

# Use of Taps and Span Ports in Cyber Intelligence Applications

## White Paper



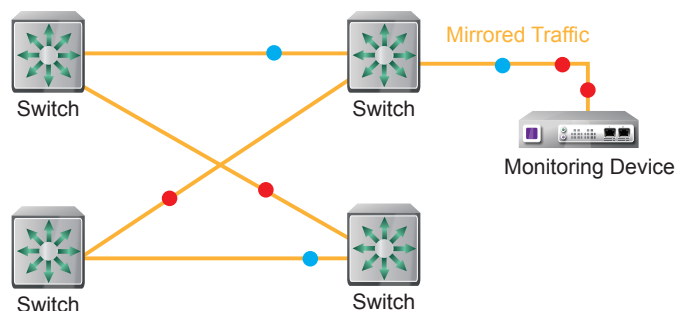
Cyber warfare is unfortunately no longer found only in speculative fiction; it is with us today. Distributed denial-of-service (DDoS) attacks have been launched against the United States, South Korea, Kyrgyzstan, Estonia, and Georgia in recent years, and military and government computer systems around the world are assaulted by intruders daily. Some attacks come from nation-states, but others are perpetrated by transnational and unaligned rogue groups. Those bent on inflicting harm on nations and citizens not only use networks as an attack vector, but also for organizing, recruiting, and publicizing their beliefs and activities.

On the other side of the fence are the good guys, the members of the cyber intelligence community who aim to understand and track the terrorists, and ultimately stymie their plans. Due to the pervasive use of networks by radical and criminal organizations in the modern world, a great deal can be learned about terrorists by examining their use of the World Wide Web, and how the Internet is used as a vector to attack both public and private systems. This field of study is called “terrorism informatics,” which is defined as “the application of advanced methodologies and information fusion and analysis techniques to acquire, integrate, process, analyze, and manage the diversity of terrorism-related information for national/international and homeland security-related applications” (Hsinchun Chen et al, eds., *Terrorism Informatics*. New York: Springer, 2008, p. xv).

Terrorism informatics analyzes information from data-at-rest sources such as blogs, social media, and databases. For other types of analyses, it is necessary to examine data in motion, in other words, information as it travels on a network. Access to data-in-motion is often obtained by eavesdropping on the network traffic using Span ports in switches. This paper focuses specifically on the implications of using Span ports in counter-terrorism monitoring applications. It shows that Span ports are particularly ill-suited to this use. Note also that the security vulnerabilities of Span ports in counter-terrorism applications apply equally when Span ports are used for other monitoring needs such as performance or compliance monitoring.

### Introduction

Span or mirror ports are a convenient and inexpensive way to access traffic flowing through a network switch. Switches that support Span ports—typically high-end switches—can be configured to mirror traffic from selected ports or VLANs to the Span port, where monitoring tools can be attached. At first glance, it seems that a Span port could be a good way to connect an intrusion detection system (IDS), forensic recorder, or other security monitoring device.



Span Ports Mirror Traffic for Monitoring

## Use of Taps and Span Ports in Cyber Intelligence Applications

### White Paper

Unfortunately, Span ports have several characteristics that can be troublesome and risky in a counter-terrorism application. These characteristics include:

- The possibility of dropping packets
- The need for reconfiguring switches
- The vulnerability of Span ports to attack
- The fact that Span ports are not passive mechanisms

These issues are elaborated in the following sections.

#### Problem #1: Dropped Packets

The first issue with Span ports in a counter-terrorism application is that the visibility of network traffic is less than perfect. In counter-terrorism monitoring, a fundamental requirement is that the security device must be able to see every single packet on the wire. An IDS cannot detect a virus if it doesn't see the packets carrying it. Span ports cannot meet this requirement because they drop packets. Spanning is the switch's lowest priority task, and Span traffic is the first thing to go when the switch gets busy. In fact, it is allowable for any port on a switch to drop packets because network protocols are specifically designed to be robust in spite of dropped packets, which are inevitable in a network. But it is not acceptable in a counter-terrorism monitoring application.

Different switches may be more or less prone to drop Span packets depending on their internal architecture, which varies from switch to switch. However, it is unlikely that the performance of the Span port was evaluated as an important criterion when the switching gear was selected. As a counter-terrorism professional, you probably don't want your security strategy to be dependent on a procurement policy that you don't control.

Nevertheless, suppose you do have switches with the best possible Spanning performance. Dropped packets may still be an issue depending on how much traffic you need to send through the Span port. If you need to see all of the traffic on a full-duplex 1 Gigabit link, a 1 Gigabit Span port won't do the job. Full duplex link traffic exceeds the 1 Gigabit SPAN port capacity when link utilization goes above 50 percent in both directions. To see all the traffic, you need to dedicate a 10 Gigabit port for Spanning, and now the Span port doesn't seem so inexpensive any more.

However, Span port visibility issues go beyond simply dropping packets. Being switch technology, Span ports by their very nature are not transparent for layer 1 and layer 2 information: for example, they drop undersized and oversized packets, and packets with CRC errors. They usually remove VLAN tags, too. In addition, Span ports do not preserve the packet timing of the original traffic, or in some cases even the packet order. This type of information can be critical for detecting certain types of network attacks such as network worms and viruses, and for some behavior-based packet classification algorithms. For example, network consultant Betty DuBois observed, "[Regarding] losing the VLAN tag information when Spanning, if there is an issue with ISL or 802.1q, how will I ever know with a Span port?" (<http://www.lovelytool.com/blog/2007/08/span-ports-or-t.html>)

#### Problem #2: The Need for Switch Configuration

Another issue with using Span ports in a counter-terrorism application is the very fact that the switch needs to be configured to send specific traffic to the Span port. This fact leads to a host of complications:

- **The configuration may not be done correctly.** "If the switch owner mistakenly or intentionally configures the Span port to not show all the traffic it should, you may or may not discover the misconfiguration. I have seen this happen countless times," said Richard Bejtlich, the highly respected author of *The Tao of Network Security Monitoring*. ([http://www.governmentsecurity.org/All/Why\\_Network\\_Taps](http://www.governmentsecurity.org/All/Why_Network_Taps))

## Use of Taps and Span Ports in Cyber Intelligence Applications

### White Paper

- **Sharing the Span port.** A switch typically supports only one or two Span ports, and the network administrator or someone else may need to use “your” Span port for one reason or another. They may or may not tell you when the Span traffic profile is changed for their needs. IT Manager Bob Huber recalled, “Span was a huge issue we dealt with on the IDS team where I used to work. We had constant issues with the Span going up and down. When there are network issues to deal with, the network engineers have priority to the limited number of Span ports available. Hoping they remember to reconfigure your Span port was a waste of time.” (<http://taosecurity.blogspot.com/2007/12/expert-commentary-on-span-and-rspan.html>)
- **Switch configuration may not be available when you need it.** If you need to change the profile of the traffic you are Spanning, or change it back after someone else used the port, it may not be easy to get the switch owner’s time to do it. In larger organizations, you may also need to get the change authorized through a Change Control Board, and then wait for a maintenance window to get it implemented.
- **Changes to the network switches for other reasons can impact the Span traffic.** Networks are constantly being reconfigured to optimize applications or support new requirements. If the counter-terrorism monitoring solution depends on Span ports, it is vulnerable to changes (planned or surprises) any time the network is reconfigured for any reason.
- **Switch configuration itself is a security vulnerability.** In any counter-terrorism activity, the network’s security is of course paramount. Switches are a highly vulnerable network point, and the ability to reconfigure them must be tightly controlled. Does it make sense to require switch reconfiguration as part of the counter-terrorism monitoring solution, when reconfiguring a switch can accidentally or deliberately expose or bring down the network?

If you have any doubt that Span port misconfiguration can be an issue, take a look at this note in the Cisco Catalyst 6500 Series documentation: “Connectivity issues because of the misconfiguration of Span ports occur frequently in CatOS... Be very careful of the port that you choose as a Span destination.” ([http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_tech\\_note09186a008015c612.shtml#topic8-1](http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a008015c612.shtml#topic8-1))

### Problem #3: Vulnerability to Attack

Span ports are usually configured for uni-directional traffic, restricted to transmitting traffic to the monitoring device. However, in some cases they can receive traffic as well (a feature Cisco calls ingress traffic forwarding), in order to enable management of the monitoring device over the same switch port and monitoring device NIC as the mirror traffic. When this configuration is used, the Span port becomes an open ingress port to the switch, creating a serious security vulnerability. Therefore, this configuration should be avoided as a best practice. If for some reason it becomes necessary to use this configuration, you should at least lock the Span port to the monitoring tool’s MAC address if possible, so an unauthorized user won’t be able to plug a laptop into the connection and hack the switch.

### Problem #4: Not Passive

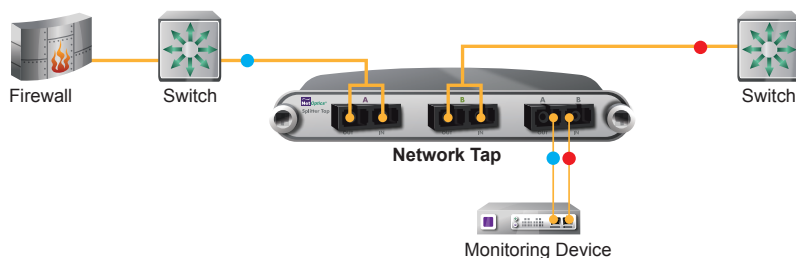
A final important consideration when using Span ports for counter-terrorism monitoring access is that Span ports are not passive: They can affect the performance of the switch’s other ports. For example, Gerald Combs, the father of Wireshark, warns, “Some switch families (e.g., the Cisco 3500 series) don’t set a lower priority on Span traffic, and will slow down the backplane in order to deliver packets to a Span port.” (<http://www.lovelymytool.com/blog/2007/08/span-ports-or-t.html>) This effect violates a primary principle of security and especially forensic monitoring, that monitoring should not affect the traffic being monitored. It may have legal as well as practical implications.

## Use of Taps and Span Ports in Cyber Intelligence Applications

### White Paper

#### The Tap Alternative

To avoid the problems that Span ports bring to counter-terrorism monitoring applications, security experts like Bejtlich recommend using traffic access ports (Taps) for access to the network traffic. Taps are specifically designed to provide 100 percent traffic visibility without any impact on monitored traffic. Optical Taps for fiber links use optical splitters to divert part of the light from the link to a monitor port, creating a true copy of the link traffic all the way down to layer 1 and layer 2 errors. Taps for copper links perform a similar function electronically. Optical Taps do not use any power at all, while copper Taps include relays which ensure that link traffic continues to flow even when the Tap loses power. Taps avoid all of the pitfalls of Span ports in counter-terrorism applications:



Fully passive fiber network Tap with optical splitters

- Taps send the monitoring tool an exact copy of the link traffic, including layer 1 and layer 2 errors and malformed packets, no matter how busy the link is. They never drop packets.
- Taps require little or no configuration. Once a Tap is installed in a link, monitoring access to the link traffic is always available, consistently and persistently.
- Taps are secure. They do not have an IP address so attackers cannot see them, and they cannot inject traffic into the network under any circumstances. In fact, a Tap actually hides the monitoring tool from the network as well, providing true “stealth” monitoring.
- Taps are completely passive. They cannot affect the link traffic, not even if they lose power.

Tap technology has evolved to offer a range of additional features as well, most of which are not available with Span ports. (Note that some of these features require a trade-off with the previously mentioned characteristics.)

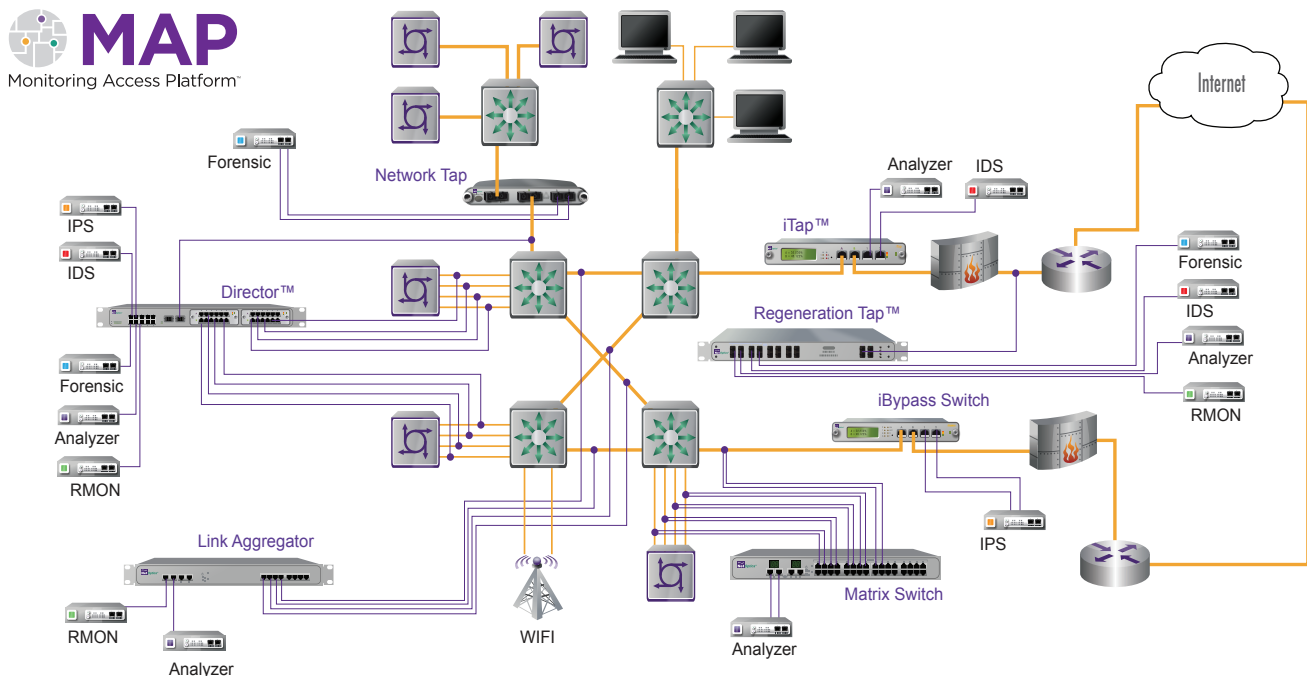
- **Regeneration Taps** produce multiple copies of the link traffic so multiple tools and multiple users can view the same traffic simultaneously. Your counter-terrorism monitoring device does not need to give up access when the network administrator needs to put an additional protocol analyzer onto the link.
- **Aggregator Taps** combine the traffic from both directions of full-duplex links and from multiple links and sends it to a single NIC on the monitoring tool. No packets are dropped as long as the aggregated traffic does not exceed the monitor port bandwidth.
- **Active Response Taps** permit monitoring tools to send response packets such as TCP resets, ICMP messages, and ACL changes into the tapped link. This feature can be used by an IDS to take action when certain types of intrusions are detected. (Active Response Taps are an exception to the Tap “one direction only” traffic rule.)
- **iTaps** provide a remote management interface and basic monitoring data about link traffic, such as packet counts and utilization levels. (Remote management interfaces require IP addresses, but they are secured with passwords, SSH, HTTPS, and other measures.)

## Use of Taps and Span Ports in Cyber Intelligence Applications

### White Paper

- **Media Conversion** refers to Taps that support different media types on their network and monitor ports. Many Taps have pluggable SFP or XFP ports enabling different media types to be accommodated simply by plugging in different transceiver types. Some Taps even perform 10 Gigabit to 1 Gigabit and 1 Gigabit to 10 Gigabit data rate conversion as well.
- **Filter Taps** enable mirrored traffic to be restricted to particular protocols, source and destination IP addresses, VLANs, ports, and other criteria, making it easier to isolate or troubleshoot issues, and relieving monitoring tools from spending valuable processing cycles on pre-filtering traffic. For example, the Net Optics Director Data Monitoring Switch supports filtering as well as regeneration, aggregation, remote management, and media conversion, all in a single device.
- **Bypass Switches** create fail-safe access ports for in-line devices such as intrusion prevention systems and firewalls.

The wide range of Tap devices available today enable appropriate monitoring access to be built into all parts of the network architecture, at the edges, distribution, LAN, and core. Such a Monitoring Access Platform (MAP) does not depend on Span ports for strategic information access, but in fact frees up the Span ports for tactical monitoring access when special needs arise. Permanent and ongoing counter-terrorism monitoring can rely on a Tap-based MAP for consistent, persistent, and secure monitoring access, immune to the vagaries of day-to-day network administration and management.



Integrated Monitoring Access Platform Based On Tap Technology



## Use of Taps and Span Ports in Cyber Intelligence Applications

### White Paper

#### Conclusion

Monitoring is an essential building block of Bejtlich's "defensible network architecture," the first of its seven key characteristics: monitored, inventoried, controlled, claimed, minimized, assessed, and current. (<http://taosecurity.blogspot.com/2008/01/defensible-network-architecture-20.html>) Utilizing Span ports for counter-terrorism monitoring access is placing that building block on a weak foundation, subject to packet loss, misconfiguration, and intrusion. A Monitoring Access Platform, based on Tap technology and integrated within the network architecture, is an alternate access approach that provides a solid base on which to build your network's security and counter-terrorism applications.

#### For further information about Tap technology for security applications:

<http://www.netoptics.com>

Net Optics, Inc.

5303 Betsy Ross Drive

Santa Clara, CA 95054

(408) 737-7777

[info@netoptics.com](mailto:info@netoptics.com)

*Customer First!*