BROCHURE

I-9100 100/40/10G Interceptor

Network Monitoring Access solutions for
today's intelligent packet optical transport networks

NetQuest

INTRODUCTION

Gathering intelligence through real-time network monitoring is a key priority for law enforcement, intelligence agencies, and other national security institutions around the world. The NetQuest I-9100 100/40/10G Interceptor provides a state-of-the-art network monitoring access platform including comprehensive traffic identification and data intercept capabilities for monitoring today's global packet optical transport networks.

The I-9100 100/40/10G Interceptor provides unique network survey functionality of the specific traffic flows inside a high-speed optical network regardless of the existing transport protocols carried over OTN, SONET/ SDH and native Ethernet. The Interceptor enables selective targeting of precise data traffic within the network and performs full traffic media conversion in order to route streams to standard Ethernet-based tools for deeper level analytics.

The I-9100 100/40/10G Interceptor is able to continuously intercept and process multi-protocol data at wire-speed while assuring no distortion from packet loss. As submarine and terrestrial networks converge and intelligent optical networks rapidly expand and evolve, the technology and solutions for accurate, real-time traffic capture, processing, and analysis are becoming increasingly expensive and complex to manage. The I-9100 100/40/10G Interceptor dramatically reduces CAPEX, OPEX and complexity of optical network monitoring while improving the accuracy and effectiveness of the overall intelligence gathering infrastructure.

I-9100 INTERCEPTOR BENEFITS

- Single access platform for monitoring 100G, 40G and 10G packet optical networks
- WAN to LAN media conversion for OTN, SONET/SDH and native Ethernet
- Real-time optical network survey and content auto-discovery
- Lossless interception of multi-protocol data
- Aggregation and filtering optimize efficiency of analytic tools
- Dramatically reduce CAPEX and OPEX while reducing complexity

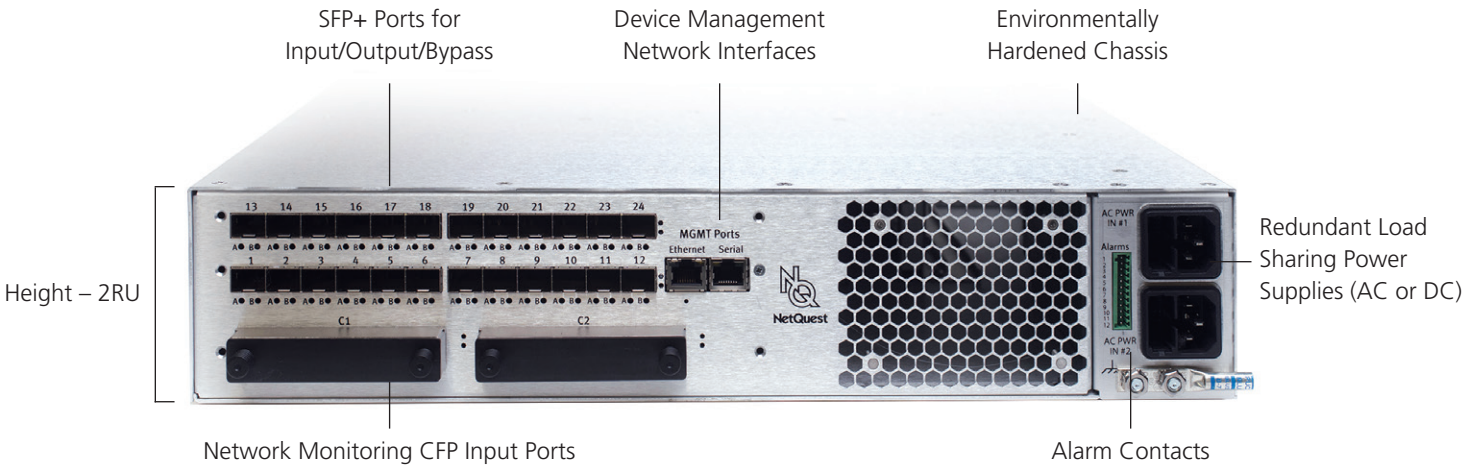


FIGURE 1 – NetQuest I-9100 100/40/10G Interceptor standard rear panel view showing key network interfaces. Interceptors are purpose-built network monitoring access solutions built on an environmentally hardened hardware platform.

MONITORING PACKET OPTICAL TRANSPORT NETWORKS

Network Service Providers (NSPs) are continuously being challenged to provide additional bandwidth to meet the demand driven exponential consumer traffic growth and evolving content. They are also being driven to reduce the cost per bit of transport and subsequently looking to derive new revenues from content based services.

To address this bandwidth growth, NSPs are deploying new core and metro packet optical transport network architectures. The need for delivering faster, better and cheaper on-demand services are pushing Data Centers closer to the network edge in order to localize user content. Network architectures are transitioning from traditional ring based topologies to intelligent mesh based networks in order to avoid bottlenecks and improve resiliency. These new Packet Optical Transport Systems are combining DWDM, OTN, and packet switching technologies to create a more robust and resilient global network.

This networking evolution is creating similar challenges for those responsible for monitoring and intercepting network traffic. The exponential growth in users and connected devices makes monitoring these endpoints prohibitively expensive. Intelligent mesh based networks force intercept capabilities to be present in the metro networks; monitoring access in the core alone is not sufficient. Deep packet inspection required by specialized analytic devices is creating massive processing challenges. The NetQuest Interceptor can be used to offload these processing challenges by targeting unique traffic flows of interest in strategically placed locations.

INTERCEPTOR APPROACH

NetQuest Interceptors are purpose-built, comprehensive intercept 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 an intelligent multi-layered optical network including packet or TDM services ranging from high speed OTN OTU-4 and 100GbE to LAN-PHY, OC-192/STM-64 and 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.

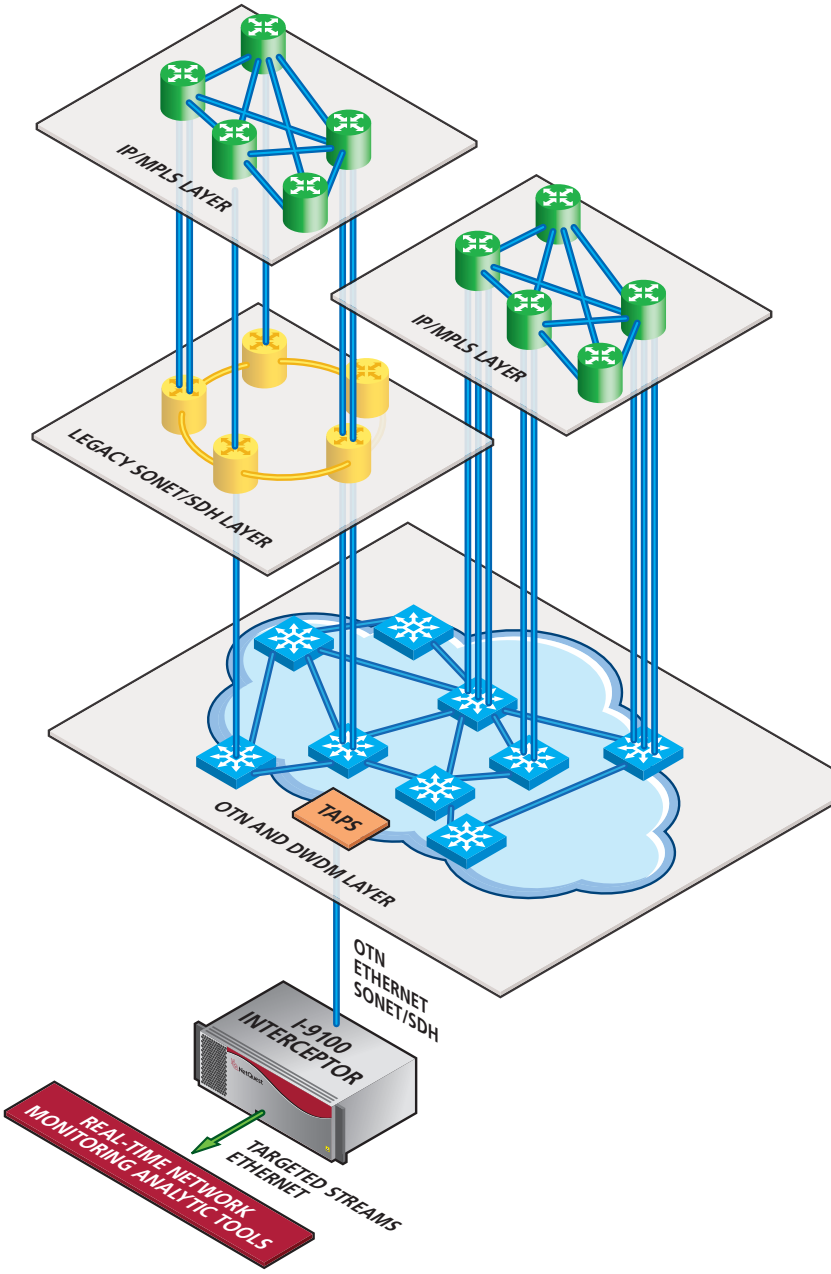


FIGURE 2 – NetQuest I-9100 100/40/10G Interceptors provide monitoring access across intelligent multi-layered optical networks.

AUTO-DISCOVERY PROCESS

The heart of NetQuest's Interceptor series is its ground-breaking Auto-Discovery process. In applications where private line, virtual private line, or Ethernet based 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 and the emergence of Software Defined Networks (SDN), which can change on a daily or even hourly basis.

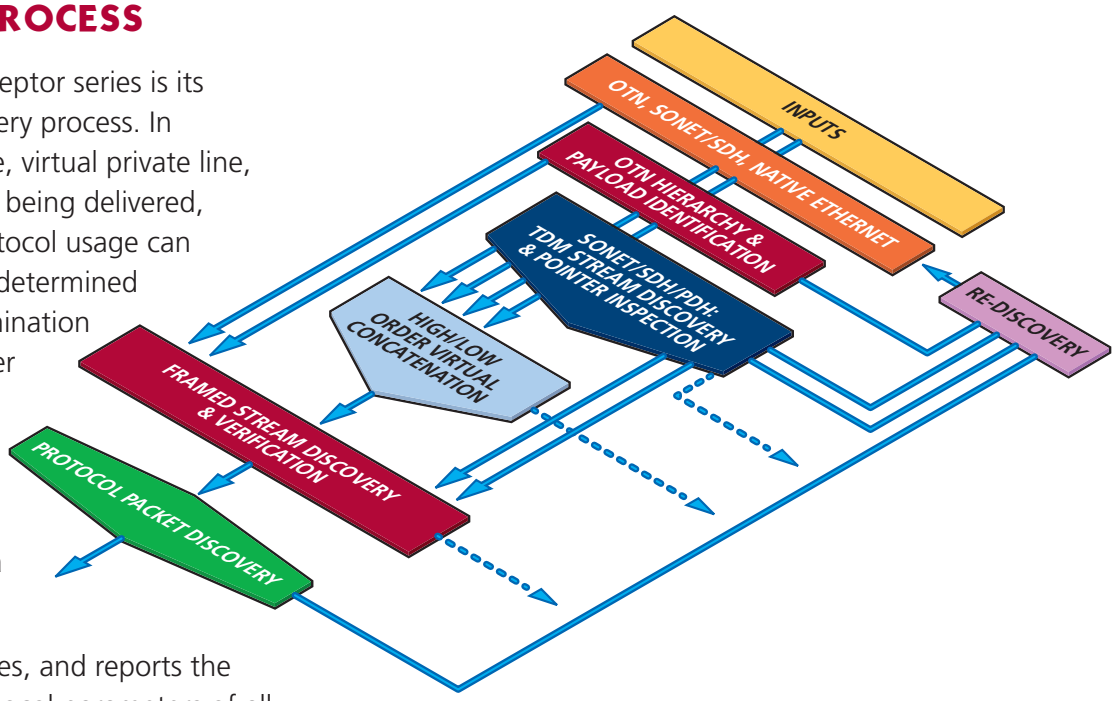


FIGURE 3 – Data flow through the Interceptor's Auto-Discovery process; each step helps identify the transport hierarchy and communication protocols within the network monitored ports.

An Interceptor detects, qualifies, and reports the physical and transmission protocol parameters of all identifiable traffic streams on OTN, Ethernet, and SONET/SDH lines. It achieves this by automatically analyzing the digital signal hierarchy of each stream to determine the signal 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, or HDLC. By further analyzing the framed messages, it also determines the type of Protocols such as PPP, MPLS, PPPoE, IPV4/IPV6, MAC, etc. The Interceptor then publishes the results to be utilized by the intercept application or network operator. The entire process runs continually in the background to ensure any changes in usage or service interruptions are detected and critical surveillance is maintained.

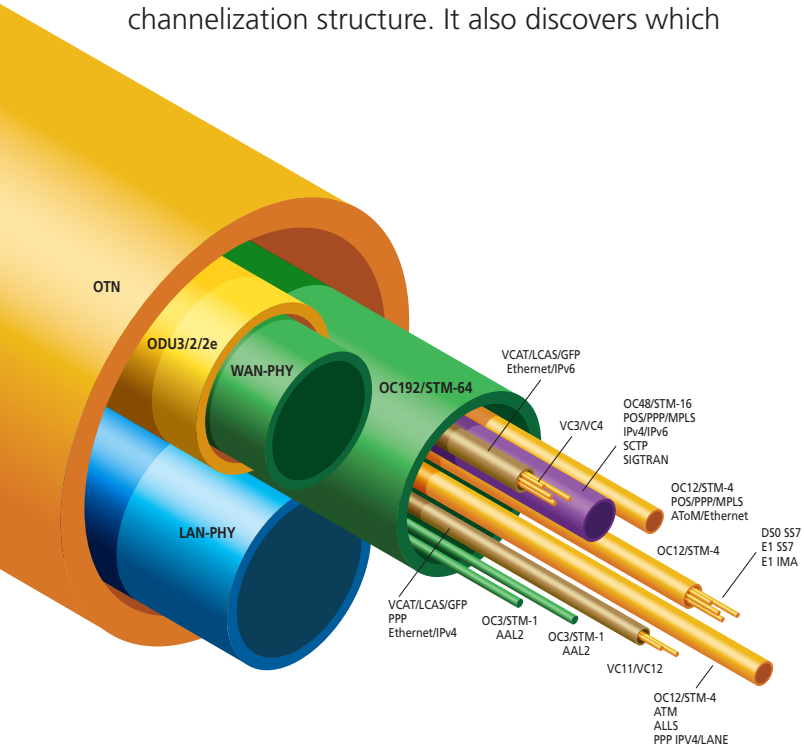


FIGURE 4 – NetQuest Interceptor Auto-Discovery process determines and displays framing structure and transport protocols within each container.

The NetQuest Auto-Discovery 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 application

TRAFFIC TARGETING

The results of the Auto Discovery process are published in a tabular format, an example of which is shown in Figure 5. Using these results, the user can target specific data of interest for further processing by the intercept application(s). The I-9100 100/40/10G Interceptor performs WAN to LAN translation by removing framing and transport protocols from the targeted traffic and providing access to the raw packet data. The Interceptor provides a significant level of packet processing functions including configurable forwarding/filtering rules, comprehensive load balancing algorithms, metadata insertion and VLAN/MPLS handling. The Interceptor delivers the targeted packets over 10GbE to real-time network monitoring analytic tools. By offloading non-essential traffic or traffic not required for surveillance, NetQuest Interceptors optimize the downstream analytic application's processing resources for higher level tasks. Traffic that cannot 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. The Interceptors also support a Raw Byte Stream feature which enables output of any traffic over Ethernet regardless of whether the Interceptor can identify the traffic content.

Stream Index	Stream Type	Data Framing	Transport Protocol	Output/Forwarding (SFP Site #)
2-0-0-0-1-..	OTU4	POS	MPLS	GigE Output (#2)
3-0-...-0-2-..	40GigE	N/A	MAC	GigE Output (#4)
4-0-0-...-1-..	OTU2e	N/A	IPV4	GigE Output (#8)
3-0-0-...-4-4	OTU4	ATM	AAL2	Bypass (#1)
4-0-0-...-1-..	OC-192	GFP	MAC	GigE Output (#3)
3-0-0-...-4-4-..	OTU4	POS	cHDLC	GigE Output (#2)
1-0-0-...-4-..	ODU2	POS	PPP	GigE Output (#5)

FIGURE 5 – Interceptors display Auto-Discovery results to enable network analysis and selective traffic targeting.

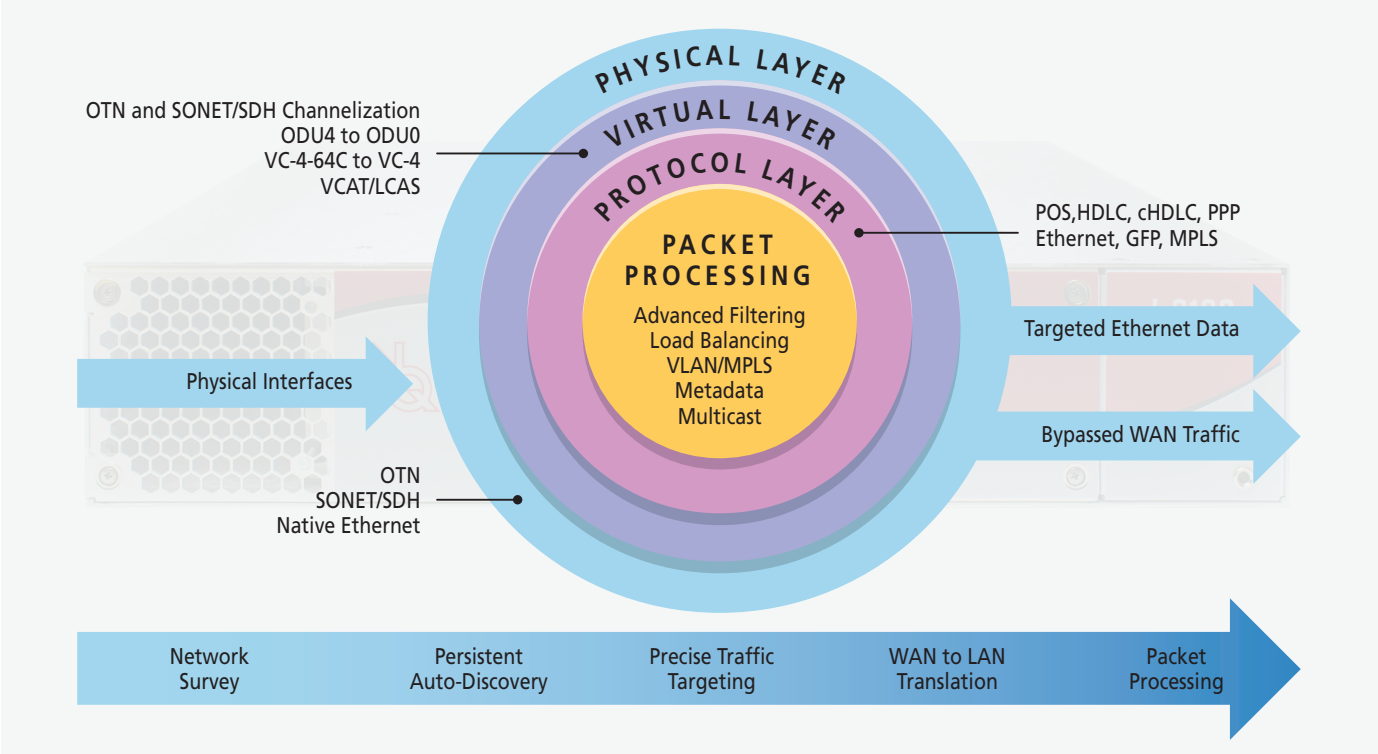


FIGURE 5 – The Interceptors handle processing and removal of multiple network layers including the physical transport hierarchy (OTN/SONET/SDH) as well as higher-layer traffic protocols providing direct access to the targeted network traffic for monitoring.

NETQUEST 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.

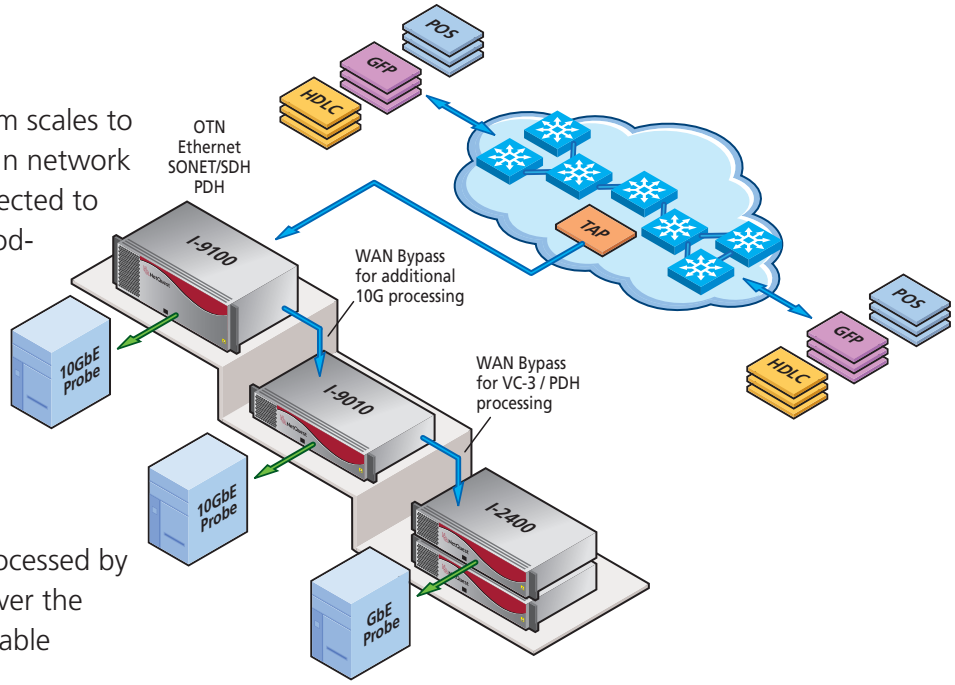


FIGURE 7 – The NetQuest Interceptor solution can scale to meet any network surveillance requirement by daisy chaining together two or more devices.

NETQUEST INTERCEPTOR PORTFOLIO

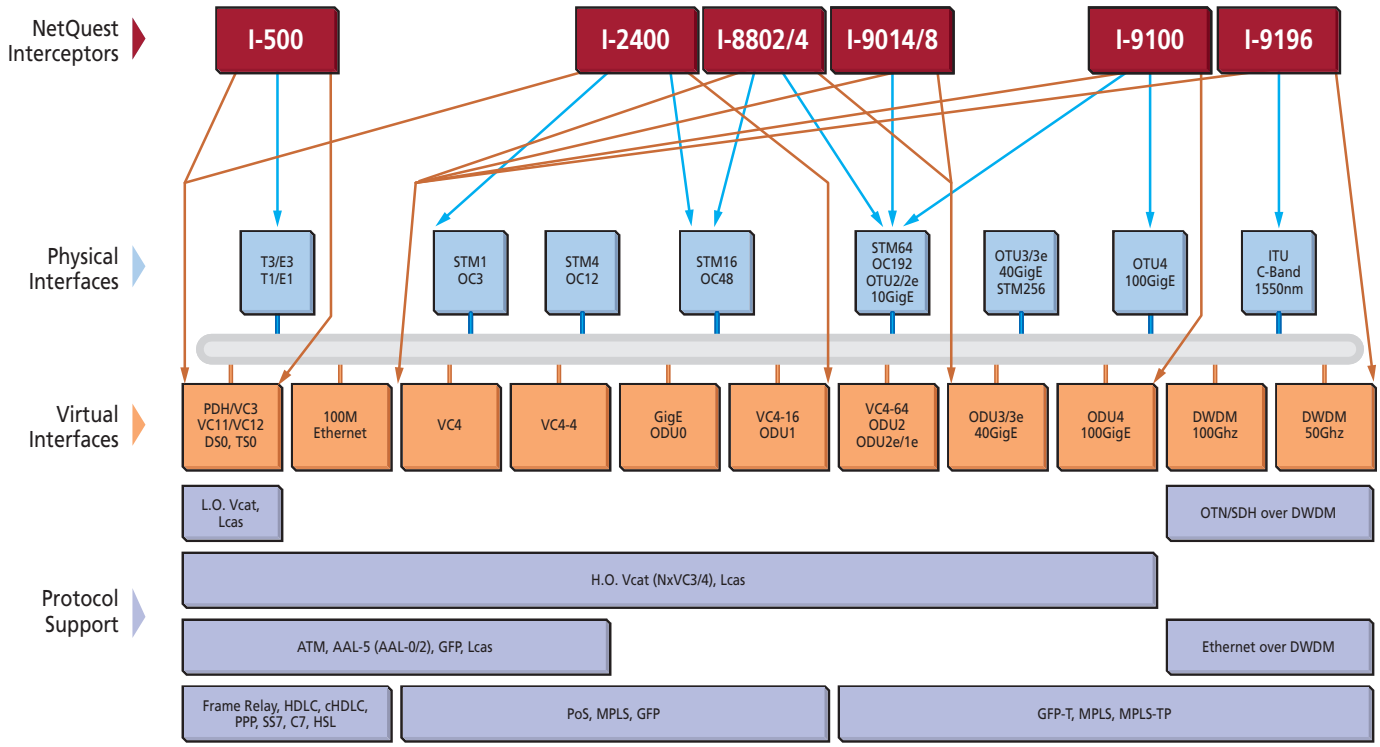
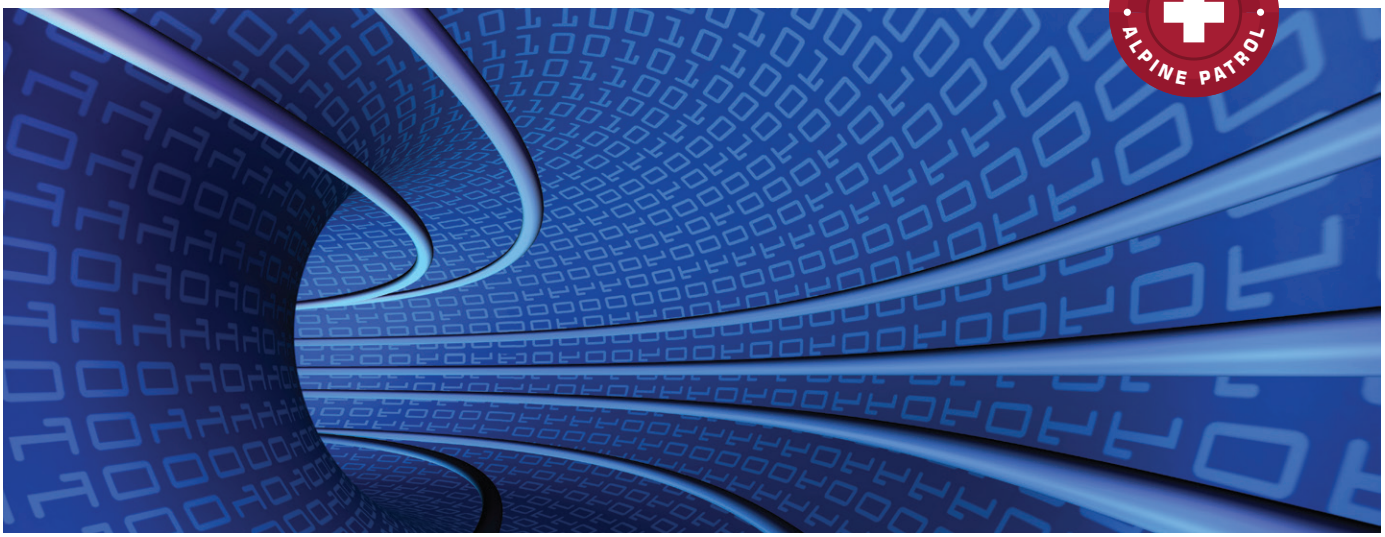


FIGURE 8 – The Interceptor Portfolio supports a wide range of physical interfaces, their virtual channelization and the protocols carried within their payloads.

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.

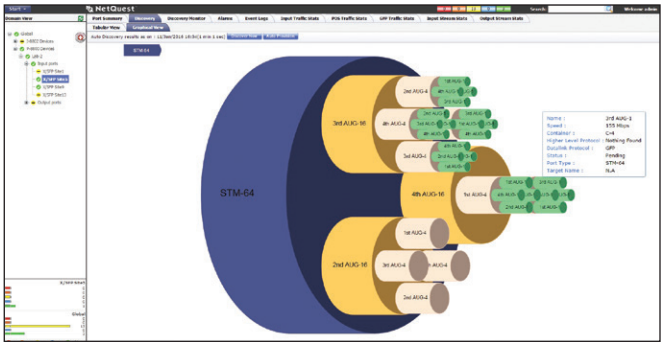


FIGURE 9 – NetQuest Alpine Patrol EMS enables graphical representation of Interceptor Auto-Discovery results and simplifies targeting setup.

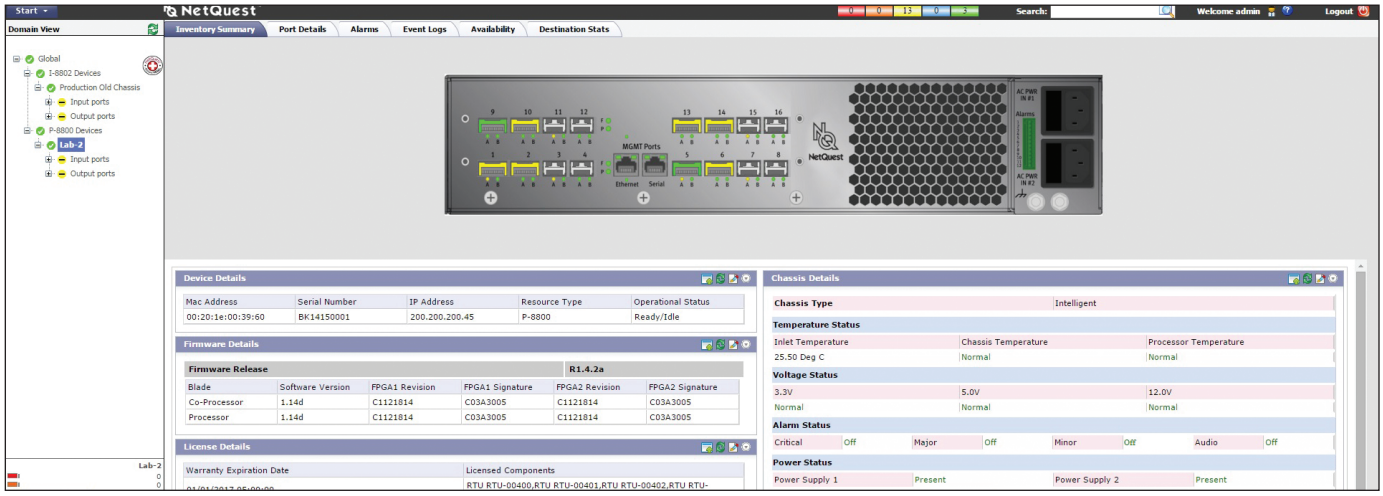


FIGURE 10 – NetQuest Alpine Patrol EMS provides an intuitive GUI interface with the ability to manage multiple Interceptor devices from a central application.

TECHNICAL SPECIFICATIONS

Monitoring Mode	100G	40G	10G
Input Ports	2 x OTU4, 100GigE	2 x OTU3/3e, 40GigE	8 x OTU-2/2e/1e, OC-192/STM-64, 10GigE
Auto-Discovery / Targeting Bandwidth	200/200 Gbps	80/80 Gbps	80/80 Gbps
Bypass Ports	Up to 16 x OTU2	Up to 4 x OC-48/STM-16 Includes any-to-any VC4-4c, VC-4 or VC-3 level	Up to 4 x OC-48/STM-16 Includes any-to-any VC4-4c, VC-4 or VC-3 level
Ethernet Output Ports	20 x 10GigE	12 x 10GigE	8 x 10GigE
OTN Auto-Discovery	From OTU4 to ODU3/2/2e/1/0 to SONET/SDH	From OTU3/3e to ODU2/2e/1/0 to SONET/SDH	From OTU2/2e/1e to ODU1/0 to SONET/SDH
SONET/SDH Stream Auto-Discovery	From OC-192/STM-64 (VC4-64c) down to VC-3 including VCAT/LCAS at Nx VC-3 or Nx VC-4		
Framed Stream Auto-Discovery	POS, EoS, WAN PHY, GFP, Ethernet		
Protocol Stream Auto-Discovery	PPP, MLPPP, cHDLC, MPLS, IPV4, IPV6, MAC		
Additional Traffic Processing Features	Layer 2-4 Packet Filtering/Forwarding, Load Balancing, Multicast, MAC address steering, MPLS label handling, VLAN tag handling, Metadata insertion		
Security / Authentication	Radius, TACACS+		
Management	Telnet, SSH, GSCP, SNMP		
Size	2RU rack mount or table top 3.5”H x 19”W x 17.25”D (8.9cm H x 48.3cm W x 43.8cm D)		
Weight	25 pounds (11.3 kg)		
Power	220 W	200 W	160 W
Operating Temp	32° – 104° F (0° – 40° C) Includes hot swap capable fan tray that has integrated fan speed control.		
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.

Product specifications are subject to change without notice.

WWW.NETQUESTCORP.COM

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