

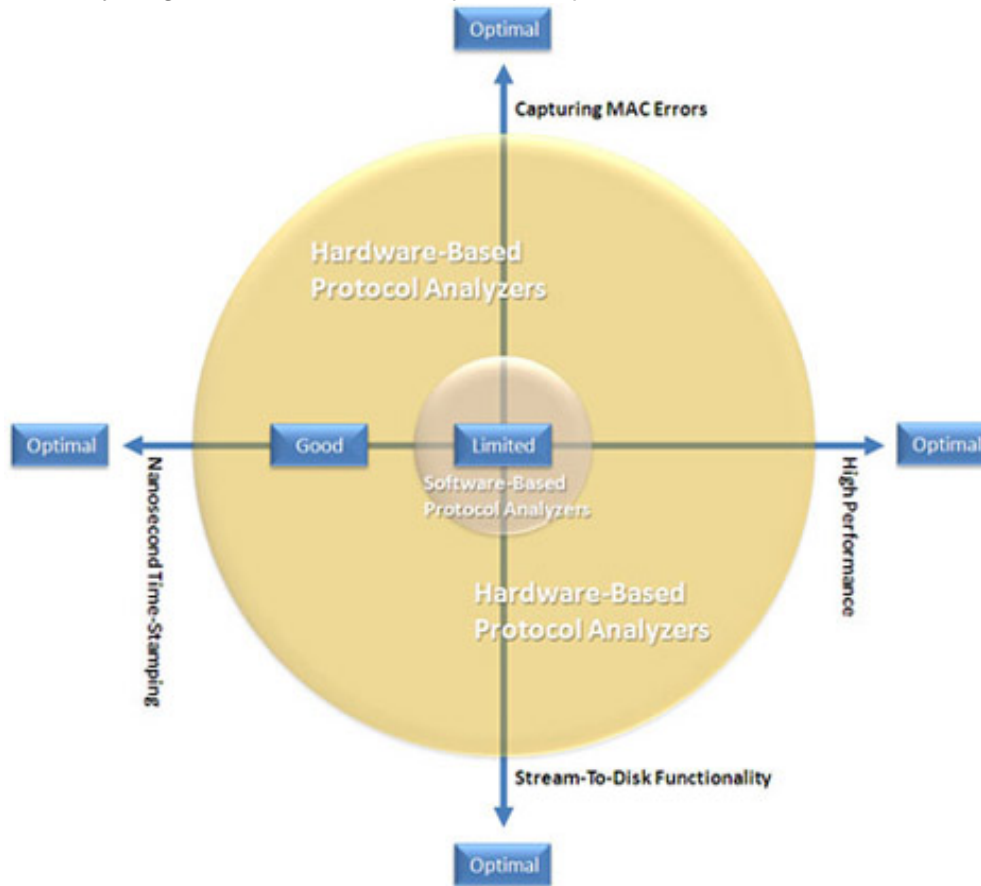
ClearSight Networks Newsletter

ClearSight External Newsletter
Sep 2009

Choosing the Right Protocol Analyzer

A protocol analyzer is computer software and/or hardware that can interpret traffic passing over a network. As data streams flow across the network, the analyzer captures each packet and decodes and analyzes its content according to the appropriate specifications.

Protocol analyzers are used to monitor network usage and resolve network problems; they can be especially helpful in identifying incidence of malicious software passed through a network. Take, for example, the recent Conficker worm that slithered onto computers on April 1 via peer-to-peer (P2P) network connections. By utilizing an analyzer to detect P2P traffic running on a network, an organization can obtain a more accurate picture of what is happening on its network. After pinpointing the offending parties, an organization is able to successfully mitigate the risk and institute policies to prevent re-occurrences.



Hardware-based protocol analyzers are superior to software-based analyzers on many dimensions

[Click to enlarge](#)

In this Issue

- ▣ [Choosing the Right Protocol Analyzer](#)
- ▣ [Rackmount or Portable? – Choosing the Right NTM](#)
- ▣ [What is a Codec?](#)
- ▣ [With NTM/CSA 7.0.6, ClearSight Networks' Superior User Experience Delivers More Effective Network Monitoring and Analysis](#)
- ▣ [eWeek's Products to Watch](#)
- ▣ [Protocols Supported on ClearSight Products](#)
- ▣ [The Lesser Known Features of the Network Time Machine](#)
- ▣ [News Flash](#)

Webinars

- ▣ [Using ClearSight Analyzer to Generate Packets](#)



[Download the Video](#)

- ▣ [Using ClearSight Analyzer Reports for Network Data Analysis](#)

Demand is also surging for high-valued services, including VoIP, video telephony, and Web conferencing. Troubleshooting the problems that emerge within these services is becoming ever more complex for network administrators.

With the large number of protocol analyzer products on the market today, how can an organization decide which will provide the best value for their network? The decision ultimately comes down to a software-based protocol analyzer and a hardware-based one. The most popular protocol analyzer is software-based and is available for Windows or Linux PCs, partially because it is freeware.

[more](#)

Rackmount or Portable? – Choosing the Right NTM

Once you have become familiar with the many network recording and analysis benefits that ClearSight's [Network Time Machine \(NTM\)](#) provides, it may remain for you to make the choice between our Portable2 model and a rackmount version. Some factors that may affect your decision are:

- Does most of the network traffic of interest flow through a single location, such as a switch?
- Is this location remote from where the network administrator works?
- Is there more than one member of the IT staff that might need to access the NTM?
- Are there several locations where you might want to set up a long-term recording capability?
- Do you need a very large (greater than 1.6 TB) storage capacity for your captured data?



Let's examine each of these factors.

Does most of the network traffic of interest flow through a single location, such as a switch? In this situation, both the Portable2 model and the rackmount versions could be suitable. A final decision might involve some of the other factors.

Is this location remote from where the network administrator works? If the location is remote from where the network administrator works, then a rackmount version is usually better. Even where the location is not physically remote (as in another city) it could be logistically easier to use the rackmount configuration, as with some wiring closets.

Is there more than one member of the IT staff that might need to access the NTM? In this situation the added capabilities of the NTMD system may make it a lot easier for multiple users to access information from a rackmount version. NTMD is not available on the Portable2.

Are there several locations where you might want to set up a long-term recording capability? If the locations are all easy to get to, then it is possible that a portable NTM would be an economical and adequate solution. IT staff could simply move the portable NTM among various points of interest. However, this would be a little more labor intensive, especially for comparing data from the various locations. You should consider the additional advantages of the NTMD system, including the Central Problem Manager, which can gather and display alarms from several remote NTM Agents in a single convenient place. If the remote locations are physically far apart, then having several remote rackmounted NTM Agents would be far better.

Do you need a very large and scalable (greater than 1.6 TB) storage capacity for your captured data? If you need the extra storage capacity, as for example to do long-term baselining on high-traffic networks, then a rackmounted version would be better.



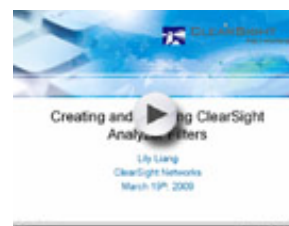
[Download the Video](#)

- ▣ [Using ClearSight Analyzer for Postcapture Analysis](#)



[Download the Video](#)

- ▣ [Creating and Applying ClearSight Analyzer Filters](#)



[Download the Video](#)

▶ Past Issues

- ▣ [Jul 2009](#)
- ▣ [May 2009](#)
- ▣ [Mar 2009](#)
- ▣ [Jan 2009](#)
- ▣ [Nov 2008](#)
- ▣ [Sep 2008](#)
- ▣ [Jul 2008](#)
- ▣ [May 2008](#)
- ▣ [Mar 2008](#)

Rackmounted versions are available with up to 44 TB of storage for captured data.

Don't be hesitant to ask for our help in making your decision. Our sales people can assist you in accessing exactly what you need. Just contact sales@clearsightnet.com.

What is a Codec?

Many network administrators and managers find the audio and visual reconstruction and replay capabilities of ClearSight products to be extremely useful in determining the root cause of streaming media problems. The ability to "listen" in or "view" live conversations and subjectively evaluate them is an important complement to the quantitative metrics offered by most tools such as MOS or R-Value for audio or VQFactor for video.

Because the transmission of multimedia content is bandwidth intensive, it is often first encoded or compressed prior to the multimedia stream being sent over the network, and then decoded or decompressed at the receiving end. Codecs are the algorithms or programs that perform these functions.

There are literally thousands of audio and video codecs available. Some are based on open standards while others are proprietary and require licensing; well-known codecs include MP3, DivX, and QuickTime.

Not all network solutions support multimedia playback; the [ClearSight Analyzer](#) and [Network Time Machine](#) products, however, do support a rich set of codecs, allowing users to actually see and hear the wide variety of multimedia traffic that is present in modern day networks.

eWeek's Products to Watch

From the new product section of eWeek: ClearSight Networks' Network Time Machine 7.0 enables enterprise network administrators to quantify voice quality on 3G mobile networks and meet the demands of increased network traffic and mobile Internet services. NTM captures and analyzes data from audio and visual network transmissions – such as video conferencing, multimedia entertainment services, surveillance, live video broadcasting, and video-on-demand.



With NTM/CSA 7.0.6, ClearSight Networks' Superior User Experience Delivers More Effective Network Monitoring and Analysis

ClearSight Networks, a worldwide provider of award-winning application and analysis tools for today's dynamic networks, announced enhanced usability features in its [ClearSight Network Time Machine®](#) (NTM) — powered by [ClearSight Analyzer](#) (CSA), an advanced network monitoring and troubleshooting tool. Providing the deep network insight and visibility required for today's complex and multi-protocol networks, the new NTM/CSA emphasizes the IT end-user experience with an intuitive interface promoting easier navigation and extended capture and record capabilities.

Read the press release at [HERE](#).

ClearSight customers on the SUS program can download the new 7.0.6 CSA software from the support area on our website at: <http://www.clearsightnet.com/support.php>

A trial version of the CSA 7.0.6 software is also available on our website at: <http://www>.

clearsightnet.com/resources.php

Protocols Supported on ClearSight Products



Through the use of ClearSight Networks' own proprietary and other embedded third party decode engines, the ClearSight Analyzer and Network Time Machine products support nearly 1,000 protocols, including many used in the transmission of multimedia data. It is even possible for proprietary decodes to be supported through the use of custom dissectors. For a comprehensive list of supported protocols, please see the collateral [List of Supported Protocols](#)

[more](#)

The Lesser Known Features of the Network Time Machine

"Oh, is that what that button is for..." How many times have you mumbled that to yourself after running across a newly discovered option in your car while driving around town. Not exactly life changing but it sure would have made life just a tad simpler. Let's apply it to our "geek" world of ClearSight network monitoring.

Are you aware of some of the subtle capabilities of your network monitoring applications and tools? Here's a sampling of seldom used features in ClearSight's Network Time Machine that may prove very useful during your network monitoring sessions:

- Port Labeling -- stores each Ethernet frame with a user definable text associated with the physical NTM monitoring port. This is a really nice feature when viewing frames in the Conversation tab. It allows the user to easily identify each frame's point of origin.
- Application Port Definitions -- allows customization of existing port numbers. It also allows definition of custom applications associated with a range of port numbers. You now have a way of tracking custom application statistics and flows, since they will appear in the Application Summary screens.
- Hardware Filtering -- allows the user to filter only frames of interest based on layer 2, layer 3, or application characteristics. This saves storage since all the "noise" will be filtered out beforehand.
- "Free" Pattern Filtering -- a software filtering option that allows matching of byte patterns at variable offsets rather than at a fixed offset. This is useful for finding text in the application layer that may appear anywhere in the payload.
- Protocol Forcing -- skips a specified number of bytes before interpreting frames of a particular protocol type. May be used when IP headers are encapsulated inside non-Ethernet frames. This allows NTM to run its application analysis for layer 3 and above.

If you have any questions on any of the above, feel free to contact us at info@clearsightnet.com.

News Flash

This section is aimed at keeping you informed with the most recent ClearSight news and articles.

Enhanced Usability Features for ClearSight Network Time Machine Launched by ClearSight Networks

(TMCnet.com - Sep 29, 2009) ClearSight Networks has reportedly launched enhanced usability features for its ClearSight Network Time Machine (NTM). The NTM is powered by ClearSight Analyzer (CSA), an advanced network monitoring and troubleshooting tool. Read the full article at TMCnet.com.

Top VoIP Technologies & Trends

(Processor - Sep 11, 2009) After more than a decade as the Next Big Thing in IT, Voice over IP is finally starting to realize its longheld promise as a costeffective enabler of agile business. Ever cheaper and wider bandwidth, more tightly integrated applications, and rapidly improving quality of service are quickly addressing the obstacles that have kept some organizations from jumping in. Read the full article at Processor.

ClearSight Rethinks Cronos Latency Product

(Inside Market Data - Jul 20, 2009) Fremont, Calif.-based network monitoring provider ClearSight Networks has suspended development of version 2.0 of its Cronos execution latency monitoring products as a result of the current economic downturn, officials say. Read the full article at Inside Market Data.

Network Time Machine, Network Time Machine Express, ClearSight Apex and Network Time Machine Atlas are registered trademarks of ClearSight Networks.

ClearSight Networks | 46401 Landing Parkway | Fremont, CA | 94538-6496
Telephone (US Toll Free): 1-800-825-7563 | (International): +1-510-824-6000 | Fax: 1-510-824-6100
Email: marketing@clearsightnet.com | Web: www.clearsightnet.com
Copyright 2004 - 2009 ClearSight Networks, All Rights Reserved.