Maximizing Visibility

Understanding the Role of Network TAPs, Packet Brokers and Hybrid Solutions

GARLAND TECHNOLOGY

See every bit, byte, and packet®

Today's networks are the lifeblood of the organization. Therefore, it's not surprising that maximizing visibility is a key priority as IT groups worldwide strive to keep them secure, healthy and performing at their peak. As a result, forward thinking companies are implementing a network access and connectivity solution to efficiently support a wide range of systems:

- Firewalls, advanced threat detection and security devices
- Network management and optimization tools
- Application performance monitoring systems
- Troubleshooting tools

Most network engineers recommend using a network TAP (test access point) to provide connected devices with 100% of the bits, bytes and packets flowing through the network. These purpose built devices can be inserted in the network at different places to provide a company's network monitoring tools and security appliances with a complete copy of the network traffic data without disrupting normal network operations.

For most applications, you can simply connect the device to the network TAP and call it a day – it will get all the traffic data it needs to do its job effectively. However, there are times when you need a more sophisticated connectivity solution. Here we'll review some of the more common scenarios that you will find in today's environment and show you how integrating a packet broker with your network TAP – or simply using a hybrid TAP – can solve a variety of issues and maximize every investment you've made in security and network monitoring technology.

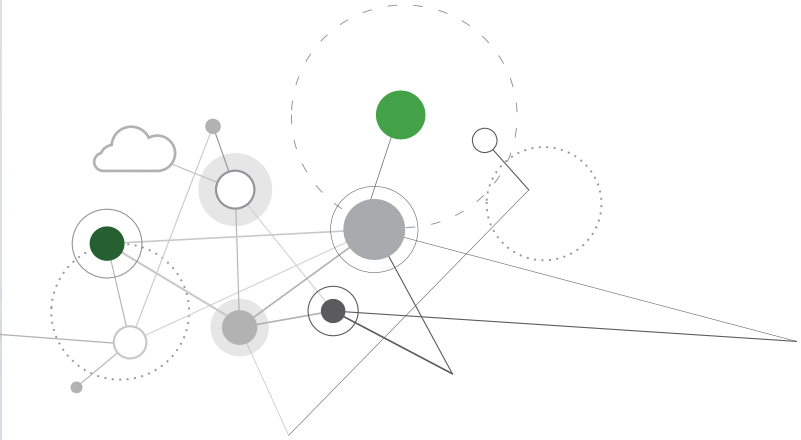
Maximizing visibility for security, troubleshooting and performance monitoring systems

Because network TAPs provide a bridge between a unique set of network specifications and appliance requirements, it's important to understand when you may need additional functionality to optimize the connection.

Regeneration

Often, companies need to send traffic data from different points in the network to multiple security appliances and monitoring systems. For efficiency, companies can use network TAPs with regeneration capabilities to copy traffic and sent it to any and all connected systems. Many network engineers choose to install network TAPs with extra ports to ensure that any new security or monitoring system that will be added in the future has the network access it needs. Additionally, this gives troubleshooting teams quick access to data from different network links to speed root cause analysis work.

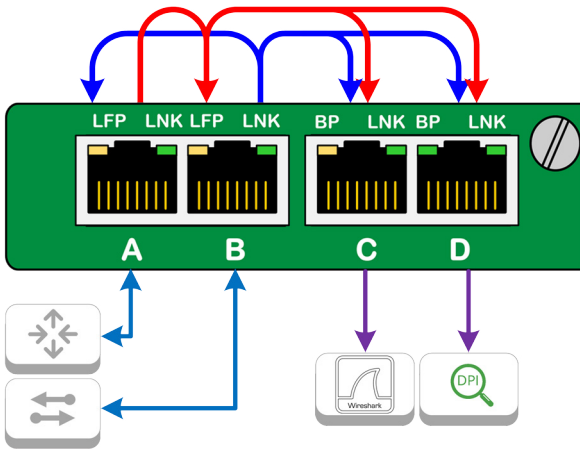
When paired with aggregating functionality (show below), network administrators can cut down on rack space, simplifying the physical data center while ensuring greater network visibility and protection.



Aggregating

To work efficiently, many security and monitoring solutions need to be able to see more traffic data than they can get from a single network access point. Consider the firewall that needs to see “both sides” of the network conversation. While most modern networks are full-duplex, transmitting data bi-directionally simultaneously, not all security appliances can support full-duplex data inputs which means they cannot see both inbound and outbound traffic. On the other hand, tools such as forensic data capture and advanced threat detection systems need to compare data from multiple links or network segments to analyze suspicious activity.

An aggregating network TAP solves this issues for a variety of appliances. In this model, the network TAP receives both sides of the conversation or data from multiple links, aggregates it and sends it to the connected appliance. This ensures that the linked solution reliably receives all of the traffic data that it needs to do its job.



The Aggregation TAP (shown) copies data in both directions for monitoring and access.

Filtering

While TAPs are designed to ensure that monitoring systems can see 100% of their network traffic, not every solution needs to see every packet. For example, appliances like VoIP recorders, web application firewalls and content filtering solutions may only need to see certain VLANs, IP addresses or ports. With a filtering functionality included with the network TAP, administrators can specify which pieces of information they want to see and exclude the extraneous data that they don't need.

Filtering also allows companies to save money on monitoring systems. Typically, the throughput of a monitoring device must match the speed of the network to ensure that it can analyze all of traffic – for example, 10Gb networks need 10Gb appliances if administrators want to analyze all the data via a single device. However, 10Gb monitoring systems are far more expensive than 1Gb appliances. By removing the unwanted data - systematically, not randomly – 10Gb network traffic can be filtered and copied to 1Gb monitoring systems, saving money without sacrificing visibility.

Load Balancing

Of all the functions you can add to a network TAP, the most important is probably load balancing. It adds a tremendous amount of versatility and flexibility to any network connectivity solution.

First, load balancing is critical for mitigating the traffic spikes that inevitably occur in networks – it ensures that connected security appliances and monitoring systems can fully capture, analyze and store all the data that comes through the network even if they don't have the capacity to take it all in at once. This is particularly important for advanced threat detection, forensic capture and other security devices that really cannot afford to lose packets.

Of all the functions you can add to a network TAP, the most important is probably load balancing.

Load balancing also ensures compatibility between networks and appliances of different capacity – companies with 40Gb networks can distribute the traffic across 4 10Gb appliances or even 40 1Gb appliances. In many ways, adding load balancing capabilities to a network TAP-based connectivity plan extends the life of all security and network monitoring assets as the network evolves. Instead of having to upgrade all the appliances every time the network is enhanced, companies can simply replace the network TAPs and use load balancing to distribute the traffic to the existing devices even though they are no longer compatible with the network. This model enables "any to any" network to appliance configurations (40Gb to 1Gb; 1GB to 100M) which is critical for sustaining core IT and security functions as companies grow and update their underlying infrastructures. Better yet, network TAPs are far less expensive than the typical network monitoring system or security solution.

Adding Functionality to Network TAPs

Regeneration capabilities are built directly into the network TAP's hardware design – simply choose a device with multiple ports. However, there are two different methods for adding aggregation, filtering and load balancing capabilities: equipping "traditional" network TAPs with packet brokers or using hybrid bypass TAPs for a more streamlined approach.

Network TAPs and Packet Brokers

Network TAPs coupled with packet brokers provide a sophisticated approach to network access – they add another level functionality that ensures greater visibility across all connected devices. Like network TAPs, packet brokers are hardware devices. When the packet broker is inserted between the network TAP and the intended security or monitoring solutions, they can intelligently route the traffic using different port mapping schemes.

By coupling network TAPs and packet brokers, network architects can design a connectivity solution complete with regeneration, aggregation, filtering and load balancing capabilities to ensure that each and every element in a network monitoring, security and performance optimization program has complete visibility to work efficiently.

Hybrid Network Bypass TAPs

The new breed of network TAPs provide an all-in-one connectivity solution by combining the packet broker capabilities that often assists in various functions. Rather than deploying multiple TAPs with many different functions, hybrid network bypass TAPs, like the EdgeLens® from Garland Technology, support filtering, aggregating, regeneration and load balancing all in a 1U box. Hybrid options give network administrators the flexibility they need deliver 100% network visibility to the wide range of security and monitoring solutions they use to ensure performance on a daily basis.

A Connectivity Solution that Maximizes Investments

The first step to getting the most from your security and network monitoring tools is realizing that they need 100% visibility to perform optimally. While some companies attempt to base their connectivity solution on switch SPAN ports, the truth is that packets get lost every time traffic spikes. Instead, a dedicated solution built on network TAPs with full regeneration, aggregation, filtering and load balancing capabilities provides a more reliable solution – one that ensures that all your security and network monitoring solutions performing optimally. When armed with all the data, network administrators can reduce the time it takes to diagnose user-impacting performance issues and today's security systems can't afford to miss packets in an era of constant attack.

A strong network connectivity solution is critical for getting the most out of your monitoring investments over the long term as well. When companies use network TAPs coupled with a packet broker – or better yet a hybrid TAP – they gain the flexibility they need to extend existing assets as the underlying infrastructure evolves. This not only increases ROI on your visibility strategy, but it also ensures the long term value of all the appliances connected to it.

When companies use network TAPs coupled with a packet broker – or better yet a hybrid TAP – they gain the flexibility they need to extend existing assets as the underlying infrastructure evolves.

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 a full line of access products: a network TAP that supports aggregation, 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