Observer offers greater insight

Network Instruments' Observer 10 distributed packet analyser introduces several welcome capabilities that ease ongoing reporting, reduce WAN congestion and improve WLAN analysis

> NETWORK ANALYSIS

Dave Bailey

Observer Suite 10 is the latest version of Network Instruments' distributed network packet analyser. It features a new architecture for performing network data analysis and processing, the ability to capture and analyse packet data from virtual LANs (VLANs) in real time, enhanced checks for wireless LANs, new reporting options and expanded data mining capabilities.

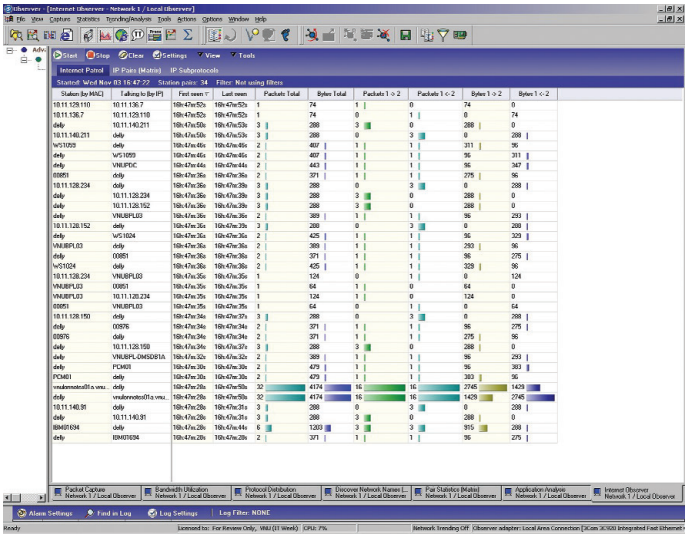
The Network Instruments Observer product family starts at £995 + VAT for the basic package, while the Expert Observer costs £2,895 + VAT and the full Observer Suite 10 package costs £3,995 + VAT.

We reviewed Observer 10 using standard desktop and laptop PCs, all fitted with dual network interface cards (NICs). The software runs only on Windows desktop and server systems. Installation was simple and we were able to perform a packet capture and start taking data off a LAN in under five minutes.

One of the most significant changes in the Observer 10 Suite is in how the Expert Probes analyse and present processed data when capturing packets at remote locations. The processing logic has been moved from the console to the actual probe so that the data is processed at the point of capture, and only screen updates are transmitted over the network.

To look at the new VLAN options, we segmented our switch, creating a VLAN for traffic passing to and from *IT Week* Labs and another VLAN for network traffic running between our email servers and networked storage shares. Using Observer 10, we could see packets received, packets transmitted, and the level of broadcasts, multicasts and overall utilisation of each VLAN – all in real time.

Network Instruments has improved the way the software monitors wireless networks, allowing admin staff to set thresholds or conditions to send alerts via email or a paging server if WEP is disabled or if a rogue access point is detected, for example. As well as security alerts, Observer 10 can also report on wireless performance parameters such as data rates and station bandwidth utilisation.



The Oserver Suite 10 packet analyser from Network Instruments can monitor LAN, virtual LAN and wireless LAN performance, displaying data in real time

We found it easy to look through uploaded packet capture files and analyse the packets individually using the connection dynamics option, or just look at a summary of the whole packet capture. This gave data on the packet size distribution and a distribution by protocols such as AppleTalk, address resolution protocol (ARP) and IP. We could also drill down into the IP statistics to see how many DHCP and domain name service (DNS) packets were moving around the network.

We did find a problem with the pair statistics matrix, a feature designed to track pairs of stations conversing on the network. The data can be presented as a list or as a circular dial, but when using the dial, if there are a lot of stations on the LAN, then the text showing individual station's MAC or IP addresses becomes very difficult to see. Using the clumsy built-in zoom function is time consuming.

Users who need to capture and analyse large amounts data over extended periods will be pleased to know that Network Instruments has improved the data mining capabilities of Observer 10 so that multiple files can be analysed. We could search multiple packet capture files for specific MAC addresses or IP addresses and analyse this data. The way the system reports and presents this data has also been improved. There are more than 20 templates that can be used as a basis for making a network summary report. NITW

FINDINGS

Observer Suite 10

Network Instruments' Observer Suite 10 offers network administrators a comprehensive package for monitoring and detecting network problems, and the expanded data mining and reporting options as well as the support for VLANs make this one of the best packet analysers around.

✓ Covers almost all network topologies and packet types; excellent wireless LAN support.

✗ Requires a high degree of expertise;

Price Observer 10, £995 + VAT; Expert Observer 10, £2,895 + VAT; Observer Suite 10, £3,995 + VAT; Advanced Expert Probe, £2,895 + VAT

Contact Network Instruments 01959 569 880

www.networkinstruments.co.uk

NETWORK IT WEEK LABS

Reprint from IT Week 14th February 2005 www.itweek.co.uk © VNU Business Publications. All Rights Reserved.