3 KEYS TO NETWORK RESILIENCY

A GUIDE TO AVOINDG NETWROK DOWNTIME

WHITEPAPER

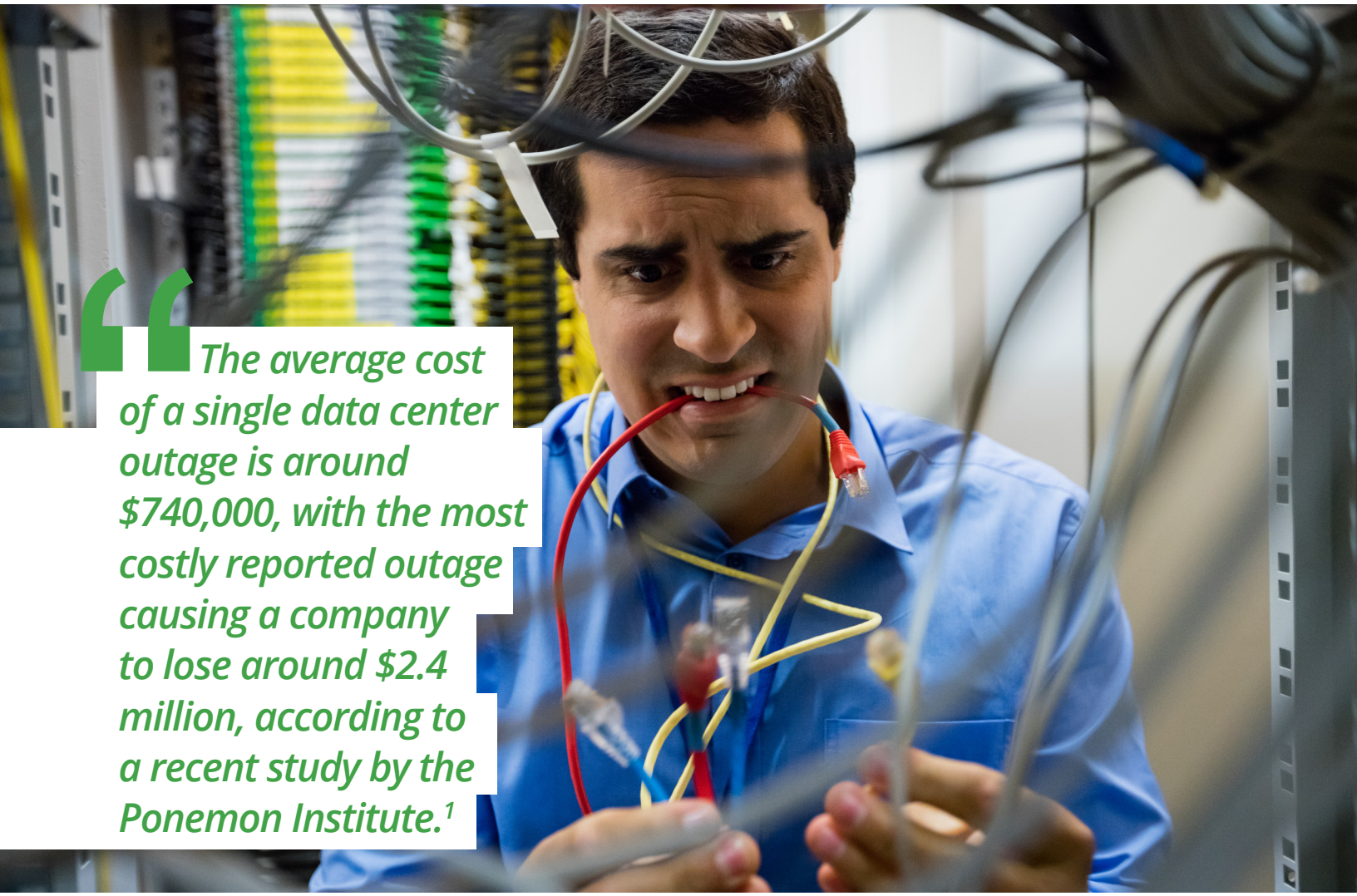
GARLAND TECHNOLOGY

See every bit, byte, and packet®

Network Resiliency | Table of Contents

What is the cost of network downtime?

In today's economy, businesses must be constantly available and capable of handling requests in order to survive. Network downtime prevents that availability, negatively affecting both revenue generation and a company's brand reputation. When the network is not running at its highest performance, companies can expect to lose tens to hundreds of thousands of dollars an hour.



> *The average cost of a single data center outage is around $740,000, with the most costly reported outage causing a company to lose around $2.4 million, according to a recent study by the Ponemon Institute.[1]*

The stakes couldn't be higher for some companies when architecting and managing critical infrastructure, As an example, Delta Airlines experienced a three day outage, grounding 2,000 flights, and resulting in an astonishing $150 million loss for the company.[2]

1 - Cost of Data Center Outages, January 2016, Ponemon Institute
2 - Delta: Data Center Outage Cost Us $150M, datacenterknowledge.com

Understanding your points of failure

When architecting your inline security network, it is critical to work through your failure and recovery scenarios. The first step is understanding where your failure points are, and how to minimize them.

The constant tug of war between network security and downtime is real. Inline tools designed to inspect and block threats in real time, such as Firewalls, Intrusion Prevention System (IPS), and Data Loss Prevention (DLP), must sit on the live network circuit. If you are deploying inline security tools, this creates a single point of failure (SPOF) in the network. When you continue to deploy more inline tools, more potential points of failure are created.

Diagram 1. Three inline tools on a live network, illustrating a failure.

Should the inline tool become unavailable for any reason such as power loss, traffic congestion, or processing errors, it will bring down the network and create general connectivity problems on the production network.

Ensuring your company's ability to generate revenue starts at the design of the network. When architecting your inline security tools into your network, incorporating bypass and failsafe technology together with network redundancy are three fundamental best practices to avoid costly network downtime.

Note:

A single point of failure (SPOF) is a potential risk either from a flawed design, configuration or system failure that brings the network down. These can be power outages, appliance failures, software failures, maintenance windows, or application bottlenecks from improperly designed architectures.

1 Bypass Technology

Bypass technology is a critical part of inline security design. When active security tools were first introduced, they would sit directly between the router and the switch, which in turn created a possible point of failure on the production network link. Bringing the link down for maintenance quickly stopped becoming a reality as 24/7 uptime became a critical requirement for modern networks.

Back in 2001, Jerry Dillard, CTO for Garland Technology, was a network engineer for an early IPS vendor. As the mission-critical functions of the tools helped to secure networks, the team knew that a failure of the inline appliance would immediately cause a complete shutdown of a client's network. So Dillard was tasked with finding a solution, where he developed the technology that would be used worldwide as "bypass technology."

> ***"Knowing the loss of time and money was unacceptable, I designed the network bypass TAP. This elegant solution continuously checked the health of the device and ensured the integrity of traffic flows regardless of their condition."***
>
> -Jerry Dillard

Bypass is exactly what it sounds like. In the event an inline device becomes unavailable, it is bypassed and traffic is automatically forwarded around the failed tool, keeping the link up.

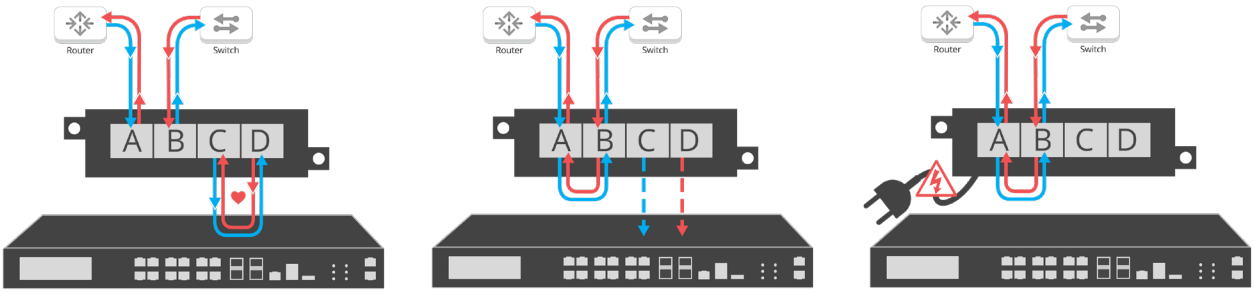
There are two basic approaches to bypass, an external, hardware-based standalone solution and an internal, NIC-based solution embedded in the appliance itself.

Both options provide a direct connection to network traffic flows and they can both be failsafe – if the power goes out, the live traffic still continues to flow. But that's where the similarities end. If there is a software malfunction or configuration error, the inline device could still pose a single point of failure. An external bypass prevents that possibility, while also providing a host of benefits we will go over.

How does a Bypass TAP work?

Typically, a network TAP (test access point) is a device that creates a 100% full duplex copy of network traffic. The Bypass TAP functions differently than other types of TAPs. Instead of generating copies of the monitoring links, the monitoring ports are used to bring a connected appliance inline without the appliance physically connecting to the surrounding network devices.

These external Bypass TAPs provide additional functionality that is not incorporated in bypass interfaces within a tool. Some vendors claim failsafe capability within the native network interfaces of their tools, but those mechanisms usually work only in the event of a full power loss to the device. There is no protection for the production network should the tool simply become congested or suffer a software failure that might impede the processing of network traffic. The combination of failsafe on the network ports and the heartbeat functionality of a TAP provides an additional layer of fault tolerance.



① Bypass Mode Inline ② Out-of-band Tap 'Breakout' Mode ③ Failsafe

The Bypass TAP monitoring ports (Diagram 1, ports C & D) are used to bring a connected appliance inline without the appliance physically connecting to the surrounding network devices. In the event an inline device becomes unavailable, it is bypassed and traffic is automatically forwarded around the failed tool (Diagram 2), keeping the link up.

In addition, bypass TAPs are also equipped with failsafe functionality on their network ports (Diagram 3, ports A & B), ensuring the link stays up.

Heartbeats Monitor the Health of Your Inline Tool

Heartbeat packets are a soft detection technology and operate bidirectionally. They are configured to monitor the health of the connected device. Instead of relying on the direct connectivity of the network to the tool, the bypass TAP is purpose-built, designed specifically to send packets to an inline tool as well as return traffic from those tools to the network. The bypass TAP is able to leverage heartbeats in order to detect a failure if there is a problem with the tool. When a heartbeat fails to return from the device connected to the monitor ports the bypass TAP will fail-open or fail-close, either bypassing the tool to keep the link up or closing it in order to not let unmonitored data through the network.

Heartbeat Note:

While an appliance is connected inline, the Bypass TAP will send heartbeats (ARP request) at a configurable rate on both monitor ports [C&D] to the inline appliance.

An appliance operating in a transparent fashion will forward the heartbeat to the opposing monitor port on the TAP, which will then silently consume the heartbeat packet. If the heartbeats are received by the Bypass TAP within the configured interval, the links are deemed to be up and the inline appliance is capable of responding. If too many heartbeats fail to return, the Bypass TAP considers the inline appliance to be down and engages Bypass into Out-of-band tap 'breakout' mode.

Benefits of Inline Bypass TAPs

When Deploying and Managing your Inline Appliance

We went over how bypass technology works, but how and why should you use it?

It's simple. An external Bypass provides the ability to see the network without being on the network. In other words, the ability to manage your inline tool any time without having to take down the network or impact business availability for maintenance or upgrades. This provides peace of mind without network downtime.

In the tense moments of unplanned downtime, a bypass TAP provides expedited problem resolution in the event of a tool failure. By not impacting the overall availability of the connected network, administrators can focus on fixing the tool rather than having to manage the related symptom. A bypass TAP offers flexibility to bypass the tool and keep the network up, failover to a redundant link, or leverage an HA solution.

During planned downtime, inline lifecycle management allows you to easily take tools out-of-band for updates, installing patches, maintenance or troubleshooting to optimize and validate before pushing back inline.

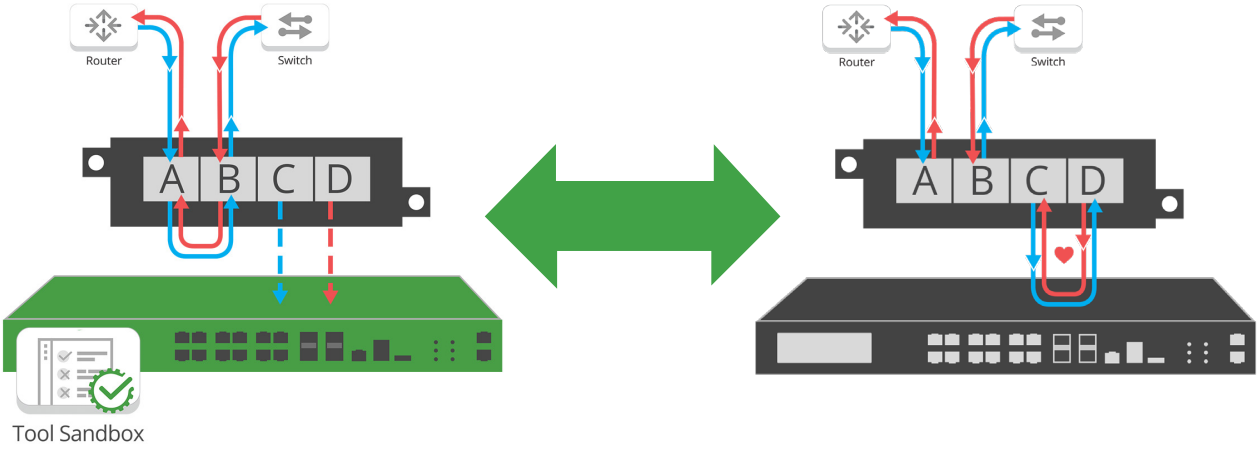
Bypass benefits include:

- **Administrative isolation** - No maintenance windows
- **Operational isolation** - Expedited problem resolution of unplanned downtime without impacting general network connectivity
- **Network resilience** - Flexibility to bypass the tool and keep the network up, or to failover to a High Availability [HA] solution
- **Deployment efficiency** - Extend the reach of the same tools into multiple network segments, when used in conjunction with a network packet broker.
- **Tool Sandbox** - Pilot or deploy new tools

Tool Sandbox
How to Optimize Your Security Strategy

One very useful benefit of an external bypass is the ability to sandbox or pilot new tools in your real environment with live packet data, without impacting the availability of the network. This provides the ability to evaluate and optimize the tool out-of-band, before deploying it live inline in your network. The tool being tested is also exposed to the same type of data it would be monitoring for a production deployment, which increases the confidence of the piloting being performed.

Tool Sandbox [Pilot or deploy new tools]



- **Evaluate & Optimize** the tool out-of-band
- **Validation** - Push active inline
- **Troubleshooting** & Maintenance

Diagram 2. Managing multiple inline devices, while sandboxing a new tool

IPS Use Case

Consider an Intrusion Prevention System (IPS). Having the IPS sit inline between a router and switch will allow it to inspect all the ingress and egress traffic on the network. If the IPS is physically connected between the router and switch, it has the potential to bring the network link down if it fails.

Diagram 3. Taking an IPS inline and out-of-band using a bypass TAP

By using a Bypass TAP, the TAP itself will establish the connection between the router and the switch and the IPS will connect to ports C and D on the Bypass TAP. All traffic entering Port A will come out Port C and into the IPS. After the IPS inspects the traffic, it will send the traffic to Port D which will then forward the traffic out Port B toward the networking device.

2 Failsafe Technology

How Failsafe Prevents a Single Point of Failure

While bypass protects the network against a failure of the inline device, failsafe refers to the concept of a device's ability to fail-to-wire in the event of a power failure.

In the event of a failure of the Bypass TAP itself, failsafe will engage to keep network traffic flowing, preventing a potential point of failure. Bypass TAPs fully ensure that neither the TAP nor the inline appliance will be a single point of failure (SPOF) in the network.

Failsafe in Copper TAPs

Copper TAPs utilize a relay with a default state that connects the networking ports together. When power is added to the TAP (diagram 5), the relays open to allow traffic to flow into an internal ethernet switch that copies traffic over to monitor ports set in breakout, aggregation, regeneration, or bypass configurations. When power is cut off, the relays return to their default position where the network ports are directly connected to each other. In turn, keeping the network links up (diagram 4), like there is not a device there.

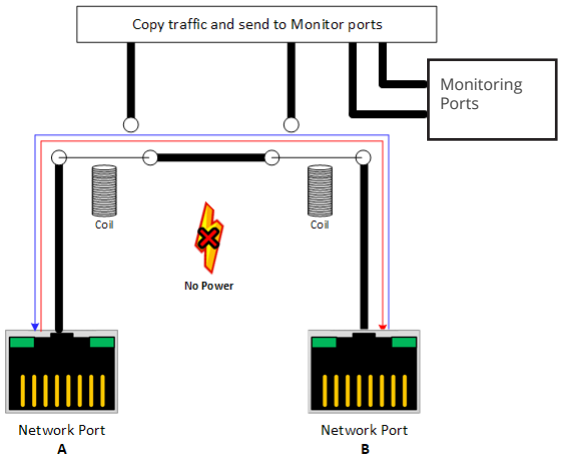


Diagram 4. Default state

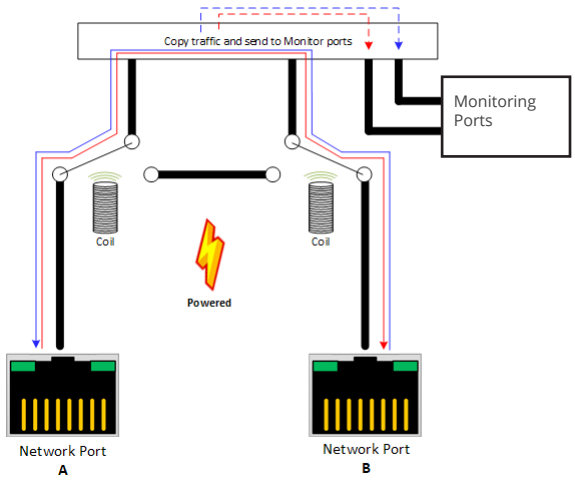


Diagram 5. Powered state

Why Gigabit Copper TAPs are Active

Gigabit copper connections negotiate with each other to decide which connection's timing uses voltage or not, while determining the traffic coming in on each lane. Power is required to accomplish each of these steps, making them an active, not a passive device. When traffic flows over a gigabit copper cable, traffic flows in each direction simultaneously. Each connector puts a certain amount of voltage on each wire to send a pair of bits. The connector knows how much voltage it placed, so by subtracting the voltage it added to the line, the connector uses the remaining voltage to determine what data was sent to it.

While each gigabit copper connector will run at 125 MHz, the timing of this clock speed must match to ensure signals are sent and received on each side when expected. To reach a synchronized state, the gigabit connections poll each other to elect a connector's clock as the master clock. In the case of failsafe copper TAPs, the TAP will ensure its clock's timing is the one each physical connector synchronizes to.

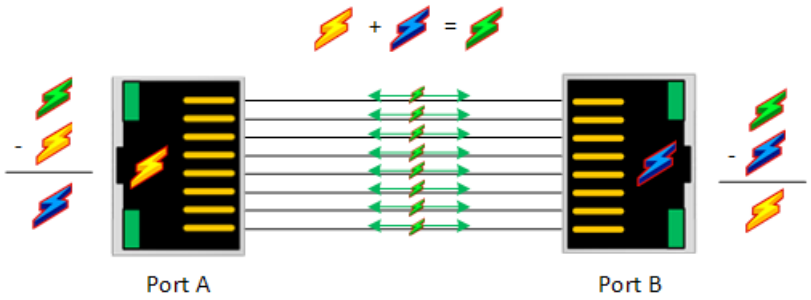
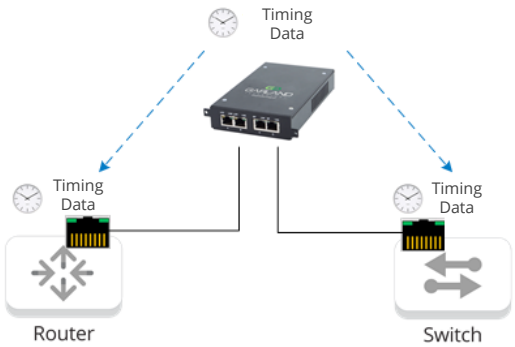


Diagram 6. Voltage on a copper wire

Once the TAP has synchronized the timing of the gigabit connections, Failsafe can be achieved as traffic will remain synchronized in the event the TAP losses power and fails open.



Failsafe in Passive Fiber TAPs

Passive fiber TAPs accomplish failsafe in a truly passive manner: no power is needed to pass traffic. Since fiber cables transmit light signals instead of electrical current, optical splitters are used instead of relays.

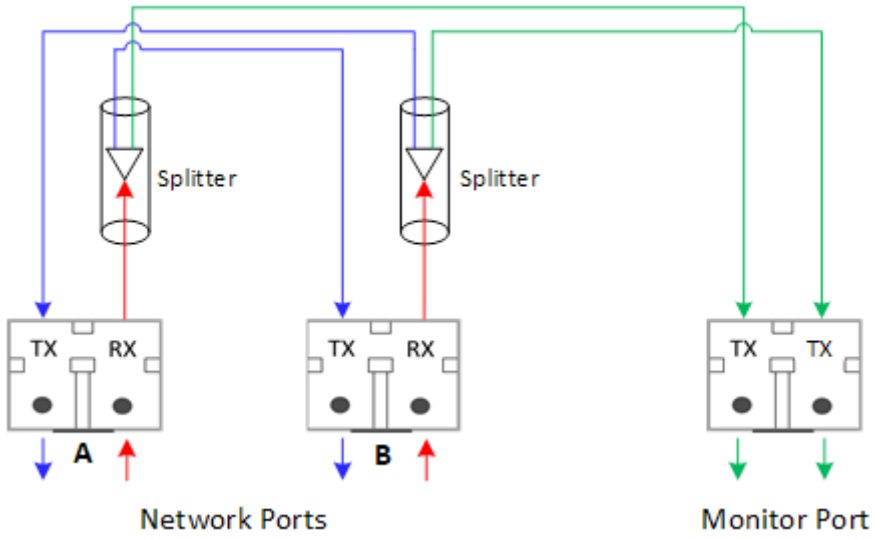


Diagram 7. Fiber breakout mode network flow

With a splitter, light coming in will travel through a prism and be split into two separate signals that are exact copies of each other. When light is split in this way, the signal will be reduced due to insertion loss. This loss of signal strength can be mitigated by selecting the appropriate split-ratio for the environment. Since splitters are only passing light, power is not required for the network ports to be directly connected to each other, effectively keeping the network links up, like there is not a device there.

Failsafe in Aggregation, Regeneration and Bypass

If a Fiber TAP is aggregating the light signal, providing regeneration over multiple ports, or injecting heartbeats into the traffic, power will be required. While the splitter is still directly connecting the network ports together, the signal will need to traverse an optical switch and get processed before exiting through the monitor ports.

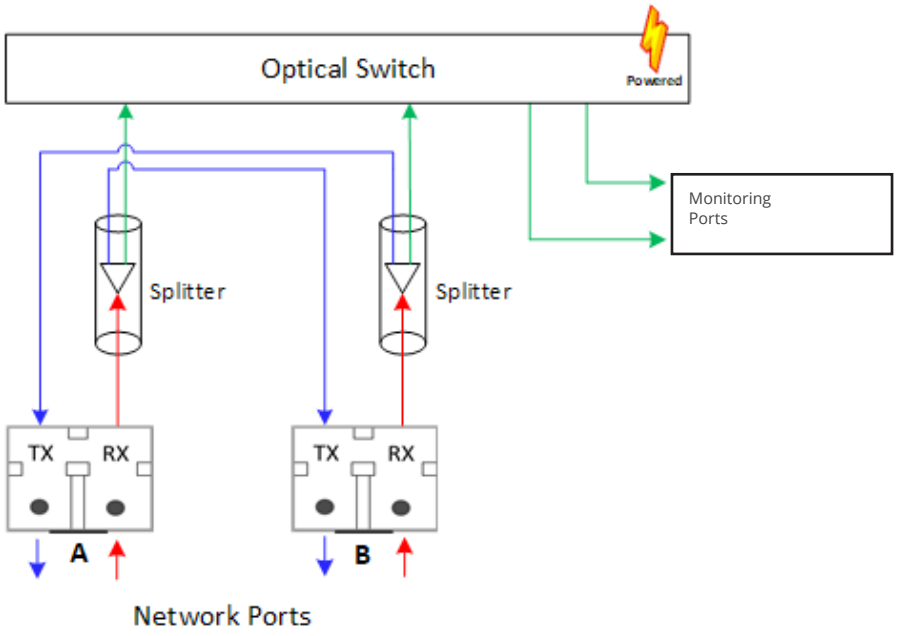


Diagram 8. Fiber aggregation, regeneration and bypass mode network flow

If the TAP loses power, the monitor ports will cease forwarding traffic, but the network ports will continue to pass traffic as normal.

3 Network Redundancy

Along with incorporating network bypass and failsafe technology into your security architecture, adding network redundancy whenever you can is the third fundamental best practice for ensuring uptime for critical network links. A visibility architecture including bypass does not replace traditional network design concepts. Bypass fits into the existing ecosystem rather than changing the fundamental way resiliency is usually delivered through good network design.

Standard bypass has one monitor path, that simply answers 'Do I forward packets, do I not forward packets?' High Availability adds a layer of intelligence 'Do I use my primary monitor path, or do I use my secondary monitor path [through redundant tools or network packet brokers]?'

Redundancy is often achieved by installing primary and secondary devices across the network. While extremely effective, this method is expensive and may not be a fiscally available option for some companies. Here are a few redundant deployment scenarios to consider to bolster the resiliency of the network and avoid lost revenue.

Deploying a Secondary Tool

HA Bypass TAPs can connect two inline appliances in a Primary / Secondary or an Active / Standby design. With these kinds of Bypass TAPs, a single network link can connect to redundant tools without adding additional complexity or a new point of failure to the network. In these single link situations, the Bypass TAP will send live traffic from the network to both tools. One tool will be the primary or "active" appliance and the TAP will bring that appliance inline. The secondary or "passive" appliance will still receive live traffic, but the Bypass TAP will not forward traffic from the secondary appliance on to the network. This provides "Hot Standby" redundancy. In the event the primary appliance goes down and the heartbeats stop being received by the TAP, the secondary appliance will immediately take over as primary and be brought inline by the Bypass TAP.

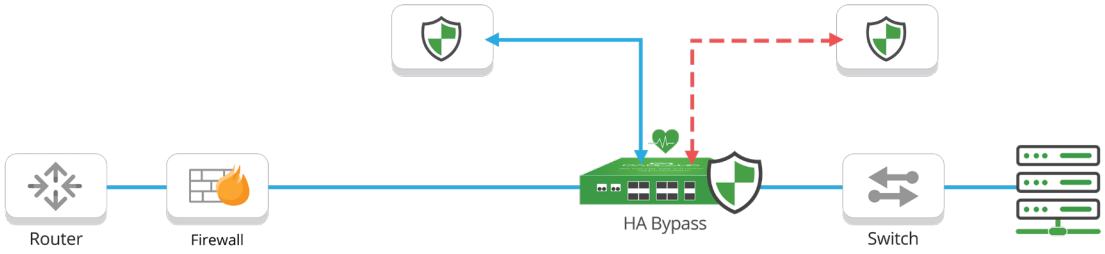


Diagram 9. High Availability (HA) solution for Active/Passive, provides failover from primary device to backup appliance

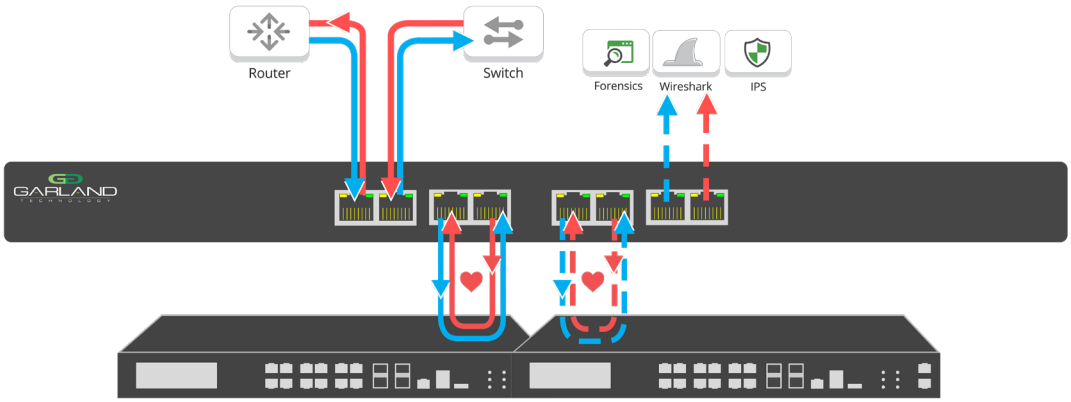


Diagram 10. Garland Technology's Integrated bypass offer's an active/passive solution

Deploying to a Redundant Link

In situations where redundant network links exist, a similar TAP design can be used, but this time the redundant appliances are cross-connected between the two HA Bypass TAPs. When setting up this Active / Active design, each redundant tool should be the primary appliance for each link, usually resulting in asymmetric routing. If an appliance goes down, the network link's traffic will fail-over to the secondary appliance, allowing all the traffic to be seen by the remaining active appliance. Using a bypass TAP in this scenario gives the appliance visibility to both directions of the conversation even when asymmetry is present, which only serves to improve the usefulness of the connected appliance.

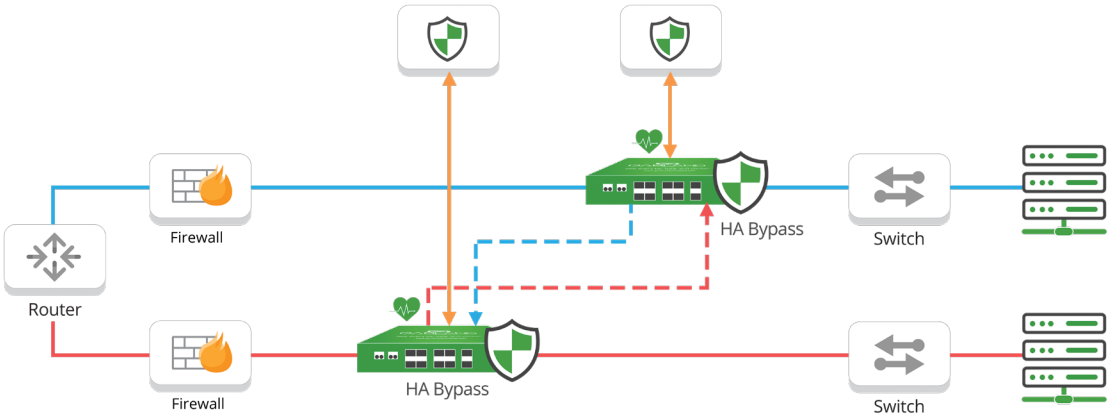


Diagram 11. High Availability (HA) solution for Active/Active, provides failover if either active device fails.

Redundant scenarios can be accomplished through HA bypass TAPs directly managing the inline tools, or in more robust architectures, coupled with network packet brokers, providing an additional layer of distribution.

Conclusion

Inline tools are now critical weapons in securing modern networks. But as reliable as their applications are for network protection, the threat of downtime is just as great.

We covered two fundamental best practices for mitigating single points of failure in the network by incorporating bypass and failsafe technology. In addition, we also went over ideas for creating network redundancy and next-gen options for managing your inline tools to avoid costly network downtime.

Using Bypass TAPs on inline appliances will not only increase the resiliency of the network, but will also provide functionality to expedite troubleshooting and shorten maintenance windows.

When architecting your inline security network, it is critical to work through your failure and recovery scenarios. Strictly focusing on architectural scenarios, for example, if you are load balancing between two tools properly, or how many links you are able to aggregate, opens yourself up for network downtime.

'What happens when a component fails?' 'What is the repercussion?' 'What happens when the network comes back up, does the system absorb eloquently and return to normal operations?' A redundant bypass architecture should be set up to recover in milliseconds, not seconds, minutes or longer. Answering these questions will help you establish not only a successful architecture, but a network security strategy that's designed with resiliency in mind.

Setting yourself up for network resiliency success

Want to learn how we can help you implement resiliency best practices? **Book a free Design-IT** consultation and one of our engineers will work directly with you on designing your network monitoring strategy.

Garland Technology is an industry leader delivering network products and solutions for enterprises, service providers, and government agencies worldwide. Since 2011, Garland Technology has developed the industry's most reliable test access points (TAPs), enabling data centers to address IT challenges and gain complete network visibility. For more information, or learn more about the inventor of the first bypass TAP, visit: GarlandTechnology.com or @GarlandTech.

Contact

sales@garlandtechnology.com

GARLAND TECHNOLOGY
See every bit, byte, and packet®