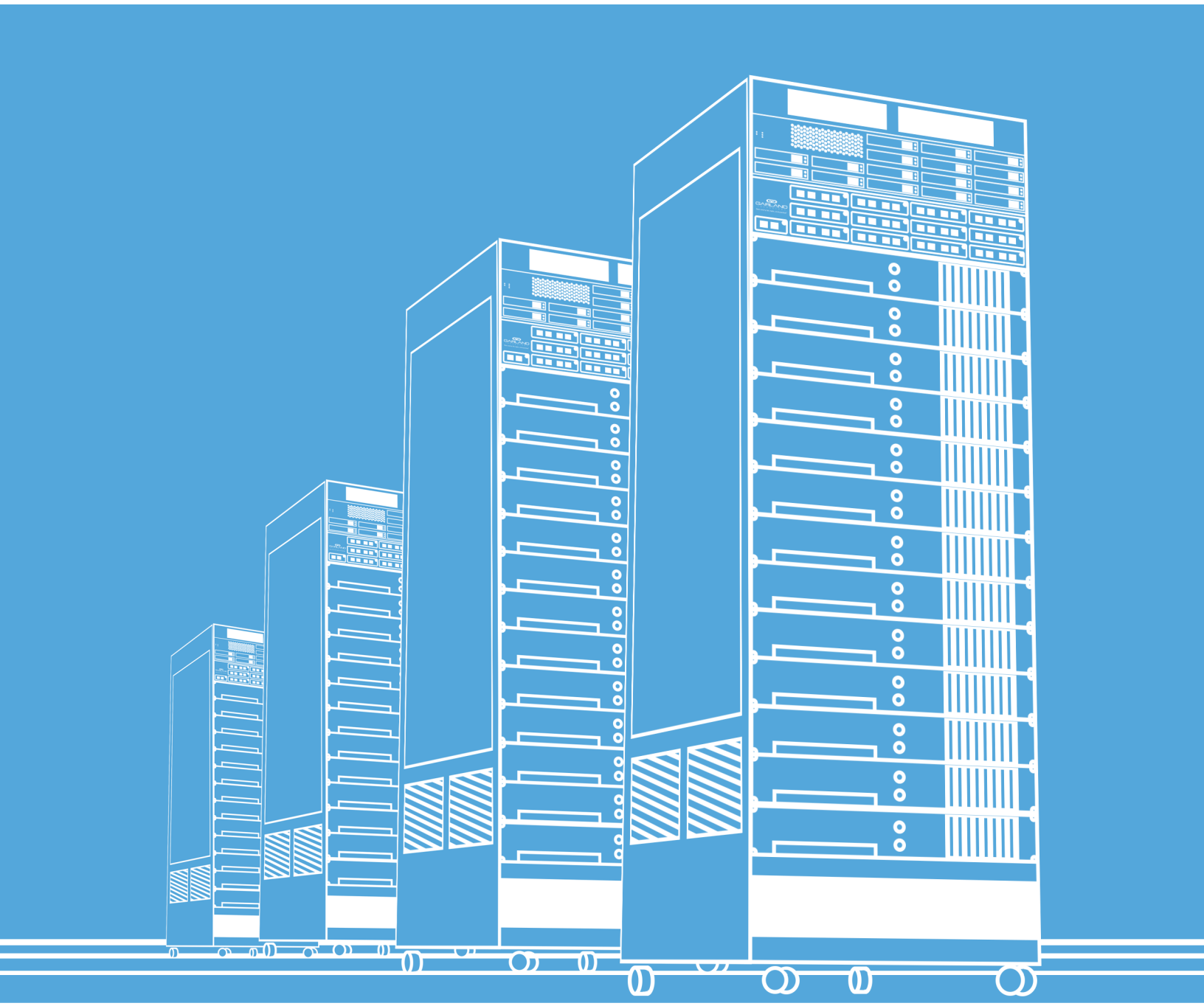
Network TAPs 101

The Networking User Guide



GARLAND TECHNOLOGY

See every bit, byte, and packet®

Table of Contents

Introduction

Providing unfettered access to all of the bits, bytes and packets flowing through a network is a critical piece of network design. Without it, security appliances, monitoring devices and analytical solutions cannot function optimally – a critical issue in a world where downtime or a security breach could cost millions.

Network TAPs

Network Test Access Points or Traffic Access Points (TAPs) were engineered in the 1970s to address this challenge. They were originally designed to passively monitor networks by sending a complete copy of the live network data to analyzers or other monitoring devices.

In the early 2000, a new type of network TAP was invented called the bypass TAP, it came to market to ensure that in-line security devices were able to access 100% of the network traffic data and prevent their failure from causing a complete network shut down.

Since then, the technology has evolved to provide network engineers with stable connectivity solutions for a range of devices and network configurations.

As you follow along, please take note of these icons to help you better remember key concepts.

TAP Tips
Save this info for later when you apply it to your own data.

Remember
Don't forget this information as it is a key concept.

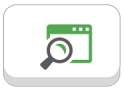
Deep Dive
Want to get technical and nerd out? This is your cue.

Why do networks need to be engineered for connectivity?

The following tools/appliances need a connectivity strategy. The investment in your security and monitoring stack is significant. Ensure your tools receive 100% of the data required to do their job to actively block or passively monitor your network. Afterall, your devices are only as good as the data they receive.

Next-gen firewalls

Intrusion Detection and Prevention Systems



Forensic tools

Web Application Firewall

Security Information and Event Management

Advanced Threat Detection and Anomaly Analyzers

Wireshark tools

Lawful Intercept solutions

Content Filter

Deep Packet Inspection

Application Performance Monitoring

DoS and DDoS Appliances

Packet Capture

Network Monitoring Analyzers

Secure Sockets Layer

Packet Injection

Data loss prevention

Guaranteed vs. Best Effort Connectivity

Today, there are two opposing approaches to network connectivity: SPAN ports vs. network TAPs. Often, non-engineers choose to obtain traffic data from the switch's mirror port or SPAN port because it seems easily available.

In this configuration, the switch makes a copy of the data it transmits and sends it to the connected device. Because "copy-send" isn't the switch's primary function, it is relegated to best-effort when a network spike occurs – an implementation flaw that routinely leads to dropped packets and gaps in security and monitoring programs. Even Cisco, the vendor that first offered SPAN ports as a switch accessory, acknowledges this reality.

"The switch treats SPAN data with a lower priority than to-port data … the best strategy is to make decisions based on the traffic levels of the configuration and when in doubt to use the SPAN port only for relatively low-throughput situations." -*Cisco*

When security and/or network management programs need to see every threat, anomaly and/or issue, only a network TAP can guarantee that level of visibility. The key is finding the solution that best fits your environment, monitoring requirements and budget.

Connectivity 101

Understanding the Network TAP

Simply put, network TAPs are purpose-built hardware devices that can be inserted anywhere into the network to provide connected appliances with an exact copy of the traffic flowing through it.

Since the first network TAP was developed, network technology has evolved – speeds have increased, new protocols have been introduced and high speed fiber optic solutions are quickly becoming the norm. At the same time, companies need a greater number of security and monitoring devices to protect digital assets, maximize uptime and optimize user experience. Network TAP technology has evolved and today there are multiple functional modes to consider when architecting a reliable connectivity architecture:

- **Breakout "Normal" TAPs**: Ensure that no packet is lost to high-priority monitoring tools.
- **Filtering TAPs**: Set rules on what data is filtered and sent to monitoring or security tools. Filtering prevents over subscription.
- **Aggregation TAPs**: Merge traffic streams into one monitoring port to reduce appliance costs, often used in conjunction with filtering taps.
- **Replication TAPs**: Create multiple copies of network data to support multiple devices from a single connectivity point.
- **Bypass TAPs**: Prevents in-line devices from causing a network shut down if they fail or need to be updated.
- **Media Changing TAPs**: Ensure compatibility between networks and connected appliances as technology evolves.

Because networks are continually growing in size and complexity, it's important to consider purchasing multi-function network TAPs. This allows engineers to configure and reconfigure operational modes as traffic levels and device requirements change.

ie. A bypass TAP can be reconfigured to support breakout "normal tap" mode, aggregation and regeneration & SPAN modes.

TAP TIP: Understanding traffic volume is critical to designing an efficient connectivity solution that doesn't oversubscribe the network-to-device connection ports. Next-gen network TAPs offer built-in management tools for alerting administrators when network utilization rates hit a designated threshold, ie: 80% and providing a chance to change modes, use load balancing or filter data to ensure that security, monitoring and analytic programs are not compromised during traffic spikes.

Breakout "Normal" TAPs

A Guaranteed Approach to Analyzing Full Duplex Traffic Streams

As mentioned above, the primary function of any network TAP is to ensure that security and monitoring appliances see 100% of the packets flowing through the network, even during spiked conditions. From a network design perspective, the best way to prevent packet loss is to deploy a breakout TAP with a 2-port tool whose throughput matches that of the network (i.e. a 100mb copper network needs a 2-port 100mb analyzer where a 1GB fiber network requires a 2-port 1GB analyzer).

The breakout TAP requires a device with two network interface cards (NICs) because eastbound traffic streams are sent separately from the westbound traffic stream – it is the tool's job to aggregate and analyze the data as needed.

For example, inserting a breakout TAP between the network router and switch lets engineers analyze every packet that comes in and out of the corporate network.

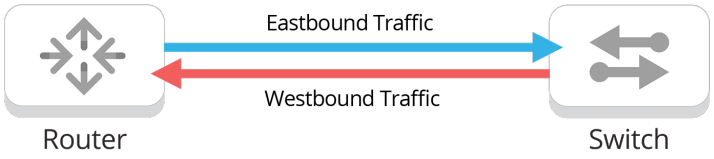


Figure 1: A full duplex network link

TAP TIP: Choose a breakout TAP when the traffic on the attached link is heavy enough to cause oversubscription if the send and receive traffic were aggregated together to one monitoring port.

TOOLS
To TAP

Here, the cable that connects the router to the switch is disconnected and connected to port A on the network TAP. A second cable attaches port B of the TAP to the port on the switch that was originally disconnected. There is no impact on network performance – the eastbound traffic from the router is sent in real-time out of the breakout TAP to the switch and sent to the network interface card (NIC) on the analyzer. The west-bound traffic flows from the switch to the router from port B to A and to the analyzer's second NIC card via port D.

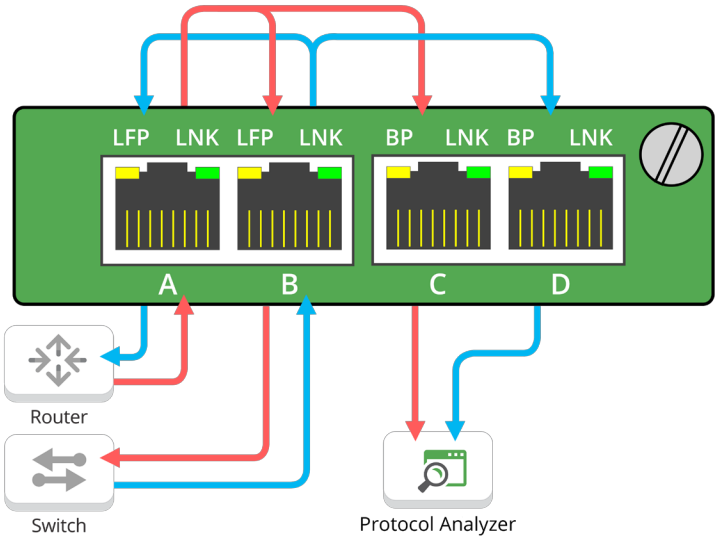


Figure 2: A breakout TAP gives connected appliances access to 100% of the network data

With a breakout TAP and a monitoring tool equipped with two Network Interface Cards (NIC), network engineers can guarantee that the analyzer will see all the network traffic running on that link – even jumbo packets and error packets will be passed along to the analysis tool. In this configuration, the monitoring ports cannot be overwhelmed by traffic spikes as their bandwidth/throughput matches that of the network.

DEEP DIVE: Breakout TAPs deployed in 1 Gigabit copper networks require a power source to push traffic through the network TAP in a copper network. Therefore, it's important to select a solution that automatically closes the network TAP's electric relays to guarantee uptime when the power goes out (the monitor ports no longer forward traffic, but the live link is still operational). Battery-powered network TAPs are not a viable alternative to this type of failsafe as they introduce an additional point of failure that can compromise the entire network, not just the connected appliances. [Click for more]

Filtration TAPs

Streamlining Connectivity Designs

While a network TAP can provide appliances with a complete copy of all the network's data, certain security and monitoring tools don't need to see it all. For example, Wireshark and VoIP monitoring solutions only need to see a fraction of the information in the data stream to be effective. Often times, lawful intercept tools are only allowed to see a portion of the network's activity to comply with a warrant.

TOOLS
To TAP

Filtering is beneficial for any monitoring or security tool to ensure ports are not over-subscribed.

Instead of purchasing a high throughput tool and making it search through the entire traffic stream for relevant data, engineers can use filtration TAPs to cut the cost and complexity of supporting these devices. During set up, the administrator can set up filters to see MAC, VLAN, IP, DSCP, TCP or UDP traffic. Alternatively, they can granularly select data from layers 2, 3 and/or 4 to create sophisticated filtration rules. This approach also ensures that the monitoring ports will not be oversubscribed during traffic spikes.

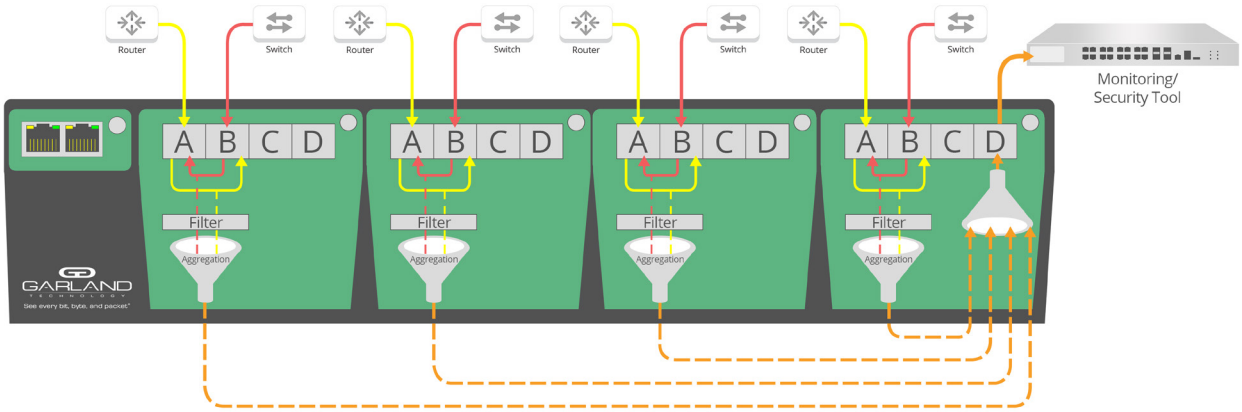


Figure 3: Here, a filter has been applied to four 1G links. The data was aggregated and then sent out via port D on the network TAP to the designated monitoring tool.

When network data is pre-filtered, it gives administrators the opportunity to aggregate data from multiple points in the environment to enrich results and cut the number of devices needed to accomplish IT's security and monitoring goals.

TAP TIP: Leverage port mapping (aka a filtering backplane) to filter/aggregate/send data to certain devices and copy/send 100% of the data to others.

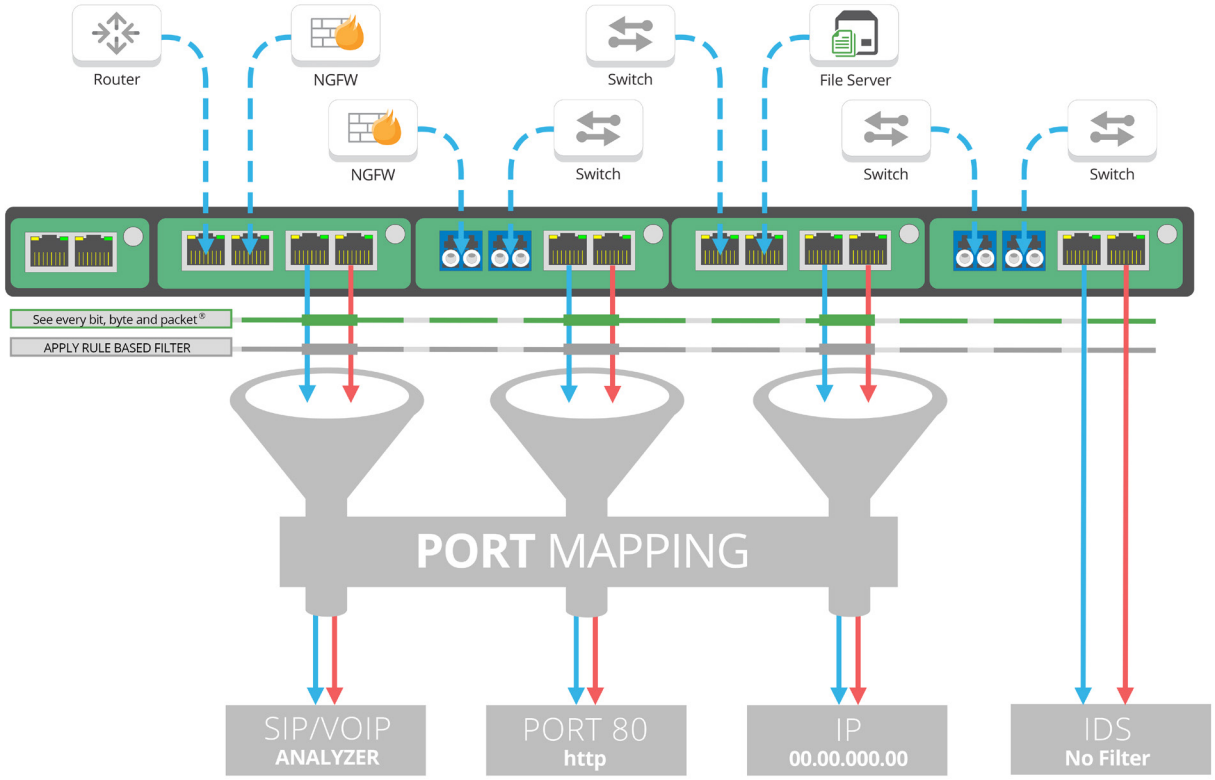


Figure 4: Network TAPs with port mapping capabilities help future-proof network connectivity plans

Aggregation TAPs

Maximizing ROI

Often, network engineers have to accommodate security and monitoring tools that only have one NIC card or input port. Other devices such as lawful intercept and advanced threat defense systems need to see patterns in traffic as it moves across multiple points in the network.

In these cases, aggregation TAPs provide the answer. When configured to operate in aggregation mode, the network TAP can merge eastbound and westbound traffic flows and send it all to the attached devices via a single port. Alternatively, aggregation TAPs can be reconfigured to operate in breakout 'normal' TAP mode if full utilization is a concern.

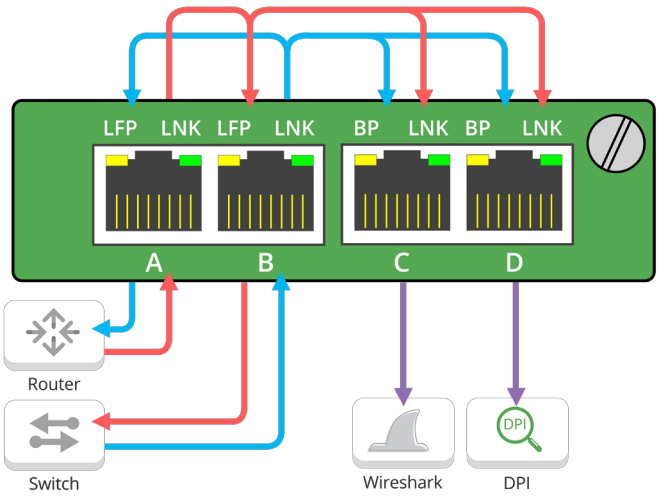


Figure 5: Aggregation TAPs copy data from both directions to support appliances with only one NIC card.

1G COPPER Packet Injection?

The right answer is based on your needs.

No packet Injection - ensures that your device is passive, listen-only for out-of-band monitoring devices.

With Packet Injection - gives you the option of being passive listen-only -or- active, in-band for security devices.

To send a full duplex link between a network router and a network switch to a single monitoring port, disconnect the cable that attaches the router to the switch from the switch end. Connect the switch end of the cable to port A on the aggregation TAP. Use a separate cable to connect port B to the connection on the switch that was previously disconnected. While the network TAP will reestablish the link and traffic will again flow between the two devices, only when powered will the traffic flow to the aggregation ports (C or D).

When configured in this mode, each monitoring port will receive all of the traffic on the link. As an added benefit, engineers can support twice as many tools from the same network TAP.

For tools that need to analyze packets as they travel throughout the network, use a network TAP with multiple input ports. These devices aggregate data from multiple points in complex environments and send it all to connected appliances without data loss, corruption, latency or timing issues.

TAP TIP: While aggregation TAPs provide an important solution to key network engineering solutions, it is important to monitor the system for oversubscription conditions. For example, if the network TAP is inserted in a 1G link, then there is a possibility that each side of the link (send and receive) could have up to 1G of traffic. When you merge the data, you could effectively have up to 2G of traffic going out to the monitoring port. When using aggregating network TAPs, make sure the link is not carrying heavy traffic or a high-throughput device is used at that connection point.

DEEP DIVE: When monitoring network links with heavy traffic, consider using an aggregation TAP equipped with a packet broker to implement filtering and load balancing to distributing traffic across multiple devices. Do not rely on buffering as this only provides a few seconds of relief before dropping packets. [Click for more]

Replication TAPs

Multi Appliance Data Distribution

As security threats increase and network complexities increase, it is clear that engineers need scalability in their connectivity plan. Even those organizations satisfied with the best-effort, copy-send function provided by the switch's SPAN port still need to find a way to support multiple appliances from a single connection.

To solve this problem, send the traffic to a replication TAP which then distributes it out to multiple different tools.

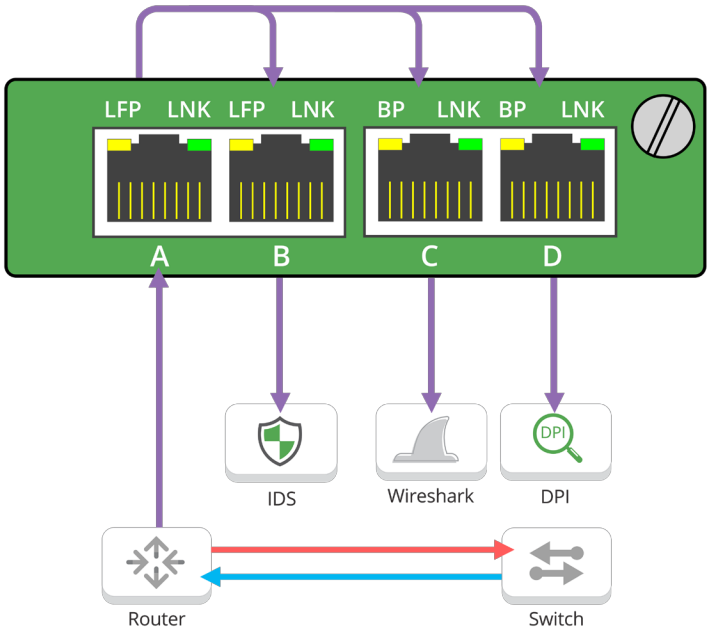


Figure 6: Aggregation TAPs copy data from both directions to support appliances with only one NIC card.

The Bypass TAP

Sophisticated Management for Critical Links

To effectively protect the network against sophisticated threats, security appliances such as next-gen firewalls and intrusion prevention systems need to actively block traffic in real-time to guarantee any malicious activity is detected from the start. To do their job effectively, they must be placed in the path of a critical link. But if the device were to falter for any reason, the traffic along that critical link could stop flowing.

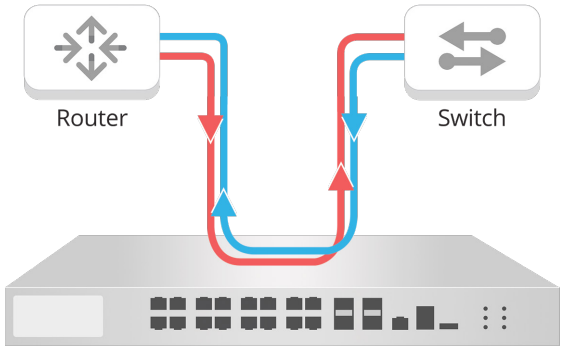


Figure 7: To work effectively, in-line appliances must be inserted into a critical network link (between the router and switch, in front of web server banks, etc).

TOOLS
To TAP

- NGFW
- IDS
- WAF
- DDoS
- DLP
- SSL Decryptor
- Packet Injection
- Packet Capture

The bypass TAP was developed to overcome these issues and prevent in-line appliances from becoming a point of failure within the network. To limit the risk of downtime due to an appliance failure, the bypass TAP sends heartbeat packets to the device along with the link traffic.

As long as the heartbeat packets continue to be returned to the TAP, administrators know that the device is functioning properly (the heartbeat packets are filtered out of the traffic before it continues along its intended path). If the heartbeat packets are not returned – indicating that the device has failed – the network TAP will automatically switch to an out-of-band/off-line mode which will keep the link traffic flowing freely.

While the network TAP is in bypass mode, it continues to send heartbeat packets out to the security appliance. Once the heartbeat packets are sent back to the TAP, it is a signal that the appliance is working again. The bypass TAP then moves the device back to in-line status and directs the network traffic back through it so it can act on the traffic flow in real-time.

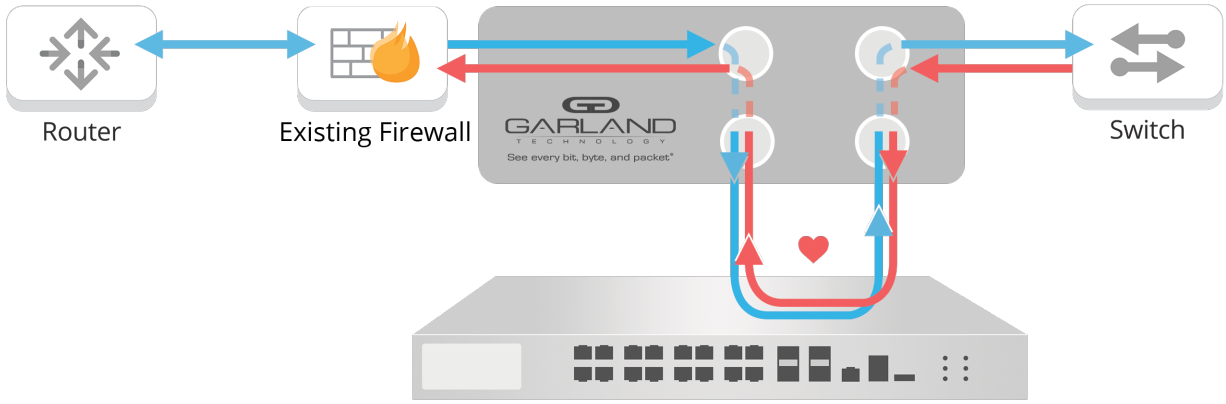
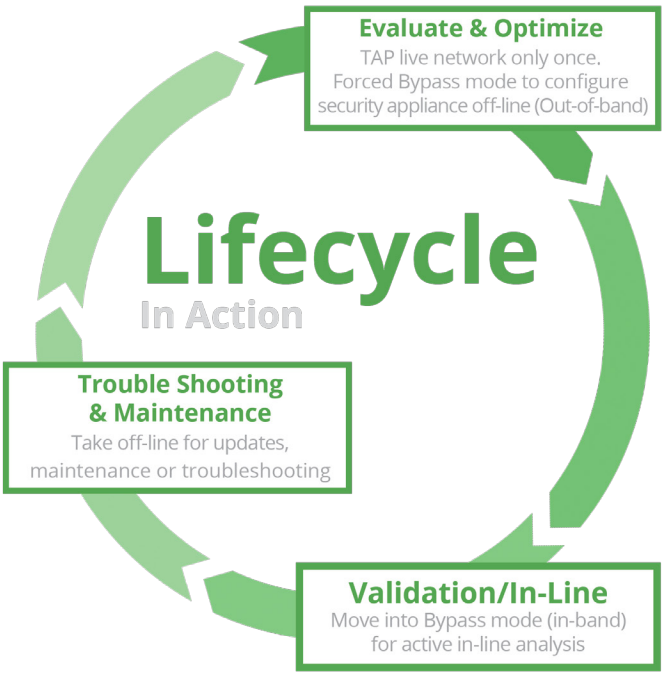


Figure 8: Bypass TAPs were designed to prevent in-line appliances from becoming a point of failure while still providing them with a copy of network traffic for analysis.

The Bypass TAP also gives engineers a solution for simplifying appliance management and to rapidly troubleshoot issues in complex environments. Before its invention, administrators had to shut down the network to deploy, update or troubleshoot in-band devices such as firewalls or intrusion prevention systems. Now, administrators can easily take in-line devices on and off-line without impacting traffic flows.



One of the biggest challenges engineers face is ensuring performance as more and more security appliances are allowed to interfere directly in traffic streams to isolate malicious packets. Often this can have an unforeseen impact on other applications, especially when new software and firmware updates are uploaded. Rather than spend days trying to find root cause in complex environments, administrators can simply switch the appliance to an out-of-band mode and see if the issue resolves itself or requires further investigation.

With a Bypass TAP, network engineers not only maximize uptime and eliminate points of failure, they increase the efficiency of their corporate security and network management by ensuring that firmware and software updates are made as quickly as possible.

TAP TIP: When deploying new appliances or upgrading existing tools, set them up in bypass (offline) mode to work the kinks out before moving them on-line. This helps isolate issues from the start and minimizes downtime and disruption for network users. To ensure safety on critical links, it is wise to utilize a back up security appliance to take over while primary appliances are being updated.

Media Changing TAPs

Normalizing Connectivity between Networks and Tools

Often times, network engineers need to find a way to accommodate security and monitoring appliances whose configurations don't match that of the network. For example, lawful intercept devices originally purchased for copper environments cannot be automatically transferred to multi-mode fiber networks. The same is true for using single-mode fiber tools in multi-mode fiber networks.

With the right media changing TAP, you can normalize connectivity between the network and the appliance without losing packets, creating timing issues or introducing latency issues.

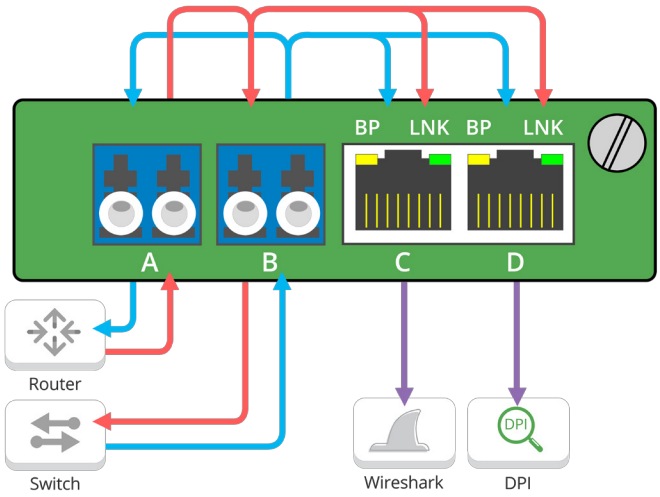


Figure 9: A media conversion TAP for converting a single-mode fiber link to copper

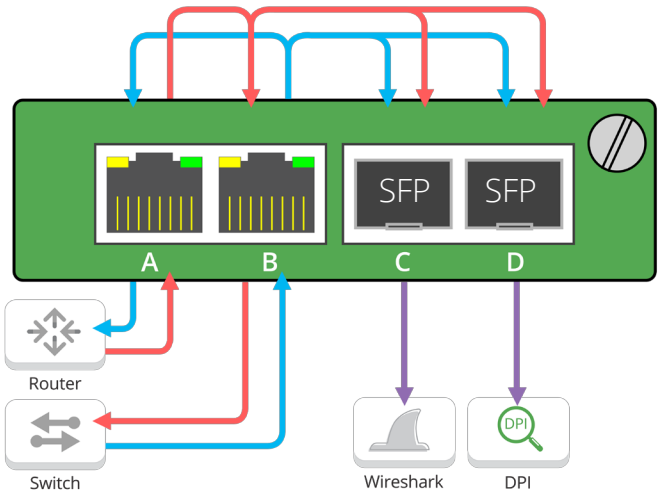


Figure 10: A media conversion TAP for converting copper over to multi-mode fiber

Environmental Considerations

Passive and Active Network TAPs

While network TAPs offer multiple functional modes (breakout, filtration, aggregation, etc.), there are also technical issues to consider when optimizing the network-tool connection.

As we discussed previously, TAPs can support copper or fiber networks and tools. You can also use taps to convert media.

Passive vs Active TAPs

In general, passive TAPs are used with monitoring tools and typically don't require power. Passive TAPs are available in copper and fiber.

Active TAPs are always powered and were designed to support in-line security applications. Active TAPs are also available in both copper and fiber.

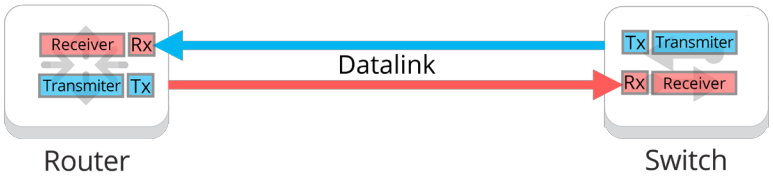
Passive Network TAPs

In general, passive network TAPs are defined as connectivity solutions that will not cause connected monitoring devices to lose their link in the event of a power failure. Used to support out-of-band tools, a passive TAP simply makes a copy of the network data and distributes it to appliances – they don't take altered traffic back from the device and resend it through to the network. Only an active network TAP can support those functions.

Passive network TAPs offer a key advantage – they typically don't require power to provide basic copy/send functions. This network design offers tremendous advantages for companies with crowded wiring closets and limited outlet availability. Additionally passive TAPs are not able to accidentally inject data into the network as the data only flows to the desired monitoring device(s).

Depending on the environment, there are variances in passive network TAPs that engineers need to understand.

TAP TIP: A standard passive network TAP operates in breakout 'normal' mode – sending eastbound traffic on one stream and westbound traffic via another stream. If the connected device only has one available port or NIC card, select a network TAP able to operate in aggregation mode. The TAP will have to be powered to work in this mode.



Passive TAPs

In Fiber-based Networks

Passive network TAPs can be used in fiber networks of all speeds, simply choose a model rated to copy/send data at the environment's transmission rate (1 Gigabit, 10 Gigabit, 40 Gigabit, 100 Gigabit, etc.). If that's all that the network TAP has to do – and there is enough light available in the fiber to split it without degrading network conditions – there is no need to power a passive TAP at all.

What is Split Ratio? A split ratio is the amount of light that is redirected from the network to the monitor ports on a passive fiber optic network TAP. To determine the correct split ratio, a loss (power) budget should be calculated (more on that later). A 50/50 split ratio would indicate that 50% of the light budget coming into the TAP from the network is passed along to the end device, and 50% of the light budget is diverted to the monitoring device. To understand how this goes as you change the ratio, for a 70/30 split ratio, 70% of the light budget is passed along to the end device and only 30% of the light budget is passed along to the network monitoring device. [Click for more]

How to Calculate Loss Light Budget: A loss light budget is the amount of attenuation that can be tolerated on the network and monitor links before the end-to-end data is corrupted. To calculate this, you must know the following network link characteristics:

- Link distance
- Fiber type
- Launch power
- Receiver sensitivity
- Number of interconnects and splices

TAP TIP: When connecting an appliance with copper input ports to a fiber-based network, use a TAP with media conversion capabilities. These devices can also be used to reduce costs as they let engineers use a single mode fiber to carry traffic from a multi-mode fiber network to the device. Again, the passive TAP will have to be powered to work in this mode.

Passive TAPs

In Copper-based Networks

While a passive network TAP can be used in any fiber-based network, it's not that straightforward in copper environments. First, passive TAPs used in copper networks must always be powered. Additionally, they can only be deployed in 10/100 Base-T networks – they cannot function properly in copper gigabit environments.

TAP TIP: To enable connectivity in copper gigabit environments, use an active network TAP.

TAP TIP: When using powered passive network TAPs, choose one equipped with fail-safe relay circuitry that will not cause a network failure when power is disrupted. To ensure reliability deploy all your networks TAPs via a rack outfitted with dual Uninterruptible Power Supplies (UPS).

Active TAPs

Active network TAPs were designed to support in-line security applications, such as next-gen firewalls, anti-malware devices, intrusion detection systems and more. These security systems are unique because they take in traffic from the outside world and act on it – attempting to block suspicious communications from getting inside the company.

Naturally, these appliances require a network TAP that can feed them all of the network traffic without losing packets – but they also need a solution able to accept the authorized traffic as well as messages from the appliance and ensure that 100% of it travels to its intended destination. Only an active network TAP can facilitate this type of communication.

TAP TIP: All connectivity solutions for Gigabit copper networks require an active network TAP to function properly. Because data is simultaneously transmitted over the copper pairs in these environments, the two endpoints on the device must link to the network TAP, regardless of the application.

Unlike best-effort connectivity solutions, a properly configured active network TAP guarantees that in-line appliances see every bit, byte and packet in the traffic stream. Active network TAPs can support breakout "normal," filtration, aggregation, bypass and media conversion modes.

TAP TIP: Because all active network TAPs require power to function properly, choose a device with fail-safe circuitry to ensure that traffic continues to flow during a power outage or appliance failure.

TAP TIP: Use active network TAPs in bypass mode to migrate threat risks by ensuring that front-line security appliances remain active. More importantly, it gives administrators the ability to move appliances to out-of-band status to quickly and effectively make the updates that let security solutions immediately respond to new threats.

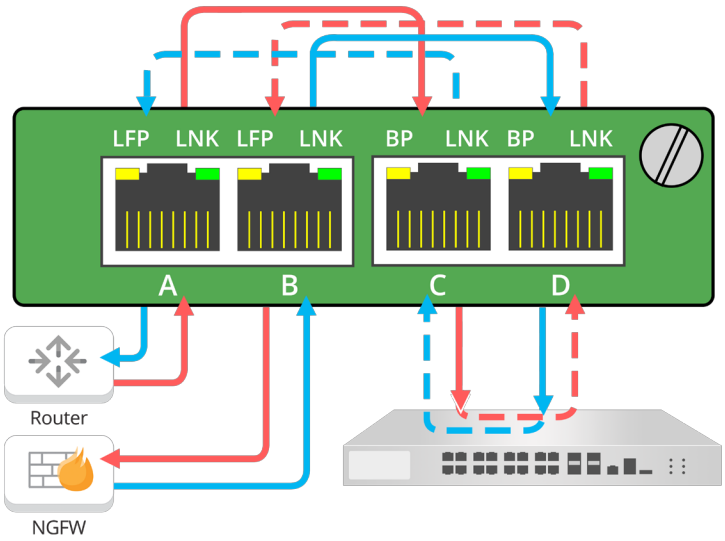


Figure 11: Supporting in-line devices using an active TAP in bypass mode simplifies administration and speeds security updates.

Managing Connectivity

When network TAPs were first designed, they were purpose-built, hardware-only solutions that provided a copy of the data for monitoring tools. As they evolved, network engineers came to rely on them to intelligently mitigate the effects of traffic spikes.

Forward-thinking vendors have added management tools to give administrators more control over the network TAPs deployed throughout their organization. They let users reconfigure network TAPs to operate in the mode that best supports the connected appliance. More importantly, administrators can take action or implement automated rules when link utilization rates spike to ensure that security and monitoring tool never miss a single packet.

Engineering End-to-End Visibility

Too often, network connectivity plans are limited to the company's LAN/WAN connection point. Certainly, this provides key visibility into the performance issues and security problems that occur at the intersection of the public and private networks. But as IT becomes increasing complex, many engineers are inserting network TAPs throughout their environments to secure all of their digital assets, speed up troubleshooting and gain the insights needed to optimize performance across the organization.

Today there are basically two types of architectures – one with native network access options capable of properly supporting any monitoring, troubleshooting or security device that the company needs and another that has to scramble to find connectivity whenever any new project starts or a performance issue crops up.

Instead of having to scramble to find connectivity for every new initiative, consider adding visibility points into the network design to analyze:

- eCommerce and web servers
- VoIP and real-time communication applications
- Data center server banks
- Dedicated connection to cloud service providers

TAP TIP: Typically, network TAPs represent less than 5% of the cost of the supported security appliances and network analyzers. Use them throughout the environment to maximize ROI on IT investments and ensure that they are able to operate optimally.

FOOTER: To work effectively, network connectivity plans must be designed for the organization's unique environment, security protocols and monitoring requirements. For a customized solution, contact the network designers at Garland Technology and start white boarding your design today.

Want to Dive Deeper?

The content for this eBook was redacted from Garland Technology's 101 Network Tap series. The 101 Network TAP series is an educational outreach blog that provides fundamental information on network connectivity for a variety of monitoring, security and analytical deployment scenarios. The following are the original source blogs for the 101 series, as well as expanded content for Deep Dives and TAP Tips.

Visit The 101 Blog Series online at:
GarlandTechnology.com/blog/topic/the-101-series

Or click title below:

- A Primer on Network TAPs
- Breakout 'Normal' TAPs
- Filtering network TAPs
- Aggregation TAPs
- Replication/Span TAPs
- Bypass TAPs
- Media Changing TAPs
- Passive TAPs
- Active TAPs

Additional resources:

- 1G Copper Network Considerations
- Aggregation and Filtering Tips for Heavy Utilization
- Split Ratio and Budget Light Loss

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

See every bit, byte, and packet®

New York + Texas + Germany | GarlandTechnology.com | sales@GarlandTechnology.com