Analyse this!

Dave Mitchell rounds up ten of the best software solutions for keeping track of your network traffic

Providing a reliable service to their users is a key function of network administrators. To be able to do this, they need to know not only what's happening on the network, but also how to identify problems and take an appropriate course of action based on that information.

Networks are no different to any other complex technology – when every component is functioning properly they work fine, but if anything goes wrong or they slow down, the reasons for these faults can be manifold. There's always a logical explanation but the biggest problem is finding the cause. With downtime a dirty word, administrators need to be able to spot a fault quickly, locate the source and rectify it with minimum impact on the service.

The network analyser is the weapon of choice for problem solving and troubleshooting, as it gives an in-depth view of what's happening on the network in real-time. Furthermore, these features are generally complemented by packet-capturing and decoding tools, allowing you to 'sniff' data from the network and view the contents of each captured packet. Unfortunately, one of the biggest drawbacks is the high cost of these products, leaving the average small or medium-sized business out in the cold. True, the majority of hardware solutions are aimed at the enterprise and come with ridiculously high price tags, but there are many alternatives that needn't break the bank. In this month's group test, we round up ten of the best software-only network-analysis solutions on the market, offering a wide range of features and prices to suit all pockets.

All the products on review can be installed on a reasonably specified Windows PC or server and will function with any network card that can operate in promiscuous mode. Basic features worth having are simple bandwidth-utilisation graphing, so you can see how your network is shaping up under pressure, and alerts to tell you the moment stress levels reach a certain point.

However, today's switched networks aren't so easy to monitor, as switches automatically segment the network into smaller collision domains to improve performance. This only allows the system with the analysis software installed to monitor and capture data from the same segment on which it's physically located. There are a number of solutions to this problem, as most products offer remote probes or agents that are installed on systems on other segments that pass data back to the central monitoring station.

This doesn't affect products that only monitor at the device level, as they all rely on SNMP (simple network management protocol) to provide this information. SNMP has been with us for a very long time, emerging in the mid-1980s and originally thought of as a 'quick fix' measure to provide inter-network management facilities while its replacement, CMIP (Common Management Information Protocol), was still undergoing development.

As its name implies, SNMP was designed to be as simple as possible. Information on various managed network devices is stored in a database called the MIB (management information base). It contains information, attributes and variables on each entity and, in a sense, represents a virtual network populated only by managed objects that have been declared. SNMP doesn't interact directly with each device but on the model that is stored in the MIB. To communicate with the MIB, an Agent also needs to be present on the managed device – on Windows systems, for example, you'd install the SNMP service. A MIB is stored locally and contains only information relevant to that device.

The method by which information is passed over the network is the use of PDUs (protocol data units) defined as Get Request, Get Next Request, Get Response, Set Request and Trap. The use of only five PDUs is a design feature that ensures SNMP doesn't become too complex by limiting what it can carry out. Furthermore, SNMP uses polling rather than interrupts to query the Agents on the managed devices.

A number of versions of SNMP are currently available, with the latest being version 3. This addresses many of the security issues surrounding previous versions, but few products, if any, actually support it. However, SNMP looks set to stay, as its supposed successor, CMIP, hasn't been taken up, mainly due to its complexity and its demands on system resources.

Along with network and device monitoring, there's a wide range of other features on offer from analysis software. Most run discovery scans on the network and create lists of all devices along with MAC to IP address and DNS resolution to make for easy identification. Some will even use this information to create maps. You'll want good alerting tools so that if a problem is identified, the software can alert you by a variety of methods such as email, pager or network message. Network trending will prove useful, as it allows historical data to be viewed to see how the network has been performing over a long period. Decent reporting tools will allow you to put this information into an easily understandable format when it's time to ask for a budget increase.

Either way, to be able to deal with the soup of protocols, platforms and applications in today's LAN, support staff will need to pick the right tool for the job and not end up with an expensive toy, so turn the page to see which product best suits your needs.

For details on how we tested, see www.pcpro.co.uk and click through to Labs.

> Administrators need to be able to spot a fault quickly, locate the source and rectify it with minimum impact on the service

Enterprise
PC PRO THE ESSENTIAL REAL-WORLD BUSINESS GUIDE

FEATURE TABLE







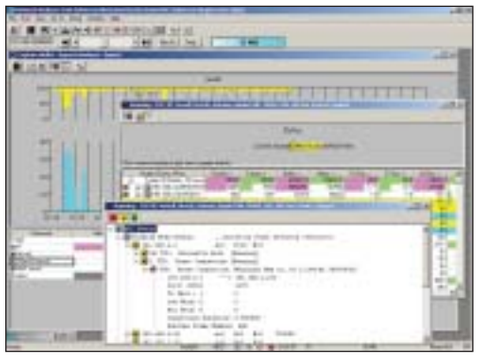

	Agilent Network Analyzer 2	Chevin TeVISTA Expert Lite 2.15	Distinct Network Monitor 4.11	eEye Iris Network Traffic Analyzer 4.06	Fluke Networks Network Inspector 5	Ipswitch WhatsUp Gold 8	Network Instruments Observer 8	Sniffer Portable LAN 4.7.5	SolarWinds.Net Engineer's Edition 5	SolarWinds.Net Orion Network Performance Monitor 6
Overall rating	★★★☆☆	★★★☆☆	★★★★☆	★★★★☆	★★☆☆☆	★★★☆☆	★★★★★	★★★☆☆	★★★★★	★★★★☆
Price (exc VAT)	£5,346	£5,500 (includes 2 SVAs)	£995 (includes 1 agent)	£680	£4,141 (250 nodes)	£530	£995	£12,775	£750	£1,342 (100 elements)
Contact	Phoenix Datacom 01296 397711	Chevin 01582 635030	Analyser Sales 0800 085 2181	eEye Digital Security 020 7470 5630	Fluke Networks 01923 281300	Unipalm 01582 635030	Network Instruments 01959 569880	Sniffer Technologies 01753 505858	Analyser Sales 0800 085 2181	Analyser Sales 0800 085 2181
Manufacturer's website	www.agilent.co.uk	www.chevin.com	www.network-monitor.com	www.eeye.com	www.flukenetworks.co.uk	www.ipswitch.com	www.networkinstruments.co.uk	www.sniffer.com	www.solarwindsuk.co.uk	www.solarwindsuk.co.uk
HOST PLATFORM SUPPORT										
Windows 95/98 SE/ME	✗/✓/✓	✓/✓/✓	✗/✓/✓	✗/✓/✓	✗/✓/✓	✗/✓/✓	✗/✓/✓	✗/✓/✓	✓/✓/✓	✗/✗/✗
Windows NT 4 WS/Server	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✗/✗
Windows 2000 Pro/Server	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓
Windows XP	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
Windows Server 2003	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
Others	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
PERFORMANCE MONITORING										
Real-time monitoring	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
GENERAL NETWORK UTILISATION										
Bar graph	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓
Line graph	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓
Dial	✗	✓	Pie chart	✗	✗	✗	✓	✓	✓	✓
Tables	✓	✓	✗	✗	✗	✗	✓	✓	✓	✓
Application monitoring	✗	✗	By port	✗	✗	✗	✗	✓	✗	✗
Utilisation by protocol	✓	✓	✓	✓	✗	✗	✓	✓	✗	✓
Connection statistics	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
Network map creation	✓	✓	✗	✗	Requires Microsoft Visio	✓	✗	✗	✗	✓
Top talkers	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓
Trend analysis	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓
MAC address resolution	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Switch/hub monitoring	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓
Remote probes	Optional	Agent	Agent	✗	Agent	✗	Optional	Optional	✗	✗
SNMP support	v1, v2	v1, v2	N/A	N/A	v1, v2	v1, v2	v1, v2	v1, v2	v1, v2	v1, v2
DIAGNOSTIC TOOLS										
Traffic generator	✓	✗	✗	✗	✗	✗	✓	✓	WAN only	✗
Trace route	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
Ping	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
DHCP monitoring	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗
DNS lookup	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Whois lookup	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗
Wake-on-LAN support	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗
TFTP server	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗
Packet capture	✓	✓	✓	✓	Optional	✗	✓	✓	✗	✗
Capture buffer max size	240MB	Disk file	Disk file	Disk file	N/A	N/A	(Total RAM-18MB) x 0.4	384MB	N/A	N/A
Record and playback	✓	✓	✓	✓	N/A	N/A	✓	✓	N/A	N/A
Protocol decoding	✓	✓	✓	✓	Optional	N/A	✓	✓	N/A	N/A
REPORTING										
Report tool availability	Optional	✓	✗	✓	✓	✓	✓	Optional	✓	✓
Report output formats	N/A	CSV (ping report), DOC, HTML	N/A	HTML	CSV, DOC, HTML, PDF, RPT, WKS, XLS	CSV, DOC, ODBC, PDF, RPT, TXT, WKS, XLS	CSV, TXT Web browser	CSV, HTML, TXT	CSV, HTML, PDF, XLS	CSV, HTML, PDF, TXT, XLS
ALERTING										
Email	Switch Advisor	Requires Exchange	✗	✗	✓	✓	✓	✓	✓	✓
Pager	✗	Via third party	✗	✗	✓	✓	✓	✓	✓	✓
Broadcast	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓
Audio	Switch Advisor	✓	✗	✗	✗	✓	✓	✓	✗	✗
Run program	Switch Advisor	✓	✗	✗	✗	✓	✓	✓	✗	✗
Other	✗	✗	✗	✗	✗	SMS	Save to disk	Save to disk	✗	✗
MIB SUPPORT										
Browser	✓	✓	✗	✗	✓	✗	✓	✗	✓	✗
Walker	✗	✗	✗	✗	✓	✗	✓	✗	✓	✗
Viewer	✓	✗	✗	✗	✓	✓	✓	✗	✓	✗
Set variables	✗	✗	✗	✗	✓	✗	✗	✗	Update System MIB	✗

Agilent Network Analyzer 2

PRICE £5,346 (exc VAT)
INTERNET www.agilent.co.uk SUPPLIER Phoenix Datacom 01296 397711
VERDICT **A highly sophisticated network-analysis and protocol-decoding product, but the price puts it beyond the reach of most small businesses.**

Agilent's Network Analyzer software is more commonly supplied as part of a complete solution including a customised hardware platform and LIMs (line interface modules), but it works just as happily on a standard PC.

Installation is swift and, although the main interface is tidy and easy to navigate, it only takes a few seconds to realise there's a wealth of tools underneath. A Wizard makes light work of the more basic tasks, providing quick access to tools for general network monitoring, viewing connected stations, bandwidth utilisation and network problems. An Expert Analyzer gives an overview of network activity, using a real-time bar graph to show health and utilisation, together with a breakdown of protocol activity below. Each protocol is accompanied by a detailed breakdown of errors or problems, and Network Analyzer provides sophisticated decoding tools.



You can easily see from here which stations are the most active. Just double-click on the display for each protocol and you'll be transported to a connection-statistics screen with details on discovered nodes and all their connections plus the protocols in use. All nodes may also be monitored from a single screen, and you can easily swap between viewing MAC, IP, Novell and AppleTalk nodes. A Switch Advisor allows you to monitor SNMP devices, view performance and generate basic alerts if problems on specific devices are detected.

A Commentator keeps an eye out for problems by performing real-time protocol analysis and displaying errors, warnings and alarms in a single screen. It also provides plenty of troubleshooting assistance, as each event is linked directly to online help files – selecting one takes you to the associated help screen.

Network Analyzer doesn't provide general network monitoring, so you can't set alerts to warn you in real-time if problems are detected. All data is captured into a local buffer, which can be set to a maximum capacity of 240MB. You're able to view the captured data using a set of recorder-style controls, modify frames and replay the data over the network.

Standard reporting tools are minimal and you'll need to factor in the extra cost of Agilent's Report Centre utility if you want to produce quality reports or export them into PDF format.

PC PRO RATINGS

EASE OF USE	★★★☆☆
FEATURES	★★★☆☆
VALUE FOR MONEY	★★☆☆☆
OVERALL	★★★☆☆

Chevin TeVISTA Expert Lite 2.15

PRICE £5,500 (exc VAT)
INTERNET www.chevin.com SUPPLIER Chevin 01582 635030
VERDICT **The network maps look dated, but TeVISTA provides good remote monitoring and comes with one of the best decoders on the market.**

A key feature of Chevin's TeVISTA analyser suite is the Software Visibility Agent (SVA), which can run on any Windows server or workstation and functions as a remote software probe. The information gathered is passed back to the central console and, as its hardware requirements are minimal, it can run on a low-specification PC, allowing you to place an agent on each segment of a switched network. TeVISTA Expert also integrates WildPackets' excellent EtherPeek NX software to provide a complete network-analysis package.

Prices across the suite vary considerably and depend on the components selected. The Expert Lite version on review targets smaller businesses and comes complete with the EtherPeek NX component and two SVAs, but this can't be upgraded or expanded so choose carefully. Installation of all components is dealt with swiftly, after which your first port of call will be the Enterprise Manager. This provides icons representing areas of the network and can be used to show, for example, departments, floors or complete buildings. Selecting one takes you to the Network Asset Manager, which scans a single IP address or a range and displays all detected devices. A Ping tool measures response times from all selected nodes and raises an alert if a threshold is breached, although this only extends to an audio alarm or running a program.

Those stations with SVAs installed are easy to spot and selecting one takes you to a real-time view of the network segment accompanied by a wealth of statistics on device and protocol utilisation. If that's not enough, a Troubleshooting tool will fill any gaps, providing in-depth details on network, node and protocol activity along with graphs revealing the most talkative stations on the network. Conversations between nodes can be monitored and packets between two devices captured via a single mouse-click. A range of filters may be applied to weed out extraneous data.

The decoding tools are second to none and provide in-depth views of packet contents for all seven OSI layers. As general statistics are saved into disk files, a lot of historical data can be gathered about your network. An offline feature allows you to view them using the Troubleshooting tool or export them into HTML or Word format reports.

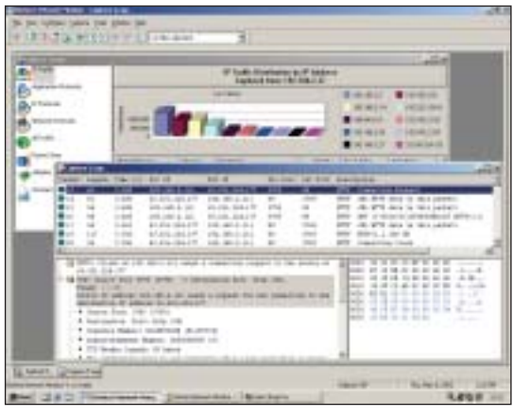
PC PRO RATINGS

EASE OF USE	★★★☆☆
FEATURES	★★★☆☆
VALUE FOR MONEY	★★★☆☆
OVERALL	★★★☆☆

Distinct Network Monitor 4.11

PRICE £995 (exc VAT)
INTERNET www.network-monitor.com SUPPLIER Analyser Sales 0800 085 2181
VERDICT **Good packet-decoding features and clear explanations of their contents make this a useful tool for troubleshooting a wide range of network problems.**

Distinct's Network Monitor (NM) takes a similar tack to eEye's Iris, as it aims to capture packets and cut through the jargon by decoding them into an understandable format. However, the similarities end here, as NM doesn't attempt to reconstruct the data into its original form – a feat that Iris does extremely well. Whereas Iris is more suited to security applications, NM aims to provide support departments with the tools to quickly pinpoint network errors.



Two modes are on offer for capturing statistics and packets and both can be activated at the same time or run separately. Statistics are on a par with Iris, as NM provides details on all or just IP traffic for the network segment on which it's loaded. Remote agents are used to monitor other segments and you get one agent included in the base price. The agent is accessed from the NM console and capture procedures are the same as for the local system, although you can't amalgamate data from different segments. Other monitoring options are viewing the top talkers on the network, protocol distribution and application activity. The latter is only shown by port number, but selecting an entry will show the IP pairs involved.

The packet-capture window is divided into three sections, with all captured packets displayed in the main window. Selecting one shows the decoded results below with the hexadecimal format to the right. NM offers a number of useful features to help cut through the morass of data by colour coding packets belonging to the same connection and offering to display packets related to a single connection.

You can also apply extensive filters to the capture process to weed out data for, say, specific ports or IP or MAC addresses. Custom filters may be applied to restrict this even further, right down to conversations between two stations and even specific packet fields. NM provides a wealth of information about each packet and displays each protocol in order. For example, an HTTP packet will show this protocol first, followed by TCP, IP and Ethernet and each is accompanied by in-depth explanations. It's worth noting that NM can be used to troubleshoot a variety of network connections, including wireless and PPP serial connections.

PC PRO RATINGS

EASE OF USE	★★★★☆☆
FEATURES	★★★☆☆☆
VALUE FOR MONEY	★★★★☆☆
OVERALL	★★★★☆☆

eEye Iris Network Traffic Analyzer 4.06

PRICE £680 (exc VAT)
INTERNET www.eeye.com SUPPLIER eEye Digital Security 020 7470 5630
VERDICT **Basic network-monitoring features but the fearsome packet-analysis functions offer decoding tools that provide an incredible amount of information.**

While Iris provides basic network-monitoring features, its primary function is as a packet-capture and decoding tool, and it simply excels at these tasks. One of Iris' key functions is its ability to decode packets and display them in plain language. eEye proudly claims it can reconstruct email messages and attachments and display them in their original format. Not only that, but it can reconstruct web pages being visited during the capture phase and simulate cookies to get into password-protected websites.

During testing, we found these claims to be absolutely correct, although it was slightly unnerving to see test emails being displayed in Iris' Decode window exactly as they were sent or received, and even seeing email account usernames and passwords being caught and displayed in plain English. This is a product that would make a network administrator's blood run cold if it fell into the wrong hands.

You can run packet capture continuously, start a session manually or schedule it for specific times of the day. The data is copied to a disk file so the only limit is the size of your hard disk; a range of filters can remove unwanted data. The capture screen is well designed, with each packet broken down into its various parts in one window, while a Packet Editor shows them in hexadecimal format and allows each one to be edited. A packet list above reveals details such as source and destination MAC and IP addresses, and packets can be selected and sent back onto the network.

The Decode window is where the fun starts. This lists each host and all associated traffic broken down into services and port numbers. Selecting one shows the relevant sessions alongside and the window below this reveals associated data. For a website, click on the Go button and Iris will take you to the site the user was viewing at the time. Choose POP3 and all incoming email will be displayed and if unencrypted will be in exactly the format in which it was sent. Selecting the Envelope icon will fire up the appropriate mail client (if installed on your system) where you can view the entire message and even open any file attachments.

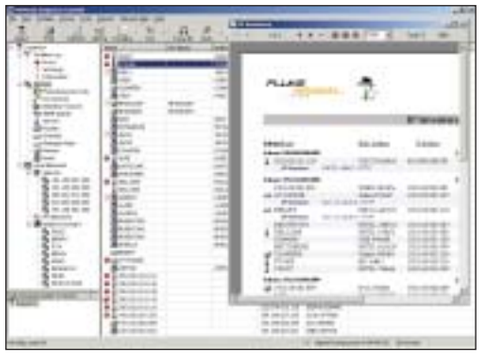
PC PRO RATINGS

EASE OF USE	★★★★★☆
FEATURES	★★★☆☆☆
VALUE FOR MONEY	★★★★★☆
OVERALL	★★★★☆☆

Fluke Networks Network Inspector 5

PRICE 250 nodes, £4,141 (exc VAT)
INTERNET www.flukenetworks.co.uk SUPPLIER Fluke Networks 01923 281300
VERDICT **A simple tool for monitoring network devices, with good alerting features, although the number of optional extras increases the price substantially.**

Network Inspector is designed with switched Ethernet networks very much in mind. The product comes with agents that can be installed on other remote systems, allowing data to be gathered from the far corners of your network. The software automatically discovers all devices on the network and is able to monitor them in real-time at the interface or port level. Event notification is particularly good, as you can set up multiple thresholds for areas such as device availability or interface utilisation and tie these in to alerting facilities via email or pager.



However, you won't get tools for monitoring general network utilisation, as the software is designed to work in tandem with other Fluke Networks products that provide these facilities. Packet capture and protocol decoding aren't on the menu either, as these tools are provided by Fluke's OptiView Protocol Expert, which adds £2,397 to the price.

Installation takes only a few minutes and includes loading a local agent, after which you can place agents on other remote systems. These maintain their own database of discovered devices locally and can manage monitoring and alerting tasks as well.

Once you've selected the network interface to be used for monitoring, Network Inspector gets on with the job of node discovery and populating its database. A mapping facility is on offer, but this increases the asking price even further, as it requires access to Microsoft's Visio. A tidy Explorer-style tree is used to display all nodes for easy selection and the main pane next-door reveals all hostnames with their IP and MAC addresses, plus NetBIOS and IPX names if applicable. Devices are automatically placed into groups for easier management, so you can easily swap between different subnets, NetBIOS domains or IPX networks and swiftly reveal those nodes that are identified as servers, switches or routers. Other groups such as nodes running SNMP agents and printers are included, but you can't create custom groups.

Selecting a node brings up its individual properties, which includes an overview of the system and a list of running services where appropriate. A display of detected problems uses three colour-coded icons for easy identification of errors, warnings and information, while a Trending tool is provided for switch monitoring.

PC PRO RATINGS

EASE OF USE	★★★☆☆☆
FEATURES	★★☆☆☆☆
VALUE FOR MONEY	★★☆☆☆☆
OVERALL	★★☆☆☆☆

Ipswitch WhatsUp Gold 8

PRICE £530 (exc VAT)
INTERNET www.ipswitch.com SUPPLIER Unipalm 01638 569600
VERDICT **A simple package for monitoring network devices. It may not be as sophisticated as Fluke's alternative, but it costs a lot less.**

Ipswitch's WhatsUp Gold looks to offer a similar set of features to Fluke's Network Inspector, but with one big difference. It aims to provide a wide range of network-mapping plus device-monitoring and alerting features at a substantially lower price. Neither product provides bandwidth utilisation and monitoring tools so you can't use them to view general network performance.

WhatsUp Gold kicks off by scanning your chosen IP subnet and builds a map populated with all discovered devices. A variety of discovery methods are available, but the easiest option is SmartScan, which queries SNMP information and also creates maps to reflect the network's hierarchy. The map doesn't provide as much detail as that of Network Inspector's Explorer-style view, although you can edit it to reflect geographical locations, buildings and offices.

While WhatsUp is in Monitor mode, all devices are polled at regular intervals and colour-coded icons swiftly reveal devices that fail to respond or are in trouble. Notification options are extensive. You can create different configurations and apply them to specific devices and then use a wide variety of alert transports including email, pager or voice messaging.

From a device's properties, it's possible to set up individual polling frequencies and link these to dependencies on other devices. From the Services tab, you select the services you want to monitor. These can include all common TCP/IP varieties such as HTTP, FTP or POP3 and you may add custom services and port numbers. If a device or service fails to respond, its icon changes shape and colour to reflect the severity of the event. A Quick Status option swiftly reveals the nature of the problem and also offers basic graphs of polling failures and a simple log file. Selecting the Status tab at the bottom of the map shows all devices and services, but this has to be the ugliest screen we've yet seen.

Reporting is good, as you can create graphs showing device response performance over hours, days or weeks and these may be exported to a wide range of formats. Ipswitch also provides a web server, so WhatsUp Gold can be accessed remotely from a browser. The Net Tools menu item is useful too, as it provides a handful of diagnostics tools for IP networks.

PC PRO RATINGS

EASE OF USE	★★★★☆☆
FEATURES	★★☆☆☆☆
VALUE FOR MONEY	★★★★☆☆
OVERALL	★★★☆☆☆

Wireless analysis

Secure your wireless network

Wireless networks are rarely out of the news and all too often for the wrong reasons, as security is their biggest weakness. If your company relies heavily on this form of communications, you need to close all your security holes and take control. Here, we round up three of the top wireless analysers to help you do just that. Both Fluke Networks and Sniffer Technologies have taken mobility to the extreme with their respective iPAQ-based solutions, while AirMagnet delivers Pocket PC and laptop versions.

Costing £2,836 for the software, Sniffer's Wireless PDA claimed to be the first wireless network analyser for a handheld device. Running on Microsoft Pocket PC 2002, Wireless PDA is simple to use. From the RT (real-time) menu, you can view a table showing general network activity or switch to a Dashboard view which is similar to that offered by the Portable LAN software (*see p186*).

The AP option displays all access points within range along with details on the ESSID, channel, encryption status, supported transfer rates and signal strength, while a table below reveals more detail about frame types. A host table provides general details on all access points and mobile units, and you can channel surf to locate more access points.


Sniffer's Wireless PDA.

To collect data, simply select the Capture option in the RT menu bar, tell it when to stop and save the data to a local file. The PC (post-capture) menu then becomes available, allowing you to analyse the capture buffer at your leisure. From here, you can view general statistics, a host table, protocol distribution charts or select a Matrix view that displays the top talkers in tabular or graphical format.

An Expert mode analyses captured data, builds a database of all devices it sees and warns you if it spots any potential problems. A useful feature is the option to create triggers so that packet capture will start and stop automatically if certain thresholds are breached or error conditions are spotted.

Coming in at £3,890, Fluke Networks' WaveRunner differs from Sniffer in that it's Linux based and supplied as a complete package. It's also very intuitive and allows you to scan for wireless APs and associated clients, check on bandwidth utilisation, run link tests and view all channel activity. If you spot a suspect access point, you can home in on it by using a signal-strength graph and an audible tracer that gets faster as you close in. Extensive traffic details are provided and can be filtered by channel or device, and you're able to keep an eye on the top ten talkers.


Fluke's WaveRunner.

WaveRunner can create detailed reports on SSID and AP lists, traffic summaries and site surveys, and these can be output to CSV or HTML format and even emailed to other users. However, while WaveRunner excels with its focus on security, it doesn't offer packet-capture and decoding tools, so if the latter is a higher priority Sniffer's Expert mode has more appeal and looks better overall value.

If you're happy to take the extra weight of a laptop, AirMagnet looks a top choice, as it offers a fine range of features. Costing £2,494 for the review version, it compares well on price and also comes complete with a Cisco AiroNet 352 wireless PC Card and proprietary drivers. The interface is well designed and offers seven main screens, with the Start option revealing all APs within range, a signal-level graph for all channels and a graph of frame types. The Channel screen gives a highly detailed breakdown of throughput, signal strength, alerts and utilisation by wireless speed, and you can swap easily between channels. Individual APs can be monitored more closely from the Infrastructure tab and security gets plenty of attention with AirWise, which detects rogue APs, unauthorised clients and DoS attacks on wireless networks.

AirMagnet also provides clear explanations of each detected security alert and advice on how to close the holes. Although not as sophisticated as the tools provided with Wireless PDA, it offers packet capture and decoding. Trace files can be saved and replayed as though live, and you're able to limit the capture process to individual wireless channels. Lastly, AirMagnet proves a bunch of diagnostics tools including traceroute, whois, a traffic generator for the link between the AirMagnet system and selected AP, and a handy site-survey tool.

With any of these products to hand, there's no excuse for running a wireless network with compromised security. The biggest variation is with packet-capture and decoding tools, but mobility is naturally a key feature. All these products can provide a wealth of information about utilisation, performance and errors, but, more importantly, identify and help plug any security holes.


AirMagnet offers a lot of information in its Start screen.

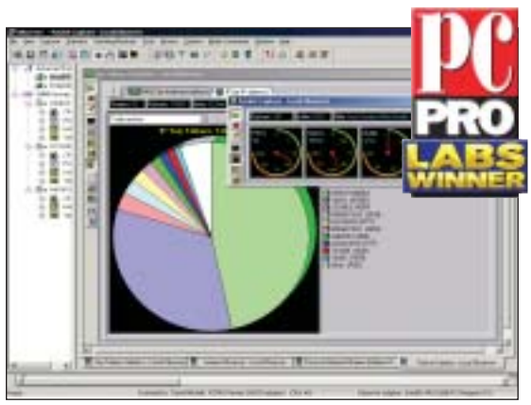
CONTACTS

SNIFFER WIRELESS PDA
Sniffer Technologies, 01753 505850
FLUKE NETWORKS WAVERUNNER
Fluke Networks, 01923 281300
AIRMAGNET
Global Secure Systems, 0870 458 1113

Network Instruments Observer 8

PRICE £995 (exc VAT)
INTERNET www.networkinstruments.co.uk SUPPLIER Network Instruments 01959 569880
VERDICT **Network Instruments is a long-time player in this market and it shows. Observer offers an unbeatable array of tools at a very tempting price.**

Introduced nearly ten years ago, Observer was one of the first software-only, network-analysis products and bucked the trend as its sensible price tag made it affordable to smaller businesses. The latter still holds true today, but the features on offer are now even more impressive. Even the basic Observer product on review delivers a full network-analysis toolbox that rivals many of the more costly alternatives.



The clear documentation sets a fine example and Observer is very intuitive, so you can start gathering information straight away. It's able to pull in data from the local-network segment, but also uses a unique feature called looping. This allows it to mirror traffic for a specific period of time from one port on manageable switches to the local port, so it can report on other network segments without using a remote probe. For more in-depth analysis, you're able to use optional RMON probes that install on a PC on the remote segment.

A panel to the left keeps a tally of local and remote probes, and you can add other SNMP and RMON devices such as switches and access them directly for utilisation data.

Monitoring tools are extensive and each loads a window in the pane opposite along with a row of controls down one side. You can quickly discover network nodes, resolve their IP addresses and start packet capture on specific systems directly from this interface. It's possible to apply custom filters to refine the information, and the buffer contents may be saved to disk for future use. For the price, Observer's decoding tools are impressive, as they provide views of raw packets and their decodes plus all protocols and summaries.

Observer lets you check on real-time bandwidth utilisation and protocol distribution, keep an eye on errors and who's generating them. There are plenty of other useful tools too, including a Web Observer that graphs Port 80 activity on up to eight web servers; a basic traffic generator for stress testing your network; and a trending mode, which allows you to capture data over a specific period or continuously. The information gathered can be viewed in graphical or tabular format and it may also be presented in a smart web browser report.

PC PRO RATINGS

EASE OF USE	★★★★★☆
FEATURES	★★★★★☆
VALUE FOR MONEY	★★★★★★
OVERALL	★★★★★☆

Sniffer Portable LAN 4.7.5

PRICE £12,775 (exc VAT)
INTERNET www.sniffer.com SUPPLIER Sniffer Technologies 01753 505858
VERDICT **Very expensive, but Sniffer offers the most comprehensive range of network-analysis, diagnostics and decoding tools and is ideally suited to larger networks.**

Part of the Network Associates empire, Sniffer Technologies has consistently offered some of the most sophisticated network-analysis solutions. As the price suggests, the Portable LAN software targets larger networks and offers an unbeatable range of tools for analysing traffic across Ethernet, Fast Ethernet, Gigabit, Token Ring and FDDI topologies.

Installation is relatively painless. The software opens with a smart dashboard providing three gauges revealing utilisation, packets per second and errors. Beneath this are line graphs for packet-size distribution, errors and general network activity, and these views can be customised. There are plenty of monitoring options – a host table displays all active stations plus the top ten talkers, the Matrix offers a variety of charts showing traffic spreads between nodes, while protocol distribution and global statistics on frame-size distribution can be viewed in graph or chart format.

As you'd expect, packet-capture tools are impressive and the Sniffer Expert analyses and decodes data in real-time. Extraneous data may be removed by applying filters, event-based triggers can be used to automatically start a packet-capture session and data from specific stations may be collected simply by selecting them from a host table listing. The ART (application response tool) could prove useful – it tracks response times for services such as HTTP. It also monitors application-layer connections between clients and servers, and links to response thresholds are used to warn you if a network service is performing poorly.

Monitor alarms can run continuously and provide warnings of problems such as excessive network utilisation. Expert alarms only function while data capture is active, but are able to provide more insight into detected problems. If a threshold is exceeded, it logs this as a symptom, but if a group of events occurs or multiple thresholds are breached Sniffer classes this as a diagnosis that requires immediate attention.

Expert alarms may be assigned one of five severity levels and Sniffer can reach you by email or pager if it spots a problem on the network. Reporting is basic – you're able to export data from the monitoring tools into CSV, PRN and TXT formats, but only the Expert can export data into HTML format. If you want more from your reports, you'll need the optional Sniffer Reporter utility.

PC PRO RATINGS

EASE OF USE	★★★☆☆☆
FEATURES	★★★★★☆
VALUE FOR MONEY	★★☆☆☆☆
OVERALL	★★★☆☆☆

SolarWinds.Net Engineer's Edition 5

PRICE £750 (exc VAT)
INTERNET www.solarwindsuk.co.uk SUPPLIER Analyser Sales 0800 085 2181
VERDICT **A huge range of tools for your money, all well integrated together and an absolute bargain as a general analysis solution.**

SolarWinds.Net offers a wide range of network-analysis software solutions and the Engineer's Edition on review looks, at first glance, to do just about everything except make the tea. More than just a collection of disparate products, it offers a comprehensive toolbox of utilities tied together neatly under one roof and accessible from a single floating menu bar.

Nine categories of analysis tools are provided, although note that packet capture and protocol decoding aren't part of the SolarWind's equation. Network discovery is at the top of the list where you can scan a single device, a subnet or IP address range and view a list of devices and their SNMP attributes. Ping and SNMP sonar sweeps build up lists of discovered systems from specific address ranges, MAC addresses can be resolved and you're able to see which devices are attached to each port on your managed Layer 2/3 switches. Address management finds out what IP addresses are being used on a subnet, DNS Audit provides forward and reverse domain name resolution, and a basic scope monitor keeps a tally on used and available addresses on your DHCP servers.

Extensive network-performance monitoring tools are provided, allowing you to keep a close eye on interface performance, utilisation, latency, errors and throughput in bar, chart, line graph or dial format and create baselines. Extensive alerting is also provided so you can create lists of monitored devices and request a range of warnings to be sent if, for example, a node goes down, utilisation is excessive or an interface is shut down. CPU loads on individual SNMP switches, routers and servers may be viewed, while SNMP graphing lets you browse and select MIBs on specific devices from which you want to gather information.

A useful bunch of utilities is provided for Cisco-centric networks and a TFTP server is included for downloading or uploading IOS configuration files and for comparing running and saved versions. A traffic generator is provided, but this is designed only to test WAN connections. Security checks are also on the menu, with tools that let you run brute force attacks on routers and switches to check on CLI password strength, while SolarWinds can attempt to break into Cisco products using a password database.

PC PRO RATINGS

EASE OF USE	★★★★☆☆
FEATURES	★★★★★☆
VALUE FOR MONEY	★★★★★★
OVERALL	★★★★★☆

SolarWinds.Net Orion Network Performance Monitor 6

PRICE 100 elements, £1,342 (exc VAT)
INTERNET www.solarwindsuk.co.uk SUPPLIER Analyser Sales 0800 085 2181
VERDICT **Good network mapping and device-discovery tools, but the icing on the cake is the excellent web-server-based remote monitoring features.**

SolarWinds.Net gets a second bite of the cherry in this group test with its Orion Network Performance Monitor (NPM) that differs radically from the Engineer's Edition. Instead of being a toolbox of various different utilities, it aims to provide a complete network-management solution and augments it with remote web browser access. System requirements are stricter, as it requires access to SQL Server and comes with Microsoft's 2000 Desktop Engine, which supports databases up to 2GB in size.

Installation is dealt with efficiently. NPM runs a configuration utility that sets up the database, creates the website and ensures all services are started correctly. Your next move is to run a discovery utility that scans the subnets you enter. Discovered devices will be automatically imported into the selected database. The price of the version on review includes support for 100 elements.

A System Manager takes you to a performance monitor tool. This is the same as that supplied with the Engineer's Edition but with one big difference – all nodes are already imported so you don't have to add them manually. There's plenty of information available on each device and their interfaces, you can view multiple graphs and keep an eye on events in a separate colour-coded list. Maps may be created to represent different areas of the network and you're able to use your own custom graphics. These are populated by dropping the device and interface icons into the appropriate position where different colour codes provide an at-a-glance status report.

NPM hits the spot with its web-server tools, as these are easily the best in this group test. The home page provides a complete list of all devices along with an event summary plus devices with high utilisation or CPU loads. It uses flashing icons to alert you to potential problems on a device. The view is fully customisable and you can import your previously created map, after which the icons become hotspots for swift access to the selected system. Access security is impressive, as you can create accounts that limit remote users to viewing groups based on areas such as nodes, machine type, manufacturer or location and even limit them to accessing one system.

PC PRO RATINGS

EASE OF USE	★★★★☆☆
FEATURES	★★★★☆☆
VALUE FOR MONEY	★★★★☆☆
OVERALL	★★★★☆☆