, 156, 190, 194
 - Domain name (of NIS) 40, 90, 165, 190
 - Drag and drop (filter editor) 184
 - Dump pane 54, 105, 108
- ## E
- .ebz (file extension) 53, 97, 102, 104
 - Editing
 - IP address book 194
 - MAC address book 195
 - Enable check mark 115, 118
 - .enc (file extension) 97, 102, 104

- Ephemeral port 42, 153
- Error in decoding data 118, 128
- Event Viewer window 149
- Exiting ASTEC Eyes 73
- Expert events 146
 - configuration 147
 - displaying 149
- F**
- File extension
 - .cap 97, 104
 - .ebz 53, 97, 102, 104
 - .enc 97, 102, 104
 - .jil 102, 104
 - .wsi 166
- File format
 - captured data 53, 97, 104
 - configuration file 166
 - continuous capture 104
 - Microsoft Network Monitor 104
 - Sniffer 53, 97
 - snoop 97, 104
 - tcpdump 97, 104
- Filter
 - caption filter 20, 56, 114
 - capture filter 59, 99, 172, 175
 - convenience filter 20, 59, 114, 121
 - display filter 114, 121, 172, 175
 - header attribute filter 20, 57, 114, 119
 - monitor filter 21, 91, 172, 175
- Filter editor 172
 - AND group 174, 181
 - condition group 174, 181
 - copy and paste 183
 - drag and drop 184
 - loading filter 174, 186
 - logical expression 174, 176
 - OR group 174, 181
 - saving filter 174, 186
 - unary expression 174
- Focus
 - Dump pane 110
 - Interface Selector window 77
 - Message window 77
 - Packet Detail pane 110
 - Summary pane 110
 - workspace 78, 167
- Font 163
- G**
- Graph Item 36, 84
 - displaying TopN 85, 161
 - Others 85, 161
 - restriction 161
 - selecting 36, 86
- H**
- Header attribute filter 20, 57, 114, 119
- Hexadecimal dump 54, 105, 108
- Host name 194
 - preference 156, 191
 - searching 39, 90, 189, 192
- Host property 140
- I**
- Installation 5
 - ASTEC Eyes 5
 - Remote Module service 8
- Interface
 - changing label 29
 - information 144

- log information 136
 - property 29, 143
 - selecting 28, 78
 - Interface Selection listbox 26, 28, 75, 76
 - Interface Selector window 26, 28, 75, 77, 133
 - Interface toolbar 76
 - Invoking
 - ASTEC Eyes 8, 25
 - IP address 92, 194
 - IP address book
 - changing display 198
 - editing 194
 - printing 204
 - searching host name 192
 - IP address table 91
 - IP Traffic 31, 83
 - IP Traffic by Destination 83
 - IP Traffic by Host Pair 83
 - IP traffic by Protocol 83
 - IP Traffic by Source 83
- J**
- .jil (file extension) 102, 104
- K**
- Key bind
 - on decode view 112
 - on legend 87
 - on stream view 112
- L**
- Legend
 - key bind 87
 - showing/hiding 35, 84, 88
- License
 - network license 7
 - Registration 6
 - stand-alone license 6
 - Line chart 32, 84
 - Loading
 - address book 203, 204
 - configuration 165, 166
 - filter 186
 - Log 129
 - deleting 131
 - directory 131, 133, 140
 - displaying 132, 135
 - interface information 136
 - log file 129
 - stopping 10
 - Logical expression 176
- M**
- MAC - IP address table 93
 - MAC address 91, 196
 - MAC address book
 - changing display 198
 - editing 195
 - printing 204
 - MAC address table 91
 - MAC Error Frames 84, 91, 122
 - MAC Frames by Size 83, 91
 - MAC Traffic 82, 122, 161
 - MAC Traffic by Address Type 83
 - MAC Traffic by Destination 83
 - MAC Traffic by Host Pair 83
 - MAC Traffic by Protocol 83
 - MAC Traffic by Source 83
 - Main window 26, 75
 - Interface Selection listbox 76
 - Interface Selector window 77

- status bar 26, 77
- toolbar 26, 76
- workspace 26, 78
- Message window 77
- Microsoft Network Monitor 97, 104
- Monitor filter 21, 91, 172, 175
- Monitor option
 - monitoring period 89, 160
 - refresh interval 160
- Monitor window 32, 81
 - bar chart 49, 84
 - displaying 32, 81
 - Graph Item 84
 - line chart 84
 - pie chart 50, 84
 - popup menu 33, 88
 - searching text 51, 86
 - table format 51, 84, 86
- Monitoring 30, 80
 - copy and paste 94
 - pausing 81
 - printing 204
 - saving information 93
 - starting 30, 80
- Monitoring period 89, 160
- Multiple selections 116

N

- Name service 39, 156, 190
- NetBIOS 39, 158, 190, 194
- Network interface
 - information 144
 - log information 136
 - property 29, 143
 - selecting 28, 78
- Network traffic 28
- New Decode View 76, 103

- NIC (Network Interface Card) 28, 78
- NIS 39, 156, 190, 194
- Number of entries in a file (log) 130

O

- Operation
 - Remote Module 139
 - Remote Module interface 142
 - window 171
- Option dialog box
 - multiple selections 116
 - Range 117
 - searching text 116
 - Substring match 116
- Options
 - capture 152
 - chart defaults 160
 - configuration 151
 - decode hint 153
 - font 163
 - host name preference 156
 - monitoring 159
- OR group (filter editor) 174, 181
- Others (Graph Item) 85, 161
- Output interval (log) 130

P

- Packet Detail pane 54, 105, 108
- Pause capture (capture option) 96, 153
- Pause capture trigger 98, 172, 175
- Pausing
 - capture 52, 76, 96, 143
 - monitoring 81
- Pie chart 50, 84
- Plug and play 22, 145
- Popup menu

- address book 197, 201
- filter editor 188
- host 129, 139
- interface 81, 142
- Interface Selector Window 137
- log 134
- Message window 77
- Monitor submenu 82
- Monitor window 33, 88, 90
- workspace 66, 167

Printing 204

Privilege

- Administrator privileges 5, 8, 25
- configuration privilege 99, 140, 144

Product support 16

Property

- host 140
- interface 29, 143
- workspace 69, 169

Protocol list 12

Proxy server 42, 153

R

- Range (Option dialog box) 117
- Record (TCP) 108
- Red check box 118, 128
- Refresh interval 160
- Registration (license) 6
- Registry (information is saved) 166
- Remote Module 3, 18, 71, 137
 - configuration privilege 140
 - connecting 71, 137
 - installing service 8
 - license registration 7
 - uninstallation 10
- Remote watching 18, 71, 137

- statistics 137

Restriction (Graph Item) 161

Reverting to the previous chart 42, 91

RFC (Request For Comments) 55, 106, 178

Runtime environment 3

S

Saving

- address book 203
- captured data 53, 97
- configuration 70, 164
- currently shown packets 121
- decoded data 76, 107, 124
- filter 174, 186
- in the registry 166
- monitoring information 93

Searching host name 39, 90, 189, 192

Searching text

- address book 203
- decode view 64, 113
- Monitor window 51, 86
- Option dialog box 116
- stream view 64, 113

Selecting

- Graph Item 36, 86
- interface 28, 78

Sniffer format 53, 97, 104

snoop 22, 97, 104

Start capture trigger 98, 172, 175

Starting

- capture 52, 76, 95, 143
- monitoring 30, 80

Statistics

- decoded data 121
- logging 129
- remote watching 137

- traffic 80
- type 82
- Status bar (Main window) 26, 77
- Stopping logging 10
- Stream view 60, 61, 103, 108
 - Dump pane 108
 - key bind 112
 - Packet Detail pane 108
 - searching text 64, 113
 - Summary pane 108
 - toolbar 110
- Substring match 116
- Summary pane 54, 105, 108
- Supported protocols 12, 22

T

- Table format 51, 84, 86
- TCP virtual stream 63, 103, 107
- tcpdump 22, 97, 104
- Toolbar
 - Common toolbar 26, 76
 - decode view 110
 - Interface toolbar 26, 76
 - stream view 110
- TopN (Graph Item) 85, 161
- Traffic
 - analysis 30
 - breakdown 35, 89
 - displaying 28, 31
 - long-term trend 129
 - statistics 80
 - type 82
- Trend of traffic 129
- Trigger
 - pause capture trigger 98, 172, 175
 - start capture trigger 98, 172, 175
- Typographical convention 2

U

- Unary expression 174
- Uninstallation 10
- Unknown Protocol 15, 42
- Unknown Response 60
- Unknown TCP Protocol 15, 42, 153
- Unknown UDP Protocol 15, 42, 153

V

- Vendor name 91

W

- Well-known port 42, 153
- Window
 - decode view 53, 54, 103, 105
 - Event Viewer 149
 - Interface Selector window 77
 - MAC - IP address table 93
 - Main window 26, 75
 - Message window 77
 - Monitor window 32, 81
 - operation 171
 - stream view 60, 61, 103, 108
 - workspace 68
- WINS 39, 156, 190, 194
- Workspace 66, 78, 167
 - property 69, 169
- Wrap around (capture option) 96, 153
- .wsi (file extension) 166