FLUKE networks

OptiView® Management Appliance with OptiView® Reporter

Network and Application Monitoring and Analysis

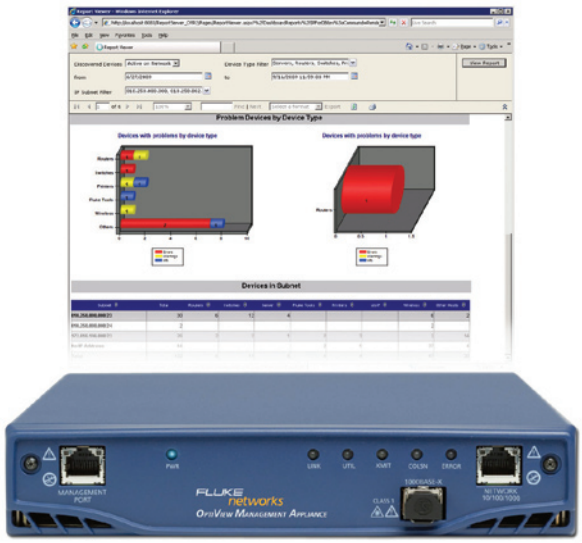
Part of the OptiView Management Suite (OMS)

OMS provides the breadth of visibility and depth of analysis for a complete picture of network and application performance. It's the only solution that combines proactive monitoring with in-depth "on-the-wire" analysis and portability to see problems up close – anywhere on the network.

By combining best of breed solutions for monitoring, analysis and troubleshooting, OMS can be used as a holistic management suite or part of your IT organization's toolset, to help reduce complexity and improve productivity in your team's daily workflow.

OptiView Management Appliance and OptiView Reporter

At the core of OMS, the OptiView Management Appliance gives you unmatched visibility into your network because it integrates NMS functions in a purpose-built appliance along with on-the-wire deep packet inspection. When used in combination with OptiView Reporter, network support organizations can create and use customizable web reports for daily operations and monitor long-term trends of network and application performance.



Proactive monitoring and "on the wire" analysis from a dedicated appliance

OptiView Management Appliance is purpose-built to proactively test and monitor network and application performance. Test information is automatically imported into OptiView Reporter for 24x7 monitoring, trending, and event notification, with easy access via customizable web reports.

When used together, this solution provides the tools needed for daily management, and the detailed information and quick visibility that you need to detect and resolve network and application problems smarter and faster. When problems occur locally or at remote sites, the guesswork is eliminated; you know what's out there, what it's doing, and how it all interconnects. With a simple click, you can immediately access remote OptiView Appliances for real-time analysis and troubleshooting.

While most NMS can take hours or even days of set up before they are collecting useful data, the OptiView Management Appliance requires only minimal configuration, and can be on the wire and collecting actionable information within minutes.

Daily proactive management

- Monitor key devices and applications for performance, not just availability
- Trend response times and packet loss on key devices and applications
- Easily identify and alarm on the top issues in the network

Web-based reporting

- Provides daily reports to "prove it's not the network" more easily
- Easy access to information and sharing across groups

"On-the-wire" visibility

- Integrates NMS functions in a purpose-built appliance along with on-the-wire deep packet inspection
- Install at critical points in the network and at remote sites to monitor performance, to observe top conversations, top protocols, who is taking up bandwidth with what applications
- Line-rate Gigabit packet capture for detailed application analysis

Network and application monitoring, trending and reporting

Technical Data

Advanced network discovery

Finds devices, networks and problems in seconds.

As soon as the Appliance is connected to the network, it automatically begins to discover devices on the network, monitoring traffic and actively querying hosts. IT staff can immediately see what devices are on the network and where they are 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 Appliance categorizes devices by type: interconnect (routers, switches, SNMP hubs and access points), servers, printers, SNMP agents, VoIP devices, wireless devices, and other hosts. Additionally, networks are classified by IPv4 and IPv6 Subnets, VLANs, VTP Domains, NetBIOS Domains, IPX Networks, and Wireless 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.

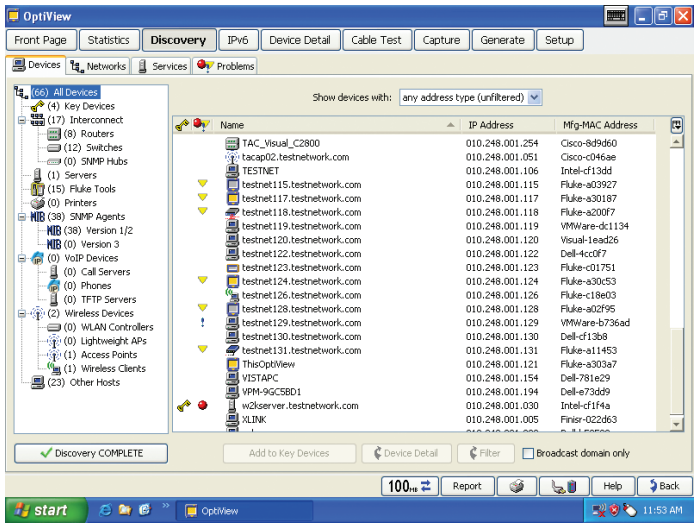
Most network analyzers and troubleshooting tools have limited visibility in today’s networks: usually a single broadcast domain or VLAN, but the OptiView Management Appliance can be configured to extend its discovery beyond the broadcast domain or local VLAN boundaries, across your enterprise network, into remote sites and users.

Enterprise network overview - See your entire network from your desk

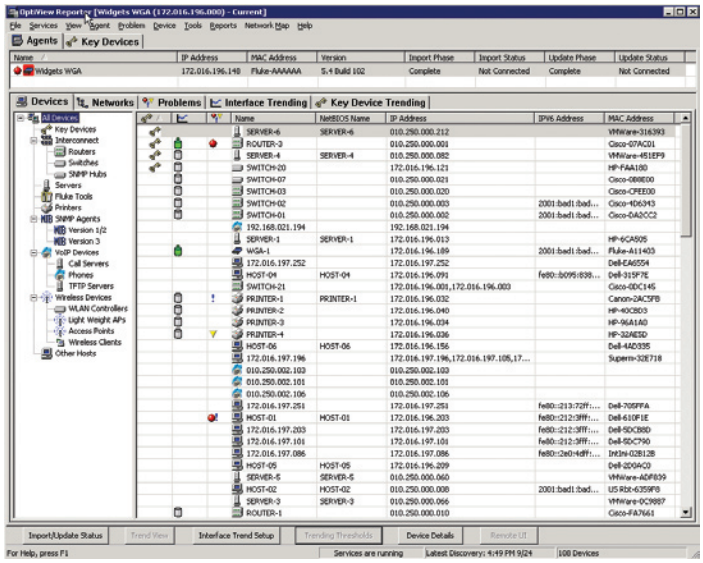
Using OptiView Reporter to import data from the OptiView Management Appliance, you get an at-a-glance summary of each of your local and remote Appliances and see the network as they see it. How many devices are out there? What kinds of devices are they? What are their names, IP Addresses, MAC Addresses? What problems have been discovered? Who is connecting to your network and when? What is the bandwidth utilization on key LAN or WAN links? The remote hardware agents know, and now you know too.

Detailed device view

- Device types: key devices, servers, routers, switches, printers, Cisco VoIP devices, and others including Wireless LAN controllers and managed wireless access points
- Names: DNS, SNMP, and NetBIOS® machine names
- Addresses: IP addresses and subnet masks, IPv6 addresses, and MAC addresses
- Interfaces: type, speed, state, MTU, slot and port, VLAN ID, and virtual circuit descriptions
- Protocols: IP, and NetBIOS protocol and configuration information
- SNMP information: name, location, contact, and description



Device discovery

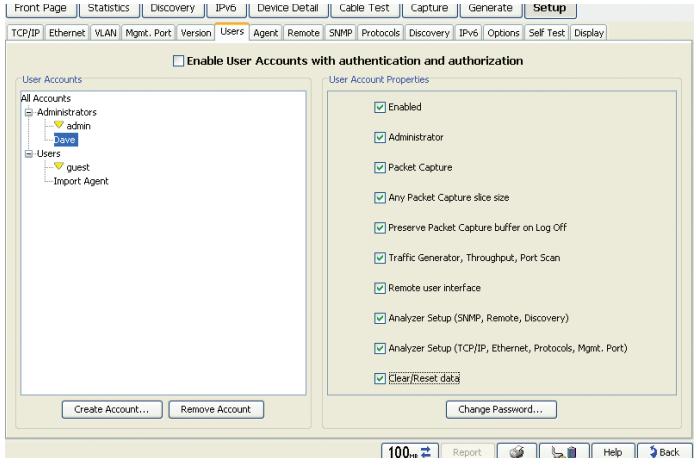


Enterprise network overview in OptiView Reporter

VoIP and wireless discovery

The Appliance will 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.

The Appliance also discovers and categorizes wireless LAN controllers, lightweight access points, intelligent access points and wireless clients. Detailed device information is provided from Cisco Wireless LAN controllers and LWAPs, including the wireless networks associated with the controller, the SSIDs, security and QoS parameters, the lightweight APs being controlled and the 802.11 protocol in use. 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.

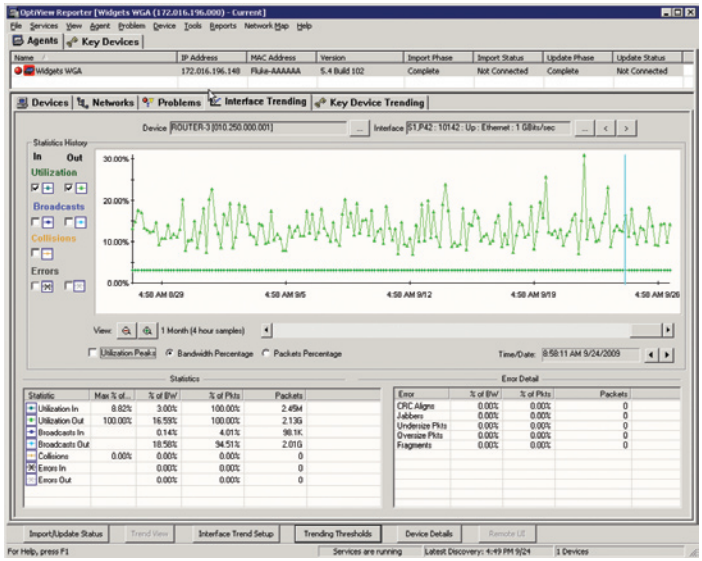


Wireless Network Discovery

Performance monitoring and trending

For network professionals to do more than react to problems, IT departments must employ some level of network monitoring in order to proactively detect issues, rather than waiting for the phone to ring. But unfortunately, many products on the market today sell "availability" as "performance". While it is essential to track the availability of key devices, it is not sufficient. OptiView Management Appliance gives you two methods for monitoring key performance metrics on your network:

- Network infrastructure interface monitoring via SNMP
- Trending of key device and application performance tests



Interface Trending View in OptiView Reporter

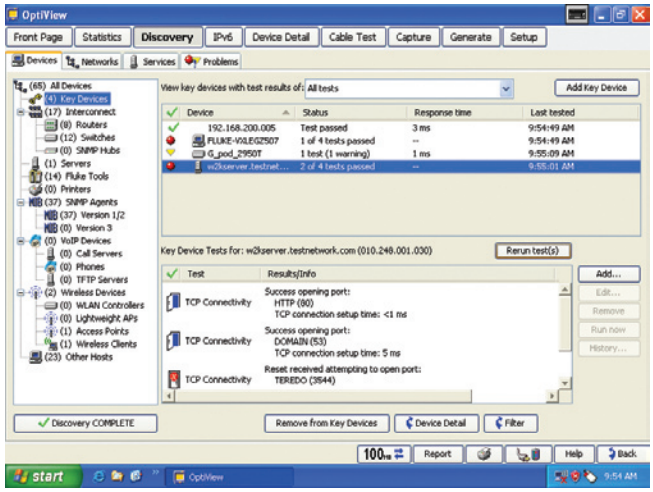
Network infrastructure interface monitoring

Vendor-independent infrastructure device monitoring via SNMP (v1, v2, or v3) gives visibility into switches and routers located anywhere on the enterprise network. With this information, along with user-configured thresholds and notifications (via email, SMS, SNMP trap) you can be more proactive – use OptiView Management Appliance and Reporter to watch for problems automatically, and notify you when they occur. Knowing interface trend data over the long term allows you to optimize network performance, improve efficiency and reduce costs while improving reliability.

Select a device and interface to see in/out utilization, broadcasts, collisions, errors, and utilization peaks for the last hour, day, week, month, three months, six months, or one year. Granularity ranges from two minutes to 48 hours (averaged) depending on the selected history interval. Most NMS pollers aggregate data over longer periods; with more granularity in Reporter, you'll be able to spot bandwidth issues that are glossed over in other products.

Trending of key device and application performance tests

OptiView Management Appliance Key Device tests are used to monitor for availability, performance and packet loss to devices such as servers, switches, routers, hosts, or any other device you choose. They show you the green/ red, up/down status of each device, name and address information, test results, as well as when the last state change occurred. Application tests are used to ensure server and application connectivity by opening specific TCP ports on servers, revealing any issues that may be due to application ports being closed on the path between the server and the Appliance. Application performance is the round trip time for the specified ports as a combination of network latency and server connection set up time (SYN/SYN ACK). Device availability as well as network response time and packet loss are provided through ping tests.



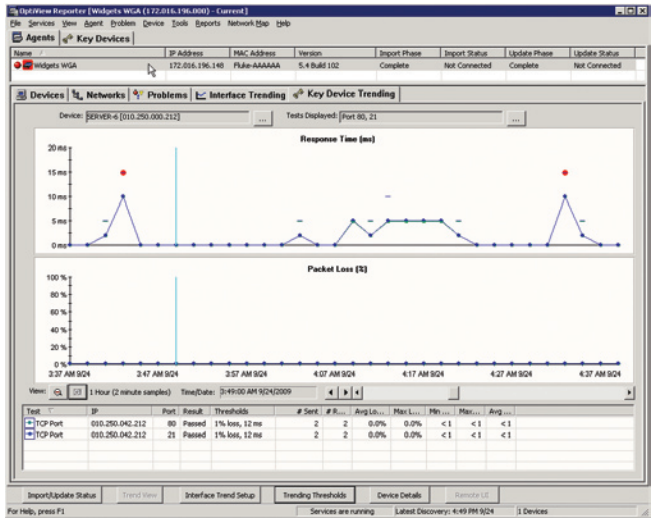
Key device tests for performance and availability in OptiView Management Appliance

Web-based Automated Reporting

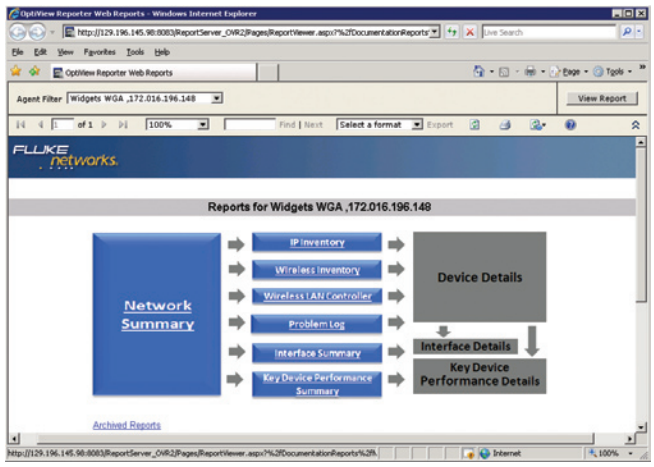
OptiView Reporter greatly reduces manual report generation, asset discovery and management, and network diagramming time and effort. For easy access and collaboration between groups, OptiView Reporter provides a web-accessible summary page with access to every report from the OptiView Management Appliance. These pages create multiple, customizable 'dashboards' for viewing critical network and application performance factors. Frequent updates (refresh of data) ensures near-real-time information.

Report types include: inventory/discovery, device and application performance, device and interface availability and performance. Summary views and "Tops" reports to identify the top problems, often used as the "hit list" for the network support group's daily tasks.

This fast, easy, and accurate documentation can be generated on-demand in Reporter's user interface, or at a user defined, scheduled interval. Reports can be customized with the user's contact information, custom header/footer, company logo, and report title. Reports can be saved in a variety of formats such as Adobe® Acrobat, HTML, XML, Microsoft® Excel, Microsoft Word, and comma-separated. OptiView Reporter's built-in Web Server lets you remotely view archived reports and maps.



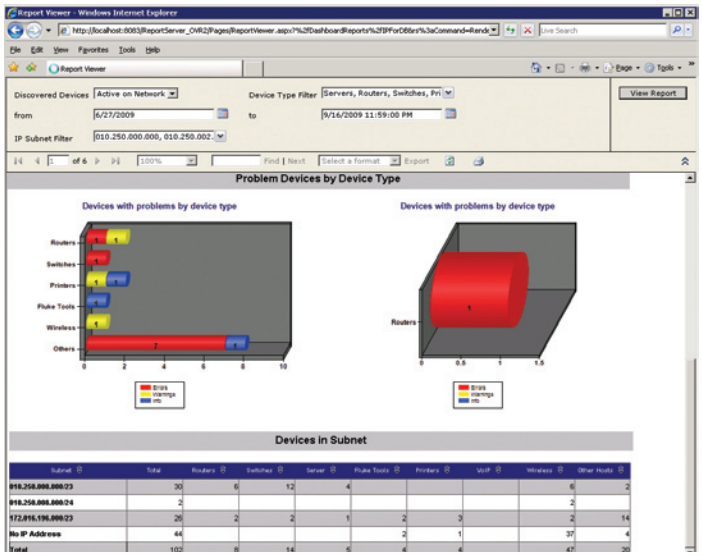
Trending of key device application performance tests in OptiView Reporter



Easy web-based access to reports

Dynamic report filtering makes it easy to find critical information

Interactive report configuration allows for custom filtering, report duration, table column sorting and hyperlinks to access detailed information from the summary reports. Multiple filters can be simultaneously applied, immediately updating the report. This allows the user to focus the results on the specific area or data desired. Filters available include: time period, subnet, SSID (for WLAN reports), device type, application type, "new on network" or "active on net" (to find new devices on the network.)



Interactive reports allow filtering to critical information

Inventory Reports include:

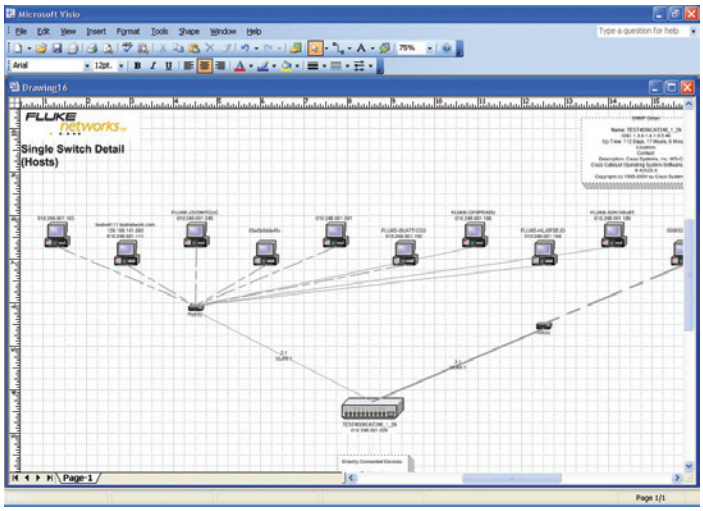
- IP
- NetBios
- VLAN
- Switch Detail
- Device Detail
- Trendable Interfaces
- Trended Interfaces
- Wireless Network and Devices
- WLAN Controllers
- AP and LWAP device detail
- WLAN Client device detail

Performance Reports include:

- Device Performance Summary
- Application Performance Summary
- Device Performance Detail
- Interface Availability, Utilization and Error summary and detail

Traffic Distribution reports include:

- Top Protocols
- Top Talkers
- Top Protocols by Host



Automated network mapping

Automated Network Mapping - Save time, keep maps up-to-date with minimal effort

Keeping network maps updated can be an overwhelming task, but not with OptiView Reporter. With Reporter's seamless integration with your Microsoft Visio mapping software, you can instantly create maps showing the links between your servers, routers, hosts, switches and hubs. Map generation is fast and easy. Just select the map you want and OptiView Reporter does the rest. The following network maps are available:

- Switch (Spanning Tree) Diagram
- Server Connections in a Switched Network
- Router Connections in a Switched Network
- Fluke Networks Tool Connections in a Switched Network
- Printer Connections in a Switched Network
- Single Switch Detail - Routers, Switches, and Servers - Printers - Hosts
- Device Connections for VLAN
- Customized Device Connections

On the Wire Traffic Analysis

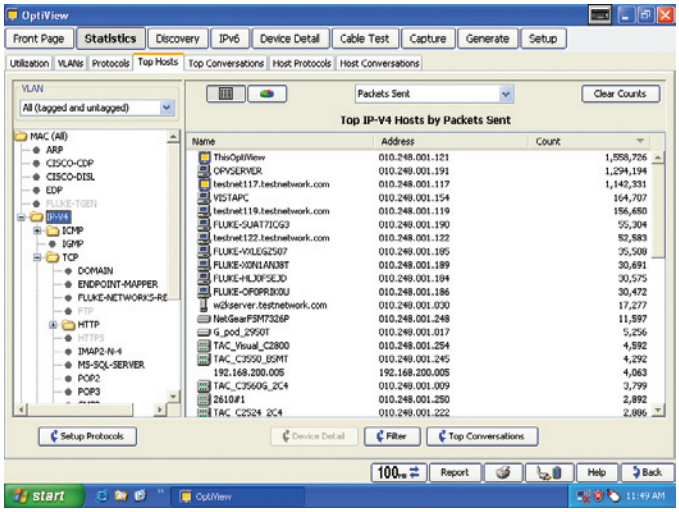
Traffic analysis at the touch of a button

The OptiView Management Appliance 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.

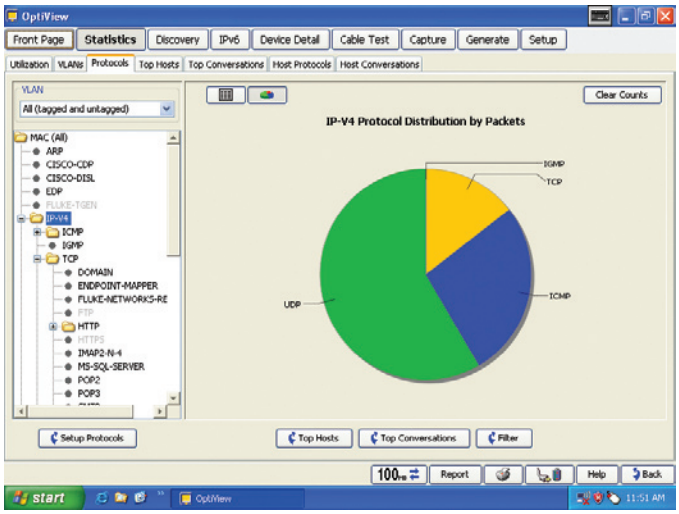
Application traffic analysis

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.

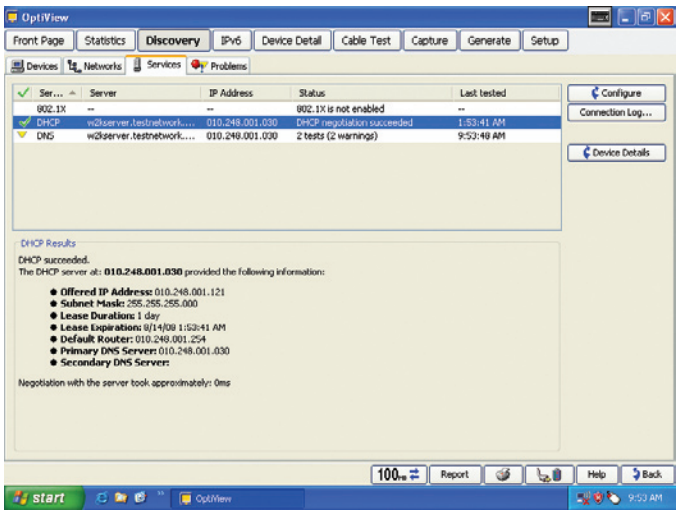
Speed up troubleshooting application and network performance issues by automatically validating that network services such as DHCP, DNS and 802.1X are available and operating correctly, ensuring that server and application connectivity is accessible by opening specific TCP IPv4 and IPv6 ports on servers and reporting the round trip time as a combination of network latency and server connection set up time. Ensure WIN servers are operating efficiently by viewing resources including number of users, processor, memory and disk utilization and services and process that are running.



Top hosts



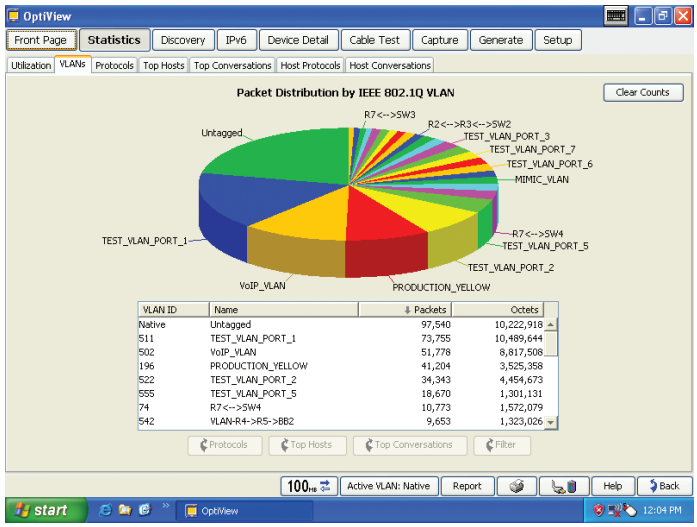
Protocol mix



Validate network services

VLAN Visibility and Trunk Analysis

Only “on the wire” appliances can provide vision into actual VLAN trunk traffic. When connected to a switch trunk port, the Appliance 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

Infrastructure Analysis

Real-time infrastructure device analysis data speeds troubleshooting

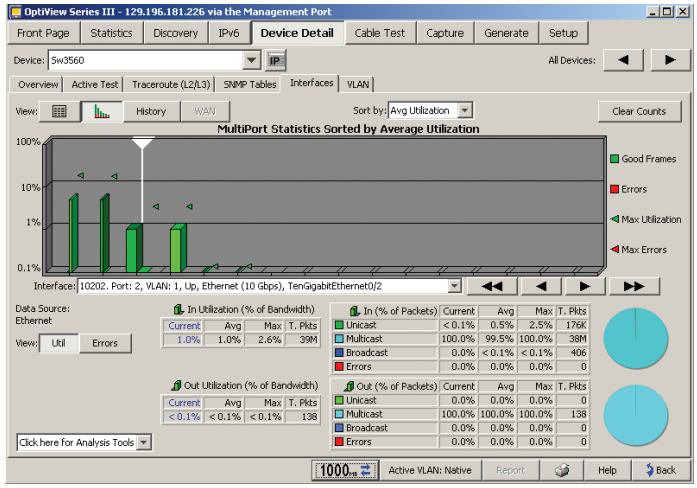
Get granular, real-time data into interface utilization and errors via SNMP – essential for troubleshooting persistent problems and determining if excessive traffic and bandwidth utilization is the cause of performance problems.

Interfaces can be quickly sorted by I/F index, utilization, broadcasts, errors, or collisions. LAN and WAN errors, alarms and utilization details are available in the trending view along with interface configuration information.

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.



Real-time multi-port interface statistics

VLAN analysis

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

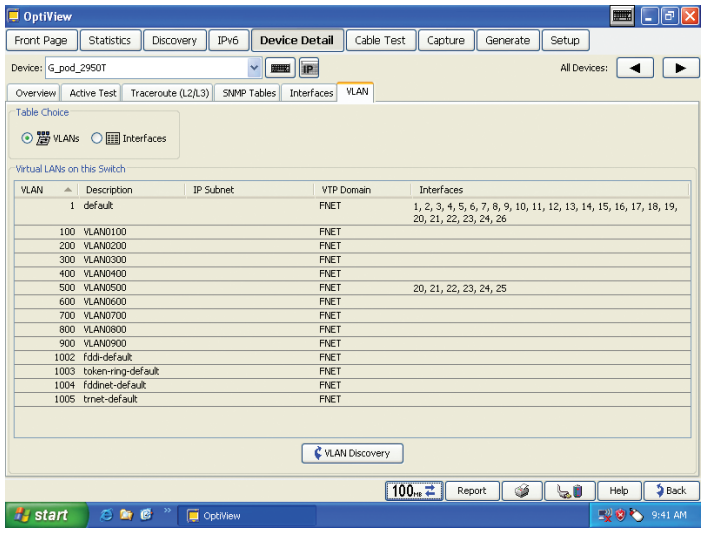
- VLANs that are configured on the switch.
- Interfaces that are members of each VLAN.
- Identification of trunk or uplink ports, together with the trunking protocol in use.
- Identification of which hosts are members of each VLAN.

Trace SwitchRoute™

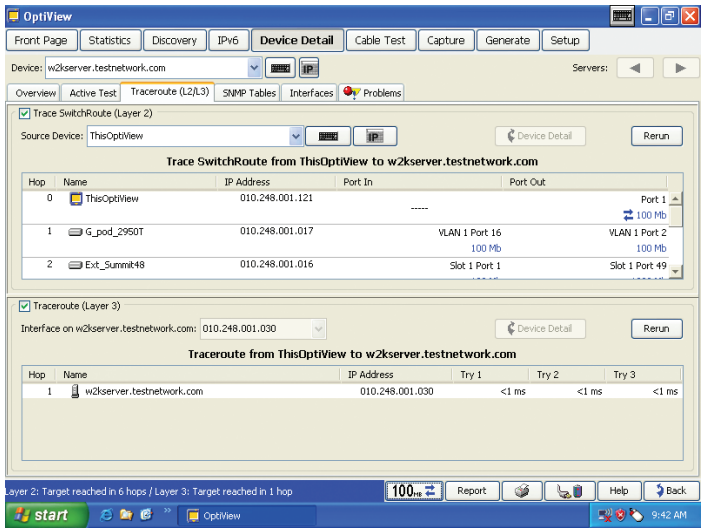
Trace SwitchRoute allows you to see the exact path two devices use to communicate through your switch fabric. Trace SwitchRoute begins its discovery from the specified Source Device and traces the path to the specified Target Device. For each switch in the path, the displayed results include the DNS 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

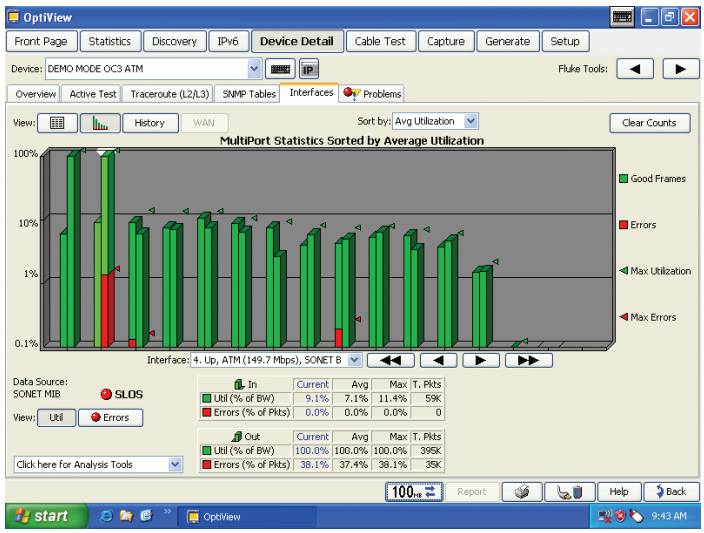
In-depth device analysis identifies Router ARP cache or routing table errors and also provides visibility to manage and troubleshoot costly WAN links. See WAN link configuration, a graphical display of utilization and error rates and identification of specific error types on ISDN, Frame Relay, T1/E1,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



VLAN discovery



Trace SwitchRoute



WAN interface statistics

Application-Centric Protocol Analysis

Full-line rate capture ensures complete analysis

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

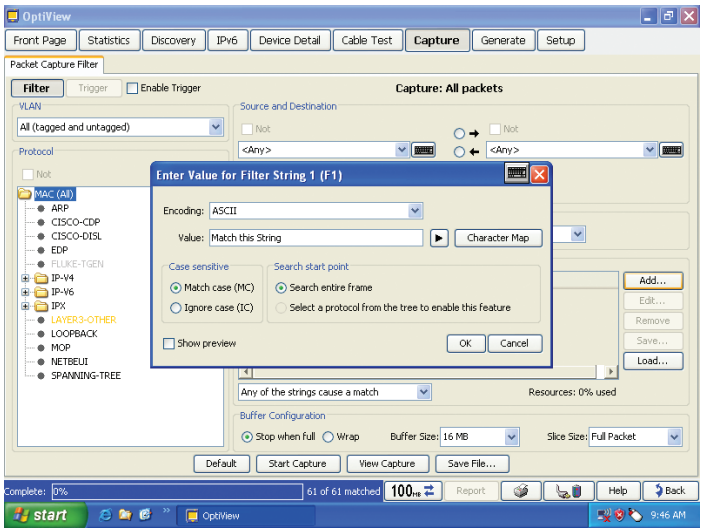
Free String Match to find and capture anything

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.

Application-centric analysis for simplified troubleshooting of application problems

Once traffic is captured, launch the ClearSight Analyzer* (CSA) to see an application-centric view of the trace file. Through a simple and intuitive front page, CSA presents a comprehensive, high-level overview of the health of applications on your network. From that framework, you can drill down to gain access to more detailed information. For example, you can display all the activity for HTTP applications, then drill down to see activities on each server, and further down to the server flow to observe the actual media content of the flow. This unparalleled level of control and visibility speeds time to application problem resolution and minimizes overall network downtime.

* Note: The optional ClearSight Analyzer software (CSN/CSA-1000) is required to be installed on the PC controlling the OptiView Management Appliance in order to decode and analyze captured traffic.



Free String Match setup

Application Summary Front Page

Automated problem/issue detection

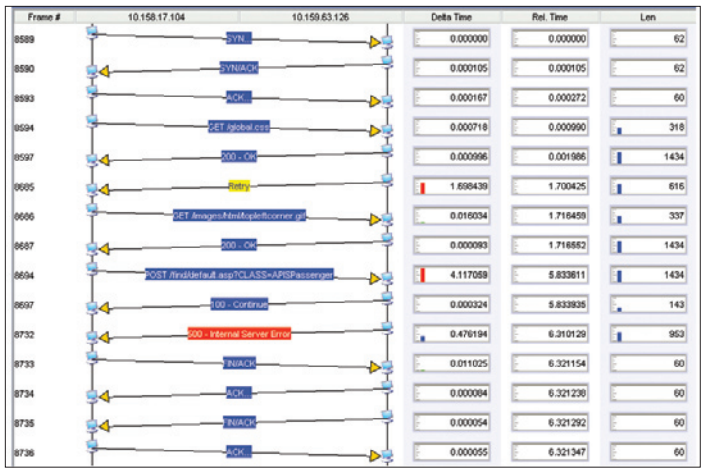
The CSA Expert Alert function automatically detects communication faults in captured packets and displays them with color coded icons. The specific application, server, or flow that has a problem can be seen at a glance from the Application Summary Front Page. Alerts detected by CSA are classified as issues (faults in the communication sequence) or problems (faults that exceed a threshold value) and can be listed separately. Lists can be sorted by simply clicking on a column header. You can drill down to the associated communication flow by right-clicking on an alert.

Unique and powerful ladder chart illustrates application flow

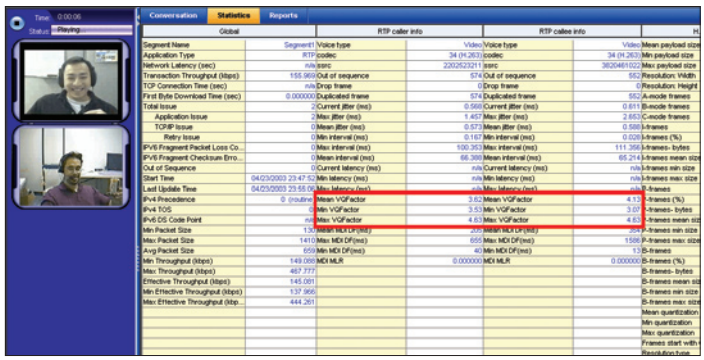
CSA ladder views (also known as application bounce chart) reveal conversations between client and server in the application command language without having to decode packets manually. It provides an extremely powerful way to understand protocol interactions between various network elements.

Content Reconstruction and Playback

You can recreate audio and video content from VoIP or video flows, either during real-time monitoring or from a tracefile. In addition, Microsoft® Exchange® email, Fax over IP, Instant Messages and HTTP-based web pages can also be reconstructed. This is very valuable as proof of compliance violation or visualization of multimedia quality.



Ladder chart



Reconstruct audio and video

Remote user interface

Simply point a web browser at the IP address of a correctly configured OptiView Management Appliance 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. Communications between the Appliance and Remote UI can also be encrypted. A single OptiView Management Appliance will support eight remote sessions for collaborative troubleshooting or opening of multiple sessions on a PC to provide a remote dashboard or multiple "NOC" views. Additionally, use the Appliance's management port to configure and monitor for out of band management independently of the network under test port.

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

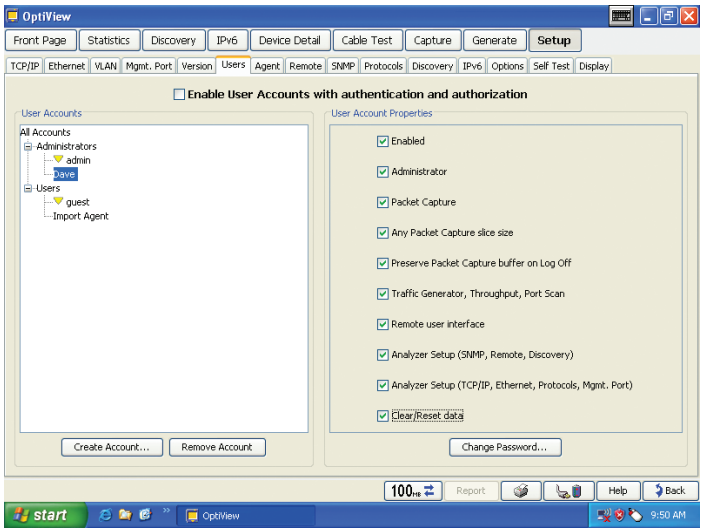
Help is contextually linked to each screen in the analyzer. While that help screen is displayed, you may select other information from the table of contents, choose an index entry, or perform a full text search on any help topic or term.

OptiView® IPv6 Analysis Option

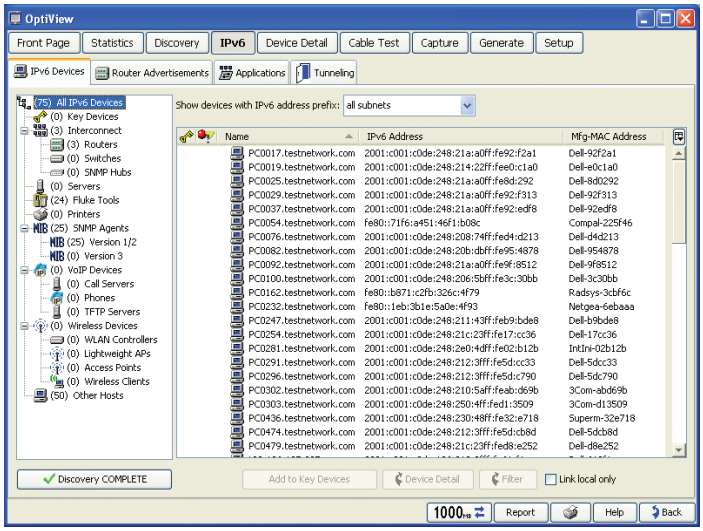
The analyzer will discover and display complete IPv6 network and device inventory including routers, switches, wireless AP's, DHCP6 servers and hosts. It enables you to identify active IPv6 devices in the network and those that may have problems in singlestack IPv6 networks. Router Advertisements are 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 userdefined 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.



User accounts



IPv6 Devices

OptiView Reporter - PC Specifications

The minimum system requirements needed to run the application with up to 40 agents on your PC are:

Number of Agents	Up to 40
System RAM	2 GB (recommended)
System RAM:	2 GB (recommended)
Processor Speed	2.8 GHz (recommended)
Browser	Windows Internet Explorer 6.0 or later
Disk space	• Installation Disk Space - 1.75 GB • Maximum Database Size - 4GB *Example Database: In a network with a 1000 device inventory, if you trend 250 devices with 3 tests each and 250 interfaces for 3 months, the database size will be approximately 1.5 GB.*
Operating system	The following 32 bit Operating Systems are supported: • Windows XP Professional SP2 or later • Windows 2003 Enterprise Server R2 SP2 or later • Windows Vista Business (32 bit) SP1 (English only) SP2 • Windows Server 2008 SP1 or SP2 (32 bit) ***Note** - We currently do not support 64-bit Operating Systems*
Languages	On any of the supported Operating Systems: • English • German • Japanese • Simplified Chinese

Specifications - OptiView Management Appliance

General Specifications	
Weight	1.63 kilograms (3.6 lbs)
Dimensions	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	Not applicable
LED Indicators	6
Power	
Battery	Not applicable
AC	AC input 85 to 265 VAC; 47/63 Hz; 25 watts
Ports	
Communication and accessory ports	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	-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

	OptiView Management Appliance MOA
Model Number/Name	**Description**
OPVS3-OMA/GIG/SP	OptiView Management Appliance
	Options
Model Number/Name	**Description**
OPVS3-IPV6	OptiView IPv6 Analysis Option
OPV-RPTR/PRO	OptiView Reporter Pro (40 Devices)
OPV-RPTR	OptiView Reporter (1 Device)
	Accessories
Model Number/Name	**Description**
OPV-TCASE	Hard shell transit case
OPV-RMK	Rack Mount Kit for one or two Management Appliances
LRPRO-REFLCT	LinkRunner™ Pro Reflector
OPV-SFP-SX	850 nm, 50 and 62.5 micron multi mode fiber 1000BASE-SX SFP adapter for OptiView Analyzers
OPV-SFP-LX	1300 nm, 10 micron single mode fiber 1000BASE-LX SFP adapter for OptiView Analyzers
OPV-SFP-ZX	1510 nm fiber 1000BASE-ZX SFP adapter for OptiView Analyzers
OPV-SFP-100FX	100BASE-FX SFP adapter
NFC-Kit-Case	Fiber Optic Cleaning Kit. See Photo
	OptiView Management Suites: Monitoring and Analysis
Model Number/Name	**Description**
OPVS3-GIG/OMS/MA-ADV	A dedicated applicance pack for monitoring and analysis at core and remote sites. It includes three OPVS3-WGA/GIG/SP - OptiView Management Appliance (3 appliances) and OPV-RPTR/PRO - OptiView Reporter Pro monitoring software for 32 devices
OPVS3-GIG/OMS/MA-EXPT	A dedicated applicance pack for monitoring and analysis at core and remote sites with the capability for "on the wire" application-centric protocol analysis. It includes three OPVS3-WGA/GIG/SP - OptiView Management Appliance (3 appliances), OPV-RPTR/PRO - OptiView Reporter Pro monitoring software for 32 devices, CSN/CSA-100 - ClearSight Analyzer Software and CSN/OPT-3045 - IP Multicast/History Reporter/Packet Generator Option for ClearSight Analyzer
	OptiView Management Suites: Monitoring, Analysis and Troubleshooting
Model Number/Name	**Description**
OPVS3-GIG/OMS/MS-ADV	An essential suite for network and application monitoring, analysis and troubleshooting. It includes OPVS3-GIG - OptiView Series III Portable Network Analyzer, OPVS3-WGA/GIG/SP - OptiView Management Appliance , OPV-RPTR/PRO - OptiView Reporter Pro monitoring software for 32 devices, OPVS3-WLIA - OptiView Wireless Infrastructure Analysis Option, NetAlly Agent and Application Troubleshooting Expert Active Tests
OPVS3-GIG/OMS/MS-PRO	An essential suite for network and application monitoring, analysis and troubleshooting plus end user experience monitoring and analysis. It includes OPVS3-GIG - OptiView Series III Portable Network Analyzer, OPVS3-WGA/GIG/SP - OptiView Management Appliance , OPV-RPTR/PRO - OptiView Reporter Pro monitoring software for 32 devices, OPVS3-WLIA - OptiView Wireless Infrastructure Analysis Option, Application Troubleshooting Expert Active Tests, OPVS3-WFA - OptiView AirMagnet WiFi Analyzer and ANALYZEAIR - WiFi Spectrum Analyzer and APPAD-TC-10 - NetAlly Application Advisor Test Center with 10 Agents
OPVS3-GIG/OMS/MS-EXPT	The complete suite for network and application monitoring, analysis and troubleshooting. It includes OPVS3-GIG - OptiView Series III Portable Network Analyzer, three OPVS3-WGA/GIG/SP - OptiView Management Appliance (3 appliances), OPV-RPTR/PRO - OptiView Reporter Pro monitoring software for 32 devices, OPVS3-WLIA - OptiView Wireless Infrastructure Analysis Option, Application Troubleshooting Expert Active Tests, OPVS3-WFA - OptiView AirMagnet WiFi Analyzer, ANALYZEAIR - WiFi Spectrum Analyzer, CSN/CSA-100 - ClearSight Analyzer Software and CSN/OPT-3045 - IP Multicast/History Reporter/Packet Generator Option for ClearSight Analyzer, APPAD-TC-10 - NetAlly Application Advisor Test Center with 10 Agents and OPV-TRKR-10 - OptiView NetFlow Tracker (10 Device)
	Support
Model Number/Name	**Description**
GLD-OPVS3-WGA	Gold Product Support Services, OptiView Management Appliance
GLD-OPVS3-WGA/DSVS	Gold Product Support Services, OptiView Series 3 Management Appliance Distributed Vision Suite
GLD-OPVS3-WGA/GIG	Gold Product Support Services, OptiView Management Appliance
GLD-OPVS3-GIG/OMS/MA-ADV	Gold Product Support Services, Advanced Monitoring Suite
GLD-OPVS3-GIG/OMS/MA-EXPT	Gold Product Support Services, Expert Monitoring Suite
GLD-OPVS3-GIG/OMS/MS-ADV	Gold Product Support Services, Advanced OMS Suite
GLD-OPVS3-GIG/OMS/MS-PRO	Gold Product Support Services, Professional OMS Suite
GLD-OPVS3-GIG/OMS/MS-EXPT	Gold Product Support Services, Expert OMS Suite

	ClearSight Analyzer
Model Number	**Description**
CSN/CSA-1000	ClearSight Analyzer Software
CSN/CSA-1000CD	ClearSight Analyzer Software on CD
CSN/CSA-1045	W/IP Multicast/History Rptr/Packet Gen
CSN/CSA-1045CD	CSN/CSA-1045CD,CSA W/IP Multicast/History Rptr/Packet Gen-CD
GLD-SW-1000	Gold Product Support Services, 1 Year software maintenance for CSA-1000
GLD-SW-1045	Gold Product Support Services, 1 Year software maintenance for CSA 1045

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**.