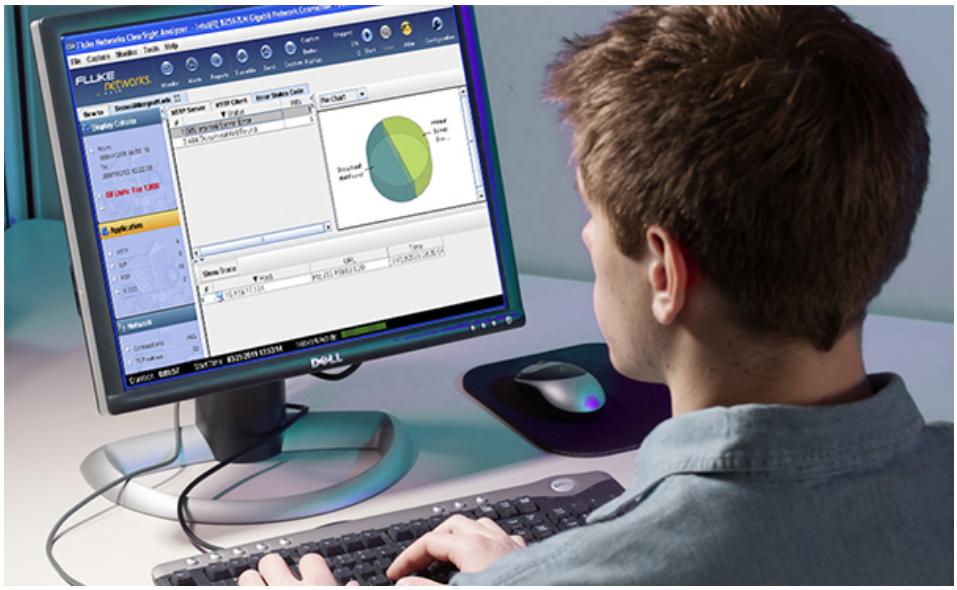
## ClearSight™ Analyzer

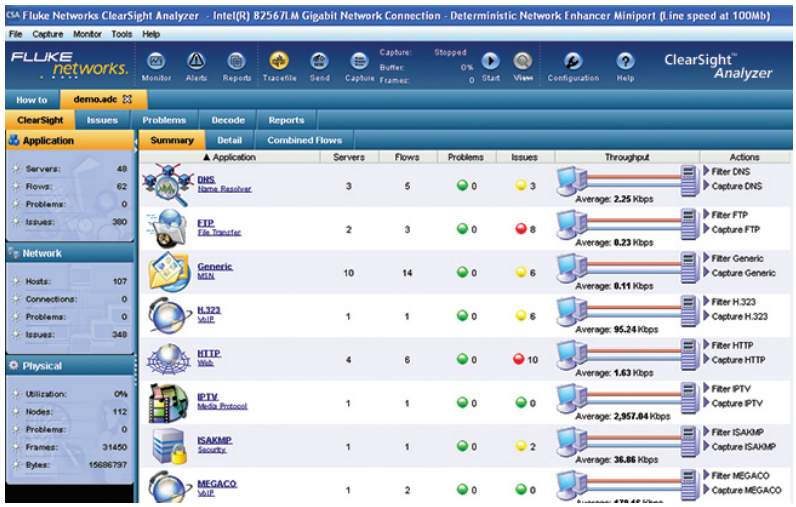
*Der preisgekrönte ClearSight™ Analyzer (CSA) bietet leistungsstarke applikationszentrierte Funktionen zur Leistungsüberwachung- und -analyse. Dank dieser Funktionen können Netzwerkadministratoren und -ingenieure der Unternehmen Applikations- und Netzwerkleistungsprobleme in Multiprotokoll-Netzwerkumgebungen verwalten, diagnostizieren und beheben. CSA unterstützt die meisten gemeinsam verwendeten Protokolle und Benutzer können Wireshark-Decodierungen importieren, um Vorteile der von der Open Source-Community bereitgestellten Protokoll-Decodierungen zu nutzen - CSA ist deshalb das vielseitigste Protokollanalyse-Tool auf dem Markt.*



***Applikationszentrierte Analysen-Software, die eine schnelle Beantwortung zu Problemen der Applikationsleistung aufbietet***

### Hauptfunktionen

- Applikationszentrische Analyse, die automatisch Datenverkehrsflüsse der Applikationen mit intuitivem Drill-Down analysiert, um die Ursache der Leistungsprobleme zu identifizieren
- Echtzeitüberwachung der Applikationsleistungmit Warnungen zur Problemkennzeichnung
- Zeitbasierte Analyse für Trace-Dateien bis zu 4 Gigabytes zur schnellen Ermittlung relevanter Pakete für die applikationszentrische Ansicht
- Echtzeitstatistiken, Bounce-Diagramme und Berichte für Flüsse auf einzelne oder mehrfache Segmente - Probleme schnell erkennen
- Video und Voice-Call Status, QoS-Analyse und Playback
- Benutzerdefinierbarer Übersichtsbericht
- Unterstützt WireShark-decodierte Funktionseinheit



## Innovative Leistungsanalyse mit Schwerpunkt auf Applikationen

Über einen einfachen und intuitiven Startbildschirm präsentiert CSA eine umfassende Detailansicht des Zustands der Anwendungen in Ihrem Netzwerk. Um genauere Informationen zu erhalten, können Sie von dieser Übersicht ins Detail gehen. Z. B. erkennt und analysiert CSA alle Abläufe einer HTTP-Anwendung und zeigt die Anzahl von Servern und Clients sowie den Durchsatz an. Mit einem einfachen Klick können Sie dann jeden Durchsatz mit einem Bounce-Diagramm und die genaue Identifikation der Pakete sehen, die das Problem verursacht haben. Dieses beispiellose Maß an Übersicht und Transparenz beschleunigt die Lösung von Anwendungsproblemen und minimiert die Ausfallzeiten im gesamten Netzwerk.

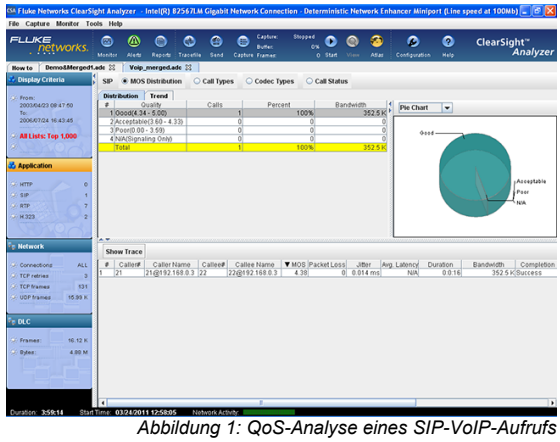


*Abbildung 1: QoS-Analyse eines SIP-VoIP-Aufrufs*

## Echtzeitüberwachung des Datenverkehrszustands mit Problem-/ Fehlerbestimmung

Die CSA Expert Alert-Funktion erkennt automatisch Kommunikationsstörungen in erfassten oder überwachten Paketen und zeigt sie mit farbkodierten Symbolen an. Die spezifische Applikation, der Server oder der problematische Datenfluss kann mit einem Blick auf der Applikationsstartseite erkannt werden.

Die durch CSA entweder in Echtzeit oder aus einer Diagnosedatei ermittelten Alarme, werden als problematisch (Störungen in der Kommunikationssequenz) oder als Probleme eingestuft (Störungen, die einen Schwellenwert übersteigen) und werden protokolliert. Listen können durch einfaches Klicken auf einen Spaltenkopf sortiert werden. Sie können bis zum entsprechenden, das Problem verursachenden Kommunikationsfluss ins Detail gehen, indem Sie während der Analyse nach der Erfassung auf einen Alarm rechtsklicken. Probleme und Fehler können per E-Mail, Pager, Skript oder SNMP Trap-Aktionen ausgelöst werden.

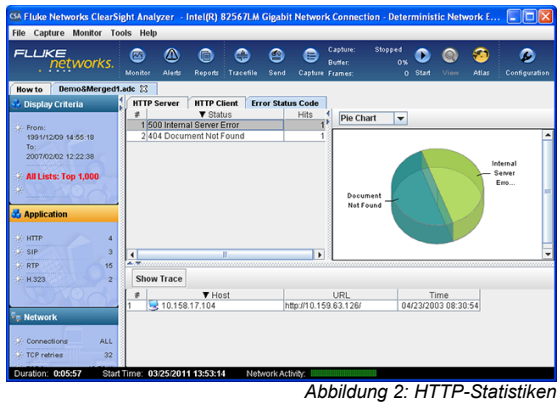


*Abbildung 2: HTTP-Statistiken*

## Zeitbasierte Analyse zur schnellen Erkennung von Problemen

Das Analysieren umfangreicher Erfassungsdateien kann eine Herausforderung darstellen, weil es generell einfach zu viele Informationen sind. CSA offeriert eine zeitbasierte Analyse der Erfassungsdateien, die ausführliche Statistiken und Trendinformationen bereitstellt. Sie können jederzeit einen Drill-Down ausführen, um angrenzende Ereignisse während der entsprechenden Zeitspanne anzusehen. Für Video und Voice-Datenverkehr, die SIP oder H.323 ausführen, kann die Analyse-Funktionseinheit die Video- und Voice RTP-Ströme auf Grundlage ihrer Qualitätswerte, des MOS oder VQFactor einstufen. Sie wird ausführliche Statistiken zu Anrufstatus und Anrufqualität von SIP oder H.323 bereitstellen. Sie können einen oder mehr der für die ausführliche Analyse oder Replay zu extrahierenden RTP-Ströme auswählen. Zusätzliche Analyse ist für HTTP verfügbar, mit aufgelisteten Tabellen mit Clients pro Server oder umgekehrt, zusammen mit den spezifischen zugegriffenen URLs sowie Fehlercodes. Mit dieser Analyse können Benutzer die Probleme schnell aufzeigen, ohne gründlicher in die Paket-Decodierungen zu recherchieren.

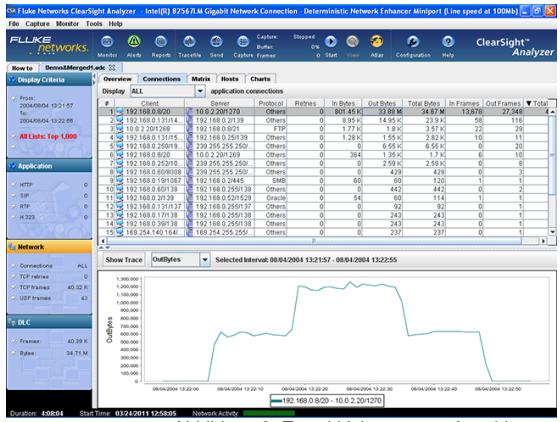



*Abbildung 3: Trend-Volumen von Anschlüssen*

## Automatisches Bounce-Diagramm

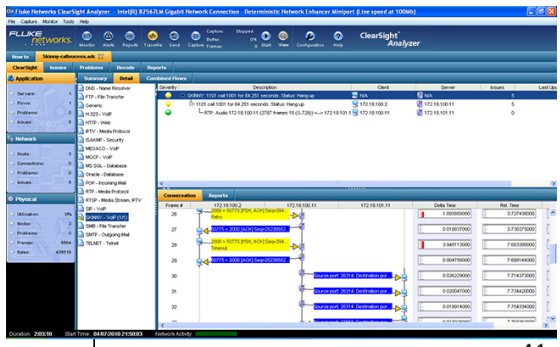
CSA erstellt automatische Bounce-Diagramme für jeden identifizierten TCP-Durchsatz. Damit wird die Dynamik des Paketflusses zwischen Clients und Servern grafisch dargestellt, ohne dass Pakete manuell decodiert werden müssen. Timing, Flussrichtung und Nutzlast-Zusammenfassung werden angezeigt, während TCP oder sonstige Fehler zur schnellen Identifizierung farbkodiert sind. Es bietet eine extrem leistungsfähige Möglichkeit, um Protokollwechselwirkungen zwischen den diversen Netzwerkelementen zu verstehen.

## Einzigartige Multisegment-Analyse

CSA unterstützt die meisten der gemeinsam verwendeten Erfassungsdateiformate. Es kann Pakete empfangen, die über maximal vier Netzwerkstandorte erfasst wurden, um daraus ein Multisegment-Bounce-Diagramm bereitzustellen. Dies ermöglicht die schnelle segmentweise Isolierung von Timing-Problemen zur Ursachenanalyse. Kombiniert mit den umfangreichen leistungsfähigen Dekodierfunktionen von CSA erhalten Netzwerkingenieure und Anwendungsanalytiker die Tools, um das Rätselraten zu beenden.

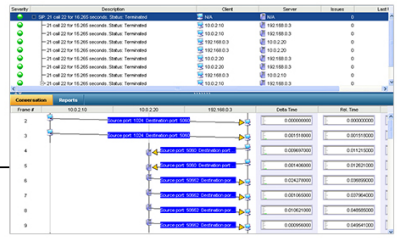
## Unterstützung von Triple-Play

Sprachqualitäts-Parameter einschließlich Paketverlust, Jitter, R-Wert und MOS werden grafisch dargestellt. Von MPEG2 über UDP implementiertes Streaming Video wird unterstützt. Der Support umfasst einen vollständigen Satz von Funktionen, einschließlich Decodieren, Filtern, Problemdefinition mit Warnungen, und einen vollständigen Satz von Berichten – Echtzeit, Geschichte, Ablaufverfolgungsdatei und Sprachqualität. Wiedergabe von Inhalten wird in Echtzeit und Post-Analyse unterstützt.



4-1

4-2



4-3

*Abbildung 4-1: VoIP Multi-Segment-Analyse — Abbildung 4-2: NAT Multi-Segment — Abbildung 4-3: SIP-Multi-Segment*

## Inhaltsrekonstruktion und Wiedergabe

Sie können Audio- und Videoinhalt von VoIP- oder Videoflüssen rekonstruieren, entweder während der Echtzeitüberwachung oder von einer Trace-Datei. Zusätzlich können Webseiten basierend auf Microsoft® Exchange® E-Mail, Fax over IP, Instant Messages und HTTP ebenfalls rekonstruiert werden. Dies ist als Nachweis bei Compliance-Verletzungen oder zur Visualisierung der Multimedienqualität sehr wertvoll.

5-1

5-2

5-3

*Abbildung 5-1: Videowiedergabe — Abbildung 5-2: E-Mail-Wiedergabe — Abbildung 5-3: Wiedergabe im Internet*

## Leistungsstarkes Filterschema

CSA unterstützt nicht nur einfache Adressen- und Protokollfilter, sondern auch auf Anwendungsbefehlen basierte Filter, IP-Teilnetzwerke, Datenschemata und anderen Kriterien. Komplexe Bedingungen (siehe Abbildung 6) können leicht spezifiziert werden, indem man Filterbedingungen mit AND-, OR- und NOT-Operatoren bei der Betrachtung des Einstellbereichs frei hinzufügt und kombiniert. Sobald eine Filterdefinition festgelegt ist, kann diese unter einem zugewiesenen Namen gespeichert und später zur Erfassung oder Trace-Dateianzeige wiederverwendet werden.

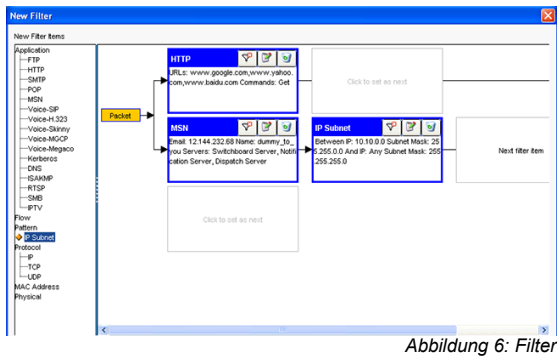



*Abbildung 6: Filter*

## Umfassender Verlaufsbericht

CSA bietet eine große Funktionsvielfalt an Standardberichten im Diagramm- und Tabellenformat, die Statistiken und die Leistung von Netzwerkverkehr, Server und Applikationen zeigen. CSA erzeugt Berichte aus Echtzeitdaten oder Trace-Dateien. Es erzeugt QoS-Berichte für Sprach- und Videoverkehr, die Quantitäten wie Jitter, Latenz, Paketverlust, MOS, J-MOS, R-Wert und Video-Qualitätsfaktor ausweisen. Elemente dieser berichte können leicht kombiniert werden, um anwendungsspezifische Berichte zu erstellen.

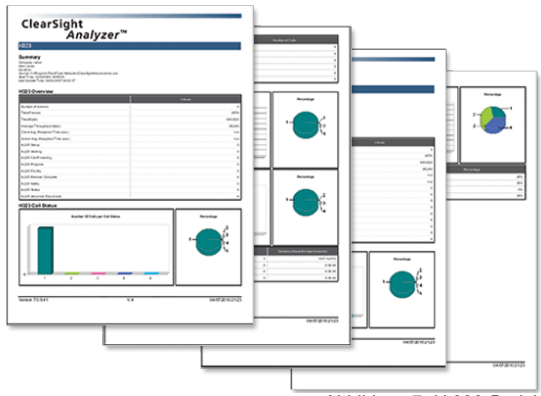



*Abbildung 7: H.323-Bericht*

## CSA-1045 fügt erweiterte optionale Funktionen hinzu

**History Reporter**

Produzieren Sie Netzwerk-, Anwendungs- und andere Trendberichte basierend auf über längere Zeit in Echtzeit gesammelte statistischen Daten.

**Packet Generator**

Ein vielseitig verwendbarer Generator erlaubt Ihnen, Netzwerkbelastungs- und Verkehrsreproduktionsprüfungen durchzuführen. Zwei Modi werden unterstützt: 1)Paketmodus: Ein bestimmtes Paket wird wiederholt gesendet, 2)Puffermodus: Der Datenverkehr wird von einer oder mehreren Trace-Dateien im Netzwerk erneut wiedergegeben.

**Multicast Analysis**

Die Multicast Visualizer-Option bietet Zähler und Statistiken, die das Verkehrsaufkommen auf jeder erkannten Multicast-Adresse beschreiben und quantifizieren. CSA extrahiert Multicast-Gruppenadressen (IGMP für IPv4 und MLD für IPv6) von Paketen, die von Hosts an Router gesendet werden.

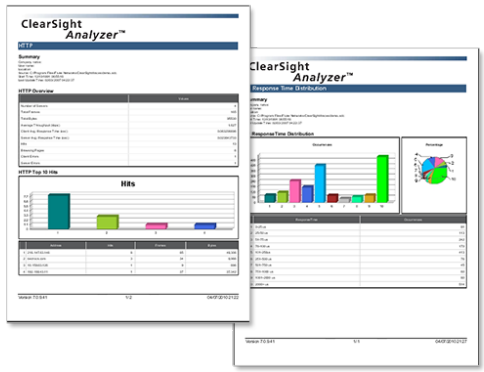
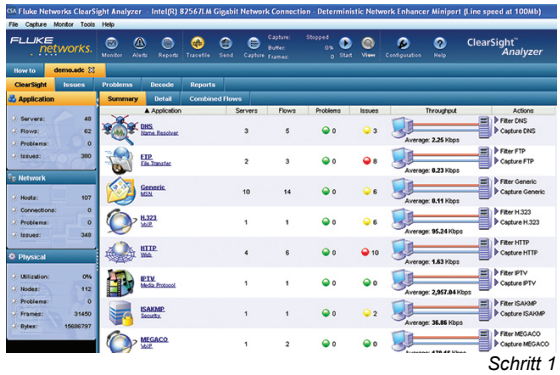



*Abbildung 8: HTTP-Bericht – Abbildung 9: IP-Response-Time-Bericht*

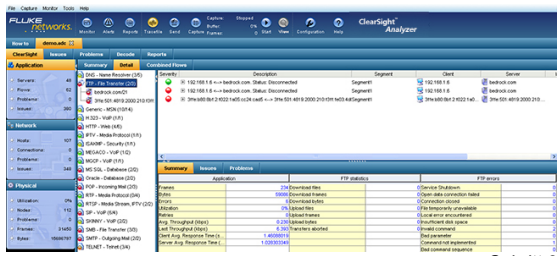
## ClearSight Analyzer - Applikationszentrierter Arbeitsablauf

Der ClearSight-Analyzer analysiert Anwendungsflüsse automatisch und kann Verkehrsaufkommen nach Anwendung klassifizieren z. B. HTTP, E-Mail und VoIP, um es leicht zu machen, den Ablauf von jeder Transaktion zu klassifizieren. Sie können auch die Untersuchung von der Datenfluss-Ansicht für eine Sitzung auf die Paketebene vertiefen und den Anwendungs-Inhalt rekonstruieren.



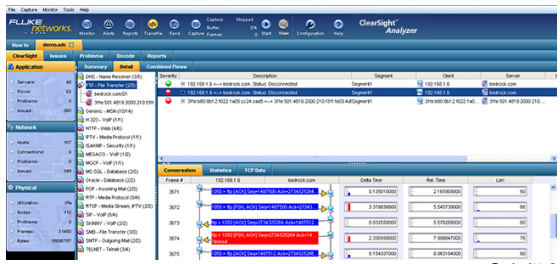
*Schritt 1*

**Schritt 1: Überwachung starten.**
Die Netzwerk-Datenverkehrsüberwachung wird automatisch gestartet. Datenverkehr wird nach Anwendung klassifiziert. Anwendungen mit Problemen und Fehlern können leicht mit gelben oder roten Symbolen identifiziert werden.



*Schritt 2*

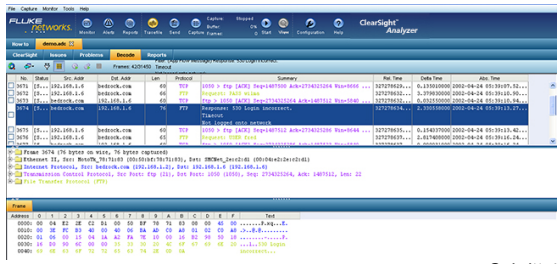
**Schritt 2: Applikation auswählen.**
Durch die Auswahl einer Anwendung wird eine Liste der jeweiligen Datenflüsse und ihrer zugeordneten Server und Hosts angezeigt. Ein rotes oder gelbes Symbol erscheint für Datenflüsse, bei denen ein Fehler oder ein anderes Ereignis erkannt wurde, daher ist es leicht zu sehen, welche Datenflüsse ein Problem haben.



*Schritt 3*

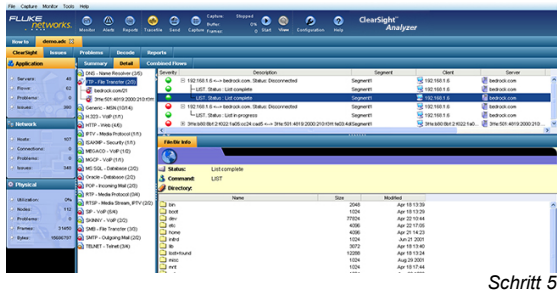
**Schritt 3: Datenfluss auswählen.**
Durch Klicken auf einen Datenfluss wird der Kommunikations-Datenfluss zwischen Client und Server (Leiter-Ansicht) angezeigt. Pakete, bei denen ein Fehler oder ein anderes Ereignis aufgetreten ist, werden durch einen roten oder gelben Pfeil gekennzeichnet, damit Sie schnell genau identifizieren können, wo und wann ein Kommunikationsfehler aufgetreten ist.

**Schritt 4: Automatische Filter/Paket-Decodierungsanzeige.**
Mit einem Klick auf die Anzeige der Applikations-Datenflussanzeige (Leiter-Ansicht) wird der Paket-Übersetzungsbildschirm geöffnet, der gefiltert wird, um nur die zugeordnete Transaktion anzuzeigen.
So sind nur einige Klicks erforderlich, um von der obersten Applikationsebene zur Anzeige des detaillierten Pakets zu gelangen, wodurch die Fehlerbehebung schneller und einfacher wird.



*Schritt 4*

**Schritt 5: Anwendungsinhalt wiedergeben.**
Der Anwendungsinhalt über einen ausgewählten Datenfluss kann in ClearSight reproduziert werden, um den tatsächlichen Inhalt anzuzeigen.



*Schritt 5*

## Zusammenfassung der Merkmale

| Modell | Beschreibung |
|---|---|
| Seite Anwendungsorientierte Zusammenfassung | Sie können sofort die Problem-Schichten sehen und schnell den Gesamtzustand vom überwachten Echtzeit-Datenverkehr oder der Trace-Datei bestimmen |
| Echtzeitüberwachung von Anwendungen | Siehe die Ansichten des Anwendungs- und Konfigurations-Datenflusses mit oder ohne Erfassung von Paketen |
| Expert-Alert-Funktion | Problem-Schwellenwerte festlegen und sofort sehen, wenn eine Anwendung, ein Server oder ein Datenfluss ein Problem hat. Programm-E-Mail-, Pager-, Script- oder SNMP-Aktionen, die bei Auftreten eines Problems ausgelöst werden. |
| Zeitbasierte Analyse von Trace-Dateien | Für Trace-Dateien bis zu 4 GByte die Analyse basierend auf einem vom Benutzer bestimmten Zeitbereich für Pakete innerhalb der Trace-Datei festlegen. Die Analyse umfasst die Anwendungsleistung für HTTP, H.323, SIP und RTP, Trending Network Layer-Eigenschaften wie Auftreten von TCP-SYN, Übertragungswiederholung, IP-Matrix und Host, auf Datenverkehrsaufkommens-Trends nach Frameanzahl/Byte/Frame-Größenzahl. Benutzer können Pakete exportieren, die den Display-Kriterien entsprechen, um eine anwendungszentrische Analyse durchzuführen. |
| Protokoll erzwingen | Protokoll erzwingen wird während der Echtzeit-Überwachung oder beim Wiedergeben einer Ablaufverfolgungsdatei angewendet, um ein in ein anderes Protokoll eingekapseltes Protokoll zu identifizieren |
| Zeitmessungsanzeige für Anwendungskonversation | Netzwerkverzögerungen und lange Reaktionszeiten stehen direkt aus der Ansicht des Anwendungs-Datenflusses heraus und identifizieren langsame Befehle, schlechten Service oder Anwendungs-Leistungsprobleme |
| Multi-Segment-Ansicht | IP-Paketfluss, UDP oder TCP zwischen zwei Hosts oder Server und Client über mehrere physische Segmente korrelieren. |
| Umfassende Filterfunktionen | Einschränkung der Überwachung, Erfassung oder Anzeige auf die Dinge, die Sie interessieren, indem Sie Filter basierend auf Anwendungsbefehlen, IP-Subnetzen, Datenmustern und vielen anderen Kriterien erstellen. Komplexe Filter aufbauen mit AND, OR und NOT-Operationen. Benennen, Speichern und Wiederverwenden von Filtern |
| Schnelles Erfassen oder Anzeigen der Filtererstellung | Rechtsklicken auf einen Datenfluss zur Anwendung eines Erfassungs-/Anzeige-Filters nur für diesen Datenfluss |
| Vollständige Paket-Decodierungen (mit Unterstützung für Jumbo-Frame) | Wechseln Sie zu einer Registerkarte „Decode“, um traditionelle vollständige Paket-Decodierungen in Zusammenfassung, in Detail und Hex-Bildschirme während der Echtzeit-Überwachung oder aus einer Trace-Datei anzuzeigen |
| VOIP Anrufprotokoll-Browser | Wenden Sie einfaches Filtern und Sortieren zum Suchen nach einzelnen Anrufen mit Kriterien wie Startzeit, Anrufdauer, IDs von Anrufer und Angerufenem sowie MOS-Wert während Echtzeit-Überwachung |
| Sprach- und Video-QoS-Analyse | Wenn erkannt wird, dass ein RTP-Datenfluss einen Video-Stream enthält, zeigt der ClearSight™ Analyzer VQFactor™-Statistik für die Videokomponente sowie MOS-Statistik für die Audio-Komponente an |

## Technische Daten für das Protokoll

| Protokoll | Beschreibung |
|---|---|
| Unterstützte Nicht-VoIP-Applikationen | 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 |
| Unterstützte VoIP-Applikationen | 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 MA, SUA, M2PA, M2TP, M2UA: RFC 3331, SS7 MTP2 MA, M3UA: RFC 3332, SS7 MTP3 UA, MAP, SCTP, ISUP), RTP, RTCP, RTSP |
| Audio-Codecs abspielen (decodieren) | G.711 (µ-law und 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_Schicht (I, II-TS, III, IV), iLBC, AMR (GSM, 3GPP), ASF |
| Mobil-Protokoll | Unterstützung für 3G-324M und LTE, das übergeordnete Protokoll für Videotelefonie in den mobilen 3G/4G-Netzwerken |
| EOAM-Decodierung | Ethernet-OAM-Frames im sowohl ITU- als auch IEEE-Format |

*Bemerkung: Unvollständige Liste wird oben gezeigt. Für eine vollständige Liste besuchen Sie bitte enterprise.netscout.com/protocolsupport*

## Systemanforderungen

| Artikel | Minimale Anforderung |
|---|---|
| Computer | Dem Industriestandard entsprechender Computer (Laptop oder Desktop) mit CD/DVD-ROM-Laufwerk für die Softwareinstallation |
| Prozessor | Pentium 4 (oder gleichwertig) mit mindestens 1 GHz (2 GHz empfohlen) |
| RAM | Min. 512 MB (1 GB empfohlen)<br>Mind. 2 GB, wenn Windows Vista oder Windows 7Professional ausgeführt werden |
| Festplattenspeicher | Festplatte mit 40 GB, mit mindestens 15 GB verfügbarem Speicherplatz |
| Betriebssystem | Microsoft Windows XP Home Edition mit SP3 (Firewall deaktivieren)<br>Microsoft Windows XP Professional mit SP3 (Firewall deaktivieren)<br>Microsoft Windows 7 Professional (32 und 64 Bit)<br>Microsoft Windows 8.x Professional |
| Bildschirm | Festplatte mit 40 GB, mit mindestens 15 GB verfügbarem Speicherplatz |
| Betriebssystem | Netzwerkverbindung mit NDIS-kompatiblem Netzwerkgerätetreiber |

## Produkt und Optionen

| Modell | Beschreibung |
|---|---|
| CSN/CSA-1000 SUPP-MSTC | ClearSight Analyzer-Software |
| CSN/CSA-1000CD SUPP-MSTC | ClearSight Analyzer-Software auf CD |
| CSN/CSA-1045 SUPP-MSTC | CSA mit IP Multicast Visualizer, History Reporter und Option für Packet-Generierung |
| CSN/CSA-1045CD SUPP-MSTC | CSA mit IP Multicast Visualizer, History Reporter und Option für Packet-Generierung auf CD |
| CSN/OPT-3045 SUPP-MSTC | IP Multicast-Visualisierung, Hist Reporter und Packet Gen für CSA |

## Support

| Modellnummer | Beschreibung |
|---|---|
| GLD-SW-1000 | MasterCare-Support Services, 1 Jahr Softwarewartung für CSA-1000 |
| GLD–SW–1045 | MasterCare-Support Services, 1 Jahr Softwarewartung für CSA-1045 |