

ETHERPEEK™/LOCALPEEK™/TOKENPEEK™ QUICKTOUR

**A Step-by-Step Guide Through Using Your
"Peek" Product Demonstration Software**



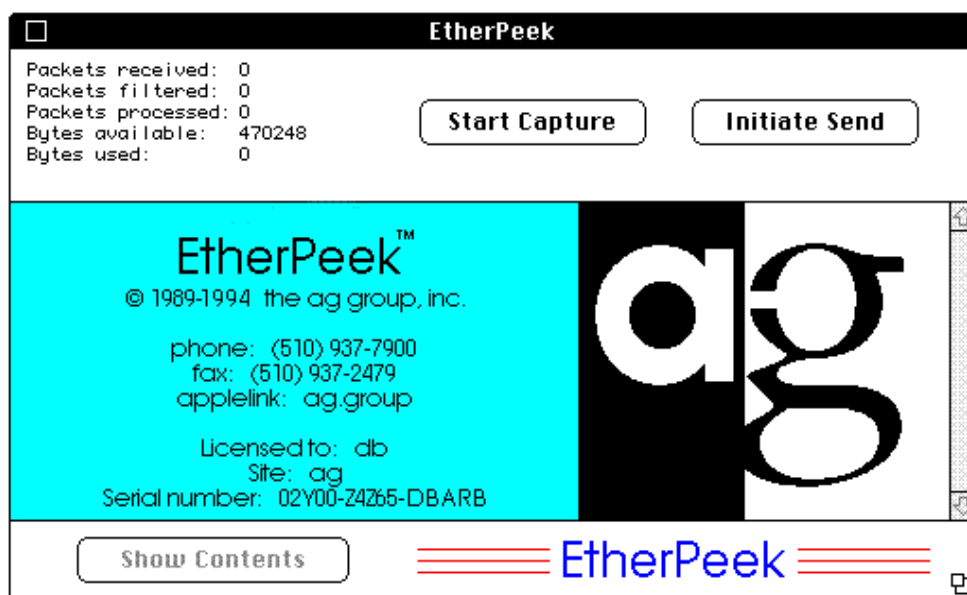
**The AG Group, Inc.
2540 Camino Diablo, Suite 200
Walnut Creek, CA 94596
USA
(800) 466-AGGP
(510) 937-7900
fax (510) 937-2479
Internet: info@aggroup.com
eWorld: AGGROUP
CompuServe: 74431,2500
AppleLink: AG.GROUP
Apple Remote Access: (510) 937-6704
Visit our Worldwide Web Site: <http://www.aggroup.com/>**

WELCOME TO THE PEEK PRODUCTS!

Welcome to this QuickTour of EtherPeek, LocalPeek, and TokenPeek (the "Peek" products) from The AG Group, Inc. The Peek products are network and protocol analysis tools designed to help you troubleshoot, optimize, plan and configure networks. They work by capturing all network traffic and allowing you to analyze and interpret traffic patterns, statistics and types. Each section of this document is a brief overview of a major feature with step-by-step examples to help you exercise the feature in the demonstration software.

GETTING STARTED— JUST DOUBLE-CLICK

The "Peeks" capture all conversations on a network, much like a telephone tap, and provide you with a wealth of features for dissecting this traffic to discover problems and patterns. This demo walks you through a look at some of the traffic from your network. If you aren't connected to a network, or you would like to use the sample traffic supplied with the demo, please see the section entitled "Exploring With Sample Packets".



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

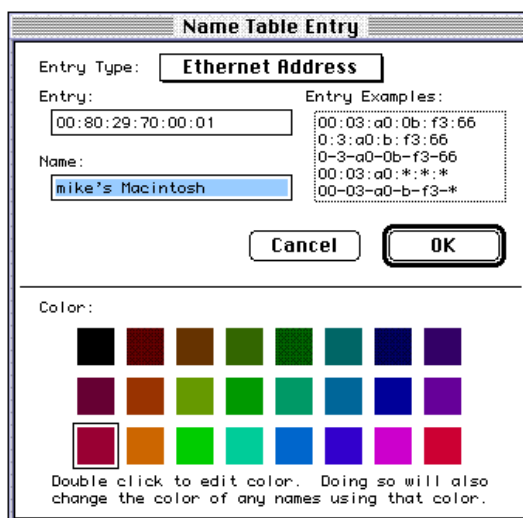
1. Launch the application by double-clicking on the "Peek Demo" icon.
2. Select an interface from which to run EtherPeek.
3. Click on "Start Capture".
4. Click "OK" to disconnect network services (If you're unsure, restart your machine before beginning the demo).

You will now begin to see packets from your network processed and displayed in the "Peek" main Window. Packet information is displayed by source address, destination address, flags (indicating errors in packets or 802.3 LLC packets), protocol type, packet size and time-stamp. For a way to easily designate names for these often-unfamiliar source and destination addresses, please see the next section.

Note: These demo versions allow live capture for 15 seconds only; in the commercial versions, your capture session is not limited. If you do not have a network connection or supported hardware interface, skip to the section entitled "Exploring with Sample Packets" and return to the Feature Focus section using the sample packets provided.

FEATURE FOCUS #1: NAME-FOR-ADDRESS SUBSTITUTION Customizable Display, Visual Cues Help Highlight Problems Quickly

Summary: EtherPeek, LocalPeek and TokenPeek are unparalleled in the level of customization they allow and the straightforward way they present network information. One feature is name-to-address mapping, which makes "Peeking" more friendly. This feature lets you show node names instead of physical or logical addresses for easy identification of network activity.



Step-by-Step Example: Add Name-for-Address Mapping

EtherPeek/TokenPeek

1. Select "Display Options" from the Display Menu.
2. Select "Name Entry" from the Node Display Format pop-up list.
3. Click "OK" to close window.
4. Click on any packet in the Main Window.
5. Select "Insert Into Name Table" from the Special menu.
6. Enter name for first address and select a color.
7. Enter name for second address and select a color.
8. Click "OK".

LocalPeek

1. Make sure AppleTalk is active by opening Chooser under the Apple Menu.
2. Select "Name Table" from the Special menu.
3. Select "Name Scan" from the Names menu.
4. Select zone(s) to scan.
5. Use Default Name Scan Options by clicking "OK".
6. Name Table will be automatically updated.

After following these steps, you'll see how the "Peek" products can substitute identifiable node names for addresses in all display windows. You can see the names you've defined in the Main Window or any node statistics window.

Note: The shipping version of EtherPeek includes GetTheirAddress™, a utility which will find Ethernet addresses for AppleTalk devices and services, automatically associate them to names, and format them for import into the Name Table. You can add other protocols, device types and services by importing any text-based list into the Name Table.

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

Each "Peek" product also includes the most current IEEE list of vendor and protocol IDs, already formatted for import into the Name Table. To import vendor names, follow these steps:

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 "EP Names and Filters" Folder. Open the folder called "Other".
5. Double-click on "Vendor IDs".

Nodes for which you have not created names now show the vendor name associate with the interface or device in place of the first three bytes of the physical address of that node.. You can repeat this exercise to add Protocol IDs (listed by protocol type in the "EP Names and Filters" folder) if you would like to have the Peek products translate hexadecimal protocol identifiers into recognizable names.

FEATURE FOCUS #2: STATISTICS

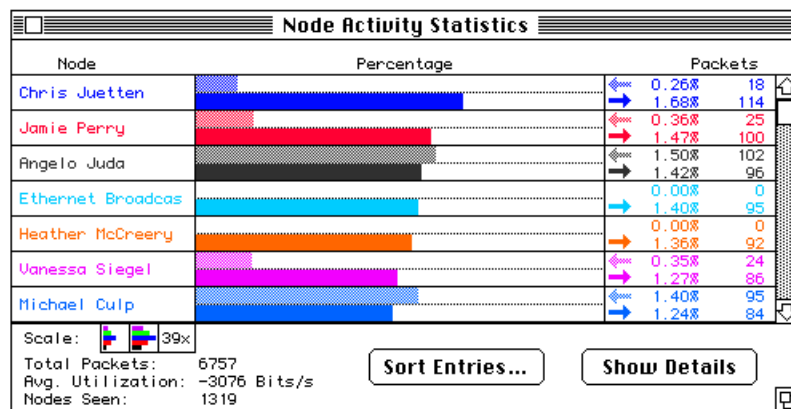
An Overview of Traffic Contribution by Node, Protocol

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.

The "Peeks" offer 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 are in use (Protocol Statistics)
- How busy the network is (Network Utilization Statistics)
- How many packets are passing a set of predefined specifications (Filter Statistics)
- Error packet content

You can see even more detailed statistics by double-clicking any node or protocol statistics bar.



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

1. Select "Dual" from the Statistics menu.
2. Look for any bars which extend further than others.
3. Double Click on this bar.
4. Check the resulting list of communication partners.

In this example, we focus on nodes which are creating the most traffic relative to others 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 in the 15-second demonstration capture period, we provide this example so you can see how the "Peek" products can help you identify the most "chatty" nodes. If your network starts performing poorly, reviewing Node Statistics is often the first step in the process of identifying a likely cause.

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

1. Select "Protocols" from the Statistics menu.
2. Double-click on a bar in the graph.
3. Check the list of nodes generating the protocol.

This example is useful in environments where 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,

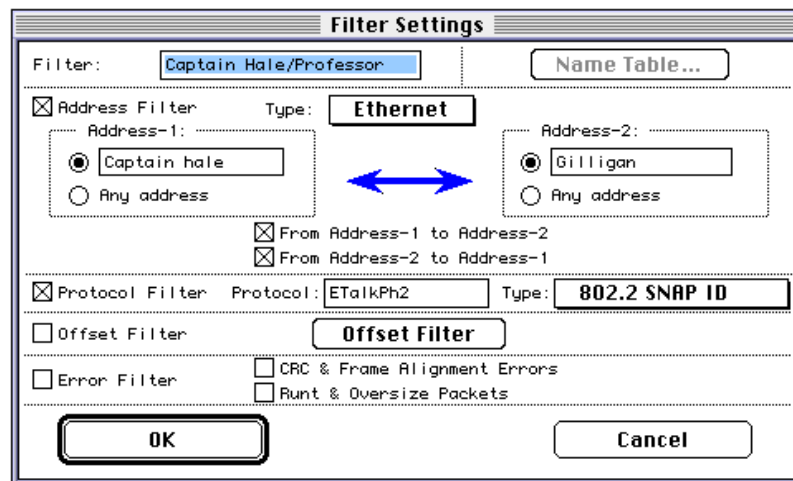
FEATURE FOCUS #3: FILTERS

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.

The Peek 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: Creating New Filters

1. Select a line in the Main Window. This line shows a communication between two nodes using a specific protocol.
2. Choose “Make Filter...” from the Special menu. A filter is created with the address and protocol fields pre-configured based upon the corresponding fields in the selected packet.
3. Assign the filter name “Test filter” (at top left) and save by clicking "OK".

These short steps create a filter which limits your search to traffic between two specific nodes using a specific protocol to communicate. You can edit this filter to be even more specific, if you wish. For example, you can:

- *Change the direction specification (to or from either node or any address) by checking either or both of the boxes "From Address-1 to Address-2" or "From Address-2 to Address-1" in the Filter Settings window.*
- *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: Loading Filters

The "Peek" products ship with hundreds of preconfigured filters. You can load these filters into your Peek program by following these steps:

1. Select "Filters" from the Capture menu.
2. Select "Load Filters" from the File menu.
3. Locate the "EP Names and Filters" folder.
4. Open any folder containing a protocol relevant to your network.
5. Double-click on a line containing filters of interest to you. The filter you select will be automatically appended to the list of available filter selections in the Filter Window.

These examples show you how to create a filter for use now or later. To search for the source of printing problems, create a filter which shows packets from any address to the printer and from the printer to any address. Then use the check box to enable the filter and watch what the printer is "saying". You may see that packets from the node are not even arriving at the printer, indicating that a cable problem may be at the root of your troubles.

Step-by-Step Example: Select Related Packets

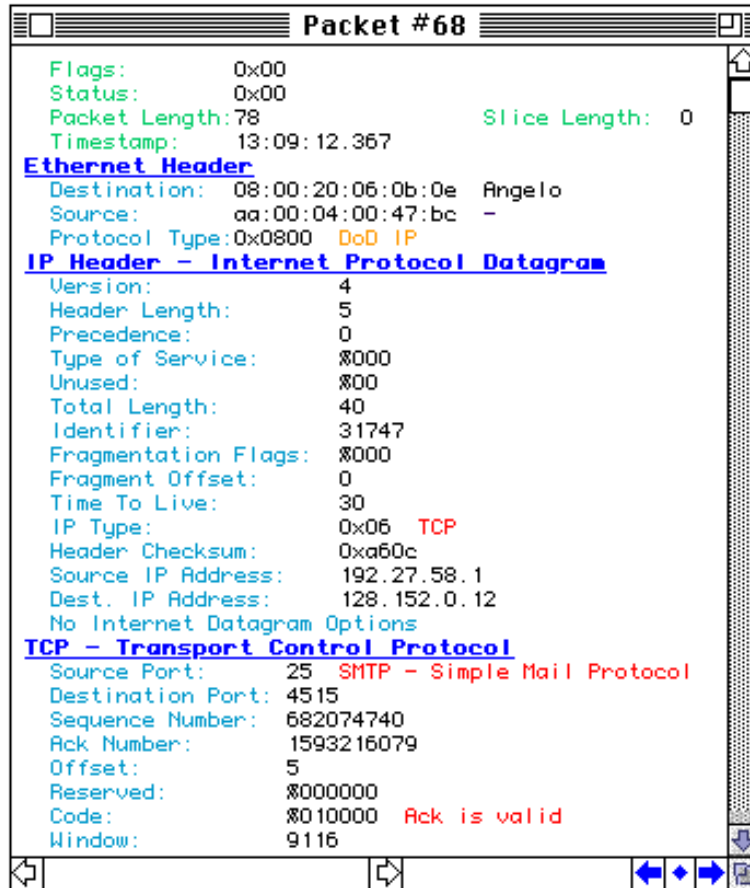
1. Select a packet in the Main Window.
2. Choose "Select Related Packets" from the Special menu. A small window displays the number of selected packets.
3. Choose "Swap Selected" from the Edit menu (this reverses the selected and de-selected items).
4. Choose "Hide Selected Packets" from the Edit menu.
5. 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 #4: 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.

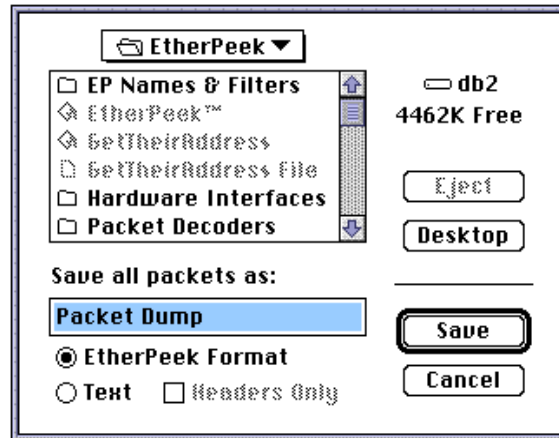
1. Bring a packet decoder window frontmost.
2. Holding down the mouse, select "Packet Decoder" from the Display menu.
3. Highlight "Show data offsets" before releasing the mouse button.
4. The packet displayed will show the data offsets in green brackets.

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. Registered EtherPeek owners can define their own decoders by requesting a Decoder Development Kit from AG Group Sales.

FEATURE FOCUS #5: SAVING PACKETS A Picture Of Network Traffic On Disk

Summary: The “Peek” products aren’t just useful for real-time applications. They can also be used to store and retrieve packets for later use in what are commonly called “packet trace files”. The ability to save packet traces lets you send traffic, like a picture or x-ray, to someone else for interpretation. This means you can share the results with colleagues and communicate more effectively with vendor technical support organizations. It also lets you export captures for use with database and charting programs. Finally, you can configure the software to capture and save packets when you’re away for later viewing.



Step-by-Step Example: Sharing a Capture

1. After capture, select “Save All Packets” from the File menu.
2. Follow the standard Macintosh “Save” dialog.
3. Copy to disk and mail.

Note: Because of the 15-second capture limit in the demo versions, you may not have enough packets to exercise this feature fully. The commercial versions of the Peek products allow you to capture all traffic until the buffer is full, then automatically save the packets to disk and restart capture.

Many technical support organizations participate in The AG Group’s Vendor Support Program. When you’re having network trouble, the best way to communicate with a technical support provider is with packet traces, or pictures of your network traffic. If they don’t have the “Peeks”, have them call us. We’ll get them copies right away!

EXPLORING ETHERPEEK USING SAMPLE PACKETS

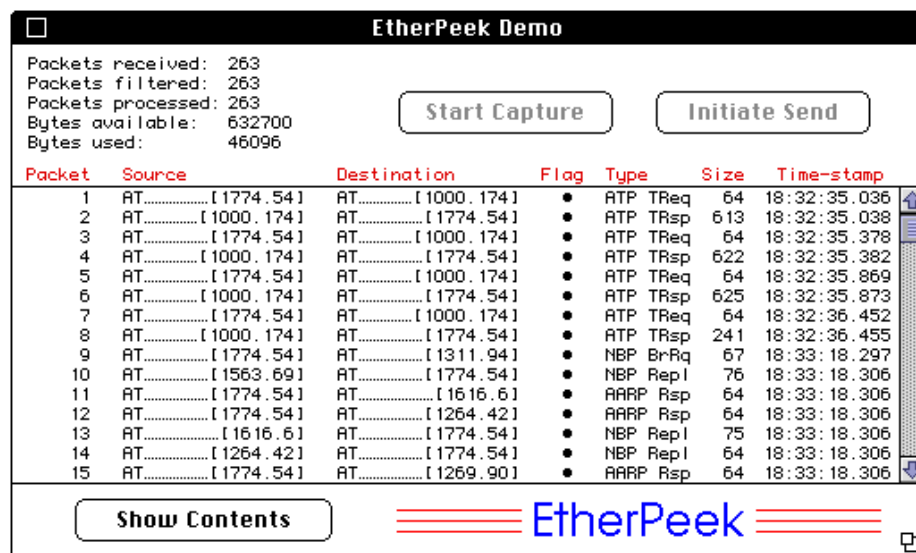
Summary: If you would like to try one of the “Peek” products using sample packets provided with the demo, follow these steps. Note: The example is based on EtherPeek, but all three “Peek” products are similar in both interface and function.

Load Packets

Your “Peek” demo disk has six EtherPeek sample trace files in a folder called “EtherPeek Samples”. After launching EtherPeek, use “Load Packets...” from the File menu to load these six files in the following order:

- 1- Open Chooser
- 2- AppleShare Login
- 3- AppleShare Logout
- 4- Print Directory
- 5- Select Zone
- 6- NetModem Lookup

Note: Our sample files contain AppleTalk packets only, but please remember that EtherPeek works with every registered Ethernet protocol!



The screenshot shows the EtherPeek Demo application window. At the top, it displays statistics: Packets received: 263, Packets filtered: 263, Packets processed: 263, Bytes available: 632700, and Bytes used: 46096. Below the statistics are two buttons: "Start Capture" and "Initiate Send". The main area contains a table with the following columns: Packet, Source, Destination, Flag, Type, Size, and Time-stamp. The table lists 15 packets, including ATP TReq, ATP TRsp, NBP BrRq, and NBP RepI. At the bottom of the window, there is a "Show Contents" button and the EtherPeek logo.

Packet	Source	Destination	Flag	Type	Size	Time-stamp
1	AT.....[1774.54]	AT.....[1000.174]	•	ATP TReq	64	18:32:35.036
2	AT.....[1000.174]	AT.....[1774.54]	•	ATP TRsp	613	18:32:35.038
3	AT.....[1774.54]	AT.....[1000.174]	•	ATP TReq	64	18:32:35.378
4	AT.....[1000.174]	AT.....[1774.54]	•	ATP TRsp	622	18:32:35.382
5	AT.....[1774.54]	AT.....[1000.174]	•	ATP TReq	64	18:32:35.869
6	AT.....[1000.174]	AT.....[1774.54]	•	ATP TRsp	625	18:32:35.873
7	AT.....[1774.54]	AT.....[1000.174]	•	ATP TReq	64	18:32:36.452
8	AT.....[1000.174]	AT.....[1774.54]	•	ATP TRsp	241	18:32:36.455
9	AT.....[1774.54]	AT.....[1311.94]	•	NBP BrRq	67	18:33:18.297
10	AT.....[1563.69]	AT.....[1774.54]	•	NBP RepI	76	18:33:18.306
11	AT.....[1774.54]	AT.....[1616.6]	•	AARP Rsp	64	18:33:18.306
12	AT.....[1774.54]	AT.....[1264.42]	•	AARP Rsp	64	18:33:18.306
13	AT.....[1616.6]	AT.....[1774.54]	•	NBP RepI	75	18:33:18.306
14	AT.....[1264.42]	AT.....[1774.54]	•	NBP RepI	64	18:33:18.306
15	AT.....[1774.54]	AT.....[1269.90]	•	AARP Rsp	64	18:33:18.306

Name-for-Address Substitution

EtherPeek displays logical (AppleTalk) addresses in a "net number.node number" format initially. To make traffic easy to recognize, first we'll substitute names for all the address numbers. To create a Name Table for our example, follow these steps:

1. Holding the "command" or "clover" key, click on packet number 1.
2. Choose "Insert Into Name Table" from the Special menu.
3. You'll be prompted for 4 entries (2 AppleTalk and 2 Ethernet addresses).
4. Enter the name “Gilligan” in the first window and click “OK”.
5. Enter the name “Captain Hale” in the second window and click “OK”.
6. Repeat steps 4 and 5.
7. You'll see these names instead of addresses in the Main Window.

Note: The shipping version of EtherPeek includes GetTheirAddress™, a utility which will find Ethernet addresses for AppleTalk devices and services, automatically associate them to names, and format them for import into the Name Table. You can add other protocols,

You can experiment further with this feature by checking the items under "Node Display Format" in the Display Options menu.

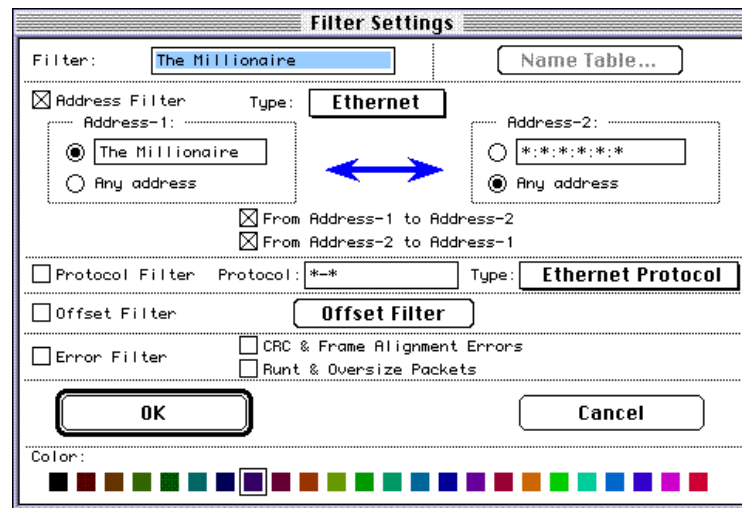
Statistics

When you select "Dual" statistics from the Statistics menu, you will see that the node "Captain Hale" is a big talker, accounting for 58.17% of the traffic generated. If he's a router or a server, that would be understandable. Or, if he's printing large files at this time, this may make sense. There's an easy way to see if this is a problem indicator. Double-click on the Captain Hale bar in the Node Activity Statistics window. If he has one communication partner, be sure these nodes are in the same zone. Since he has multiple partners, Captain Hale looks to be a router or server.

To find the least talkative node, click on the button that says, "Sort Entries..." and sort by packets sent. At the bottom of this list is a node with an Ethernet address of 00:00:89:01:93:72. To name this node, highlight the bar, select "Insert Into Name Table" from the Special menu, and type the new name, The Millionaire.

Filters

The least talkative node is The Millionaire, who has sent one packet and received one packet. How would we find these two packets among a large capture session? This is a perfect application of filters. EtherPeek has several filtering mechanisms which let you define your interest before, during or after capturing packets. Since we already have the packets, we are going to use the "Select" post-capture filtering mechanism.



1. Choose "Select" from the Edit menu, then "Add" from the Filters menu.
2. Name the filter "The Millionaire".
3. Enable the address portion of the filter with the check box at the upper left, then click the radio button by the "Address 1" box. Because we have entered this node into the name table, we don't need to look up the 8 byte Ethernet address. You can simply type the name "The Millionaire", or place the cursor in the Address 1 field and click on the "Name Table" button at the top right corner of the window. Locate "The Millionaire" and double-click on it to insert this node into the field. Since we are interested in traffic to AND from this node, click on the space between the address pair until a bi-directional arrow appears. Finally, click "OK".
4. In the "Selection Criteria" window, click on the radio button to enable Filters, then scroll to the bottom of the list to check "The Millionaire" filter. Leave the other radio buttons unselected.
5. Click on "Select" EtherPeek finds the two packets

To hide the other packets, follow these steps:

1. Go to the Main Window
2. Select "Swap Selected" from the Edit Menu.
3. Select "Hide Selected Packets" from the Edit Menu.

You are left with 2 packets to look at! Note that the statistics display is recalculated based on your "Hide" command. To search for other packets, select "Unhide All" from the Edit menu and all the packets reappear.

Tip: *Alternately, you can save time by using the "Do Not Match Criteria" radio button in the Selection Criteria window. This option is another way to select and/or eliminate groupings of packets.*

Protocol Decoders

Protocol Decoders allow you to follow a conversation between nodes in extreme detail. A simple "conversation" to look at using your sample packets is contained in the file "1- Open Chooser". The eight packets in this file show you what happens when you open the Chooser and prepare to select, for example, a new printer.

Here is a description of the conversation, step-by-step:

1. Double-click on packet #1. As you scroll through the packet, you see the different layers of the AppleTalk protocol. At the bottom of the window, you can see that this is a Zone Information Protocol (ZIP) packet called "Get Zone List". When you open Chooser, it must show you available zones, so it immediately sends this packet onto the network.
2. Click on the right-facing arrow at the bottom right corner of the decode window. This opens the next packet in the buffer. Scrolling to the bottom of the packet shows you that this is a ZIP packet returning 65 zone names. The first value under the ZIP heading says "Last Flag: 0". Since the value is 0, this flag is off. This means this is NOT the last packet--there are still more zones. Go to the next packet.
3. Since the "last flag" was off, Captain Hale queries the router, Gilligan, to send the rest of the list. Because our zone list is very long, it requires four inquiries before the entire list is returned.
4. Inspect packet #8. The "Last Flag" value is 1, which means the end of the zone list has arrived. Chooser compiles the list and allows you to pick your printer.

To experiment further on your own network, locate some Zone Information Protocol (ZIP) GetZoneList reply packets. These packets can be generated by opening Chooser, which needs to display a list of zones for you. When you decode these packets, you can see the zone lists generated by a particular router. This feature can be invaluable when attempting to resolve routing table conflicts (when routers disagree about zone lists).

THERE'S MORE!

There are many more features to explore with the demo software, but not enough space here to document them all. To evaluate the software more fully, we suggest you look at these additional features:

- **Capture Buffer Options.** Tell the "Peeks" how to handle packets during longer captures, including automatically saving to disk and restarting capture. Experiment with 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, so you can focus captures with pinpoint accuracy. Look for trigger options under the Capture menu.
- **Alerts.** The "Peek" products 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 a sound, a dialog box, 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.
- **Filters and Filter Statistics.** Filters are extremely powerful tools visited only briefly in Feature Focus #3. 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.
- **Network Statistics.** This option displays overall network utilization and error levels graphically and in real time. Look under the Statistics menu.

THANKS FOR YOUR TIME AND INTEREST IN OUR PRODUCTS!

PEEK PRODUCT ORDERING INFORMATION*

The Peek Products are available from:

- The AG Group (800) 466-AGGP, sales@aggroup.com
- MacWarehouse (800) 255-6227
- Other direct mail catalogs
- Your favorite software reseller

EtherPeek

Suggested List Price \$795

LocalPeek

Suggested List Price \$495

TokenPeek

Suggested List Price \$995

Resellers may order these products from Ingram Micro:

EtherPeek PN#162119

LocalPeek PN#162120

TokenPeek PN#162124

Online Ordering!

You can order any AG Group product via the Worldwide Web. Just visit our web site at <http://www.aggroup.com> and select the pointer to the online order form.

*Prices subject to change without notice.

**Education, Developer, Government, and Consultant Discounts Available. Please contact AG Group Sales for further information.

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™ Ethernet Network Analyzer

LocalPeek™ LocalTalk Network Analyzer

TokenPeek™ Token-Ring Network Analyzer

Network Monitors

Skyline™ Network Traffic Archiving and Analysis Program

Satellite™ Network Traffic Data Collection Engine

Net Watchman™ AppleTalk Network Early Warning Monitor

Network and AppleShare Utilities

Nok Nok™ Personal File Sharing Monitor

Nok Nok A/S™ AppleShare Server Monitor

Silver Cloud™ Hierarchical Chooser Replacement

EtherHelp™, LocalHelp™, TokenHelp™ Remote Capture Utilities

Network Management Training

Network Troubleshooting Videotape Series

Network Troubleshooting Starter Kits for Ethernet and LocalTalk

AG Group Service Contracts

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
- Free product updates and bug fixes
- Free documentation updates
- First run copies of Node News, our quarterly newsletter
- Regular TechTips mailings
- Pre-release software access
- Discounts on other AG Group products

HOW TO REACH THE AG GROUP

By Telephone:

800-466-2447

510-937-7900

By Fax:

510-937-2479

By Electronic Mail:

AppleLink: AG.GROUP

Compuserve: 74431,2500

eWorld: AGGROUP

Internet: info@aggroup.com

Online Archives

Internet: ftp.aggroup.com

Worldwide Web: <http://www.aggroup.com/>

CompuServe: Go AGGROUP

AppleLink: Third Parties (A-G)/AG Group

eWorld: Go AGGROUP

By U.S. Mail (Or To Visit!)

The AG Group, Inc.

2540 Camino Diablo, Suite 200

Walnut Creek, CA 94596