

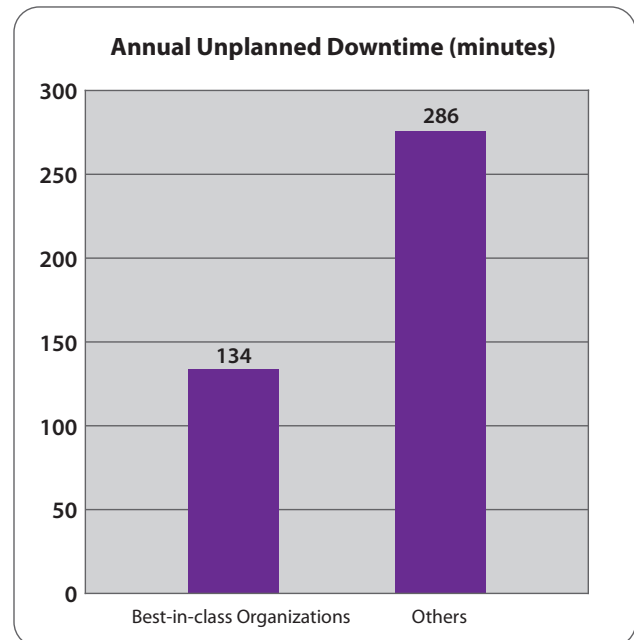
Has Your Network Outgrown SPAN Ports?

Technology Brief



High-performance networks are essential for efficient operations in most organizations today. They carry the data for distributed Enterprise Resource Planning, Customer Relationship Management, and accounting systems to name a few. They transport e-mail, instant messaging, and even telephone traffic between employees in the same building or around the world. They bridge between the organization and its business partners, customers, and investors. And they bring the ubiquitous Internet to desktops and laptops for research, communication, transactions, and entertainment. It is difficult to think of a single business function that does not rely on an organization's network.

With this dependence, it is not surprising that a study by the Aberdeen Group found that in some cases network downtime costs corporations as much as US\$1.5 million per minute. Keeping the network up and functioning at peak performance is now mission-critical. This paper looks at the advantages of a cohesive monitoring plan to successfully manage network operation for continuous uptime, optimal performance, and meeting compliance guidelines. It also addresses why SPAN ports may not satisfy necessary monitoring requirements.



Source: Aberdeen Group

Planning for a Monitoring Solution

An opportunity exists to install best-of-class monitoring appliances and test access ports (Taps) within the network in a way that provides access to important data, delivers 100 percent of the data that needs to be captured, and does not interfere with everyday operations. The solution also provides the ability to correlate traffic from multiple links and enable administrators to

- Maximize network performance and detect anomalies quickly to prevent outages
- Defend against security threats
- Enforce compliance policies

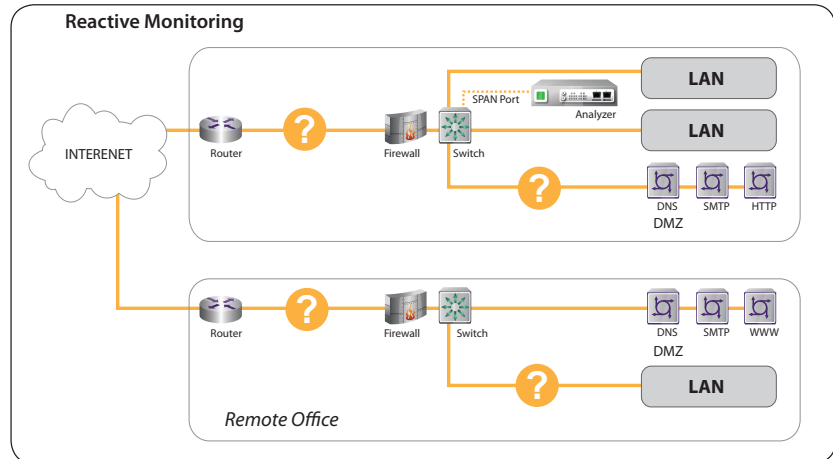
Has Your Network Outgrown SPAN Ports?

Technology Brief

Avoiding Past Pitfalls

Monitoring has traditionally been done using access methods that worked fine in the less demanding environments of the past. However, these techniques have drawbacks that limit their usefulness in today's network environments. An overview of 3 methods used in the past and what to avoid follow:

1. SPAN or Mirror ports
2. In-line deployment of tools
3. Hubs



1. SPAN/Mirror ports - Connecting a monitoring tool to a SPAN Port off of a networking switch is a useful approach, but can be misleading, because the tool may not see what you think you ultimately need. Yes, SPAN ports are flexible and nearly free (if you have a spare port on your switch), but be aware of these SPAN port limitations:

- SPAN ports drop packets if they are oversubscribed or when the switch gets busy.
- SPAN ports do not pass packets that are undersize, oversize, or contain CRC errors, and such packets may be involved in the problem you are investigating.
- Configuring a SPAN port changes the behavior of the switch, which again may change the nature of the problem.

2. In-line Tools - Most tools do not support an in-line configuration, however if you can find one that works, direct in-line placement does provide complete access to all of the link traffic. Considerations that warrant thought include; in-line tool deployments may introduce latency and can be a reliability risk, because the link will go down if the tool loses power or experiences a software crash. In-line deployment also limits the tool's flexibility to be used elsewhere. And, once in-line, it may not be easy to quickly take down links to remove and insert elsewhere for trouble-shooting purposes.

Placing multiple tools in-line that serve different purposes can also increase latency issues, cause cabling mishaps and limit the tools usefulness.

3. Hubs - Inserting a hub into the link you want to monitor is a quick-and-dirty solution for 10/100 networks. As they are often inserted and removed from the network after their use, it may cause two network outages each time a problem on the link is investigated. Also, most hubs do not support today's Gigabit and 10 Gigabit network speeds, and models that support legacy network speeds are rapidly disappearing from the market.

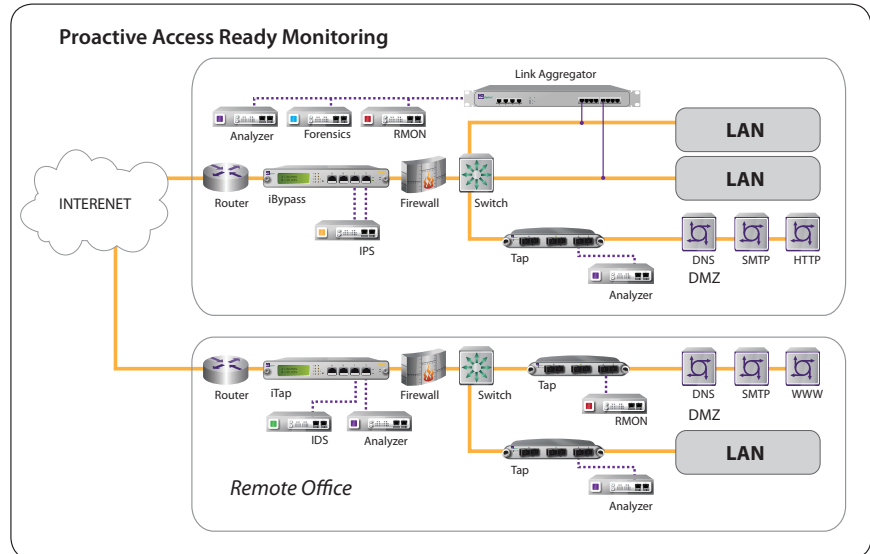
These and other issues that limit the usefulness of SPAN ports in a modern monitoring solution are discussed in the next section.

Has Your Network Outgrown SPAN Ports?

Technology Brief

Tap Into Accessibility

To eliminate the shortcomings previously described regarding SPAN ports, the use of network Taps provide a new level of access and flexibility. A Tap is a fully passive device that is placed within a network link between two network devices, for example a switch and router. It replicates a copy of the traffic to a monitoring tool such as a protocol analyzer without affecting the network traffic in any way. The monitoring tool sees a true copy of 100 percent of the traffic, with no dropped frames no matter how fast or highly utilized the link is. There is no possibility for missed packets of importance, such as the microburst traffic generated by financial institutions' market data and trading systems.



Important Tap characteristics include:

- Traffic timing is preserved, so the monitoring tool can accurately measure interframe gaps of time-sensitive traffic like VoIP and streaming video.
- Taps are fault-tolerant: they do not affect link traffic even in the absence of power. In fact, optical Taps do not require power at all, saving energy and outlet space.
- Taps are secure because they have no IP addresses.

Another important advantage of Taps is that they require minimal configuration. For example a security administrator who requires access to a specific link does not need the administrator responsible for the switch to reconfigure anything. Reconfiguration issues are not a determining factor and time to resolution is optimized.

Other features that enhance the overall Tap-based solution include:

- Regeneration Taps - create identical copies of the link traffic to multiple ports, eliminating contention between different groups that need access simultaneously.
- Aggregator Taps - combine traffic from multiple links, and from both directions on full-duplex links, so a monitoring tool can see more traffic through a single network interface card (NIC).
- A new generation of Taps that provide RMON statistics and filtering functions, creating a richer automated and manageable environment.

Has Your Network Outgrown SPAN Ports?

Technology Brief

Build The Access Ready Network

Taps and SPAN ports may both have a place in a complete enterprise monitoring infrastructure, because of the range of monitoring requirements and different costs and benefits. Best-in-class organizations are building in monitoring access as a fundamental building block of the network architecture, anticipating monitoring needs before issues arise. The ability to integrate distributed monitoring tools to collect and correlate input from multiple probes and Taps strategically placed throughout the network, gives them an on-going, proactive monitoring capability across the entire network.

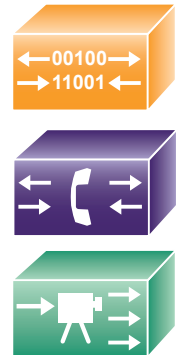


The combination of monitoring tools with access devices that are built into the network infrastructure can be thought of as a Monitoring Access Platform or MAP. Organizations ensure that their MAP supports current and anticipated monitoring needs, because they know that ad hoc solutions implemented on an as-needed basis are more costly and less efficient than building in a solid platform up front.

Bottom Line Value

Given the value of high-performance networking in today's organizations, keeping the network up, responsive, and secure is mission critical. This objective is achieved with a monitoring plan that gives administrators the ability to proactively respond to anomalies, secure the network, enforce compliance rules, and plan for growth. A Monitoring Access Platform that is integrated within the network infrastructure makes use of all forms of passive Taps and filtering capabilities to give enterprise-class monitoring tools visibility across the entire network.

Where SPAN ports come up short in today's converged data, voice, and video networks due to dropped packets, loss of timing information, and configuration complication, Taps provide the highest level of visibility and the fewest deployment issues, enabling monitoring tools to leverage their full capabilities. With complete monitoring access across the enterprise, administrators have the help they need to make the network an asset that continuously adds value to the organization's bottom line.



Contact Net Optics for a white paper that explains how a Monitoring Access Platform increases network administrator efficiency and leverages investments in expensive network monitoring tools.

For further information on Tap technology:

<http://www.netoptics.com>
Net Optics, Inc.
5303 Betsy Ross Drive
Santa Clara, CA 95054
(408) 737-7777
info@netoptics.com

Customer First!