



## Ten Reasons You Should Deploy VSS Monitoring Distributed Traffic Capture Systems™ In Your Financial Services Network

---

What is your latency? Average? Peak?

How do you solve hard-to-diagnose network performance issues such as jitter?

How do you ensure consistent performance?

What is your monitoring infrastructure costing you?

Network visibility is critical to heading off the increasing number of application performance issues, outages, and data breaches impacting large-scale networks. It is vital to accommodating growth of users and protocols, and the implementation of Ethernet speeds to 100 Gigabits per second (Gbps) and beyond. It is essential to meeting the demands of government regulation, crucial to achieving the lowest possible latency and vital for maximum efficiency.

Up to now complete visibility of large Ethernet networks has been infeasible due to the prohibitive cost of deploying analytical devices at every point where network traffic needs to be captured.

The solution is distributed traffic capture, which collects a copy of traffic at multiple points and sends it in real time to centralized monitoring tools. VSS Monitoring's Distributed Traffic Capture System comprises intelligent traffic capture devices deployed where needed throughout the network, architected between network infrastructure and the analytical equipment as one virtual traffic capture system. The benefits are proactive control of your network and reduced costs of your monitoring infrastructure.

Total visibility is the only way to meet the performance targets and regulatory initiatives that demand you have proactive control of your network. This paper presents ten reasons why you should consider deploying a VSS Monitoring Distributed Traffic Capture System in your network.

### *1. Total Network Visibility*

Distributed traffic capture means capturing a copy of each packet at every point needed in an enterprise network. It delivers complete, selectable and centralized visibility in real time.

Total real time packet-level visibility is essential to proactive network control and to scalability.

It is the only way to identify every factor potentially affecting latency. It is the only way to achieve the proactive control essential to delivering on performance and throughput targets, and for ensuring compliance with regulatory initiatives.

A Distributed Traffic Capture System:

- Covers every point in a network where traffic needs to be captured.
- Captures traffic inline from network as well as SPAN ports.
- Adapts as rapidly as needed to changing network conditions.
- Delivers multiple secure views of the network simultaneously, so that each monitoring group sees the view appropriate to its function.
- Delivers the data you need to strategically optimize network monitoring for latency, performance, throughput and security.

Essential to a Distributed Traffic Capture System are these capabilities:

- **Selective Aggregation** – Combines the copy of traffic collected from two to many points into one stream, maintaining session and packet order integrity.
- **Filtering** – Removes unwanted traffic by protocol (type of signal, such as HTTP, VoIP, etc.) and address (destination).
- **Packet Slicing** – Allows the inspection of packet header information that may be necessary in identifying hard to solve performance issues. Packet slicing can also be used to remove unneeded information.
- **Load Balancing** – Distributes traffic across multiple monitor ports, fully utilizing their bandwidth. In addition to maintaining packet order, load balancing guarantees a consistent output port for any single conversation. This ensures that a monitor tool will see every packet of a given conversation.
- **Distributed Management** – Allows any one device in a traffic capture system to manage any or all of the other devices.
- **Fault tolerance** – Provides automatic failover should a link or traffic capture device fail, routing the copy of traffic via the highest-speed link with the lowest number of hops.

*Why capture inline:* Many exchanges and trading firms have been reluctant to add devices into the transactions path. Therefore all means to measure the system have been via utilization of SPAN, or mirror, ports from the network switches. SPAN ports may be convenient but they are limited in their ability to provide a true measure of network performance.

## 2. Security and Risk Avoidance

VSS Monitoring traffic capture devices improve the performance of network intrusion detection systems (IDS) at critical entry points by placing the IDS between the entry router and a switch, thus alerting IT personnel to, or preventing, attacks before they reach the switch.

VSS traffic capture devices are invisible to the network as their ports have no IP addresses. They are highly secure with granular permissions for viewing control screens and for making configuration changes.

Regulatory initiatives demand that you have proactive control of your network. Total visibility is the only way to deliver that. You can't monitor what you can't see.

A traffic capture device is inline and passive, allowing traffic to pass in the event of power loss to the device. For copper Gigabit networks, where both sides transmit simultaneously, truly passive monitoring is not possible. If the traffic capture device loses power, it must failover quickly enough to avoid interruption and additional latency of the link being monitored. All VSS Monitoring traffic capture devices have a proprietary technology—vAssure™—which ensures Gigabit copper traffic will failover in less than 150 milliseconds (typically 30 to 60 ms), leaving VoIP and video uninterrupted.

## 3. Traffic Capture at Ultra-Low Latency

VSS Monitoring traffic capture systems process the copy of traffic captured in real time, solely in hardware. They perform all operations the user specifies—such as selective aggregation, filtering, packet slicing and load balancing—and forward the copy at full wire speed, currently up to 10 Gbps per link (80 Gbps in load-balanced deployments).

The traffic capture system operates at ultra-low latency. Assuming a packet length of 60 to 1,514 bytes and a line speed of 1 Gbps, the latency in each device for the copy of traffic from network port (network input) to monitor port (output to the monitoring infrastructure) is 4 to 27 microseconds.

For the original network traffic, the latency from one network port (network input) to another network port (network output) is fixed at 350 nanoseconds. In comparison, a 100-meter Ethernet cable causes 536 nanoseconds delay.

Depending on the model, VSS traffic capture devices can be specified to provide a fixed (deterministic) latency of 350 nanoseconds from network port to monitor port, regardless of line speed or packet size, as opposed to variable latency.

Benefits of low latency traffic capture include:

- Latency identification during the normal operational day.
- Acquire capacity planning utilization information on the network at a very granular level.
- Provide early warning to any incident, thereby reducing recovery time from any failure or slow response period.

#### *4. Performance Optimization*

Latency can occur anywhere.

Multi-point traffic capture coupled with the appropriate analytical tools provide knowledge of where the latency points are so that IT staff can pinpoint improvement areas to optimize network performance. Selectively aggregating and grooming the traffic going to analyzers help ensure that the monitoring infrastructure has real time visibility into performance.

During the normal operational day, high water marks or tolerance-level measures may set triggers to send alerts that network performance may deteriorate, allowing IT to take proactive action beforehand such as identification of bandwidth bottlenecks, distributed-denial-of-service attacks, or workloads not required to consume bandwidth at that time.

#### *5. Network Capacity Planning*

Distributed traffic capture provides a packet-level look at each capture point in the network. This allows for analysis of traffic peaks such as microbursts, or very high bandwidth utilizations over very short time. These can increase latency and jitter but are very difficult to detect.

Jitter, for example, can be detected only at OSI Layer 2, where packets are assembled into frames for a router. Algorithmic trading produces high trade rates, which can create microbursts and in turn be adversely affected by jitter.

Only an inline traffic capture device is capable of identifying jitter. VSS Monitoring's Distributed Traffic Capture System timestamps packets as they enter the traffic capture device. This can help IT staff identify a packet delay due to jitter.

In addition, VSS Monitoring's ConditionalSlice™ technology triggers packet slicing if traffic matches certain user defined conditions such as traffic type. Users can set slice point as well as offset for a true floating slice. Slicing can occur at speeds from 10/100 to 10 Gbps. For example, users may specify that the traffic capture system remove unessential packet information in order to ensure the analyzer(s) are not overloaded by a traffic peak or that user identifiable data is seen by only authorized individuals.

#### *6. Protocol Agnostic*

As long as the application or networking protocol is IP based, VSS Monitoring Distributed Traffic Capture Systems can capture its packets, including, for example, CMS, FIX, InfiniBand, ITCH, and OUCH. The system's sophisticated traffic grooming capabilities allows users to selectively aggregate and filter this traffic depending on the requirements of the implementation of the application such as port number and IP address.

#### *7. Global Management/Global Reach*

VSS Monitoring Distributed Traffic Capture Systems allow for a global deployment across multiple WANS, with the ability to leverage monitoring tools across the enterprise. The traffic capture system can be managed from any location via a Web browser. Unlike any competitive technology, management is fully distributed and highly secure, with the ability for the master administrator to control the entire system via a local or remote connection to any one traffic capture device. In addition, VSS's vStack+™ feature supports a fully redundant mesh topology whereby your analytic, security and diagnostic tools will receive traffic even in event of the failure of one or more traffic capture devices.

#### *8. Global Time Stamping/Distributed Latency Measurement*

A time stamp at point of capture is essential for a true analysis of latency across a global network.

Timestamping is used to count packet order entering and leaving the traffic capture device, and to mark each packet at the capture point with an absolute time ranging from submicroseconds to submilliseconds depending on the distance traveled and the time source.

These measurements help ensure that the traffic copy received by analytical tools is on a uniform calendrical time, which is used to ensure performance.

### 9. Maximized Monitoring ROI with Fewer Network Analyzers

A Distributed Traffic Capture System optimizes the use of monitoring infrastructure.

Key capabilities are selective aggregation, filtering, packet slicing, and load balancing. The first three are used in combination to groom the traffic in real time, ensuring each analyzer sees only the traffic of interest. The fourth ensures the analyzer tool will see every packet of a given conversation.

By sending only the traffic of interest to the analyzers and fully subscribing each one with traffic, the fewest possible number of analyzers can provide complete visibility into the network.

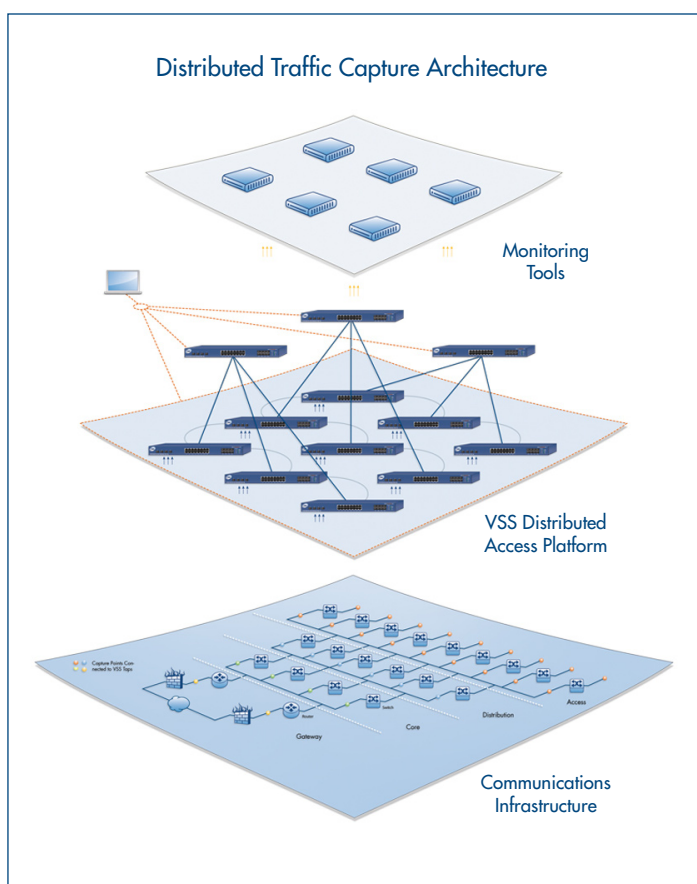
Deploying distributed traffic capture devices reduces the number of analyzers needed and can be far more cost effective, since traffic capture devices are usually much less costly than analyzers. With fewer analyzers, fewer IT personnel may be needed to interpret and act on what they report.

### 10. Total End-to-End Application Performance Knowledge

With distributed traffic capture multi-point devices in place and with the appropriate analytical, diagnostic and security tools, the enterprise has knowledge of end-to-end application performance and latency in real time.

Financial services organizations can strategically evaluate the costs to reduce latency even further while optimizing the ROI of their monitoring tools.

Network traffic-capture devices are deployed as a fully distributed virtual mesh across a network. This eliminates a single point of failure in traffic capture and ensures optimum routing of the traffic captured to a central location for analysis.



Network Visibility. Optimized.

USA  
 (Corporate HQ)  
 + 1 650 697 8770 phone  
 + 1 650 697 8779 fax  
 38 Adrian Court  
 Burlingame, CA 94010  
 USA  
[www.vssmonitoring.com](http://www.vssmonitoring.com)

Japan  
 + 81 422 26-8831 phone  
 + 81 422 26-8832 fax  
 T's Loft 3F, 1-1-9,  
 Nishikubo, Musashino,  
 Tokyo, 180-0013  
 Japan  
[www.vssmonitoring.co.jp](http://www.vssmonitoring.co.jp)

China  
 + 86 10 6563-7771 phone  
 + 86 10 6563-7775 fax  
 C519, 5 Floor,  
 CBD International Tower  
 16 Yong'An Dong Li,  
 Beijing, China 100022  
[www.vssmonitoring.com.cn](http://www.vssmonitoring.com.cn)

VSS Monitoring, Inc. is the world's leading innovator of Distributed Traffic Capture Systems and network taps, focused on meeting the rapidly evolving requirements of security and performance conscious network professionals. Distributed Traffic Capture Systems herald a new architecture of network monitoring, one which fundamentally improves its capability and price-performance.

VSS, Distributed Traffic Capture System, vAssure, LinkSafe, ConditionalSlice, and vStack\* are trademarks or registered trademarks of VSS Monitoring, Inc. in the United States and other countries. Any other trademarks contained herein are the property of their respective owners.