JDSU PacketPortal™ Solution

PacketPortal™

Applications

- IPTV service quality monitoring
- LTE mobile and data network monitoring and troubleshooting
- Troubleshoot and monitor IP networks
- Performance and SLA management
- Network security and customer analytics monitoring
- Revenue-generating new service deployments

Key Features

- Decoupled data collection and management for dramatic reach, visibility, and scale
- Centralized configuration, management, and aggregation of data feeds
- Secure, protected, and encrypted communications with IP-Lock™
- Extensible platform powered by an open API and developers toolkit to fuel applications and tools
- Green: reduced cost, footprint and energy consumption
- Auto-discovered, self-configured cloud accelerates rollout, ROI, and reduced OpEx
- Extended packet-capture capabilities to the edge of the network

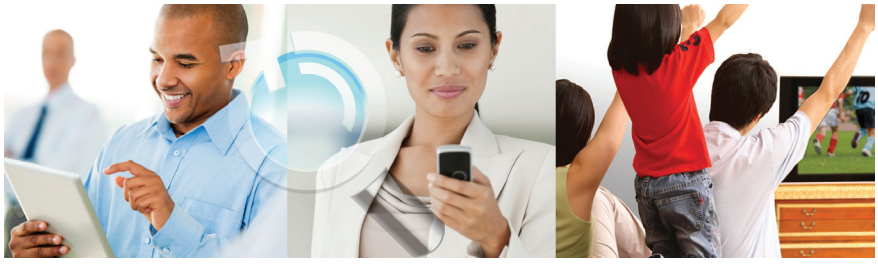
Key Benefits

- Improve the customer experience with proactive monitoring of subscribers, applications, and content from anywhere in the network
- Gain valuable intelligence to optimize performance, minimize revenue leakage, improve troubleshooting, and introduce new services
- Easily obtain critical data, eliminate monitoring ports, taps, costly overlay networks and remote packet-inspection appliances
- Realize a risk-free return on investment, complement and increase the value of existing tools and applications, and use existing network devices more fully
- Instantly reach critical information anywhere in the network on an unprecedented scale
  - Turn standard Gigabit Ethernet optical SFP ports into packet-collection probes
  - Collect intelligence for monitoring, management, and business applications

PacketPortal - Redefining customer,content, and network intelligence

PacketPortal is a revolutionary cloud-based approach that embeds data-capture technology throughout the network, delivering in-line intelligence to any monitoring, management, or business application. PacketPortal lets you see the network the way your customers experience it.

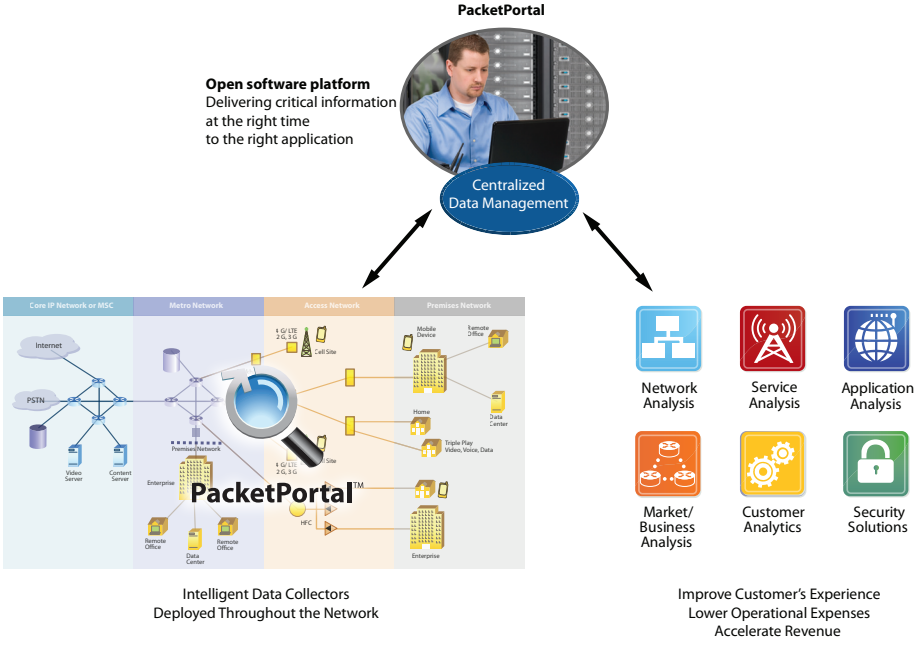
It unleashes network applications and tools with the insight they need to solve problems faster, optimize performance, and minimize revenue leakage while enabling additional revenue opportunities and services. PacketPortal is powered by an open platform that brings unprecedented visibility and reach that scales throughout any network to obtain critical information on demand. PacketPortal-enabled Gigabit Ethernet small form factor pluggable (SFP) transceivers embedded with intelligence collectors provide deep in-line visibility to information previously hidden within networks.



Solution Overview

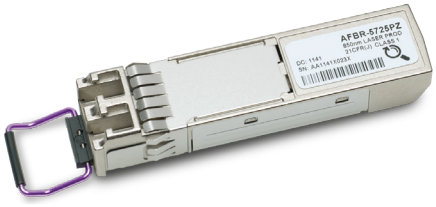
The JDSU PacketPortal solution is a software platform that uses passive, inline intelligent packet director (IPD) transceivers to selectively copy and forward packets from an Ethernet network to a target application. Due to its revolutionary form-factor, it can be affordably distributed where traditional tools are not practical; allowing network operators and managers to access packets and data at any point in the network where optical Ethernet SFPs are used.

The PacketPortal solution examines packets at full-duplex line-rate speeds, empowering the IPD to identify packets of interest that are then copied from the network, accurately time-stamped, encapsulated into a results packet, and inserted back into the network for routing to the targeted application—all without causing loss or disruption to the original flows.



Intelligent Data Collectors
Deployed Throughout the Network

Improve Customer's Experience
Lower Operational Expenses
Accelerate Revenue

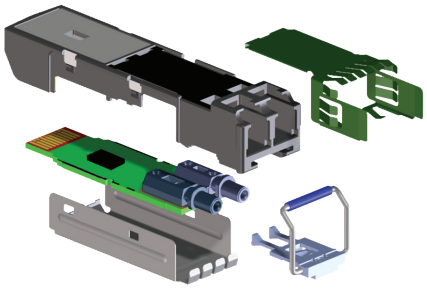


The PacketPortal SFProbe™

The JDSU SFProbe™ IPD Transceiver

This IPD innovation is the result of a joint development initiative between Avago Technologies®, JDSU, and industry-leading network equipment manufacturers (NEMs) to build intelligence into industry-standard SFP transceivers by leveraging unused power within the package for a specialized, embedded, application-specific integrated circuit (ASIC). This new intelligent SFP transceiver, the SFProbe, is designed and manufactured by Avago Technologies with inspection and packet-capture technology developed by and licensed from JDSU.

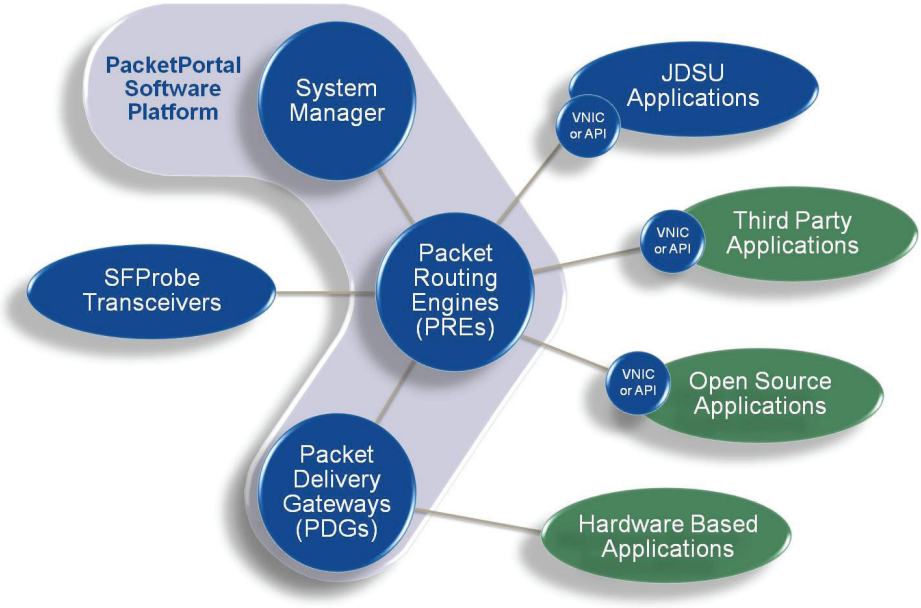
SFProbes redefine how and where operators can gather packets throughout today's networks by eliminating the limitations of SPAN port, tap, aggregator, or mirror port availability and locations. SFProbes can replace any standard 1 GE SFPs, adding PacketPortal's intelligent packet collection capabilities to any network element. SFProbes turn any optical Gigabit SFP port, at any location, into an intelligent remote monitoring port. Packets may then be forwarded to any instrument, monitoring, management, or business application for analysis or collection.



Integrated ASIC with JDSU technology

PacketPortal Architecture

The JDSU PacketPortal solution consists of carrier-grade modular components that allow for scalability from hundreds to thousands of SFProbes. The PacketPortal cloud-based architecture separates data capture from data analysis, providing more centralized access to remote data throughout the network. This capability enables faster, more cost-effective network troubleshooting, service monitoring, and network analysis while delivering additional revenue opportunities by enabling new and innovative services or applications.



The PacketPortal Solution Architecture

System Manager

The System Manager provides user management and system access through an easy-to-use, web-based graphical user interface (GUI) that users can access through any compliant browser. The intuitive user interface of the System Manager allows for quick, easy access to the features, functionality, and management of the entire system. Online help and contextual prompts ensure quick, easy navigation of PacketPortal for accessing network data and targeting packets without requiring extensive training or detailed understanding of network protocols, encapsulations, and architectures.

Packet Routing Engine (PRE)

JDSU designed the PacketPortal solution for flexibility and scalability. The PRE provides scalable management and control of SFProbes across the network. Each PRE manages and controls up to 500 SFProbes.

A PRE maintains network connections, state, time synchronization, encryption, and discovery, and it routes captured result packets for the SFProbes in its domain. Decoupling the PRE functions from the central System Manager lets a PacketPortal system scale to sizes never before conceived of for packet-access solutions. PREs may be synchronized with a global time source, such as a global positioning system (GPS), network time protocol (NTP), or IEEE 1588 master clock. And, with IP-Lock secure 128-bit encrypted discovery and communications between PREs and SFProbes, operators can rest assured that critical network access and measurement information is protected against unauthorized access.

Packet Delivery Gateway (PDG)

A key value of PacketPortal is the ability to preserve investments in current, legacy, and future network tools and instruments. The PDG is one element that makes this possible. A PDG allows one or more applications to connect to a PacketPortal system and receive time-aligned packets as if they were locally connected to a monitor port or tap at the remote location. The PDG uses capture timestamps and sequence numbers from the SFProbe to replay aggregated streams out its monitor port. These streams maintain proper sequencing and inter-packet timing that represents what the packets experienced while passing through the remote network port.

PDGs can feed packets to any device or application that would normally connect to a tap, SPAN port, aggregator, mirror port, or equivalent technology. It enables applications to reside in central locations instead of remote locations where it may not be economically practical to deploy.

Virtual NIC Driver (VNIC)

The VNIC is a software component that, when installed on a PC or server, emulates a physical network interface card (NIC) driver and allows virtually any Ethernet-based software application to receive feeds from a PacketPortal system through its NIC interface. The VNIC receives PacketPortal feeds, removes the transport headers and metadata to reveal the network traffic, and retransmits the original packets to the PC's network stack. The traffic is replayed using the original capture timestamps and sequence numbers to accurately represent the traffic as it was captured at the remote element. The replay may be configured to output on a specific transmission control protocol (TCP) or user datagram protocol (UDP) port from the PRE to the VNIC.

The VNIC can also read captured network data files in the packet capture (PCAP) format and replay them similarly to how live traffic is processed through the PacketPortal system.

JDSU PacketPortal Enabled

JDSU PacketPortal is empowering a new generation of tools and applications for network monitoring, management, troubleshooting, analysis, security, performance analysis, and service assurance. Even though PacketPortal easily interfaces with existing tools and equipment with the PDG and VNIC drivers today, the comprehensive PacketAccess API allows application developers to create new and even more powerful applications that can exploit the reach and intelligence gathering capabilities of the PacketPortal solution.

The JDSU PacketPortal Enabled logo program helps system operators identify both hardware and software designed and tested to work with PacketPortal. Looking for the PacketPortal Enabled logo lets users quickly and easily identify software and hardware that has been tested against and takes advantage of PacketPortal features.

The true value of PacketPortal comes from the unlimited set of applications that the system can support. Indeed, most Ethernet-based applications used today can immediately benefit from the pervasive reach and information PacketPortal provides; protecting and enhancing the investment made in existing network tools and applications.

PacketPortal-Enabled Applications

- The **Triple Play Analyzer (TPA)** — a powerful and complete monitoring and troubleshooting solution to help you install and troubleshoot voice, data, and video applications. Now enabled by PacketPortal, you can view actual customer video, network errors, packet loss, and voice quality from the network edge in your own office—so you find and fix customer service issues significantly faster.
- The **Network Analyzer (NA)** — letting you detect and fix network service problems, its protocol-analysis capability, combined with the reach of PacketPortal, provides an unprecedented network and protocol test solution.
- The **Signaling Analyzer Real Time (SART)** — the test industry's most complete, end-to-end analysis and troubleshooting solution for mobile networks, including LTE, providing comprehensive monitoring and network diagnostics by interpreting, correlating, and analyzing protocol signaling messages produced by multiple network technologies at mobile network interfaces.

PacketPortal-Validated Applications

PacketPortal-validated applications have been JDSU tested and certified for use with the PacketPortal system's PDG and VNIC. These applications include:

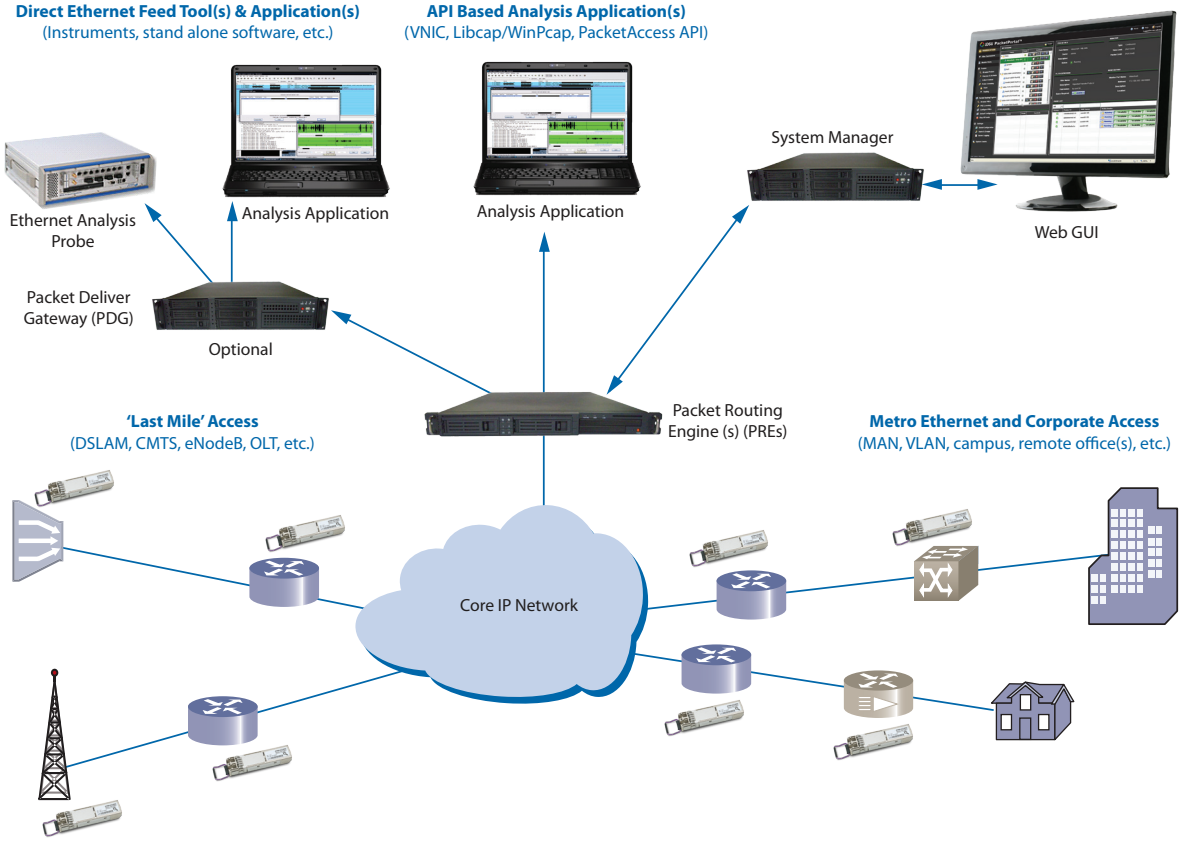
- **Wireshark** — the most widely used, open-source packet analyzer for network troubleshooting and analysis. PacketPortal lets Wireshark provide access from one central office to data across your entire network, to the edge, and to remote offices.
- **nProbe** — an open-source application software utility that creates NetFlow records from monitored network packets. PacketPortal can feed nProbe from across the network, generating NetFlow records with more reach, less cost, and without impacting element performance. NetFlow is a Cisco Systems® technology that collects IP traffic information and has become an industry standard for traffic monitoring.

Solution Features

Carrier-Class SFProbe Hardware and System Software

SFProbes meet all the same safety, regulatory, reliability, and environmental specifications as traditional SFPs. Operators can confidently deploy SFProbes knowing that they pass GR-468-CORE, UL, RoHS, FCC, and TUV requirements and have mean time between failures comparable to equivalent optical 1 GE SFP transceivers.

PacketPortal's scalable architecture lets the system grow with the network and customer base. The central System Manager handles user and element management through an Adobe Flex web interface. All software is hardened and designed for sustained operation and availability.



SFProbes deployed in core, edge, and access element SFP ports

Auto Configuration and Discovery

PacketPortal simplifies both management and deployment of SFProbes throughout a network. Unlike traditional probing and analysis systems, PacketPortal does not require operators to maintain or configure addresses or communication protocols on SFProbes. SFProbes employ JDSU technologies that learn the network encapsulations and addresses needed for communications. Users simply install a SFProbe within the network and send a discovery message from the System Manager. The SFProbe recognizes the discovery message, interprets and incorporates the network encapsulations for all communications, establishes a secure encrypted communication channel, and provides addresses that may be used to communicate with it. This revolutionary technique enables operators to easily manage, install, and control systems employing thousands of access locations.

Secure Management

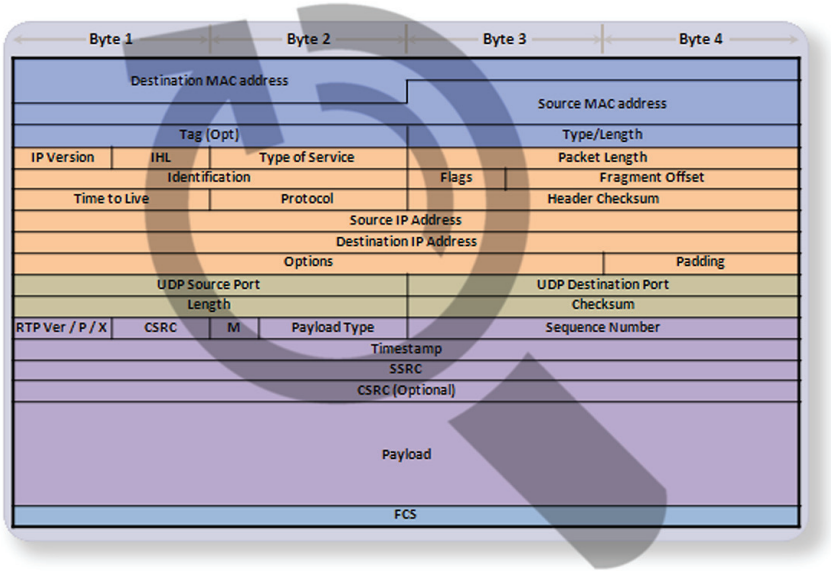
IP-Lock™, PacketPortal's security technology, is the cornerstone of the secure communications architecture. The system employs sophisticated session-based 128-bit Grain cipher encryption algorithms in addition to controlled, unique activation keys for every SFProbe. Individual sessions are additionally protected from unauthorized access through session key hopping, command and control sequencing, and other proprietary methods.

Time Synchronization

Accurate time-synchronized measurements across a network allow for resolving problems faster and with greater precision and confidence. PacketPortal provides globally accurate time synchronization throughout the system from PRE to SFProbe. PREs may be time-synchronized using IEEE 1588v2 Master Clocks, Network Time Protocol (NTP), or GPS. PREs then synchronize the SFProbes on their domain.

Line Rate Deep Packet Inspection Technology

The JDSU PacketPortal solution provides the performance needed to handle even the most used Gigabit Ethernet connections. SFProbes can perform full line-rate (1 G) inspection. SFProbes do not add any additional central processing unit (CPU) load to network equipment and guarantee 100 percent original network traffic throughput without the risk of dropping network packets.



Examine and logically filter on any bit or byte within any Ethernet packet, IPv4 (shown), or IPv6

Data and Packet Acquisition

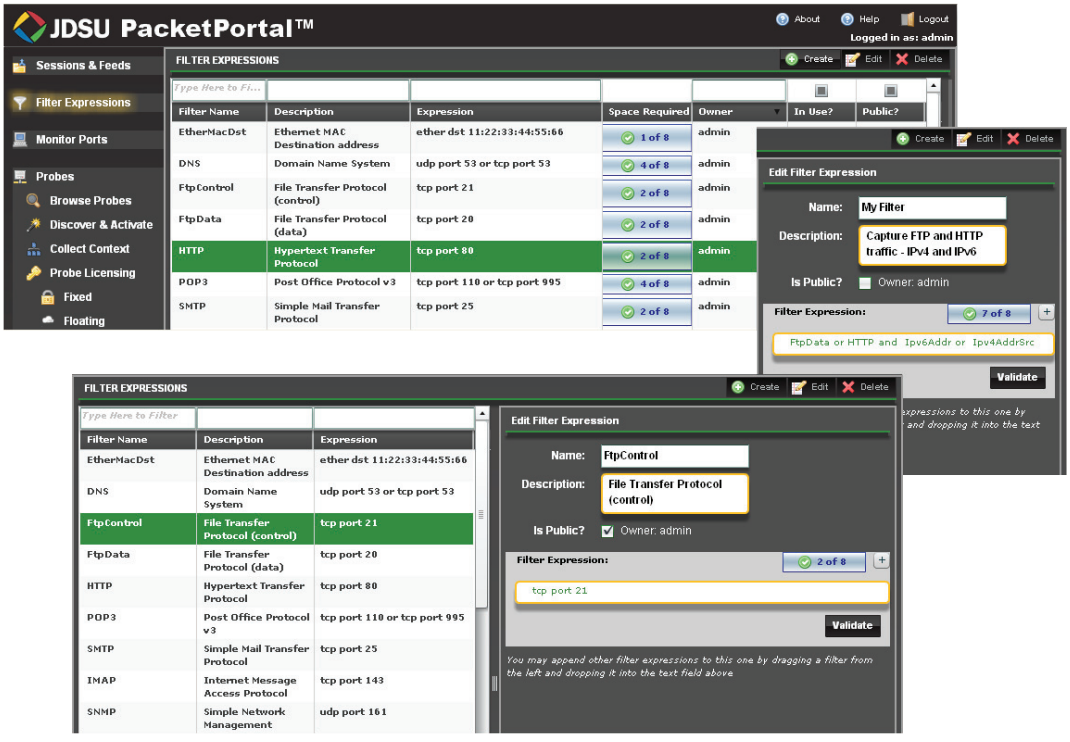
PacketPortal simplifies the burden of quickly accessing critical network data. It delivers, on demand, information of interest to the tools and applications that need it by leveraging unused bandwidth on the network being monitored. Costly analysis applications and measurement equipment can now be centrally located and extend their reach all the way to the edge of the network where they can add the most value.

The SFProbe is a true inline device that does not require a separate network connection to deliver captured packets. Instead, it incorporates JDSU subchannel technology. The subchannel in the SFProbe allows the system to take advantage of interpacket gaps and unused bandwidth in a network when it needs to communicate or send results. When an idle period is detected, a results packet is inserted into the network for routing back to the system and subsequently the destination applications or tools. The subchannel guarantees no network packets will be dropped while passing through the SFProbe.

Adaptive Boolean Filtering

PacketPortal makes acquiring the necessary data to resolve even the most complex network issues easier than ever. Next-generation networks constantly evolve and may use different protocol encapsulations throughout the network. To simplify data and packet acquisition, every SFProbe incorporates a protocol header parser (PHP) that automatically identifies most major protocols over virtually any network encapsulation. This PHP works in conjunction with four programmable filter banks, which may be activated in every SFProbe. Each filter bank may hold up to eight bidirectional independent filter patterns that define the network traffic to be captured and forwarded.

Users can quickly set up simple or complex filters using the System Manager web-based GUI. They can use libpcap-like expressions and Boolean logic without having to worry about the underlying encapsulations. The PHP automatically adjusts to network changes, eliminating the need to manually maintain or adjust filters. Advanced Boolean logic allows for setting up complex filters that target just the data needed by using logical expressions such as ANDs, ORs, and NOTs. Users can filter based on any value or byte in a header. In addition, filters can be set to look for pattern matches at set or variable offsets that account for variable length headers or differing protocol encapsulations.



Collect intelligence with intuitive filtering on any aspect of any packet

Adaptive Header Slicing and Sampling

JDSU realizes that every bit has a cost and many problems do not need the entire packet returned for analysis. PacketPortal allows users to determine how much or how little data to return to the analysis application. An SFProbe can be programmed to send entire packets or only packet headers, with the payload sliced out, even for protocols with variable-length headers. Statistical intelligence is also made possible through sampling. Every Nth packet can be sampled instead of every packet. This capability allows operators to efficiently manage bandwidth and receive only the data required for the target application.

A Multiuser and Multi-Application System

PacketPortal improves existing applications and tools by giving them the network access and reach needed to realize their true potential. The solution provides Packet Delivery Gateways (PDGs) and an open application programming interface (PacketAccess™ API) that let any Ethernet-based applications receive packets and data from the system. The VNIC and libpcap/WinPcap drivers let software-based applications receive packets without needing modification. The PacketAccess API lets users write or modify applications using the rich metadata, timestamps, and sequence numbers returned with every results packet. All these capabilities are in a hardened, multiuser, multi-access system with administrated levels of access and control that accelerate and simplify user management and system access.

Rapid Return on Investment

PacketPortal redefines how and where critical information is accessed throughout a network. Its pervasive data reach and visibility unleashes network applications and tools with the insight needed to solve problems faster and to drive additional revenue with new innovative services.

PacketPortal delivers a fast return on investment and value from initial installation through final deployment. Scaleable start-up costs and multiple tiers of functionality let the system grow with network and data collection demands. The solution's open system lets it work out-of-the-box with the applications used today to manage, troubleshoot, and maintain networks. PacketPortal improves upon these applications by extending their reach, expanding their access, and enabling appliance and application centralization. In addition, PacketPortal enables a new generation of applications through its open, PacketAccess API features that provide deeper packet metrics and empower new value-added applications.

Specifications

Supported encapsulations for PacketPortal command and control

IPv4/IPv6
IPv4/IPv6-IPv4/IPV6
IPv4/IPv6-GRE-IPv4/IPV6
IPv4/IPv6-GRE-MPLS{n}-IPv4
MPLS{n}-IPv4
MPLS{n}-IPv4-IPV4/IPv6
MPLS{n}-IPv4-GRE-IPv4/IPv6
MPLS{n}-IPv4-GRE-MPLS{n}-IPv4/IPv6
MPLS{n}-Ethernet-PPPoE-PPP-IPv4
MPLS{n}-IPv4-GRE-MPLS{n}-IPv4
PPPoE-PPP-IPv4/IPv6
VLAN{n}-IPv4/IPv6
VLAN{n}-IPv4/IPv6-IPv4/IPv6
VLAN{n}-IPv4/IPv6-GRE-MPLS{n}-IPv4
VLAN{n}-IPv4/IPv6-GRE-IPv4/IPv6
VLAN{n}-MPLS{n}-IPv4
VLAN{n}-MPLS{n}-IPv4-IPv4/IPv6
VLAN{n}-MPLS{n}-IPv4-GRE-IPv4/IPv6
VLAN{n}-MPLS{n}-IPv4-GRE-MPLS{n}-IPv4/IPv6
VLAN{n}-MPLS{n}-Ethernet-PPPoE-PPP-IPv4
VLAN{n}-PPPoE-PPP-IPv4/IPv6

Note: (n) represents multiple layers of a particular protocol header and can range from 1 to 8 stacks for VLAN and 1 to 4 for MPLS.

Supported protocols for automatic packet matching

Data link layer protocols:

Ethernet
VLAN (up to 8 layers)
MPLS (up to 8 labels)
GRE
L2TP (L2F/v2/v3)
PPP/PPPoE
PPP-HDLC
ARP
Provider Backbone Bridge (PBB)
Pseudowire Emulation Edge-to-Edge PWE3

Network layer protocols:

IPv4 and IPv6
IGMP
IPsec (ESP, AH) note: no decryption is done
ICMP
ICMPv6/MLD

Session to application layer protocols:

GTPv0/1/2
GTP'v0/1/2
RTP
RTCP
MPEG-TS
SCTP chunks

Transport layer protocols:

TCP
UDP
SCTP/M3UA

SFProbe

Multi-Source Agreement (MSA) INF-8074i SFP, Rev 1.0 compatible
MSA SFF-8472 Diagnostic Monitoring Interface (DMI) for Optical Transceivers, Rev 10.4
GR-468-CORE (Generic Reliability Assurance Requirements for Optoelectronic Devices Used in Telecommunications Equipment) certified
Class 1 eye-safety certified
Packet capture time stamp resolution: 16 nanoseconds
Packet inspection delay (every packet): 2.46 microseconds; maximum variable delay of up to 16.69 microseconds when inserting packets at the same time a packet is arriving
Four programmable filter banks. Each filter bank may hold up to eight independent bidirectional filter patterns that define the network traffic to be captured and forwarded or sliced.

SFProbe SX

IEEE 802.3-2008 Gigabit Ethernet (1.25 GBd) 1000Base-SX
850 nm vertical cavity surface emitting laser (VCSEL)
Supports 62.5/125 µm and 50/125 µm multimode fiber
Up to 550 m range

SFProbe LX

IEEE 802.3-2008 Gigabit Ethernet (1.25 GBd) 1000Base-LX
1310 nm Fabry-Perot (FP) laser
Supports 9/125 µm single-mode fiber
Up to 10 km range

System Manager

Supports up to 30 simultaneous users, supports up to 500 user accounts
Controls up to 100 packet routing engines
Supports a maximum of 10,000 SFProbes network wide
Client Requirements:
- Adobe Flex web user interface
- Web browser HTTPS required

Packet Routing Engine (PRE)

Supports up to 500 activated and managed SFProbes per PRE
Maximum throughput: 350,000 packets per second
- Up to 1 G max for incoming flows and up to 1 G for outgoing flows per PRE

Time Synchronization (recommended)

Time synchronization: IEEE 1588 v2 or NTP or GPS
Timestamp accuracy between multiple SFProbes on a single PRE is less than one millisecond

Packet Delivery Gateway (PDG)

Up to 300 Mbps for incoming flows and up to 300 Mbps for outgoing flows per PDG

VNIC

Throughput:	up to a maximum of 500 Mbps for Linux and 300 Mbps for Windows XP

Server and PC Requirements

System Manager, Packet Routing Engine, or Packet Delivery Gateway:

Processor:	Intel Chipset (single processor) Intel™ Xeon 5650 (2.66 GHz with 6 cores) or better
Cache:	12 MB
Bus speed:	1,333 MHz
Network interface card (PCIe)	
Chipset:	Intel
Number of ports on card:	4
Additional # of Ethernet ports in chassis:	1 (Telemetry Port)
Memory:	8 GB
HDD:	500 GB
Operating system:	SUSE Linux Enterprise Server 11 Service Pack 1 (SLES 11) (64 bit) Red Hat Enterprise Linux Server 6.0 (RHELS 6.0) (64 bit)

Note: each application requires its own server. Virtual machines (VMs) are not supported

VNIC:

Processor:	Intel Chipset (single processor) Intel™ Xeon 5650 (2.66 GHz with 6 cores) or better
Cache:	12 MB or greater
Bus speed:	1,333 MHz
Network interface card :	Intel recommended
For remote access (RDP) an additional NIC is required	
Memory:	8 GB or greater
HDD:	500 GB
Operating system:	SUSE Linux Enterprise Server 11 Service Pack 1 (SLES 11) Red Hat Enterprise Linux Server 6.0 (RHELS 6.0) Windows XP Service Pack 3 (32 bit)

VNIC – Laptop Configuration (performance not guaranteed)

Processor:	Intel Chipset (single processor) Intel™I7 M620 or later (2.66 GHz with 4 cores) or better
Cache:	4 MB or greater
Bus speed:	1,333 MHz
Network interface card :	Intel recommended
For remote access (RDP) an additional NIC is required	
Memory:	3 GB or greater
Free HDD space:	1 GB
Operating system:	Windows XP Service Pack 3 (32 bit)

Test & Measurement Regional Sales

NORTH AMERICA
TEL: 1 866 228 3762
FAX: +1 301 353 9216

LATIN AMERICA
TEL: +1 954 688 5660
FAX: +1 954 345 4668

ASIA PACIFIC
TEL: +852 2892 0990
FAX: +852 2892 0770

EMEA
TEL: +49 7121 86 2222
FAX: +49 7121 86 1222

WEBSITE: www.jdsu.com/test

 30168465 000 0212 PACKETPORTAL.DS.NSD.TM.AE February 2012