

CLEAR SIGHT

Analyzer

Enhanced VoIP and Streaming Support

New ClearSight Reporter

Enhanced IPv6 Support

Analyzer



Next Generation Network Troubleshooting Tool — CLEARsight

Features

Simple and intuitive user-interface

The ClearSight Analyzer uses a hyperlink style user interface whereby you can click screen elements such as counters or icons to drill down to more detailed information. The intuitive user interface makes it easy to access the information you need. Examples include the ladder view and packet translation links, and the one-touch filter menu opened by clicking the right mouse button, which filters the display to show packets from a particular connection only.

A Data is organized into three levels: application, network, and physical.

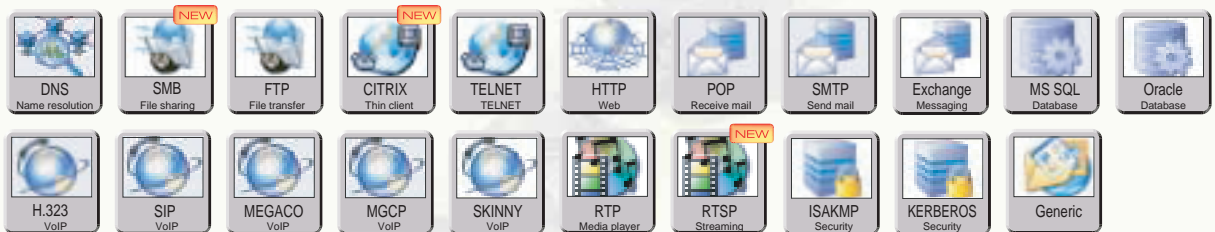
B Switch between realtime monitor, trace file, and capture analysis modes.

C Servers and flows are shown by application.

D Errors and event counts are shown for each application with severity indicated by color icons.

E Applications and traffic throughput are shown using animations.

ClearSight View

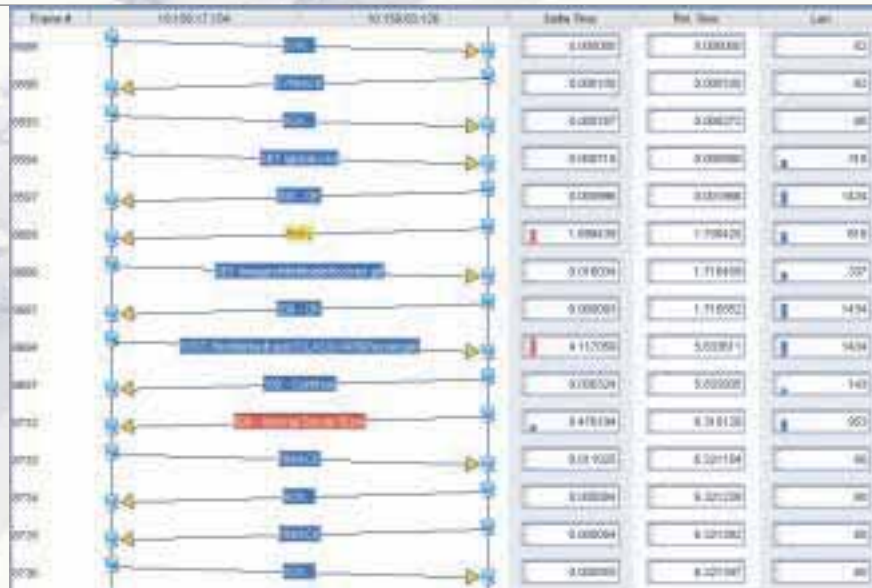


Real-time application flow analysis ... Ladder view

The ClearSight analyzer displays the transactions in each application flow in ladder format.

This simplifies the complex message interaction between client and server, by displaying the ladder interaction sequentially. It is easy to spot errors or abnormalities in the communication protocol.

The flow analysis function is not just restricted to trace files, but can display the traffic in real-time to give an on-the-spot view of the communication flow. When troubleshooting, this saves you from having to make a handwritten diagram of the communication flow based on the packet translation from the protocol analyzer.



Ladder view can be exported to pdf file

Playback function reconstructs the application content from the packets

For applications such as FTP, Telnet, email, databases, and VoIP, You can reconstruct user activity or application content from the packets flowing across the network in real-time, or captured beforehand in a trace file.

Instead of just traffic statistics and counters, ClearSight shows You what is actually happening on the network in real-time.



Automatic detection of communication faults!! Alert list allows quick & easy drill down flow (during post analysis).

Multi-segment view for analyzing the communication flow spanning multiple segments.

Reporter automatically generates standardized application and network reports.

Powerful VoIP analysis functions are supported as a standard feature. Voice and application data can be analyzed simultaneously.

File format compatible with Sniffer™, Ethereal & many others

Available in 10/100M full duplex Ethernet and Gigabit Ethernet Versions

Use ClearSight for

• Network troubleshooting

• Monitoring the status of critical application servers

• Monitoring network performance

• Network testing and debugging

Next generation network troubleshooting — Top-down/drill-down analysis

The ClearSight analyzer's function to automatically analyze application flows 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 within ClearSight

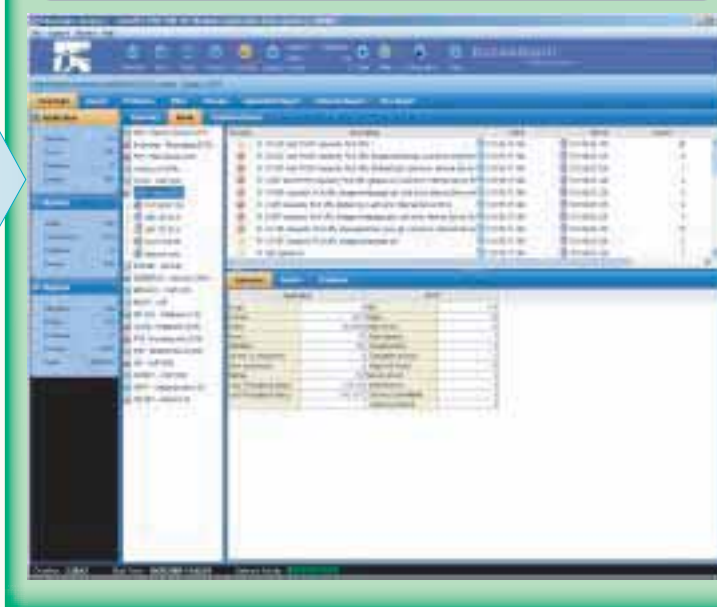
Start monitor



STEP 1

Network traffic monitoring starts automatically when you start ClearSight. Traffic is classified by application and faults and other events are detected automatically.

Select application



STEP 2

Selecting an application displays a list of servers and connections for that application. As a red or yellow icon appears for servers or flows for which a fault or other event has been detected, it is easy to see which servers have a problem.

Select connection

STEP 3

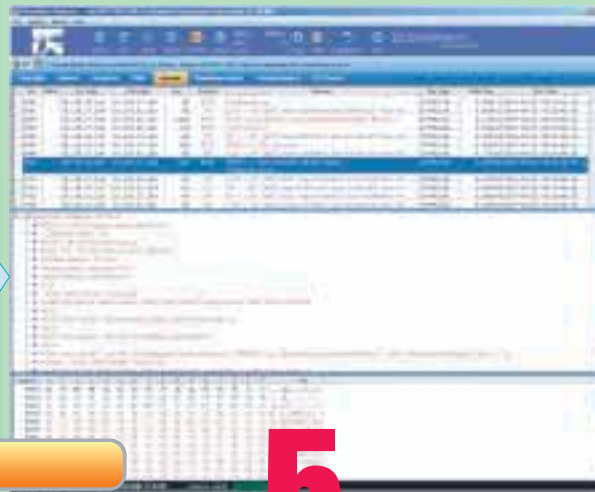
Clicking a connection selects that connection and displays the flow of communication between the client and server (ladder view). Packets for which a fault or other event has occurred are indicated by a red or yellow arrow, so you can quickly identify where a communication problem has occurred.



Automatic filter and packet decoding display (for trace file analysis)

STEP 4

Clicking a packet in the application flow display (ladder view) opens the packet translation screen which is filtered to show only the associated transaction. It only takes a few clicks to go from the top screen to the detailed packet display, making troubleshooting quicker and easier.



Replay application content

STEP 5

The application content over a selected connection can be reproduced in ClearSight to show the actual content.



Advanced application flow analysis



The volume of VoIP traffic is increasing rapidly along with the spread of broadband, not just in the corporate world but also into the home. ClearSight can perform detailed analysis of this traffic for connectivity and speech quality.

Support for VoIP and Streaming Signaling Protocols

Supports the various signaling protocols used to control IP telephony connections and streaming

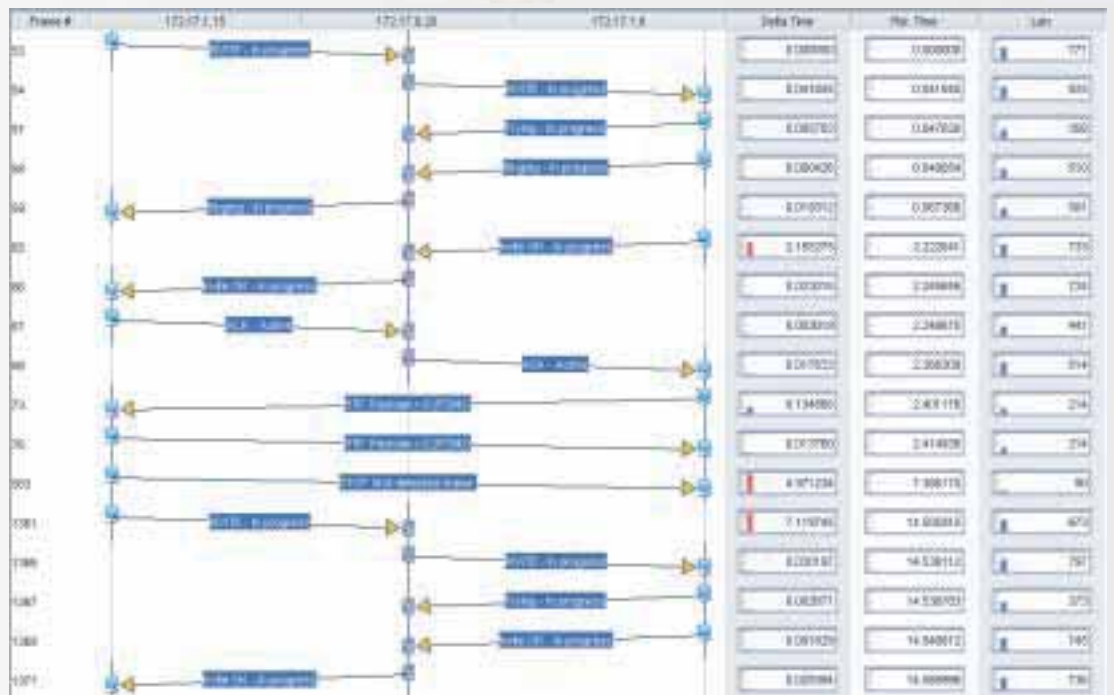
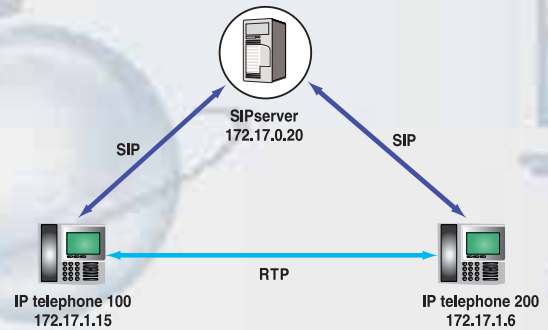
Supports analysis of various signaling protocols including SIP, H.323, Cisco® SKINNY™, MGCP, MEGACO, and RTSP.

Flow data is classified by call

The signal flow and audio flow are grouped by call.

The multi-segment ladder display shows the progress of the call at a glance.

The exchange of packets between multiple nodes including telephone terminals and relay servers is automatically grouped by call and displayed in the Multi-segment ladder view. The entire sequence from initiating the connection through to the conversation between telephones and disconnection can be viewed in real-time (or from a trace file).



using CLEAR SIGHT

Speech quality measurement --- The quality of VoIP speech or video can be measured quantitatively.

Detailed statistics for every call including R value and MOS

Selecting the statistics tab in an RTP flow displays detailed statistical information about the flow. In addition to the minimum, maximum, and mean values for the RTP packet interval, jitter and loss, the display includes the results of calculating the MOS and R value speech quality indicators. These provide a quantitative assessment of speech quality on IP telephony.

Audio and video playback function supports various CODECs

QoS analysis for all RTP CODECs, and playback functions for the following CODECs. Replay can be used in both real-time and when performing post analysis of a trace file.

Audio CODEC

- G.711(U-law), G.711(A-law),
- G.729, GSM mono, G.723 mono,
- G.722, G.726,
- 4-bit mono DVI 8 kHz,
- 4-bit mono DVI 11.025 kHz,
- 4-bit mono DVI 22.05 kHz,
- MPEG layer (I, II, III)
- AMR (GSM, 3GPP)
- iLBC
- video Codec
- H.264
- Data Codec
- T.38 Fax over IP



Both Audio and Video data can be exported to Windows standard format (wav and mpg).

Video CODEC

- JPEG (411, 422, 111),
- H.263 Mode A, H263 Mode B
- MPEG4

VoIP QoS Report

You can generate a QoS report for a VoIP call simply by selecting the desired call and clicking the [Report] tab. The results for measured speech quality parameters including packet loss, jitter, R value, and MOS are displayed graphically, and a report, which includes an overall ranking out of five stars, is generated automatically.



Advanced application flow analysis

Application Flow Analysis for HTTP



ClearSight analyzes HTTP traffic in real-time to identify communication faults. HTTP is the most important application for displaying information content on the internet and corporate intranets.

Traffic is classified by HTTP connection

HTTP traffic is displayed in a list sorted by server and by connection.

Display a list of URLs for a connection

Seq#	Time	Source	Destination	Length	Status	Method
1	0.000	10.100.1.1	10.100.1.1	1024	200	GET
2	0.000	10.100.1.1	10.100.1.1	1024	200	GET
3	0.000	10.100.1.1	10.100.1.1	1024	200	GET
4	0.000	10.100.1.1	10.100.1.1	1024	200	GET
5	0.000	10.100.1.1	10.100.1.1	1024	200	GET
6	0.000	10.100.1.1	10.100.1.1	1024	200	GET
7	0.000	10.100.1.1	10.100.1.1	1024	200	GET
8	0.000	10.100.1.1	10.100.1.1	1024	200	GET
9	0.000	10.100.1.1	10.100.1.1	1024	200	GET
10	0.000	10.100.1.1	10.100.1.1	1024	200	GET

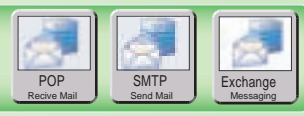
The connection summary lists the number of GET and PUT methods used, and individual connections can be expanded to show a list of the URLs.

HTTP Content Replay

Web content can be reconstructed from HTTP packets and displayed on the ClearSight Analyzer. URLs can also be selected from a list as required and data downloaded from the network and displayed on the screen by pressing the GO button.



Application Flow Analysis for Email



ClearSight performs real-time analysis of application traffic for email and messaging, an important medium for network communications.

Support for POP and SMTP Protocols

Flow analysis supports both POP and SMTP, the two most widespread email protocols in current use.

Reconstruct Email Content

Send or receive mail content can be extracted from the email traffic and displayed in mailer format.



Support for Exchange™ Groupware

Flow analysis and reconstruction of message content are supported for Exchange groupware.



using CLEAR SIGHT

Application Flow Analysis for Databases



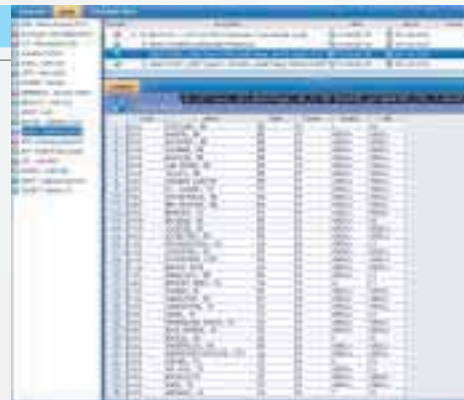
ClearSight can perform detailed analysis of the client-server traffic for database applications used in critical company systems and diverse business applications.

Support for Oracle® and MS SQL™

ClearSight supports flow analysis of the protocols used by Oracle and MS SQL, two of the most widely used databases in corporate networks.

Reconstruct Database Table Content

The content of database tables requested by users can be displayed based on the database traffic.



Application Flow Analysis for Security



The new ClearSight 5.0 security application flow function supports the ISAKMP key exchange protocol and KERBEROS authentication protocol.

ISAKMP(IKE)

The key exchange sequence performed as part of establishing a secure communication channel on a VPN network using IPsec can be viewed on the ladder display.



KERBEROS

This protocol is used during user authentication and access control on Windows 2000 networks and Mac OS X. Authentication errors and their causes can be identified quickly using the ladder display.



Application Flow Analysis for Instant Messenge(New)

ClearSight can perform detailed analysis of the client-server traffic for instant applications.

ClearSight supports flow analysis of the protocols used in MSN Messenger and Skype, the chat content can be shown in the table. MSN is fully supported, including application summary display, conversation flow, statistics, text content, some voice and video replay, alarms, and filtering.



Application Flow Analysis for IPTV(New)

IPTV – streaming video implemented by MPEG2 over UDP is supported. The 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 triple play. Content playback is supported in both real time and post analysis.

NOTE: You must use the ClearSight Decode Engine to decode MPEG2 over UDP.



Expert Alert Function Automatically Detects Communication Problems

The ClearSight Analyzer's Expert Alert function automatically detects communication faults in the captured packets and displays alerts using five-step color coded icons. Which application, server, or flow has a problem can be seen at a glance.

Alert list supports drill-down

Alerts detected by ClearSight, either in real-time or from a trace file, are classified as events (faults in the communication sequence) or problems (faults that exceed a threshold value) and can be listed separately. Lists can be sorted simply by clicking on a column header, and you can drill down to the associated communication flow by right-clicking on an alert during postcapture analysis.



Comprehensive Filter Functions

The filter menu in ClearSight supports not just simple address and protocol filters, but also filters based on application commands, IP subnets, data patterns, and other criteria.

Visual AND/OR/NOT Setting

Complex conditions can be specified with ease by freely adding and combining filter conditions using AND, OR, and NOT operators while viewing the setting panel. Once specified, a filter definition can be saved with an assigned name, and then reused at a later time, during capture or trace file display.



ClearSight Reporter

The powerful reporter function in ClearSight Analyzer can collate statistics on items such as applications, servers, and network status, and use this information to generate standardized reports automatically. The reports can be collated and displayed from either realtime monitor results or the contents of packets contained in a trace file.

Real-time / Trace File Reports

Reports based on the accumulated data for each statistical data item can be generated immediately, simply by clicking the report item in the list displayed on the screen. The reports can be printed in the format in which they appear on the screen, or saved in PDF, HTML, or RTF format using the export function. User-defined reports that combine selected report items can also be generated.



Real-time Report Screen

ClearSight History Reporter Module (option)

Network, application, and other trend reports can be produced by accumulating real-time statistical data in a database over long periods. The period covered by the report can be specified by day, week, or any user-specified period, simplifying the process of producing periodic network reports.

- The save interval for historic data can be set in the range 1 to 60 minutes.
- By clicking on statistical items such as hosts or frame counts in the cumulative report for the specified period, a trend graph for that item can be generated. Multiple items can be selected at a time and displayed superimposed on the same graph.
- Reports can be exported to PDF, HTML, and RTF format. Once created, reports can be further edited using software such as MS Word.

Report Samples



SIP MOS Report



Application Distribution Report



History report (Option)

Call Browser

The Call Log browser lets user 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.



Wireless Support

WiFi Post Analysis

By opening Sniffer™ format (*.cap) or pcap format trace files captured from a wireless LAN environment in ClearSight, packet decoding and application flow analysis can be performed on WiFi packets in the same way as Ethernet. As WEP key decoding is supported, encrypted packets can also be analyzed in ClearSight by entering the WEP key.



※A third-party WLAN analyzer is required to capture wireless LAN packets.

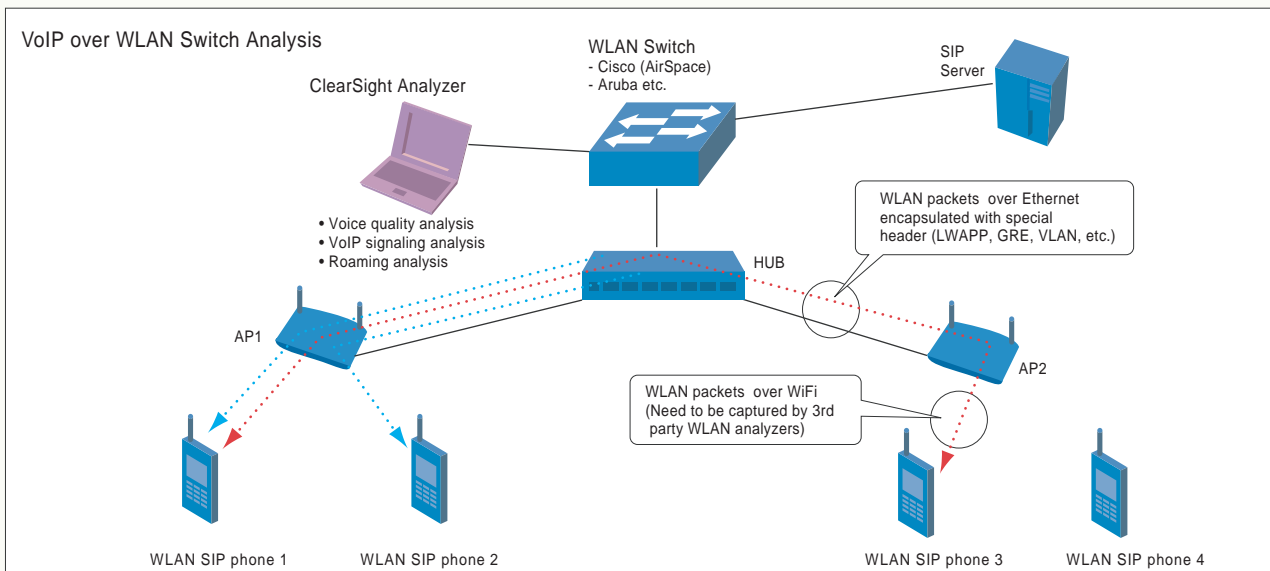
WiFi Ethernet Support

Analysis of WiFi packets encapsulated in the LWAPP, GRE, and VLAN headers used over Ethernet in a wireless LAN switch environment is also supported. This enables real-time application monitoring of encapsulated WiFi packets sent over Ethernet between AP-WLAN switches.



VoIP Support over Wireless LANs

A wireless IP telephony (Voice over WiFi Phone) trace file captured on a wireless segment can be opened in ClearSight, and the header display can be used for signaling analysis. Speech quality measurement based on the RTP packets can also be performed.



Other troubleshooting support functions

The ClearSight analyzer supports more than just next generation application analysis. It also incorporates a full range of the key functions required by a LAN analyzer. These functions provide powerful backup when troubleshooting in the field.

RealTime Decode both in Application, network, Physical, and RealTime.

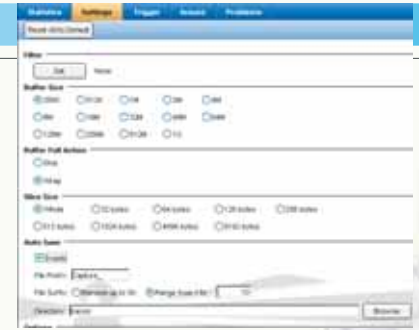
This function translates and displays the currently transmitted packets on the decode screen in realtime. This can be used during activities such as troubleshooting and network testing to confirm whether the packets of interest are being transmitted.



Auto Save Function

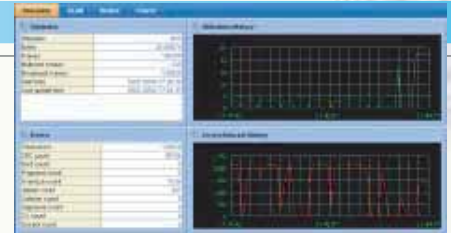
When the capture buffer becomes full, the captured data can be automatically saved to the hard disk. As data can be progressively appended to the file, you can capture data for as long a time as you have disk space available.

※Packet loss may occur during hard drive writes.



Error Packet Capture

You can monitor and capture error packets using a special 10/100M/Gigabit NIC and driver. Investigating the error packets resulting from data collisions and network device or cable faults helps identify hardware faults.



Trace Route

By right-clicking on an application or connection flow displayed in ClearSight, a Trace Route can be executed for host addresses associated with the flow.



Open multi trace in separate windows

User can open several trace files concurrently by setting in configuration. This can be used in many conditions, such as comparing the difference between multiple trace files.

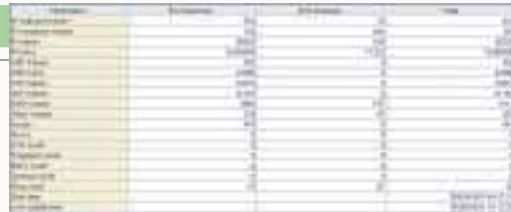


IPv6 Solution

The ClearSight Analyzer includes powerful IPv6 analysis functions, and the ClearSight application flow analysis function also works in an IPv6 environment. By adding the "ClearSight IP Multicast Visualization Module" option, you can also perform performance analysis of IPv6 multicast communications.

IPv4 vs. IPv6 Packet Summary

In environments where both IPv4 and IPv6 are used, statistical data is listed for both types of IP packet. This provides an easy way to see what proportion of packets use IPv6.



IP Version	Protocol	Packet Count
IPv4	TCP	12345
IPv4	UDP	6789
IPv4	ICMP	101
IPv6	TCP	5432
IPv6	UDP	2109
IPv6	ICMP	50

IPv6 Real-time Monitoring and Ladder Display

Advanced ClearSight functions such as real-time application flow analysis, ladder view, and content playback can be used in an IPv6 environment also without requiring any special setup. You can perform application analysis without needing to worry about which IP layer is used.



IPv6 Address Filtering / Address Book

Filter settings can be specified for IPv6 addresses in the same way as for IPv4 addresses. IPv6 addresses can also be saved in the Address Book and displayed with a unique name within ClearSight.



Filter Setting



Address book Setting

ClearSight IP Multicast visualization Module (option)

The following types of IPv6 multicast traffic analysis can be performed when this option is added.

- Generates tables for each MLD (Multicast Listener Discovery) group ID
- Measures the response of PIM-SM (Protocol Independent Multicast – Sparse Mode) JOIN and PRUNE
- Analyzes IPv6 fragmentation

※ This option also supports PIM-SM over IPv4 analysis



Group ID	Source Address	Group Address	Join Time	Last Update Time
00000000000000000000000000000000	2001:db8::1	2001:db8::1:1	2008-01-01 10:00:00	2008-01-01 10:00:00
00000000000000000000000000000000	2001:db8::2	2001:db8::1:2	2008-01-01 10:00:00	2008-01-01 10:00:00

ClearSight Packet Generator

The ClearSight Packet Generator is an ideal traffic generation software package for use in simple network load testing and traffic reproduction testing. The software supports packet mode, in which the same packet is sent repeatedly, and buffer mode, in which traffic captured from the actual network is reproduced on the network. The software is available in two different forms: a simple-to-use standalone package and an optional module that can be incorporated into ClearSight Analyzer.

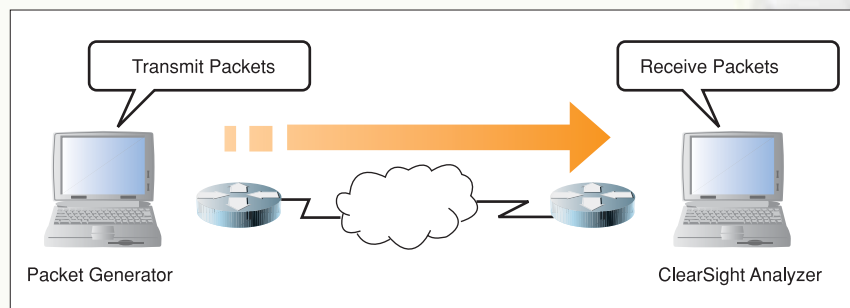
Features

- Supports general-purpose NDIS-compatible 10/100M and Gigabit Ethernet cards
 - ※ ClearSight Packet Generator does not support the ClearSight Analyzer 10/100M Full Duplex adapter and Gigabit adapter.
- Packet editing function allows easy editing of the address and port number for transmitting packets.
- Profile function allows multiple configurations to be stored and reused when needed.
- Information about packet transmission can be displayed visually in the form of statistical data and graphs.
- Testing can be automated using JavaScript.

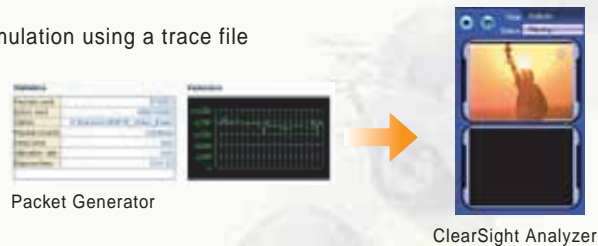


Example Applications

1. Exchange packets with a ClearSight Analyzer across the network for network availability testing and simple network performance testing.



2. Voice and video traffic simulation using a trace file



3. Use of trace files to simulate abnormal traffic such as network faults, unauthorized network attacks, or virus activity.
4. Reproduction of client-server traffic for network training or demonstrations.

Gigabit and 10/100M Full Duplex Ethernet High Performance Solution

The ClearSight Analyzer combines a powerful portable PC with the leading-edge high-performance PCI-X 10/100M/Gigabit module to deliver a strong Gigabit and 10/100M full duplex solution.

System Configuration

Common items

- ClearSight Analyzer Software
- Portable PC Platform
(CPU: Xeon 2.8Ghz, 2GB memory, 80GB hard drive, Windows XP)
- PCI-X 10/100M/Gigabit Ethernet card

10/100M FDX supported model

- 10/100M full duplex tap

10/100M/Gigabit supported model

- 10/100M full duplex tap
- 1000BaseT tap
- Option: Giga SX SFP modules and multi-mode splitter tap
- Option: Giga LX SFP modules and single-mode splitter tap



10/100M full duplex tap



Gigabit fiber splitter tap

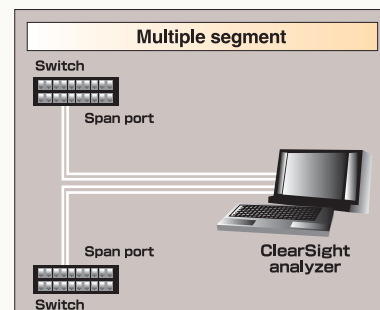
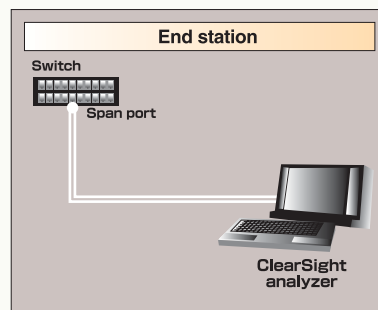
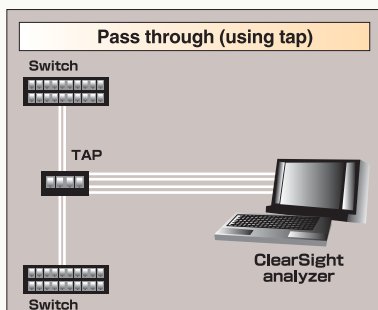
※Specifications subject to change without notice.

Features

- The new PCI-X Gigabit card supports 10/100M full duplex and Gigabit Ethernet. The card includes two RJ45 ports for 10/100/1000Base-T and two SFP ports for the fiber interface.
 - ※ The RJ45 ports and SFP ports cannot both be used at the same time.
- 100% full-rate capture is supported for a 10/100M full duplex Ethernet link.
- The 128MB shared streaming buffer allows high-performance real-time monitoring and capture.
- Supports capture of jumbo frames up to 10Kbytes from Gigabit Ethernet.
- Supports both an end-station connection and a pass-through mode connection using a tap.

Gigabit Channel monitor screen

Connection Procedure



MSV (Multi-Segment View)

MSV (Multi-Segment View) is a new function in ClearSight Analyzer. MSV tracks communication automatically across multiple segments and generates a multi-point ladder display. The function enables a whole range of new applications that you would never have considered in the past, including analysis of problems such as packet loss and delay in relay equipment (routers, switches, etc.) and analysis of end-to-end communication performance.

MSV (Multi-Segment View) Features

- Traces from different segments can be combined in the ladder view either automatically or manually.
- Analysis can compare up to four different segments at a time.
- TCP/IP performance report
- The 10/100M full duplex analyzer and Gigabit analyzer support real-time ladder analysis of two segments at the same time.
- Trace files captured at separate locations can be merged.

Potential Applications

- Analysis of communication data from different segments
- Analysis of communication data that passes through multiple nodes
- Analysis of communication data in which node IP address and port data is converted
- Education and training

Data Collection

1 Simultaneous capture of two segments

When using the 10/100M full duplex analyzer or Gigabit analyzer, traffic from two different segments can be captured simultaneously using the same PC clock. In test lab or machine room environments where routers and switches are concentrated, data from different segments can be captured and compared without needing to worry about time synchronization issues (provided they are physically located close enough for the cable to reach).

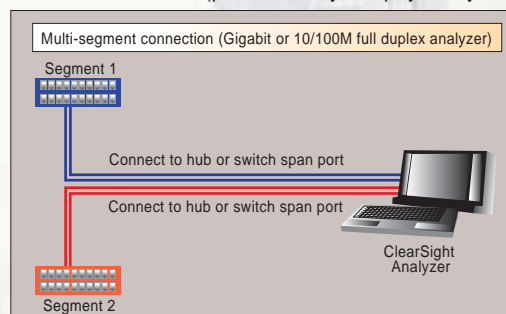
Mode _____

End Station (Use for connecting to Monitor Port or Network Tap)

Multiple Segment

First Segment's Name:

Second Segment's Name:



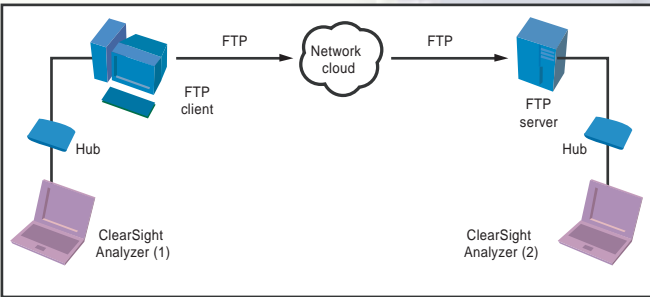
2 Trace file merge

Trace files captured simultaneously on separate ClearSight analyzers can be merged to create a multi-segment trace file. Merging of up to four trace files is supported and the offset times can be easily adjusted by pressing the Auto Sync button to compensate for the time differences between the original trace files.



Automatic Analysis using AutoDiscovery

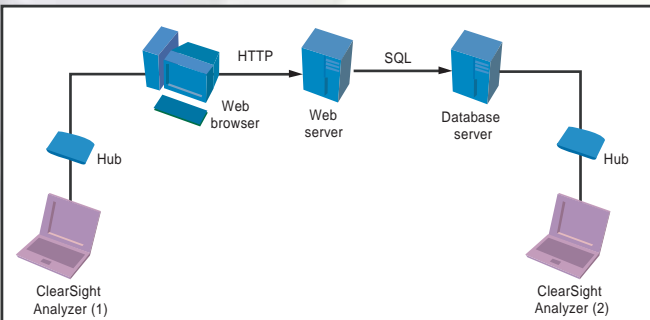
If the same IP address and port pair is found on different segments, then the flows on each segment are related. The multi-segment ladder display is generated automatically in realtime or when the trace file is opened.



Multi-tier Analysis (post-analysis only)

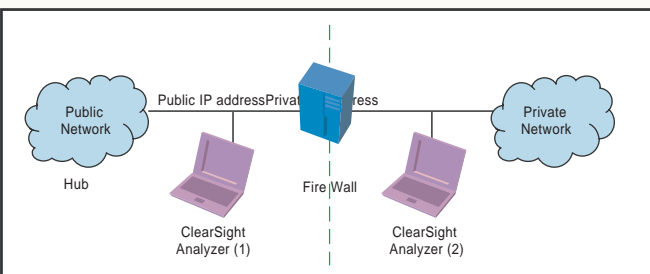
Reference to a different server, address conversion, communication using different protocols, and similar can be linked manually to a specific transaction and displayed in an easy-to-understand ladder display.

- Example uses for multi-tier analysis:
HTTP client -> HTTP server -> SQL Server



Network Address Translation (NAT) Support

ClearSight Analyzer can merge trace files captured from either side of a firewall that uses a NAT function and automatically associate packets with different IP addresses from opposite sides of the firewall. This function is useful when investigating packet loss or delays due to the firewall.



TCP/IP Performance Report

ClearSight can automatically generate a TCP/IP performance report by performing a comparative analysis of the same flow captured on different segments. The report can isolate communication bottlenecks in the client, server, or network, and display the analysis results graphically.





 One Full Year of Software Updates and Support bundled with every ClearSight Product.
 Specifications subject to change without notice.
 Trademarks are owned by their respective holders.



ClearSight Networks, Inc.
 46401 Landing Parkway
 Fremont, CA 94538-6496
 Ph: 510-824-6000
 800-825-7563
 fax: 510-824-6100
www.clearsightnet.com

For more information:
sales@clearsightnet.com
info@clearsightnet.com

For Media relations:
pr@clearsightnet.com