Stacking EndaceProbes using the Ixia Vision Edge Series Network Packet Broker

Scale capacity and throughput by creating a logical probe from a stack of individual EndaceProbes.

Fast and effective response to network security and performance issues means being able to see exactly what's happening on the network and quickly identify the root cause of critical events. Leading organisations record at least a month of rotating network history to enable them to rapidly investigate, triage and remediate issues.

As your network grows and traffic volumes increase, so does your need to scale network history recording infrastructure. This is increasingly challenging as bandwidth consumption grows and new technologies are introduced - such as 25, 40, or 100GbE. What's required is a modular solution that can easily and economically scale to monitor any network, at any line rate, reliably with 100% accuracy. Organizations need capacity that can scale easily, in modular increments as traffic volumes increase, so they can maintain the required length of network history.

This solution brief provides an overview of how Endace and Ixia have teamed up to deliver a solution that scales easily with your growing network to deliver 100% accurate network visibility.

EndaceProbes are the highest capacity and throughput network recorders on the market. In addition to recording network traffic, EndaceProbes allow you to host a wide variety of third-party analytics tools, allowing them to analyze both real-time and recorded traffic at high speed. This unique, open platform approach gives you the freedom to choose best-of-breed security and performance analytics applications and deploy them onto the EndaceProbes in the network quickly without the need to deploy additional hardware.

Ixia's Vision series NPB's incorporate advanced visibility features with an easy-to-use, point-and-click web interface for high-performance, lossless visibility.

Leveraging Ixia's high performance Network Packet Brokers (NPB's), multiple EndaceProbes can be combined into a "stack", creating a logical probe of even greater capacity and throughput, e.g. to monitor a 100GbE link, and/ or extending storage capacity to keep weeks or months of Network History.

PRODUCTS

- Ixia Vision Network Packet Brokers
- EndaceProbe Analytics Platforms

BENEFITS

- Capture packets at essentially any line rate or packet capture rate, e.g. 200Gbps sustained capture on a bidirectional 100GbE link.
- Scale to support practically any storage depth, e.g. to keep 6 months of network history.
- Single pane of glass, centralized UI for performing searches and data mining across stacks of EndaceProbes.
- Fast search - a game changer for productivity. Advanced search algorithms allow operators to execute "needle-in-the-haystack" searches on a stack of EndaceProbes in less than a minute. Search times remain fast even when searching across multiple, large stacks of EndaceProbes.
- N+1 redundancy for ultra-high availability and hitless software upgrades. With N+1 redundancy, stacks continue to function (with reduced capacity) even if one EndaceProbe is offline for any reason. Hitless software upgrades can be done, without downtime, by upgrading each EndaceProbe in sequence.
- Easily adjust what and where you monitor with Ixia's easy-to-use, point-and-click web interface.
- See inside encrypted traffic with Ixia SecureStack, using active or passive SSL decryption.
- Take advantage of Ixia's advanced PacketStack or AppStack features such as Application Filtering, Deduplication, or Data Masking for PCI compliance.

Diagram 1. Stacking EndaceProbes
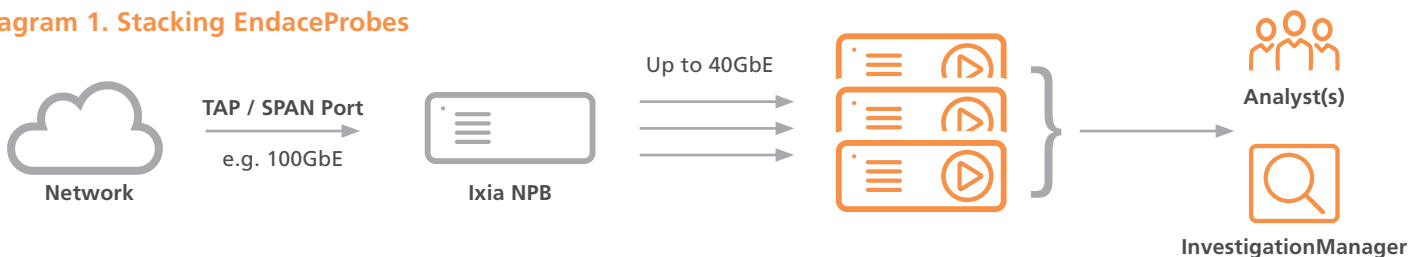
Stacking EndaceProbes

An EndaceProbe stack may be built by connecting more than one EndaceProbe to an Ixia Vision E100, E40 or Vision ONE. The choice of NPB model will depend on the speed of the link being monitored and the number of monitoring ports that are being connected to the EndaceProbes for capturing and recording traffic. The Vision E100 supports up to 100GbE, whereas the Vision E40 and Vision ONE support up to 40GbE.

In a stack configuration, Ixia Vision NPB's receive network traffic through TAPs or SPAN ports, and load-balance this traffic across the stack of EndaceProbes. Any line rate can be monitored by choosing an NPB that supports that line rate. Advanced such as application filtering, deduplication, or Data Masking, can be applied to traffic before delivering it to the EndaceProbes for recording.

A stack of EndaceProbes becomes a logical EndaceProbe of higher throughput and capacity, with a single-pane-of-glass UI. Endace InvestigationManager™ a VM-based software application, provides centralized search, visualization, and analysis across all EndaceProbes in a stack.

EndaceCMS™ Central Management Server provides centralized administration and management of individual EndaceProbes, stacks of EndaceProbes and InvestigationManager instances.

Example Configurations

	Single 9200 Series EndaceProbe[2]	Three 9200 Series EndaceProbes	Five 9200 Series EndaceProbes
Rack space required	4RU	13RU	21 RU
Storage size[1]	Native: 432 TB Packets: > 1 PB	Native: 1.3 PB Packets: > 3 PB	Native: 2.1 PB Packets: > 5 PB
Storage length 1 at average throughput of…	5 Gbps: Up to 18 days 10 Gbps: Up to 9 days 40 Gbps: Up to 2.2 days	5 Gbps: Up to 53 days 10 Gbps: Up to 27 days 40 Gbps: Up to 7 days 50Gbps: Up to 5.3 days 100Gbps: Up to 2.7 days	5 Gbps: Up to 89 days 10 Gbps: Up to 45 days 40 Gbps: Up to 11 days 50Gbps: Up to 9 days 100Gbps: Up to 4.4 days
Write to disk	40Gbs sustained > 40Gbs compressed 80Gbps burst for >300ms	120Gbps sustained > 120Gbps compressed 240Gbps burst for >300ms	200Gbps sustained > 200Gbps compressed 400Gbps burst for >300ms
Maximum flow creation rate	100k flows per second	300k flows per second	500 flows per second
Maximum concurrent flows	1 million	3 million	5 million
Number of application dock instances	x 12	x 36	x 60
Search performance	Less than 1 minute to search the entire storage of one EndaceProbe	Less than 1 minute to search the entire storage of multiple EndaceProbes	
Example Orderable Parts (Must be validated against full requirements before ordering.)	**Endace:** 1 x EP-92C8-G4	**Endace:** 3 x EP-92C8-G4 N x Endace Transceivers 1 x VPRB-CMS or EP-4000-CMS N x VPRB-IM **IXIA:** 1 x SYSE100-32P4X-xx 1 x LIC-E100-INLN N x Ixia Transceivers + optional 1 x LIC-E100-32PC-U	**Endace:** 5 x EP-92C8-G4 N x Endace Transceivers 1 x VPRB-CMS or EP-4000-CMS N x VPRB-IM **IXIA:** 1 x SYSE100-32P4X-xx 1 x LIC-E100-INLN N x Ixia Transceivers + optional 1 x LIC-E100-32PC-U

[1] Effective packet storage accounting for RAID and metadata overheads and assuming a 4.5:1 ratio for compression and Smart Truncation of packet data.

[2] To conduct a single "needle-in-the-haystack" search across the entire time range with 100% of the packet storage on the EndaceProbe(s) consumed.

IXIA Part Number Reference

Choose from Ixia Vision Edge 40 or 100 Network Packet Brokers:

Part Number	Description
SYSE100-8PC-AC, or… SYSE100-8PC-DC	Ixia Vision Edge 100 system chassis with fixed (32) QSFP28 100GE ports. SYSE100-8PC-xx includes (8) licenses. Each license enables (1) port of 100G or 40G or (4) ports of 10G.
SYSE40-24PX-AC, or… SYSE4048PX6P4XDC	Ixia Vision Edge 40 system chassis with fixed (48) 1G/10G and (6) 40G ports; Includes license for (24) 1G/10G or (6) 40G ports
SYS-V116PX8PGAC, or… SYS-V116PX8PGDC	Ixia Vision ONE hardware with 48 physical SFP/SFP+ ports and 4 QSFP+ ports.

Related Documents

Type	Name
Solution Brief	Distributing and Stacking EndaceProbes with EndaceFabric
Technical Brief	EndaceFabric Design Guidelines
Technical Brief	Design Guidelines for Stacking EndaceProbes

For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com

endace.com