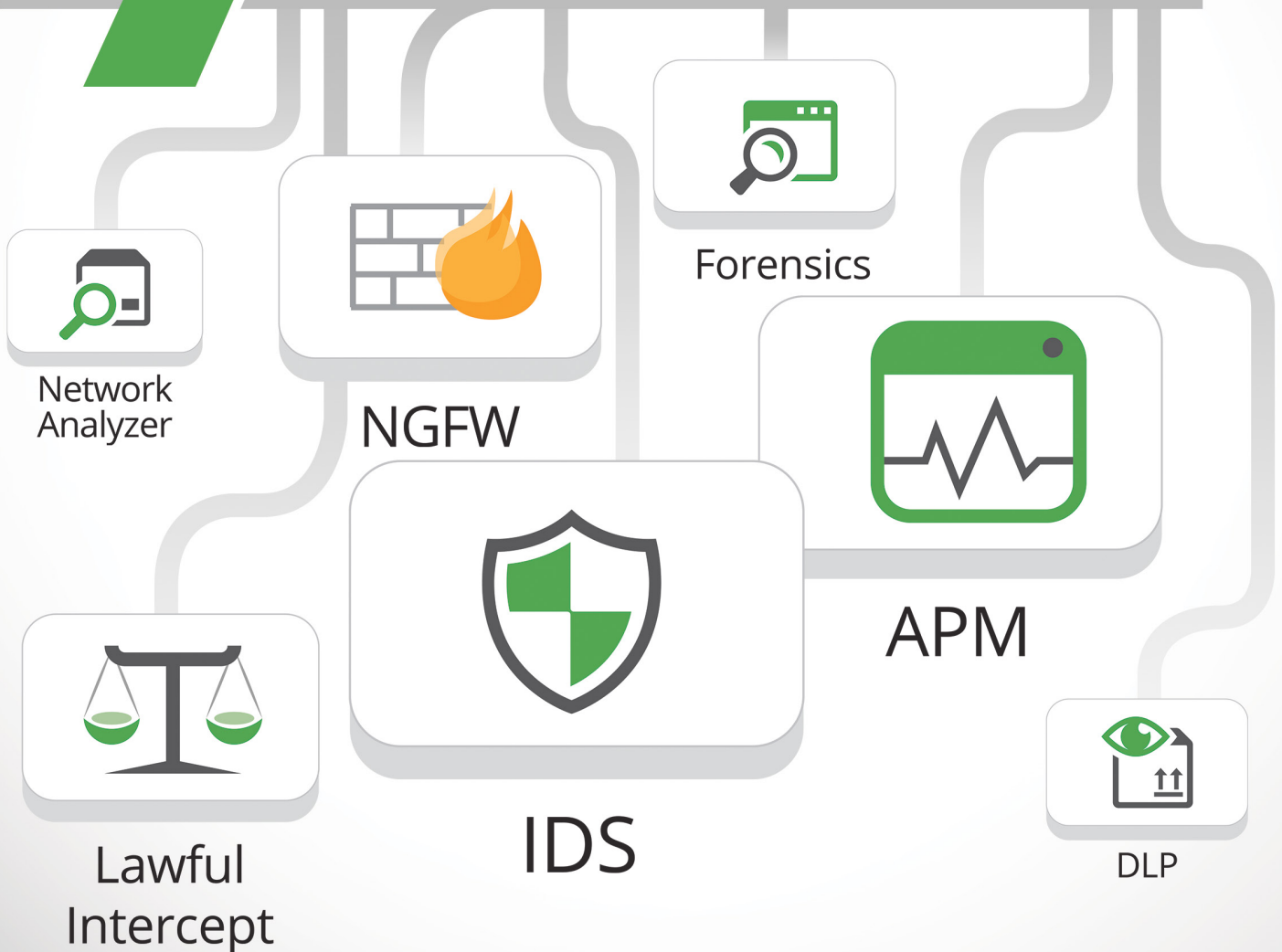


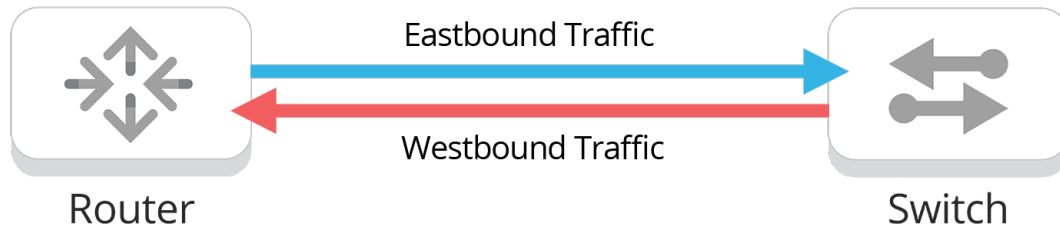
WHAT YOUR NETWORK IS MISSING

7 Tools To TAP



Introduction

A network Test Access Point, or **network TAP**, is an oft-confused or even unknown technological hardware device. It provides a simple and cost effective solution for connecting different monitoring, security, or analysis tools to your network. Also known as a Traffic Access Point, the device is placed between two ends of a network to monitor the traffic flowing between the network devices, whether for network management, security, or analysis.

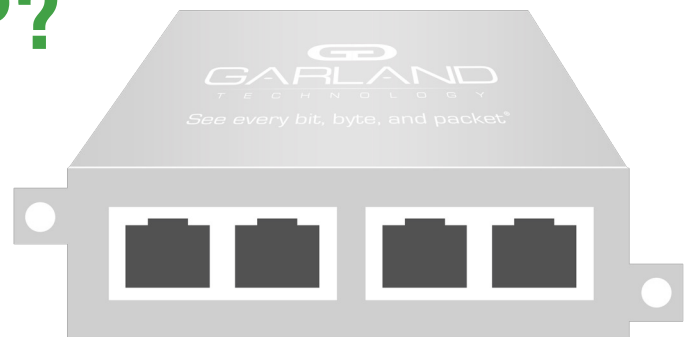


Rather than a standard network cable, the network TAP is installed between the two network devices with a pair of cables. The traffic on the network then flows through the TAP without interruption, while the TAP sends a complete copy of the live network traffic to the monitoring port without notifying the network. These devices are able to work in 10/100/1000-megabit, 10-gigabit, 40-gigabit, and 100-gigabit networks, letting traffic flow seamlessly and uninterrupted while copying every bit, byte, and packet.[®]

Whether you're building your own network or connecting other network tools, network TAPs enable you to link one or multiple tools while maximizing your network's security and efficiency.

Why A Network TAP?

A TAP guarantees that your network tools receive a complete copy of all live network traffic. Below are the seven products that most commonly connect with network TAPs.



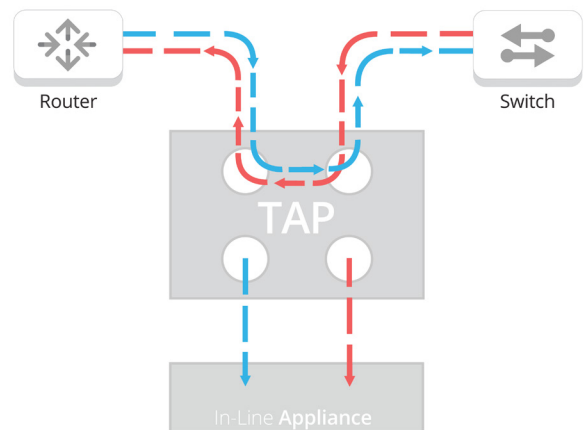
Network Analyzer

1

Network analyzers – also known as “sniffers” – are hardware or software applications that intercept, inspect, and collect data traffic for the analysis of network statistics and problems, detection of intrusion attempts, and more.

Successful network analysis is an impossible task without complete access to a system’s network traffic. Full access is essential for network analyzers. [Compared to SPAN ports](#), TAPs are a smarter option in this function. An over-subscribed SPAN port will not provide 100 percent of a network’s traffic data. In addition, the SPAN port is often not available when oversubscribed.

If you need to monitor multiple network segments simultaneously, an Aggregation TAP (shown above) copies data in both directions (east and west) for monitoring and access. TAPs allow you to aggregate data to your network analysis tools, or simultaneously replicate data to more than one network tool.



Next-Generation Firewall

2

Combining application awareness and deep packet inspection, next-generation firewalls give you more control over applications, while also detecting and blocking malicious threats. Unlike traditional firewalls, these network platforms are able to identify the applications you use, including those on the Internet. Rather than allowing traffic to pass through typical Web ports, a next-generation firewall distinguishes between your CRM and Netflix. It then applies policies based on your business’ rules.

Because next-generation firewall appliances need to be installed in-line, they will create network downtime for maintenance, troubleshooting and updates. Each time the network link is brought down can be thousands of dollars of lost revenue. A [bypass network TAP](#) will keep the link flowing if the in-band security appliance were to go off-line for any reason. It will also keep the link flowing even if the TAP were to lose power.

Computer Forensic Analysis and Data Capture

3

Computer forensics is applied in many ways, such as analyzing computer systems belonging to a defendant in a legal case, recovering data after hardware or software failure, and analyzing a system attack.

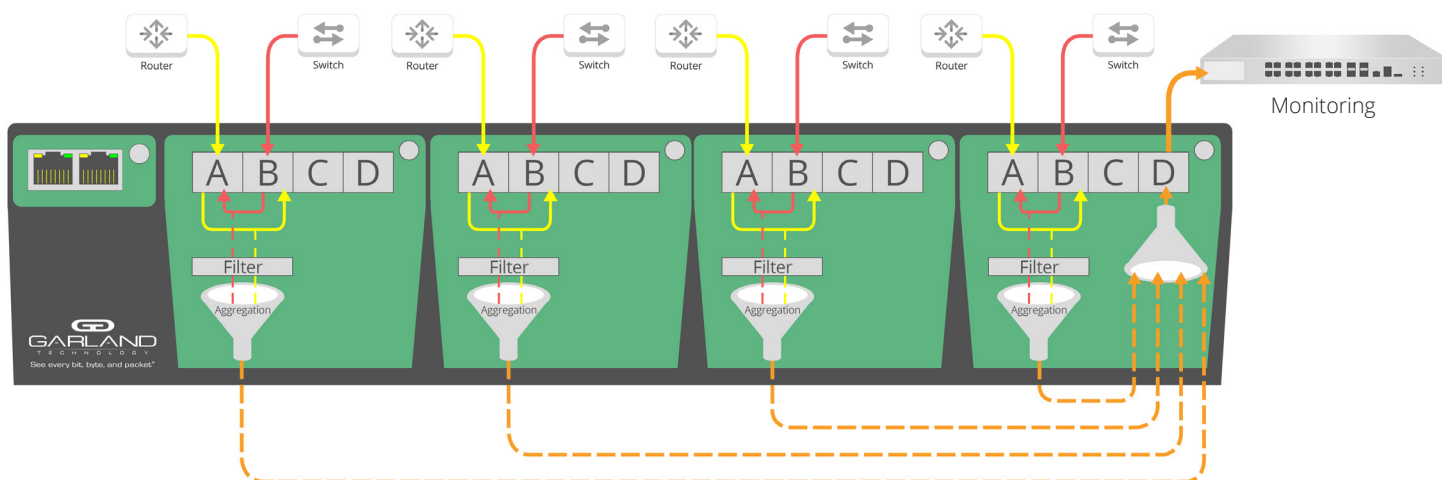
As with network analysis, gaining access to complete network traffic is essential for successful forensics research. In this case, data from SPAN ports are not submissible in a court of law because they do not provide 100% of the network traffic when over-subscribed or unavailable. If forensic tools need to simultaneously monitor multiple network segments and aggregate data or replicate data to multiple network tools, TAPs are the best connectivity solution.

Application Performance Monitoring

4

Application performance monitoring (APM) is the monitoring and management of the performance and availability of software applications. APM strives to detect and diagnose application performance problems to maintain an expected level of service.

This layer of the network has become a “hacker’s playground.” Many breaches happen at the application level; black hats are using trusted applications to exploit gaps in perimeter security. [Filtering and aggregating traffic](#) to the proper tools closes these gaps and detects breaches.



Data Leakage Prevention (DLP)

5

DLP tools are designed to detect and prevent unauthorized transmission of data to outside parties. These tools process highly classified or sensitive information, and they are prevalent with government agencies as well as banking and insurance companies.

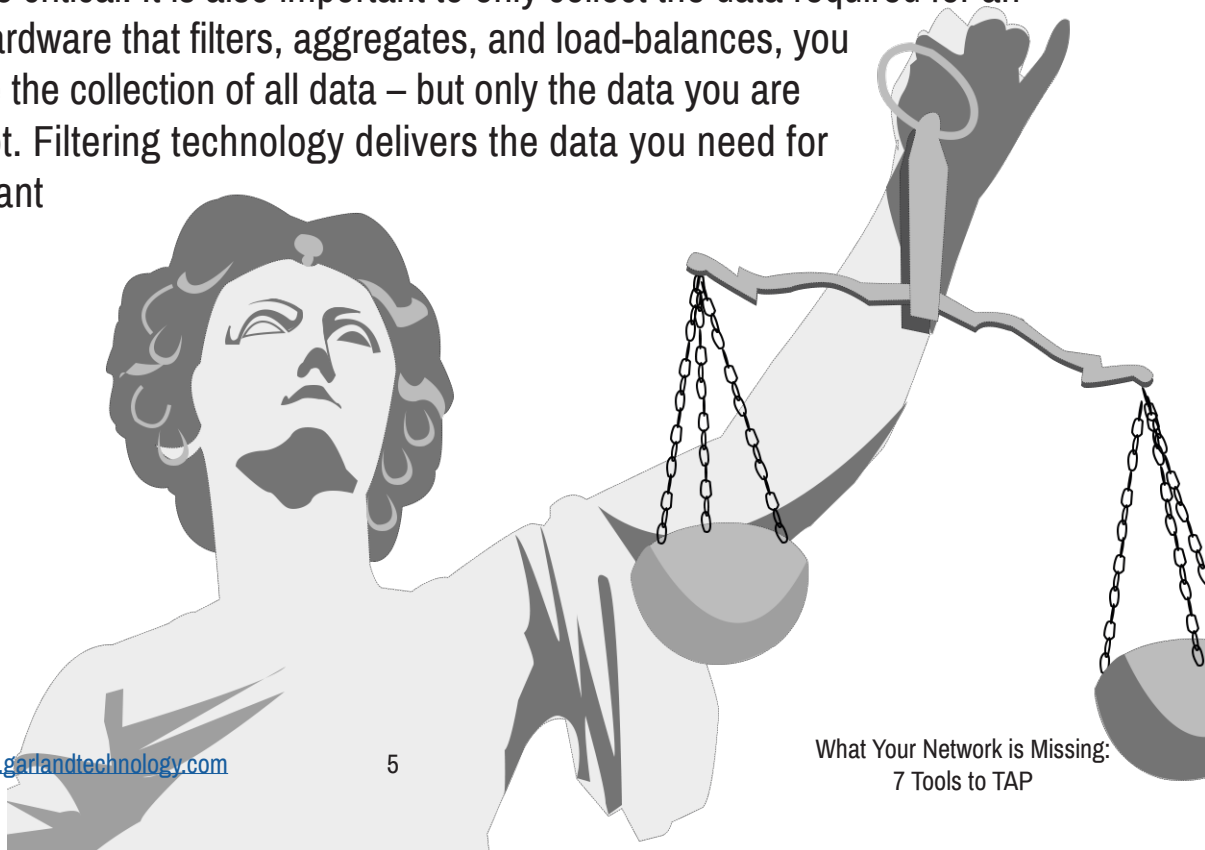
These tools combine the main concerns of the previous four products. They run the same downtime risks as with next-generation firewall products, and they have the same concerns as with forensic and network analysis in gaining complete access to network traffic and multiple networks. Often DLP systems are deployed with additional security and monitoring tools, in this scenario a bypass tap is required for the active, in-line appliances along with a [packet broker](#) for aggregating and filtering the data.

Lawful Interception

6

Lawful interception is the security process that enables companies to provide law enforcement officials with access to private email messages or phone calls. Countries are enacting laws to regulate lawful interception procedures.

Again, complete access to network traffic and the ability to simultaneously monitor multiple network segments are critical. It is also important to only collect the data required for an intercept. By using hardware that filters, aggregates, and load-balances, you are able to guarantee the collection of all data – but only the data you are supposed to intercept. Filtering technology delivers the data you need for thorough and compliant lawful interception.



Intrusion Detection and Prevention Systems (IDS, IPS)

7

An intrusion detection system (IDS), as aptly named, detects unwanted attempts to access your network or to manipulate or disable your computer system. An intrusion prevention system (IPS) prevents such access.

These tools enable devices to send packets back to the live network in an effort to stop these threats. They are also installed in-line, so they run the risk of bringing your network down should the tool crash or need maintenance. With a bypass TAP, however, intrusion detection and prevention systems provide the same type of protection but do not carry the aforementioned risks.

When considering any of these network tools, it's easy to overlook how to connect the tool to a network. But the manner in which it connects has ramifications. Network TAPs are an industry best practice to guarantee 100% access and visibility to the data. The security or monitoring tools your adding to your network are only as good as the data they receive. By budgeting for a TAP from the start of your project, you have the connectivity you need right from the start.

With TAPs, you have an easy and affordable way to get all of the data you need without the dangers of over-subscribing or downtime inefficiencies.

Garland Technology is all about connections – connecting your network to your appliance, connecting your data to your IT team, and reconnecting you to your core business. It's all about better network design. Choose from full line of access products: a network TAPs that supports aggregation, filtering, regeneration, bypass and breakout modes; packet brokering products; and cables and pluggables. We want to help you avoid introducing additional software, points of failure and bulk into your network. Garland's hardware solutions let you **see every bit, byte, and packet®** in your network.

Contact

Sales, quotations, product inquiries:
sales@garlandtechnology.com

Garland Technology, LLC.
New York | Texas | Germany

Originally published 2014 - Republished Fall 2016. Copyright © 2016 Garland Technology. All rights reserved.