



## OmniEngine™ Software Probe

Building on WildPackets' award-winning network analysis technology, OmniEngine™ software probe performs real-time network analysis on traffic from one or more network interfaces, including Ethernet, Gigabit, 10 Gigabit (10G), and 802.11 a/b/g/n wireless. OmniEngine captures and analyzes data in real-time, and records data for post-capture analysis. With WildPackets® OmniEngine, network engineers can rapidly troubleshoot faults—even faults occurring at remote locations—without leaving their office.

Designed for data centers, network operations centers and large application servers, OmniEngine software probes extend network analysis capabilities through distribution to any network segment or function, even to remote locations. OmniEngine software probes can perform data capture and network analysis on multiple network interfaces, and over all network topologies, as well as providing advanced Voice and Video over IP analysis. OmniEngine software probes are best deployed in large scale, distributed networks that include remote locations, providing continuous network monitoring and analysis without the need for local network engineering support. To completely cover your network analysis needs, one or more OmniEngine software probes should be deployed at each remote location, with every server farm, and within the network operations core.

OmniEngine software probes run as a service on standard Windows platforms as well as on WildPackets' network recorders, which are available in both Windows and Linux configurations. By installing OmniEngine software probes in each business location, a network engineering team gains real-time visibility into all its remote networks. Enterprises that cannot

afford to staff each office with a network engineer can use OmniEngine software probes to ensure that every business location receives the network engineering support it needs.

OmniEngine software probes provide comprehensive network service analytics, including:

- Analyze traffic from all network segments, including 10 Gigabit, Gigabit, Ethernet, and 802.11a/b/g/n (including 3-stream) segments
- Ability to monitor networks, application performance and multi-media in separate high-level views, or "Dashboards," and instantly drill down to see which traffic characteristics are affecting network performance.
- Application-layer expert diagnoses, application performance, and application response time (ART) analysis.
- Complete Voice and Video over IP media and signaling analysis, including MOS and R-Factor scores, detailed packet flow visualization of each call, call data record (CDR), and call playback.
- Complete analysis for leading solutions such as Avaya, Cisco, and MGCP.
- Complete visibility into MPLS and VLAN networks by monitoring, gathering statistics, and making graphs and alarms on packet-switched and virtual environment.
- Expert Systems Diagnoses, including streams-based packet analysis and correlations between events and conversations.
- Statistical Analysis, including packet flows and details about nodes, protocols, and subprotocols.



**Total Network Visibility**



**Edge to Core Network Analysis**

### WildPackets' solutions enable businesses to

- Gain unprecedented visibility into networks and applications
- Accelerate find-to-fix times
- Discover and close network security gaps
- Maximize ROI on existing networks and applications
- Increase IT efficiency and responsiveness
- Reduce costs associated with network downtime and service degradation
- Reduce IT labor costs
- Increase end user productivity

- Packet Analysis, including protocol decodes and descriptions of physical errors.
- Detailed reporting of all statistical network analysis in a range of output formats, including real-time graphs, HTML, PDF, and CSV.
- Flexible Capture Settings tuned to meet every need, from detailed, real-time analysis to high-speed capture-to-disk for post-capture analysis.
- Forensic search tools to quickly isolate and process data from multiple capture files.
- Infrastructure Monitoring, including 24x7 monitoring and analysis of network traffic. When network problems occur, OmniEngine executes SNMP traps, notifying SNMP monitoring systems, such as HP OpenView, of potential problems. Because it captures the traffic that generated the error, OmniEngine software probes provide network engineers the detailed information they need in order to investigate and resolve problems.

While other packet analysis products offer only simplistic threshold-based alarms, OmniEngine offers a wealth of information and features that network engineers can use to rapidly troubleshoot faults.

## OmniEngine Enterprise

OmniEngine Enterprise performs real-time network analysis on traffic from one or more network interfaces, including full-duplex 10G and Gigabit, Ethernet, and 802.11 a/b/g/n wireless. OmniEngine captures and analyzes data and multimedia in real time, and records data for post-capture analysis. OmniEngine Enterprise software provides advanced Voice and Video over IP functionality including signaling and media analyses, voice and video Expert Analysis, and monitoring of the entire multi-media network. OmniEngine Enterprise is also ideal for IT organizations responsible for application performance and network service level agreements (SLAs) for the entire organization.

When running on a WildPackets Network Recorder, OmniEngine Enterprise software can capture and store hours or even days of network traffic for forensic analysis.

## OmniEngine Desktop

WildPackets' OmniEngine Desktop is a Windows service that runs on desktop computers and captures packets for analysis. OmniEngine Desktop software provides network engineers with the visibility into end user computers they need in order to accelerate troubleshooting and to maximize productivity. Packet captures can be initiated by network engineers or Help Desk representatives running the OmniPeek® network analyzer; alternatively, captures can be initiated automatically when specific trigger conditions are met. Once a capture is complete, network engineers can transfer the packets into OmniPeek for analysis.

## TimeLine™ Network Recorder

The TimeLine network recorder brings capture and analysis of network and media traffic on highly utilized networks to a whole new level. TimeLine is the fastest, continuous network traffic capture and analysis solution in its class that displays the key network and media statistics in real-time with no negative impact on write-to-disk rate. TimeLine sets a new standard in capture-to-disk speeds, offering unsurpassed network traffic collection and recording, the most complete sets of real-time statistics, quick data rewinding, simultaneous real-time network monitoring, and rapid search and forensic analysis of collected data. With TimeLine, network issues of any type can be identified, analyzed, reconstructed, and resolved quickly and efficiently.

## Omnpliance® Network Recorder

The Omnpliance network recorder is a turnkey, continuous capture solution that gives network engineers unprecedented, real-time and post-capture visibility into remote network segments. Each network recorder runs WildPackets' OmniEngine Enterprise software and sends real-time analytics and monitoring results to a central OmniPeek console. The Omnpliance is an ideal data recorder for network forensics applications, such as incident response operations and policy compliance investigations.

## WildPackets Distributed Network Analysis

WildPackets gives network engineers real-time visibility into every part of the network—simultaneously from a single interface—including 10/100, Gigabit, 10G Ethernet, 802.11 wireless, and VoIP. Using OmniPeek's local capture capabilities, centralized console, distributed OmniEngine intelligent software probes, Omnpliance and TimeLine network recorders, and Expert Analysis, engineers can monitor their entire network, rapidly troubleshoot faults, and fix problems to maximize network uptime and user satisfaction.

## About WildPackets, Inc.

WildPackets develops hardware and software solutions that drive network performance, enabling organizations of all sizes to analyze, troubleshoot, optimize, and secure their wired and wireless networks. WildPackets products are sold in over 60 countries and deployed in all industrial sectors. Customers include Boeing, Chrysler, Motorola, Nationwide, and over 80 percent of the Fortune 1000. WildPackets is a Cisco Technical Development Partner (CTDP). For more information, visit [www.wildpackets.com](http://www.wildpackets.com).



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

[www.wildpackets.com](http://www.wildpackets.com)