WildPackets

OmniEngine™ Software Probe

The Challenge

Enterprises and service providers depend on reliable network performance. Configuration errors, network faults, and security attacks can jeopardize operations—and the corporate bottom line. To keep networks performing optimally, engineers need to be able to continuously monitor their networks and troubleshoot problems wherever they occur, as quickly as possible. They need real-time analysis for every type of network segment—Ethernet, 1/10/40 Gigabit, 802.11, and voice and video over IP—and for every level of network traffic, including spikes in usage. These analysis capabilities must be available 24/7 in an easy-to-deploy, easy-to-use solution.

The Solution: OmniEngine™ Software Probe

Building on WildPackets' award-winning network analysis technology, the OmniEngine™ software probe performs real-time network analysis on traffic from one or more network interfaces, including Ethernet, 1/10 Gigabit, 802.11, and voice and video over IP. OmniEngine captures and analyzes data in real-time, and records data for post-capture analysis. With OmniEngine, network engineers can rapidly troubleshoot faults—even faults occurring at remote locations—without leaving their office.

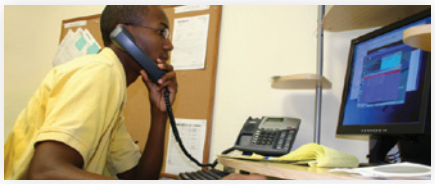
Designed for data centers, network operations centers, and large application servers, OmniEngine software probes extend network analysis capabilities through distribution to any network segment or function, even to remote locations. OmniEngine software probes can perform data capture and network analysis on multiple network interfaces, on all network topologies, as well as providing advanced voice and video over IP analysis. When OmniEngine software probes are deployed in remote locations, they provide 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 are available as stand-alone Windows software, or as part of WildPackets® network analysis and recorder appliances, 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:

- Analysis of traffic from all network segments, including Ethernet, 1/10 Gigabit, 802.11, and voice and video over IP.
- Ability to monitor networks, application performance, and multi-media in separate high-level dashboards, and instantly drill down to see which traffic characteristics are affecting network performance.

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

- 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 records (CDR), and call playback.
- Complete analysis for leading VoIP solutions such as Avaya, Cisco, and MGCP.
- Full path visibility, with hop-by-hop latency and health analysis, by correlating captures between OmniEngines using multi-segment analysis.
- Complete visibility into MPLS and VLAN networks by monitoring, gathering statistics, and creating graphs and alarms on packet-switched and virtual environments.
- Expert systems diagnoses, including stream-based packet analysis and correlations between events and conversations.
- Statistical analysis, including packet flows and details about nodes, protocols, and subprotocols.
- 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.
- Forensics search tools to quickly isolate and process data from multiple live captures or stored 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 with 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 Ethernet, 1/10 Gigabit, 802.11, and voice and video over IP. OmniEngine captures and analyzes data and multimedia in real time, and records data for post-capture analysis. OmniEngine Enterprise 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. The Timeline view makes OmniEngine Enterprise ideal for IT organizations responsible for application performance and network service level agreements (SLAs) by providing real-time visibility, instant investigation, and work flow escalation.

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

OmniEngine Desktop

OmniEngine Desktop is a Windows service that runs on desktop computers and is available 24x7 to capture network data for analysis where it matters most—at the end user. 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 remotely 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 to OmniPeek for analysis.

WildPackets Distributed Network Analysis

WildPackets gives network engineers real-time visibility into every part of the network—simultaneously from a single interface—including Ethernet, 1/10/40 Gigabit, 802.11, and voice and video over IP. Using OmniPeek's local capture capabilities, centralized console, distributed OmniEngine intelligent software probes, Omnipliance® network analysis and recorder appliances, 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.

WildPackets
1340 Treat Blvd, Suite 500 | Walnut Creek, CA 94597
(925)937-3200 | fax (925)937-3211 | www.wildpackets.com

OESP-20131118