VIAVI Solutions

White Paper

Optical TAPs for the Enterprise

Abstract

In an age when television commercials show everyday people effortlessly accessing their bank account's information from a street corner by way of a cellphone, it is ironic that accessing data flowing within its physical source—the network—is, without advanced preparation, nearly impossible.

The truth is that, for many IT organizations, the network itself has become an impenetrable black box. This is particularly true for Storage Area Networks (SANs). While the new technology has yielded the desired result—increased speed—it has made access to the data flowing through connections within the network more difficult. Unlike peer-to-peer networks with centralized data flows, where access is a simple matter of acquiring data as a peer node, switched networks have a decentralized structure with no ready access points. When network problems or slowdowns occur, or when monitoring becomes desirable, administrators often do not have the necessary access to network data flows to diagnose their problems or to monitor.

This paper discusses one of the simplest, most effective, and most cost-efficient ways to gain access to the data within switched networks—the Traffic Access Port (TAP).

What is a TAP?

As the name implies, a Traffic Analysis Point or Traffic Access Port (TAP) is a hardware device that provides access to traffic flowing on a physical connection (link) between two or more points within a network. The TAP normally resides in the link between the network devices, termed "inline". In other words, a single physical link connection between two points is replaced with two; the first from point A to the TAP, and the second from the TAP to point B. The TAP provides an output which copies or mirrors the data flowing between the two network points. (See Figure 1)

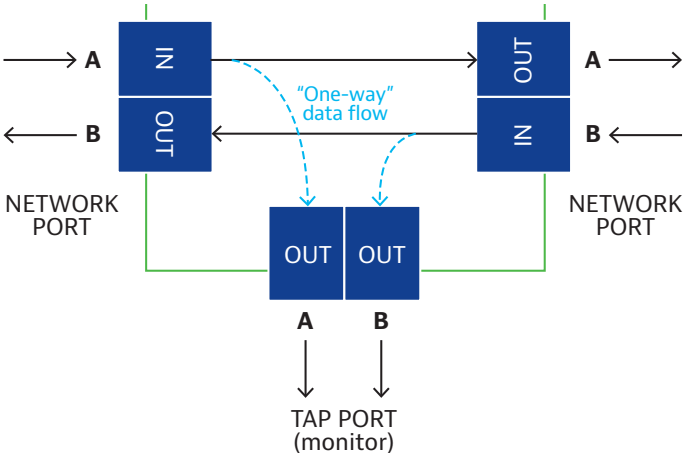

Figure 1: General TAP Functional Diagram

Three important characteristics of TAPs are:

1. The TAP provides one or more outputs that mirror the data passing through the device.
2. The monitoring outputs do not have the ability to modify or degrade the signal passing through the device.
3. A TAP continues to pass data on its Network Ports without disruption, requires no power, and has no electrical components.

Taken as a whole, these characteristics demonstrate that TAP designers know what is important to those who deploy or maintain networks. When correctly installed, TAPs provide access to data flowing across a network. They do not create a location to modify or corrupt data, and they do not represent a prospective point of failure.

Why Instrument your Network?

"Instrumenting" a network entails installing TAPs on the links between two points in the network. Perhaps the most compelling reason for installing TAPs is that installation allows network maintenance activities requiring network data visibility without disturbing or stopping (bringing "down") the network. With the cost of network downtime for some business critical networks exceeding $6.45 million dollars per hour[1], the ability to troubleshoot the network without bringing it down pays for the installed TAPs in literally less than a second, given the insignificant cost of the devices—typically less than 1% of the cost of the network. Even on networks without such a high a cost of downtime, a simple cost analysis shows that installing TAPs can save considerable time and money. Another compelling but less well known reason is that often bringing down the network to install analysis or monitoring equipment to resolve a problem can hide or mask the issue. When the link is reestablished the communications are reset as well. This can temporarily resolve the issue until the conditions that caused the problem in the first place reoccur and the problem once again appears. Without TAPs in place administrators and field support personal often have to chase a problem around the network and try and trigger it to occur. With TAPs in place instrumentation can be put in place while the problem is still present on the network allowing for much quicker diagnoses.

Figure 2: Enterprise High Density TAP allowing 16 TAP ports in 1RU

With so many network administration activities requiring TAPs (see TAP Uses below) a more appropriate question than "why instrument your network" is "why not instrument your network?" Most often the reason IT organizations do not instrument their networks seem to be that there are other priorities when deploying the network. During deployment the primary focus in most corporate environments is keeping on schedule, with controlling costs a close second. This is an understandable position as, during the installation, the IT department is most likely inundated with the inevitable questions, "When is it going to be done?" by users, and "How much is it going to cost?" by management. Often during deployment little thought is given to future questions such as "Why is the network so slow?" or, "Why can't I access the database?" However, if organizations give consideration to the network's diagnostic layer and include TAPs in their network deployment plan, their installation requires little technical effort or cost and no network downtime later on.

1 Source: "Developing Return on Investment and Business Case Support for Storage Area Networks", David R. Merrill, Hitachi Data Systems, July 2001; RBC Capital Markets

Even though many organizations understand the value of TAPs, they often balk at the added cost, however small. This approach is similar to choosing not to install smoke detectors in your home. Not installing smoke detectors saves the insignificant cost of the smoke detector, but if a fire breaks out the detector provides advanced warning of a potentially fatal event. (For this reason most states mandate smoke detectors in houses.) With networks, TAPs are a very small incremental cost when compared to the cost of HBAs, switches, and storage. While they may sometimes sit idle, TAPs pay for themselves many times over in saved time and effort the first time network problems occur.

TAP Uses

While users have come to expect some network slowdowns, how can you know what typical behavior is, and when it is time to upgrade the network for more capacity? And, if network speed suddenly grinds to a halt, how can you determine the cause? With today's increased security concerns, how can you know if your organization is under attack or rogue applications are generating unnecessary storage traffic or worse manipulating the data itself? These activities point to the real need for ongoing network monitoring and troubleshooting.

TAPs form the cornerstone of knowing what's going on within a network. Installing TAPs during network installation, prior to operation, sets the stage for gathering network intelligence later on. An instrumented network provides ready non-disruptive access to the data flows within for primary IT activities: Monitoring and Analysis.

Monitoring

Network monitoring assists those using the network much the same way that traffic helicopters assist commuters. Monitoring answers such questions as: where are the network traffic jams or accidents and who is creating the traffic? This data, when accumulated and plotted over time, provides insight for activities such as capacity planning. Like roadway planning, capacity planning in a network is helped by knowing when, where, and how much traffic flows about the network. TAPs provide the necessary access points for network monitoring equipment to accumulate data flow statistics.

When a network device begins to fail, data corruption often heralds the device's decline. Unfortunately, network protocols can mask these problems by automatically retrying erred transactions, and as a result, the corruption occurs "silently". Monitoring can detect network errors and warn administrators that future danger may be lurking. Again TAPs provide not only the necessary access points for monitoring equipment, but also a view important for device failure detection not available from other network components: Link Layer access. Network equipment strips away Link Layer information, which often contains error information. Inline TAPs present all the information flowing between network components, from the Physical to the Application Layer.

Analysis

When networks have problems, affected organizations want to troubleshoot the network to get it running again to its full capacity. Troubleshooting begins by identifying the affected subsystem, and then usually proceeds to connecting an analyzer into the data path between suspect network devices to collect copies of the conversations going on between the equipment. These conversations, or traces, allow technicians (or expert software) to analyze the commands flowing between the equipment. Analysis usually provides the answer to the network's problems, or at least a clue, allowing a quick diagnosis and a start to remedying the network's problem.

With TAPs installed in a network, analysis is a simple activity. With no change to the network, analyzers can be connected inline into any link with a TAP. If one location does not provide answers, the analyzer can be quickly moved to any other TAP without interrupting network traffic flow.

To perform analysis without TAPs usually involves breaking the links between network equipment. This not only stops data flows between the affected devices, but in many situations (such as within SANs) stops data flows between all devices on the network as the network tries to reconfigure itself to compensate for the disconnected link. This leads to poor performance or downtime, or both. Since downtime is so expensive in terms of both lost productivity and data access, organizations usually do not allow breaking links or taking down the network to install analyzers.

They usually limp along with a problem until a maintenance cycle, and then try to install an analyzer at that time to solve the problem. However, waiting has associated costs too, as decreased performance keeps the network from performing to its full potential.

Often the outage required to install an analyzer when no TAP is in place causes the systems to reestablish their communication, which temporarily resolves the problem or moves it to another link. This can be one of the biggest challenges to diagnosing a problem with an analyzer. Not only do you have to wait for down time to put the analyzer in place, often you must introduce errors on the network by resetting equipment or altering configurations to try in recreate the problem once the analyzer is in place. With a TAP in place, the analyzer can be added to the link while the problem condition is still occurring, thereby eliminating the need to chase or recreate a problem.

Passive Optical TAPs

Passive optical TAPs provide a simple and powerful way to monitor optical networks. As the name implies, passive optical TAPs require no power. (Figure 3) Light signals passing through them are unaffected regardless of what happens to the power for the rest of the data center.

The signal carrier for optical networks—light—has signal properties different from electricity, the carrier for copper networks. Perhaps most importantly, light travels in only one direction. This property enables passive optical TAPs to monitor by "splitting" the input signal's light energy. Splitting the light in the TAP provides a monitoring point without the possibility that the original signal might be corrupted. Light introduced into the monitoring point has no effect on the input signal, as it would travel in the wrong direction.

Best Practices

The most effective time to install TAPs is when the network itself is built. This is the method preferred by large industry-leading customers, particularly in industries where timely information is critical to business. For example, in the Financial Services sector, large organizations commonly add TAPs to all critical ports in order to ensure maximum SAN uptime.

However, this is not always an option, particularly for those who inherit existing networks. In this case, the ideal time to install is during scheduled downtime or when equipment is being changed out for some other purpose, whether replacement or consolidation. It is not necessary to install TAPs at all desired points in order to experience the benefits of an instrumented network. TAPs can be installed piecemeal as different parts of the network are brought down for maintenance. After installation, that section of the network can then be "tapped" at any time.

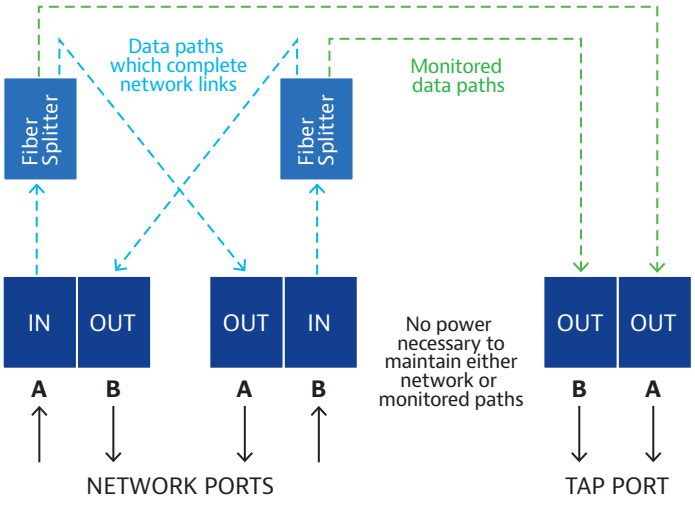

Figure 3: Passive Optical TAP

Summary

- TAPs are a simple, effective, and cost-efficient way to gain access to the data within switched networks
- TAPs allow access to network traffic in real-time for troubleshooting, analysis, or monitoring without affecting network operation
- Installing TAPs during deployment of a SAN allows for future troubleshooting without bringing down the network or breaking links.
- Implementing a network Diagnostic Layer can be the difference between weeks of frustration and potential downtime or proactive problem resolution before an event can grow into a critical situation.

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

opticaltaps-wp-san-tm-ae
30162825 500 1009