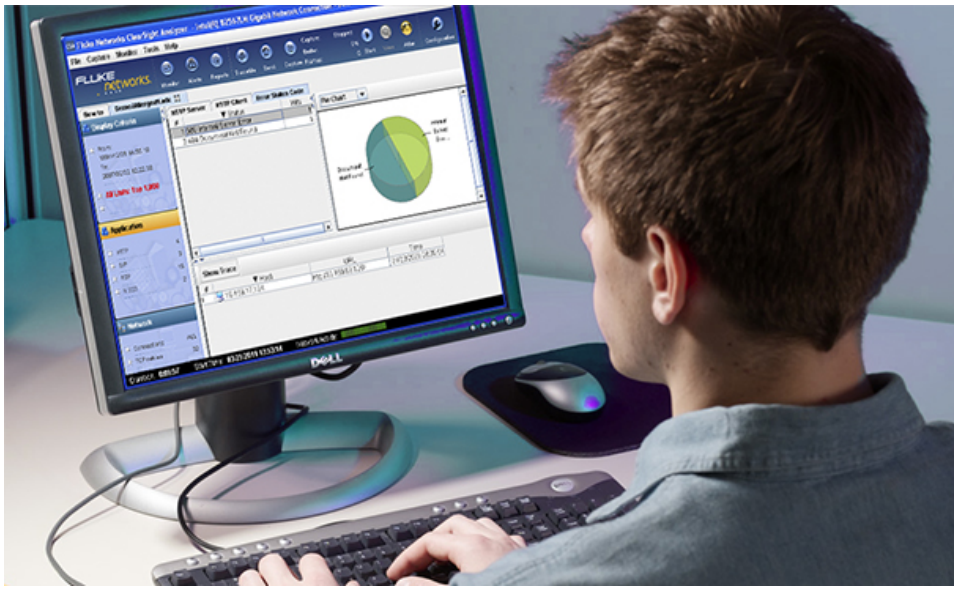
ClearSight™ Analyzer

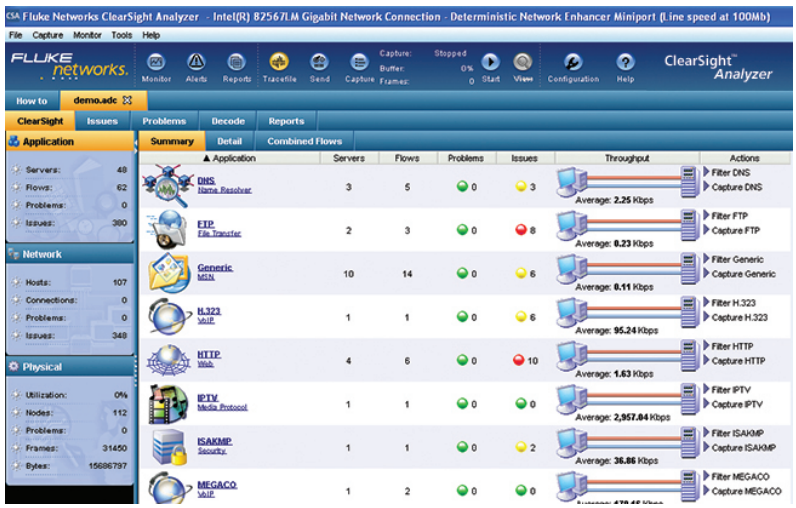
The award–winning ClearSight™ Analyzer (CSA) offers advanced application–centric monitoring and performance analysis, enabling enterprise Network Administrators and Engineers to maintain, diagnose, and resolve application and network performance issues in multi–protocol network environments. CSA supports most of the commonly used protocols, and users can import Wireshark decodes to take advantage of decodes contributed from the open–source community — making CSA the most versatile application analysis tool in the market.



Application–centric analysis software delivering answers for application performance problems

Key Features

- Application–centric analysis that automatically analyzes application flows with intuitive drill down to identify the root cause of performance issues
- Real–time application performance monitoring with alarms for problem identification
- Time–based analysis for trace files up to 4 Gigabytes to quickly identify relevant packets for the application–centric view
- Real time statistics, bounce charts and reports for flows on single or multiple segments — to see issues quickly
- Video and voice call status, QoS analysis and playback
- User customizable summary report
- Supports WireShark decode engine



Innovative application–centric analysis

Through a simple and intuitive front page, CSA presents a comprehensive, high–level application health overview of your network. From that framework, you can drill down to gain access to more detailed information. For example, CSA will recognize and analyze all flows of an HTTP application, display the number of servers, clients and throughput. With a simple click, you can then see each flow with a bounce chart and expert identification of the packets that caused the problem. This unparalleled level of control and visibility speeds time to application problem resolution and minimizes overall network downtime.

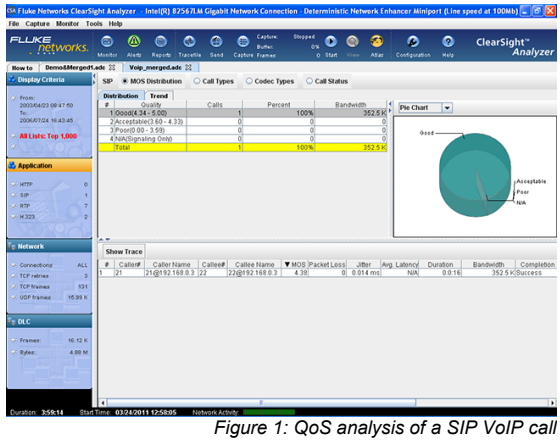


Figure 1: QoS analysis of a SIP VoIP call

Real-time monitoring with problem/ issue detection

The CSA Expert Alert function automatically detects communication faults from captured or monitored 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, either in real–time or from a trace file, are classified as issues (faults in the communication sequence) or problems (faults that exceed a threshold value) and are logged. Lists can be sorted by simply clicking on a column header. You can drill down to the associated flow causing the problem by right–clicking on an alert during post–capture analysis. Problems and issues can trigger email, pager, script, or SNMP trap actions.

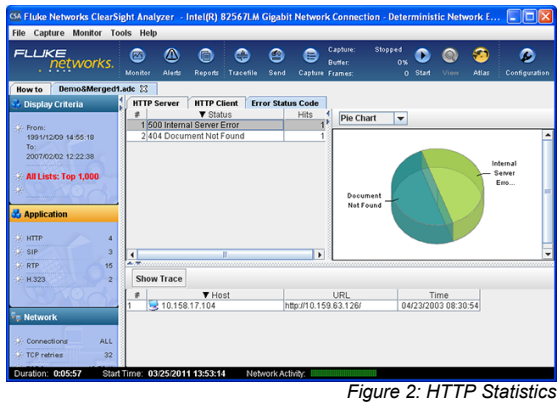


Figure 2: HTTP Statistics

Time–based analysis to identify problems quickly

Analyzing large capture files can be difficult because there is just too much information to sort through. CSA provides a time-based analysis of capture files providing detailed statistics and trending information. You can drill down in time to look at adjacent events during the time of interest. For video and voice traffic running SIP or H.323, the analysis engine can classify the video and voice RTP streams based on their quality score, MOS or VQFactor. It will provide detailed statistics of the SIP or H.323 call status and quality of calls. You can select one or more of the RTP streams to be extracted for detailed analysis or replay. Additional analysis is available for HTTP, listing tables clients by server or vice–versa along with specifc URLs accessed and error codes. With this analysis, users can identify the problems quickly, without drilling into packet decodes.

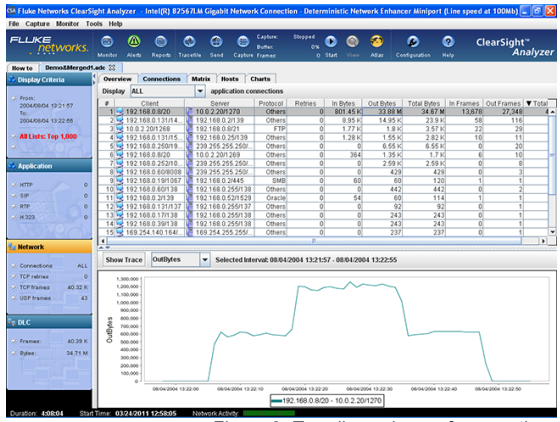


Figure 3: Trending volume of connections

Automatic bounce chart

CSA automatically creates bounce charts for each TCP flow identified. This graphically reveals the dynamics of packet flow between clients and servers without having to manually decode packets. Timing, direction of flow, and payload summary, are displayed while TCP or other errors are color coded for quick identification. It provides an extremely powerful way to understand protocol interactions between various network elements.

Unique multi–segment analysis

CSA supports most of the commonly used capture file formats. It can receive packets captured from up to four locations on the network and merge them to provide a multi–segment bounce chart. This allows timing issues to be isolated quickly by segment for root cause analysis. Combined with the powerful decode feature of CSA, this provides network engineers and application analysts the tools to end finger pointing.

Triple play ready

Speech quality parameters including packet loss, jitter, R value, and MOS are displayed graphically. Streaming video implemented by MPEG2 over UDP is supported. Support includes a complete set of functions, including decode, filter, problem definition with alerts, and a full set of reports – real–time, history, trace file, and voice quality. Content playback is supported in both real–time and post analysis.

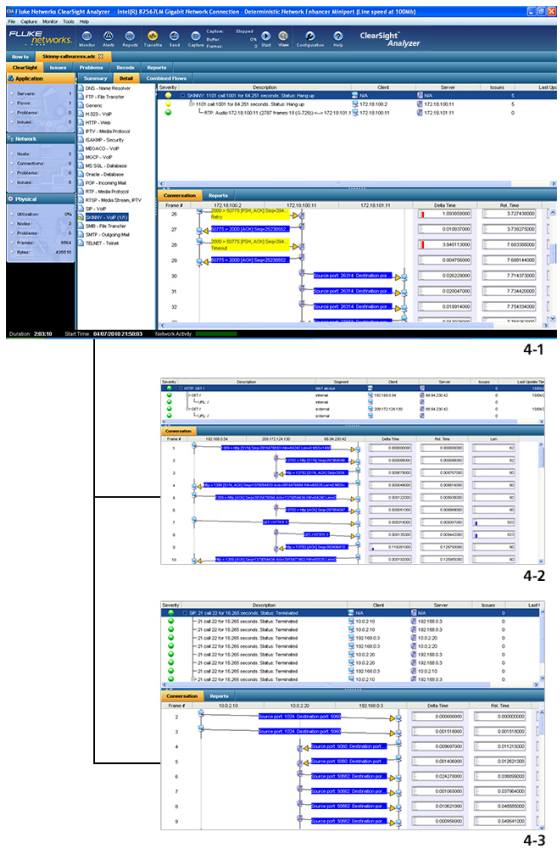


Figure 4-1: VoIP Multi–Segment Analysis — Figure 4-2: NAT Multi–Segment — Figure 4-3: SIP Multi–Segment

Content reconstruction and playback

You can recreate audio and video content from VoIP or video flows, either during real–time monitoring or from a trace file. In addition, Microsoft® Exchange® email, Fax over IP, instant messages and HTTPbased web pages can also be reconstructed. This is very valuable as proof of compliance violation or visualization of multimedia quality.

5-1

5-2

5-3

Figure 5-1: Video playback — Figure 5-2: Email Playback — Figure 5-3: Web Playback

Powerful Filtering Scheme

CSA not only supports simple address and protocol filters, but also supports filters based on application commands, IP subnets, data patterns, and other criteria. Complex conditions (see Figure 6) can be specified with ease by freely adding and combining filter conditions using AND, OR, and NOT operators while viewing the settings panel. Once specified, a filter definition can be saved with an assigned name and then reused at a later time for capture or trace file display.

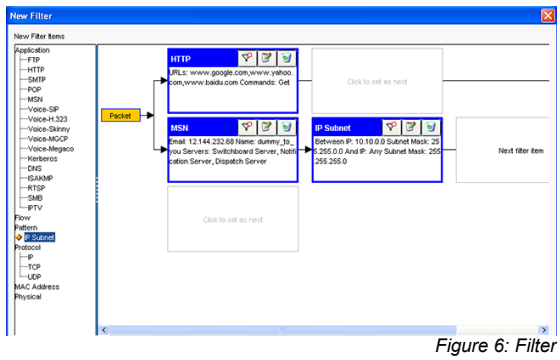


Figure 6: Filter

Comprehensive Traffic Report

CSA provides a large inventory of standard reports in chart and table formats showing statistics and performance for network traffic, servers, and applications. CSA generates reports from real–time data or trace files. See QoS reports for voice and video traffic, showing statistics such as jitter, latency, packet loss, MOS, J–MOS, R–value, and video quality factor. Elements of these reports can be easily combined to produce custom reports.

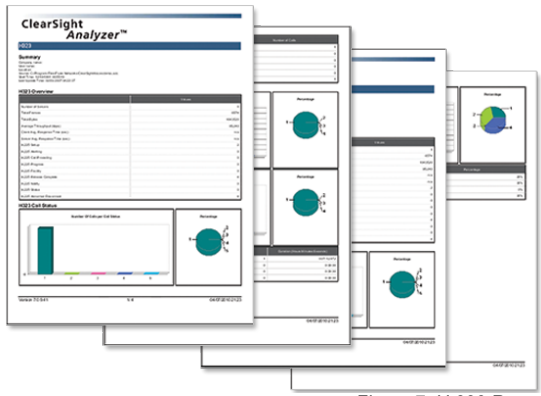


Figure 7: H.323 Report

CSA-1045 Adds Advanced Optional Features

History Reporter

Produce network, application, and other trend reports based on real–time statistical data accumulated over longer periods of time.

Packet Generator

A versatile generator allows you to perform network load testing and traffic reproduction testing. Two modes are supported: 1)Packet mode; a specified packet is sent repeatedly, 2)Buffer mode; traffic from a trace file is reproduced on the network.

Multicast Analysis

The Multicast Visualizer Option provides counters and statistics describing and quantifying the traffic on each detected multicast address. CSA extracts multicast group addresses (IGMP for IPv4 and MLD for IPv6) from packets sent by hosts to routers.

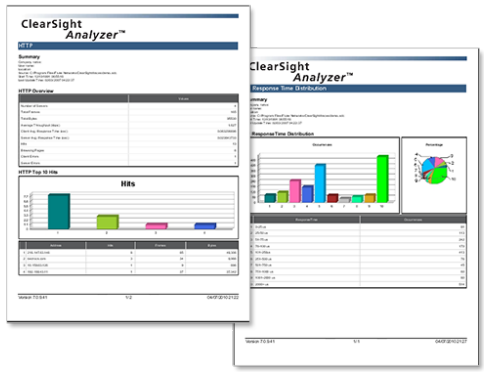
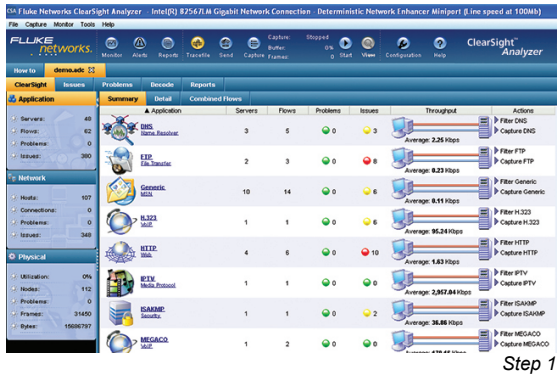


Figure 8: HTTP Report — Figure 9: IP Response Time Report

ClearSight Analyzer application–centric analysis workflow

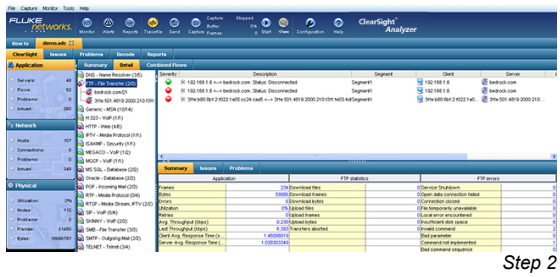
The ClearSight Analyzer automatically analyzes application flows, and can classify traffic by application such as HTTP, email, and VoIP to make it easy to see the flow of each transaction. You can also drill down from the flow view for a session to the packet level and reconstruct the application content.

Step 1: Start Monitor.
Network traffic monitoring starts automatically. Traffic is classified by application. Applications with problems and issues can easily be identified with Yellow or Red icons.



Step 1

Step 2: Select Application.
Selecting an application displays a list of respective flows and their associated servers and hosts. A red or yellow icon appears for flows for which a fault or other event has been detected, so it is easy to see which flows have a problem.



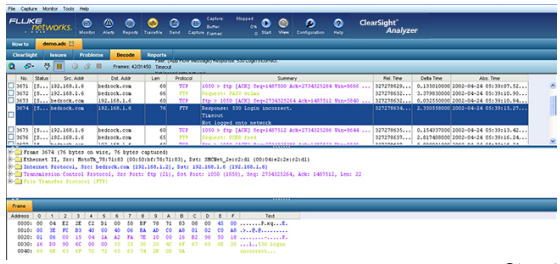
Step 2

Step 3: Select Flow.
Clicking a flow selects and displays the flow of communication between the client and server (ladder view). Packets for which a fault or other event has occurred are indicated by a red or yellow arrow, so you can quickly identify exactly where and when a communication problem has occurred.

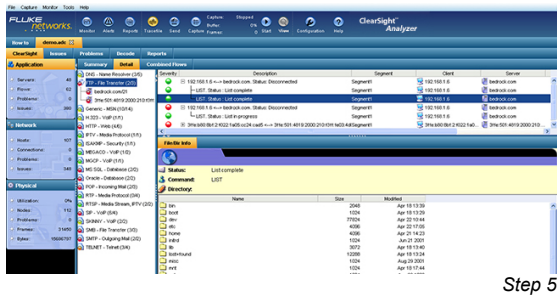
Step 3

Step 4: Automatic Filter/Packet Decoding Display.
Clicking a packet in the application flow display (ladder view) opens the packet translation screen which is filtered to show only the associated transaction.
As such, it only takes a few clicks to go from the top application level to the detailed packet display, making troubleshooting quicker and easier.

Step 5: Replay Application Content.
The application content over a selected flow can be reproduced in ClearSight to show the actual content.



Step 4



Step 5

NETSCOUT

Features Summary

Model	Description
Application-centric Summary Page	Immediately see the problem layers and quickly determine overall application health from real–time traffic monitored or trace file
Real-time monitoring of applications	See application and configuration flow views with or without capturing packets
Expert Alert Function	Set problem thresholds and see immediately when an application, server, or flow has a problem. Program email, pager, script, or SNMP actions to be performed when a problem occurs
Time–based analysis of trace files	For trace files up to 4GByte in size, conduct analysis based on user defined time range for packets within the trace file. Analysis includes application performance for HTTP, H.323, SIP and RTP, Trending Network Layer characteristics such as occurrence of TCP SYN, Retransmission, IP matrix and Host, to traffic volume trend by frame count/byte/frame size count. Users can export packets that fit the display criteria to conduct application–centric analysis.
Protocol Forcing	Apply protocol forcing during real–time monitoring or when replaying a trace file to identify protocol encapsulated in another protocol
Timing displays for application conversation	Network delays and poor response times pop right out of the application flow view and identify slow commands, poor service, or application performance issues
Multi–Segment View	Correlate IP packet flow, UDP and/or TCP between two hosts or server and client across multiple physical segments.
Comprehensive Filtering Functions	Limit monitoring, capture, or display to those things that interest you by creating filters based on application commands, IP subnets, data patterns, and many other criteria. Build up complex filters using AND, OR, and NOT operations. Name, save, and reuse filters
Quick capture or display filter generation	Right–click on a flow to apply capture/display filter for that flow only
Full packet decodes (with support for Jumbo Frame)	Switch to a Decode tab to see traditional full packet decodes in Summary, Detail, and Hex screens, during real–time monitoring or from a trace file
VOIP Call Log browser	Apply simple filtering and sorting to browse for individual calls using criteria such as start time, call duration, caller and callee identifiers, and MOS score during real–time monitoring
Voice and Video QoS Analysis	When an RTP flow is recognized as including a video flow, ClearSight™ Analyzer displays VQFactor™ statistics for the video component as well as MOS statistics for the audio component

Protocol Specifications

Protocol	Description
Supported Non-VoIP Applications	DNS, HTTP, FTP, TELNET, Citrix, POP3, SMTP, Exchange, ISAKMP, KERBEROS, MS SQL, Oracle, SMB, AIM, BOOTP, Gopher, Media Player, Napster, NETBIOS, NFS, NNTP, QuickTime, RIP, RIPNG, SNMP, TFTP, X Windows, Yahoo Messenger, MSN, Skype
Supported VoIP Applications	H.323 (H.225, H.245, RAS), SIP (RFC 3261, T.38 Fax over IP), MGCP, MEGACO or H.248, SCCP (Skinny), SIGTRAN (IUA: RFC 3057 ISDN UA, SUA, M2PA, M2TP, M2UA: RFC 3331, SS7 MTP2 UA, M3UA: RFC 3332, SS7 MTP3 UA, MAP, SCTP, ISUP), RTP, RTCP, RTSP
Play (decode) Audio Codecs	G.711 (µ-law and a–law), G.721, G.722, G.723, mono, G.726, G.729, GSM mono, 4–bit mono DVI 8 KHz, 11.025 KHz, 22.05 KHz, MPEG layer (I, II-TS, III, IV), iLBC, AMR (GSM, 3GPP), ASF
Mobile Protocol	Support for 3G–324M and LTE the umbrella protocol for video telephony in 3G/4G mobile networks
EOAM Decode	Ethernet OAM frames in both ITU and IEEE format

Note: Partial list shown above. For full list, please visit enterprise.netscout.com/protocolsupport

System Requirements

Item	Minimum Requirement
Computer	Industry standard computer system (laptop or desktop), with a CD/DVD-ROM drive for software installation
Processor	Pentium 4 (or equivalent) running at 1 GHz minimum(2 GHz recommended)
RAM	512 MB minimum (1 GB recommended) 2 GB minimum if running Windows 7 Professional Edition
Hard Disk Space	40 GB hard drive with at least 15 GB of available space.
Operating System	Microsoft Windows XP Home Edition with SP3 (Disable the firewall) Microsoft Windows XP Professional with SP3 (Disable the firewall) Microsoft Windows 7 Professional Edition (32 and 64 bit) Microsoft Windows 8.x Professional
Monitor	40 GB hard drive with at least 15 GB of available space.
Operating System	Network connection with NDIS–compliant network device driver

Product and Options

Model	Description
CSN/CSA–1000	ClearSight Analyzer Software
CSN/CSA–1000CD	ClearSight Analyzer Software on CD
CSN/CSA–1045	CSA with IP Multicast Visualizer, History Reporter and Packet Generation option
CSN/CSA–1045CD	CSA with IP Multicast Visualizer, History Reporter and Packet Generation option on CD
CSN/OPT–3045	IP Multicast Visualization, Hist Reporter, and Packet Gen for CSA

Support

Model Number	Description
GLD–SW–1000	Gold Support Services, 1 Year Software Maintenance for CSA–1000
GLD–SW–1045	Gold Support Services, 1 Year Software Maintenance for CSA–1045