10G thru PDH Interceptors

A portfolio of Automated Network Monitoring Access solutions
for today's transport networks

NetQuest

INTRODUCTION

Gathering intelligence through real-time network monitoring is a key priority for law enforcement agencies, national security concerns, and other intelligence gathering institutions the world over.

The technology and solutions for accurate, real-time traffic capture, processing, and analysis are becoming increasingly complex as additional network protocols and tunnels are added to support network convergence. For network monitoring applications to continue to be effective, the monitoring access infrastructure must also evolve to meet a dynamic converged global network. This access infrastructure has traditionally been composed of a collection of standard network elements such as routers, switches, and muxes that are forced into performing specialized monitoring tasks for which they were not designed. NetQuest's Interceptor portfolio offers a new solution.

BENEFITS

- Automate the discovery/survey of private line circuit utilization
- Provide lossless interception of multi-protocol data
- Reduce capex, footprint, and power requirements for monitoring and surveillance
- Accelerate intercept and SIGINT applications by pre-processing and filtering
- Provide unified IP access for probes, independent of transport protocols
- Enable selective, real-time access to data of interest
- Reduce opex associated with network re-provisioning

INTERCEPTOR APPROACH

NetQuest Interceptors are purpose-built, comprehensive access solutions enabling intelligent intercept and monitoring applications. Without any prior knowledge of the network provisioning, the Interceptors are capable of discovering and reporting the contents of a variety of packet or TDM service networks ranging from high speed OTN OTU-2, LAN-PHY, OC192/STM-64 to low speed T1/E1 and DS0. Subsequently, the NetQuest Interceptors enable selective targeting of precise data traffic by removing framing/transport protocols and routing this traffic to specialized Ethernet-based tools for deeper level analysis.

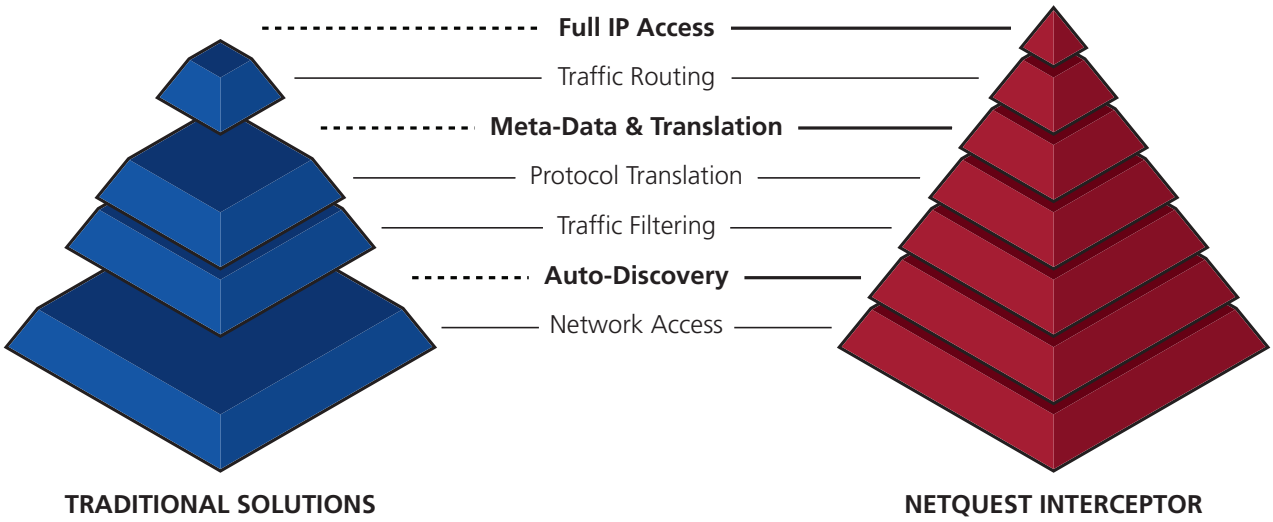

FIGURE 1 – While traditional methods of monitoring access perform some of the functions required for full IP data access, only Interceptors offer access to any IP or non-IP data at any speed on any transport technology without prior knowledge of the network provisioning.

TRADITIONAL ACCESS VERSUS INTERCEPTOR ACCESS

BEFORE INTERCEPTOR

Figure 2 depicts a traditional monitoring access configuration where a collection of network elements and diagnostic equipment from multiple vendors is assembled to access a range of services. Managing these disparate tools quickly becomes a tedious task. Moreover, configuring and maintaining this infrastructure is a time-consuming, manual process due to the sheer number of possible physical and logical connections on today's high speed packet optical transport networks. Any one line may carry one or more high speed and many low speed tributaries. Each of these traffic streams may be framed and transported by a number of possible framing formats and protocols. The information about the specific stream provisioning is difficult to obtain and is often outdated or wrong due to the frequent changes in network provisioning and end-user configurations.

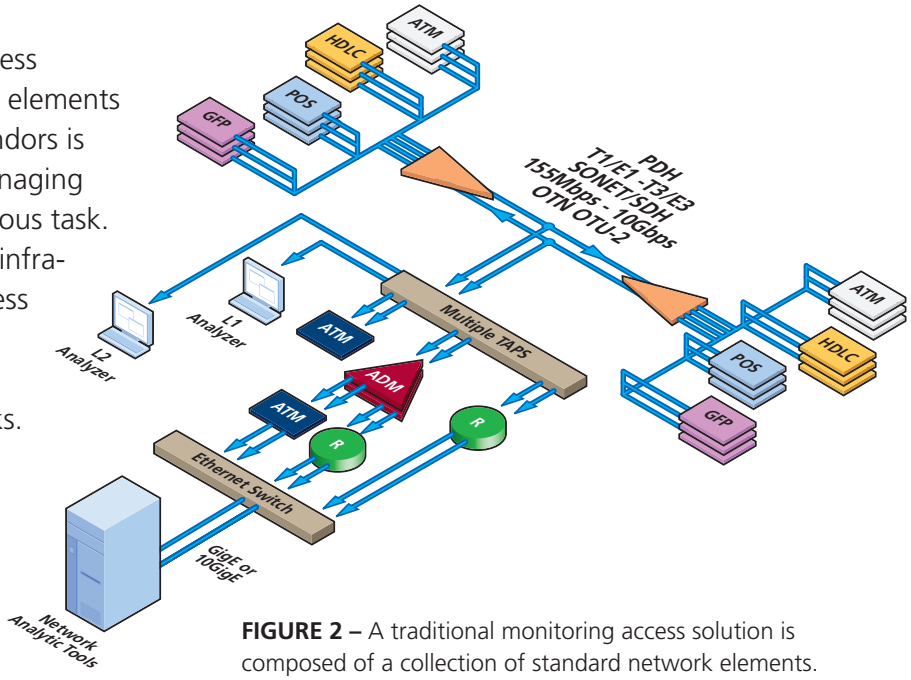

FIGURE 2 – A traditional monitoring access solution is composed of a collection of standard network elements. This solution can be costly and difficult to manage.

AFTER INTERCEPTOR

The NetQuest Interceptor product line is specifically designed for selective monitoring access. An Interceptor consolidates conventional access functions with advanced network Auto-Discovery capabilities and precise traffic targeting in a highly integrated platform, shown in Figure 3. Its ability to discover and automatically adjust to the detection of standard network signals and transport protocols makes it function independent of network re-provisioning. This, in turn, greatly simplifies the management of the overall network monitoring system. Further, the Interceptors can translate WAN input traffic to standard Ethernet output as well as off-load the processing requirements on the downstream network monitoring analytic tools by filtering and pre-processing traffic. These Interceptor functions enable the overall network monitoring solution to be more efficient by processing only the data of interest. The Interceptor solution is highly scalable to the specific network access monitoring requirements.

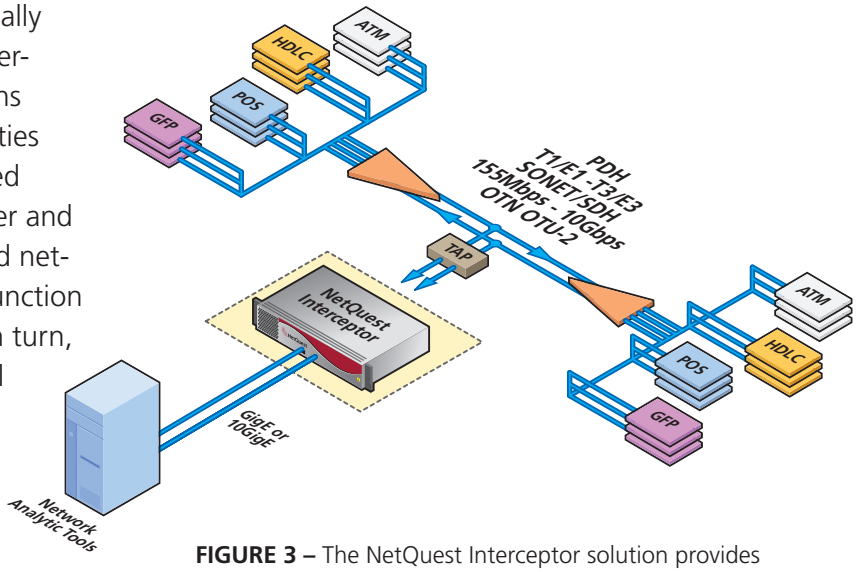

FIGURE 3 – The NetQuest Interceptor solution provides a purpose-built comprehensive monitoring access solution regardless of network technology or speed. An Interceptor costs significantly less than the sum of the various conventional network elements it replaces.

AUTO-DISCOVERY PROCESS

The heart of NetQuest's Interceptor product line is its ground-breaking network Auto-Discovery process. In applications where private line or virtual private line services are being delivered, bandwidth allocation and protocol usage can vary greatly because they are determined by the end-user's specific termination equipment. This issue is further complicated by the dynamic nature of network provisioning, which can change on a daily or even hourly basis. Auto-Discovery eliminates the need for external test equipment to analyze circuit utilization, the ongoing manpower needed to operate this test equipment, and the subsequent task of re-provisioning traditional multi-element access solutions.

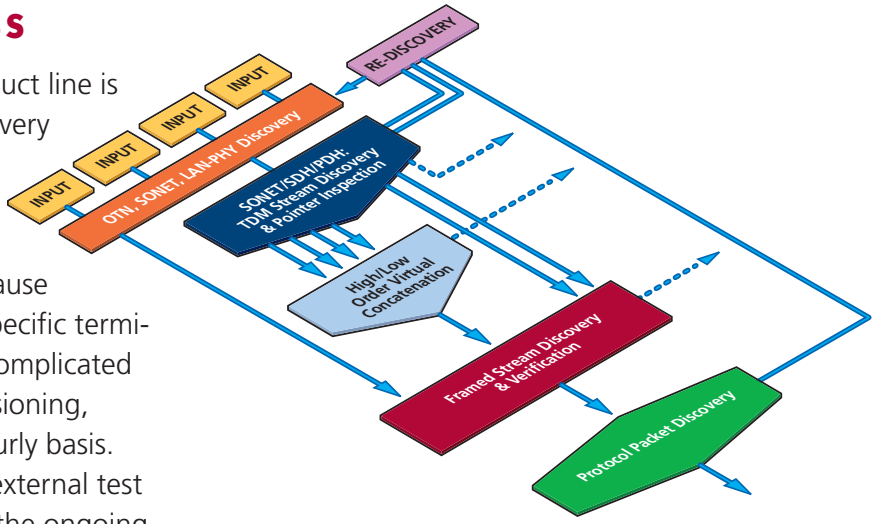

FIGURE 4 – Data flow through the Interceptor's Auto Discovery process; each step helps identify the transport hierarchy and communication protocols within the network monitored ports.

An Interceptor detects, qualifies, and reports the physical and transmission protocol parameters of all identifiable traffic streams carried over OTN and SONET/SDH/PDH. It achieves this by automatically analyzing the digital signal hierarchy of each signal to determine the speed, framing format and channelization structure. It also discovers which tributary containers are in use and can determine the types of framed streams being utilized within the containers, for example, POS, GFP, ATM, or HDLC. By further analyzing the framed streams, the Interceptor also determines the type of protocols such as PPP, Frame Relay, MPLS, cHDLC, PPPoE, etc. The Interceptor publishes the results so the user can make intelligent decisions regarding which traffic will be forwarded downstream for deeper level analysis. The entire process runs continually in the background to ensure any changes in usage or service interruptions are detected and critical surveillance is maintained.

The Interceptor Auto-Discovery process provides:

- Fast and reliable network identification
- Intuitive signal contents reporting
- Automated re-provisioning for detecting network changes
- Eliminates use of equipment not intended for monitoring applications

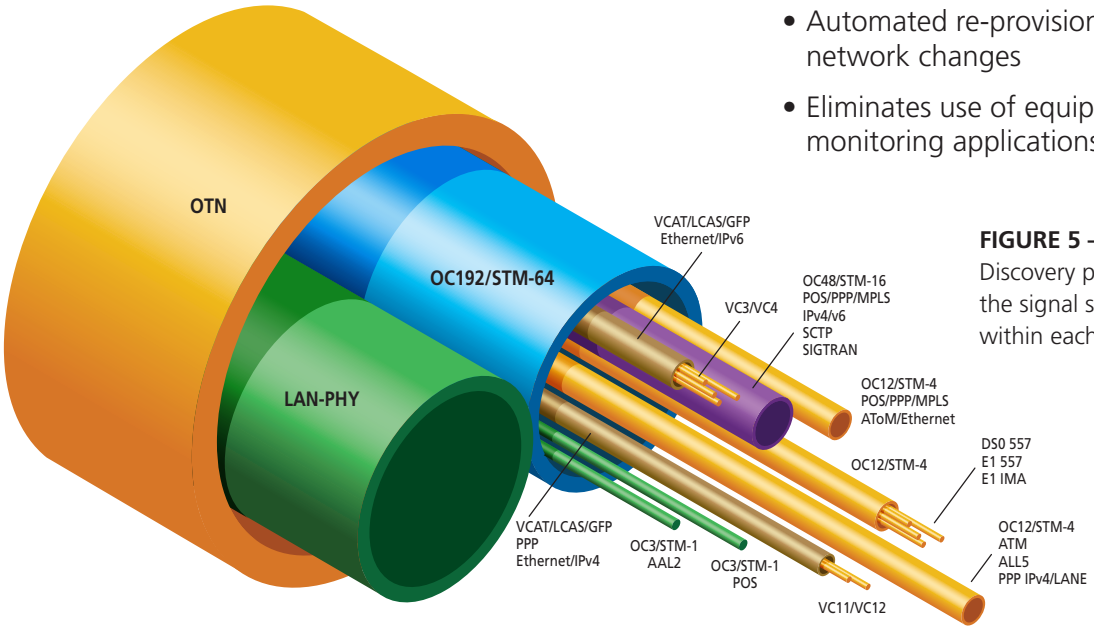

FIGURE 5 – The Interceptor's network Auto-Discovery process determines and displays the signal structure and transport protocols within each container.

TRAFFIC TARGETING

The results of the NetQuest Interceptor's Auto-Discovery process are published in a tabular format, an example of which is shown in Table 1. Using these results, the user can target specific data of interest for deeper level processing.. The Interceptors perform WAN to LAN translation by removing framing and transport protocols from the targeted traffic and providing access to the raw data. The Interceptor delivers the targeted traffic over Ethernet to real-time network monitoring analytic tools. By off-loading non-essential traffic or traffic not available for surveillance, NetQuest Interceptors optimize the downstream analytic application's processing resources for higher level tasks.

Stream Index	Stream Type	Data Framing	Transport Protocol	Output/Forwarding (SFP Site #)
2-0-0-0-1-…	OC12c	POS	MPLS	GigE Output (#2)
3-0-…-0-2-..	DS3	HDLC	PPP	GigE Output (#4)
4-0-0-…-1-..	OC3	ATM	AAL2	Bypass (#3)
3-0-0-…-4-4	E1	N/A	N/A	Bypass (#1)
4-0-0-…-1-..	OC3c	GFP	MAC	GigE Output (#3)
3-0-0-…-4-4	DS0	HDLC	SS7	GigE Output (#1)
1-0-0-…-4-..	STS-3	ATM	AAL5	GigE Output (#2)

Traffic targeting can be utilized in a single or multi-stage approach depending on the application's requirements. Both approaches are depicted in the figure below:

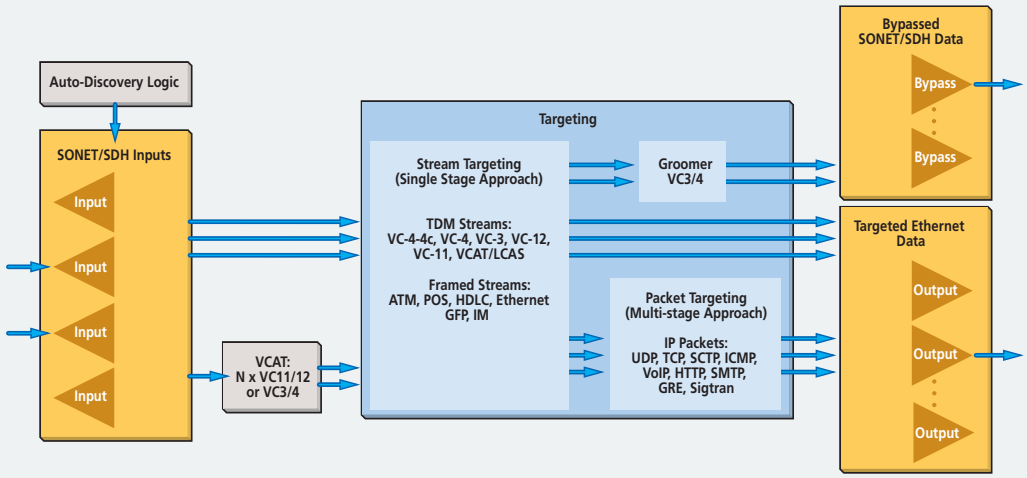

FIGURE 6 – Traffic targeting selects and filters precise traffic of interest for further processing by downstream network monitoring analytic equipment.

SINGLE STAGE APPROACH

Precise targeting of select traffic at the TDM and framed stream level (for example VC-4 POS). The selected traffic is extracted, all TDM overhead is removed, raw data is translated into Ethernet frames, and traffic is forwarded to the Interceptor's output port(s).

MULTI-STAGE APPROACH

Includes all benefits of single stage approach but also provides advanced filtering capabilities where specific protocols and packet information can be used to filter out and/or redirect targeted traffic to specific outputs for analysis by network analytic tools..

Traffic that could not be identified beyond the SONET/SDH level can be efficiently groomed and redirected to clear channel or channelized bypass ports. This enables further investigation by external systems, ensuring no potentially threatening data is lost.

INTERCEPTOR'S MODULAR APPROACH

The NetQuest Interceptor product platform scales to meet the most challenging requirements in network surveillance by providing a solution architected to grow with your application. Utilizing a modular approach, Interceptors are able to provide monitoring access to a wide array of optical network architectures including DWDM, 100G OTN, channelized SONET/SDH, and legacy PDH circuits. Each of the NetQuest Interceptors support the ability to identify and bypass specific network traffic that cannot be processed by that particular Interceptor model and deliver the traffic over its WAN bypass ports to a suitable NetQuest Interceptor device.

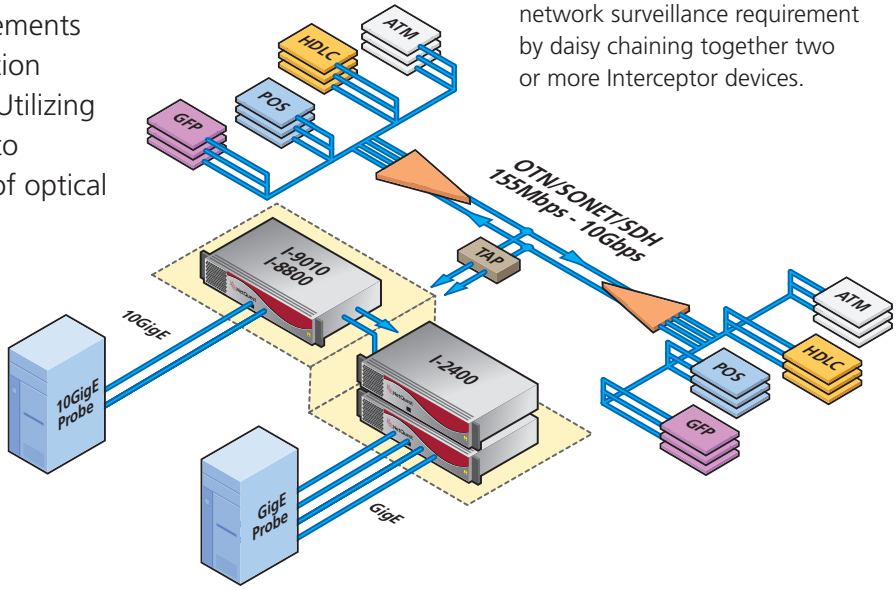

FIGURE 7 – The Interceptor solution can scale to meet any network surveillance requirement by daisy chaining together two or more Interceptor devices.

COST SAVINGS REALIZED

An Interceptor costs significantly less than the sum of the various conventional access products it replaces (see Figure 2). Besides its lower acquisition cost and unique automated network discovery process, the Interceptor delivers the following long term cost of ownership benefits:

- Reduced management costs
- Simpler to install and less cabling
- Less rack space and power required
- Lower long term maintenance costs

NETQUEST INTERCEPTOR PORTFOLIO

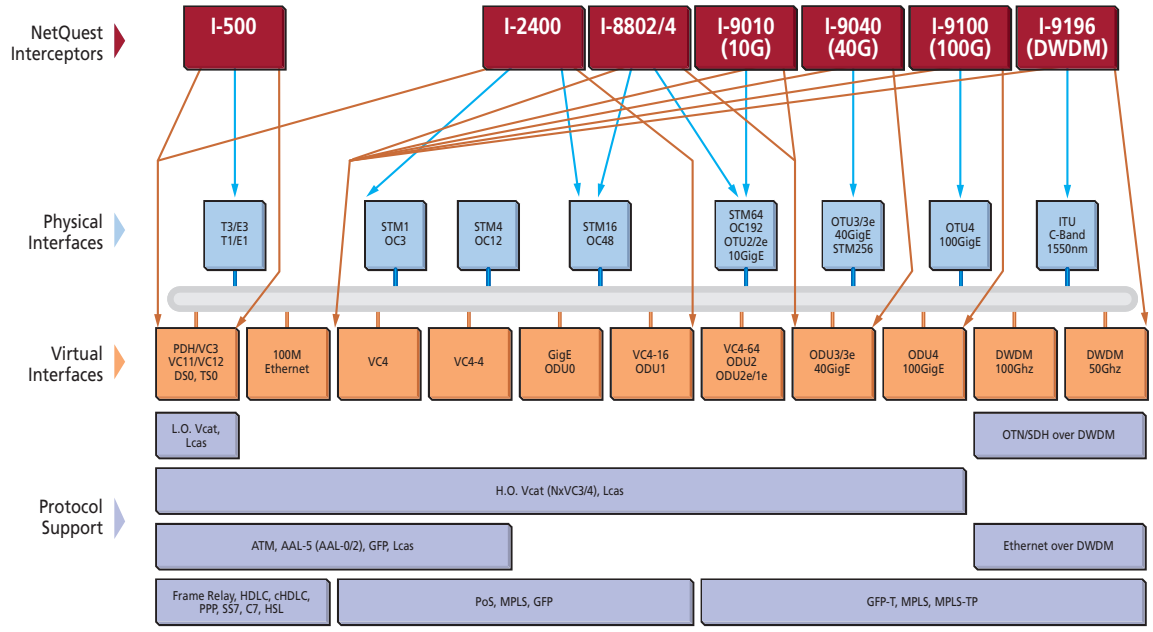

FIGURE 8 – The Interceptor Portfolio supports a wide range of physical interfaces, their virtual channelization and the protocols carried within their payloads.

MANAGEMENT AND CONTROL

NetQuest supports device management of the Interceptors via the Alpine Patrol EMS as well as standard menu driven screens accessed via Telnet/SSH. Alpine Patrol is an optimized EMS platform supporting the full FCAPS device management model. Both device management methods provide secure access through a multi-level password protection system that leverages Radius or TACACS+. The Interceptors also have integral Syslog support along with an SNMP V1-V3 agent that supports trap functionality, making it possible to audit and manage configuration changes and alarm notifications in a networked environment.

For applications where a tight integration between the Interceptor and the intercept application system or LI management system is required, NetQuest has developed a machine-to-machine interface called GSCP, a proprietary UDP-based control protocol. Integrating GSCP with the intercept application system enables solution providers to present a unified solution at every level.

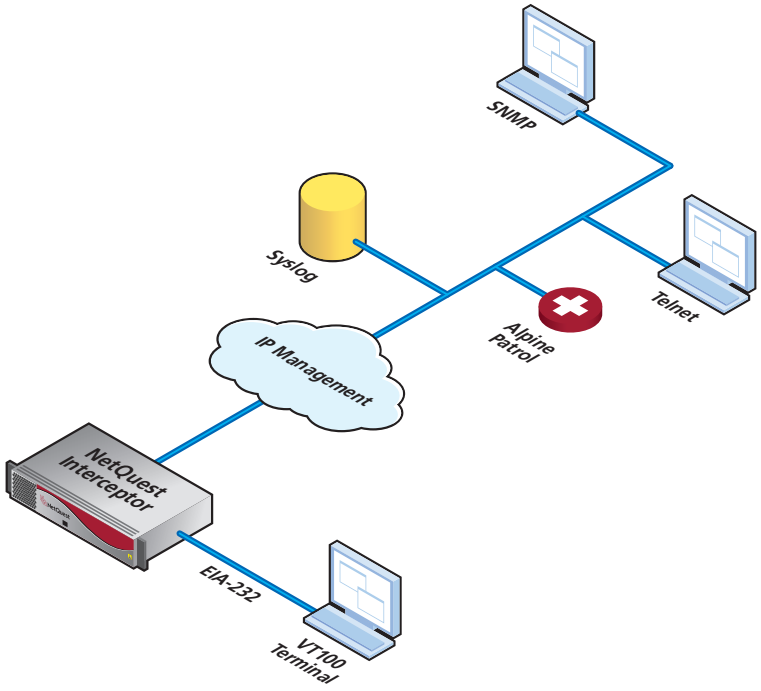

FIGURE 9 – The Interceptor can be managed locally through the EIA-232 port or remotely via NetQuest Alpine Patrol EMS or Telnet/SSH. It also supports SNMP and Syslog.

TECHNICAL SPECIFICATIONS

Model	I-500	I-2400	I-8800	I-9014/18
Input Ports	28 x T-1/E-1 12 x T-3/E-3	4 x OC3/STM-1 or OC12/STM-4 or 1 x OC48/STM-16	2 x OTU-2/2e/1e or 2 x OC192/STM-64 or 4 x OC-48/STM-16 or 2 x 10GigE (OTN option required)	4/8 x OTU-2/2e/1e or 4/8 x OC192/STM-64 or 4/8 x 10GigE
Auto-Discovery and Targeting Bandwidth	0.6Gbps	2.5Gbps	20Gbps	40/80Gbps
Bypass Ports	Up to 4 T1/E1 and 2 T3/E3	Up to 8 OC3/STM-1 or OC12/STM-4	Up to 2 OC48/STM-16	Up to 2/4 OC48/STM-16
Bypass Grooming Level	Includes any to any E1/T1 to E1/T1; E3/T3 to E3/T3	Includes any to any VC11; VC12; VC2; VC3; VC4; VC4-4c. (VT-1.5; VT-2; VT-6; STS-1; STS-3c; STS-12c)	Includes any-to-any VC-4-4c or VC-4 level	Includes any-to-any VC-4-4c or VC-4 level
Ethernet Output Ports	2 x GigE	4 x GigE	4 x 10GigE	4/8 x 10GigE
TDM Stream Auto-Discovery	PDH from T3/E3, T1/E1, FT-1/FE-1 and DS0	From OC48/STM-16 to VC4/VC3, PDH from VC4/VC3 to VC12/VC11 and DS0, VCAT/LCAS	From OC192/STM-64 (VC4-64) down to VC4 including VCAT/LCAS at Nx VC3 or Nx VC4	From OC192/STM-64 (VC4-64) down to VC4 including VCAT/LCAS at Nx VC3 or Nx VC4
Framed Stream Auto-Discovery	ATM, HDLC, IMA	POS, EoS, ATM, HDLC, GFP, IMA, Ethernet	POS, EoS, GFP, WAN PHY, Ethernet	POS, EoS, GFP, WAN PHY, Ethernet
Protocol Stream Auto-Discovery	PPP, cHDLC, MPLS, Frame Relay, SS7, MLPPP	PPP, cHDLC, MPLS, Frame Relay, SS7, MLPPP	PPP, cHDLC, MPLS, MLPPP	PPP, cHDLC, MPLS, MLPPP
Size	2U rack mount or table top chassis: 3.5"H x 19"W x 17.25"D (8.9cm H x 48.3cm W x 43.8cm D)			
Weight	18 pounds (8.16 kg)			
Typical Power	100 W	140 W	140 W	160 W
Operating Temp	32° – 122° F (0° – 50° C) A hot swap capable fan tray that has integral speed controlled.			
Humidity	10 – 90% non-condensing			
Compliance	FCC, UL, CE, RoHS			

ABOUT NETQUEST

NetQuest Corporation designs, manufactures and markets innovative monitoring access products for applications in tele-communications service provider, government, and enterprise networks. Founded in 1987 and based in Mount Laurel, New Jersey, NetQuest is an employee owned company. With more than a 20 year track record of providing cutting edge monitoring access solutions, NetQuest has developed a global customer base, marketing directly and through a network of value added resellers and representatives.

WWW.NETQUESTCORP.COM

NetQuest Corporation • 523 Fellowship Road • Mount Laurel, NJ 08054 USA • +1.856.866.0505 • Fax: +1.856.866.2852