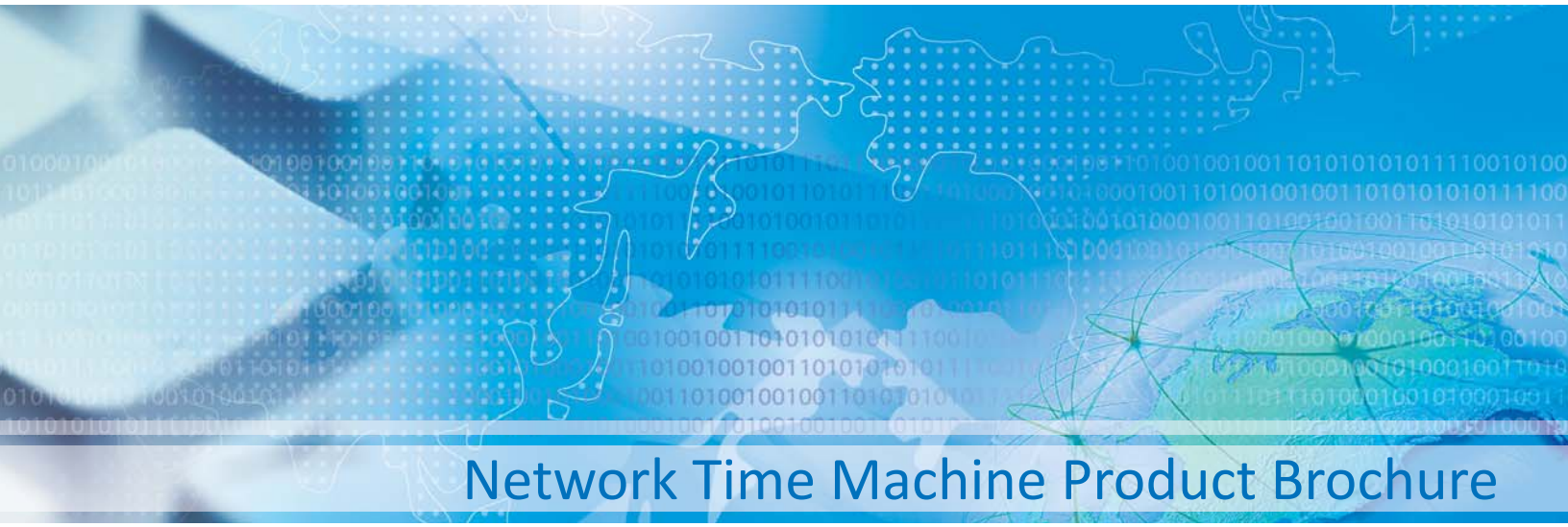
ClearSight Networks™



# Network Time Machine Product Brochure

Long Term Capture,

Network Forensics and Data Mining,

Performance Monitoring,

Protocol Analysis Appliance for R&D,

Service Provider, and

Enterprise Network Environments

***New! 10 GbE Support!***

***New! NTM Express!***

The ClearSight Network Time Machine® (NTM) is designed to provide unprecedented levels of prevention and diagnosis on Ethernet based networks. The solution allows extended capture and store capabilities coupled with deep packet monitoring, inspection and analysis functionality. With the new Atlas module available in version 6.5, users now have a powerful, time-based, historical analysis product set to capture, index and archive all network traffic. The fully turn-key appliance offers multi-user capabilities, allowing for up to four simultaneous users to access a single NTM probe.

## DIAGNOSIS AND PREVENTION IN ENTERPRISE NETWORK MANAGEMENT

Network IT groups that are chartered to manage complex network environments require a sophisticated set of tools and capabilities for the monitoring and diagnosis of network problems and issues. The complexity of many enterprise LANs is directly related to the multiple numbers of network elements and layers: from switches to routers to load balancers to firewalls and even operating systems. In addition, today's corporate networks carry multiple tiers of data from voice traffic to video to email information.

Traditional protocol analyzers cannot provide the sophisticated diagnosis and prevention capabilities necessary to manage, maintain and support even the most modest of enterprise networks. Intermittent and acute network problems must be quickly diagnosed and a solution immediately applied. More chronic and systemic problems must also be quickly detected and resolved. Typically these tools are equipped with very small amounts of physical buffer space. This limitation makes it extremely difficult, if not impossible, to diagnose many problems plaguing enterprise networks today.

## CLEARSIGHT NETWORK TIME MACHINE FAMILY

ClearSight Network Time Machine (NTM) can be used to effectively manage and diagnose problems affecting enterprise networks (*see Figure 1*). Its unique capabilities maximize the network administrator's ability to proactively monitor and analyze their networks to maintain network uptime and stave off unexpected outages which can adversely affect mission critical applications and ultimately enterprise business. Users can ensure the health and reliability of their networks by pinpointing problems and performance bottlenecks that other network monitoring and analysis solutions cannot even detect.

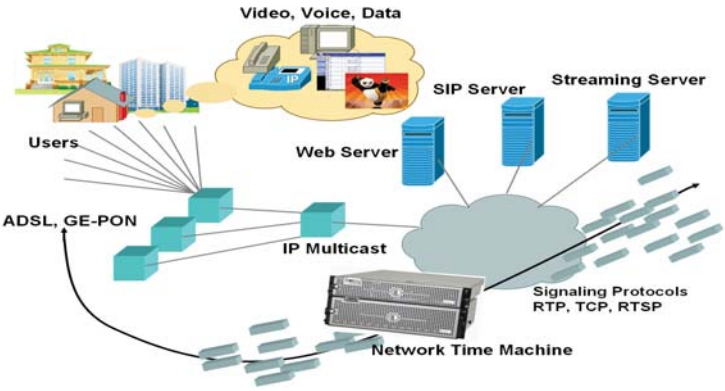



*Figure 1: Deploying NTM into an Enterprise Setting*

## NETWORK TIME MACHINE WORK FLOWS

Strategically located at varying points and segments in an enterprise network, the NTM monitors and captures every single packet. Unlike some products which rely on a generic network interface card, the NTM employs a sophisticated FPGA processor based line card.

The card can capture four GbE links (or two 10 GbE links on the 10 GbE version) continuously without ever dropping a packet, even at full line rate with filtering and trigger functions fully enabled. Many experienced engineers will tell you that the loss of even a single packet within an application flow can make analysis difficult, if not impossible.

The captured data are monitored extensively—relevant LAN metric, graphs (*see Figure 2*) statistics and alerts are accessible to NTM users through a powerful, but simple-to-use graphical user interface.

It is from within this context that the administrator can launch into their analysis and troubleshooting work. During real-time monitoring, reports can be created and viewed.

*Figure 2: Physical Layer Trend Display*

The NTM solution can capture up to 44 terabytes (configuration B)[1] of network traffic. This makes it possible to capture almost 38 days of data on single GbE link of a typical corporate network (*see Figure 3*)[2]. Difficult applications, including data forensics, SOX compliance verification, and data mining become possible to the network administrator.

| | 10 Mb/s | 100 Mb/s | 1 Gb/s | 2 Gb/s | 4 Gb/s |
|---|---|---|---|---|---|
| Express | 44 days | 4 days | 11 hours | 5 hours | 2.5 hours |
| Portable2 | 142 days | 14 days | 34 hours | 16 hours | 8 hours |
| Standard2 | 142 days | 14 days | 34 hours | 16 hours | 8 hours |
| Premium2 | 375 days | 38 days | 4 days | 2 days | 1 day |
| Configuration A[1] | 3 years | 101 days | 11 days | 6 days | 3 days |
| Configuration B[1] | 12 years | 353 days | 38 days | 21 days | 11 days |

*Figure 3: Length of Time a NTM Can Capture Network Traffic[1]*

## CLEARSIGHT ANALYZER

The award-winning ClearSight Analyzer (CSA) is integrated with the NTM, providing unparalleled protocol analysis and decode capabilities (*see Figure 4*). The NTM can be put into CSA mode and turned into a standalone protocol analyzer that is not limited by the size of the analyzer's capture buffer like many traditional analyzers.

CSA offers complete Triple-Play support, providing analysis tools for most video and voice codecs. It allows for the reconstruction and playback of both video and audio streams, and instantly identifies network problems and issues.

[1] *Special order item; please check with ClearSight*
[2] *Assuming network utilization rates that average 10%*

In addition, CSA offers sophisticated capabilities not found on most analyzers. A multi-segment ladder display (*see Figure 5*) shows the progress of data between multiple exchange points on a network making it easy to pinpoint the source of a problem. The analyzer supports over 1,000 protocols (*see Figure 6*) including many from the Ethernet family. A choice of two decode engines allows you to harness the power of third-party solutions.

*Figure 4: Trace File Workspace*

## NETWORK TIME MACHINE CONFIGURATIONS

The ClearSight NTM architecture maximizes the LAN engineer's ability to implement a wide variety of configurations, based on the business needs, as well as to add NTM and NTM components as budget and time permits.

The NTM is managed through an Agent Manager which can be located locally on the NTM or on any Windows based PC. The client can access and control an NTM from anywhere in the world through an IP network. Each NTM can support up to four con-current users. The Agent Manager can in turn manage multiple numbers of NTMs.

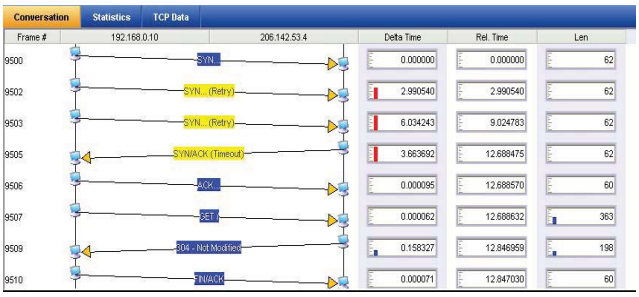


*Figure 5: Ladder View*

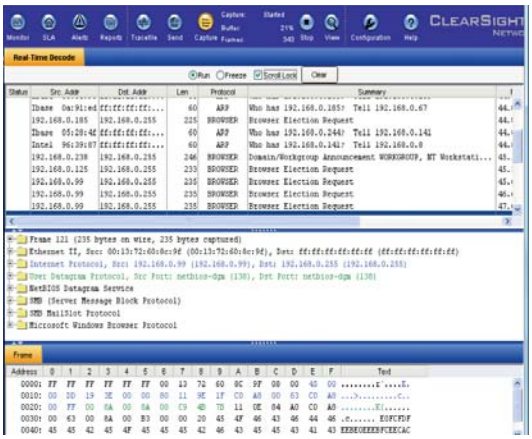


*Figure 6: NTM Also Provides Traditional Protocol Analysis*

## NETWORK TIME MACHINE ATLAS

A key feature of Atlas and the NTM platform is the ability to capture, index, and classify complex network information. At the heart of the index and classification engine is a powerful RDMS (relational database management system) which crunches and makes sense of volumes (many terabytes worth) of network data in near real time.

This information is then used to create unique views that are critically valuable to assisting network engineers and administrators to proactively manage and service their networks. These views are shown in the Atlas workspace, and are easily accessible by a few mouse clicks.

It is similar to the way in which one can use, say, a world atlas combined with a powerful almanac – first they see large area maps such as continents, then they can dive in to see detailed maps of much smaller areas such as states and cities, and then, they can look up relevant statistics such as population, climate, and economic data – except in this case we are talking about an enterprise class Ethernet network.

The framework provides an extremely intuitive method of troubleshooting networks, and represents a revolutionary new way to manage and service your them.

Atlas is currently designed to support four main upper layer application types: HTTP, H.323, SIP, and RTP. Future revisions of the software will support additional applications and functionality.

For example: for the H.323 VoIP application, a network engineer can review all the H.323 (*see Figure 7*) data that has traversed the network over the last few days. You can also check the quality of the calls and where they were first initiated. For calls that have low MOS scores, which is an indicator of poor audio quality, the engineer may drill down to look at the network at the instance in which the problem might have occurred — and then may choose to drive in and look at the packet decode, and perform packet analysis (*see Figure 6*).

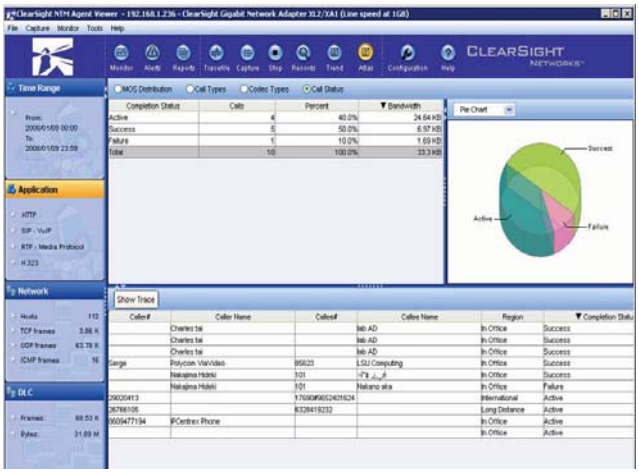


*Figure 7: Call Status Distribution in the Atlas H.323 Application Display*

Performance bottlenecks and issues are often very difficult to detect. They are even more difficult to characterize and remedy. Atlas provides a wealth of performance data, including network latency and jitter, which are key metric for understanding multimedia IP performance; service/application response times and network throughput are also important statistics to gauge how good the QoS experience is with applications such as H.323 and SIP.

## NETWORK TIME PROTOCOL SUPPORT

Fundamental to all network monitoring and analysis solutions is the notion that frames and packets that are observed and captured are accurately time-stamped. Without this, these solutions would fail to detect a network anomaly or could report one that is not there. It could also hinder root-cause analysis once a problem is detected. Synchronization with NTP Servers ensures that captured network information, log files, reports, and application flows are time-stamped accurately.

| Features | Benefits |
|---|---|
| HIGH PERFORMANCE HARDWARE CAPTURE | Never drop a packet during capture, even at full line-rate with filtering and packet slicing fully enabled and 4 port capture turned on |
| HARDWARE BASED 10NS TIMESTAMPING | Accurately time stamp 4 GbE links to 20ns resolution in hardware; and 10ns for 10 GbE |
| CAPTURE AND STORE UP TO 44[1] TERABYTES | Capture, store, index, categorize, archive and recall up to 44 TBs of network data. Perform packet analysis and decode on the fly |
| HARDWARE TRIGGERS AND FILTERS | FPGA/hardware implemented filter and trigger capabilities at full line rate speeds |
| REAL TIME NETWORK MONITORING | Show network statistics and information with trending graphs. Easily identify throughput problems and anomalies |
| PAYLOAD SLICING | Save valuable buffer capture space by capturing only important protocol information |
| PROTOCOL ANALYSIS and DECODES | Show packet decodes and perform packet analysis for nearly 1,000 protocols including those in the TCP/IP, UDP/IP, RTP and HTTP families -- at all 7 layers of the OSI networking model. Understand protocol interactions completely |
| VIDEO AND VOICE PLAYBACK | Reconstruct and replay both video and voice data in real time and under post-capture scenarios |
| R-VALUES and MOS STATISTICS | Assess voice quality over long durations of time |
| MDI AND VQFACTOR METRICS | Characterize video quality over an extended period of time |
| MULTI-SEGMENT ANALYSIS | Perform time correlated analysis across 4 network segments. Track application flows through routers, switches and network points |
| ATLAS NAVIGATION SYSTEM | Mine network data, and conduct data forensic over a long period of time; drill down on application structure for lower layer information |
| PROTOCOL LADDER VIEWS | Reveal the progress of network transactions in an easy to follow display |
| MULTI-USER, REMOTE ACCESS | Support up to 4 concurrent remote users |
| ENTERPRISE CLASS RAID SYSTEM | Advanced Serial Attached SCSI (SAS) 24x7 technology coupled with high-end RAID storage system provides the ultimate in data performance and protection |
| NETWORK TIME PROTOCOL SUPPORT | Synchronize with NTP servers to perform better, more accurate analysis |
| VIRTUAL DATA LOCK | Protect and lock packet data that is related to problems such as those based on SNMP traps |
| MOBILE PROTOCOL SUPPORT | Support for 3G-324M, the umbrella protocol for video telephony in 3G mobile networks |
| 4 GbE PORTS, 2 10 GbE PORTS | Simultaneously monitor, trigger and record up to 4 GbE or 2 10 GbE independent links |
| PLUG AND PLAY APPLIANCE | Full turnkey solution. Be up and running within a hour. No complicated setup or installation procedures |
| WIRESHARK INTEROPERABILITY | Benefits from all the post-capture capabilities of Wireshark including protocol decodes and display filters |
| DMA PACKET COPY TO APPLICATION SPACE | Offload captured network data at over 1 GB/s (Gigabyte) with little or no CPU intervention |
| SAS (SERIAL ATTACHED SCSI) DRIVES | High performance 24x7 enterprise class SAS drive technologies |
| RAID 5 PROTECTION | Redundant Array of Inexpensive Drives (RAID) to provide highest levels of performance and reliability. The highest performing NTM, the Premium2, employs a RAID system of 15 SAS drives |
| COMPREHENSIVE REPORTING | Track and report application performance trends, quality measurements, network statistics over extended periods of time |
| EXPERT ANALYSIS ENGINE SUPPORT | Optional software automatically provide real-work assessment of captured network data through an extensive knowledge base of over 500 problems and issues |
| DISTRIBUTED SYSTEM | Manage and access NTMs anywhere in the world through an IP network |
| 1 YEAR HARDWARE WARRANTY | Protect your investment with industry-leading first year free hardware warranty program. Additional years of protection are offered at a faction of the equipment cost |
| 1 YEAR FREE SOFTWARE UPDATES | Benefit from all the fixes and enhancements that ClearSight provides to its customers on a regular basis |

[1] *Special order item; please check with ClearSight*

| Product Name | Network Time Machine Express | Network Time Machine Portable2 | Network Time Machine Standard2 | Network Time Machine Premium2 |
|---|---|---|---|---|
| Model Number | 10/100/1000 MbE version: CSR-EXPRESS-A<br>10/100 MbE version: CSR-EXPRESS-1-A | 10/100/1000 Mb/s version: CSR-4530-H<br>10 Gb/s version: CSR-4530-H-10G | CSR-4430-2 | 10/100/1000 Mb/s version: CSR-4431-2<br>10 Gb/s version: CSR-4431-2-10G |
| Capture Filter | No | Yes | Yes | Yes |
| Save Filter | No | Yes | Yes | Yes |
| Display Filter | Yes | Yes | Yes | Yes |
| Payload Slicing | No | Yes | Yes | Yes |
| Realtime Alert | Yes | Yes | Yes | Yes |
| Realtime Statistics (RMON1) | Yes | Yes | Yes | Yes |
| Realtime Flow Analysis | Yes | Yes | Yes | Yes |
| Post Analysis | Yes | Yes | Yes | Yes |
| Realtime Report | Yes | Yes | Yes | Yes |
| History Report | Yes | Yes | Yes | Yes |
| Trace File Report | Yes | Yes | Yes | Yes |
| Atlas Option Support | Standard | Yes | Yes | Yes |
| Multi-user, Remote Access | No Multi-User; Yes Remote Access | No | Yes | Yes |
| Storage Capacity | 500 GBs | 1.6 TBs | 1.6 TBs | 4.2 TBs / 13 TBs[1] / 44 TBs[1] |
| Additional Storage Array Support | No | No | No | Yes |
| Redundant Power Supply | No | No | Yes | Yes |
| RAID Level | Does Not Support RAID | RAID 0 | RAID 0 | RAID 5 |

[1] *Special order item; please check with ClearSight Networks*

### Network Time Machine Standard2

### Network Time Machine Portable2

### Network Time Machine Express

### Network Time Machine Premium2

| Product Name | Network Time Machine Express | Network Time Machine Portable2 | Network Time Machine Standard2 | Network Time Machine Premium2 |
|---|---|---|---|---|
| Model Number | 10/100/1000 MbE version: CSR-EXPRESS-A<br>10/100 MbE version: CSR-EXPRESS-1-A | 10/100/1000 Mb/s version: CSR-4530-H<br>10 Gb/s version: CSR-4530-H-10G | CSR-4430-2 | 10/100/1000 Mb/s version: CSR-4431-2<br>10 Gb/s version: CSR-4431-2-10G |
| Form Factor | 1U rack<br><br>Short Depth 1U<br>14" (D) x 16.75" (W) x 1.7" (H)<br>356mm (D) x 426mm (W) x 43mm (H)<br><br>14.5 lbs (6.6 kgs) | All-in-one Portable with Integrated 17" WUXGA+ LCD - 1920 x 1200<br><br>5.69in (D) x 16.8in (W) x 11.44in (H)<br>14.5cm (D) x 42.7cm (W) x 29cm (H)<br><br>13.5 - 19.5 lbs (depending on configuration)<br>(6.1 - 8.9 kgs) | 2U rack<br><br>29.3in(D) x17.5in(W) x3.4in(H)<br>74.4cm(D) x44.4cm(W) x8.6cm(H)<br><br>2U: 51 lbs (23 kgs) | 2U rack with 3U storage unit<br><br>2U: 29.3in(D) x17.5in(W) x3.4in(H)<br>74.4cm(D) x44.4cm(W) x8.6cm(H)<br><br>3U: 18.9in(D) x17.5in(W) x5.2in(H)<br>48cm(D) x44.4cm(W) x13.2cm(H)<br><br>2U: 51 lbs (23 kgs)<br>3U: 78 lbs (35.5 kgs) |
| CPU | Single Quad Core Intel x3320, 2.50Ghz, 1333Mhz, 6MB L3 Cache | Two Quad Core Xeon 5335 Processor2x6 MB Cache, 2.0 GHz, 1066 MHz FSB | Two Quad Core Xeon X5450 Processor2x6 MB Cache, 3.0 GHz, 1333MHz FSB | Two Quad Core Xeon X5450 Processor2x6 MB Cache, 3.0 GHz, 1333 MHz FSB |
| OS | Microsoft Windows XP | Microsoft Windows 2003 Server | Microsoft Windows 2003 Server | Microsoft Windows 2003 Server |
| Memory | 4 GB DDR3 1333Mhz Unbuffered DIMMs | 4 GBs Direct Connect DMA Striping Channels Memory | 4 GBs 667 MHz Dual Ranked Fully Buffered DIMMs Memory | 4 GBs 667 MHz Dual Ranked Fully Buffered DIMMs Memory |
| Drives | Storage Capacity: 500 GBs | Storage Capacity: 1.6 TBs<br>OS: 1x200 GB SATA<br>Packet Store: 8x200 GB SATA | Storage Capacity: 1.5 TBs<br>OS & Packet Store: 6x400 GB 10K 3G SAS | Storage Capacity: 4.2 TBs<br>OS: 6x400 GB 10K 3G SAS<br>Packet Store: 15x300 GB 15K 3G SAS |
| Monitor/Capture Ports | 2 Ports (Copper & Optical)<br><br>**Model CSR-EXPRESS-A:** 10/100/1000 MbE version<br><br>**Model CSR-EXPRESS-1-A:** 10/100 MbE version | **Model CSR-4530-H:** 4 GbE Ports (Copper & Optical)<br><br>**Model CSR-4530-H-10G:** 2 10 GbE Ports (XFP -- supports CX4 copper & Optical) | 4 GbE Ports (Copper & Optical) | **Model CSR-4431-2:** 4 GbE Ports (Copper & Optical)<br><br>**Model CSR-4431-2-10G:** 2 10 GbE Ports (XFP -- supports CX4 copper & Optical) |
| Power Supply | Auto-switching 260 Watt 100-240V, 60-50Hz, 4 Amp Max | 400/520 W auto-switching 110/220V AC | Redundant 750 W hot-plug auto-switching 110/220V AC | 2U: Redundant 750W hot-plug auto-switching 110/220V AC<br><br>3U: Redundant 550W hot-plug auto-switching 100/240V AC |

The minimum system requirements for the NTM Distributed Agent Manager and Remote Viewer are shown below.

| Item | Minimum Requirement |
|---|---|
| Computer | Industry standard computer system (laptop or desktop), with a CD drive for software installation |
| Processor | Pentium 4 (or equivalent) running at 1 GHz minimum<br>(2 GHz recommended) |
| RAM | 512 MB minimum (1 GB recommended)<br>2 GB minimum if running Vista |
| Hard Disk Space | 250 MB. In addition, you should have space to store saved trace files. Individual trace files can be as large as 1 GB, but it is not recommended to open a trace file larger than 256 MB<br>2 GB minimum if running Vista |
| Operating System | Microsoft Vista (32 bit)<br>Microsoft Windows 2000 Professional with SP3+<br>Microsoft Windows XP Home Edition and XP Professional with SP1+<br>*(Disable the firewall if you are using SP2 or SP3)* |
| Monitor | VGA color monitor with 1024 x 768 resolution and 256 colors |
| Network Adapter | Standard Ethernet network interface card |


46401 Landing Parkway
Fremont, CA 94538-6496

For more information, call or email us:
Telephone (US Toll Free): 1-800-825-7563
Telephone (International): +1-510-824-6000
Fax: 1-510-824-6100
Email: sales@clearsightnet.com
www.clearsightnet.com