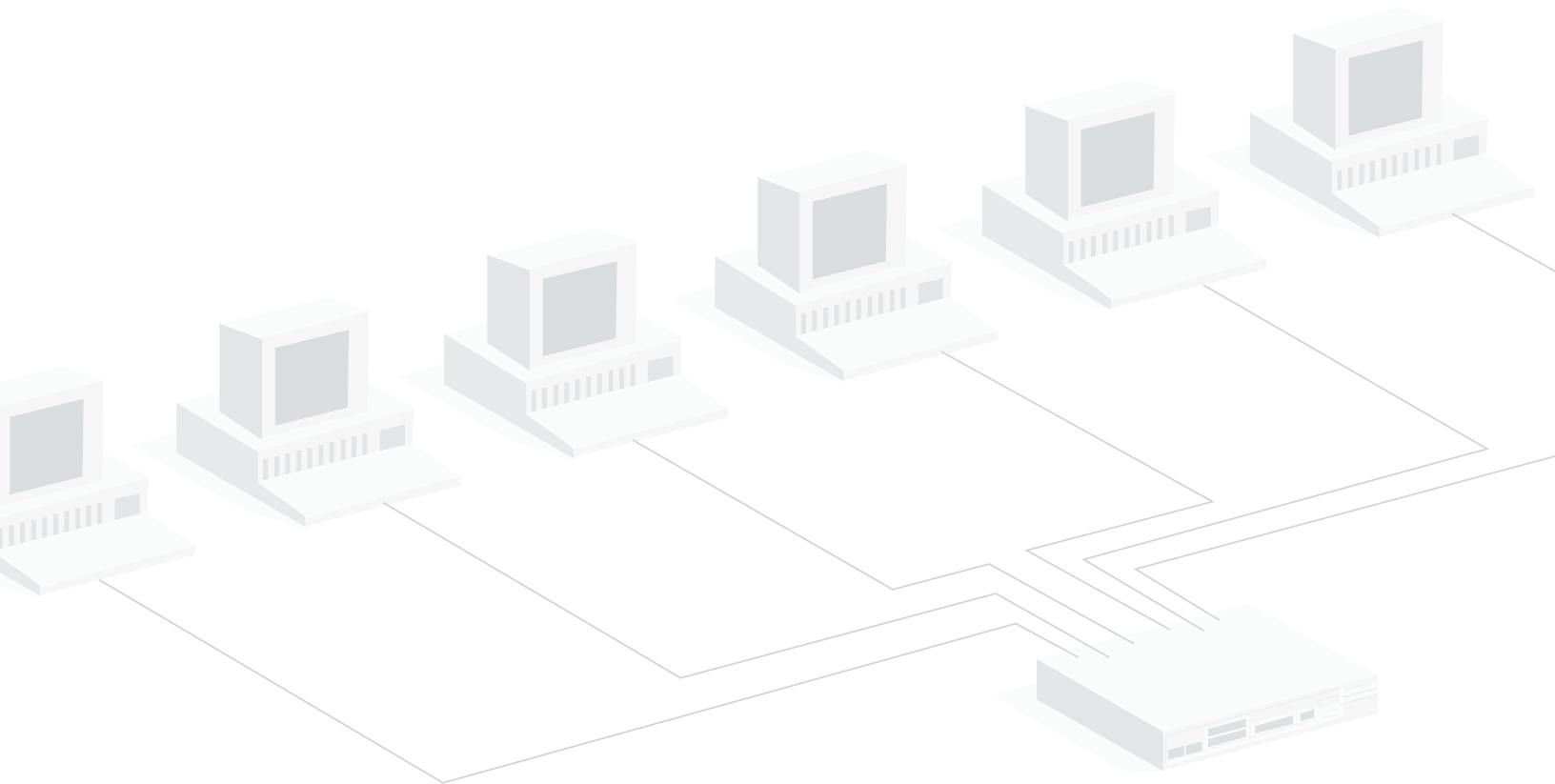


# Analyzing Full-Duplex Networks Through SPANs, Port Aggregators, and TAPs

There are a number ways to access full-duplex traffic on a network for analysis: SPAN or mirror ports, port aggregators, and TAPs are the most common. This paper discusses the technical issues you should understand before you decide which type of technology to deploy in various places on a network.



## Overview

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

- Attaching a standard monitoring or analysis device to a full-duplex switch's analyzer port (in Cisco terminology, a Switch Port ANalyzer, or SPAN) to monitor a full-duplex link
- Attaching a standard monitoring or analysis device to a port aggregator inserted into a full-duplex link
- Attaching a full-duplex monitoring or analysis device to a TAP (Test Access Port) inserted into a full-duplex link

Because of the architectural limitations of switches and port aggregators (which are essentially buffered switches), a TAP is the only solution for monitoring full-duplex networks utilized at more than 50%. Even if bandwidth is below 50%, SPANs and port aggregators still have limitations making them less than ideal for situations where it is necessary to see every packet on the wire. A SPAN or port aggregator can be appropriate when monitoring lightly utilized and/or non-critical portions of a network. To effectively detect security threats or troubleshoot connection problems in high-traffic situations, however, requires the transparency and robustness of a TAP.

## Introduction

Whether you want to monitor a network for security threats or capture and decode packets to troubleshoot problems, you need a reliable way to see the network traffic. Regardless of what analyzer or intrusion detection solution you choose, you must decide on a mechanism to give your analysis equipment physical access to network traffic.

There are three common ways to accomplish this:

- Connect standard analysis or monitoring equipment to the SPAN or mirror ports on critical switches. The interface on the analyzer must be at least as fast as the link being monitored. For example, you can monitor a 10/100 network with either a 10/100 analyzer or a gigabit analyzer, but it is not recommended to monitor a gigabit network with a 10/100 analyzer.
- Insert port aggregators on the full-duplex links between switches and critical devices, to which you connect standard analysis or monitoring equipment. This is equivalent to the SPAN solution, with some limited protection against packet loss provided by the port aggregator's built-in memory buffer.
- Insert TAPs on the full-duplex links between switches and critical devices, then plug in a full-duplex analyzer (i.e., an analyzer equipped with a dual-receive interface) as needed without interrupting the links.

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 workstation connected to the switch. Although TAPs are an extra expenditure (both in the TAP itself and in the specialized interface required for the analyzer), the investment is justified where traffic levels are high or where you do not wish to have hardware errors filtered out by the switch.

One might think that the port aggregator would make a good compromise between the TAP and SPAN options; although it costs about as much as a TAP, it does not require a specialized interface on the analysis device. Like a TAP, it is independent of the network, making it invulnerable to security threats.

But in a sense, a port aggregator gives you the worst of both worlds when compared to SPANs and TAPs: It is not remotely configurable like a SPAN. It is not included for free with most switches like a SPAN. Although an aggregator usually includes an internal memory buffer to mitigate the bandwidth problems associated with SPANs (which is described on the next page), in practical terms that buffer is meaningless. And like a SPAN, an aggregator always filters out hardware-level errors from your analysis or monitoring device.

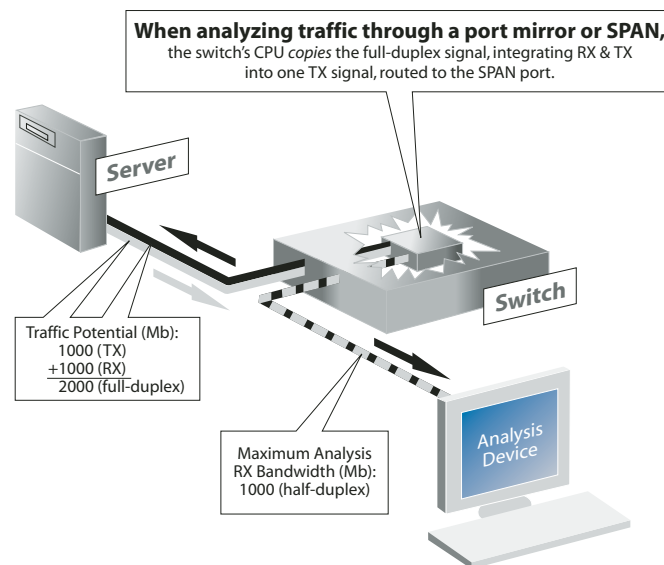
## Using a switch's SPAN or mirror port

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 analysis or monitoring equipment and network performance. Depending on a SPAN or port mirror for network visibility presents a number of risks:

- As the total bandwidth usage for both channels exceeds 50% of the full-duplex link, the switch starts dropping the redirected packets. There just isn't enough bandwidth on the SPAN or mirror port's send channel to carry both sides of the full-duplex connection. Monitoring a 10/100 network through a gigabit SPAN or mirror port and analyzer can be a work-around to the bandwidth problem, but does nothing to alleviate the potential for switch overload described below.
- The switch's CPU must act as both a network switch and a packet replicator. 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 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 way to tell when the SPAN or mirror port is dropping packets or delivering inaccurate time stamps.
- If the switch itself is not working (either through a hack attack or hardware failure) you may not be able to analyze the problem. If you are using a TAP or port aggregator, you will retain visibility even if the switch is compromised. SPANs can also be hijacked, allowing hackers access to potentially sensitive corporate data.

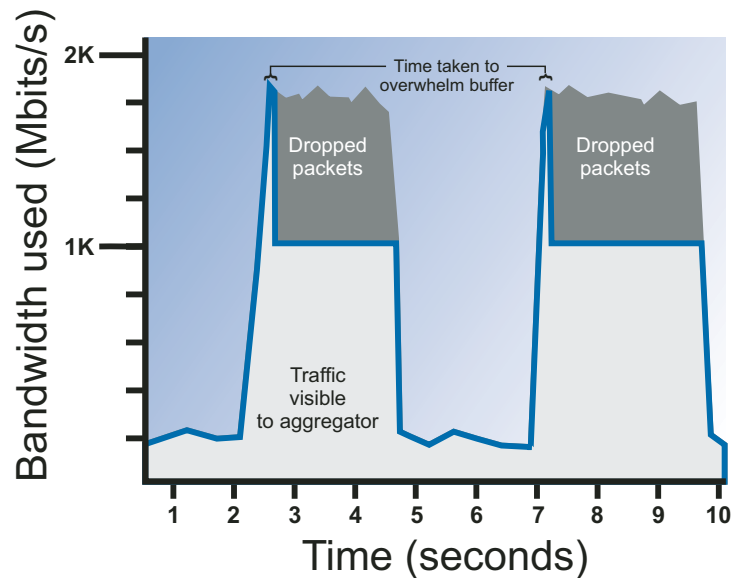


A SPAN or mirror port can deliver satisfactory results when used to monitor lightly used, non-critical networks. If usage exceeds 50%, however, the SPAN or mirror port's bandwidth will be insufficient to keep up with the traffic. The result is packet loss—which invalidates analysis, and makes monitoring 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.

## Using a port aggregator on the link

A port aggregator is essentially a small switch devoted to mirroring a link for analysis. It includes network in and out ports that provide link connectivity for the devices, and a standard full-duplex port, which mirrors packets traveling the link to the analyzer port. Its advantage over a SPAN is in its independence from the switch. Like a TAP, it is not an addressable device on the network, and therefore not susceptible to security threats. It also usually includes an internal memory buffer, most commonly 1 MB. Although vendors may claim the port aggregator's 1 MB memory buffer provides some protection against packet loss, it does not offer much. On a fully saturated gigabit line, a 1 MB buffer provides a capture window of 1/12th of a second; on a 100 Mb link, the window is 1.2 seconds, after which the aggregator will simply drop packets. A longer capture window than this is required to analyze or solve most (if not all) network problems.

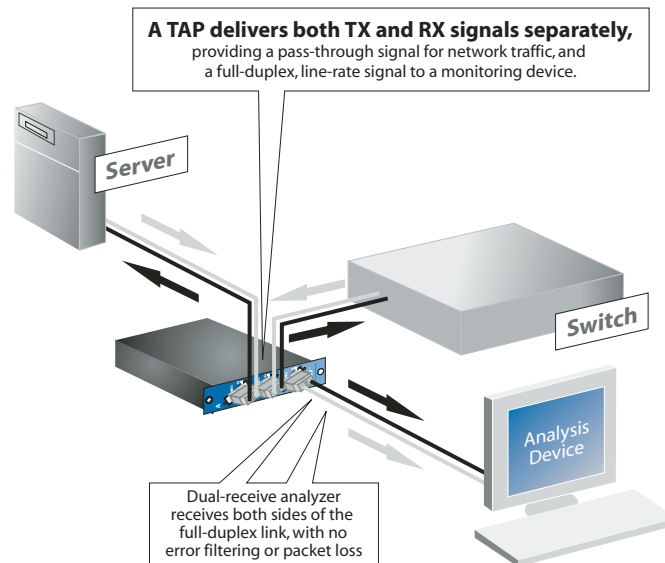
The bandwidth utilization graph below was taken as a user downloaded files from a server. All of the usage spikes shown are more than 2 seconds, and would therefore overwhelm the aggregator's small memory buffer.



## Using a TAP on the link

A TAP is a passive splitting mechanism that you install between a full-duplex "device of interest" and the network. Different TAPs are available for monitoring various media (optical or copper) at different speeds (10/100/1000). An optical TAP uses prisms to optically split the full-duplex gigabit signal into two identical full-duplex signals. One signal maintains the network link, while the other is simultaneously passed to the analysis or monitoring appliance. A copper TAP performs the same function, but uses electronic circuitry to duplicate the signals. Because the 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, regardless of traffic levels or switch limitations.

To be effective, a full-duplex TAP should be coupled with a probe or monitoring device capable of receiving both channels of a full-duplex signal.



TAPs deliver a number of conveniences in addition to eliminating the technical limitations of using SPAN ports or aggregators:

- TAPs never drop packets, regardless of bandwidth saturation.
- Unlike the port mirror/SPAN mechanism on a switch, a TAP does not filter physical-layer error packets from the data stream sent to the analyzer.
- A TAP is completely passive; it cannot interfere in any way with the full-duplex network.
- A TAP is not an addressable device on the network, and is therefore not subject to hack attack.

## Side-by-side comparison

The table below summarizes the advantages and disadvantages of TAPs, SPAN or mirror ports, and port aggregators.

Feature	SPAN or Mirror Port	Port Aggregator	TAP
Can it process high levels of traffic accurately?	No. A SPAN or mirror port is not capable of transmitting all the data from a fully-saturated full-duplex link.	No. A port aggregator is not capable of transmitting all the data from a fully-saturated, full-duplex link for more than a fraction of second on a gigabit link.	Yes. A TAP is capable of keeping up with a fully-saturated network. ✓
Is it included for free with a switch?	Yes, for most enterprise-level managed switches. ✓	No.	No.
Is it invulnerable to security threats?	No. A switch can be compromised by a hack attack, and the mirrored port can be hijacked.	Yes. Like a TAP, a port aggregator is not an addressable device on the network. ✓	Yes. A TAP is not an addressable device on the network. A TAP can't compromise analysis performance or corporate security. ✓
Is it remotely configurable?	Yes. You can change port mirror assignments from anywhere you can administer the switch. ✓	No.	No.
Does it show all the packets?	No. A SPAN can drop packets in high-bandwidth situations; it always filters physical errors from the data stream.	No. An aggregator can drop packets in high-bandwidth situations; it always filters physical errors from the data stream.	Yes. A TAP is the only failsafe way to ensure that you are seeing every bit being transmitted in both directions across a full-duplex link. ✓

## Conclusion

Monitoring a full-duplex connection via a SPAN port or port aggregator is valid only for low-bandwidth, non-critical links. Even in low-bandwidth environments, use the SPAN or aggregator only to obtain statistics (i.e. not to capture packets). This is because neither of these options provide any warning or indication of packets being dropped.

Monitoring a full-duplex connection using a TAP and a dual-receive gigabit capture interface ensures complete, full-duplex capture for monitoring, analysis, and intrusion detection regardless of speed, bandwidth saturation, or any other network condition.

**Corporate Headquarters** Network Instruments, LLC • 8800 West Highway Seven • Fourth Floor • Minneapolis, MN 55426 • USA  
toll free (800) 526-7919 • telephone (952) 932-9899 • fax (952) 932-9545 • www.networkinstruments.com

**European Office** 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

**France, Italy and Spain** Network Instruments • 1 rue du 19 janvier • 92380 Garches • Paris • France  
telephone +33 (0) 1 47 10 95 21 • fax +33 (0) 1 47 10 95 19 • www.networkinstruments.fr

© 2004 Network Instruments, LLC. All rights reserved. Network Instruments and the Network Instruments logo are trademarks or registered trademarks of Network Instruments, LLC.