

OptiView™ Protocol Expert

Total integration.

Total control.

Total Network SuperVision.

Our OptiView Network Analysis Solution is a breakthrough in integrated portable and distributed monitoring and analysis hardware and software. It gives you a fast, complete view of your entire enterprise, from portable devices to workgroup analyzers to high-performance gigabit line-rate link analyzers – across multiple vendors. Only OptiView combines the analysis techniques of packet capture, statistical analysis and network discovery to deliver new speed. New ease of use. New depth of vision. New control to optimize the performance of WAN, LAN and wireless networks.

Standard key features

- Complete seven-layer packet capture, decode for Ethernet and Token Ring Networks
- Decode packets captured by any OptiView Analyzers
- Real-time monitoring of network traffic
- Expert Analysis System
- Cisco ISL, 802.1Q VLAN Traffic Analysis
- Powerful alarm system with 150 preset alarms that trigger notifications via email, paging and SNMP Trap
- Advanced multi-stage filtering enables triggering or capturing of specific events
- Decodes more than 250 protocols

OptiView™ Protocol Expert Plus adds:

- Control of remote OptiView Protocol Expert Plus and OptiView Link Analyzers while monitoring local traffic activities
- Multiple user access level privileges
- Packet editing and creation
- Replay of captured packet file and traffic pattern generation to load network segment

VoIP Option:

- Support H.323, Cisco SCCP, SIP and other VoIP related protocols
- User definable “Quality Grades” and alarm threshold for real-time QoS assessment: R-Factors, Jitter, Packet Drop and Setup Time
- Real-time call and channel parameter summary table for more than 2000 calls
- Audio playback and store as .wav file

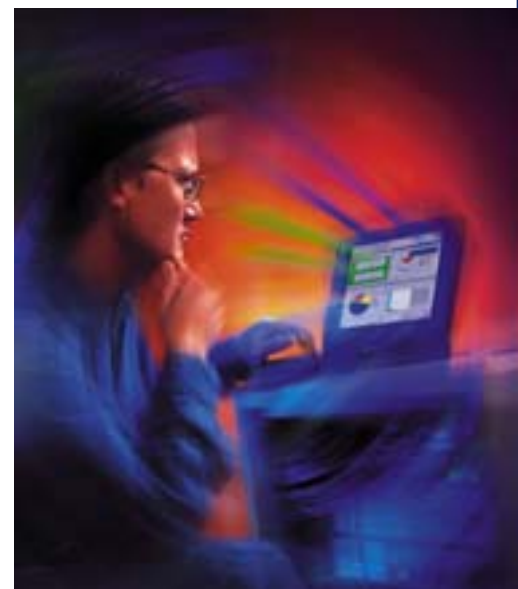
OptiView Protocol Expert is a Windows-based (2000/NT/XP) application that provides seven-layer visibility to your network. Protocol Expert provides comprehensive information about your network for quick problem detection and resolution. With extensive decodes and expert analysis, Protocol Expert allows you to easily identify and solve tough problems on switched segments, including those on Inter-switch Links.

OptiView Protocol Expert can be directly launched from OptiView™ Console. OptiView Console can auto-discover device name to network address correlation information and pass it to the Protocol Expert’s name table. When analyzing traffic captured by remote OptiView Analyzers, DNS or IPX user names will be shown in place of MAC or IP addresses for quicker packet source identification and reduction in troubleshooting time.

OptiView Protocol Expert Plus software adds a sophisticated traffic generation function, and the ability to remotely monitor one or more OptiView Protocol Expert Plus and OptiView Link Analyzers. This distributed analysis feature allows users to see activities on other parts of the network maintaining visibility of activities on the local segment. It also facilitates collaboration between IT staff to speed isolation of tough problems.

OptiView Protocol Expert Plus can remotely control the OptiView Link Analyzer, which offers full line-rate traffic monitoring, alarm and packet capture even on full-duplex Gigabit Ethernet links. Together, they provide the timing accuracy and performance required to solve tough problems such as slow application response or poor quality of service on highly utilized switch links.

Add the **VoIP Option** to troubleshoot VoIP call setup problems in Cisco AVVID, SIP or H.323 based VoIP deployment. Use the OptiView Link Analyzer and OptiView Protocol Expert Plus for the real-time QoS assessment of multiple VoIP calls.



Protocol analysis for in-depth troubleshooting

Comprehensive network monitoring

OptiView Protocol Expert provides seven-layer packet decodes and real-time network health statistics. Many network vital signs can be monitored such as:

- Utilization and error rate
- Frame size distribution
- Protocol distribution
- Top senders/receivers
- Conversation matrices
- VLAN traffic analysis
- Expert analysis
- Application response time analysis

Advanced Packet Decode and Filtering

OptiView Protocol Expert decodes packets captured by OptiView™ Analyzers. Multiple sessions of the packet decode window can be opened simultaneously. Traffic analysis tools, such as conversation matrix and protocol mix view can be used to help quickly narrow down packets of interest. Advanced filters and display filters are easy to set up, using a combination of protocol types, source/destination addresses, TCP/UDP port numbers and bit patterns.

Powerful alarm system

The OptiView Protocol Expert offers 150 pre-defined alarm conditions to effectively trap abnormal or intermittent problems. Custom alarm conditions are easily created using capture filters and OptiView Protocol Expert's unique custom counter feature. Multiple thresholds can be set for each alarm condition to trigger different actions based on severity.

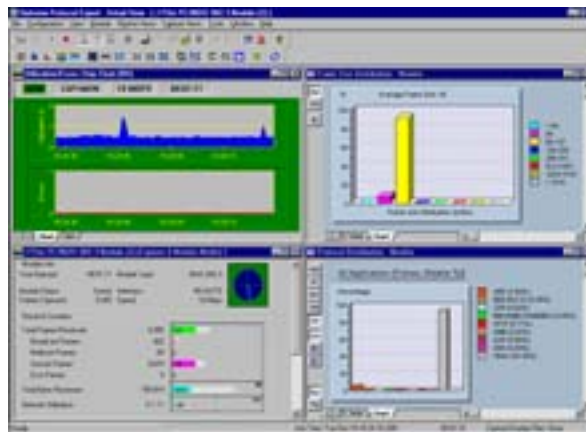
The actions include:

- Saving alarm messages into a log file
- Restarting a monitoring or capture session
- Stopping and saving a capture session
- Sending email or paging notification
- Sending an SNMP trap
- Launching an application program

Data storage and reporting

The traffic analysis results from monitoring or packet decoding, such as conversation matrix or protocol mix, can be exported to comma-separated (CSV), or saved as bitmap (BMP) file formats.

The data logging function can store key traffic utilization and error statistics, and data sampled at user defined intervals over a long period of time. A Microsoft Excel® report template is available for quick graphical report generation from the stored data.



Detail View shows multiple network health statistics simultaneously (by simply clicking on a resource in the Monitor View area of the main window).

| Variable | Sample Type | Warning Value | Fatal Value | Severity | Action | Filter | Enabled |
|---------------------------|-------------|---------------|-------------|----------|-----------|--------|---------|
| # BROADCAST Packets | Bytes | 500 | | Normal | Message | | |
| # BROADCAST Data Bytes | Bytes | 10000 | | Normal | Message | | |
| # BROADCAST IP Packets | Bytes | 500 | | Normal | Message | | |
| # BROADCAST IP Data Bytes | Bytes | 10000 | | Normal | Message | | |
| # PING Packets | Bytes | 500 | | Normal | Message | | |
| # PING Data Bytes | Bytes | 1000 | | Normal | Send Trap | | |
| # ICMP Packets | Bytes | 10000 | | Normal | Message | | |
| # ICMP Data Bytes | Bytes | 500 | | Normal | Log File | | |
| # TCP RST Packets | Bytes | 10000 | | Normal | Send Trap | | |
| # TCP Packets | Bytes | 5000 | | Normal | Message | | |

Alarm Editor allows multiple levels of alarm actions to be set for each of the 150 different preset alarm conditions based on severity.



Advanced Filter conditions can be easily set to capture only packets of interest or to specify a packet from a large amount of captured data.

Expert Analysis speeds up troubleshooting

The Expert View of OptiView Protocol Expert automatically detects problems while monitoring real-time traffic, or analyzing captured packets collected by OptiView Protocol Expert or the OptiView™ Analyzers.

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.

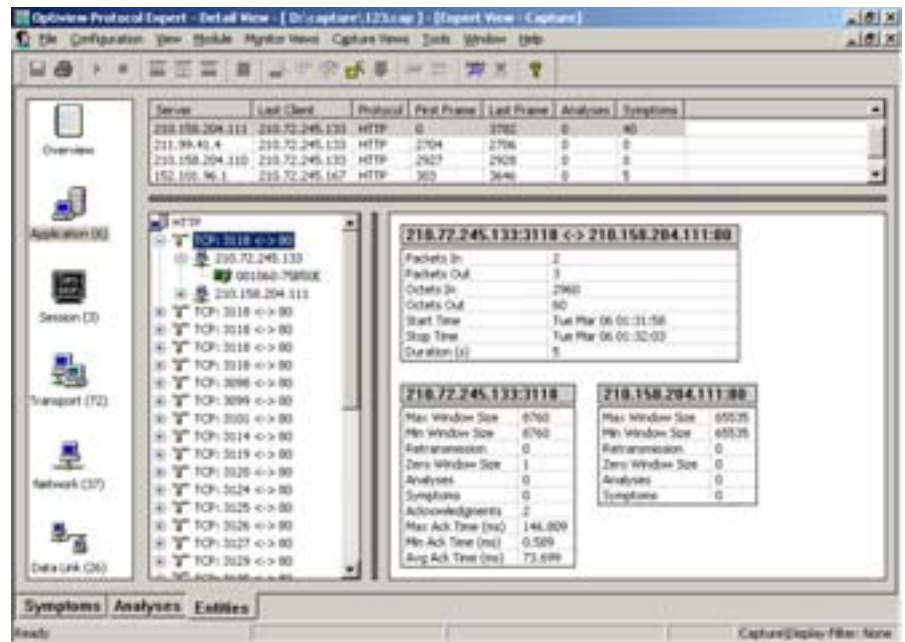
The Expert System will identify symptoms such as:

- **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

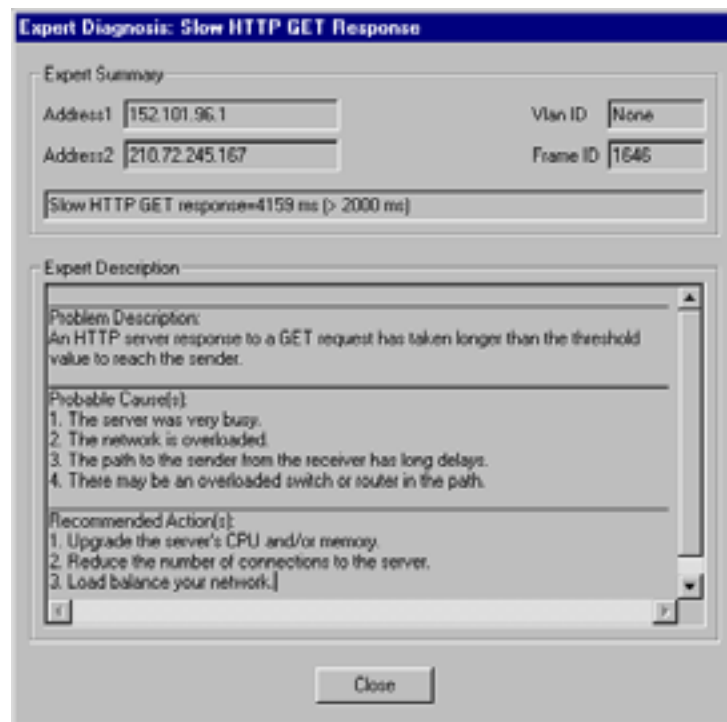
Double clicking on the Expert Symptom button displays the Expert Diagnosis window that provides a description of the station symptom, a probable cause and recommended action(s). Click on any of the stations listed in the Expert View to get a detailed view of the traffic captured.

Integrated Alarm System

The Expert System is integrated into OptiView Protocol Expert's alarm system to trigger necessary actions. Problems detected by the Expert System can trigger a Stop and Auto-Save of a captured session. The Traffic that caused the problem is stored and available for detailed analysis.



Expert View detects problem spots, categorizes the problem types and provides device level analysis for quick problem isolation.



Expert Diagnosis provides a description of the problem detected, possible cause(s) and recommended corrective actions.

OptiView™ Protocol Expert Plus

Key features:

Contains all functions of OptiView Protocol Expert and

Remote Access

- Peer-to-peer distributed analysis architecture
- Integrated portable and distributed analysis
- Four levels of password protected, user-access security
- Optional packet encryption for additional security when communicating over non-secure network links

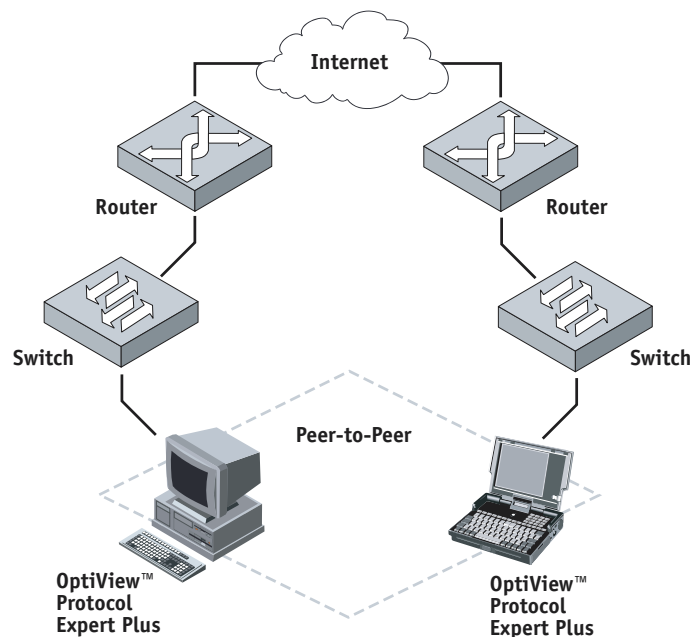
Traffic Generation

- Traffic pattern generation speed can be specified by frame rate, percentage of utilization, or packet gap
- Protocol templates are available for creating quick, custom traffic patterns
- Flexible packet editor allows you to add "bad" packets for testing your network's response
- Automatically generates CRC and recalculates checksum during packet editing or generation
- Supports burst count and auto-sequence number generation to send traffic streams for packet loss and out-of-sequence testing
- Retransmits previously captured real-time traffic to test network response under "real world" load

Integrated portable and distributed analysis

OptiView Protocol Expert Plus can analyze traffic monitored by one or more remote units or OptiView Link Analyzers while maintaining visibility of local traffic. Unlike other distributed analysis platforms that use a console-agent architecture,

OptiView Protocol Expert Plus uses a unique peer-to-peer architecture to conduct distributed monitoring while allowing mutual monitoring between peers. Network engineers in the field can collaborate with peers in the IT center while troubleshooting network problems.



Each copy of OptiView Protocol Expert Plus can monitor remote stations and monitor the output from the SPAN port on the local switch. (Assuming that the Switch will allow the software to communicate through the SPAN port)



OptiView Link Analyzer (OPV-LA) with a 8-port Fiber Tap (FTAP-8M)

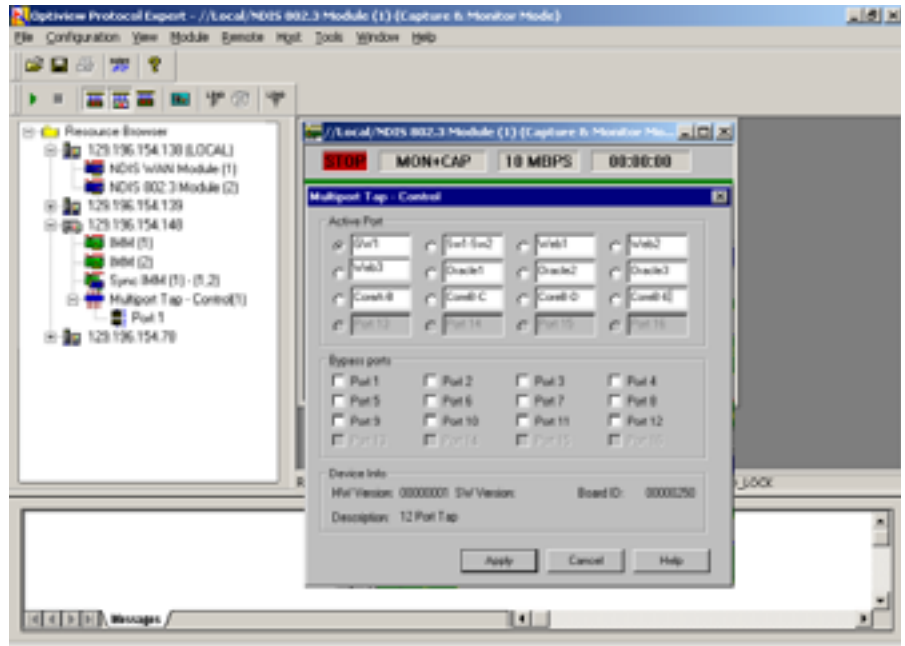
Multi-port taps offer more flexibility

Fluke Networks offers multi-port copper and fiber taps that provide access to traffic on multiple switch lines. When a multi-port tap is connected to an OptiView Link Analyzer, the switch links monitored by the taps can be remotely selected from OptiView Protocol Expert Plus. Just one OptiView Link Analyzer can monitor up to 16 100/1000 Mbps fiber links or 12 10/100 Mbps copper links. Combining this flexible hardware architecture with the real-time expert analysis feature of OptiView Protocol Expert Plus software, it is easy and economical to isolate problems on a switched Ethernet network.

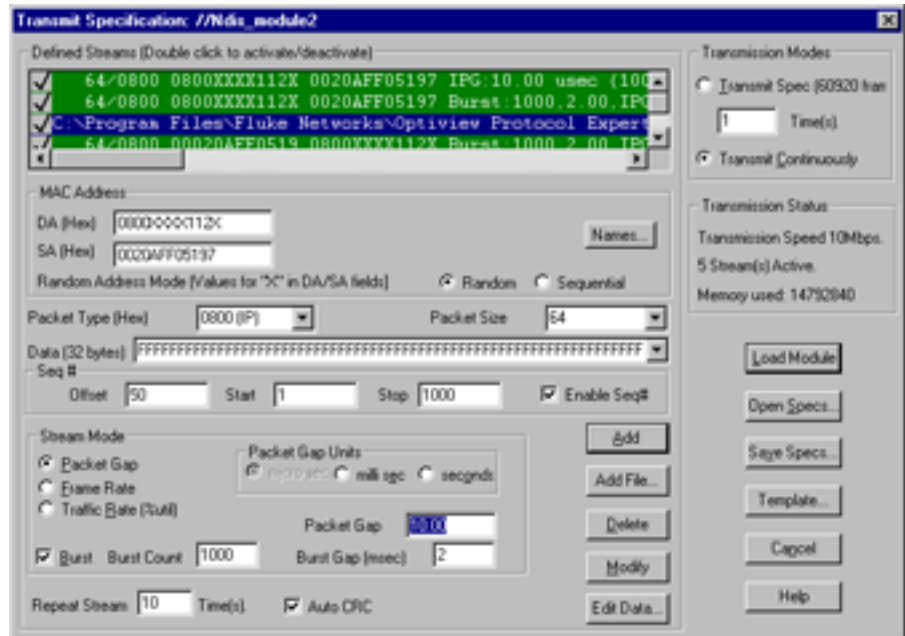
Sophisticated Traffic Generator reviews hidden problems

When utilization is low, the bandwidth and resources available can mask most network problems. OptiView Protocol Expert Plus can generate traffic by replaying captured data streams to review hidden problems before applications are deployed.

Predefined protocol templates are available for quick traffic pattern creation. Custom packets can be created from scratch, or by editing captured packets. For precise inter-packet time gap or utilization control to simulate live traffic, a packet stream can be loaded onto the OptiView Link Analyzer hardware utilizing the line-rate traffic generation feature in its ASIC based interface.



Remote selection of port monitored through a Multi-port Tap that is connected to OptiView Link Analyzer (IP address 129.196.154.148).



Traffic Generation configuration window with data stream consists of several repetitions of frames and two different previously captured traffic patterns (capture files).

Voice over IP Option

Key features:

- Supports decoding of a wide range of VoIP protocols, including ASN.1, MGCP, SGCP, H.323, Cisco SCCP, SIP et al
- Real-time view of key QoS parameters by completed calls, active calls, and calls initiated using H.323, Cisco Skinny and SIP
- User-definable “Quality Grades” for R-Factor, Jitter, Packet Loss, and Setup Time
- Real-time bar charts showing calls that fall within “Quality Grades” for each QoS parameter
- Calls exceeding a user-definable threshold can trigger alarm
- Easy to configure capture or display filters from call view to capture VoIP packets between two stations participating in the call
- Export call and channel information to CSV file
- VOIP Call Playback Audio data in VOIP calls that use PCMU or PCMA codec can be saved as .wav files for playback

Real-time VoIP QoS Analysis with Quality Grading

Service providers need to ensure QoS meets Service Level Agreements (SLA). By monitoring traffic in each Point of Presence (POP), the VoIP option and OptiView™ Protocol Expert Plus work with the OptiView™ Link Analyzer. You will see real-time QoS assessment on every 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 calls in each grade are clearly shown in a tabular view to allow quick identification of the route taken and the gateway involved, allowing you to troubleshoot quickly. The R-Factor is based on ITUG.107/G.108 offering near MOS assessment.

| Protocol | Stream ID | User R-Factor | Network R-Factor | RTCP | RTCP Dropped | Status | Source Address | Destination Address |
|----------|-----------|---------------|------------------|------|--------------|----------|----------------|---------------------|
| H323 | 1762 | 96 | 47 | 137 | 0 | Complete | 192.168.1.190 | 192.168.1.43 |
| H323 | 4630 | 96 | 47 | 137 | 0 | Complete | 192.168.1.190 | 192.168.1.43 |
| H323 | 2998 | 28 | 29 | 136 | 4 | Complete | 192.168.1.190 | 192.168.1.43 |
| H323 | 5176 | 96 | 47 | 137 | 0 | Complete | 192.168.1.190 | 192.168.1.43 |
| H323 | 5176 | 96 | 47 | 137 | 0 | Complete | 192.168.1.190 | 192.168.1.43 |
| H323 | 3884 | 96 | 47 | 137 | 0 | Complete | 192.168.1.190 | 192.168.1.43 |
| H323 | 1336 | 96 | 47 | 137 | 0 | Complete | 192.168.1.190 | 192.168.1.43 |
| H323 | 9622 | 96 | 47 | 137 | 0 | Complete | 192.168.1.190 | 192.168.1.43 |
| H323 | 9607 | 96 | 47 | 137 | 0 | Complete | 192.168.1.190 | 192.168.1.43 |
| H323 | 14 | 0 | 0 | 0 | 0 | Complete | 192.168.1.190 | 192.168.1.43 |

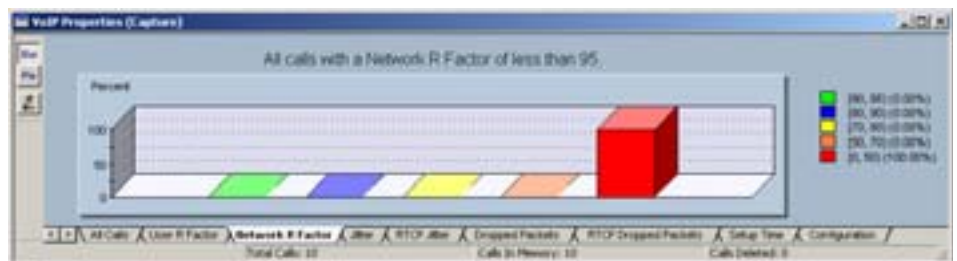
All Call View shows key QoS metrics for all calls monitored. Buttons on the left select the type of call displayed: completed calls, active calls, and calls initiated using H.323, Cisco Skinny and SIP.

Jitter Threshold Range Editor

| | | | |
|---------|----------|----------|---|
| Range 1 | [1000] | [∞] | <input checked="" type="checkbox"/> Enabled |
| Range 2 | [600] | [1000] | <input checked="" type="checkbox"/> Enabled |
| Range 3 | [200] | [600] | <input checked="" type="checkbox"/> Enabled |
| Range 4 | [100] | [200] | <input checked="" type="checkbox"/> Enabled |
| Range 5 | [10] | [100] | <input checked="" type="checkbox"/> Enabled |

Buttons: OK, Cancel, Restore Defaults

Jitter Threshold Range Editor allows users to define “Quality Grades” to rank call QoS performance.



User R-Factor summarizes the User R-Factor quality grading of all monitored calls. Detailed VoIP related parameters for calls that fall within a quality grade can be reviewed by double clicking on the respective bars on the chart. Similar charts are available for Network RTP Jitter, R-Factor, RTP Dropped Packets, RTCP Jitter, RTCP Dropped Packets and Call Setup Time.

Performance you can rely on

When conducting a QoS analysis of VoIP traffic, the measurement device must have accurate timing and keep up with high traffic rates regardless of the load size. Standard NICs may not have the accuracy and performance for the task, especially when the network is under high load. The OptiView Link Analyzer uses custom ASIC to provide nano-seconds of timing resolution and real-time monitoring without missing a packet, even at high utilization.

Solve Call Setup problems

The VoIP option provides a detailed decode of the most commonly used VoIP protocols. 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 QoS Problem Alarm

The VoIP option's QoS analysis is integrated into its powerful alarm system. Calls exceeding alarm conditions can trigger an auto-save of captured data to ensure that problem traffic patterns are available for detailed analysis.

For instance, when a call exceeds the Jitter threshold by a large number, the VoIP Option stops the capture session and saves the packets that displayed the problem.

H.323 Detail Call View

This call has completed

| | | | |
|--------------------------|-------------------|-------------------------------|---------------------------|
| Frame ID : | 5 | Destination Reference Value : | 3912 |
| Source Reference Value : | 3912 | Destination Address : | 192.168.1.43 |
| Source Address : | 192.168.1.190 | Destination Q.931 Port : | 1720 |
| Source Q.931 Port : | 1040 | Destination H.245 Port : | 1059 |
| Source H.245 Port : | 1041 | Destination Number : | Unknown |
| Source Number : | Unknown | Destination Alias : | Unknown |
| Source Alias : | Unknown | Destination H.323 Ver : | 1 |
| Source H.323 Ver : | 1 | Destination Product : | Intel Video Phone |
| Source Product : | Intel Video Phone | Product Version : | 2.0 |
| Product Version : | 2.0 | Fast Start : | No |
| Start Time : | 3/1/1999 23:16:40 | Release Code : | 16 (Normal call clearing) |
| Stop time : | 3/1/1999 23:17:27 | | |
| Setup Time (ms) : | 194 | | |

[View Channel Details](#) [Single Call Toolset Filter](#)

H.323 Detail Call View shows real-time key call setup parameters using H.323 protocols. Similar tables are available for calls initiated using SIP and SCCP.

H.323 Channel Details (Capture) [Total Entries: 4]

| Channel | Dst Addr | Dst Port | Src Addr | Src Port | Sync Source | Packet Count | Byte Count | Dropped | Codec | Jitter (ms) | Min Jitter |
|---------|--------------|----------|--------------|----------|-------------|--------------|------------|---------|-------|-------------|------------|
| Audio | 192.168.1.43 | 1060 | 192.168.1.19 | 1042 | 4281729902 | 236 | 32568 | 0 | G.723 | 101.250000 | 40.625000 |
| Audio | 192.168.1.19 | 1042 | 192.168.1.43 | 1060 | 4259060512 | 127 | 17526 | 0 | G.723 | 18.625000 | 18.625000 |
| Video | 192.168.1.43 | 1062 | 192.168.1.19 | 1044 | 1162924873 | 80 | 29556 | 0 | H.263 | 16.066667 | 0.000000 |
| Video | 192.168.1.19 | 1044 | 192.168.1.43 | 1062 | 575796467 | 80 | 26586 | 0 | H.263 | 0.722222 | 0.000000 |

SCCP Channel Detail View shows key VoIP parameters associated with each logical channel used by a multimedia signal for each monitored call.

ALARM EDITOR

MAC | Application Response | Network | Token Ring | VoIP | Expert

| Variable | Threshold Val | Codec Type | Severity | Actions | Enabled |
|---------------------|---------------|------------|----------|-----------|-------------------------------------|
| Setup Time | 200 | N/A | Normal | Message | <input type="checkbox"/> |
| Jitter | 100 | All Codecs | Normal | Message | <input type="checkbox"/> |
| Packet Dropped | 5 | All Codecs | Normal | Message | <input type="checkbox"/> |
| RTCP Jitter | 100 | All Codecs | Normal | Message | <input type="checkbox"/> |
| RTCP Packet Dropped | 5 | All Codecs | Normal | Message | <input type="checkbox"/> |
| User R Factor | 50 | All Codecs | Normal | SNMP Trap | <input checked="" type="checkbox"/> |
| | 50 | All Codecs | Normal | Pager | <input checked="" type="checkbox"/> |
| Network R Factor | 50 | All Codecs | Normal | SNMP Trap | <input checked="" type="checkbox"/> |

OK Cancel Help

VoIP Alarm can trigger different actions based on the severity of a QoS violation. Different thresholds can be set for each type of Codec supported.

OptiView™ Protocol Expert Specifications

Minimum system requirements

| Item | Description | | | |
|-------------------|--|-------------------|---------|----------------|
| Processor | Minimum: 233 MHz for 10/100 MB/sec Ethernet and Token ring Recommended: 1 GHz for 1000 MB/sec Ethernet | | | |
| Operating system | Windows® NT Service Pack 6 or higher (Administration privilege required) Windows® 2000 Windows® XP | | | |
| Disk space | 25 MB for installation | | | |
| CD ROM | Required for installation | | | |
| Display | 800 x 600 (SVGA) | | | |
| Network interface | NDIS 10/100/1000 Mbps Ethernet Adapters or NDIS 4/16 Mbps Token Ring Adapter and must be in promiscuous mode (not all Token Ring Adapters are supported) | | | |
| Web browser | Internet Explorer 5.5 or higher or Netscape 4.0 or higher for Link Analyzer Web access | | | |
| Memory | Capture Buffer Size - Local or Remote | Pentium Processor | RAM | Virtual Memory |
| | 16 MB | PII | 64 MB | 64 MB |
| | 32 MB | PII | 128 MB | 500 MB |
| | 64 MB | PIII | 256 MB | 600 MB |
| | 128 MB | PIII | 512 MB | 700 MB |
| | 256 MB | PIII | 1000 MB | 1000 MB |

Traffic Analysis Statistics available

| Metric | Summary View (Single View) | Detail View (Multiple Views) | Capture View (Static Data) |
|--|----------------------------|------------------------------|----------------------------|
| MAC Statistics | Y | Y | N |
| Utilization/Errors Strip Chart | Y | Y | N |
| Frame Distribution | Y | Y | Y |
| Protocol Distribution | Y | Y | Y |
| MAC Layer Host Table | Y | Y | Y |
| Network Layer Host Table | Y | Y | Y |
| Application Layer Host Table | Y | Y | Y |
| MAC Layer Host Matrix | Y | Y | Y |
| Network Layer Matrix | Y | Y | Y |
| Application Layer Matrix | Y | Y | Y |
| VLAN | Y | Y | Y |
| Address Map | Y | Y | Y |
| Duplicate Address | Y | Y | Y |
| Expert View | N | Y | Y |
| Application Response Time | Y | Y | Y |
| Packet Summary (real-time protocol decode) | Y | Y | N |
| Ring Statistics (Token Ring only) | Y | Y | Y |
| Capture View (protocol decode) | N | Y | Y |
| VoIP View (VoIP Option Only) | N | Y | Y |

Y = Data View Supported

N = Data View Not Supported

VoIP QoS Metrics (available only with VoIP Option)

Cisco SCCP QoS metrics in Call Table View

| Field Name | Description |
|----------------------|---|
| FID | Frame ID of the first frame from which the conversation was detected. This field is useful when doing post capture analysis. If there is a need for in-depth analysis of a specific call, the first frame associated with the call can be quickly determined. |
| Caller Addr | IP address of the end point initiating the call |
| Caller Port | TCP port of the end point initiating the call |
| Caller Name | Caller's name |
| Caller Number | Phone number of the calling party |
| Callee Addr | IP address of the end point receiving the call |
| Callee Port | TCP port of the end point receiving the call |
| Callee Name | Callee's name |
| Callee Number | Phone number of the called party |
| Start Time | Time at which the call was started |
| Stop Time | Time at which the call was completed |
| Setup Time | Time that was taken for the call to be setup (the time taken from the start of the call until the phone rings) |
| SCCP Version | SCCP Protocol Version used in this call |
| Call Status | Status of the call. An active call has the status of "Setting up" or "Setup complete". A completed call has the status of "Setup failed", "Aborted", or "Complete". |

Cisco SCCP QoS metric in Channel Table View

| Field Name | Description |
|------------------------|--|
| Channel | Channel type: Audio, Video or Data |
| Src Addr | IP address of the caller |
| Src Port | UDP port of the caller |
| Dst Addr | IP address of the callee |
| Dst Port | UDP port of the callee |
| Sync Source | Synchronization Source. Internal number identifying the source |
| Packet Count | This value is calculated by the OptiView Protocol Expert VoIP Option |
| Byte Count | This value is calculated by the OptiView Protocol Expert VoIP Option |
| Dropped Packets | This value is calculated by the OptiView Protocol Expert VoIP Option |
| Codec | Codec/Decoder type. (DataType in H.245) |
| Jitter (ms) | Average Jitter in milliseconds. This value is calculated by the OptiView Protocol Expert VoIP Option. It uses the formula described in RFC 1889 to calculate jitter. |
| Min Jitter (ms) | Minimum Jitter in milliseconds. This value is calculated by the OptiView Protocol Expert VoIP Option. It uses the formula described in RFC 1889 to calculate jitter. |
| Max Jitter (ms) | Maximum Jitter in milliseconds. This value is calculated by the OptiView Protocol Expert VoIP Option. It uses the formula described in RFC 1889 to calculate jitter. |
| Low Seq Num | Lowest Sequence Number. Lowest RTP sequence number seen. |
| High Seq Num | Highest Sequence Number. Highest RTP sequence number seen. |

SIP QoS metrics in Call Table View

| Field Name | Description |
|----------------------|--|
| FID | Frame ID of the first frame from which the conversation was detected, i.e., the frame ID of the first INVITE message. |
| Call-ID | Globally unique ID to identify an SIP call. |
| Caller | SIP URL or other URI of the caller, i.e., the addr-spec in the "From" parameter. |
| Caller Name | Display name of the caller, i.e., the display name in the "From" parameter, if it exists. |
| Caller Tag | The tag of "From," if it exists. |
| Caller IP | The IP address of the initiator of the call. |
| Callee | SIP URL or other URI of the callee, i.e., the addr-spec in the "To" parameter. |
| Callee Name | Display name of the callee, i.e., the display name in the "To" parameter, if it exists. |
| Callee Tag | The tag of "To," if it exists. |
| Callee IP | The IP address of the receiver of the call. |
| SIP Ver | The version of SIP being used. |
| Start Time | Time at which the call was started, i.e., the time of first INVITE message of the call. |
| Stop Time | Time at which the call was complete. |
| Setup Time | Time that was taken for the call to be setup. This is the duration from "INVITE" to 180 or 183 (ringing) response if available, or to 200 response otherwise. If none of these responses are received, this field value is set to "Unknown." |
| Response Code | The status code from the latest response. This is useful to identify the cause if setup fails. |
| Call Status | Status of the call. An active call has the status of "Setting up" or "Setup complete". A complete call has the status of "Setup failed," "Aborted" or "Call complete." |

H.323 QoS metrics in Call Table View

| Field Name | Description |
|------------------------------------|---|
| FID | Frame ID of the first frame from which the conversation was detected. This field is useful when doing post capture analysis. If there is a need for in-depth analysis of a specific call, the first frame associated with the call can be quickly determined. |
| Source Reference Value | The Call Reference Value used by H.225.0 at the source side |
| Src Addr | The IP address of the initiator of the call |
| Src Q.931 Port | The Q.931 TCP port of the sender of the call |
| Src H.245 Port | The H.245 TCP port of the initiator of the call |
| Src Number | Phone number of the initiator of the call |
| Src Alias | An alias of the initiator of the call |
| Src H.323 Ver | The version of H.323 being used by the initiator of the call |
| Src Product | The product being used by the initiator of the call |
| Src Version | The product version being used by the initiator of the call |
| Destination Reference Value | The Call Reference Value used by H.225.0 at the destination side |
| Dst Addr | The IP address of the receiver of the call |
| Dst Q.931 Port | The Q.931 TCP port of the receiver of the call |
| Dst H.245 Port | The H.245 TCP port of the receiver of the call |
| Dst Number | Phone number of the receiver of the call |
| Dst Alias | An alias of the receiver of the call |
| Dst H.323 Ver | The version of H.323 being used by the receiver of the call |
| Dst Product | The product being used by the receiver of the call |
| Dst Version | The product version being used by the receiver of the call |
| Fast Start | Indicates whether or not Fast Start was used during call setup |
| Release Code | Code indicating the status of the call when it was completed |
| Start Time | Time at which the call was started |
| Stop Time | Time at which the call was completed |
| Setup Time | Time that was taken for the call to be setup |

H.323 and SIP QoS metrics in Channel Table View

| Field Name | Description |
|-----------------------------------|--|
| Channel | Channel type: Audio, Video or Data |
| Dst Addr | The destination IP address |
| Dst Port | The destination UDP port |
| Src Addr | The source IP address |
| Src Port | The source UDP port |
| Syn Source | Synchronization source. Internal number identifying the source |
| SID | Session Identifier. (Session ID in H.245) |
| Direction | Stream origination. Forward = stream originating at the caller Reverse = stream originating at the callee |
| Packet Count | This value is calculated by the OptiView Protocol Expert VoIP Option |
| Byte Count | This value is calculated by the OptiView Protocol Expert VoIP Option |
| Dropped Packets | This value is calculated by the OptiView Protocol Expert VoIP Option |
| Codec | Codec/Decoder type. (DataType in H.245) |
| Jitter (ms) | Average Jitter in milliseconds. This value is calculated by the OptiView Protocol Expert VoIP Option. It uses the formula described in RFC 1889 to calculate jitter. |
| Min Jitter (ms) | Minimum Jitter in milliseconds. This value is calculated by OptiView Protocol Expert VoIP Option. It uses the formula described in RFC 1889 to calculate jitter. |
| Max Jitter (ms) | Maximum Jitter in milliseconds. This value is calculated by the OptiView Protocol Expert VoIP Option. It uses the formula described in RFC 1889 to calculate jitter. |
| Low Seq Number | Lowest Sequence Number. Lowest RTP sequence number seen |
| High Seq Number | Highest Sequence Number. Highest RTP sequence number seen |
| RTCP Packet Count | Real-time Transport Control Protocol (RTCP) Packet Count |
| RTCP Byte Count | RTCP Byte Count |
| RTCP Rtp Packet Count | Real-time Transport Control Protocol (RTCP) RTP Packet Count |
| RTCP Rtp Byte Count | RTCP RTP Byte Count |
| RTCP Jitter (ms) | RTCP reported jitter. Average reported RTCP interarrival jitter |
| RTCP Min Jitter (ms) | RTCP reported minimum jitter. Minimum reported interarrival jitter |
| RTCP Max Jitter (ms) | RTCP reported maximum jitter. Maximum reported interarrival jitter |
| RTCP High Seq Num | High Sequence Number reported by RTCP |
| RTCP Sender Report Count | Number of RTCP Sender Reports seen |
| RTCP Receiver Report Count | Number of RTCP Receiver Reports seen |
| RTCP Source Description Count | Number of RTCP Source Descriptions seen |
| RTCP Goodbye Count | Number of RTCP Goodbyes seen |
| RTCP Application Definition Count | Number of RTCP Application Definitions seen |
| RTCP Unknown Report Count | Unknown Report Count. Count of all other RTCP reports seen |
| RTCP CName | Canonical Name. (RTCP Source Description, CNAME field) |
| RTCP Name | User's Name. (RTCP Source Description, NAME field) |
| RTCP Email | User's electronic mail address. (RTCP Source Description, EMAIL field) |
| RTCP Phone | User's phone number. (RTCP Source Description, PHONE field) |
| RTCP Location | User's geographic location. (RTCP Source Description, LOCATION field) |
| RTCP Tool | Name of application or tool. (RTCP Source Description, TOOL field) |
| RTCP Note | Notice about the source. (RTCP Source Description, NOTE field) |

Protocols supported by OptiView Protocol Expert V5.0

| | | | | | |
|-------------------------|----------------------------|---------------------------|-------------------|---------------------|--|
| AppleTalk Phase 2 | Codec | FM | | | NNTP |
| AARP | CellB | NC | IPX/SPX | MPLS | NTP |
| ADSP | G.711 | NetBEUI | Diagnostic | CR-LDP | OSPF |
| AEP | G.721 | NetBIOS | Error | RSVP-TE | PH |
| AFP | G.722 | SC | IPX | Oracle | POP3 |
| ASP | G.723 | XID | IPX BCAST | TNS (TCP/IP only) | PORT MAPPER |
| ATP | G.728 | IETF | IPX EIGRP | SQLNET | RARP |
| AURP | G.729 | MGCP | IPX Ping | PPP Suite | RIP (Version 2) |
| DDP | H.261 | RTCP | IPX RIP | PPPCHAP | RPC |
| DDP EIGRP | H.263 | RTP | IPX WAN | PPPIPCP | RTSP |
| LAP | JPEG | RTSP | NBCAST | PPPIPX | SGCP |
| NBP | MPEG (v1, v2) | SGCP | NCP | PPPLCP | SLP |
| PAP | PCMA | SIP | NDS | PPPNBFCP | SMTP |
| RTMP | PCMU | Intel | NetBIOS | PPP over Ethernet | SNMP (v1, v2, v3) |
| ZIP | DECnet Phase IV | MGCP | NLSP | Sybase | TCP |
| Banyan Vines | CTERM | MTP2 | Packet Burst | TDS (TCP/IP only) | TELNET |
| VARP | DAP | MTP3 | SAP | TCP/IP Suite | TFTP |
| VICP | DRP | RTSP | Serialization | ARP | TPKT |
| VIP | FOUND | SCCP | SPX | BGP (Version 4) | UDP |
| VIPC | LAT | SIP | SPX II | BOOTP | Unix Remote Services (lpr, rcp, rexec, rlogin, rsh) |
| VRPC | LAVC | TCAP | Watchdog | CharGen | |
| VRTP | MOP | IP Multicast Suite | ISO | DHCP | VRRP |
| VSPP | NICE | DVMRP | CLNP | Discard | WebNFS |
| Bridge Protocols | NSP | MOSPF | CONP | DNS | WhoIs |
| BPDU | Extreme | PIM-DM | ISIS | Echo | XDMCP |
| GARP (802.1p) | EDP | PIM-SM | ISIS | EGP | XDR |
| GMRP | ESRP | RSVP | ISO | Finger | Xwindows |
| GVRP | Fujitsu Suite | IpSec/Security | LOA | FTP | VPN |
| IEEE 802.1D | FNA | AH | LOA | GGP | L2TP |
| IEEE 802.1Q VLAN | LNDFC | ESP | MAC Layer | Gopher | LDP |
| Cisco | H.323v2 and V4 | ISAKMP | Ethernet type II | HTTP | PPPOEDS |
| CDP | ASN.1 | KERBEROS | IEEE 802.1x | HTTPS | PPPOESS |
| DISL | GK DISC | RADIUS | IEEE 802.2 | ICMP | XNS |
| EIGRP | H.225.0 | SOCKS | IEEE 802.3 | Ident | Echo Protocol |
| HSRP | H.245 | SSH | IEEE 802.5 | iFCP | Error Protocol |
| IGRP | H.450.1 | TACACS | IEEE SNAP | IGMP | IDP |
| ISL | Q.921 | TLS | Loopback | IMAP | NetBIOS over SPP |
| VTP | Q.931 | IPV6 | MAC Control Frame | IMSP IP | PEP |
| RUDP | RAS | DHCPng | SNAP | iSGSI | RIP |
| SCCP | T.120 | ICMPng | Microsoft | LDAP | SPP |
| SSP | T.38 | IDRng | NMPI | MIME | Other |
| | IBM & SNA Suite | IPng | SMB | Mobile-IP (A11) | CCMAIL |
| | 3270 | OSPFng | SMB+ (CIFS) | MOUNT | Fluke Networks RSP |
| | FDC | RIPng | WebNSF | NetBIOS | Lotus Notes |
| | FID2 | RSVPng | | NFS | iFeP Mobile-IPT-38 |
| | | | | NIS | XWIN |

Highlighted protocols are supported with the purchase of the VoIP option only.



Ordering Information

| Model | Description |
|-------------|--|
| OPV-PE/PRO | OptiView™ Protocol Expert software |
| OPV-PE/PLUS | OptiView™ Protocol Expert Plus software (adds remote control and traffic generation functions) |
| OPV-PE/VOIP | VoIP Option for OptiView™ Protocol Expert |
| OPV-PE/EP | Upgrade from OPV-PE/PRO to OPV-PE/PLUS |
| OPV-LA | OptiView™ Link Analyzer |

Note: OPV-LA requires OPV-PE/PLUS to operate.

In-Line Taps and Accessories

| Model | Description |
|----------|--|
| TAP-1G | Single-Port Tap, 1000 BASE-T, RJ-45 |
| TAP-1P | Single-Port Tap, 10/100Mbps Ethernet, RJ-45 |
| TAP-12 | 12-Port Copper Tap, 10/100Mbps Ethernet RJ-45 |
| FTAP-8M | 8-Port Fiber Tap, Multi-mode, SC connector |
| FTAP-8S | 8-Port Fiber Tap, Single-mode, SC connector |
| FTAP-101 | Single-Port Tap, Multi-mode Fiber, SC connector |
| FTAP-102 | Single-Port Tap, Single-mode Fiber, SC connector |
| FTAP-003 | Rack mount kit for three Single-Port Fiber Taps |
| FTAP-012 | Rack mount kit for twelve Single-Port Fiber Taps |
| OPV-LX | 1000 BASE-LX GBIC MAU |
| OPV-T | 1000 BASE-T GBIC MAU |

Our Gold SuperVision Support plans give you exclusive services and 24/7 technical assistance.

Sign up for our Gold SuperVision Customer Support plan and you'll enjoy outstanding privileges to protect and add value to your investment in Fluke Networks equipment. They include unlimited tech assistance seven days a week, 24 hours a day via phone or at our web site support center. Repairs on covered items and overnight exchange/loaner units for uninterrupted service. Free software upgrades. Scheduled calibration and performance verification services. 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.

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.flukenetworks.com/contact.

©2003 Fluke Corporation. All rights reserved.
Printed in U.S.A. 8/2003 1609415 D-ENG-N Rev F