How PacketPortal Works

PacketPortal is a completely new approach to gathering, distributing, and analyzing information from a distributed Ethernet network. The PacketPortal software solution uses embedded microprobe technology throughout the network to manage data and make it available in real time, through the cloud, to virtually any kind of monitoring, management, or business application. This improves the effectiveness and value of existing tools and applications by extending reach to the distributed access and end points that most closely represent an end-user's experience.

In its initial implementation, microprobe technology is embedded in standard SFP transceivers to create SFProbes™: intelligent packet-director transceivers that collect and route packets from anywhere in the network, up to the very edge.

The Viavi Solutions™ PacketPortal solution consists of carrier-grade modular components that allow for scalability from hundreds to thousands of data collectors. PacketPortal 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, and adds revenue opportunities through new and innovative services and applications.

PacketPortal™

White Paper

The PacketPortal system consists of six architectural components:

- **SFProbe Intelligent Packet Director (IPD) Transceivers —** optical gigabit Ethernet transceivers that selectively copy packets from the network and transmit them via a designated packet-routing engine to target applications and components.
- **The Packet-routing Engine (PRE) —** provides scalable management and control of SFProbes and aggregates and distributes captured traffic to target applications and components.
- **The System Manager (SM) —** provides user management and system access.
- **The Packet Delivery Gateway™ (PDG) —** receives PacketPortal data and captured network traffic and passes it to a physical network device.
- **The Virtual NIC Driver (VNIC) —** a software integration component that, when installed on a PC, emulates a physical network interface card (NIC) driver and allows any Ethernet-based software application to receive time aligned feeds from a PacketPortal system through its NIC interface.
- **The PacketAccess™ API —** allows software or hardware manufacturers to adapt their equipment or systems to directly accept PacketPortal data feeds, along with the rich metadata included in them.

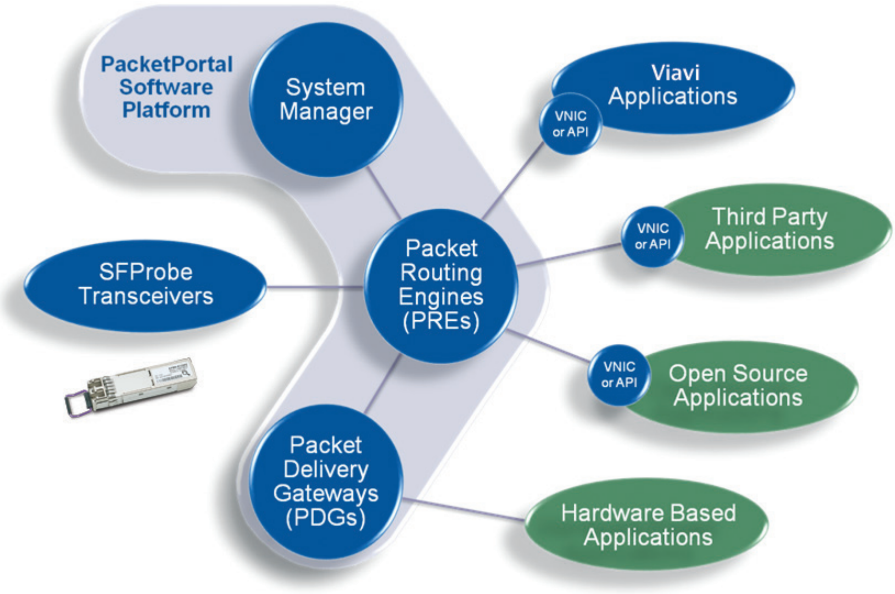

Figure 1. PacketPortal architecture overview

SFProbe Intelligent Packet Director (IPD) Transceivers

The Viavi PacketPortal solution uses SFProbes as intelligent packet director (IPD) transceivers to collect packets from Gigabit Ethernet networks. SFProbes comply with the IEEE 802.3-2008 Gigabit Ethernet standard, are compatible with MSA SFF standards, and seamlessly replace standard 1 GE SFPs. They can be affordably distributed where standard SFP transceivers are used today, allowing network operators and managers to access packets and data at any point in the network where SFPs are used. This improves the effectiveness and value of existing tools and applications by extending reach to the distributed access and end points that most closely represent an end user's experience.

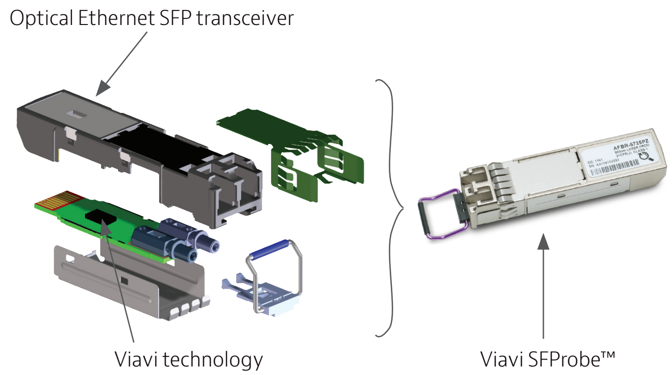

Figure 2. The Viavi SFProbe

The SFProbe uses deep packet inspection (DPI) technology to examine packets at full duplex line rate speeds, letting the SFProbe identify packets of interest which are then selectively copied from the network, time-stamped, encapsulated into a results packet, and inserted back in-line into the network for routing to a designated PacketPortal packet routing engine (PRE). The PRE then forwards the captured data to an application or component requiring the data—all without loss or disruption to the original packet flows.

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. They can be plugged into any SFP-compatible elements such as switches, routers, DSLAMs, and OLTs at the network edge, and can be used throughout the network to replace any standard 1 GE SFP. All SFProbes in the network can be globally time synchronized, to less than one millisecond, using a secure Viavi proprietary time synchronization protocol; this enables synchronized measurements and captures that were not previously possible.

Specifications

SFProbes have an equipment side and a network side. The equipment side plugs into the SFP port on a network device, and the network side transmits and receives data on the fiber optic cables. SFProbes can collect and forward both network-traffic and network-context information without disrupting the original network-traffic flow. SFProbes meet all the same safety, regulatory, reliability, and environmental specifications as standard SFPs. Operators can confidently deploy SFProbes knowing they pass GR-468-CORE, UL, RoHS, FCC, and TUV requirements and have mean-time-between-failure rates nearly identical to equivalent 1 G SFPs.

Key Compliances

- Multi-Source Agreement (MSA) INF-8074i SFP, Rev 1.0 compatible
- MSA SFF-8472 Diagnostic Monitoring Interface (DMI) for Optical Transceivers, Rev 10.4
- Generic Reliability Assurance Requirements for Optoelectronic Devices Used in Telecommunications Equipment (GR-468-CORE) certified
- Class-1 eye safety certified

Key Features

- Line-rate deep packet inspection of any header or payload value
- Selectively copies packets of interest with four independent banks containing eight discrete protocol filters in each direction
- Automatic packet header parser eases filter configuration
- Globally accurate time synchronization enabling cross-network analysis
- Hot-pluggable with bail-wire de-latch
- Single 3.3 V DC power supply
- Industry-standard duplex LC optical connectors
- Available in two operating temperature ranges: 0~+85° C standard and −40°C ~+85°C extended
- 128-bit encrypted discovery and sequenced communications

The Packet-Routing Engine (PRE)

Viavi designed the PacketPortal solution for flexibility and scalability. The PRE provides scalable management and control of SFProbe transceivers across the network. PREs can be deployed on various classes of PCs or servers to enable flexible deployment costs and performance. As systems grow and require higher performance, additional PREs can be deployed quickly and easily. The central system manager (SM) controls and manages the system of PREs through its graphical web-user interface, but their presence and functions remain primarily transparent to the end user and analysis applications.

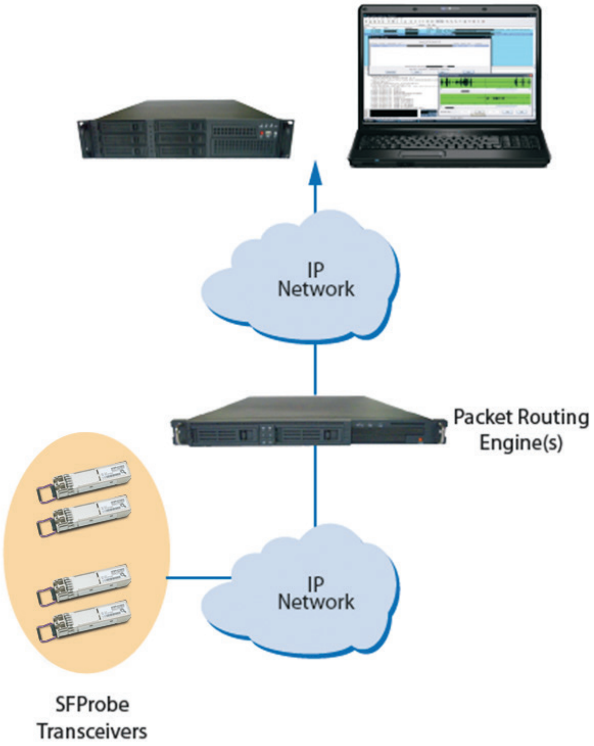

Figure 3. Packet-routing engine configuration

SFProbes inspect all packets against filter expressions defined by a user. When desired data packets are detected, they are copied by the SFProbe into an internal buffer, encapsulated into a results packet and, during idle periods on the link, the results packets are inserted into the network for routing to the designated PRE. The PRE processes the packets and repackages them for routing to the designated network analysis tools or applications determined by the SM user on a user-definable TCP or UDP port.

Specifications

The PREs serve as the conductors of the solution. They maintain connections, state, time synchronization, encryption, and discovery, and then route captured result packets for the SFProbes in their domain. Decoupling the PRE functions from the central SM enables a PacketPortal system to scale to sizes unprecedented in packet-access solutions. A solution requires a minimum of one PRE that can reside on either the SM server or a standalone server. An SM can support up to 100 PREs and each PRE can manage and control up to 500 SFProbe transceivers, giving users ultimate flexibility in designing a solution that meets both their cost and performance requirements. A PRE may only be managed by a single SM and each SFProbe may only be managed by a single PRE.

It is recommended for all PREs to be synchronized with a global time source, such as a global positioning system (GPS), network time protocol (NTP), or IEEE 1588 master clock. Depending on the time synchronization methods, a system can maintain better than sub-millisecond synchronization with all SFProbe transceivers in the solution, thus enabling precision, synchronized distributed analysis throughout the entire network.

The System Manager (SM)

The SM is the heart of a PacketPortal system and provides user management, system administration, and user access through an easy-to-use, web-based graphical user interface (GUI) accessible through any HTTPS-compliant browser. The intuitive user interface provides 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.

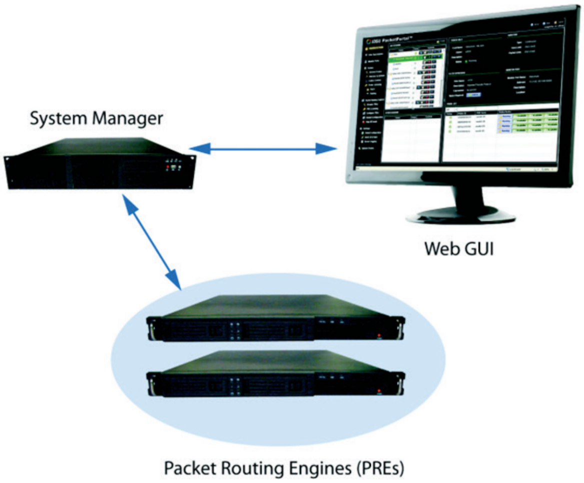

Figure 4. System manager configuration

Key features include:

- Adobe Flex web GUI
- secure license management
- multiple levels of user-defined access groups
  - configurable functionality and accessibility per group
  - extensive logging and user activity tracking
- auto configuration and discovery of SFProbe transceivers
- custom, definable SFProbe attributes
- automatic discovery of probe context
  - identifies SFProbe host element and port information
  - identifies network side element and port information
- adaptive Boolean filtering: does not require knowledge of network encapsulations
- adaptive header slicing and sampling to reduce network bandwidth used
- configurable limits protect network bandwidth and prevent flooding
  - limits maximum packet injection bandwidth by direction
  - configurable maximum link bandwidth threshold
  - definable threshold sample window down to 30 microseconds protects against micro bursts
- secure management of users and SFProbes
- scalable architecture supports and easily manages tens of thousands of SFProbe transceivers
- embedded help and user documentation.

The Packet Delivery Gateway

A key value of a PacketPortal solution is its ability to preserve investments in current, legacy, and future network tools and instruments. The Packet Delivery Gateway (PDG) is the element that makes this possible. The PDG is a software-based appliance that extracts packets from SFProbe data feeds and replays them over a physical network device. The PDG can reside on a standalone server or may co-reside with the SM or a PRE.

Specifications

A PDG lets one or more applications or appliances connect to a PacketPortal system and receive time-aligned packets as if they were locally connected to a mirror port, monitor port, or tap at a remote location. The PDG receives sequence-numbered and accurately time-stamped streams from one or more SFProbes distributed throughout a network. It then replays the aggregated streams out its monitor port with accurately reproduced sequencing and inter-packet timing. The SFProbe streams may optionally be time aligned and merged with streams captured from a locally connected mirror port, monitor port, or tap. The egress feeds from the PDG accurately duplicate what the packets experienced while passing through the remote network port(s), but will be delayed in overall absolute time.

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 lets applications reside in central locations instead of remote locations where it may not be economically practical to deploy measurement equipment. Additionally, data collection is no longer limited to the capabilities or limitations of the remote network element.

The PDG transmits received packets locally through its egress port without examining them for any potential problem conditions. All packets are played back, as is, regardless of how erroneous they may be as long as the NIC and NIC driver allow transmission of these erroneous packets.
For example:

- packets arriving at the PDG listening port may have bad FCS or other errors
- packets arriving at the PDG for playback may have been captured with different network encapsulations
- packets arriving at the PDG for playback may have been captured travelling in different directions on the same wire
- packets arriving at the PDG for playback may actually contain the same packet more than once. This can happen if the same packet is captured by different SFProbes as it traverses the network. This packet would be replicated by each SFProbe and sent to the PDG from each point of capture. Duplicated packets are not identified in the PDG egress stream.

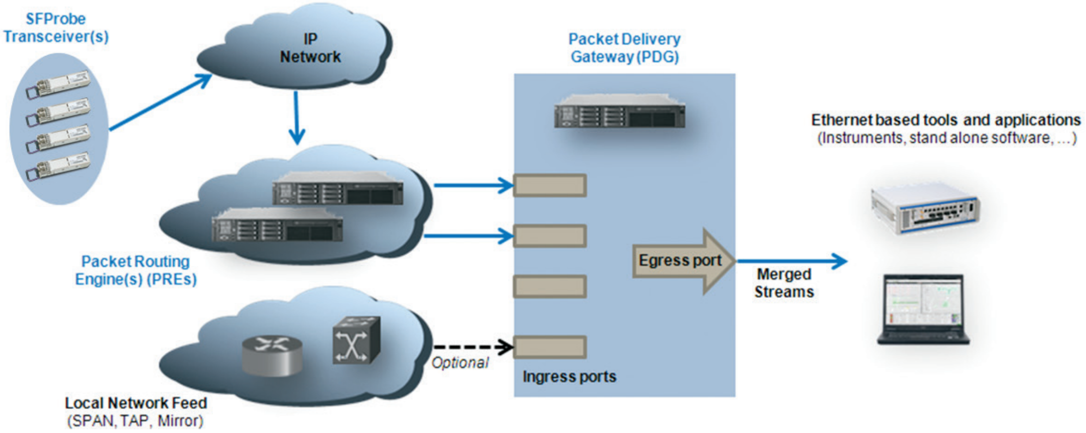
SFProbe Transceiver(s)
IP Network
Packet Delivery Gateway (PDG)
Ethernet based tools and applications
(Instruments, stand alone software, ...)
Packet Routing Engine(s) (PREs)
Egress port
Merged Streams
Optional
Ingress ports
Local Network Feed
(SPAN, TAP, Mirror)

Figure 5. Packet Delivery Gateway configuration

The Virtual NIC Driver (VNIC)

The VNIC is a software utility that emulates a physical network interface card. It allows any Ethernet-based software application to receive feeds from PacketPortal through its NIC interface. The VNIC receives feeds from the PRE, unpacks them, and replays them so that you can view them with an NDIS-ready application.

The VNIC runs on the same PC that runs the network analysis application. To the network analysis application, the traffic on the VNIC appears as if the packets were captured directly at the source (for example, where the SFProbe is physically located). The VNIC re-inserts gaps in order to maintain the original time delays between packets to allow network analysis applications to display the data feeds in their original form.

Specifications

The replay from the PRE to the VNIC occurs through a user-configured TCP or UDP port. The VNIC can differentiate PacketPortal packets from other network packets through this port allocation. This way, the VNIC passes only the desired packets to the application without corrupting the flows with irrelevant network packets on the same port. The VNIC can also read captured network data files in the PCAP format and replay them in the same way that live traffic is processed through the PacketPortal system, preserving the inter-packet gaps.

The communication between PRE and PDG or VNIC is configured through the SM. This is done by specifying the target IP, port, and TCP or UDP protocol when creating new feed destinations. The VNIC driver sits between the NIC card of the feed destination and the target application receiving the data. Windows-based VNICs create an accurate reproduction of packets with regards to order and inter-packet time, but delayed in overall time from when the packets were originally collected. The stream looks just like it did on the line at the time of capture, but it is delayed in absolute time. The Linux version passes on timestamps through the TUN/TAP drive so it also gives the accurate absolute timestamps that the packets received while being captured.

The VNIC driver lets users configure multiple VNICs on a single PC and can feed multiple applications simultaneously. In addition, the driver lets users map SFProbe IDs to virtual LAN (VLAN) IDs. This supports the IEEE 802.1Q version of the networking standard. Twelve address bits limit the number of SFProbes that can be mapped to VLAN IDs to 4096 (0 – 4095). When the mapping is done, the VLAN header is plugged in after the packet header. This allows VLAN-capable applications to differentiate and display data from different SFProbes enabling multi-SFProbe multi-segment measurements and analysis in a single view.

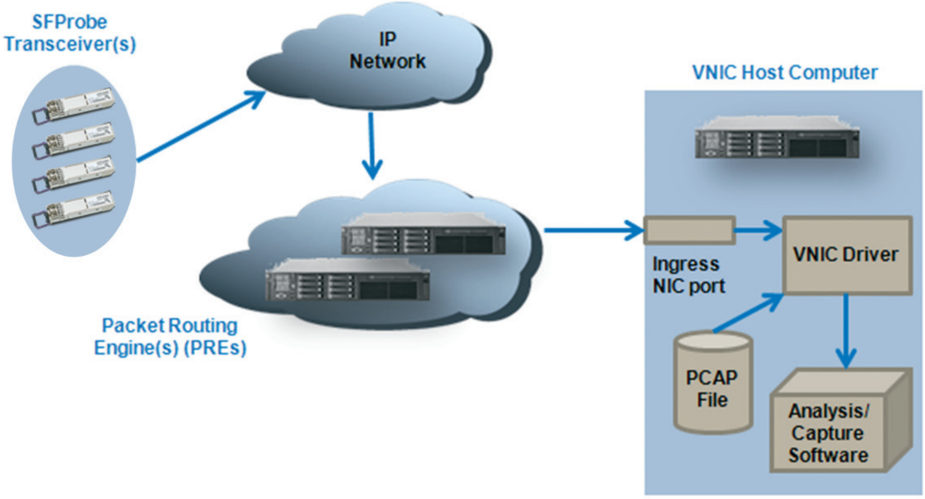

Figure 6. VNIC configuration

The PacketAccess API

PacketPortal offers a comprehensive software development kit and the PacketAccess API that lets software or hardware manufacturers adapt their equipment or systems to directly accept PacketPortal data feeds, along with the rich metadata included within them. This enables integrated applications to receive PacketPortal feeds, remove and interpret the transport headers, and read probe identifiers, timestamps, and other metadata. This ability, coupled with the affordable and ubiquitous reach provided by the SFProbes, empowers applications to deliver more insightful information, quickly solve complex multi-segment problems, and unleash an integrated application's true potential.

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the Viavi office nearest you,
visit viavisolutions.com/contacts.

Product specifications and descriptions in this document are subject to change without notice.