

Innovative Ideas from the "Network Storage and Analysis" Experts

# ClearSight's Atlas Gives You a Clear, Complete View of Your Network

by Richard "Zippy" Grigonis

ClearSight Networks ([www.clearsightnet.com](http://www.clearsightnet.com)) is known for its ClearSight Network Time Machine® (NTM), a multiuser, turnkey appliance for Fortune 1000 companies that goes far beyond traditional protocol analyzers and "sniffers" with its ability to capture up to 13 terabytes of data (44 terabytes if you order the special configuration) over four 1 gigabit Ethernet links, thanks to a special RAID storage subsystem. (13 terabytes represents about 26 hours of continuous capture on a fully-saturated 1 gigabit Ethernet line. But network load levels rarely max out – they typically run at only 20 percent capacity. So, multiplying 26 hours by 5 yields an amazing 130 hours of data capture.)

And now, ClearSight offers a particularly useful option available for the NTM – the Atlas Navigation System. With network recorders becoming more and more popular, and now with the ability to store many terabytes of data, there's no way humanly possible to carefully analyze so much network traffic, nor would anybody want to do it. That's why ClearSight created Atlas – to do the 'heavy lifting' for you.

"Our new Atlas option is a software module that runs on the NTM and acts as a processing engine," says Steve Wong, ClearSight's Vice President of Marketing. "As the NTM captures packets, Atlas can index, categorize and make sense of these terabytes of network data and certain applications without resorting to complicated packet decodes, and that information is then stored in another, relational database. For example, this first release of Atlas can index many of the Voice-over-IP (VoIP) applications that use such protocols as SIP (Session Initiation Protocol), RTP (Real-Time Protocol) and H.323. Atlas can also index HTTP traffic and future releases call for support of additional applications."

Atlas allows you to do your own packet decodes if you like, almost 1,000 protocols are supported, but most people generally prefer to avoid such minutia and instead start troubleshooting at the network's highest layer, not the lowest. That's why Atlas is particularly strong in generating reports for VoIP and HTTP-type applications. It also provides you with all of the network

layer information. For example, if you were looking at a VoIP application, Atlas will display all relevant metrics and statistics, such as latency measurements, MOS [Mean Opinion Score], jitter measurements and R-values regarding the Quality of Service [QoS] of your voice signal. Atlas can show you trending graphs and other visual representations of what's happening in your network.

"In fact," says Wong, "that's the reason we call the product Atlas – the software works like a geographic Atlas for your network. You can look at a high level and see 'continents' of applications, and then you can drill down into the network and see what's happening in the 'cities' of the packets in the lower layers."

"Customers who buy the NTM appliance from us can insert it into the network via a tap or mirror ports and they can get it up and running within about half an hour," says Wong. "Now they can not only capture data, but make sense of it with Atlas processing."

NTM should be great for people who do "data forensics". For example, let's say something happened in the network last week. With a conventional analyzer, chances are that you certainly missed the event and there's no way you can troubleshoot the problem "after the fact". The only thing you can do is set a trigger and wait for the event to – hopefully – occur again. But because of the NTM's storage capabilities, you can actually "go back in time" to the event as it happened a week ago, say, and play it out and take a look at it. That's a tremendous help.

"The NTM can be used to verify various forms of compliance, such as Sarbanes-Oxley," says Wong. "And you can use it to determine if people are accessing your network illegally, and, if they are, you now have evidence of that. So the NTM can be used in law enforcement applications, too. And when you combine the NTM with Atlas, you can examine an application and then 'drill down' to the network layer, all the way to the DLC [Data Link Control] layer, look at the packet decodes, and then switch your focus back to a higher level. This contextual way of troubleshooting and protocol analysis is really the way network engineers should do testing as the industry moves forward."

There are probably many other applications suitable for the NTM and Atlas that are out there waiting to be discovered by ClearSight customers. Perhaps you'll find one for your own business.

Network Time Machine pricing starts at US\$33,700. **IT**