FLUKE networks

OptiView® Series III

Network Analyzers

The more your network changes, the more you need to improve network vision and control.

Today's networks are typically very stable. The problem is they aren't static. Management and users are constantly demanding new technologies, new services, and better performance, which inevitably require changing infrastructure, deploying new applications, and dealing with security. And in the process you need to control IT costs and minimize disruption to your organization. That means you need to be able to clearly see all aspects of your network to accurately assess the impact of adding new technologies and services and to make sure it is delivering maximum performance with what you already have.

It's not easy.

But the powerful new Fluke Networks OptiView Series III Network Analyzers are available in two form factors to give you a clear view of your entire enterprise – providing visibility into every piece of hardware, every application, and every connection on your network. Chose the Integrated Network Analyzer for portable all-in-one analysis or the Workgroup Analyzer for permanent or semi-permanent deployment in the core or remote sites – both offer vision and capabilities to help you:

- Deploy new technologies and applications
- Manage and validate infrastructure changes
- Solve network and application performance issues
- Secure network from internal threats

They show you where your network stands today and help you accurately assess its readiness for the changes you need to make.

OptiView Series III new release features:

- Application Troubleshooting Expert Option validates network services, application connectivity and provides detailed application flow analysis
- IPv6 Analysis Option provides a complete inventory of IPv6 networks and devices, applications using IPv6, router advertisements and tunneling protocols
- Wireless LAN Infrastructure Analysis Option identifies Wireless LAN Controllers, Lightweight AP's, Intelligent AP's and wireless clients - from the wired side of the network
- Wireless Network Analysis Option now supports 802.11n

Assess, verify and prove network readiness for new applications, new technologies and infrastructure deployment

Conduct network discovery, traffic analysis, infrastructure device analysis and documentation. Deploy, secure and troubleshoot wireless LANs.

Validate new configurations and end-user performance

Identify VLAN configurations; validate network health, audit switch/router configurations and performance. Response time analysis of key business applications from source to end-user perspective.

Secure the network from the inside

Maintain network integrity by discovering unauthorized devices and misuse of network equipment. Perform routine audits to identify regulatory compliance violations (HIPPA, SOX) and detect downloading or sharing of restricted documents and confidential information through advanced packet capture and filtering on specific words or text strings. Verify 802.1x configurations, SNMP community strings and MAC level port security.

Improve utilization of existing network equipment

Eliminate unwanted applications through deeper traffic analysis, differentiating between specific audio, video, image or data applications.

Reduce MTTR and minimize network outages and degradations

Resolve network performance issues in real-time using vendor independent infrastructure analysis, sophisticated packet capture, decode with Expert analysis and free string match.

Improve IT staff efficiency

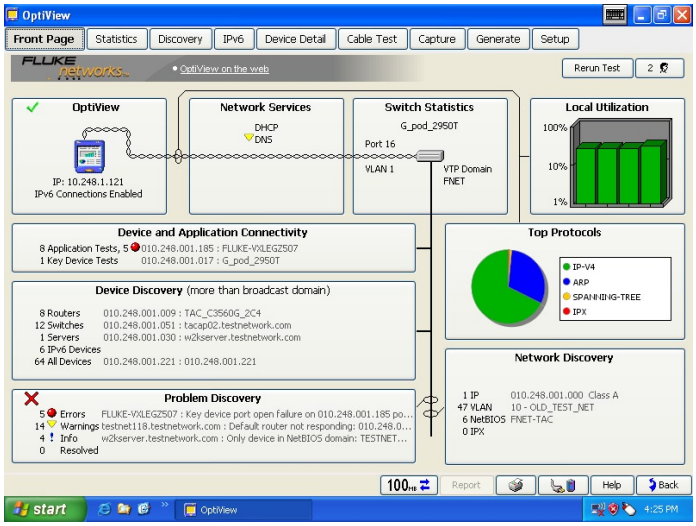
Allow IT staff to efficiently locate any device within the enterprise network, and understand a user's or application's bandwidth utilization in real time.

Traffic analysis at the touch of a button

The OptiView Series III provides real-time statistics for traffic on the wire which enables the user to understand how network resources are being used and increase user satisfaction with faster response times for networked applications.

Quickly and easily identify top talkers, multicasters and broadcasters or select top conversations to determine which hosts may be over utilizing resource bandwidth. Determine who is using server bandwidth by viewing top conversations to a single host.

Analyze protocol mix to identify top protocols being used and also discover unwanted and custom protocols and see which protocols are being used by each host.



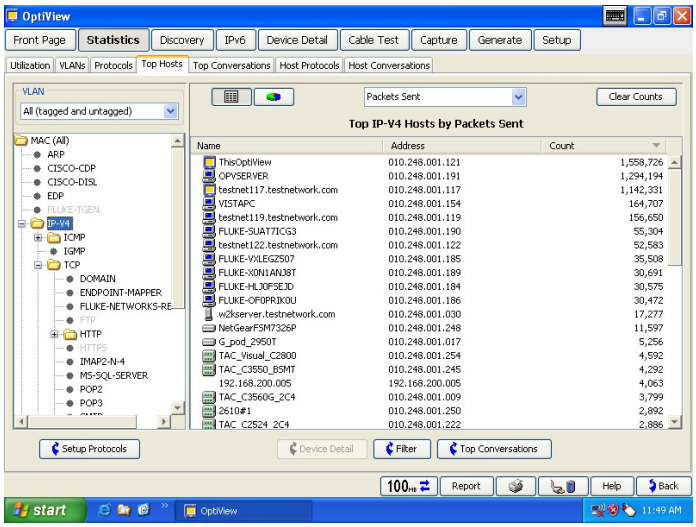
Front page

Application traffic analysis

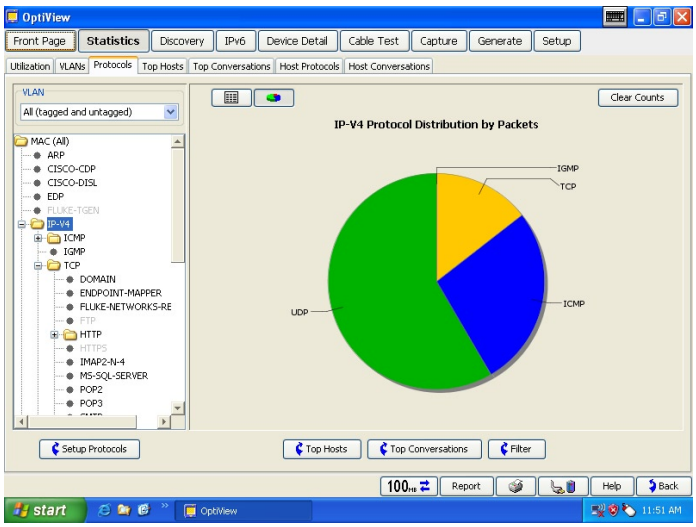
Automatically discover all protocols and sub protocols from the MAC layer to the application layer. This enables IT staff to identify applications utilizing link bandwidth including those that use dynamically assigned port numbers to see and validate the impact of applications on bandwidth usage and also identify to use of illicit applications.

Perform application analysis in real-time on Gigabit links and determine the specific endpoints (server, host) using that application. Plus, perform a layer 3 or layer 2 trace route to identify the switch or router interface to which the endpoint is connected for each application. Differentiate between specific audio, video, image, and data applications, and show the level of bandwidth usage of each, including:

- **HTTP traffic to: database, application, audio, image, text, video, x-world (VRML)**
- **HTTP applications to 58 applications: such as Lotus® Notes, Microsoft® Word, RealAudio®, Adobe®, Liquid Audio, etc.**
- **RealNetworks® RDT into audio, video, data**
- **RTSP into embedded media and session control**
- **VoIP**
  - RTP video and audio and sub-classification on whether set-up through H.323, SIP, RTSP, Skinny
  - VoIP call signaling and call control for H.323, SIP, and Cisco Skinny
  - H.323 VoIP and video conferencing
- **SAP R/3 classified into service manager, app server, and gateway**
- **Oracle®**
  - Connection Manager & Connection Manager Gateway
  - Oracle VP
- **Oracle TNS**
  - MS ODBC & OLE
  - Oracle SQL Plus & Oracle Forms
  - PeopleSoft
- **Instant Messenger (AOL and MSN)**
- **KaZaA® Downloads**



Top hosts



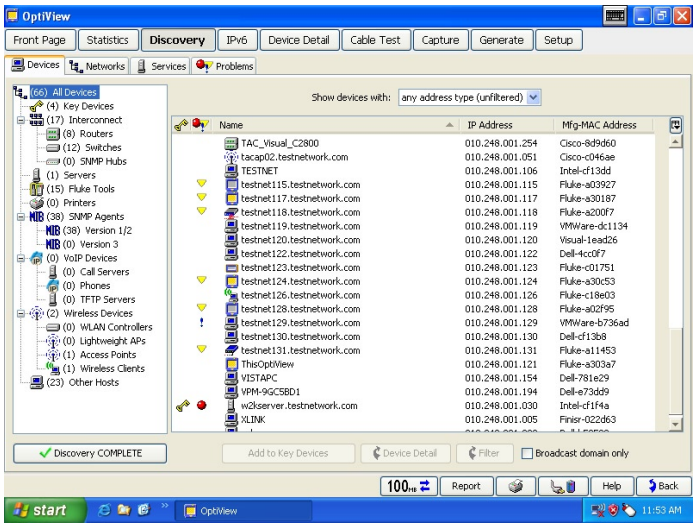
Protocol mix

Advanced discovery techniques finds devices, networks and problems in seconds.

As soon as the analyzer is connected to the network, it automatically begins to discover devices on the network, with no interaction required, by monitoring traffic and actively querying hosts. IT staff can immediately see what is on the network and where it is connected, by switch, slot and port number. They can investigate and quickly locate “suspect” devices and with minimum effort identify problems associated with device mis-configurations.

The analyzer categorizes devices into interconnect (routers, switches, SNMP hubs and access points), servers, printers, SNMP agents and other hosts. Additionally, networks are classified by IPv4 and IPv6 Subnets, VLANs, NetBIOS Domains and IPX Networks, together with host membership within each classification. Network devices that may be experiencing problems are also discovered. Examples of problems detected are: duplicate IP addresses, incorrect subnet masks, default router not responding and many more.

The analyzer can also be configured to perform a discovery on an off-broadcast domain subnet to provide visibility of devices at remote sites. Generate up-to-date HTML format inventory reports of devices both on the attached network and also on networks at remote sites.



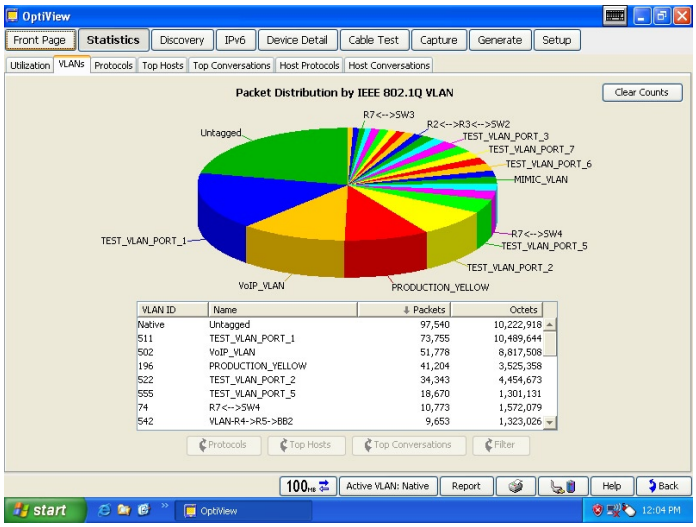
Device discovery

VoIP Device Discovery

The analyzers active discovery has been extended to discover VoIP devices including call managers and IP phones from Cisco, Nortel, Avaya and Mitel. Device capabilities and configurations may be viewed, allowing the user to easily identify and correct configuration issues during VoIP deployment.

VLAN Trunk Analysis

When connected to a switch trunk port, the analyzer will detect all VLANs available on that trunk, measure the traffic distribution across all the VLANs and provides the user with the capability of selecting a specific VLAN. If an individual VLAN is selected, device discovery, traffic statistics and packet capture data will only be displayed for that VLAN.



VLAN statistics

Vendor independent infrastructure device analysis

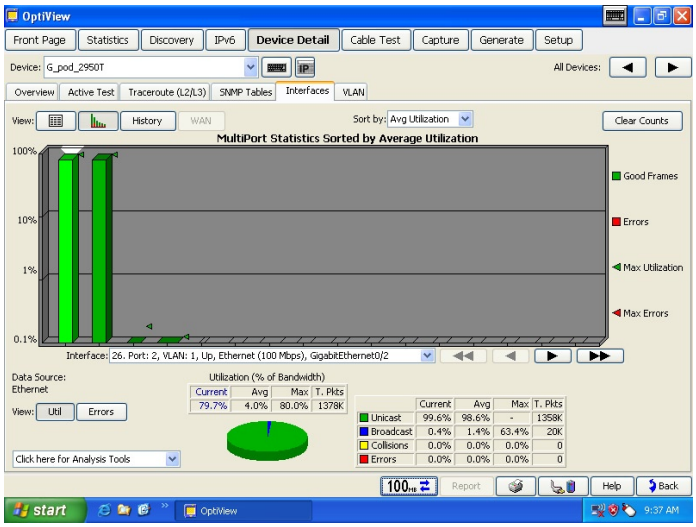
Get visibility into switches and routers located anywhere on the enterprise network. With this information, you can optimize network performance, improve efficiency and reduce costs while improving reliability and security. Easily manage and validate infrastructure configurations when deploying SNMPv3 with the analyzers capability of supporting configurable credential sets including authentication with and without privacy.

Multi-port switch statistics

In-depth analysis, including:

- A tabular view of all switch port configurations, including the identity of each host and where it is connected to the switch for both layer 2 and 3.
- A graphical view of utilization and error rates on each switch port to see over subscribed or errored ports at a glance.

Detect over-utilization, excessive errors, and locate inactive switch ports to determine if performance problems are related to link speed or duplex mis-configurations, or are related to the number of hosts on a port.

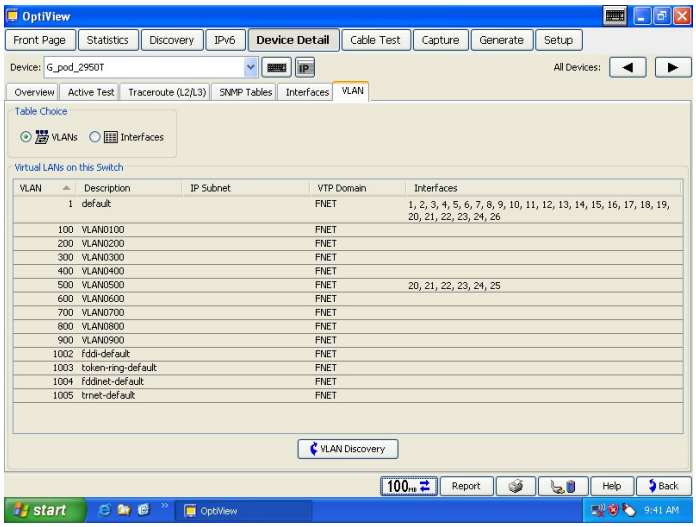


Multi-port statistics

VLAN analysis

Determine if connectivity problems are related to VLAN configuration by seeing information such as:

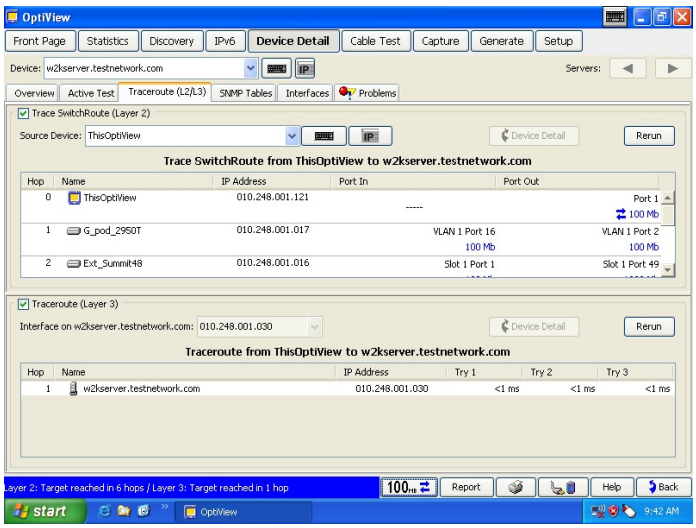
- VLANs that are configured on the switch.
- Interfaces that are members of each VLAN.
- Identification of trunk or uplink ports, together with the trunking protocol in use.
- Identification of which hosts are members of each VLAN.



VLAN discovery

Trace SwitchRoute™

Trace SwitchRoute allows you to see the exact path two devices use to communicate through your switch fabric. Trace SwitchRoute begins its discovery from the specified Source Device and traces the path to the specified Target Device. For each switch in the path, the displayed results include the DNS name and IP address, the inter- switch connections by port number, together with link speed and VLAN information. Highlighting any device in the Trace SwitchRoute name column and selecting Host Detail allows you to view that device's network configuration information.



Trace SwitchRoute

Router and WAN link analysis

In-depth device analysis identifies Router ARP cache or routing table errors and also provides visibility to manage and troubleshoot costly WAN links. See WAN link configuration, a graphical display of utilization and error rates and identification of specific error types on ISDN, Frame Relay, T1/E1, T3 and ATM links.

Telnet and web browser links to allow reconfiguration of devices directly from the analyzer.

Traffic generation and throughput

Assess network readiness for new deployments by determining the impact of the new application, or the addition of network users, by stressing your network with simulated traffic – up to 1 Gbps.

Protocol type, frame size, frame rate, percentage utilization and number of frames to transmit are user configurable, along with the type of traffic: Broadcast, Multicast or Unicast.

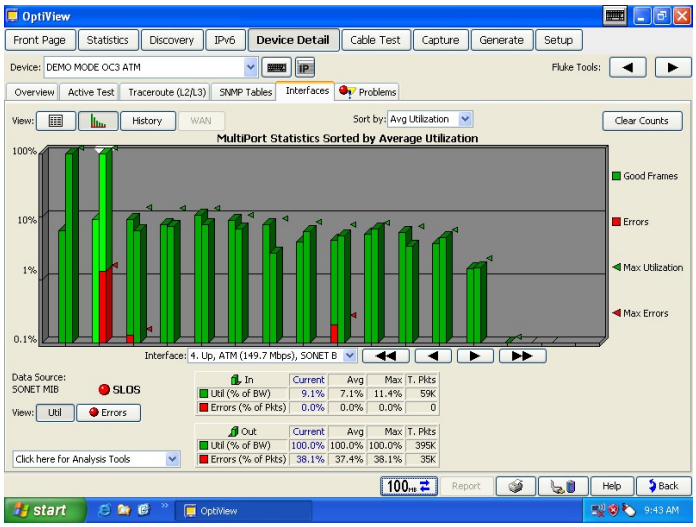
Selectable protocols include: Benign Ethernet, Benign LLC 802.2, NetBEUI, Benign IP, IP ICMP Echo, IP UDP Echo, IP UDP Discard, IP UDP NFS and IP UDP NetBIOS. Selecting an IP protocol allows you to select Time to Live (TTL) parameters and TOS (QOS) parameters such as Minimum Delay, Maximum Throughput, Maximum Reliability, Minimum Monetary Cost and Maximum Security to ensure correct routing configurations.

The throughput test will, measure bidirectional data flow between two Fluke Networks devices to validate LAN and WAN throughput capabilities. The throughput test requires a second device to communicate with on your network. That second device can either be an OptiView Integrated or Workgroup Analyzer, or an EtherScope™ or OneTouch™ Network Assistant, or LinkRunner Pro Reflector.

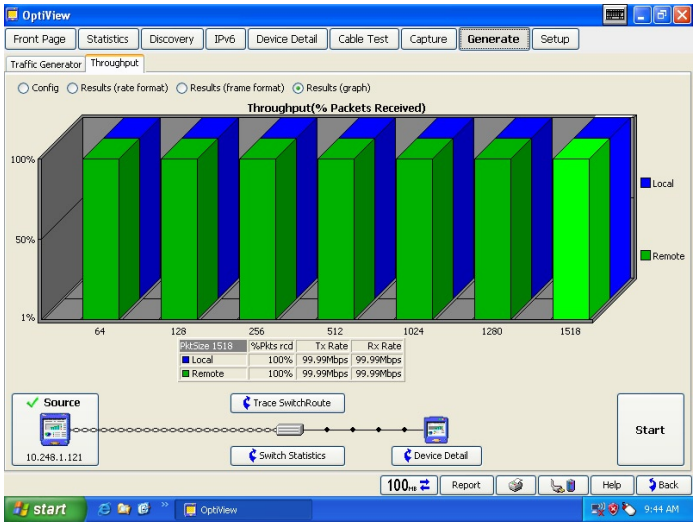
The Throughput Option allows you to configure the following parameters:

- Data speed (up to 1 G bps) – maximum rate is determined by the link speed and duplex.
- Frame size – choose from seven different frame sizes or select sweep to run the test on all seven frame sizes.
- Content – select payload for all 1s, all 0s, alternating 1s and 0s or random.
- Test duration can be 2 seconds to 18 hours.

Test results can be viewed in a tabular or graphical format. The Rate format tabular view indicates the local and remote transmit and receive rates together with the total percentage of frames received by both devices. Switching to tabular Frame Format view shows the number of local and remote frames transmitted and received, together with the total percentage of frames received by both devices.



WAN interface statistics



Throughput results

Port based network access control (802.1X)

To speed deployment of IEEE 802.1X, the OptiView Series III is capable of performing a full 802.1x transaction with an authentication server to ensure correct credentials are being deployed. The analyzer supports 802.1X authentication through most common EAP (Extensible Authentication Protocol) types, 15 in total, allows import of software certificates and can store multiple authentication profiles to allow connectivity to different broadcast domains or networks with multiple authentication servers for deployment, validation and troubleshooting. A connection log for detailed 802.1X protocol exchange analysis is also generated.

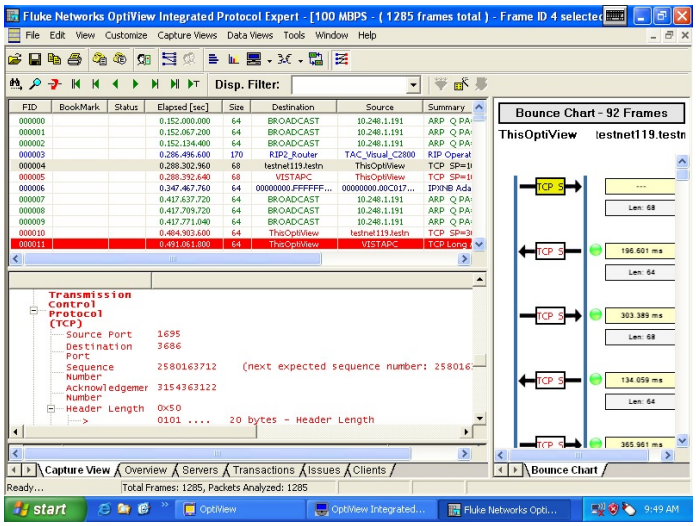
Packet capture and decode

Get Gigabit line rate packet capture and filtering to troubleshoot problems where packet level analysis is required and perform advanced troubleshooting when deploying new applications.

Sophisticated capture filters allow collection of more relevant data and limit the amount of traffic to analyze by filtering on individual addresses or conversation, address range for IPV4, IPv4 subnet, IPv6 prefix and protocols.

The capture process may be started or stopped through a user defined trigger event – capture the traffic before, after or around an event occurrence without being present. This ensures you capture the event the first time and avoids initiating random traffic captures that may not contain anything of interest.

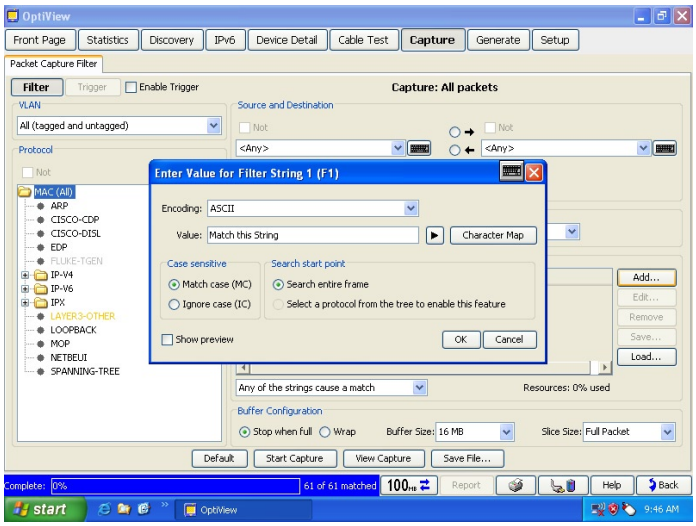
With the captured traffic, launch the OptiView Integrated Protocol Expert to examine packet level decodes and detail in combination with a graphical representation of individual conversation threads. Captured data will automatically be sorted into conversations and displayed by the timeline as an Application Bounce Chart to make application performance and troubleshooting easier to visualize and resolve. For more detailed application performance analysis, add the Application Troubleshooting Expert option.*



Packet decode with application bounce chart display

Free String Match to find and capture anything

Match any set of words or phrases when detected (regardless of the position in the packet – payload or header) in real-time to trigger the analyzer to start or stop capturing and/or filter traffic. Use free string match to capture traffic around any application error message, detect traffic containing certain words or phrases in non-encrypted emails, web pages, file transfers or documents to identify illicit use of the network or detect downloading of restricted documents based on content or filenames (.doc, .xls, .pdf). Additionally, use free string match to identify and track applications that are not allowed on the network such as streaming media that may consume valuable bandwidth, or P2P traffic that may pose a security risk. A total of eight sets of triggers or filters can be defined to trigger a capture unattended for later analysis, allowing analysis when you have time, not when the event occurred.



Free String Match setup

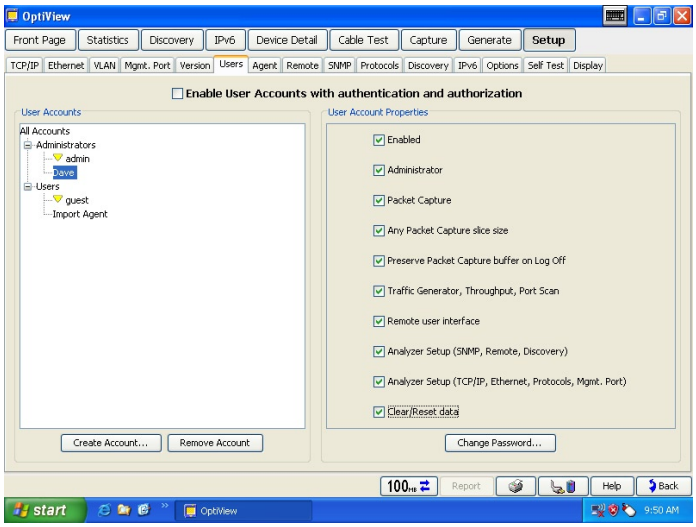
Reporting/documenting

While viewing the statistics, discovery or detail screens, pressing the Reports key will generate HTML reports on Protocols, Top Hosts, Top Conversations, Devices, Networks, Problems and many more. These reports are saved and may be viewed locally or remotely using a web browser. For advanced documentation, add OptiView Reporter and automatically import the OptiView Analyzer data for reporting, trending and event notification. OptiView Reporter's integration with Microsoft Office Visio diagramming program allows you to create network maps showing the links between your servers, switches, routers and hosts.

* ***Note:*** *The OptiView Protocol Expert (OPV-PE/PRO) is required to be installed on the controlling PC of an OptiView Workgroup analyzer in order to decode captured traffic.*

Remote user interface

Simply point a web browser at the IP address of a correctly configured OptiView Series III Integrated Network Analyzer to retrieve saved reports and capture files. You can also install a Remote User Interface (UI) and use your PC to obtain remote access to an analyzer over a TCP/IP connection. Once the Remote UI is installed, simply give the interface the IP address of the analyzer to monitor and see an almost identical interface to the analyzer's local interface. Communications between the analyzer and Remote UI can also be encrypted. A single integrated analyzer will support seven remote sessions (eight sessions on the Workgroup analyzer) for collaborative troubleshooting or opening of multiple sessions on a PC to provide a remote dashboard view. Additionally, use the analyzers management port to configure and monitor for out of band management independently of the network under test port.



User accounts

User accounts

Through the user accounts screen, you can add and modify analyzer security information for each individual analyzer user, which prevents unauthorized use of certain analyzer features for easier compliance with regulatory requirements. Features that can be disabled include packet capture and decode, traffic generation, remote user interface and analyzer configuration.

Context sensitive help

Help is contextually linked to each screen in the analyzer. While that help screen is displayed, you may select other information from the table of contents, choose an index entry, or perform a full text search on any help topic or term.

Integrated Network Analyzer removable hard drive option for classified environments

See what's happening on your classified network by simply connecting one single tool that ensures any sensitive data stored on your network analyzer's hard drive never leaves that environment.

Fluke Networks OptiView Series III Integrated Network Analyzer with removable hard disk drive is a new approach to classified environment network analysis that provides you with the Network SuperVision you need for all seven layers, along with the speed and simplicity your organization demands. Network information discovered by the OptiView Series III Integrated Network Analyzer can be stored on the removable hard drive which allows the analyzer to be moved from classified environments of different levels and between classified and unclassified systems by simply replacing the hard drive.

Optional removable hard drive

OptiView® Application Troubleshooting Expert Option

The OptiView Application Troubleshooting Expert speeds up troubleshooting application and network performance issues by automatically validating that network services such as DHCP, DNS and 802.1X are available and operating correctly, ensuring that server and application connectivity is accessible by opening specific TCP IPv4 and IPv6 ports on servers and reporting the round trip time as a combination of network latency and server connection set up time. A combination of layer 2 and layer 3 trace routes identifies the entire network path between the application client and the application server. Server resource utilization may also be viewed.

When analyzing captured packets collected by the OptiView analyzer, the Application Troubleshooting Expert provides detailed application flow analysis for various protocols such as DNS, DHCP, HTTP, HTTPS, SMTP and SMB and presents information such as:

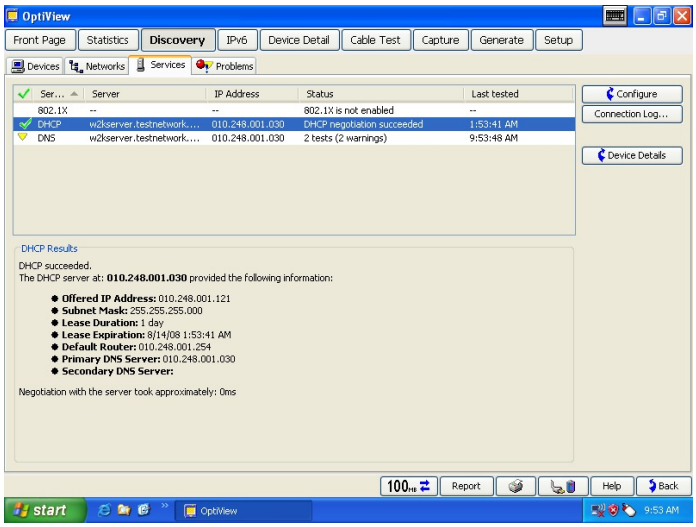
- an overview of the protocols on the trace
- aggregate throughput for individual applications over time
- a list of servers and clients by protocol
- detailed transactions for each application layer protocol including a list of individual commands
- application turns
- throughput for each application transaction including payload vs. header data
- server response time from client request to first data sent by server
- connection setup time
- any issues detected during the application session

A bounce chart also shows at-a-glance information for connection setup times, connection setup packets, error packets and transport layer packets.

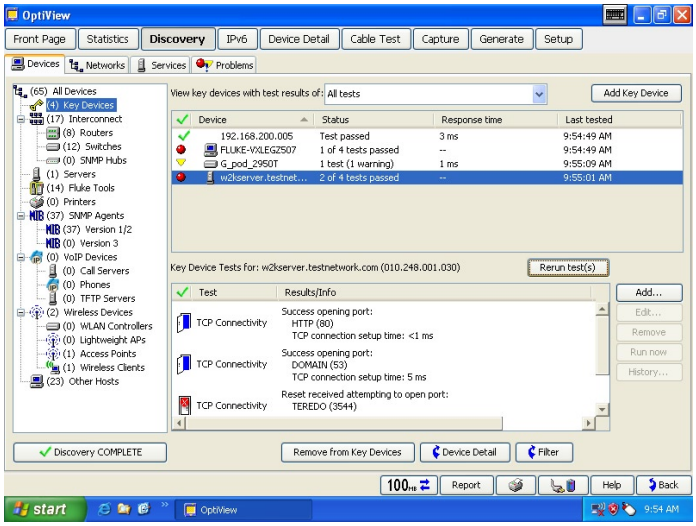
For Network related performance problems, the expert will categorize the problems detected by OSI layers. It summarizes the address or name of the stations involved, and the position of frames in the capture file that trigger the Expert System to identify the problem. The Expert System will identify symptoms such as Excessive ARP, Excessive BOOTP, NFS Retransmission, TCP/IP checksum error,

TCP/IP Fast Retransmission, TCP/IP Retransmission, TCP/IP Frozen Window, TCP/IP Long Ack and TCP/IP SYN Attack and many others. Double clicking on the Expert Symptom button displays the Expert Diagnosis window that provides a description of the station symptom, a probable cause and recommended action(s).*

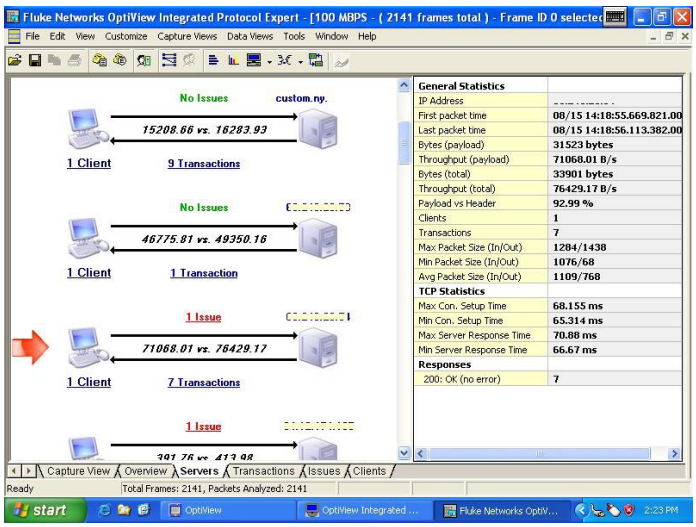
* ***Note:*** *The network services and application connectivity tests are enabled on the OptiView Workgroup analyzer. For post capture application analysis, the OptiView Protocol Expert (OPV-PE/PRO) is required to be installed on the controlling PC of an OptiView Workgroup analyzer in order to decode captured traffic.*



Application Troubleshooting Expert Services



Application Troubleshooting Expert Active Tests



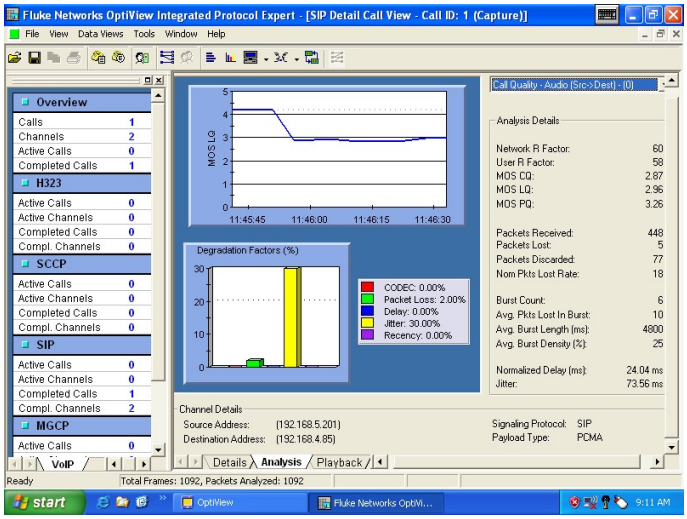
Expert analysis

OptiView® Voice over IP Option

Voice over IP is one of the most mission critical applications being deployed by IT organizations today. The rollout of VoIP services is accompanied by the expectation of toll availability and sound quality. It is therefore imperative IT organizations have the proper tools to monitor VoIP call QoS during and after implementation. OptiView Integrated Network Analyzer with the VoIP option can process a capture file and use advanced algorithms to grade the voice quality being delivered. QoS assessments are generated for each call without the need to perform detailed decoding.

"Quality Grading" thresholds can be set for key VoIP QoS parameters, such as R-Factor, Jitter, Packet Drop and Call Setup Time. The number of calls that fall within each Quality Grade is shown for key QoS parameters. Detailed VoIP call information for every call is clearly shown in a tabular view to allow quick identification of the route taken and the gateway involved, allowing you to troubleshoot quickly. As networks evolve and traffic patterns change with new applications and users, VoIP QoS can often degrade in imperceptible steps, or extreme failure. An initial VoIP deployment might run fine initially, but incremental changes to the network can slowly erode VoIP performance or completely eliminate availability. OptiView ensures visibility of VoIP performance and allows quick resolution of issues due to network growth and development.

The VoIP option provides detailed decodes of the most commonly used VoIP protocols including H.323, Cisco Skinny (SCCP), MGCP and SIP. Detailed information supports quick isolation of call setup problems. Combined with the easy-to-use single call filter and Call and Channel Table Views, call setup failures commonly caused by configuration errors, network equipment incompatibilities, or interoperability can be easily solved.



VoIP call quality

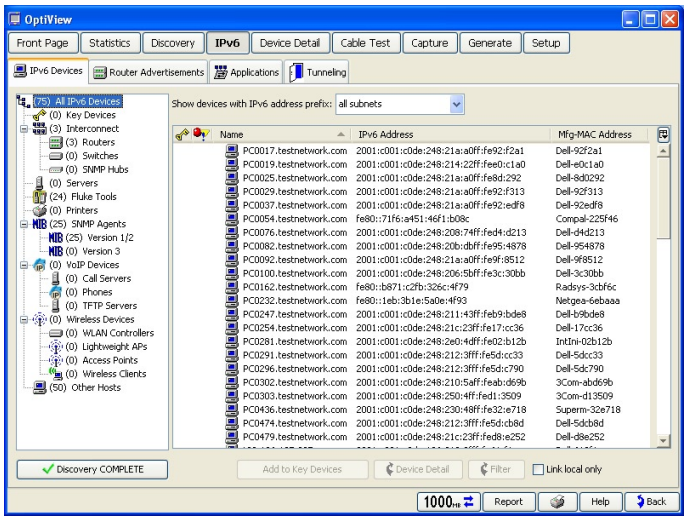
The Voice over IP Option helps you ensure Quality of Service (QoS) for this mission-critical application. And, by measuring call quality at different locations on the network, IT staff can isolate network segments that need reconfiguration or upgrading.

OptiView® IPv6 Analysis Option

The analyzer will discover and display complete IPv6 network and device inventory including routers, switches, wireless AP's, DHCP6 servers and hosts. It enables you to identify active IPv6 devices in the network and those that may have problems in single-stack IPv6 networks. Router Advertisements are analyzed and the analyzer displays information gathered from routers (by subnet) such as the router name, auto configuration, MTU, preferred lifetime, valid lifetime, network name, subnet, local prefix, on link, and user-defined name.

Easily identify applications that may be communicating using both IPv4 and IPv6 protocols. In a dual stack network, IPv4 and IPv6 can be running at the same time but if the network becomes pure IPv6, the application my not continue to run.

Detect devices using tunneling mechanisms and identify the tunnels in use. Undetected or unauthorized tunneling could represent a serious security risk.

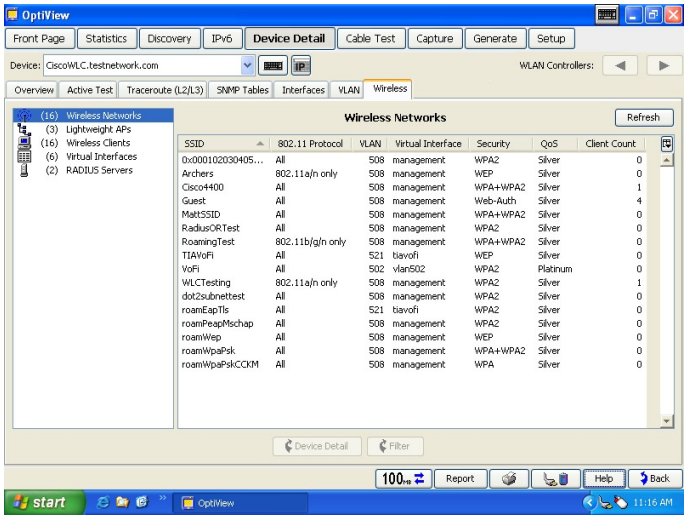


IPv6 Devices

OptiView® Wireless LAN Infrastructure Analysis Option

The analyzer now discovers and categorizes Wireless LAN controllers, Lightweight access points, Intelligent access points and wireless clients. The Wireless LAN Infrastructure Analysis Option provides detailed device information for Cisco Wireless LAN controllers controllers including the wireless network associated with the controller together with the SSID, security and QoS parameters, the lightweight APs being controlled and the 802.11 protocol in use.

Detailed device information provided for Cisco LWAP's include the Wireless networks associated with the AP together with the SSID, security and QoS parameters, the 802.11 protocol in use and the client count. Additional information is available for each wireless client including the name, IP and MAC address, the 802.11 protocol used, RSSI (Receive Signal Strength Indicator) and SNR (Signal to Noise Ratio) and the client status.



Wireless Network Analyzer

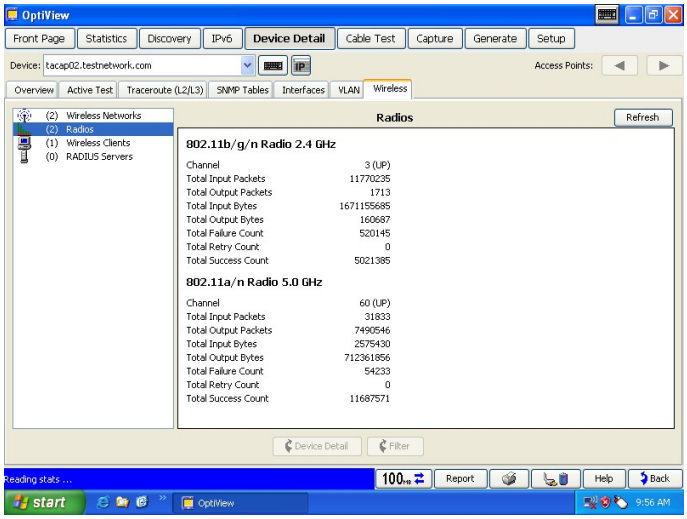
OptiView® Wireless Option

Fluke Networks gives you the visibility you need to manage both your 802.11 a/b/g/n wireless and 10/100/1000 Ethernet copper and fiber wired networks. By extending the award-winning OptiView Integrated Network Analyzer with Wi-Fi detection, verification and troubleshooting, Fluke Networks again ensures that OptiView is the network visibility tool of choice.

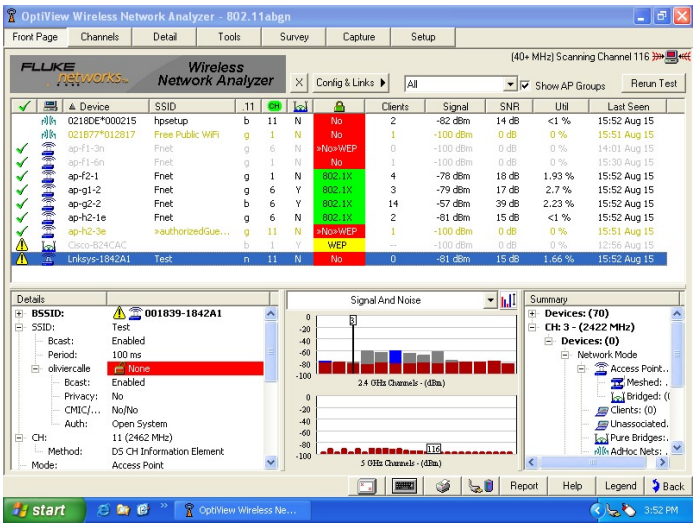
With the OptiView wireless option, get total visibility into your network. It's a solution that brings value to key wireless network tasks such as:

- Discovery of wireless access points and clients.
- Detection and location of rogue APs.
- Active client based connectivity testing.
- Channel monitoring.
- Packet capture and decode for complete analysis of 802.11 a/b/g/n WLAN's.

In addition, load Fluke Networks' powerful wireless stand-alone software on the analyzer such as InterpretAir™ WLAN Survey Software for site survey analysis to quickly optimize coverage and performance, or AnalyzeAir™ Wi-Fi Spectrum Analyzer to detect, identify and locate RF emitting devices that interfere with 802.11 and cause intermittent performance problems.



Wireless LAN Infastructure



Wireless Network Discovery

OptiView® Fiber Inspector Option

Dirt, dust and other contaminants are the enemy of high-speed data transmission over optical fiber. With today's network applications requiring more bandwidth and loss budgets being tighter than ever before, it is imperative that all optical connections are clean and free of contaminants to ensure network operation. Fluke Networks' OptiView Series III Integrated Network Analyzer, together with the OptiView Fiber Inspector Option, is the solution.

The OptiView Fiber Inspector Option, a portable video microscope that connects to a USB port on an OptiView Series III Integrated Network Analyzer, gives you superior vision by enabling you to inspect all types of installed fiber terminations in hardware devices and patch panels. It saves you time by eliminating the need to access the rear of patch panels or disassemble hardware devices prior to inspection. Instead of removing each individual fiber, you need only insert the video probe to inspect the fiber while it's still in place.

The OptiView Fiber Inspector:

- Easily inspects fiber connectors already installed on patch panels.
- Quickly determines whether fiber connectors on a hardware device are clean and in good condition – without disassembling the device!
- Eliminates the hazards of inspecting live fiber.
- Is compatible with standard ST, SC, and FC connectors, and other connector types including small form factor connectors with optional adapter tips.
- Leverages the investment already made in the OptiView Series III Integrated Network Analyzer by eliminating the need for a separate display.

Vision Suites

The Vision Suites turn the OptiView Series III Network Analyzers into a complete solution of visionary network management products that work with the Integrated Network Analyzer to monitor, analyze and troubleshoot, giving you control of every situation that pops up. You get enterprise-wide vision with the power to drill down seven layers deep.

You can identify problems through the application layer with OptiView™ Protocol Expert. It can analyze capture files from the OptiView analyzer for full seven-layer decodes with expert analysis. Advanced filtering and triggering let you find offending packets. And, OptiView™ Reporter software together with your hardware agents allows trending of user defined ports in your switched network. Or, set it up to collect data from your analyzer. With a single click, you can generate network connection diagrams with our unique link to Microsoft® Office Visio® software. And if a key device, router, or switch port is overloaded, you'll know about it in a heartbeat.

Our Network SuperVision Gold Support

plans give you exclusive services and 24/7 technical assistance. Sign up for our Gold Support plan and you'll enjoy outstanding privileges to protect and add value to your investment in Fluke Networks equipment. They include unlimited technical assistance seven days a week, 24 hours a day via phone or at our web site support center. Repairs on covered items and "next day" dispatched loaner units for uninterrupted service. Free software upgrades. Scheduled annual performance verification service. Web based training. Access to our extensive Knowledge Base library of operation and application related technical articles. And Gold "Members Only" special prices and promotions. Some benefits are not available in all countries. See **www.flukenetworks.com/goldsupport** for more information.

Product Comparison

Model	OptiView Series III Integrated Network Analyzer	OptiView Series III Workgroup Analyzer
General		
Operating System	Microsoft® Windows Vista® Business (including a downgrade right to Microsoft® Windows® XP Professional) VxWorks for Network Measurements	Remote UI PC Dependant VxWorks for Network Measurements
Display	800 x 600 pixels, active color panel, CCFT backlight and bezel, touch pad	None; Requires remote user interface installed on a PC
Hard Drive	Included	
USB Ports	3	0
PCMCIA	1	0
SVGA Output	1	0
Power	Battery or AC	AC Only
Network Connections		
RJ-45	RJ-45 10/100/1000BASE-T Ethernet	RJ-45 10/100/1000BASE-T Ethernet
1000BASE-SX	SFP	SFP
1000BASE-LX, ZX	Option (SFP)	Option (SFP)
802.11a/b/g/n Wireless	Option	Not available
Traffic Analysis	•	•
Discovery	•	•
Device Detail	•	•
Application Troubleshooting		
Network Services test	Option	•
TCP Port Connectivity	Option	•
Port open response time	Option	•
Post Capture application diagnostics	Option	Requires DSVS suite or OptiView Protocol Expert (OPV-PE/PRO)
IPv6 Analysis	Option	Option
Wireless LAN Infrastructure Analysis	Option	Option
Utilities		
OptiView Browser	•	From controlling PC
Telnet/SSL	•	From controlling PC
Web Browser	•	From controlling PC
FTP	•	From controlling PC
MIB Browser	•	From controlling PC
Packet Capture and Decode		
Capture	•	•
Decode	•	Requires DSVS suite or OptiView Protocol Expert (OPV-PE/PRO)
Free String Match Trigger and Filter	•	•
Capture Buffer Size	480MB	480MB
VoIP Analysis	Option - OPVS2-VOIP	Option - OPV-PE/VOIP
Traffic Generation	•	•
Setup/Other	•	•
Remote control sessions	7	8
Cable Test		
Opens/shorts etc	•	•
Length	•	•
Fiber Microscope (OPV-FT500)	Option	Not available

Models, Options and Accessories

	OptiView Series III Integrated Network Analyzer
Model	**Description**
OPVS3-GIG	OptiView Series III Integrated Network Analyzer Gigabit (1000BASE-SX)
OPVS3-GIG/W	OptiView Series III Integrated Network Analyzer with Wireless (802.11 a/b/g/n) Option
OPVS3-GIG/S	OptiView Series III Integrated Network Analyzer Gigabit with Wireless (802.11 a/b/g/n), VoIP Analysis and Application Troubleshooting Expert Options
OPVS3-GIG/RHD	OptiView Series III Integrated Network Analyzer Gigabit with Removable Hard Drive
OPVS3-GIG/PSVS	Professional Vision Suite with OptiView Series III Integrated Network Analyzer Gigabit
OPVS3-GIG/RHD/PSVS	Professional Vision Suite with OptiView Series III Integrated Network Analyzer Gigabit with Removable Hard Drive
OPVS3-GIG/PSVS/W	Professional Vision Suite with OptiView Series III Integrated Network Analyzer and Wireless (802.11 a/b/g/n) Option
OPVS3-GIG/PSVS/S	Professional Vision Suite with OptiView Series III Integrated Network Analyzer with Wireless and VoIP Analysis and Application Troubleshooting Expert Analysis Options and AnalyzeAir Wi-Fi Spectrum Analyzer
OPVS3-GIG/PSVS/C	Professional Vision Suite with OptiView Series III Integrated Network Analyzer with Wireless (802.11 a/b/g/n), Cisco WLAN Infrastructure Analysis, VoIP Analysis and Application Troubleshooting Expert Analysis Options and AnalyzeAir Wi-Fi Spectrum Analyzer
	OptiView Series III Workgroup Analyzer
Model	**Description**
OPVS3-WGA/GIG	OptiView Series III Workgroup Analyzer Gigabit (1000BASE-SX)
OPVS3-WGA/GIG/DSVS	Distributed Vision Suite with OptiView Series III Workgroup Analyzer Gigabit
	Options and Accessories for INA and WGA
Model	**Description**
OPVS3-WLIA	OptiView Cisco Wireless LAN Infrastructure Analysis Option
OPVS3-IPV6	OptiView IPv6 Analysis Option
OPV-RPTR	OptiView Reporter
OPV-RPTR/PRO	OptiView Reporter (40 Devices)
LRPRO-REFLCT	LinkRunner™ Pro Reflector
OPV-SFP-SX	850nm, 50 and 62.5 micron multi mode fiber. 1000BASE-SX SFP adapter
OPV-SFP-LX	1300 nm, 10 micron single mode fiber. 1000BASE-LX SFP adapter
OPV-SFP-LX10	1310 nm, 10 micron single mode fiber. 1000BASE-LX SFP adapter
OPV-SFP-ZX	1550 nm fiber. 1000BASE-ZX SFP adapter
OPV-SFP-100FX	100BASE-FX SFP adapter
NF430	Fiber Optic Cleaning Kit
	Options and Accessories for INA only
Model	**Description**
OPVS3-ATE	Application Troubleshooting Expert Option
OPVS2-VOIP	VoIP Analysis Option
OPV-WNA3	OptiView Wireless Analysis Option 802.11 a/b/g
OPV-WNA4	OptiView Wireless Analysis Option 802.11 a/b/g/n
OPV-WNA4/C	OptiView Wireless Analysis Option 802.11 a/b/g/n and Cisco WLAN Infrastructure Analysis Option
INTAIR-LAP	InterpretAir WLAN Site Survey Software
ANALYZEAIR	AnalyzeAir Wi-Fi Spectrum Analyzer
IA-AA	Wireless Software Suite includes: InterpretAir WLAN Site Survey Software and AnalyzeAir Wi-Fi Spectrum Analyzer
OPVS3-WLESS	Wireless Suite includes: OptiView Wireless Analysis Option 802.11 a/b/g/n, InterpretAir WLAN Site Survey Software and AnalyzeAir Wi-Fi Spectrum Analyzer
OPVS3-WLESS/C	Wireless Suite includes: OptiView Wireless Analysis Option 802.11 a/b/g/n, Cisco WLAN Infrastructure Analysis Option, InterpretAir WLAN Site Survey Software and AnalyzeAir Wi-Fi Spectrum Analyzer
OPVS2-KB	Mini Keyboard (USB)
OPVS2-BP	External Battery Pack
OPVS3-RHD	Removable Hard Drive for OPVS3-GIG/RHD

Models, Options and Accessories continued

OPVS3-RHD/4	Pack of four Removable Hard Drives for OPVS3-GIG/RHD
OPV-FT600	OptiView Fiber Inspector
OPV-HCASE	Hard Carrying Case
	Accessories for WGA only
Model	**Description**
OPV-TCASE	Hard shell transit case
OPV-RMK	Rack Mount Kit for one or two Workgroup Analyzers

Specifications

	Integrated Network Analyzer	Workgroup Analyzer
General Specifications		
Weight	Without external battery 2.2 kilograms (5.0 lbs) With external battery 3.0 kilograms (6.6 lbs)	1.63 kilograms (3.6 lbs)
Dimensions	26.0 x 23.4 x 6.4 centimeters (10.3 x 9.2 x 2.5 inches)	4.1 x 21.1 x 32.8 cm (1.6 x 8.3 x 12.9 in), one half of a standard 19 in rack mount width
Display	LCD touch screen, 800 x 600 pixels, active color panel, CCFT back-light and bezel, touch pad	Not applicable
LED Indicators	16 (21 with external battery)	6
Power		
Battery	Internal battery Lithium Ion 11.1 V DC (nominal), 2 Ah External battery Lithium Ion 11.1 V DC (nominal), 6 Ah	Not applicable
AC	External AC adapter/battery charger AC input: 120 V – 240 V, 50/60 Hz, 1.5 A DC output: 15 V, 4.0 A	AC input 85 to 265 VAC; 47/63 Hz; 25 watts
Ports		
Communication and accessory ports	3 USB, 1 PC Card type II, 1 VGA out 15-pin connector	Serial Configuration Port RS-232 (9-pin male)
Network analysis ports	RJ-45 10/100/1000BASE-T Ethernet, fiber 100/1000BASE-X SFP GBIC	
Management port	10/100/1000BASE-T (RJ-45) Ethernet	
Network Standards		
LAN Interfaces	IEEE 10BASE-T, IEEE 100BASE-TX, IEEE 100BASE-FX, IEEE 1000BASE-X	
Standard SNMP MIBs Used	RFCs: 1213, 1231, 1239, 1285, 1493, 1512, 1513, 1643, 1757, 2021, 2108, 2115, 2127, 2495, 2515, 2558	
Media		
Cable Types	Unshielded Twisted Pair LAN cables (100 and 120 Ohm UTP category 3, 4, 5, 5E, and 6 ISO/IEC Class C and D); Foil-screened Twisted Pair cables (100 and 120 Ohm ScTP category 3, 4, 5, and 6 ISO/IEC Class C and D)	
Cable Length 1	1 to 153 m (3 ft to 500 ft) +/- 2 m (6 ft)	
Environmental and Safety		
Operating Temperature	10°C to 30°C (50°F to 86°F) with up to 95% Relative Humidity 10°C to 40°C (50°F to 104°F) with up to 75% Relative Humidity	
Non-Operating Temperature	-40°C to +71°C (-40°F to +159.8°F)	-20°C to +60°C (-4°F to +140°F)
Approvals		
Shock and vibration	Meets requirements of MIL-PRF-28800F for Class 3 equipment	
Laser	Class 1 Laser Product, complies with 21 CFR 1040.10 & 1040.11, CFR(J), and EN60825-1:1994/A1:1997/A2:2002	
Safety	Complies with CAN/CSA-C22.2 NO. 60950-1 Canadian Standards, and UL 60950-1 (U.S. standards) (CE) Complies with EN60950	

Note: All PSVS Suites include OPVS3-ATE Application Troubleshooting Expert, OPV-RPTR/PRO OptiViewReporter Pro and OPV-PE/PRO Protocol Expert Pro.
All DSVS Suites include OPV-RPTR/PRO OptiView Reporter Pro and OPV-PE/PRO Protocol Expert Pro.

NETWORKSUPERVISION

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to **www.flukenetworks.com/contact**.

Printed in U.S.A. 9/2008 1590227 D-ENG-N Rev 0