

Network Visibility and Monitoring in Decentralized Network Environments

Overview

In today's business environment, it is no longer just network administrators who need to monitor and analyze traffic flowing through the company's vast network. Visibility into network traffic is required by an increasing number of departments, including financial, operational, security, and application development. In many cases, whether for legal reasons, logistics, or matters of company policy, it is the responsibility of each department and not that of some centralized IT department to purchase and manage the devices it requires to monitor and analyze network traffic.

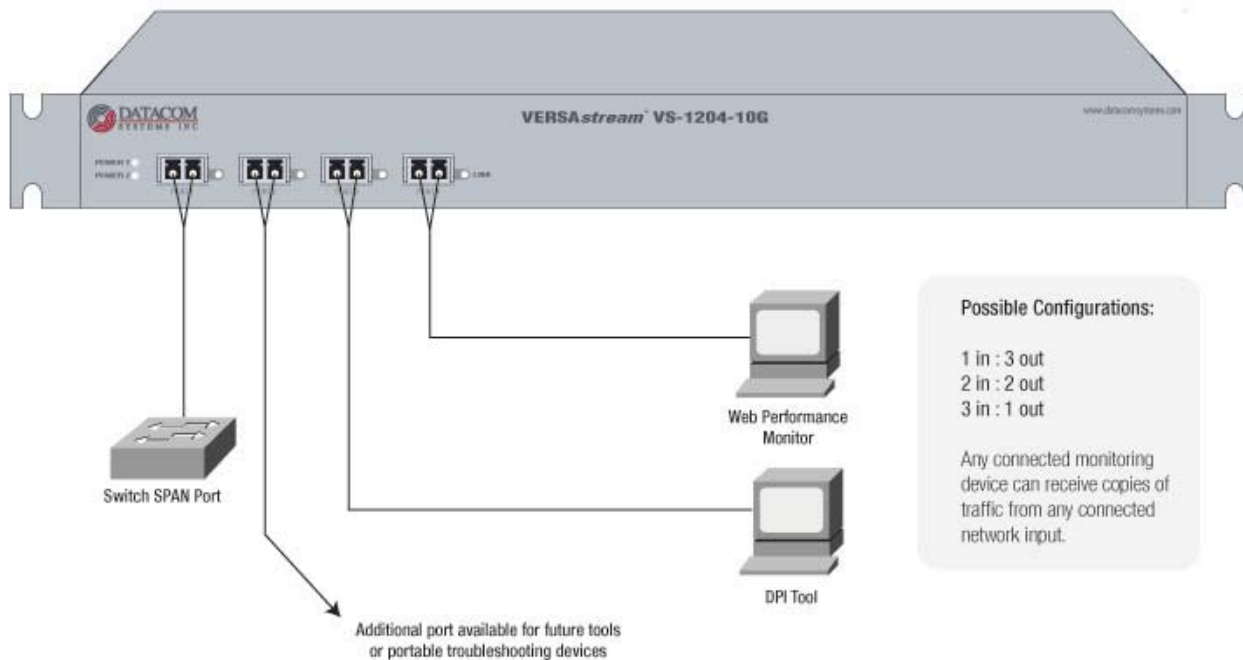
Here are three examples of where organizations with decentralized applications and autonomous personnel required a monitoring access solution to support their operations.

Scenario #1: Fortune 100 Software Company

A computing division in one of the world's largest software companies is required to perform deep packet inspection on network traffic to look for signs of intellectual property leakage in dozens of remote centers worldwide. Due to strict company policy, at each of these remote centers, this department is only allowed access to data through a single SPAN port on an incoming switch. Complicating matters even further, another department is already using the same SPAN port full-time to perform web application analysis.

While this may not be the ideal means of accessing data for this company, the department has no other choice but to comply with company policy. They have requirements that need to be met and an approaching deadline to implement a monitoring solution. Because the department operates autonomously, fulfilling its requirements is the sole responsibility of the department and not a centralized IT department and includes everything from the purchasing decision through day to day management of their tools. Attempting to optimize the entire monitoring access architecture and strategy for one of the world's largest companies to meet the emerging business requirements of a single department is unrealistic. Instead, they need a simple, cost-effective, and flexible solution that will keep up with the speed of business.

The first challenge the department must overcome is that it needs to share a SPAN port with another department. Second, the solution needs to be easy to implement and manage. Third, the solution needs to be flexible and scale to the dozens of global locations where it will be deployed. Finally, the solution needs to make economic sense.

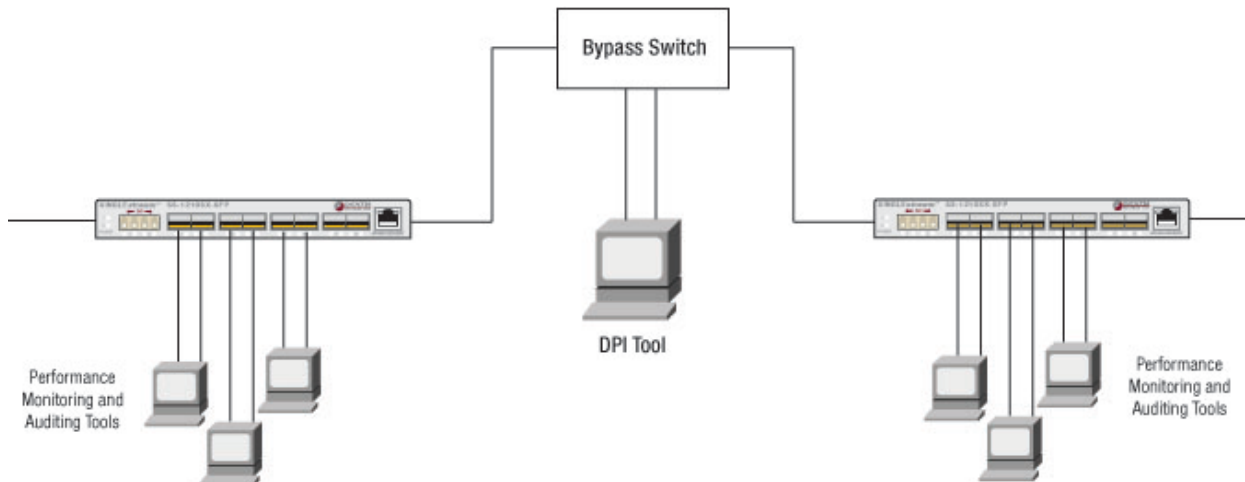
Solution #1 Diagram:


A four-port data access switch installed as a permanent SPAN port regenerator in each location provides a simple plug-and-play solution meeting the company's exact requirements in the most cost-effective manner possible. The data access switch can send multiple exact copies of the SPAN session to all the monitoring tools that are connected to it. In this example, an additional port is also available for a portable network troubleshooting tool, so both the DPI tool and the existing web performance monitor never have to be disconnected.

Scenario #2: Large Government Agency

Members of a security unit for a branch of the United States government perform deep packet inspection in hundreds of remote offices around the country. At each location a DPI tool has been permanently inserted in-line between two critical network endpoints in order to capture all the traffic traveling across the segment. Due to the sensitive and critical nature of the information they are monitoring, the onsite personnel must be sure to collect 100% of all the data that travels through this segment of the network.

In addition, federal guidelines require that onsite personnel monitor the performance of the network and audit the data before and after it is inspected by their DPI tool. Therefore, they need passive monitoring access to the network on each side of the DPI tool to ensure that independent monitoring and auditing tools can receive copies of 100% of the traffic on both sides of the DPI tool.

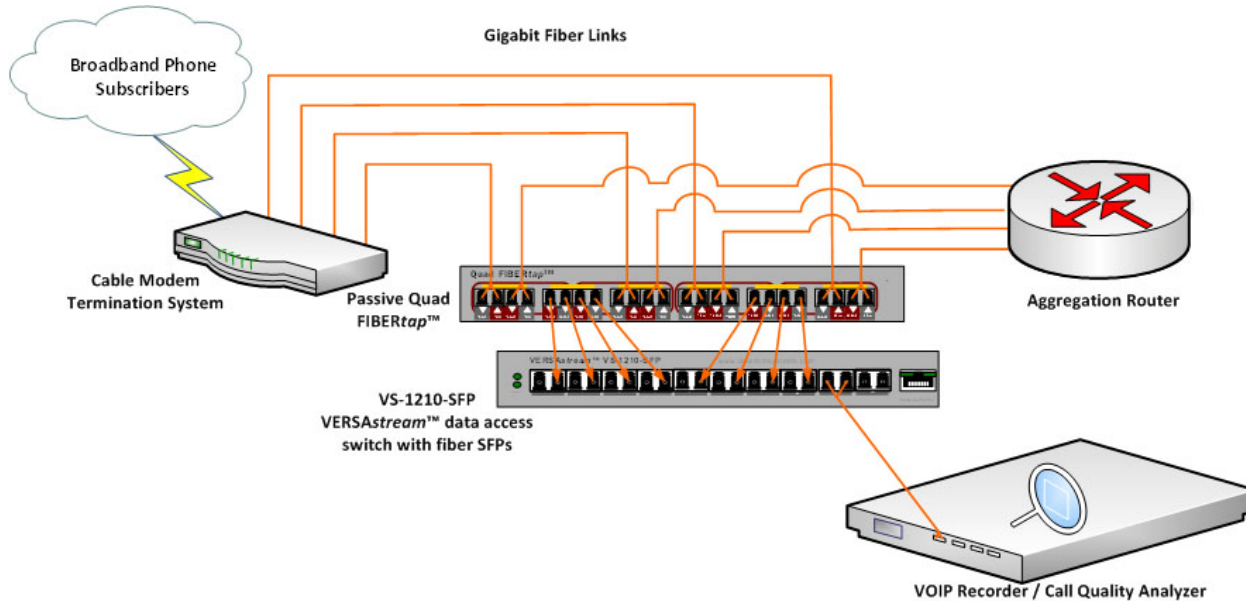
Solution #2 Diagram:


Two fiber regeneration taps are inserted in the link on each side of the DPI tool. Both taps send multiple copies of the traffic to each of their monitoring ports, which will allow onsite personnel to perform the required performance analysis and auditing with a collection of tools. Being fiber, both taps are totally passive and will not affect the network traffic even in the event of power failure. Not only will the DPI tool continue to receive all the traffic it requires without latency or distortion, network taps will also capture 100% of all network traffic at full line rate, so the connected tools will receive 100% of the data without risk of dropped packets. This application provides a cost-effective means for this government agency to meet its requirements and can be easily replicated to each office across the country that needs to perform the same function.

Scenario #3: A Leading Communications Service Provider

A leading media and communications service provider has hundreds of points of presence (POP) offices located in metro areas around the country in order to service local subscribers. In each of these locations incoming Voice over IP (VoIP) traffic from the subscriber base is converted to Ethernet by the cable modem termination system (CMTS) and handed off to the internal network. Network personnel monitor the incoming traffic and perform VoIP analysis to measure performance and ensure call quality. In many cases, these locations only have a handful of links that need to be monitored. However, these locations are spread out across the country, and each location is responsible for its own monitoring and analysis.

Solution #3 Diagram:



A four-channel passive tap is inserted into the network to capture 100% of the incoming VoIP traffic from the four links off the CMTS. Copies of the traffic from each channel is handed off to a data access switch which aggregates all four channels into one output stream of data for the connected VoIP analyzer. This provides an easy, cost-effective method for one VoIP analyzer to monitor multiple incoming links. Based on traffic volume and link utilization, additional analyzers could be added, traffic could be load balanced, or a data access switch with filtering could be installed to eliminate traffic the VoIP analyzer does not need to see.

Conclusion

While new tools are emerging with claims to centralize network monitoring functions, implementing these tools is often complicated, cost-prohibitive, and unrealistic, especially when applications and departments are decentralized. In such cases, simplicity, flexibility, and economics will often drive successful test and monitoring access implementations. Monitoring access solutions should be designed with some key questions in mind:

- Does the solution support the method by which a company or department is allowed to access the data it needs to perform its critical business functions?
- What is the total number of links in each physical location that need to be monitored?
- How many test and monitoring tools need to access each of those links?
- Who is responsible for purchasing, managing, and using each of these tools, and is it reasonable to expect any or all of them to work together?

Answers to these questions will begin to help companies and departments design an expedient and cost-effective network access solution to meet their needs.