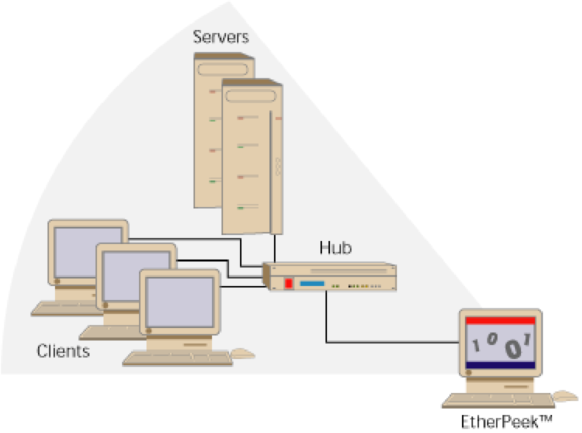
Monitoring, Troubleshooting and Securing Networks with EtherPeek

WildPackets

Monitoring, Troubleshooting and Securing Networks with EtherPeek

Contents



Introduction

This paper gives examples of how to use EtherPeek's broad set of features to perform three of the most important functions of network management:

- Monitoring your network's performance and looking for unusual or problem conditions.
- Troubleshooting your network to narrow the search for the causes of any trouble.
- Setting up, maintaining and supporting a security system for your network.

Whole books are written on these subjects, many of which are listed on our website at www.wildpackets.com/resources. In addition, WildPackets Academy offers network analysis courses centered on practical applications of protocol analysis techniques for Ethernet LANs. (Please visit http://www.wildpacketsacademy.com for complete course information.)

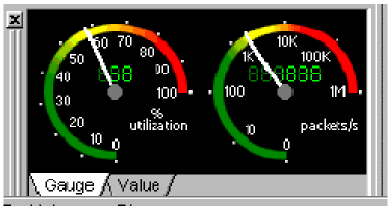
In this limited space, we will show how EtherPeek fits into one common approach to monitoring and troubleshooting, and give specific pointers on how to apply particular EtherPeek capabilities to solving representative troubleshooting and security problems.

Monitoring with EtherPeek

Network managers generally have a favorite rule of thumb in their approach to monitoring their network: moving from the general to the specific, for example, or from the most immediate to longer term concerns.

Many managers look first at the best over-all indicators of network health, then scan for errors and similar problems. If they have a little more time, they typically begin to look for anything out of the ordinary, anything that might indicate a problem or simply a change in the network. The rest of this section describes how to use EtherPeek in such an approach to network monitoring.

Overall performance and utilization



The **Network Statistics** window is a great quick view of overall network health, showing percent utilization and traffic volume, and packets per second. The dial indicators are easy to read at a glance. This makes it the sort of display a network manager might want to keep on the screen (perhaps along with the **Error Statistics** window). Another way to monitor overall network performance is through periodic output of **Node**, **Protocol** and **Summary Statistics**. By using **Statistics Output Options** in EtherPeek, you can keep track of network performance on remote segments, even on remote networks.

Errors and related problem indicators

After the first glance to make sure everything is normal, most managers scan key indicators, looking for signs of current or impending trouble. Error packets in themselves are normal for Ethernet networks, but some patterns of errors are not. In the Troubleshooting section below, a clear-cut case is described where a high percentage of the traffic on a network is made up of undersized or runt packets. Please see "Undersized or runt packets" on page 4, below. Such plain signs of trouble are scanned for, many times a day.
User complaints of an unavailable or malfunctioning service are a common starting point for quick investigations. That is, the investigations *can* be quick if EtherPeek is used to diagnose the problem. For an example of using EtherPeek to diagnose a service problem, see "Trouble with ftp services" on page 3, below.

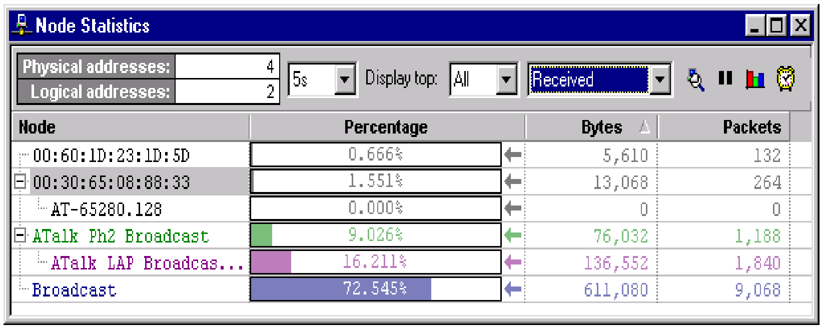
In addition to such common problems as service troubles or flagged errors, each network has its own particular set of features that are under watch from time to time. There might be a new file server or a new router whose configuration is still suspect. The very newness of these parts of the network might put them at the top of the network manager's watch list. A quick glance at the **Protocol Statistics** and/or the **Node Statistics** windows may be sufficient to assure that these new devices are performing as expected.
If particular problems are suspected, a Capture window can be set up with filtering to restrict capture to those items that will help diagnose the problem. Perhaps a trigger could be set to begin capture when a certain kind of traffic is seen, or at the time of day when the problem has occurred in the past.

Baselining your network

If the network's vital signs seem in order and no obvious problems present themselves, the next level of detail for many managers is simply a scan for anything out of the ordinary. To recognize what is out of the ordinary, however, you must first have a fair picture of what is *ordinary* for your network.

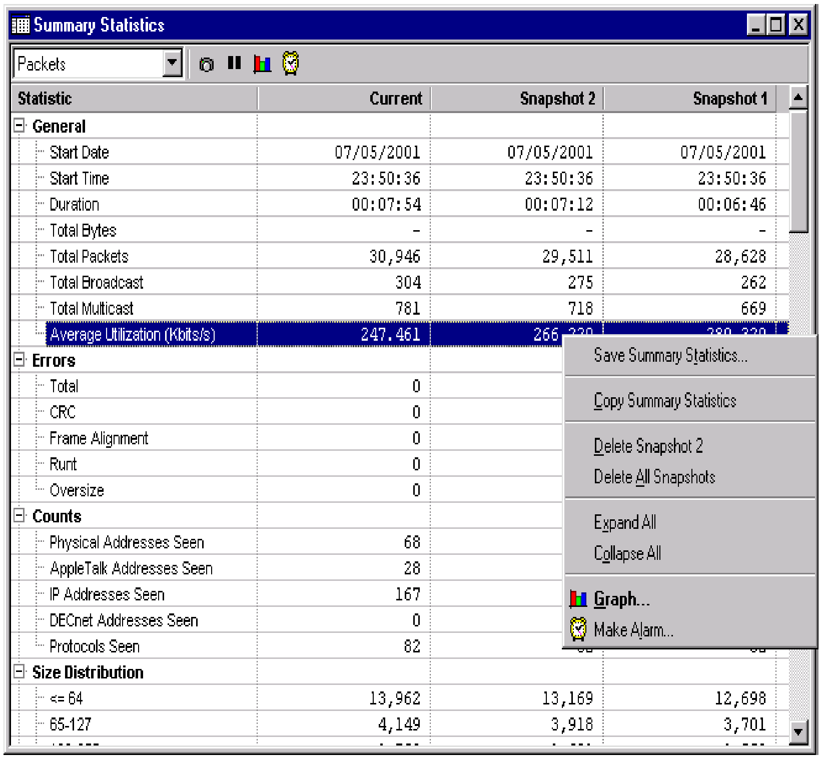
Effective network management, and especially network security, requires a fairly detailed understanding of how a particular network operates: how it is configured, what kinds of traffic to expect, from whom, when, and so forth. If you are new to a network (or if it is changing so fast it sometimes seems new to you), simply browsing with EtherPeek can be a great way to get to know the network better. Beyond that, however, EtherPeek can help establish a clear and a precise picture of normal conditions on your network.

The **Summary Statistics** window provides a good all-around view of key


Node Statistics

Physical addresses: 4
Logical addresses: 2
5s
Display top: All
Received

Node	Percentage	Bytes	Packets
00:60:1D:23:1D:5D	0.666%	5,610	132
00:30:65:08:88:33	1.551%	13,068	264
AT-65280.128	0.000%	0	0
ATalk Ph2 Broadcast	9.026%	76,032	1,188
ATalk LAP Broadcas...	16.211%	136,552	1,840
Broadcast	72.545%	611,080	9,068



Statistic	Current	Snapshot 2	Snapshot 1
General			
Start Date	07/05/2001	07/05/2001	07/05/2001
Start Time	23:50:36	23:50:36	23:50:36
Duration	00:07:54	00:07:12	00:06:46
Total Bytes	-	-	-
Total Packets	30,946	29,511	28,628
Total Broadcast	304	275	262
Total Multicast	781	718	669
Average Utilization (Kbits/s)	247.461	266.330	280.330
Errors			
Total	0		
CRC	0		
Frame Alignment	0		
Runt	0		
Oversize	0		
Counts			
Physical Addresses Seen	68		
AppleTalk Addresses Seen	28		
IP Addresses Seen	167		
DECnet Addresses Seen	0		
Protocols Seen	82		
Size Distribution			
<= 64	13,962	13,169	12,698
65-127	4,149	3,918	3,701

network parameters. You can take snapshots of the **Summary Statistics** window and look at them again later for easy comparison. A library of snapshots of different segments of the network under various normal conditions can be invaluable in troubleshooting elusive problems.

Even something as simple as a well-conceived Name Table can be a great help in distinguishing known from unknown entities, allowing you to quickly focus on what's different. The **Notifications** capability of alarms and many of the plug-ins is a great help in keeping tabs on the new and unusual. By enabling the right set of alarms and plug-ins for your network and setting their notification behavior correctly, you can let EtherPeek do much of the scanning for you.

Scanning for suspicious traffic or for possible attacks is also an important part of network management. This is covered in a separate section below. Please see "EtherPeek and network security analysis" on page 4.

Troubleshooting with EtherPeek

Troubleshooting is always a process of narrowing the possibilities. The troubleshooter wants to find out how and why the problem is happening. The examples that follow assume that the troubleshooter already knows something at least about the symptoms. EtherPeek helps to find the causes.

Trouble with ftp services

For example, a user complains that FTP services at the server are unavailable from his workstation. FTP appears to be working fine for other users. The manager can use a ***Details*** view of the **Node Statistics** to isolate just the FTP traffic between the server and that user's workstation. If no problems are evident there, keep the ***Detail*** view open, highlight the FTP conversations between the workstation and the server, and use the **Make Filter** command to create a new filter that will capture all the FTP traffic between those two nodes. You can then set up a Capture window with this new filter enabled. Its buffer will contain only the traffic related to this particular problem. You might want to set a Start Trigger for this new Capture window with its Trigger Event keyed to the new filter. You could also set a notification to be sent (by whatever Actions you have enabled in the **Notifications** dialog) when the Trigger Event occurs.

When this user next attempts to connect to the FTP server, the conversation will be recorded, you will know the conversation has started (if you set a notification), and you can either investigate further right away or do it later, offline. Either way, EtherPeek lets you look not only at statistics and a detailed packet list, but also at the contents of individual packets. You can check to see: Are the packets well formed? Is the login correct? Are the server's responses what you would expect?

If the user's problem is intermittent, it can make diagnosis more difficult. You must be there when it is happening in order to capture the relevant traffic. One approach that can help is to add packet slicing to the procedure above and to increase the size of the capture buffer. Packet slicing can capture all the relevant parts of the conversation without filling the buffer with the payload portions of all those FTP packets. This allows the same buffer to capture over a longer period of time. Where the conversations have long gaps between sessions, you might get even better results by setting up packet slicing and setting the Capture window's buffer to Continuous Capture, Save to Disk. With a larger sample size, you can improve your chances of finding the packets that betray the cause of an intermittent problem.

Undersized or runt packets

Ethernet compliant packets are at least 64 bytes long. Packets under that size are considered to be runt packets and are reported and flagged as errors. A certain number of packets on any network will be these undersized runts. When their number increases dramatically, it is a clear indication of trouble. Runts typically indicate a physical layer problem. There are two main causes for runts, the most common being a broadcast domain that is too big. A good rule of thumb is not to exceed 4 hops across hubs. If you do, the latency induced by regenerating and re-sending the data at each concentrator could lead to more than one device trying to talk on the wire at the same time. This causes collisions.

A faulty NIC will often announce its failure with a barrage of runt packets. A failing card may have difficulty accurately detecting other data on the wire. When this happens, it just starts jabbering. This jabbering may register as runt packets.

Runts can also be generated by concentrators and switches. The fix for the concentrator or switch-generated runt packets may be as simple as power cycling the device.

There are many anomalous conditions that could cause runts, but if you are not exceeding the length limitation and number of hops, try to narrow where the runts are coming from. Unfortunately, runts are often not proper packets at all but rather the random debris left over from collisions. If they are caused by a broken NIC, you can eliminate all those working properly and work backwards to find the culprit. If you have manageable concentrators, look for reports of runts on each port to narrow the search.

EtherPeek and network security analysis

EtherPeek is a definitive security analysis tool, and one of the few tools on the market that can actively verify firewall and router configurations and insure that the firewall or router is functioning as intended.

EtherPeek is extremely useful when installing, testing and verifying security products in use on networks, as well as essential in tracking down and gathering evidence against hackers and other intruders.

For example, many network file servers, mail systems, and databases have a default installation that allows for clear text passwords. In today's world, it is critical to disable these defaults and insure that at least the login passwords to these systems are encrypted. EtherPeek can examine the various logins to determine whether they are correctly configured and do, in fact, provide the password encryption needed.

Other uses of EtherPeek in the security business include the collection of messages looking for passwords. File Transfer Protocol (ftp) application in the TCP/IP suite has a PASSWORD embedded command in the command stream channel that is ideal for filter writing. By setting up EtherPeek with a filter for PASSWORD commands embedded in FTP (by using the String Filter or Value Filter), the security person can quickly examine why systems are failing password connections or where high connection count password attempts are coming from when trying to find the source of random login hacking.

Another popular security use for EtherPeek is the filtering of connection-request messages to security-sensitive high transaction servers from unauthorized address groups in various protocols. Looking for what does not belong on the network, as well as for what does, allows the security analyst to identify potential security issues before they become problems. For instance, if there are many connection attempts from a specific address outside the authorized group, it is time to pay a visit to the offender and find out what is going on before it gets serious.

EtherPeek and intrusion detection

The majority of LANs today consist of a switched Ethernet network connected through a firewall to a router and then to the Internet. In some cases, the firewall and router may be combined into a single product. EtherPeek can be used as a separate, undetectable (passive network analysis based) intrusion detection system. Typically, it is run on a separate host and records information to its own hard drive. The typical interface for this system would be a pager running on the same box.

To observe and record all hostile network activity, the user installs EtherPeek on the outside of the firewall and sets it to record all attack information to a log file. In this way, the user can have an additional record of attacks to supplement the log file from the firewall itself. Firewalls vary greatly in the degree to which they actively log information. Some flood the log files with arcane information, while some have no logging capability at all. Adding EtherPeek to an overall security plan can supplement logging activities or customize them for enhanced readability.

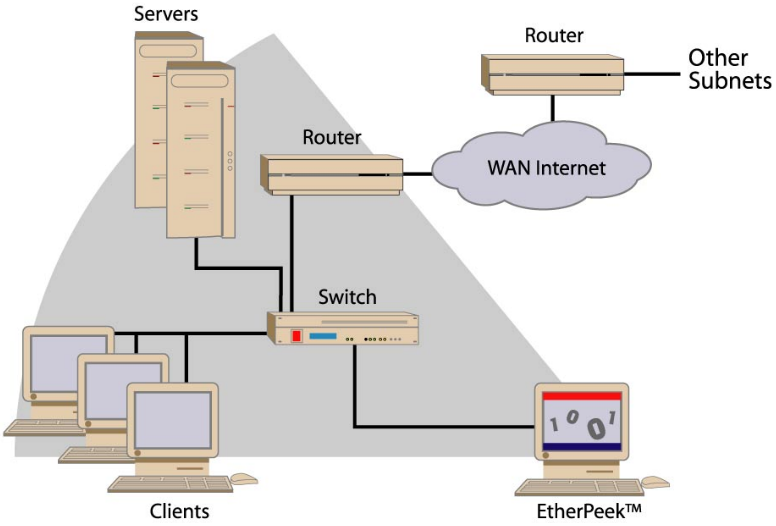
EtherPeek can also be set up just inside a firewall to monitor exactly what kind of traffic is getting through. Some form of Notification should also be set for EtherPeek to alert the network manager to any illegal traffic seen. This provides a means of keeping tabs on your firewall to insure that it has not been misconfigured, breached, or become outdated.

Finally, the user may want to set up a monitoring station to observe all traffic to and from certain servers. This is especially true if a user is running a server farm with a great concentration of servers within one protected subnet. Repeated studies show that upward of 90% of all successful attacks come from within networks from trusted users.

Testing firewall implementations

EtherPeek is essential in the installation and testing of firewalls. By using a small repeater hublet on the untrusted side of the firewall and wiring in EtherPeek on the untrusted side connection, a network manager can monitor all message traffic from the trusted side to the untrusted side. This allows verification that proper security rules and policies implemented in the firewall are functioning as expected. Such actions are also critical in monitoring for security packet leaks from the firewall to the untrusted side so they can be cleaned up before they are used to compromise the network.

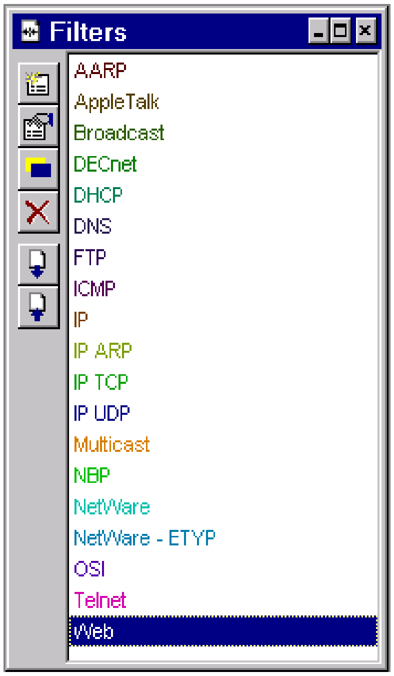
The performance analysis capabilities of EtherPeek allow the network security analyst to watch traffic levels to and from the firewall so the network can be adjusted for optimal security performance. For instance, larger packets



improve security system efficiency by reducing the number of IP headers that must be examined by the firewall system for a given message. If a message can be reduced to 1,000 packets instead of 10,000 packets, there are only 1,000 IP headers to examine and this improves performance in the firewall dramatically. Using EtherPeek to perform normal network performance analysis also improves security processing when the systems are adjusted properly.

Firewalls are extremely difficult to configure correctly, particularly if used in conjunction with access lists (filters) on routers. The filter editing facilities on most routers are cryptic, at best. The **Make Filter** command combined with the **Show Data Offsets** option for the Packet Decode window can make writing filters much easier, especially for the manager who only needs to write filters occasionally. In addition, EtherPeek can quickly test the filtering set-up of any router or firewall. EtherPeek can probe firewalls, hosts and routers and, more importantly, can directly observe the results of probing. WildPackets' iNetTools is an IP utility suite shipped with EtherPeek. It contains many useful applications that supplement EtherPeek, including the ability to generate port and service scans. Using EtherPeek and iNetTools together, the user can simultaneously probe and observe packets on the same network. A port scan generates a ping for each port within TCP and UDP. It is commonly used to determine what services are running on a UNIX workstation or server. With the introduction of Internet technology, IP services are now run on a wide range of hosts and operating systems. By port-scanning a device, the user can find misconfigured or unknown services. A service scan looks for a single TCP or UDP port within a range of IP addresses. It is a good idea to conduct a service scan monthly for FTP, HTTP, and telnet services. By default, these services are configured with no security whatsoever and can easily be used to compromise other devices on your network.

Firewalls are typically configured to allow certain services to be advertised on the outside interface. All other services and IP addressees should be blocked. Many firewalls can be configured for Network Address Translation (NAT) and/or Port Address Translation (PAT).



Another way to test a router or firewall is with two NICs — one configured to be used by EtherPeek, and the other configured to be used by iNetTools. In this configuration, the user can inject a probe on the outside of the firewall with iNetTools and listen on the inside with EtherPeek. Each product must be properly configured to use a separate NIC, and each NIC must be attached to the appropriate LAN or firewall network interface.

Validating network attacks

EtherPeek can test various denial of service attacks or determine exactly what is causing specific network services to fail. Use EtherPeek to capture what you believe to be the offending packet, then retransmit it in a test setting and observe the results. Depending on the type of problem you are trying to diagnose, you might want to use **Send Selected Packets** or set one particular packet as the Send Packet and test the results with that one alone. Broken packets can be captured in several ways. In some cases it may be possible to use **Make Filter** and/or the **Edit Filter** dialog to create a filter that will capture all the broken packets. Alternatively, you can run a full packet capture and then discard packets that are known to be good. The rest of the packets can then be sent again and the results observed. By following this process in a series of steps, you will eventually discard all good packets until only the broken packet(s) remain.

Triggers are also useful. Triggers in EtherPeek can be set to start capturing at a specific time or based on the occurrence of a specific packet appearing on the wire. For example, you might offer FTP or HTTP services at some non-standard port for users who are offsite. You might set a Start Trigger to capture *any* traffic to that port between the hours of midnight and 6:00 am.
Using EtherPeek as a data analyzer is essential for identifying specific hacker activities on a network. For instance, it can easily identify specific IP addresses seen in firewall logging facilities in any suspicious trusted-to-untrusted IP traffic. Using the firewall activity logs (especially on stateful & proxy combination firewalls), suspicious activities are logged by IP address and event. Firewalls usually do not capture enough information for legal prosecution to be airtight. Creating an address filter in EtherPeek for the suspicious IP addresses, and collecting data at the right place in the network produces evidence of activities and events that back up the logging in the firewall and other network devices. Proper evidence is vital in gaining either civil or criminal judgement against a hacker.

Shared, switched, and distributed networks

As networks get larger, their workstations more numerous and powerful, and traffic more bandwidth-intensive; shared media networks like Token Ring and Ethernet cannot easily keep up. Networks must be segmented and subsegmented to accommodate the increased traffic.

EtherPeek and switches

Because switched devices forward packets only to the specific port to which they are addressed, EtherPeek and all packet analyzers are limited to capturing broadcast and multicast packets and the traffic sent or received by the device(s) attached to a single port. This, of course, negates the program's ability to capture and diagnose all traffic on a LAN segment.

There are, however, several techniques for effectively using EtherPeek in a switched environment. EtherPeek can provide both global port balancing information, through Node Statistics and other statistics views, and specific troubleshooting information using Capture windows and Packet Decode windows. Most switches also allow for port monitoring to mirror any port's traffic to the port where EtherPeek is installed. EtherPeek can then see and diagnose all traffic from the port(s) that have been mirrored.

Please refer to WildPackets' white paper entitled **"Applying EtherPeek to Switched Network Management,"** at http://www.wildpackets.com/resources.

EtherPeek and enterprise networks

WildPackets' white paper entitled **"EtherPeek in the Enterprise Environment"** describes a simple solution to manage the complex distributed networks found in today's enterprise environment. EtherPeek, together with Netopia's Timbuktu™, provide a method for monitoring performance across the enterprise network, from multiple local segments to a remote LAN. This paper is available at http://www.wildpackets.com/resources.

WildPackets Professional Services

WildPackets offers a full spectrum of unique professional support services, available on-site, online or through remote dial-in service.

On-Site Consulting

When protocol analysis support is needed at your site, the network experts at WildPackets will work with you and your support team to resolve network problems.

Performance Baseline and Network Capacity Planning Report

When it is necessary to know the real performance and capacity issues facing your network, a WildPackets consultant can create a baseline report, from a simple evaluation of a single critical server or router up to an assessment of your overall network infrastructure.

Infrastructure Design Analysis Services

The network experts at WildPackets can help you sort through the details of multi-vendor proposals for hardware and software installation and systems integration, providing you with an unbiased, third party perspective on your proposed network planning,

Remote Consulting Services

WildPackets' Remote Consulting Services may resolve challenging network problems for you without requiring an on-site visit. Our protocol analysis experts will accurately analyze specific trace files you send in to them or capture live traffic from your network and provide a general characterization of network performance and potential problems.

WildPackets Academy

WildPackets Academy offers the most effective and comprehensive network and protocol analysis training available, meeting the professional development and training requirements of corporate, educational, government, and private network managers. Our instructional methodology and course design centers around practical applications of protocol analysis techniques for both Ethernet and 802.11b wireless LANs. WildPackets Academy also provides instruction and testing for the industry-standard **NAX™ (Network Analysis Expert) Certification.**

For more information about consulting and educational services, including complete course catalog, pricing and scheduling, please visit http://www.wildpacketsacademy.com. NAX examination and certification details are available at http://www.nax2000.com.

Live Online Quick Start Program

WildPackets now offers one-hour online Quick Start Programs on using EtherPeek and AiroPeek, led by a WildPackets Academy Instructor. Please visit http://www.wildpackets.com/events for complete details and scheduling information.

WildPackets, Inc.

Since its inception in 1990, WildPackets has been developing affordable tools designed to simplify the complex tasks associated with designing, maintaining, troubleshooting and optimizing computer networks. In the past eighteen months, WildPackets has acquired two key partner organizations and greatly expanded its product development expertise and professional services capabilities in the process. WildPackets customers include Ameritech, Cisco Systems, Lucent Technologies, Microsoft, National Institutes of Health, Yahoo! and others. Strategic partners include Cisco Systems, Symbol Technologies and Agere Systems.

WildPackets, Inc.
2540 Camino Diablo
Walnut Creek, CA 94596
Tel 925-937-7900
Fax 925-937-2479
www.wildpackets.com