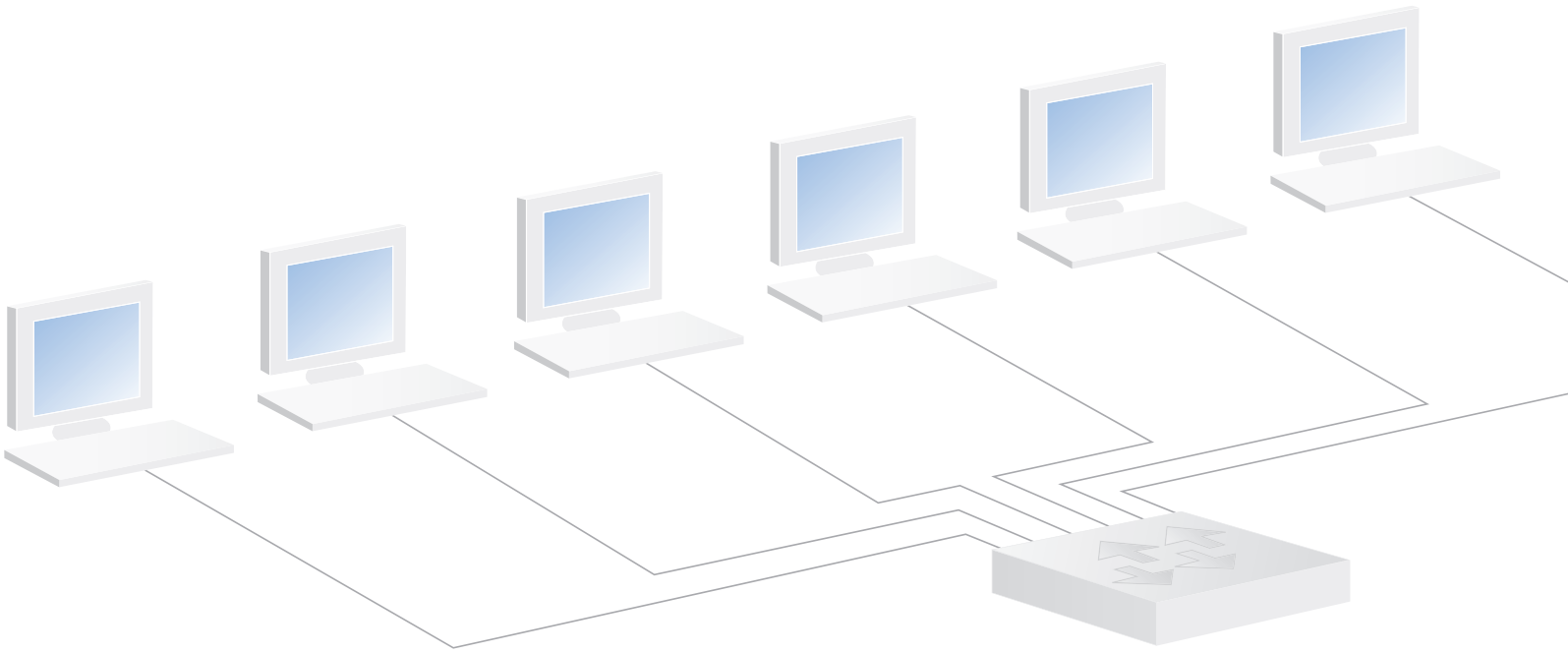
Analyzing Full-Duplex Networks

There are a number ways to access full-duplex traffic on a network for analysis: SPAN or mirror ports, aggregation TAPs (Test Access Ports), or full-duplex TAPs are the three most common. This paper discusses the issues involved in deciding which type of technology to deploy. In short, your answer will depend on the rate of traffic being monitored, and the level of visibility you require.



NETWORK® INSTRUMENTS

Overview

This paper describes the advantages and disadvantages of three common methods of accessing traffic from full-duplex networks for purposes of analysis, monitoring, or forensics:

- Attaching a monitoring or analysis device to a switch's analyzer port (in Cisco terminology, a Switch Port ANalyzer, or SPAN) to monitor a full-duplex link. Because this setup uses standard full-duplex connectors (one channel transmits, the other receives) on both the switch and the analysis device, it creates a potential bottleneck when trying to mirror both sides of a full-duplex link to the analyzer's single receive channel.
- Attaching a monitoring or analysis device to an aggregation TAP inserted into a full-duplex link. As with a SPAN, the aggretator TAP copies both sides of a full-duplex link to the analyzer's single receive channel. Its use of buffering makes it somewhat better able to keep up with high traffic levels than a SPAN.
- Attaching a dual-recieve monitoring or analysis device to a full-duplex TAP inserted into a full-duplex link. Dual-receive means that the network card on the analysis device has two receive channels rather than the transmit and receive channels associated with a standard full-duplex link.

Each approach has advantages and disadvantages. SPANs and aggregation TAPs allow the use a of standard (and usually less expensive) network card on the analysis device, but their limitations make them less than ideal for situations where it is necessary to guarantee the visibility of every packet on the wire.

A full-duplex TAP is the ideal solution for monitoring full-duplex networks utilized at more than 50 percent, but their design requires that the analyzer be a specialized device with a dual-receive capture interface that is capable of capturing the TAP's output and recombining the data for analysis.

Introduction

Whether you are monitoring a network for security threats or capturing and decoding packets while troubleshooting, you need a reliable way to see the network traffic. Traffic levels on the given segment, coupled with how much visibility you require will suggest the most economical solution. There are three common ways for an analysis device to capture traffic from a network:

SPAN

The advantage to the SPAN port solution is its cost, as this feature is included for free with virtually every managed switch on the market. A SPAN is also remotely configurable, allowing you to change which ports are mirrored from any system connected to the switch.

The limitation with a SPAN or port mirror stems from the aggregation that must take place to merge full-duplex network traffic in to a single receive channel on the analyzer. Therefore when traffic levels on the network exceed the output capability of the SPAN, the switch is forced to drop packets. Another reason that a port mirror may not be the right choice is because Layer 1 and 2 errors are not mirrored, and therefore never reach the analyzer. When troubleshooting, seeing these errors can be important.

Aggregation TAP

An aggregation TAP makes a good compromise between the SPAN and full-duplex TAP options. It costs more than a full-duplex TAP due to the added complexity and memory requirements of its built-in buffer. But it does not require a specialized (and potentially more expensive) dual-receive capture interface on the analysis device. Like a full-duplex TAP, it is independent of the network, making it invulnerable to security threats.

An aggregation TAP includes an internal memory buffer to mitigate the bandwidth problem associated with converging both sides of the full-duplex traffic from the network into one side of the full-duplex link to the analyzer. The buffer is able to cache some spikes in network utilization, but it drops packets when the bursts of activity exceed buffer capacity.

Although some aggregation TAPs pass along layer 1 and 2 errors, all aggregation TAPs can drop packets under heavy network utilization.

Full-duplex TAP

A full-duplex TAP is the only method of the three alternatives that will guarantee that all of the network traffic, including layer 1 and 2 error information, makes it to the analysis device. It is more complex and potentially expensive to implement, but where there is high network utilization and it is important to guarantee the capture "everything on the wire" along with errors from all network layers, a full-duplex TAP is the only choice.

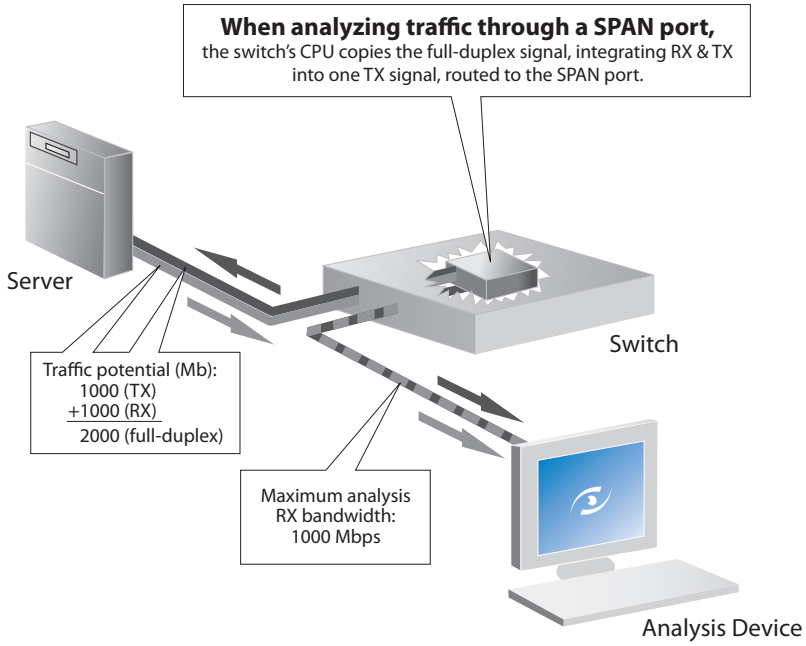
Using a SPAN or Port Mirror

When monitoring a full-duplex link through a SPAN or mirror port on a switch, the switch does three things:

1. Copies both the send and receive data channels
2. Reconstructs an integrated data stream from the two channels
3. Routes the integrated signal to the send channel of the SPAN or mirror port

Each of these activities burdens the switch's internal processor. These demands on the switch's CPU have implications for both your monitoring equipment and general network performance. Using a SPAN or port mirror to capture network traffic for analysis presents the following risks:

- As total bandwidth usage for both channels exceeds the capacity of the outbound (analyzer) link, the excess traffic is dropped from the outbound stream. There simply is not enough bandwidth to transmit both sides of the full-duplex traffic across a single standard interface.
- The switch's CPU must act as both a network switch and a packet-copier. The switch's CPU must also integrate the two data streams (send and receive) together correctly. Both packet copy/re-direction and channel integration is affected by switch load. This means the SPAN or mirror port may not deliver accurate captures when the switch is under heavy load. Monitoring a 10/100 network through a gigabit SPAN or mirror port and analyzer does not alleviate these concerns. Also, there is no notification when the SPAN or mirror port is dropping packets or delivering inaccurate time stamps.



A SPAN or mirror port can deliver satisfactory results when used to monitor lightly used, non-critical networks. If network utilization exceeds the capacity of the outbound (analyzer) link, packet loss results—which invalidates many types of analysis, and makes monitoring for certain kinds of network activity impossible. For example, you might miss a virus signature because packets are being dropped. When analyzing a transaction or connection problem, the analyzer may detect problems where none exist because expected packets are being dropped by the SPAN. Hardware and media errors will also be impossible to troubleshoot through a SPAN, as layer 2 errors are not mirrored.

Using an Aggregation TAP

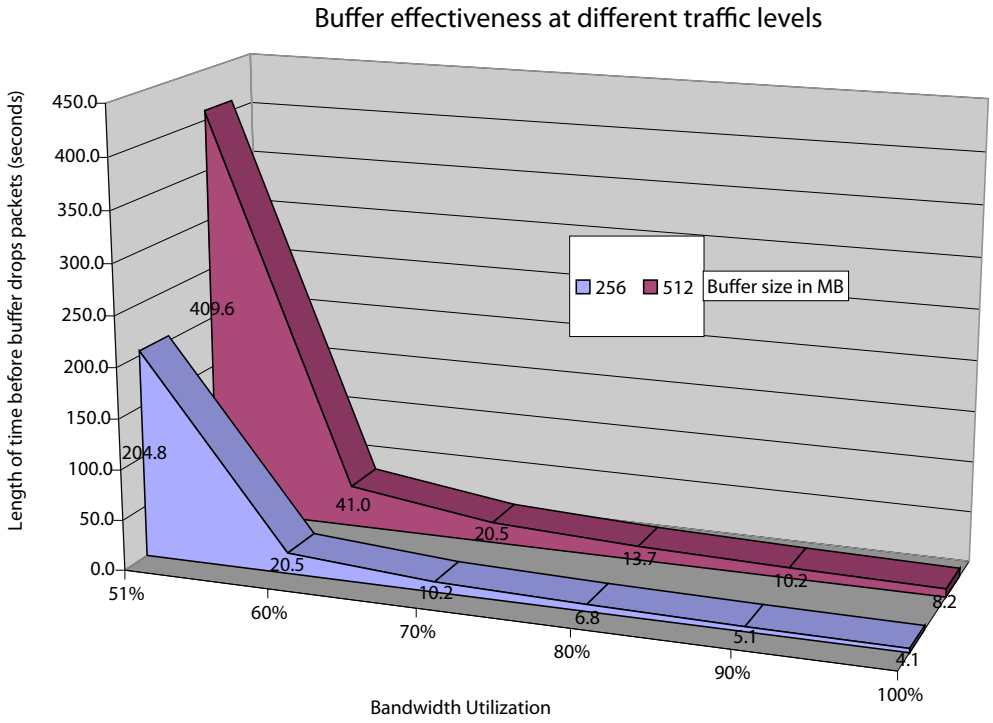
An aggregation TAP is much like a small switch dedicated to mirroring a link for analysis. Its advantage over a SPAN is that the aggregation TAP buffers the analyzer output, which makes it less likely than a SPAN to drop packets during short spikes of high usage. Under sustained high utilization (over 50%), an aggregation TAP will drop packets. An aggregation TAP is not an addressable device, and therefore not vulnerable to security threats.

An aggregation TAP is ideally suited to work with an analysis device with a standard (single-receive) capture interface. This means that a laptop or a standard system can be deployed as an analysis device, rather than the more expensive specialized analyzers or appliances that are designed to accept full duplex traffic via a dual-receive capture interface.

Just like a SPAN, an aggregation TAP is ideal for a lightly used network that occasionally has utilization peaks above the capture capacity of the analyzer. Unlike a SPAN, the aggregation TAP will forward layer 1 and 2 errors to the analysis device.

Another advantage the aggregation TAP has over a SPAN or port mirror session is its internal memory buffer, most commonly 256 or 512MB. The memory buffer provides limited protection against packet loss, and if the network utilization does not regularly exceed the capacity of the analyzer's capture card, an aggregation TAP may be the right choice.

It is important to understand that once the buffer is full, an aggregation TAP will drop packets. The graph below is meant to give some idea how long a spike in utilization can be absorbed before packets are dropped.

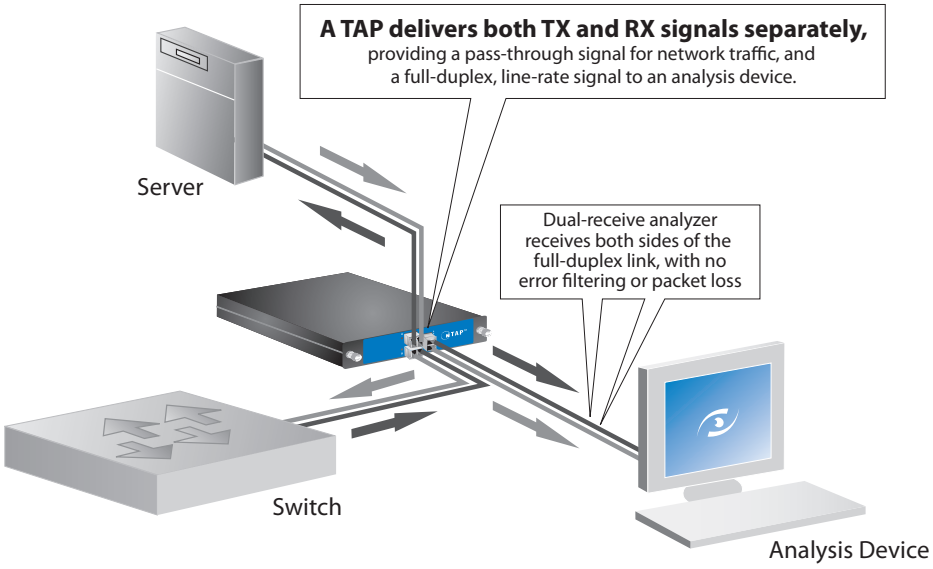


Please note: The role of the buffer is to absorb traffic spikes of over 50% full-duplex bandwidth saturation, because the analyzer's single-receive interface simply cannot move the bits fast enough to keep up at line rate. The data in the buffer is released when utilization drops to the point where the analysis interface can move both the "live" data plus the data released from the buffer. Packet loss is unavoidable if the utilization spikes exceed the capacity of the buffer.

Using a Full-duplex TAP

A full-duplex TAP is a passive mechanism that is installed between two full-duplex network devices. TAPs are available for monitoring optical or copper at different speeds (10/100/1000 for copper and up to 10Gb for optical). An optical TAP is non-electronic (no power) and optically splits the full-duplex signal into two full-duplex signals. One signal maintains the network link, while the other is passed to the analysis or monitoring appliance equipped with a dual-receive capture card. A copper TAP performs the same function, but uses electronic circuitry to duplicate the signals. Because a full-duplex TAP copies both the send and receive channels from a full-duplex link to the analyzer (where the data is integrated), the analyzer can monitor a full-duplex network at line rate, assuming the capture card in the analyzer is capable of keeping up.

A full-duplex TAP must be coupled with a probe or monitoring device capable of receiving both channels of a full-duplex signal and recombining the two channels back into a full-duplex data stream. Although this can be the most expensive solution, it is also the only solution that guarantees complete accuracy even when the network is 100 percent saturated.



Conclusion

The appropriate solution for capturing full-duplex data for analysis depends on the rates of traffic you must monitor, and what level of visiblity you require. When monitoring a lightly-used network, using a SPAN or aggregation TAP to supply an analysis device with a standard full-duplex (i.e., single-receive) interface can be an economical choice. The aggregation TAP can provide some protection against packet loss, but if usage spikes exceed its buffer capacity, the aggregation TAP will drop packets.

To monitor a critical, heavily utilized full-duplex link, a full-duplex TAP is the only fail-safe alternative. Monitoring a full-duplex connection using a full-duplex TAP and an analyzer with a dual-receive capture interface guarantees complete, full-duplex capture for monitoring, analysis, and intrusion detection regardless of bandwidth saturation.

About Network Instruments

Network Instruments provides in-depth network intelligence and continuous network availability through innovative analysis solutions. Enterprise network professionals depend on Network Instruments' Observer product line for unparalleled network visibility to efficiently solve network problems and manage deployments. By combining a powerful management console with high-performance analysis appliances, Observer simplifies problem resolution and optimizes network and application performance. The company continues to lead the industry in ROI with its advanced Distributed Network Analysis (NI-DNA™) architecture, which successfully integrates comprehensive analysis functionality across heterogeneous networks through a single monitoring interface. Network Instruments is headquartered in Minneapolis with sales offices worldwide and distributors in over 50 countries. For more information about the company, products, technology, NI-DNA, becoming a partner, and NI University please visit www.networkinstruments.com.

Solution Bundles

Contact a Network Instruments representative or dealer to ask about product bundles that cover all of your network management needs.

Corporate Headquarters
Network Instruments, LLC • 10701 Red Circle Drive • Minnetonka, MN 55343 • USA
toll free (800) 526-7919 • telephone (952) 358-3800 • fax (952) 358-3801
www.networkinstruments.com

European Headquarters
Network Instruments • 7 Old Yard • Rectory Lane • Brasted, Westerham • Kent TN16 1JP • United Kingdom
telephone + 44 (0) 1959 569880 • fax + 44 (0) 1959 569881
www.networkinstruments.co.uk