

EtherPeek™v. 3.5 QuickTour

**A Step-by-Step Guide Through Your
EtherPeek Software**



**The AG Group, Inc.
2540 Camino Diablo, Suite 200
Walnut Creek, CA 94596
USA**

(510) 937-7900

fax (510) 937-2479

Email: info@aggroup.com

Internet: [ftp.aggroup.com](ftp://ftp.aggroup.com)

Visit our Worldwide Web Site: <http://www.aggroup.com/>

WELCOME TO ETHERPEEK™ v. 3.5

EtherPeek is a network and protocol analysis tool designed to help you troubleshoot, optimize, plan and configure networks. EtherPeek works by capturing all network traffic and providing the tools to filter, analyze and interpret traffic patterns, data packet contents, statistics and protocol types.

While EtherPeek is an excellent diagnostic tool for determining the source of network problems as they occur, it also has a rich set of features that allow you to proactively baseline and monitor your network. Using EtherPeek's many graphical displays, including the new Summary Statistics window incorporated in this release, you can easily learn what various protocol communication links look like and understand the composition of traffic on your network. Becoming familiar with network usage patterns can alert you to potential performance and configuration problems, and provide you with the information to quickly identify and remedy any anomalous network condition.

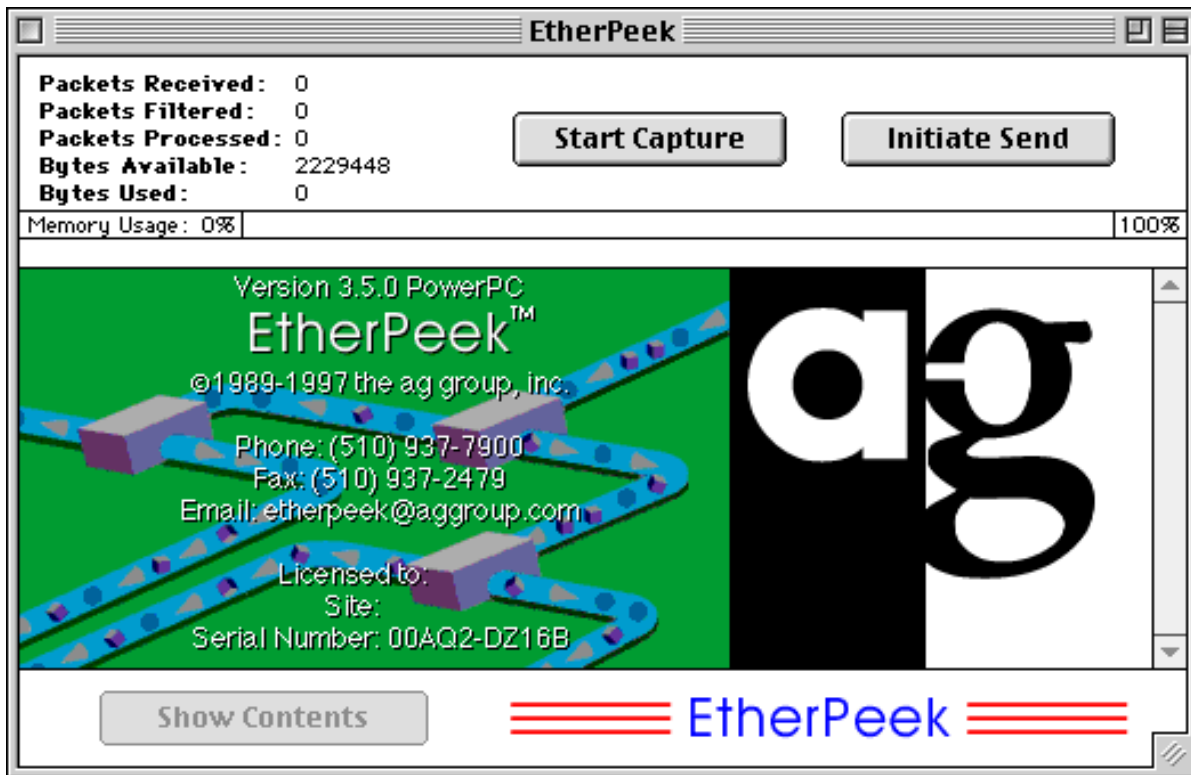
Each section of this document is a brief overview of a major feature of EtherPeek 3.5, our most current release, with step-by-step examples to help you exercise key features of the software.

GETTING STARTED— JUST DOUBLE-CLICK

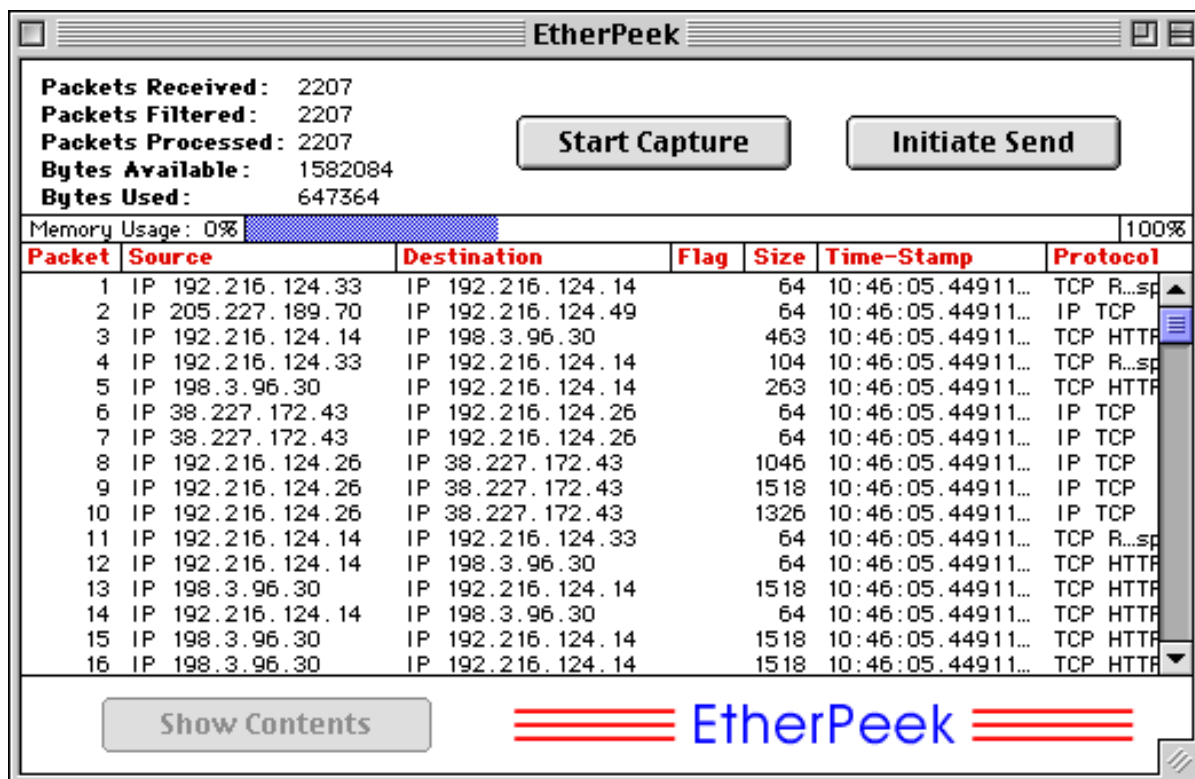
EtherPeek captures all conversations on a network, much like a telephone tap, and provides you with a wealth of features for dissecting this traffic to discover potential network problems and traffic patterns. This QuickTour walks you through a look at some of the traffic from your network.

To see live traffic on your network, just follow these point-and-click instructions:

1. After running the Installer program, launch the application by double-clicking on the "EtherPeek™" icon.
2. Select an interface from which to run EtherPeek.
Note: If you are launching EtherPeek from a non-PCI Macintosh with only one Ethernet interface, your machine will be dedicated to the program's use while EtherPeek is capturing packets. During capture, all other network services (email, filesharing, etc.) will be disabled. If you wish to maintain network services while capturing packets with EtherPeek, we recommend that you run EtherPeek from a machine with two Ethernet interfaces - one from which you can run EtherPeek and one from which network services can be run.
IMPORTANT: If you are launching EtherPeek from a PCI bus-based, non G3 Desktop Macintosh with Open Transport and wish to use the built-in port for capturing packets, choose the Slot 0: Macintosh 4a option from the Select Ethernet window. The second choice, the motherboard option, will only work with Desktop G3 PowerMacintoshes.
3. Click on "Start Capture."
4. Click "OK" to disconnect AppleTalk network services if prompted to do so.



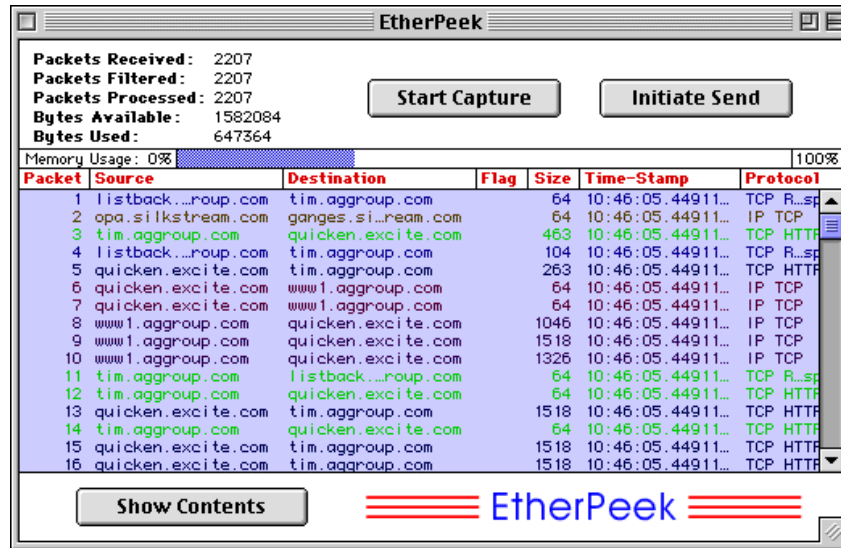
You will now begin to see packets from your network processed and displayed in EtherPeek's Main Window. Packet information is displayed by logical source and destination address, flags (indicating errors in packets or 802.3 LLC packets), protocol type, packet size and time-stamp. To change the packet information displayed in the Main Window and rearrange column positions, please see Feature Focus #2. For a way to easily designate names for many of these often-unfamiliar source and destination addresses, please review Feature Focus #1.



FEATURE FOCUS #1: AUTOMATIC NAME RESOLUTION

Name-To-Address Mapping Keeps Your Network Familiar

Summary: For easy identification of network activity, use EtherPeek to automatically map IP and AppleTalk network IDs to corresponding machine names and show node names instead of physical or logical addresses in the Main Window and Statistics Windows.



By default, EtherPeek displays source and destination information for each data packet in logical (IP, AppleTalk, DECnet, IPX, etc.) address format. To make this information easier to recognize, you can create a Name Table that correlates each network device name with its logical address(es) as well as the device's Ethernet or physical address.

Resolving Names for IP and AppleTalk Logical Addresses:

1. Launch EtherPeek and capture packets, or load a saved packet file into EtherPeek's memory.
2. When packets are displayed in the Main Window, select all of them by using the "Command A" key, or the "Select All" Command from the Edit menu.
3. Choose "Resolve Names" from the Special Menu.

IMPORTANT: This feature actively requests name information from the network. In order for it to work, EtherPeek needs to be able to send packets out using AppleTalk and TCP/IP services. If you attempt to resolve names while EtherPeek is actively capturing packets and network services have been disabled for your Ethernet interface, then it cannot resolve names unless you have a second active Ethernet interface. Alternately, you can wait until packet capture has stopped and then resolve names when network services have been restored.

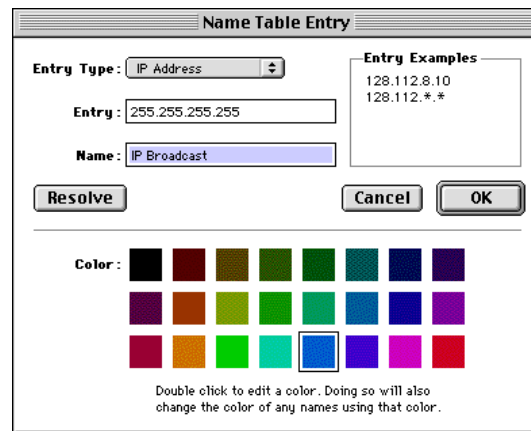
EtherPeek will then actively query Domain Name Services for any IP device names, and send Name Binding Protocol (NBP) requests for AppleTalk user or machine names associated with your selected packets. A small progress window will be displayed as the name resolution operation proceeds. Once the search is completed, any names discovered will be added to EtherPeek's Name Table, and name entries will automatically replace logical or physical address representations for packet source and destination information in the Source and Destination columns in the Main Window.

Note: EtherPeek 3.5 also resolves physical addresses for IP and AppleTalk devices. During the name resolution process, entries that map names to Ethernet addresses will also be added to the Name Table.

Besides making packet information more familiar for you as you monitor and analyze your network, creating Name Table entries provides the ability to view the name, logical and physical address for network devices side-by-side in the Main Window so that you can easily maintain a current inventory of devices and their corresponding network addresses.

Step-by-Step Example: Adding Name Table Entries Manually

1. Click on any packet in the Main Window.
2. Select "Insert Into Name Table" from the Special menu.
3. Enter name for first address and select a color.
4. Enter name for second address and select a color.
5. Click "OK".



After following these steps, you'll see that EtherPeek substitutes identifiable node names for the addresses you've selected in the Main Window or any node statistics window.

Step-by-Step Example: Add Vendor IDs to Name Table

EtherPeek ships with a current IEEE list of Vendor IDs, properly formatted for the Name Table.

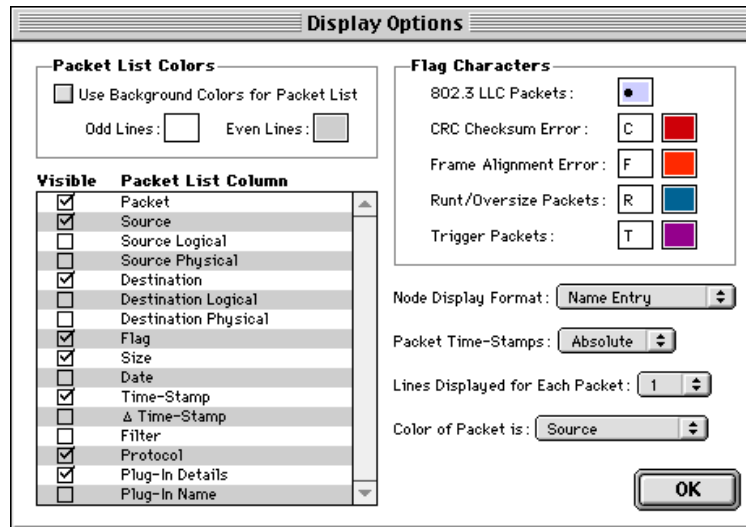
These IDs provide the vendor name associated with the NIC or device in place of the first three bytes of the physical address of that node. When Vendor IDs are added to the Name Table, EtherPeek can display the manufacturer's name associated with the physical address of each device sending or receiving packets from your network in the Main Window and all node statistics windows. If you are trying to track down a network problem and the majority of your network traffic is not IP or AppleTalk, you can import Vendor IDs to associate the packet data with specific manufacturer's names for communicating NICs and network devices.

1. Select "Name Table" from the Special menu.
2. Select "Import Names" from the File menu.
3. Choose "No" when asked if you wish to clear existing entries from the Name Table.
4. Locate the "Names and Filters" Folder. Open the folder called "Vendor IDs". The full list of Vendor IDs will be appended to the bottom of the names list that already exists in EtherPeek's Name Table.

FEATURE FOCUS #2: CUSTOMIZABLE MAIN WINDOW

Customizable Display, Visual Cues Help Highlight Problems Quickly

Summary: The column content, color, and format in which packet information is displayed in EtherPeek's Main Window can be changed and re-arranged for customized viewing. For example, you can view logical and physical addresses side-by-side, flag error packets, colorize web server traffic, change timestamp representations, and more.



To view and exercise the many options available for customizing the Main Window display, follow these steps:

1. Choose "Display " from the Options Menu.
2. Select elements of the packet to display, and format the information for easy reading:
 - **Packet List Colors:** Enable the use of alternating colors for odd and even numbered packets by checking "Use Background Colors for Packet List."
 - **Packet List Column:** Check the elements of the packet you would like to display in the Main Window.
 - **Flag Characters:** Re-define the way 802.3, error and trigger packets are flagged and colorized.
 - **Node Display Format:** Select whether packets will be identified by physical address, logical address or symbolic name if there is a Name Table entry for a node.
 - **Packet Time-Stamps:** Choose absolute time (Macintosh system clock), relative time (elapsed time since last packet was received) or session time (from Start Capture command).
 - **Lines Displayed for Each Packet:** Select the number of lines per packet that will be displayed in EtherPeek's Main Capture Window. Multiple lines per packet displays the data as hexadecimal digits and ASCII text.
 - **Color of Packet is:** Determine how colors will be used in displaying packets.
3. Click "OK" to close the Display Options Window and view your changes in EtherPeek's Main Window.

Re-positioning Main Window Columns

You can rearrange the Main Window columns by moving your cursor to the column headings. The cursor will then change into a hand that can "grab" the heading and move it to any other column heading position.

FEATURE FOCUS #3: PLUG-INS

Expert Analysis Features Expand EtherPeek's Built-in Functionality

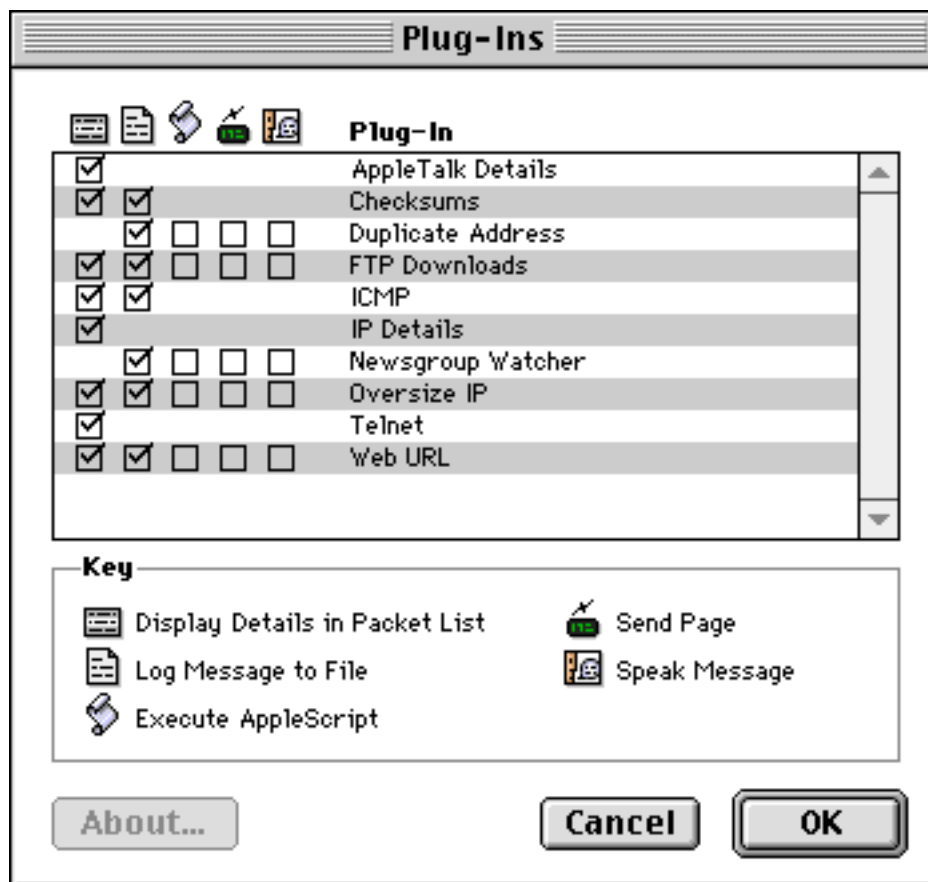
Summary: Plug-in modules included with EtherPeek increase the program's built-in functionality. Plug-ins provide an automatic method of analyzing packet contents during or after capture - sorting, displaying or logging specific information from some or all of the packets captured.

The current set of EtherPeek 3.5 Plug-ins provide the ability for the program to:

- Extract AppleTalk packet details (Transaction IDs, NBP Lookups, etc.)
- Verify checksums for AppleTalk and IP packets
- Detect duplicate IP addresses in use
- Log ftp transfer file names
- Detect when a destination host or port is unreachable.
- Extract IP packet detail like Transaction IDs, Session IDs and port numbers.
- Detect Land Attacks.
- Display Ping of Death packets.
- Display contents of Telnet sessions.
- Log Web URL and Usenet newsgroup accesses.

Activate Plug-In Modules:

1. Select "Plug-Ins" from the Special Menu.
2. Check to specify an action based on the capture of packets through a particular Plug-In.
3. Click "OK" to apply.



Note: By default, all Plug-in modules are enabled when EtherPeek is launched for the first time. Packet filtering by Plug-ins can provide overhead that may tax Macintoshes with slower processors. To maximize Plug-in results and EtherPeek's effectiveness at capturing all packet traffic when analyzing your network, it is suggested that you enable only those Plug-ins relevant to your purpose.

Post-capture Plug-In Use:

Plug-ins can be applied to incoming packets as well as packets already loaded into EtherPeek's memory. For post-capture plug-in use, first select the packets in the Main Window with the "Command A" keys and then select "Apply Plug-In" from the Special Menu to specify and activate a plug-in.

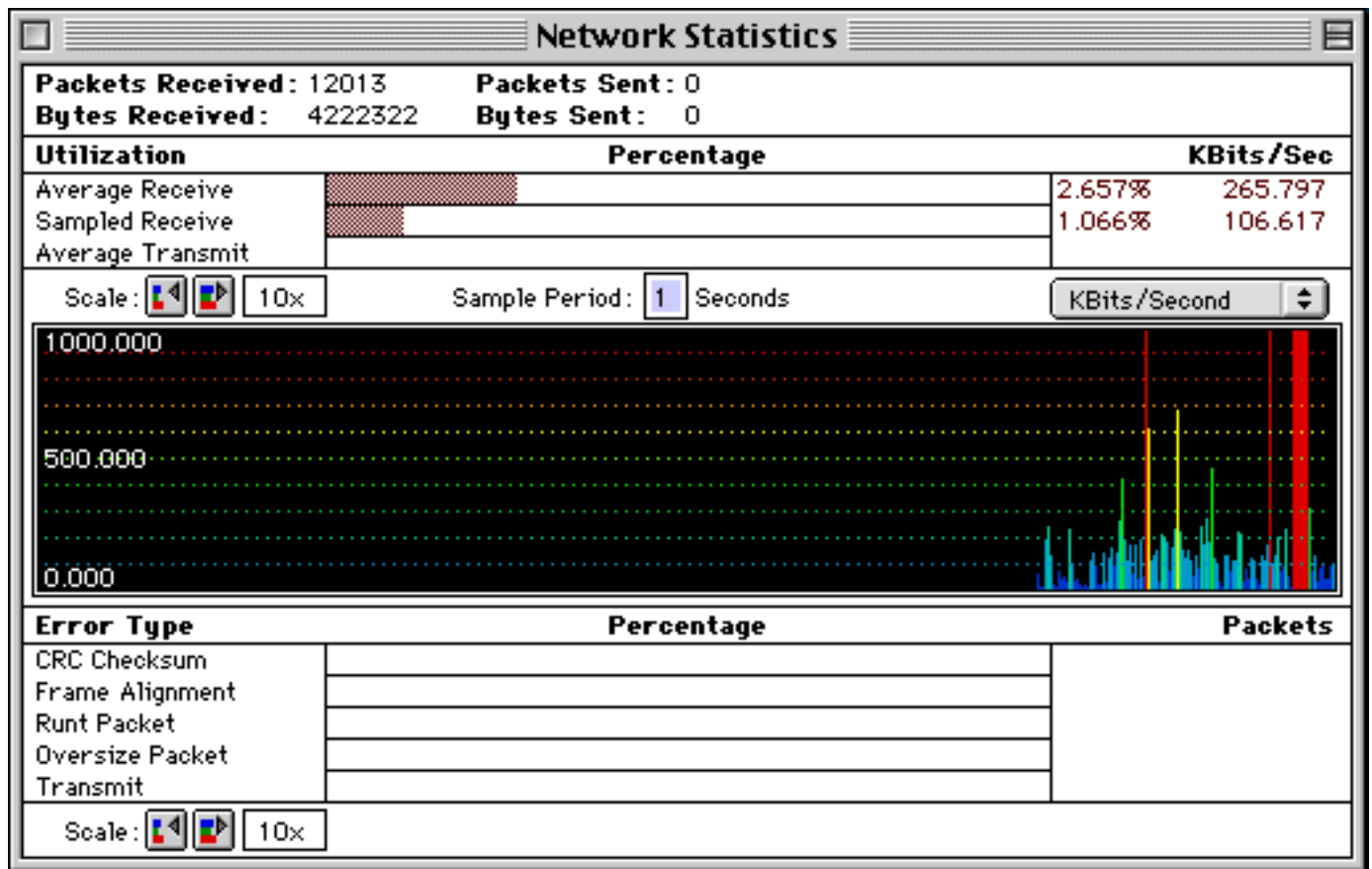
Note: To view the contents of the log file, select "Log Window" under the File Menu. In addition to Plug-in information, the log also keeps track of other events such as EtherPeek launch times, quit times, traffic alarms, trigger events, etc.

FEATURE FOCUS #4: STATISTICS

Real-time Network Statistics To Monitor Traffic Patterns

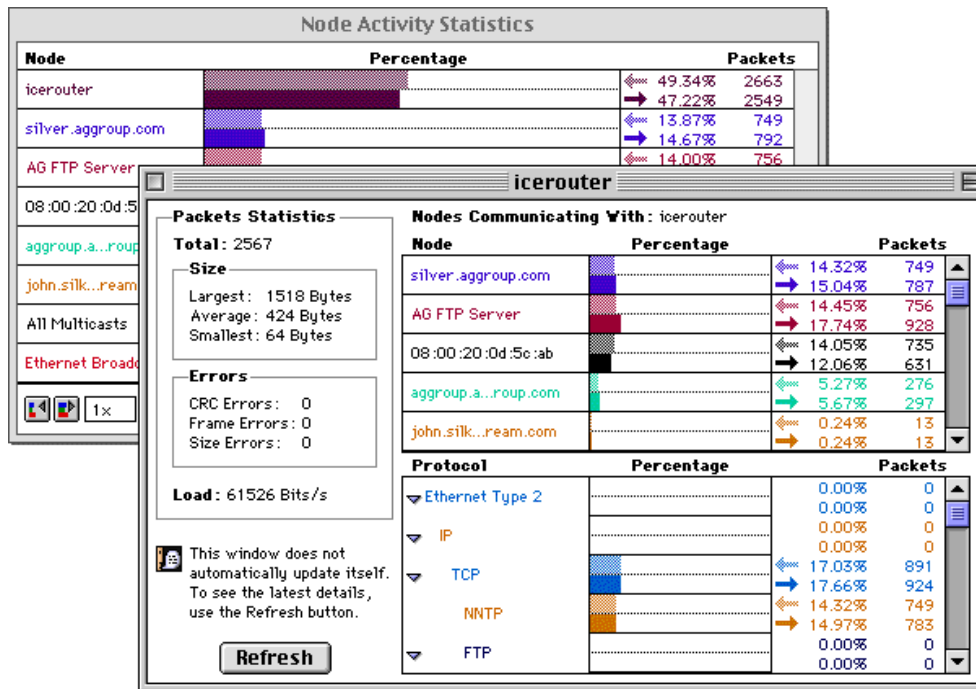
Summary: Statistics provide insight into the overall flow of network traffic. They are like the view from a traffic helicopter and can indicate bottlenecks and anomalies. Use these windows to locate potential problem areas or bandwidth abusers on your network. EtherPeek offers a breakdown of traffic by:

- Who is sending packets (Source Statistics)
- Who is receiving packets (Destination statistics)
- Traffic levels in and out of each node (Dual Statistics)
- What protocols and subprotocols are in use (Protocol Statistics)
- How busy the network is (Network Statistics)
- How many packets are passing a set of pre-defined specifications (Filter Statistics)
- The level of frequency of relevant network elements (Summary Statistics)



Step-by-Step Example: Finding Major Bandwidth Users and Abusers

1. Start capturing packets, or load a saved packet file into EtherPeek's memory.
2. Select "Dual" from the Statistics menu.
3. Choose the "Sort" button and sort the list by packets sent. The window will be redrawn with the largest contributors to bandwidth use at the top.
4. Double Click on the bar associated with the top contributor.
5. Check the resulting list of communication partners.



In this example, we focus on nodes which are creating the most traffic relative to other devices on the network. Identify communication partners using the detail graph, then consider if closer scrutiny is in order. Though you may not find any significant bandwidth overuse or abuse, we provide this example so you can see how EtherPeek can help you identify the "chatty" nodes. If your network performance drops, reviewing Node Statistics is often the first step in the process of identifying a likely cause.

For example, if, upon examining the data provided in a node statistics window, you discover that a node and one particular communication partner appear to be using more than their fair share of the network, you can create an address filter for the two devices and easily determine if the traffic they are generating is in line with expectations, contains many retransmissions or error packets, etc.

Step-by-Step Example: Finding the Sources of Specific Protocol Traffic

1. Start capturing packets, or load a saved packet file into EtherPeek's memory.
2. Select "Protocols" from the Statistics menu.
3. Double-click on a bar in the graph.
4. Check the list of nodes generating the protocol.

This example is useful in environments in which you want to isolate different protocols. For instance, if there is a requirement that only IP appear on the backbone but AppleTalk appears in the graph, you can find the culprit with a double-click!

Step-by-Step Example: Monitoring Your Network with Summary Statistics

The new Summary Statistics feature included with EtherPeek 3.5 allows you to monitor key network statistics in real-time and save these statistics for later comparison. Use this feature to baseline "normal" network activity, save the data, and then compare these saved statistics with those observed during periods of erratic network behavior to help pinpoint the cause of the problem.

Summary statistics are also extremely valuable in comparing the performance of two different ethernet segments or two different networks. For example, a field support engineer could compare the real-time statistics on a client's network with a saved "healthy" router snapshot and easily diagnose or eliminate the source of inconsistent or poor router performance.

To view Summary Statistics, follow these steps:

1. Start capturing packets.
2. Select "Summary" from the Statistics menu.
3. Click the "Take Snapshot" button. Data relating to your real-time network traffic will be displayed in a column identified with a date and start time.
4. Click "Reset Values" to refresh the data in the current column.
5. Select "Save Statistics" from the File menu.

Start Date	1/22/98
Start Time	10:55:21 AM
Duration	0:02:14
Total(p)	15,645
Collected(p)	15,638
Multicast Packets(p)	169
Broadcast Packets(p)	72
Total Errors(p)	-
CRC Errors(p)	-
Frame Errors(p)	-
Runt Packets(p)	-
64 Byte Packets(p)	8,112
64-127 Byte Packets(p)	3,008
128-255 Byte Packets(p)	824
256-511 Byte Packets(p)	452
512-1023 Byte Packets(p)	1,966
1024-1517 Byte Packets(p)	147
1518 Byte packets(p)	1,123
Oversize Packets(p)	-
AARP Request(p)	46
AARP Response(p)	46
ATalk Multicast(p)	105
ICMP Packets(p)	60
ICMP Dest Unreach(p)	42
ICMP Host Unreach(p)	20
ICMP Port Unreach(p)	11
ARP Requests(p)	6
ARP Responses(p)	6

Total Items: 35 Snapshots: 0

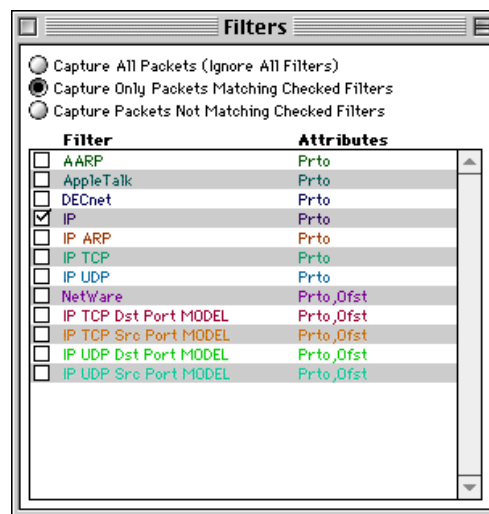
FEATURE FOCUS #5: FILTERS

Pinpointing Traffic Of Interest

Summary: Filters let you focus on specific traffic. If you think your problem is limited to communication between certain nodes (e.g., between one computer and a printer) or to specific packet types (e.g., Address Resolution [ARP] packets), filters eliminate irrelevant packets so you can readily see and understand what is happening to prevent effective communication on your network.

EtherPeek's filter mechanism lets you focus on traffic using the following variables:

- Source address (packets sent from a specific device)
- Destination address (packets sent to a specific device)
- Protocol type (AppleTalk, IP, DECnet, NetWare, etc.)
- Offset (more specific packet types to the bit level, such as "NBP LkUp Reply")
- Error type (Runt , CRC, Frame Alignment, Oversize Packet errors)



Step-by-Step Example: Setting an Address Filter

An Address Filter is very useful for focusing on packets between specific network devices or packets being sent to or received from a device. In this example, we will step you through the process of creating an address filter to capture packets between two devices.

1. Select "Filters" from the Capture Menu. When the Filter Window opens, a new Filters menu listing will appear in the menu bar.
2. Choose "Add" from the Filters menu. The Filter Settings dialog will open.
3. Type the name "Example Filter" in the fill-in box at the top of the dialog.
4. Click in the Address Filter check box to enable the address attribute of the filter.
5. Select a type for your source and destination address through the "Type" pop-up menu. This will tell EtherPeek the type of address, i.e., the location of the address in the packet. The choices are physical Ethernet addresses or IP, AppleTalk or DECnet higher-level addresses.
6. Click the radio button preceding the Address 1 edit field.
7. Place your cursor in the Address 1 edit field.
8. Click the "Name Table" button in the lower left-hand corner of the dialog. The Name Table window will open.
9. Double-click an entry for which you wish to capture packets (e.g., a server). The server entry will now appear in the Address 1 edit field.

10. Repeat steps 6-9 for the Address 2 edit field, selecting a device from the Name Table that you know to be in communication with your server (or other device you have chosen for Address 1).
11. Select the “Address 1 to Address 2” and the “Address 2 to Address 1” checkbox. A double-headed arrow will appear between the Address 1 and Address 2 edit fields, indicating that you wish to capture all packets between these two devices.
12. Click OK at the bottom of the dialog. The listing "Example Filter" will now appear at the bottom of the list of Filters in the Filters window.
13. Enable your filter by clicking in the box next to its name.

If you start a capture session now, only those packets between the devices specified in your address filter will be captured and displayed in the Main Window, and statistics windows will report on their activity only.

Step-by-Step Example: An Easy Way to Create a Protocol Filter

1. Click once on a protocol or subprotocol name in the Protocol Statistics Window.
2. Choose “Make Filter...” from the Special menu. The Filter Settings window opens and a filter is created with the protocol fields pre-configured.
3. Assign a filter name and save by clicking "OK".
4. Enable your filter by clicking in the box next to its name.

These short steps create a filter which limits your search to a specific protocol or subprotocol. You can edit this filter to be even more specific, if you wish. For example, you can:

- Fine-tune the filter to test for specific bits within the packet by adding an offset limitation by clicking on the "Offset filter" button.
- Search for error packets only by checking the boxes under "Error Filter" in the Filter Settings window shown above.

Step-by-Step Example: Selecting Related Packets

1. Select a packet in the Main Window.
2. Choose “Select Related Packets” from the Edit menu. A small window displays the number of selected packets.
3. Choose “Hide Unselected Packets” from the Edit menu.
4. The window now contains only packets to and from the two nodes in the original packet and using the same protocol. All statistics are recalculated based on the packets showing.

This example shows you a very simple way to analyze a conversation between two nodes on a network. It's a way to create a temporary filter and select similar packets so you can take a quick look at the results.

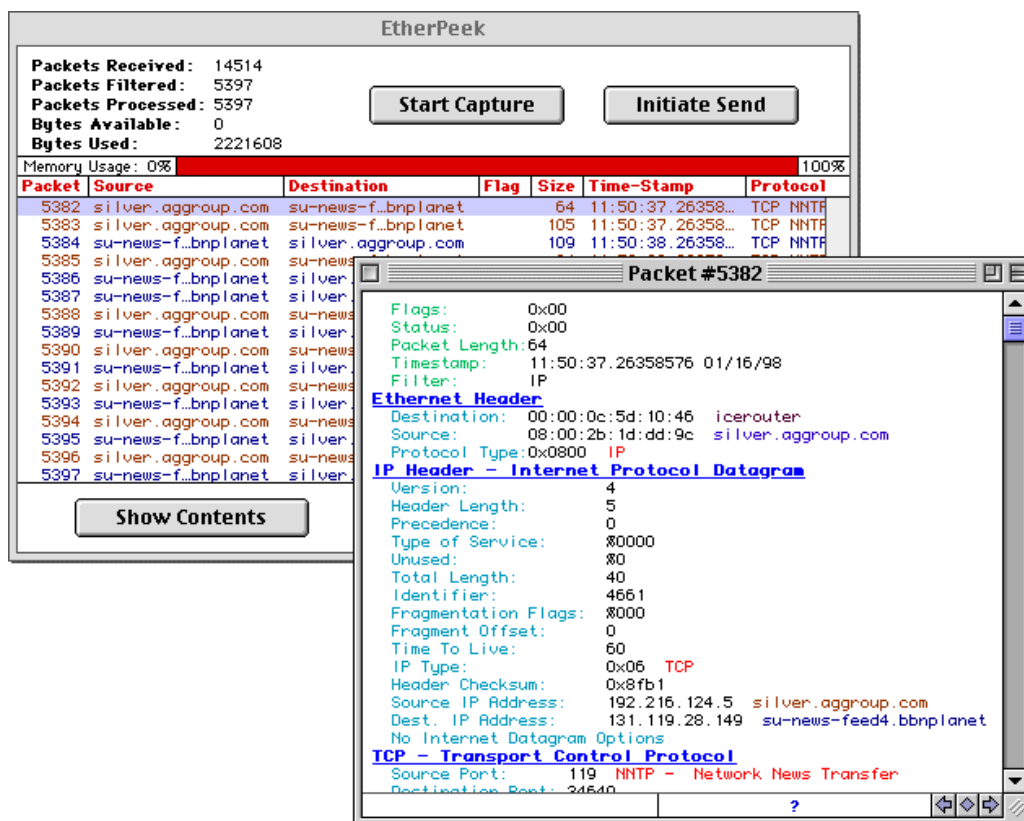
FEATURE FOCUS #6: PROTOCOL DECODERS

Revealing the Source of Problems

Summary: Sometimes network problems are revealed by information contained in a packet. Protocol decoders allow you to open packets and look inside, pinpoint sources of error packets, track down faulty hardware and cabling, and learn about and examine protocol structure and compliance.

Step-by-Step Example: Inspecting Packet Contents

1. Double-click on a packet in the Main Window.
2. Read the contents. The header information includes the source and destination addresses and packet type. If this were an error packet, this source information would point you directly to the faulty hardware or software creating it.
3. Investigate the layers. Each blue title line represents a different layer of the OSI 7-Layer model (Physical, DataLink, Network, Transport, Session, Presentation, Application, easily remembered by this mnemonic: "Please Do Not Take Sales Person's Advice" [care of Allan P. Hurst, Stoney River Networks, Sunnyvale, CA and STACKS: The Network Journal]).
4. See Raw Data. Click on the diamond at the bottom right of the decode window. This toggles between the decoded packet and hexadecimal data. Without the packet decoder files, you'd see this "raw" data only.
5. Move Forward or Backward. Click on either arrow at the bottom right corner of the window to see a decode of the previous or subsequent packet in the data stream.

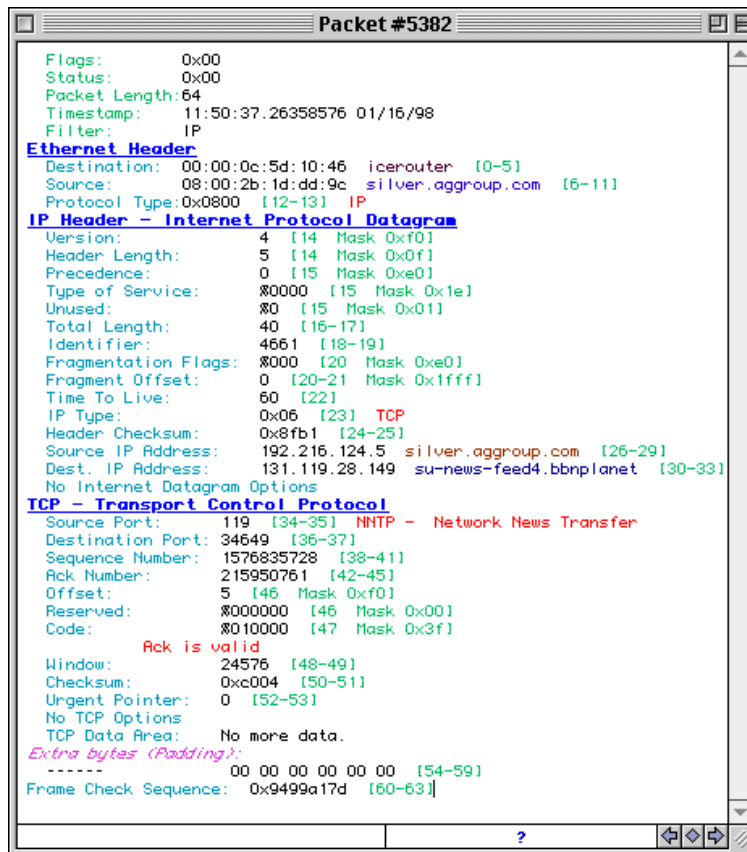


Packet decoders provide unique insight into how networks work. This example demonstrates how you can easily examine the contents of individual packets to find and fix problems as well as learn about network communications using packet decoders.

Step-by-Step Example: Viewing Data Offsets (for advanced users)

The packet decoder window is also useful for identifying offsets for creating your own offset filters.

1. Bring a packet decoder window to the front.
2. Holding down the mouse, select "Packet Decoder" from the Display menu.
3. Highlight "Show data offsets" before releasing the mouse button.
4. The packet displayed will show the data offsets in green brackets.



```
Packet #5382
Flags: 0x00
Status: 0x00
Packet Length: 64
Timestamp: 11:50:37.26358576 01/16/98
Filter: IP
Ethernet Header
Destination: 00:00:0c:5d:10:46 icerouter [0-5]
Source: 08:00:2b:1d:dd:9c silver.aggroup.com [6-11]
Protocol Type: 0x0800 [12-13] IP
IP Header - Internet Protocol Datagram
Version: 4 [14 Mask 0xf0]
Header Length: 5 [14 Mask 0xf0]
Precedence: 0 [15 Mask 0xe0]
Type of Service: 00000 [15 Mask 0x1e]
Unused: 0 [15 Mask 0x01]
Total Length: 40 [16-17]
Identifier: 4661 [18-19]
Fragmentation Flags: 0000 [20 Mask 0xe0]
Fragment Offset: 0 [20-21 Mask 0x1fff]
Time To Live: 60 [22]
IP Type: 0x06 [23] TCP
Header Checksum: 0x8fb1 [24-25]
Source IP Address: 192.216.124.5 silver.aggroup.com [26-29]
Dest. IP Address: 131.119.28.149 su-news-feed4.bbnpplanet [30-33]
No Internet Datagram Options
TCP - Transport Control Protocol
Source Port: 119 [34-35] NNTP - Network News Transfer
Destination Port: 34649 [36-37]
Sequence Number: 1576835728 [38-41]
Ack Number: 215950761 [42-45]
Offset: 5 [46 Mask 0xf0]
Reserved: 0000000 [46 Mask 0x00]
Code: 010000 [47 Mask 0x3f]
Ack is valid
Window: 24576 [48-49]
Checksum: 0xc004 [50-51]
Urgent Pointer: 0 [52-53]
No TCP Options
TCP Data Area: No more data.
Extra bytes (Padding):
----- 00 00 00 00 00 00 [54-59]
Frame Check Sequence: 0x9499a17d [60-63]
```

Users who wish to create their own offset filters can save a great deal of time by using these predetermined data offsets!

Note: The AG Group can provide you with a recommended reading list if you are interested in learning more about specific protocol specifications. As a registered EtherPeek owner, you can define your own decoders by requesting a Decoder Development Kit from AG Group Sales (sales@aggroup.com).

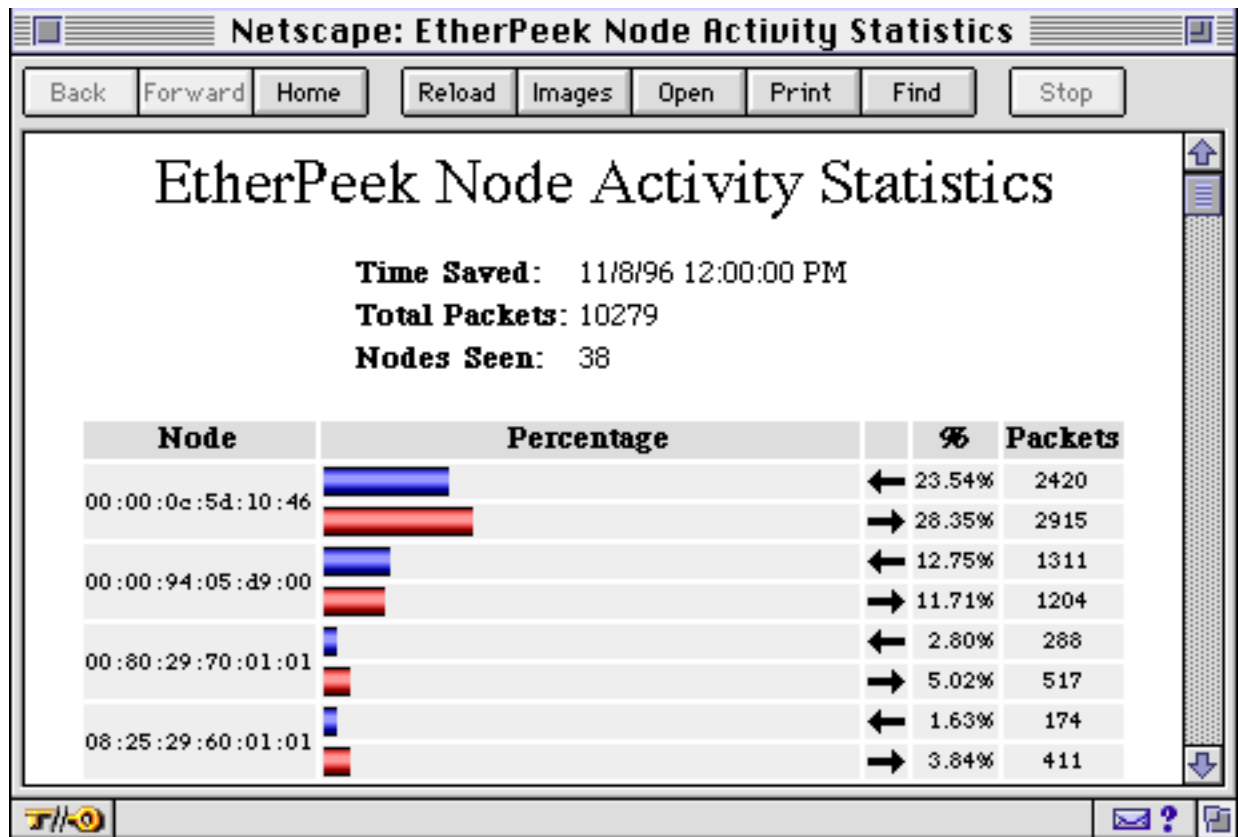
FEATURE FOCUS #7: VIEWING STATISTICS WITH YOUR WEB BROWSER

Remote analysis of your network's performance

Summary: EtherPeek 3.5 supports the ability to periodically save statistics as HTML files, enabling you to view network information with a web browser. Use the new “HTML Output...” command in the Statistics menu to access a dialog in which you can enable this feature and select a template folder and an output folder. EtherPeek will process all text files in the template folder you select and replace special keywords with packet statistics values and write the resulting files to the output folder.

This method allows you to have almost complete control over the HTML that is produced. For example, you can customize the format and appearance of the tables that are produced, include your own text, graphics, and links, and you can keep separate files for each statistics table, or combine them into a single HTML document. Every piece of information in the source, destination, node activity, protocol and filter statistics windows can be accessed.

A set of template files that you can use without modification, or as a starting point for customizing your own statistics tables is included in the HTML Folder that accompanies the EtherPeek demo application.



Important!

- The corresponding statistics window must be open in order to output a statistics table as HTML. Why? Because otherwise EtherPeek doesn't spend the time to calculate the statistics in the first place.
- Output filenames are based on the template filename and are given the filename extension “.html”. Any existing filename extension on the template file is not used.
- Avoid choosing the same folder for templates and for output or templates may be overwritten (if they end in “.html” for example).

THERE'S MORE!

There are many more features to explore with EtherPeek 3.5, but not enough space here to document them all. We suggest you look at these additional features:

- *Capture Buffer Options.* Tell EtherPeek how to handle packets during longer captures, including automatically saving to disk and restarting capture. View these options under the Capture menu.
- *Triggers..* Automate the start and stop of capture using triggers. Any filter can be specified as a trigger criterion, or choose to start and stop packet capture based on time and date settings, so you can focus captures with pinpoint accuracy. Look for trigger options under the Capture menu.
- *Alerts.* EtherPeek can notify you when certain events occur on the network, such as the appearance of new nodes, new protocols, or when statistics exceed a threshold. Notification options include sound, dialog box, AppleScript execution, speech notification or an electronic page (via a separate page server), so you can take proactive measures at problem occurrence and know immediately if standards are violated. The Alert Window under the Special menu is enabled when you highlight a node or protocol line in a statistics window.
- *SmartDecoders™.* SmartDecoders allow you to identify conversational threads buried among the overall stream of network traffic. As these threads develop, SmartDecoders collect intelligence about the packets in the dialogue, and this knowledge is then exploited to automatically decode successive packets to upper layers. By this method, "response" packets, which reply to corresponding "requests," can be decoded to provide rich amounts of information about network transactions.
- *ProtoSpecs™.* AG Group's ProtoSpec technology offers a very fine level of protocol layer detail by identifying the top-level "parent" protocol and breaking-out each sub-protocol layer in a hierarchical view. Look for ProtoSpecs in EtherPeek's Main Window and filter and protocol statistics windows. Display protocol information based on a total of the sub-protocols under the parent protocol, or by each subprotocol broken-out by individual layers. Setting filters based on specific sub-protocols is as easy as clicking on the desired protocol layer and choosing the "Make Filter" command from the Capture menu.
- *Protocol Definitions.* EtherPeek provides a definition of what a protocol abbreviation stands for and a concise description of what a protocol is used for. This on-line help mechanism will assist you in determining the purpose of previously unseen packets on the network as well as help to increase your knowledge of LAN/WAN protocols. To view the definition for any particular protocol or sub-protocol from the Main Window or Protocol Statistics Window, click on your selection and then choose the "Protocol Info..." command from the Special menu.
- *Filters and Filter Statistics.* Filters are extremely powerful tools visited only briefly in Feature Focus #5. When combined with Filter Statistics, you can track certain types of traffic with a glance and even include alarms for threshold conditions. Try Filter Statistics under the Statistics Window.



**The AG Group, Inc.
2540 Camino Diablo, Suite 200
Walnut Creek, CA 94596
USA**

**(800) 466-AGGP
(510) 937-7900
fax (510) 937-2479
Email: info@aggroup.com
Internet: [ftp.aggroup.com](ftp:ftp.aggroup.com)**

ADDITIONAL PRODUCT INFORMATION

ABOUT THE AG GROUP, INC.

The AG Group, Inc. specializes in easy-to-use software tools for troubleshooting, optimizing, maintaining and expanding multivendor computer networks. While designed to take advantage of the intuitive, graphical interface of the Macintosh, our products can be used in virtually any heterogeneous networking environment.

Please call us for more information on:

- Network Analysis Training
- Network Analysis Consulting
- Recommended Reading

AG GROUP PRODUCT OFFERINGS

Network Analyzers

EtherPeek™ for Macintosh

EtherPeek™ for Windows 95/NT 4.0

Network Monitors

Skyline™ Multi-Segment Network Traffic Archiving and Analysis Program

NetMeter™ Real-Time Multimedia Monitoring Modules

Satellite™ Network Traffic Data Collection Engine

Network Management Training

Network Troubleshooting Videotape Series

Network Troubleshooting Starter Kits for Ethernet and LocalTalk

AG Group Extended Product Maintenance

Service contracts are a cost-effective way to ensure that you grow along with The AG Group as new versions and ideas are incorporated into the products. All AG Group customers are entitled to technical support for the life of their purchase and 90 days of automatic shipments of free updates and bug fixes. Service Contracts extend the free update period for one or two years and provide an extra level of service, including:

- Priority telephone, electronic mail, remote access and fax technical support
- Monthly maintenance holder email with passwords to access a special Service folder from our ftp site
- Free product updates and bug fixes
- Free documentation updates
- Regular TechTips mailings
- Pre-release software access