vMesh™

Solution Brief

Challenges

- Managing individual traffic capture devices one at a time is cumbersome, time consuming, and error prone
- Failure of a traffic capture port or device isolates a link, which results in loss of monitoring data
- Individual network tools are either over-subscribed or underutilized
- Scaling up the number of traffic capture ports is cost prohibitive
- Packet source link-layer information is lost when traffic is aggregated
- Using traditional aggregators creates silos of monitoring/security tools for separate network segments, making overall tool CapEx prohibitive
- Unable to grow the data access/capture layer on a pay-as-you grow model

Benefits

- Unprecedented global visibility without breaking the budget
- Traffic can be port- and time-stamped for a cost-effective distributed mesh covering all links
- Extends existing tool lifecycles (filtering and session-aware load balancing relieve congested analyzers by sending only traffic of interest to tools allowing for more efficient processing)
- Enables the centralization of tools, significantly reducing total CapEx
- No client software maintenance required (platform-independent, browser-based user interface)
- Simplified, efficient management from a single interface
- No hardware configuration required (auto-discovering, self-configuring mesh)
- Zero-touch failover (self-healing mesh)

Features

- Interconnect up to 256 VSS Network Packet Brokers (NPBs) and 10,000+ ports
- Flexibly decide and adjust how the NPBs are interconnected across LAN, WAN, and internet boundaries
- Aggregate and load balance monitoring traffic over the vMesh toward and across multiple tools, no matter where they are located
- User definable aggregated bandwidth between NPBs
- Automatically performs discovery and configuration of the meshed links
- Architect automatic failover and load redistribution in the event of link failure
- Easily and seamlessly manage all interconnected NPBs

What is vMesh?

vMesh is a resilient, high-availability fabric architecture that connects VSS Monitoring Network Packet Brokers (NPB), using VSS' underlying vStack+™ technology, to enable a system-level approach to the network monitoring and security infrastructure. It creates unprecedented visibility, density, and scalability for NPBs and for the analysis and service assurance solutions they support.

vMesh provides the benefit of:

- A unified visibility fabric
- Unprecedented density and scalability
- Logical links to leverage existing tools

Unified Visibility Fabric

Interconnecting over 10,000 ports across up to 256 VSS Monitoring NPBs in a self-configuring, self-healing monitoring fabric, vMesh allows the monitoring infrastructure of a global network to be fully interconnected and can be managed from a single browser-based dashboard.

By integrating the NPBs into a single mesh topology, vMesh eliminates the need for duplicate or multiple appliances required to connect standalone legacy monitoring devices, reducing TCO and improving ROI.

With vMesh you can create as many aggregation layers as required to monitor and secure all relevant network segments. vMesh brokers captured traffic from a local NPB, which communicates with other NPBs to aggregate and filter to a higher-layer (possibly more capable) NPB, which in turn grooms and balances the traffic to centrally located tools in a network operations center or distributed across the global network.

The connections that form the vMesh can be created at the level most appropriate for the underlying network infrastructure.

- Layer-1 connection via direct cable between vStack+ ports of NPBs
- Layer-2 tunneling (e.g. GRE or L2TP) or pseudowire (e.g. L2VPN) connection between vMesh ports across a WAN
- Layer-4 encrypted TCP connection between vStack+ ports at any point in the network, co-located or remote

Unprecedented Density and Scalability

The mesh topology can range from a single link between two NPBs to a full mesh among 256 NPBs. Complex mesh topologies provide the benefit of bandwidth aggregation and redundant paths. vMesh automatically aggregates bandwidth across parallel paths and redundant paths, automatically reconfiguring monitor output to alternate paths in the event of link or NPB failure.

As a result, network engineers can quickly scale the number of and bandwidth of access points, as well as the tools, to meet the demands of the traffic and monitoring/security requirements. Auto–discovery and self-configuration automatically responds to any changes in the mesh, guaranteeing full system redundancy. Connections between NPBs serve as a virtual backplane to incrementally and cost-effectively add or remove ports as required.

Logical Links to Leverage Existing Tools

Placing an underutilized analyzer on each link is cost-prohibitive. Connecting monitoring ports through vMesh allows traffic from local or geographically dispersed network segments to be directed to any analyzer in the network. This capability frees the design of the service assurance or customer experience management solution from the physical constraints of the layer 1 network and avoids unnecessary proliferation of underutilized tools.

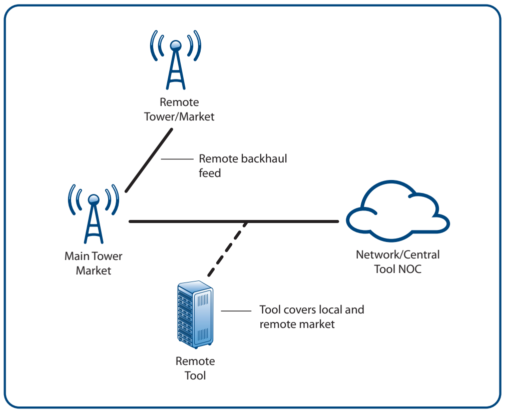
Solving Monitoring Problems with vMesh

The unified visibility fabric and scalability of vMesh solves many of the problems associated with full-coverage monitoring of every link in a network, whether confined to a single data center or distributed globally.

Expand Monitoring Coverage to 100 Percent of the Network

It can be cost-prohibitive to place an expensive analyzer at a branch office to monitor the performance, availability, and health of the remote network. For example, because of the volume of traffic to backhaul, tools in telecom networks are often deployed at each aggregation site. However, it is not cost-effective to deploy tools on secondary spurs or links with few customers.

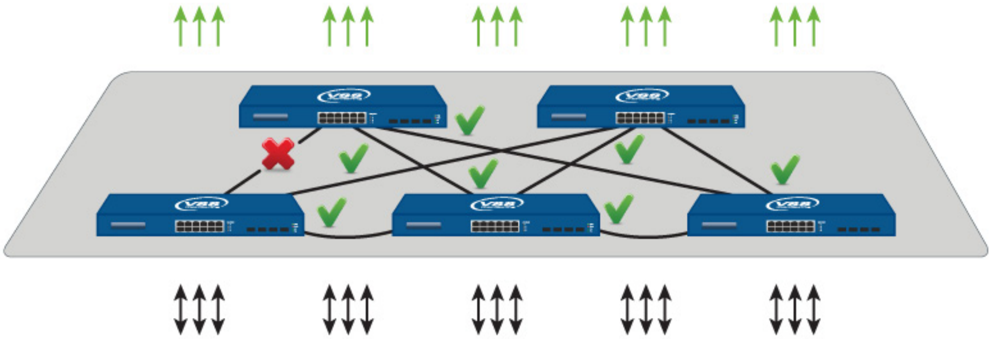
vMesh allows you to place a cost-effective NPB on every network segment and send the captured traffic to any destination on the network, such as an analysis tool centrally located in the network operations center (NOC). Any network segment can be monitored by any tool, regardless of its' respective location, eliminating gaps in coverage.



Eliminate Points of Failure to Avoid Monitoring Traffic Loss

With legacy traffic-capture devices, a failure in the traffic-capture infrastructure means loss of monitoring data, creating gaps in coverage until the failure is corrected. In addition, when an analysis or security tool fails, monitoring or protection is compromised as the system continues to send captured traffic to the non-responsive tool.

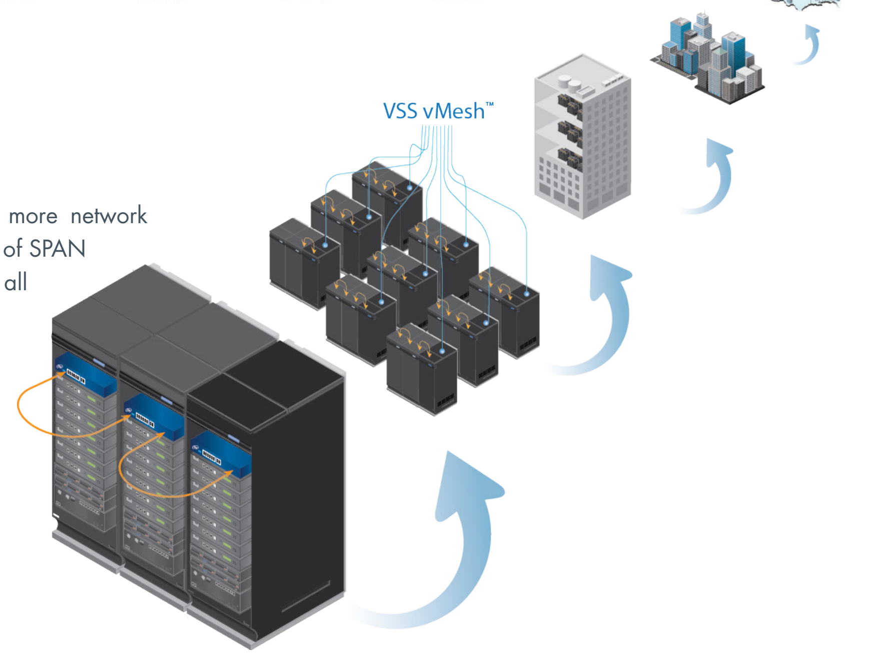
The user-configurable self-healing topology created by vMesh automatically routes around a failure, whether a link failure, a port failure, a tool failure, or even poor tool performance, and sends the traffic to a different NPB or tool, as appropriate.



Scale Up Port-Density in a Location

Maybe you want to add a new tool or to monitor more network segments with an existing tool. You can quickly run out of SPAN ports or TAPs, crippling your ability to monitor or secure all the services in your network.

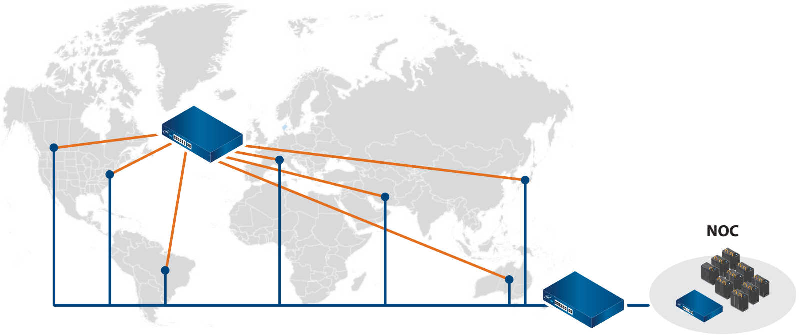
By using the Layer-1 connection to create a virtual backplane between the existing NPBs in that location and a new one, you can incrementally and cost-effectively add more ports at any location, extending your coverage. The 10,000+ port capability of vMesh gives you a lot of headroom.



Monitor Traffic in a Globally Dispersed Network

In a global, or even regional network, placing an analysis tool on each segment is not cost effective. Many choose the fallback position of capturing traffic at aggregation points, which results in gaps in coverage.

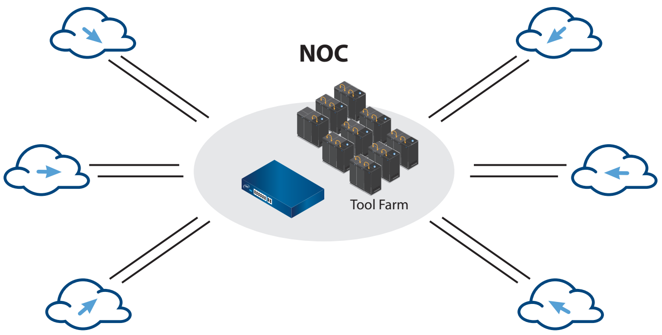
Because VSS Monitoring NPBs can be connected with vMesh, you can put an NPB on each network segment and route the traffic to the analysis tools wherever they may be, regionally distributed, localized, or centralized.



Centralize Analysis Tools in a NOC

A traditional traffic-capture design forces an analysis tool to be placed at each segment to be monitored. Not only is that approach cost-prohibitive for a large network, it makes it impossible to gain visibility into the whole network from regionally distributed or centralized NOCs.

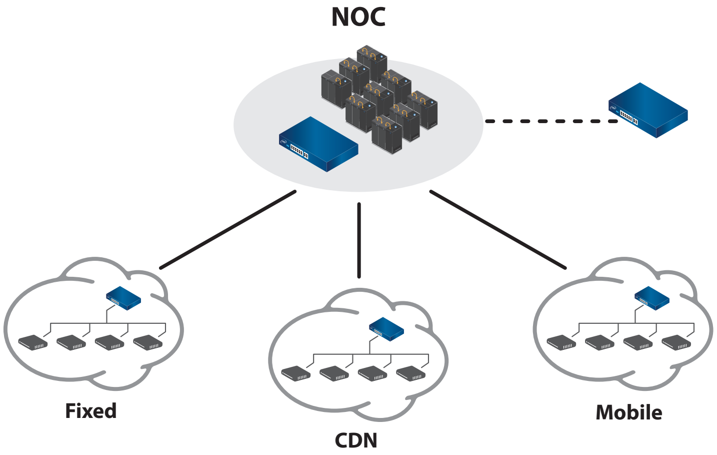
Being able to monitor over 10,000 ports through a single mesh that views up to 256 NPBs as a single system allows you to monitor every network segment, regardless of how remote, from a single operations center, or even remotely if the need arises.



Grow a Monitoring Infrastructure Incrementally

It may be that the budget won't allow 100 percent coverage immediately. Or it may be that you anticipate growth and want your monitoring infrastructure to grow transparently along with your network. You can find yourself painted into a corner when the next model of traffic-capture device isn't compatible with what is already installed.

Because all VSS Monitoring NPBs share the same platform, they can all be connected with vMesh, regardless of model, guaranteeing seamless, transparent growth and the ability to take advantage of new features and innovations without fear of obsolescence.



For more information please contact us at info@vssmonitoring.com

VSS Monitoring is a world leader in network packet brokers (NPB), providing a visionary, unique systems approach to integrating network switching and the broad ecosystem of network analytics, security, and monitoring tools.

www.vssmonitoring.com