

EtherPeek™

Ethernet Protocol Analyzer

Tackle Tough Network Problems

WildPackets award-winning EtherPeek is an intuitive, powerful network and protocol analyzer for Ethernet networks. Available for Windows and Macintosh platforms, EtherPeek simplifies the complex tasks of troubleshooting mixed-platform, multi-protocol networks. EtherPeek sets the industry standard for ease-of-use while offering all of the decoding, filtering and diagnostics of a high-end analyzer.

Well-known for its friendly graphical interface, EtherPeek provides a wide variety of detailed information on network utilization, node conversations and packet contents. Use EtherPeek to localize network problems, perform sophisticated diagnostic tests, monitor network traffic and events, trace illicit network activities, and test and debug network hardware and software.

Quickly Isolate & Diagnose Network Trouble

Similar to a phone tap, EtherPeek captures all data packets exchanged between nodes on the Ethernet wire — regardless of the types of hardware and software installed on your network. EtherPeek interprets the protocol layers of a captured frame and exposes the core information. By monitoring, filtering, decoding and displaying packet data, EtherPeek easily pinpoints protocol errors and detects network problems such as unauthorized nodes, misconfigured routers and unreachable devices.

Monitor Network Performance in Real-Time or in Retrospect

You can't afford network slowdowns or bottlenecks. EtherPeek's real-time network statistics depict traffic in terms of overall utilization, nodes, conversations and protocols. History statistics provide performance data through traffic captured for a specified time interval.

By viewing current or saved traffic (restored for post-capture analysis), you can easily identify "talkative" nodes or "chatty" protocols generating unnecessary traffic. Discover which protocols consume the most bandwidth and which nodes communicate most frequently. Or check to see how a router is handling traffic during peak hours.

Remote Analysis in a Distributed Network

EtherPeek, combined with the free and freely distributed remote packet capture application EtherHelp, is an enterprise-wide fault and network performance management solution that distributes "Peek" network monitoring, packet filtering and triggering capabilities to key segments (LAN, WAN and Gigabit Ethernet) throughout the network. The ability to focus on specific traffic remotely makes this powerful tool perfect for extended and physically separated networks.

Detect device failures and faulty software

Identify routing and addressing problems

Track internet usage

Packet	Source	Destination	Flags	Size	Absolute Time	Proto
1	IP-192.216.124.78	IP-192.216.124.1		89	11:03:37.699445	DNS
2	IP-192.216.124.1	IP-192.216.124.78		294	11:03:37.715292	DNS
3	IP-192.216.124.78	IP-204.123.2.75		66	11:03:37.763714	HTTP
4	IP-204.123.2.75	IP-192.216.124.78		66	11:03:37.772616	HTTP

Packet: 2

- Status: 0x00
- Packet Length: 294
- Timestamp: 11:03:37.715292 09/30/1997
- Ethernet Header
 - Destination: 08:00:07:3C:00:46
 - Source: 08:00:20:83:5D:91
 - Protocol Type: 0x0800 IP
- IP Header - Internet Protocol Datagram

0000: 08 00 07 3C 00 46 08 00 20 83 5D 91 08 00 45 00 ...<.F...l...E.
0016: 01 14 9F E9 40 00 FF 11 60 EE C0 D8 7C 01 C0 D8 ...@... ..
0032: 7C 4E 00 35 80 00 01 00 40 E8 00 18 85 80 00 01 |N.5...@.....
0048: 00 05 00 03 00 03 03 77 77 77 09 61 6C 74 61 76www.altav
0064: 69 73 74 61 07 64 69 67 69 74 61 6C 03 63 6F 6D ista.digital.com
0080: 00 00 01 00 01 C0 0C 00 05 00 01 00 00 1C 20 00
0096: 17 09 61 6C 74 61 76 69 73 74 61 07 64 69 67 69 ..altavista.digi

Packets: 136 Duration: 00:00:14

EtherPeek's 3-pane view of packet list, packet decode, and hex view. Capture Windows show packets as they are processed. Multiple capture windows can be used to simultaneously filter for conversations, protocols or various statistics of interest.

Powerful

Affordable

Easy-To-Use



"WildPackets' EtherPeek earned the top spot in the competition for the breadth of protocols it could decode, its low cost, the ease with which we could navigate its screens to determine the cause of a problem, and the clarity of its reports."

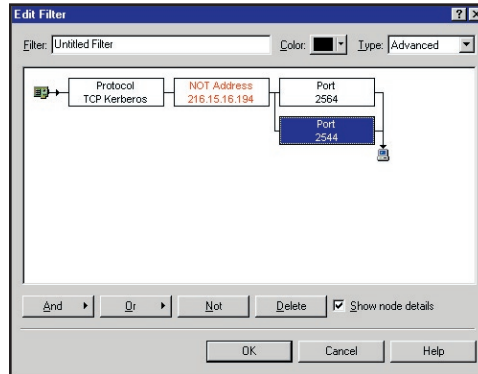
Network World Global Test Alliance

"EtherPeek is a rarity, combining powerhouse features with a handsome interface..."

EtherPeek Earns PC Magazine Editors' Choice Award May, 2001

Filter for Specific Traffic Easily

EtherPeek's powerful packet filtering mechanism helps locate and remedy network problems quickly and easily. Use these flexible, powerful filters during or after capture to isolate traffic by specific node, protocol, error type and/or packet content. EtherPeek's simple "Make Filter" command allows you to immediately create and filter for specific network traffic by highlighting a packet line. Advanced filtering capabilities add OR, AND, and NOT support in filter creation and implementation.



Be Notified of Network Events

Take proactive measures by setting alarms to warn of significant network events and indications of trouble before they escalate. Set a threshold alarm on any node, protocol or network statistic. In addition to visual, audio, and pager notification options, EtherPeek can execute a batch process (Windows version) or an Applescript (Mac version), such as "send an email," whenever a network event occurs.

Debug Network Hardware & Software

EtherPeek is a powerful tool for assisting network hardware and software developers to:

- Check for protocol compliance
- Generate traffic to test varying loads
- Send packets to test device reactions
- Customize or alter packets for testing
- Develop custom packet decoders & filters for use with uncommon or proprietary protocols

EtherHelp

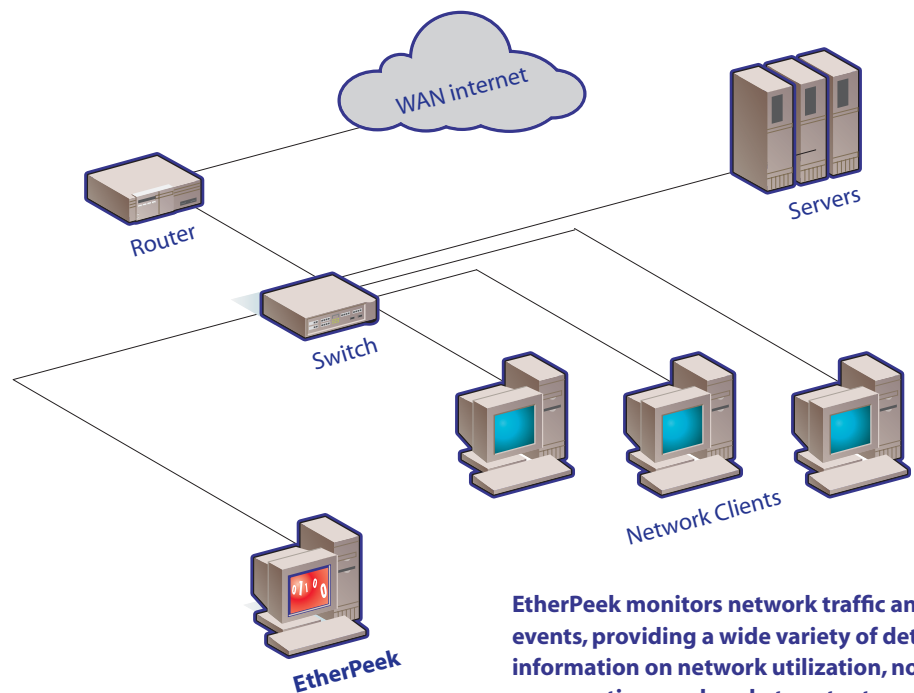
- Helps people who design, build, manage and support multi-protocol, multi-topology networks perform remote analysis on a LAN/WAN segment.
- Captures all network traffic, (or a specified portion of that traffic), then saves that traffic in a packet file.

Choose Your Format

EtherPeek can save in text, Peek, or Sniffer(.enc) format so that you can share packet traces between legacy systems and our software. Further extend EtherPeek's scope and the interplay with legacy analyzers by using ProConvert™ to convert packet traces between almost any hardware or software-based analyzer and EtherPeek.

Enhanced Report Generation

Output statistics to your web pages to access data concerning your network's health anywhere, anytime. Automatically generate statistics reports in XML format through templates provided with the software.



EtherPeek monitors network traffic and events, providing a wide variety of detailed information on network utilization, node conversations and packet contents.



EtherPeek Features

EtherPeek Benefits

Customizable, Multi View Display

EtherPeek's 3-Pane View displays the packet capture list, single packet decode, and hex view of raw data, altogether or in any combination, providing a wealth of information at a glance.

Multiple Capture Windows

Capture and view conversations, node and protocol activity in separate buffers simultaneously. Quickly create new capture windows with exact settings from saved template.

Thousands of protocol & sub-protocol decoders

Interpret data for packets from ALL major protocol suites.

Powerful real-time & post-capture filtering

Locate and remedy network problems quickly by limiting packet captures to data of Real-time event triggers interest with user-definable triggers and filters.

Grouped Name Tables

Work with familiar, identifiable names for easy packet, port, and device analysis.

ProtoSpecs™ protocol layer hierarchical

Facilitate protocol filtering, monitoring and analysis. Learn the meaning and function of any break outs with definitions protocol discovered.

Simple and advanced filtering

Enhanced filter application allows instant creation of a filter based on any packet attribute, as well as automatic "accept" or "reject" matching subset of packets.

Extensive notification capabilities including visual, audio, pager, speech and email

Take proactive measures — Identify precursors to major problems.

Modular plug-in architecture

Expand EtherPeek's built-in functionality with standard Plug-in analysis modules including InternetAttack, ICMP Details, FTP Analysis, Telnet, Web URL, and more.

Generate traffic — Send/alter packet function

Test varying loads and device reactions to specific packet types.

Real-time HTML and enhanced XML traffic statistics report generation

Monitor live network traffic from any location with your Web browser.

Summary statistics

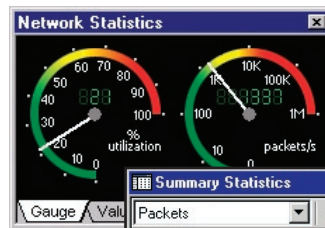
Baseline key network data at requested intervals for a comparative look at network performance.

History statistics

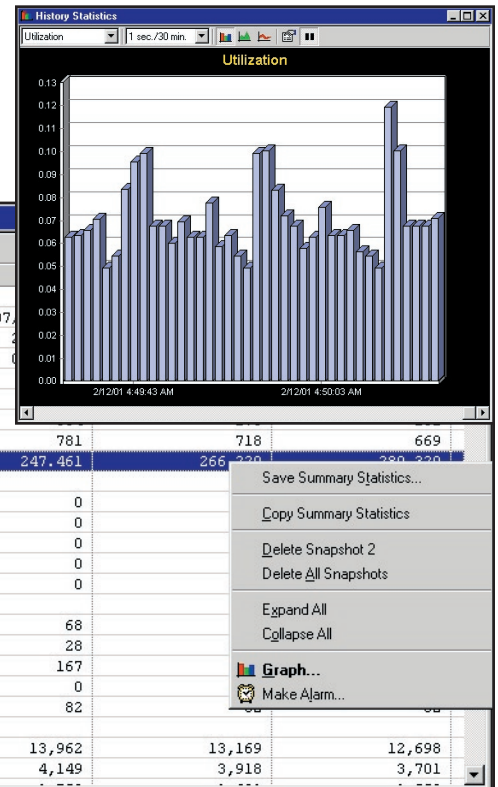
Easily identify performance statistics over time for your network, including: utilization, packets/second or bytes/second for a specified time interval.

Analyze Network Trends

Sophisticated graphing and trending features allow the analysis of any node, protocol, network or summary statistic. This analysis can be collected, displayed, saved and analyzed over a user-specified period of time. View trends through a variety of graph options from within the program. Output data in enhanced XML format for web access, or save statistics in tab-delimited form that can be exported to an external charting application.



Summary Statistics	
Statistic	
General	
Start Date	07/21/2001
Start Time	4:49:43 AM
Duration	0:00:00
Total Bytes	611,080
Total Packets	13,962
Total Broadcast	4,149
Total Multicast	13,169
Average Utilization (Kbits/s)	3,918
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
65-127	4,149



Node Statistics		
Physical addresses:	4	5s
Logical addresses:	2	Display top: All
Received		
Node	Percentage	Bytes
00:60:1D:23:1D:5D	0.666%	5,610
00:30:65:08:88:33	1.551%	13,068
AT-65280.128	0.000%	0
ATalk Ph2 Broadcast	9.026%	76,032
ATalk LAP Broadcas...	16.211%	136,552
Broadcast	72.545%	611,080



Product Extensions

EtherHelp

EtherHelp extends EtherPeek's powerful packet capture and filtering capabilities to multiple LAN/WAN local and remote network segments.

EtherPeek Plug-Ins

External plug-in modules help you find and log duplicate IP address use, verify checksums, log Web usage and FTP downloads. EtherPeek includes a Plug-in SDK, so anyone with programming experience can extend the capabilities of the program by writing custom add-in enhancements.

WebStats Analysis Module

This flexible, highly configurable analysis module focuses on capturing information that helps you improve customer acquisition, optimize content placement and analyze the effectiveness of your website.

Decoders

Decoders help expand your capabilities. EtherPeek's Decoder files, which include over 1000 primary protocols and subprotocols, are separate from the program and extensible.

A Decoder SDK is included with EtherPeek for any user with programming experience to customize or add their own decoders.

NetSense ProAnalyst

NetSense™ performs expert analysis of peer-to-peer conversations on packets captured from over 20 different supported protocol analyzers. NetSense extracts critical information from each packet and displays it in several different formats, empowering you to view trace files in a highly graphical and interactive fashion.

iNetTools

Add iNetTools™ for Internet and IP-based networks to EtherPeek's Tool menu (WIN version ONLY) during EtherPeek's installation process to get ready access to a variety of testing tools, including Ping, Trace Route, DNS Lookup and more!

ProConvert

Trace File Converter ProConvert™ supports two-way LAN packet capture file interchange between the "Peeks" and over 20 different protocol analyzers and packet capture formats.

WildPackets Academy

WildPackets Academy meets the professional development and protocol analysis training requirements of network managers at all levels. All course offerings are available in public venues and as on-site programs that can be tailored to meet specific customer requirements.

Course offerings include:

- Foundations of Network Protocol Analysis
- Network Troubleshooting Methods
- Full-Duplex and Switched Ethernet Analysis
- TCP/IP Protocol Analysis
- LAN/WAN Special Topics

For a complete course outlines and schedules, instructor bios or a course catalog visit:

www.wildpacketsacademy.com

Product Maintenance

All WildPackets products include 90 days of product maintenance during which all product updates and upgrades are free.

One and two year extended maintenance is also available, providing priority response technical support, on-line or automatic shipment of product upgrades and updated documentation, monthly technical mailings, free utility software, and more.

Ordering Information

WildPackets products are available from our Channel Partners, directly from sales@wildpackets.com or from the electronic purchase area at:

www.wildpackets.com

Download a Demo!

Demos are available for all of our products at:

www.wildpackets.com/demos

System Requirements

To minimize the chance of packet capture loss and to optimize EtherPeek's overall performance, a system with at least a 600 MHz processor, 256 MB RAM, running Windows XP or Windows 2000* is recommended.

Microsoft Internet Explorer 5.0 or later required for XML and HTMLreporting/saving features.

*Also tested on Windows NT 4.0 Workstation

For Gigabit analysis: A 64-bit PCI bus is required, and at least 1 GHz and 1GB RAM is recommended.

WildPackets, Inc.

Since 1990, WildPackets has been developing powerful, affordable tools designed to simplify the complex tasks associated with designing, maintaining, troubleshooting and optimizing computer networks.

Solution Suites

Our solution suites perform a variety of network management tasks, including: performance management, fault management, throughput analysis, trend analysis and more. They are available for purchase in various configurations: single license, site license and bundles.

Our representative solution suites include:

Wireless Analysis
Remote Analysis
Gigabit Ethernet
Network Management Suitcases
Training Bundles

For more information, visit
www.wildpackets.com/products

WildPackets

1340 Treat Blvd, Suite 500
Walnut Creek, CA 94597
main (925)937-3200
fax (925)937-3211

www.wildpackets.com

