



# OptiView™ Series III

## Integrated Network Analyzer

**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 Integrated Network Analyzer gives you a clear view of your entire enterprise – providing visibility into every piece of hardware, every application, and every connection on your network. No other portable tool offers this much vision and all-in-one capability to help you:

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

*It shows you where your network stands today and helps you accurately assess its readiness for the changes you need to make.*



### OptiView Series III new release features:

- 802.1x authentication
- Gigabit line rate capture, traffic generation and Internetwork Throughput
- Free string match filtering and triggers
- Encapsulation independent protocol filtering
- Triggering to control capture and provide event analysis
- Application level traffic analysis
- Application layer bounce charts for application performance visualization

#### 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.

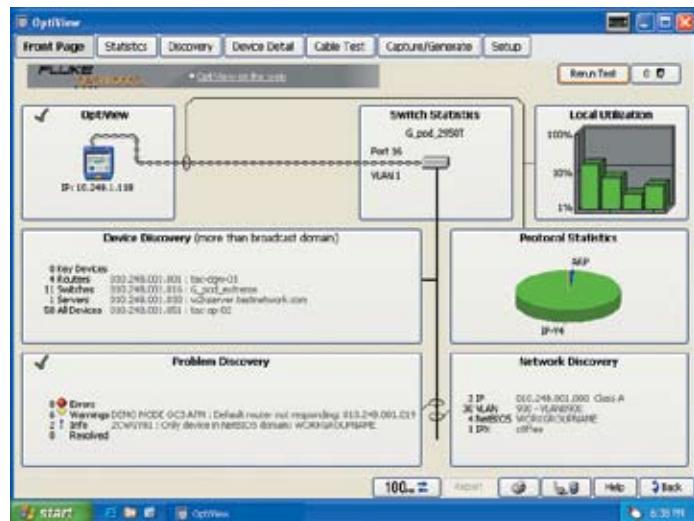
Analyze protocol mix to identify top protocols being used and also discover unwanted and custom protocols and see which protocols are being used by each host.

## Application traffic analysis

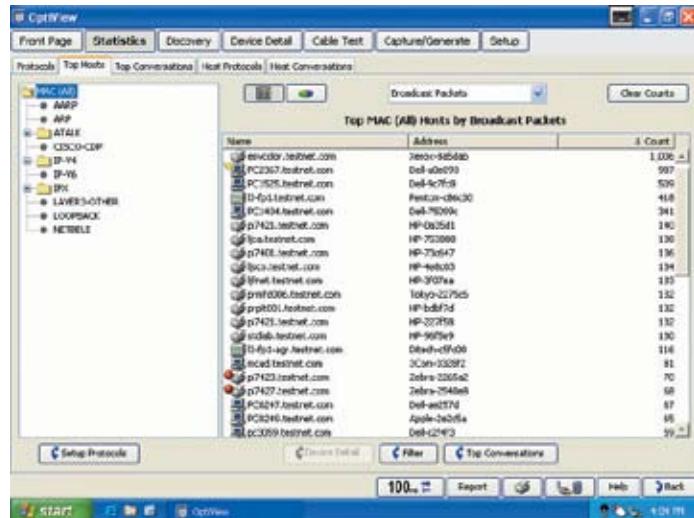
Automatically discover all protocols and sub protocols from the MAC layer to the application layer. This enables IT staff to identify applications utilizing link bandwidth including those that use dynamically assigned port numbers to see and validate the impact of applications on bandwidth usage and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



Front page



## 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 IP 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 IT staff user can add a device to Key Devices and the analyzer will automatically test connectivity from the attached segment to that device by performing an IP or IPX ping. A key device that fails to respond, will show up in the Problem Discovery as "Key Device not responding," providing you with at-a-glance monitoring of critical network devices. 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.

## Vendor independent infrastructure device analysis

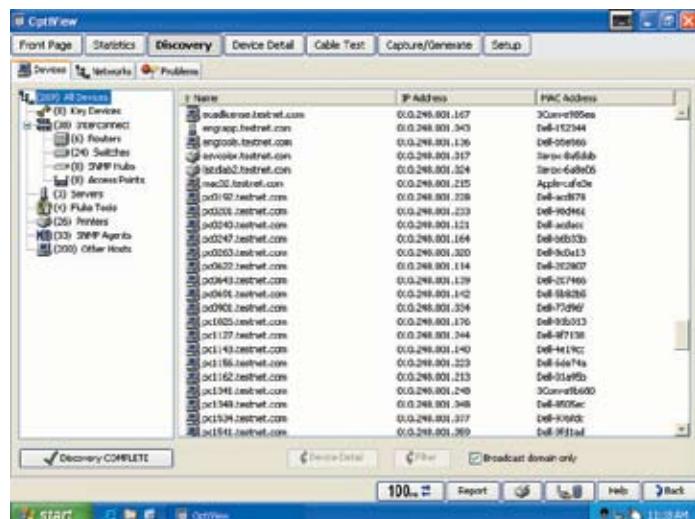
Get visibility into switches and routers located anywhere on the enterprise network. With this information, you can optimize network performance, improve efficiency and reduce costs while improving reliability and security.

### Multi-port switch statistics

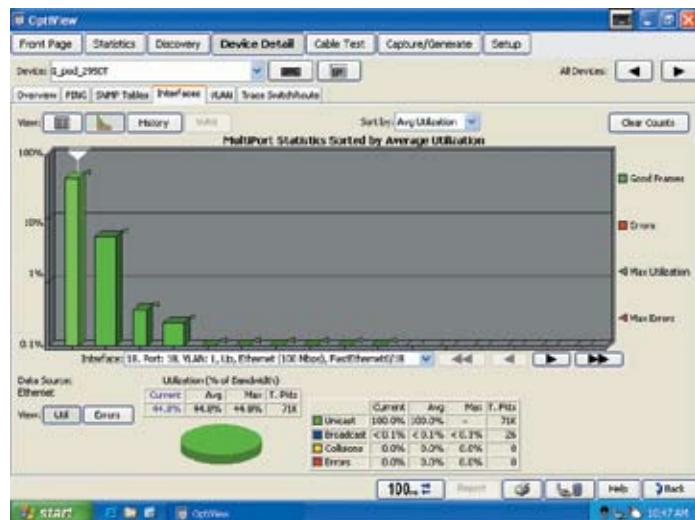
In-depth analysis, including:

- 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.



Device discovery



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.

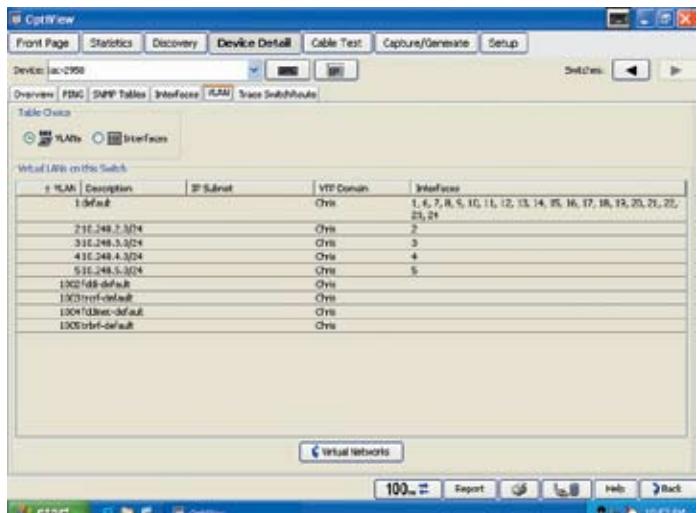
# Trace SwitchRoute™

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.

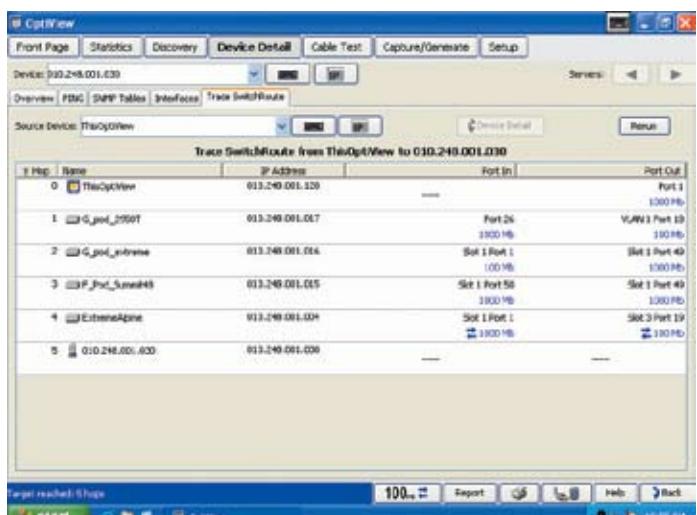
## Router and WAN link analysis

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.

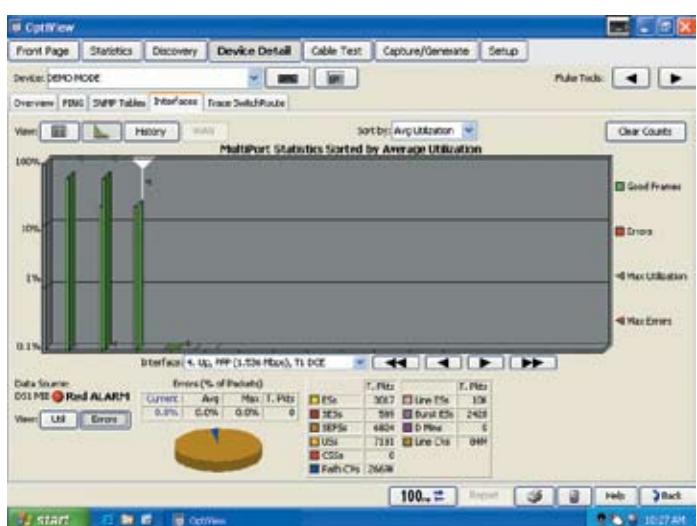
Telnet and web browser links to allow reconfiguration of devices directly from the analyzer.



### *VLAN configuration*



### *Trace SwitchRoute*



### *WAN interface statistics*



## Traffic generation

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.

## 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.

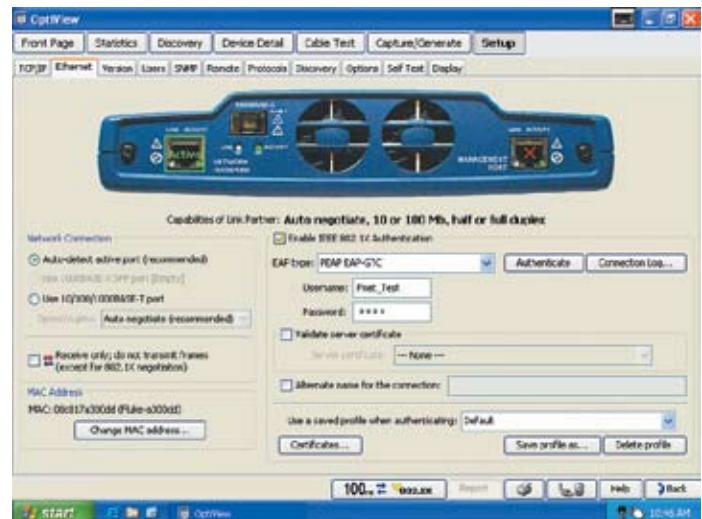
## Packet capture and decode

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.

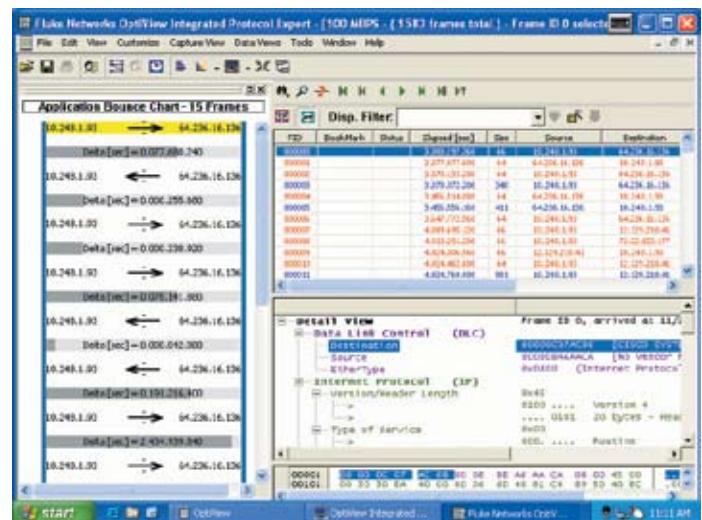
Sophisticated capture filters allow collection of more relevant data and limit the amount of traffic to analyze by filtering on individual addresses or conversations, address range for IPV4, IP subnet and protocols.

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.



802.1x configuration



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.

## Reporting/documenting

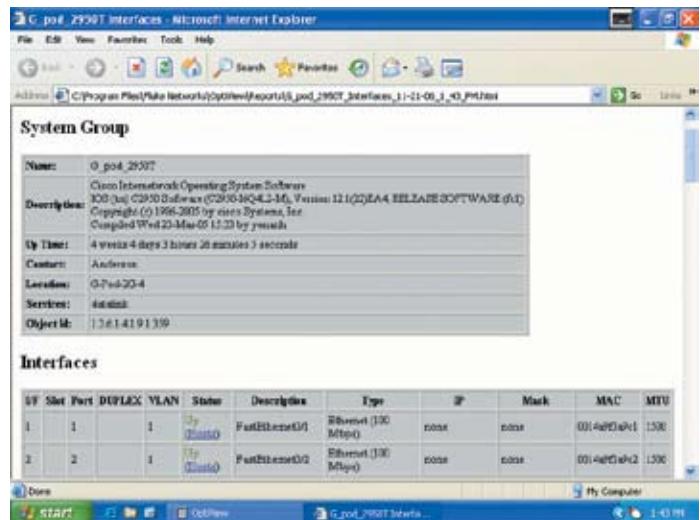
While viewing the statistics, discovery or detail screens, pressing the Reports key will generate HTML reports on Protocols, Top Hosts, Top Conversations, Devices, Networks, Problems and many more. These reports are saved and may be viewed locally or remotely using a web browser.

## 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 analyzer will support seven remote sessions for collaborative troubleshooting or opening of multiple sessions on a PC to provide a remote dashboard view.



Free String Match setup



Reports



## 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.

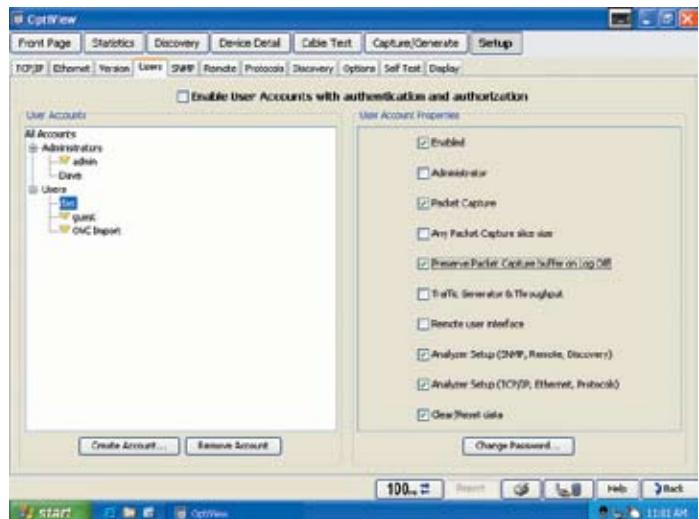
## OptiView™ Throughput Test

With the Throughput Test, 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.

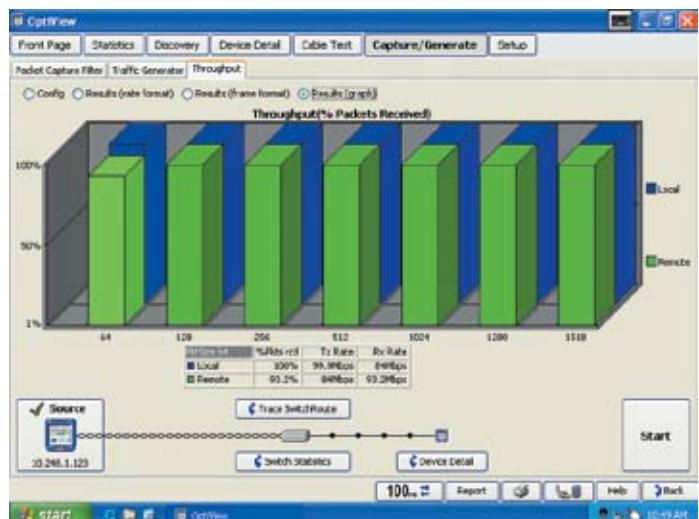
The Throughput Option allows you to configure the following parameters:

- 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.



User accounts



Throughput option



## 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

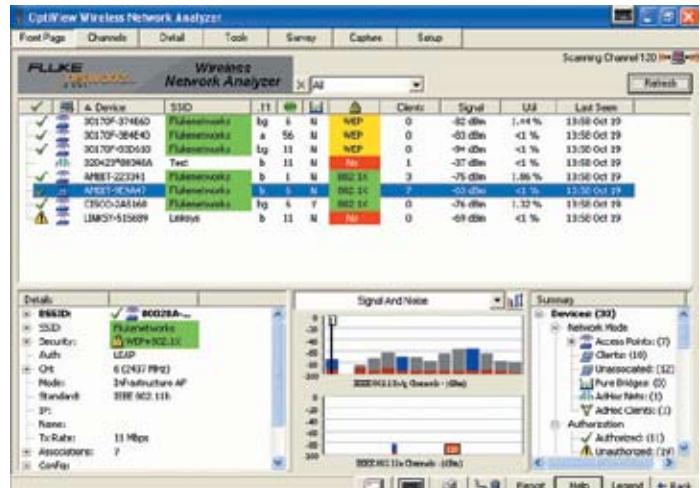
## OptiView™ Wireless Option

Fluke Networks gives you the visibility you need to manage both your 802.11 a/b/g 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 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 front page



## OptiView™ Expert Analysis Option

The OptiView Expert Analysis Option speeds up troubleshooting by automatically detecting problems while analyzing captured packets collected by the OptiView Analyzer. The Expert View categorizes 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:

- Application Layer: Excessive ARP, Excessive BOOTP, NFS Retransmission, HTTP Get Response, HTTP Post Response, Slow Server Connect, Slow Server Response.
- Transport Layer: Non-responsive station, TCP/IP checksum error, TCP/IP Fast Retransmission, TCP/IP Retransmission, TCP/IP Frozen Window, TCP/IP Long Ack and TCP/IP SYN Attack.
- Network Layer: ICMP Errors and Unstable MST.
- Datalink Layer: Illegal MAC Source Address, Broadcast/Multicast Storms and Physical Errors.

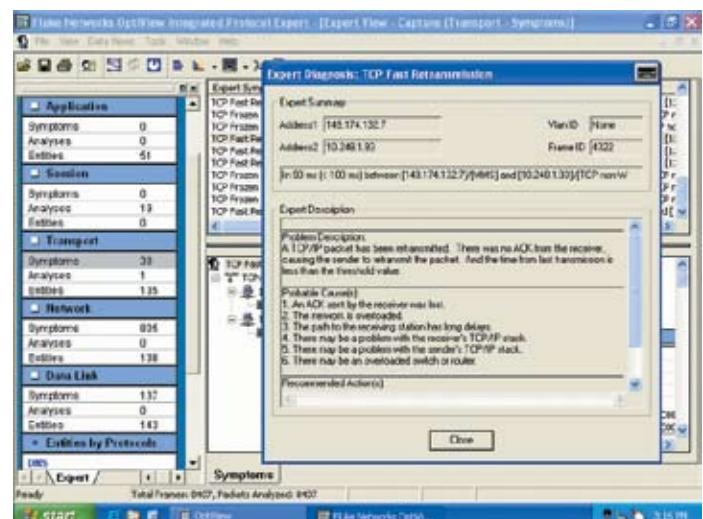
Double clicking on the Expert Symptom button displays the Expert Diagnosis window that provides a description of the station symptom, a probable cause and recommended action(s). Click on any of the stations listed in the Expert View to get a detailed view of the traffic captured.

## OptiView™ Voice over IP Option

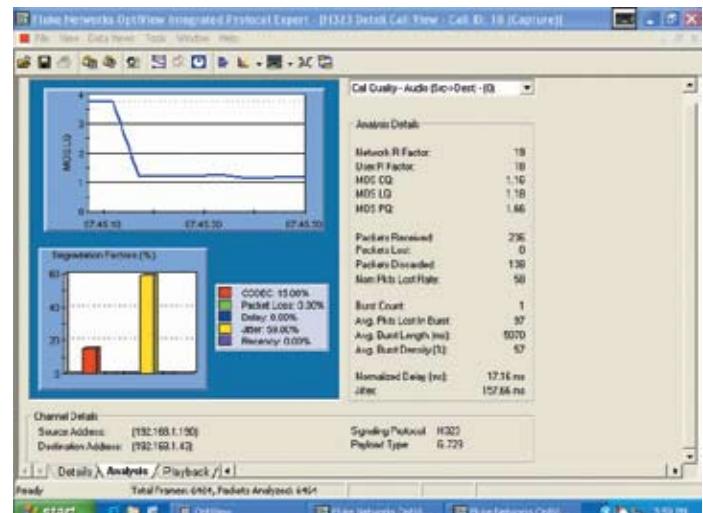
Voice over IP is one of the most mission critical applications being deployed by IT organizations today. The rollout of VoIP services is accompanied by the expectation of toll availability and sound quality. It is therefore imperative IT organizations have the proper tools to monitor VoIP call QoS during 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.



Expert analysis



VoIP call quality

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.

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™ 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.

## Professional Vision Suite

The Professional Vision Suite turns the OptiView Series III Integrated Network Analyzer 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™ Console software monitors and trends 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 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.fluenetworks.com/goldsupport](http://www.fluenetworks.com/goldsupport) for more information.



## Specifications

General Specifications	
Weight	Without external battery 2.2 kilograms (5.0 lbs) With external battery 3.0 kilograms (6.6 lbs)
Dimensions	26.0 x 23.4 x 6.4 centimeters (10.3 x 9.2 x 2.5 inches)
Display	LCD touch screen, 800 x 600 pixels, active color panel, CCFT back-light and bezel, touch pad
LED indicators	16 (21 with external battery)
Power	
Internal battery	Lithium Ion 11.1 V DC (nominal), 2 Ah
External battery	Lithium Ion 11.1 V DC (nominal), 6 Ah
External AC adapter/battery charger	AC input: 120 V – 240 V, 50/60 Hz, 1.5 A DC output: 15 V, 4.0 A
Ports	
Communication and accessory ports	3 USB, 1 PC Card type II, 1 VGA out 15-pin connector
Network analysis ports	RJ-45 10/100/1000BASE-T Ethernet, fiber 1000BASE-X SFP GBIC
Network Standards	
LAN Interfaces	IEEE 10BASE-T, IEEE 100BASE-TX, 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 <sup>1</sup>	1 to 153 m (3 ft to 500 ft) +/- 2 m (6 ft)
Environmental and Safety	
Operating Temperature <sup>2</sup>	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)
Altitude	Operates up to 4600 m (15091 ft)
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 and 1040.11, CFR(J)
Safety	(CSA) Complies to CSA C22.2 No. 950 (Canadian standards), and UL 1950 (US standards) (CE) Complies with European Union directive EN60950

<sup>1</sup> Length accuracy is dependent on the cable type selected in the Cable Test screen with its ideal NVP (nominal velocity of propagation) matching the NVP of the cable under test. <sup>2</sup> Battery will not charge below 12°C (53.6°F)



## Models, Options and Accessories

Model	Description
<b>OPVS3-GIG</b>	OptiView Series III Integrated Network Analyzer Gigabit (1000BASE-SX)
<b>OPVS3-GIG/W</b>	OptiView Series III Integrated Network Analyzer with Wireless Option
<b>OPVS3-GIG/S</b>	OptiView Series III Integrated Network Analyzer Gigabit with Wireless, Expert and VoIP Options
<b>OPVS3-GIG/RHD</b>	OptiView Series III Integrated Network Analyzer Gigabit with Removable Hard Drive
<b>OPVS3-GIG/PSVS</b>	Professional Vision Suite with OptiView Series III Integrated Network Analyzer Gigabit
<b>OPVS3-GIG/RHD/PSVS</b>	Professional Vision Suite with OptiView Series III Integrated Network Analyzer Gigabit with Removable Hard Drive
<b>OPVS3-GIG/PSVS/W</b>	Professional Vision Suite with OptiView Series III Integrated Network Analyzer and Wireless Option
<b>OPVS3-GIG/PSVS/S</b>	Professional Vision Suite with OptiView Series III Integrated Network Analyzer and Wireless, Expert and VoIP Options



Model	Description
<b>OPVS2-EXPT</b>	Expert Analysis Option
<b>OPVS2-VOIP</b>	VoIP Analysis Option
<b>OPV-WNA3</b>	OptiView Wireless Option 802.11 a/b/g
<b>INTAIR-LAP</b>	InterpretAir WLAN Site Survey Software
<b>ANALYZEAIR</b>	AnalyzeAir Wi-Fi Spectrum Analyzer
<b>IA-AA</b>	Wireless Software Suite includes: InterpretAir WLAN Site Survey software and AnalyzeAir Wi-Fi Spectrum Analyzer
<b>OPVS2-WLESS</b>	Wireless Suite includes: OptiView Wireless Option 802.11 a/b/g, InterpretAir WLAN Site Survey software and AnalyzeAir Wi-Fi Spectrum Analyzer
<b>OPV-SFP-SX</b>	850nm, 50 and 62.5 micron multi mode fiber. 1000BASE-SX SFP adapter
<b>OPV-SFP-LX</b>	1300 nm, 10 micron single mode fiber. 1000BASE-LX SFP adapter
<b>OPV-SFP-LX10</b>	1310 nm, 10 micron single mode fiber. 1000BASE-LX SFP adapter
<b>OPV-SFP-BX</b>	1490 nm fiber. 1000BASE-BX SFP adapter
<b>OPV-SFP-ZX</b>	1550 nm fiber. 1000BASE-ZX SFP adapter
<b>OPVS2-KB</b>	Mini Keyboard (USB)
<b>OPVS2-BP</b>	External Battery Pack
<b>OPVS3-RHD</b>	Removable Hard Drive for OPVS3-GIG/RHD
<b>OPVS3-RHD/4</b>	Pack of four Removable Hard Drives for OPVS3-GIG/RHD
<b>OPV-FT600</b>	OptiView Fiber Inspector
<b>NF430</b>	Fiber Optic Cleaning Kit

### NETWORK SUPERVISION

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.fluenetworks.com/contact](http://www.fluenetworks.com/contact).

©2007 Fluke Corporation. All rights reserved.  
Printed in U.S.A. 1/2007 1590227 D-ENG-N Rev K