

Ten Questions to Ask Your Traffic Capture Vendor

A Reality Check by VSS Monitoring, Inc.

Take these questions to your next vendor meeting!

January 05, 2010

Know the Details

The key to achieving complete, end-to-end network visibility for centralized monitoring of large networks is understanding the details of how the copy of traffic captured gets to your monitoring tools.

Only a visibility integration system such as VSS Monitoring's Distributed Traffic Capture System™ can provide the connectivity and intelligence to capture traffic at any point and groom it as needed to match your monitoring infrastructure, maximizing its efficiency.

Below is a check-list that provides a guide to the realities of large-scale traffic capture.

Put your vendor to the test. Ask them the following ten questions. See if they are shipping traffic capture solutions that provide complete, end-to-end visibility for centralized monitoring.

How would they score?

Keep this list as a reference to use as you evaluate traffic capture technologies.

QUESTIONS

- Are your Gigabit copper taps failsafe?
- Can users interconnect your taps in any topology, including full mesh? Can they connect them over a WAN? Is the traffic capture system failsafe?
- Do your taps provide session-aware load balancing of monitor port traffic? Is the load balancing automatic? What happens if a link is lost?
- How many 10 Gigabit/second (Gbps) taps do you offer? What is their range of port densities?
- Is there a graphical user interface (GUI) for every operation of the tap?
- Do your traffic capture solutions support inline as well as SPAN port capture?
- Do your taps have time and port stamping at the network ingress, before they groom traffic?
- Do you have local support in my geographic region?
- What high-value traffic capture technology have you invented, and what does it deliver?
- Do your traffic capture products interoperate as one integrated system?

VSS ANSWERS

- Are your Gigabit copper taps failsafe?

The Gigabit (Gbps) Ethernet protocol for copper media specifies that both sides transmit simultaneously. Accordingly, inline taps cannot be fully passive.

VSS Monitoring's vAssure™ reduces the fail-over time to below the threshold for time-sensitive applications, helping ensure that they continue to function uninterrupted. Gigabit taps without vAssure cause a momentary link failure when power is lost or restored.

vAssure's failover time is typically 30-60ms. What is it for your vendor's taps?

- Can users interconnect your taps in any topology, including full mesh? Can they connect them over a WAN? Is the traffic capture system failsafe?

Connected or stacked taps should *not* drop packets or create a single point of failure.

The only ways to prevent these are:

- 1. Fault tolerance via full-mesh capable topology:** If a link is lost, the tap system should provide alternate routing for the copied traffic, including multipath, automatically choosing the highest-speed link(s) with the least number of hops. All vendors except VSS Monitoring limit you to a daisy-chain connectivity or to a hub-and-spoke stacked connection. Each introduces a single or multiple points of failure. This puts your monitoring system at risk if even a single stack link fails.
- 2. Session-aware load balancing:** Automatically load balance across multiple stack ports, using session-aware criteria that match your environment, not just one or two criteria such as IP Source and IP Destination. VSS Monitoring provides nine criteria to ensure even distribution of traffic to the monitor tools. How many does your vendor provide, if they provide load balancing at all?
- 3. Multiple, flexible ports:** Any port can be a stack (inter-tap connectivity) port for maximum bandwidth and redundancy.

VSS Monitoring offers virtual connectivity via vStack+™. vStack+ provides auto-sensing which monitors for link failures and routes around them. Auto-sense is exclusive to VSS.

In addition,

- **Worldwide connectivity:** Links between devices should be capable of running worldwide over a WAN, not restricted to a campus or a wiring closet.
- **Full availability:** Any distributed or intelligent tap in the vendor's product range should be stackable, not just one or two models.

- ☑ *Do your taps provide session-aware load balancing of monitor port traffic? Is the load balancing automatic? What happens if a link is lost?*

VSS load balancing is an automated, session-aware distribution of traffic across monitor ports so that network sessions are not broken up and packet integrity is maintained.

Some vendors use the term “load balancing” when they really mean filtering of traffic. You should know the difference:

- Filtering is a **manual** distribution of traffic, configured by the administrator. It cannot adapt automatically to changing conditions such as a link loss or a traffic burst. Requiring manual configuration, and, if necessary, manual intervention, increases complexity and the likelihood of error.
- Complex filtering can be difficult to implement. An incorrectly configured filter may cause packet loss without warning.
- Filtering does not allow you to choose among a variety of session criteria in order to provide a smooth traffic flow.

Load balancing should be fault tolerant. If a link is lost, the load balancing function should redistribute the packets evenly across the ports without dropping packets and, if the traffic capture devices are configured as a stack, without breaking the stack.

As with stacking, your vendor should offer load balancing on a range of its 1 and 10 Gbps taps, not just on a few devices.

- ☑ *How many 10 Gbps taps do you offer? What is their range of port densities?*

VSS Monitoring currently offers more than 23 10 Gbps taps, more than five times the number of the next largest vendor. Our entire tap product line is almost twice as large as that of the next largest vendor. From simple 10/100 taps with four ports to highly intelligent 10 Gbps Distributed Taps with 30 ports, VSS has a product for every node of an Ethernet network, no matter how small or large and complex. See for yourself: http://www.vssmonitoring.com/products/product_finder.asp

Visibility system: Your vendors’ taps should interoperate to form a visibility system. This is the only way to achieve end-to-end network coverage for centralized monitoring of large networks. Other vendors’ taps have only very limited interconnectivity.

- ☑ *Is there a graphical user interface (GUI) for every operation of the tap?*

Some vendors warn their users that their GUI should not be used for complex operations, such as filters and port connections. Even essential configuration settings such as stacking connections are not available in their GUI.

Forcing users to use a command-line interface for complex operations greatly increases the time needed to configure

and maintain a tap network and introduces risk of packet loss in event of misconfiguration.

- ☑ *Do your traffic capture solutions support inline as well as SPAN port capture?*

Since its inception, VSS Monitoring has offered both inline and SPAN port capture.

Some traffic capture vendors offer only SPAN port capture, requiring third-party taps for inline capture.

You may need to use SPAN ports in part of your network. And SPAN ports can be useful because they are ubiquitous.

But before you commit to a SPAN port capture-only approach, make sure you know the limitations:

- Depending on switch model and configuration, SPAN ports can drop packets at random when the switch is busy.
- SPAN ports can potentially degrade switch performance, and drop under- and oversized packets.
- SPAN ports can mask cyclic redundancy check (CRC) errors, which are useful in identifying packet errors.
- SPAN ports may attempt to correct bad packets or add packets from other than the link(s) being monitored.
- SPAN ports cannot identify jitter, one of the three major factors in latency (along with throughput and consistency). Jitter occurs at OSI Layer 2, as packets are assembled into frames. Only real-time inline traffic capture can help identify the packets where jitter occurs.

- ☑ *Do your taps have time and port stamping at the network ingress, before they groom traffic?*

VSS Time Stamping™ and VSS Port Stamping™ allow latency-sensitive monitoring applications to fully utilize grooming operations such as aggregation, filtering and load balancing without worrying about latency (however minimal) or out-of-order packet receipt. Ultimately this leads to maximized visibility for each tool and fewer analyzer tools required.

No other traffic capture vendor offers ingress time stamping, where the traffic is stamped as it enters the network ports, leaving the network traffic unaffected. Nor does any vendor offer time stamping on 1G as well as 10G ports.

Port stamping allows users to trace traffic on an aggregated stream back to the node on which it was captured, essential for applications such as forensics.

- ☑ *Do you have local support in my geographic region?*

VSS Monitoring has local support via its offices in Asia: Beijing, Singapore and Tokyo; in Europe: London; and in the U.S., plus its network of more than 50 traffic capture / network monitoring solution providers worldwide in the Americas, Asia and Europe.

Does your traffic capture vendor speak your language? The VSS Monitoring Website and key product documents are available in Chinese, English, French, Japanese, Korean, Polish, Russian, and Spanish.

What high-value traffic capture technology have you invented, and what does it deliver?

VSS Monitoring has introduced many breakthroughs in distributed traffic capture. Only VSS traffic capture devices have:

- The fastest link switch-over for copper Gbps links and the only traffic capture devices not to cause link loss: **vAssure**
- Failsafe, virtual traffic-capture connectivity: **vStack+**
- Time and port stamping at the network ingress port: **VSS Packet Optimization™**

Do your traffic capture products interoperate as one integrated system?

Only VSS provides a Distributed Traffic Capture System for complete and flexible visibility integration.

Inline network taps have not had the range of port densities and intelligent traffic grooming operations—such as selective aggregation, traffic filtering, packet slicing, session-aware load balancing and distributed management features—to make them more than a standalone solution. If multiple taps are connected, administrators needed to manage each tap separately, and if one tap failed, the entire traffic capture system could fail.

A Distributed Traffic Capture System comprises intelligent traffic capture devices deployed anywhere they need to be, architected between network infrastructure and the analytical equipment as one virtual system. In this way traffic capture closely meshes with the network's topology and can be reconfigured dynamically, in real time.

Because it functions as one system, distributed traffic capture gives network monitoring, for the first time, fault tolerance, ultra low latency, infinite flexibility and full optimization. A Distributed Traffic Capture System not only adapts as rapidly as conditions require but also delivers multiple views of the network simultaneously, so that each monitoring group can see the view appropriate to its function.

The day of the standalone tap is over.

A Distributed Traffic Capture System is the only way to achieve the power of unrestricted visibility. It is the only solution that gives you the flexibility seeing what you want, wherever you need to see it, in real time, at the packet level.

For more information please contact us at:

phone: + 1 650 697 8770

email: csupport@vssmonitoring.com

www.vssmonitoring.com

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, vStack+, VSS Packet Optimization, VSS Time Stamping and VSS Port Stamping 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.