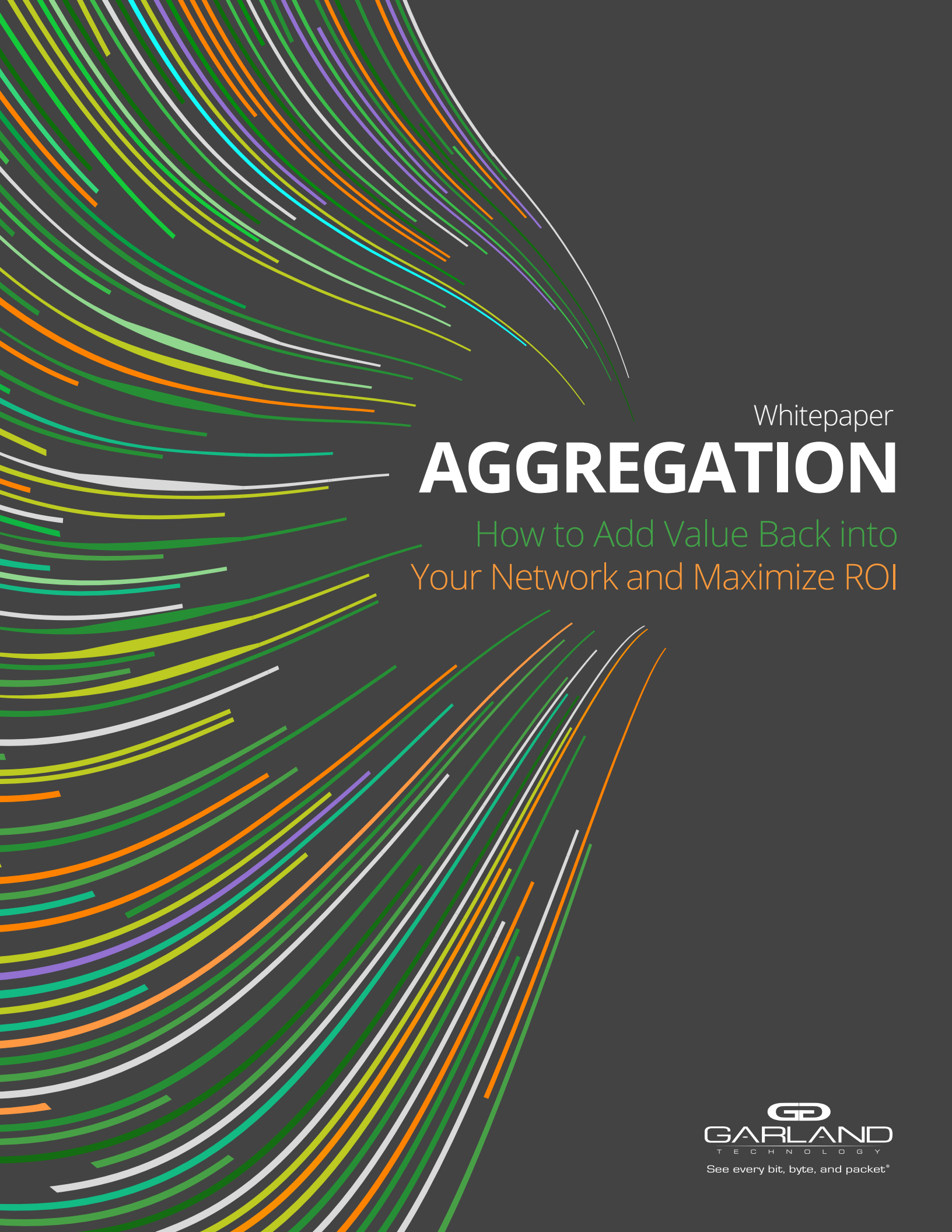


Whitepaper

AGGREGATION

How to Add Value Back into Your Network and Maximize ROI

GARLAND TECHNOLOGY

See every bit, byte, and packet®

Aggregation | Table of Contents

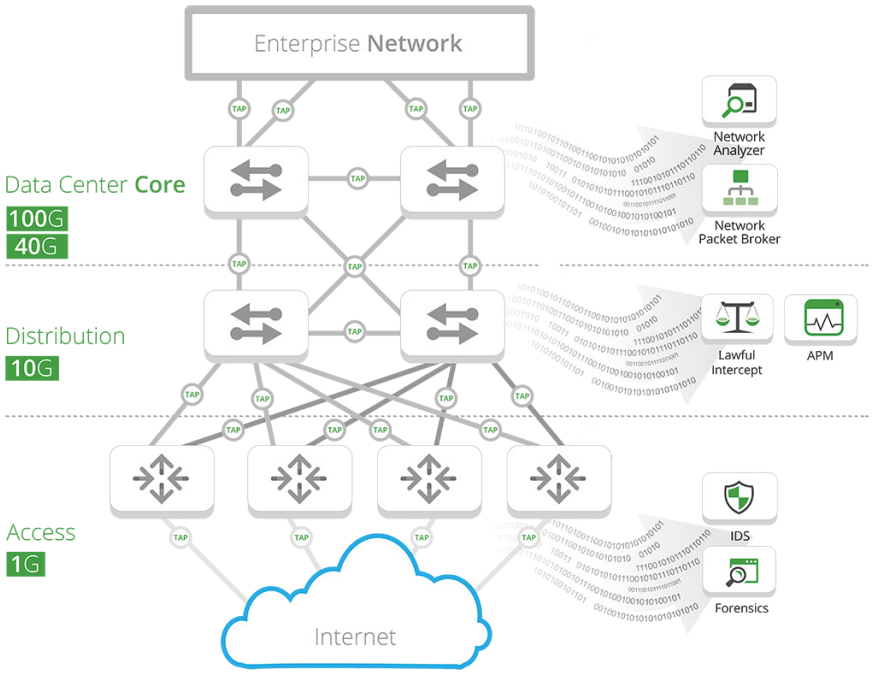
Where Aggregation Fits in Your Network

As a network grows and an enterprise needs to monitor either a large number of network segments, or a large, distributed network, the need for aggregation arises. Aggregation allows an organization to consolidate a high number of low utilization 1G network links down to just a few ports on a higher speed (40G or 100G) monitoring tool or Network Packet Broker. This aggregation of ports results in a simplified way to reduce the per port cost on expensive NPBs.

Routers and switches are the fundamental building blocks of any business network. From facilitating communications and collaboration to maintaining employee productivity, improving security, and enabling remote connectivity, routers and switches create the support system that keeps your business up and running.

As network speeds rise and data center demands grow, the topology of your routers and switches will evolve and become increasingly complex. Maintaining visibility of all traffic is essential to seeing returns on tech investments across your business—but doing so is easier said than done with modern data center designs.

When factoring visibility into data center design, there are three main layers to focus on.

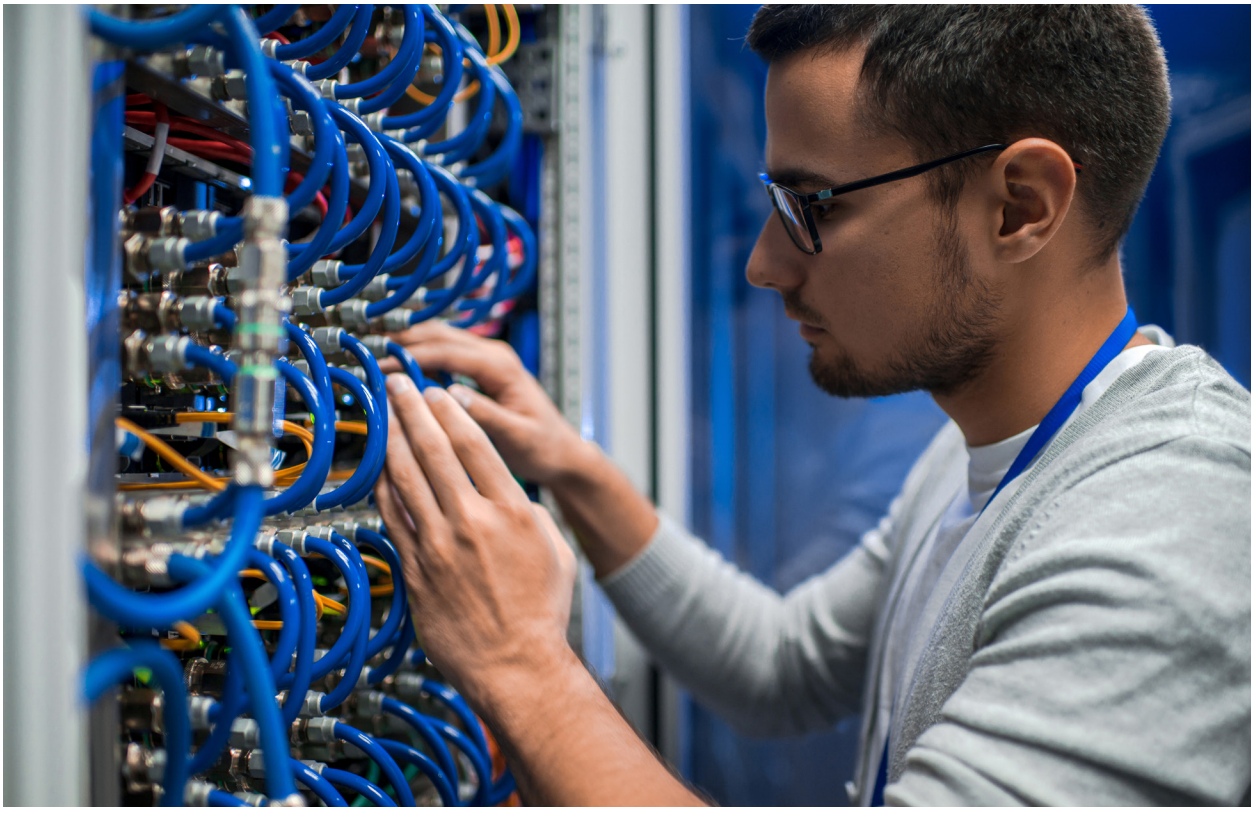


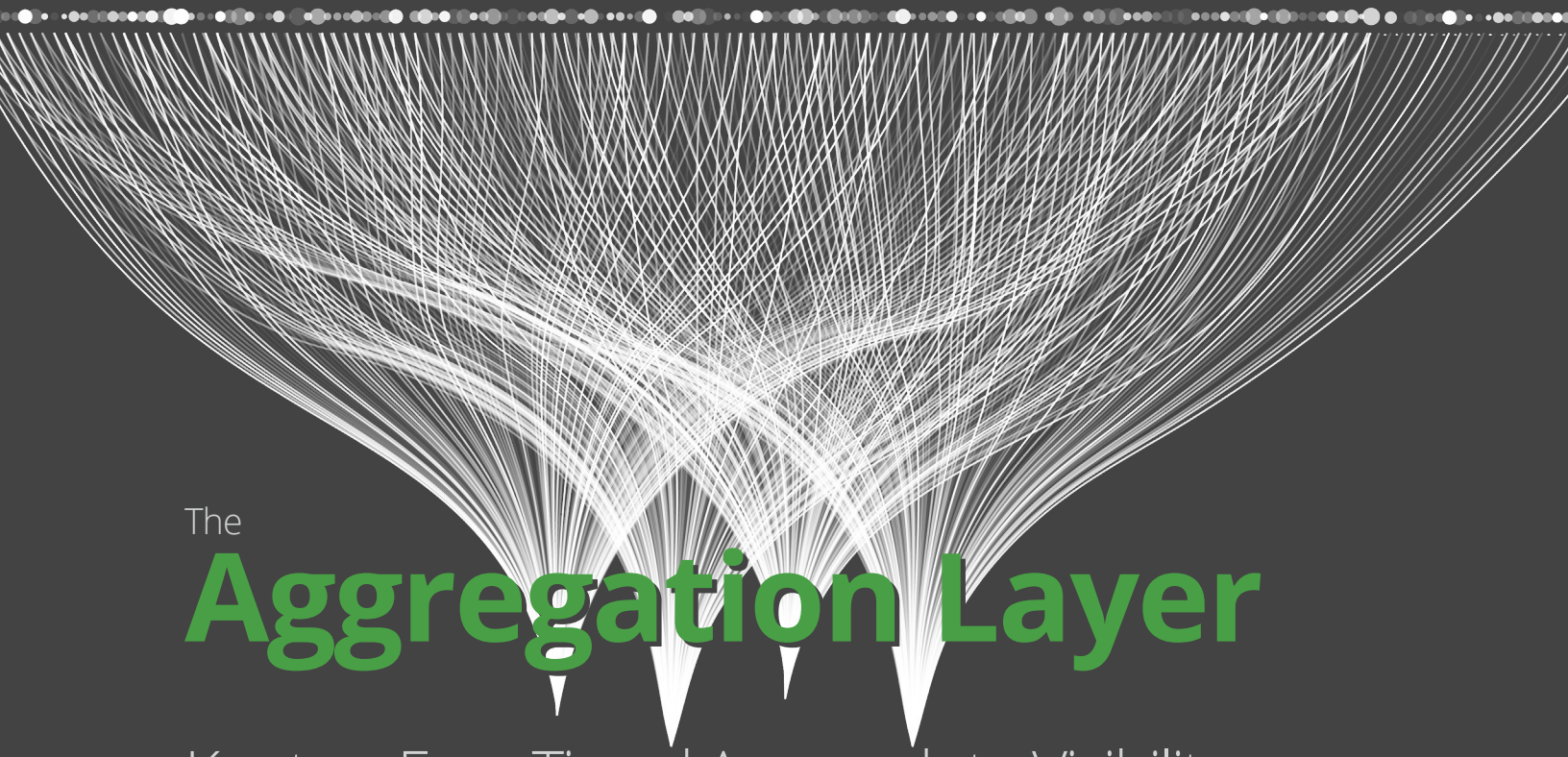
- **The Access Layer**: Where all servers and connected devices physically (or wirelessly) attach to the data center network. This layer consists of high port density switches that support packet flow and offer an efficient means of organizing packets to forward to the core.

- **The Aggregation or Distribution Layer**: A boundary for the Layer 2 and Layer 3 environments of the data center design. Especially for large, distributed networks, the aggregation layer serves as a necessary component of data center design to improve management capabilities.

- **The Core Layer**: The backbone of a data center network made up of Layer 3 routers that source and manage traffic across LAN, WAN, and cloud components of the design. Routers are the logical choice here because the core layer is responsible for segmenting traffic as it moves across the network.

Each of these layers presents unique opportunities to use Network TAPs and advanced aggregation to improve visibility across your network. Taking the right steps to aggregate these layers and increase visibility will, in turn, maximize the ROI of networking and security investments.





The

Aggregation Layer

Key to a Four-Tiered Approach to Visibility

It took a long time for IT teams to start recognizing the inherent limitations of SPAN ports for network visibility. However, networking demands have reached a level that SPAN ports simply can't match, leaving IT teams no choice but to find new designs that support network visibility and performance.

As a result, there's been a widespread shift to a traditional three-tiered approach to network visibility that includes network TAPs in the physical network, network packet brokers (NPBs), and the assortment of tools used for application performance monitoring, security, data forensics, and more.

The only problem is that tools continue to represent the most expensive aspect of networking monitoring with increasingly advanced features. To support these tools, network architects have had to deploy more complex NPBs, which has only added to the costs of network design and diminished long-term ROI.

To address these new challenges, the three-tiered approach to visibility now has to evolve to a four-tiered approach—one that hinges on an aggregation layer.

The Four Tiers of Network Visibility

The reality is that many network links only use 60% utilization. And as those links move further and further from the core layer, utilization can drop to 5% or even lower. Couple that with the fact that per port costs of network packet brokers are so high, network architects are left with minimal ROI.

Adding an aggregation layer to the traditional three-tiered approach solves the ROI problem. When the aggregation layer is included, network visibility includes:

Physical Layer TAPs: Hardware tools that access and duplicate network traffic, supplying full line rate traffic without oversubscription. Packets are sent from these TAPs to the new aggregation layer (instead of going straight to NPBs).

Aggregation Layer: Advanced aggregators serve to increase the efficiency and cost effectiveness of NPBs. By pre-filtering traffic prior to forwarding to NPBs and reducing the number of ports necessary for monitoring and security tools to see necessary packets, the aggregation layer plays a key role in maximizing ROI.

Network Packet Brokers: Devices that are responsible for funneling data from network TAPs to the security and monitoring tools that maintain network performance and data protection. Network packet brokers replicate traffic and reduce the volume of packets sent to each tool, keeping network architects from having to invest in new, high-cost tools.

Tools: The appliances and applications used to analyze packets forwarded by NPBs, including data leakage protection, application performance monitoring, SIEM, intrusion detection systems, and more.

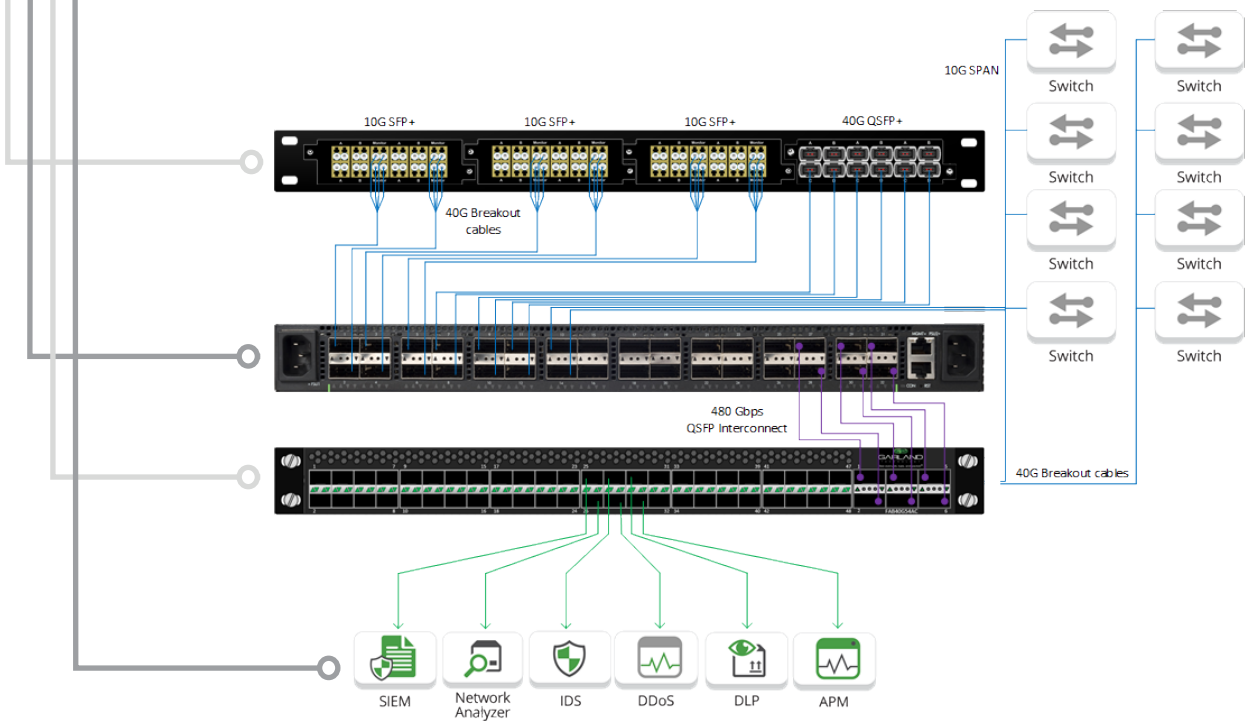


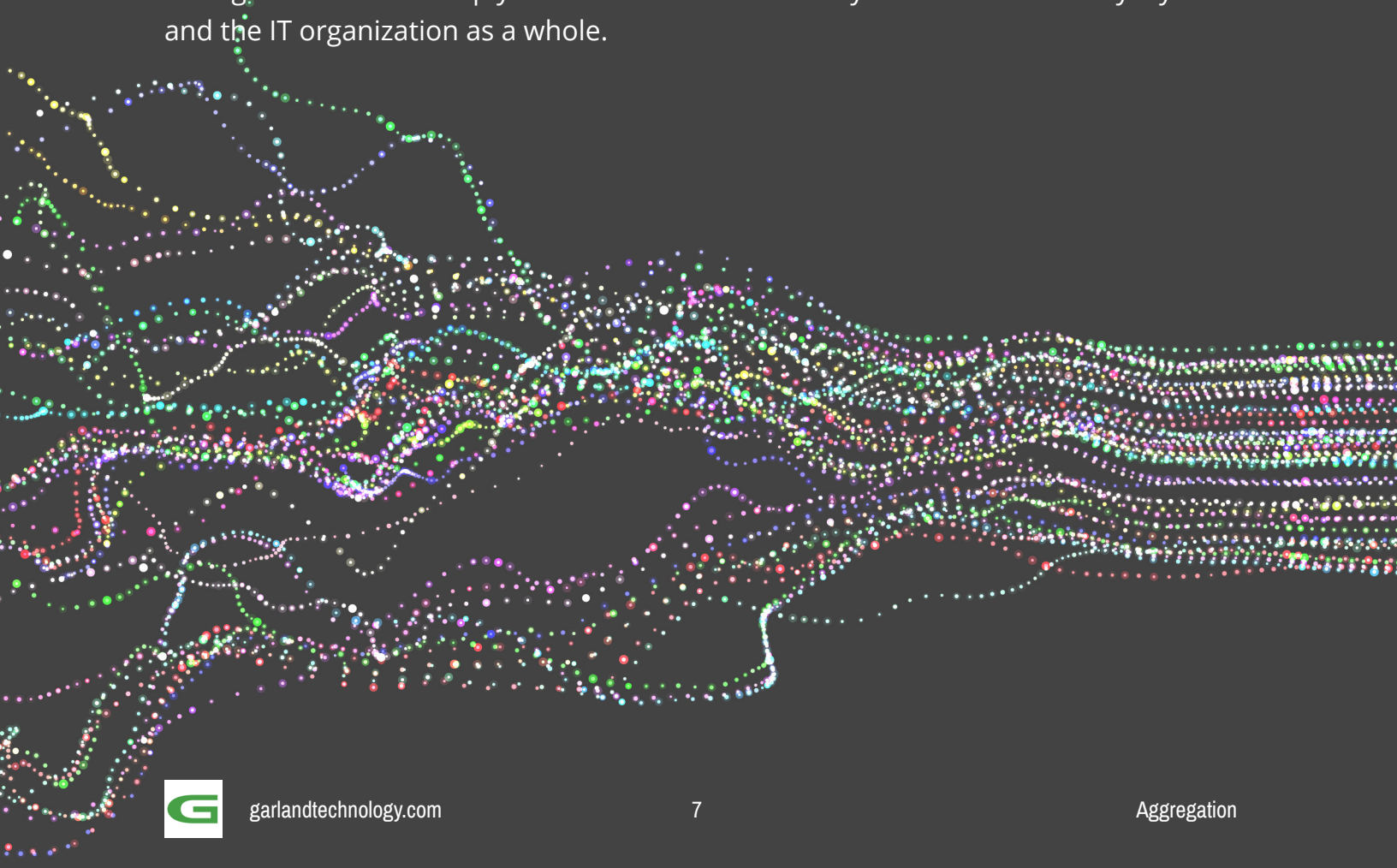
Diagram: 4-Tiered Visibility Fabric Architecture

The difference made by this new aggregation layer is significant. Consider this simple example. If an existing NPB has 50% utilization on all ports, aggregators have the potential to free up the other half of those ports. This extends the timeline for purchasing new NPBs and allows network admins to monitor parts of the network that have long been neglected.

When purchasing aggregators to maximize ROI, costs should not exceed $1,000 per 100G interface. That pricing alone is 50% to 75% less than full-featured, under-utilized NPBs. In addition to cost, network architects should also look for aggregators that:

- Support multiple speeds and media types
- Offer high-density form factors
- Have selective Layer 2 to Layer 4 pre-filtering
- Integrate with management software through APIs
- Include remote management options

But choosing the right devices isn't just about cost efficiency. Strategically deploying the right devices can help you add additional value to your network visibility layer and the IT organization as a whole.



Adding Value to Your Foundation of Visibility

It is important to understand that the benefits of aggregation do not have to be limited to the aggregation layer itself. For added efficiency and ROI, network architects can aggregate traffic in the access layer using TAPs, consolidating packets and uplinks before they reach the aggregation layer.

The purpose of switches in the access layer is to create peer-to-peer connectivity that can also uplink to the core layer. The result is a significant amount of East-West traffic flowing within the access layer, as end-user devices communicate with one another. Supporting this East-West traffic is essential for employee productivity—but it creates challenges for the monitoring and security appliances or services within the aggregation layer.

Aggregation in the access layer can help overcome two challenges that lead to maximum ROI.

1. There are many security and monitoring tools in the aggregation layer that will only have one NIC card or input port. With potentially hundreds or thousands of East-West links in the access layer, it's impossible to create one-to-one connections between the aggregation layer and edge switches.

2. There are tools like lawful intercept and advanced threat defense systems that don't just need visibility into traffic on a single link—they need to spot patterns as traffic moves across multiple points in the access layer.

Adding aggregation TAPs in the access layer helps network architects overcome these challenges by merging eastbound and westbound traffic flows, copying all traffic from one or many ports (depending on the inputs) and transmitting those copies to security and monitoring tools via a single link.

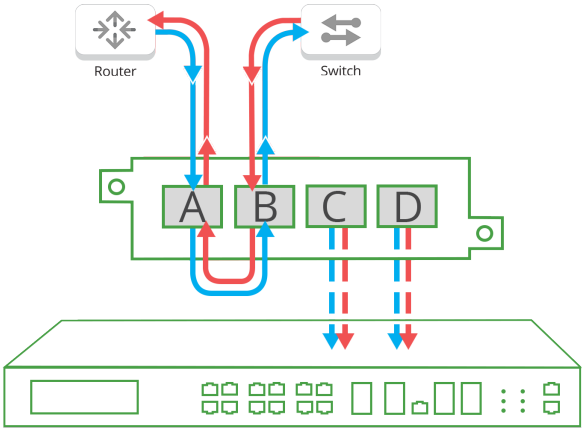


Diagram: Aggregation TAPs copy data from both directions to support appliances with only one NIC card.

However, network architects can't simply copy every bit, byte, and packet® with aggregation TAPs and expect the data center to run smoothly. Increasing network usage and heavy traffic spikes must be addressed when designing a network. This ensures that port oversubscription does not become a problem that leads to low performance and security risks.

Utilizing aggregation TAPs effectively in the access layer requires architects to rely on a few key best practices:

- **Managing Aggregation Groups**: When multiple points of the network are combined into a single aggregation TAP, it's important to pay close attention to utilization rates. As they increase, admins should limit the number of traffic streams that are aggregated simultaneously.

- **Applying Traffic Filters**: XtraTAP™ with aggregation includes granular filtering capabilities to ensure that security and monitoring tools only see exactly as much data as necessary. Filters help you reduce port requirements and support more tools via aggregating TAPs, ultimately improving cost efficiency and ROI.

- **Leveraging Breakout Mode**: If oversubscription or full utilization becomes a concern, aggregation TAPs can alternatively be configured to operate in TAP "breakout" mode. This feature breaks transmit and receive traffic apart and copies it to two separate monitoring ports to avoid packet loss.

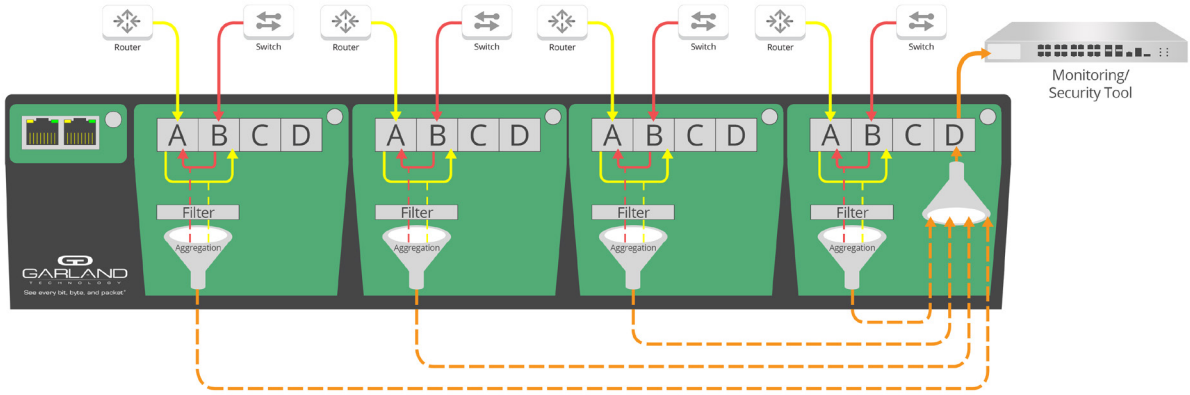


Diagram: Add filters and aggreagtion to send 4 links to one monitoring tool without oversubscription.

Introducing aggregating TAPs to the access layer is the first step to achieving a level of reliability that will fuel long-term ROI. In many cases, network architects will rely on SPAN ports to achieve a similar sense of traffic mirroring. However, it's important to use aggregating TAPs in place of SPAN configurations as much as possible to avoid performance degradation and ensure packet fidelity.

Once the access layer is made reliable and simplified by aggregating network TAPs, architects can focus on the actual aggregation layer. Optimizing the design of the aggregation layer, in addition to using aggregation at the access layer, is what will add real value back to the data center network.

How to Successfully Leverage Your Tapped Links with Advanced Aggregation

Advanced Aggregators and Network Packet Brokers deliver only the traffic required by the specific tools they're connected to. To do this, NPBs have a variety of filtering and aggregation options to help them act as the middle-man between network TAPs and the tools themselves.

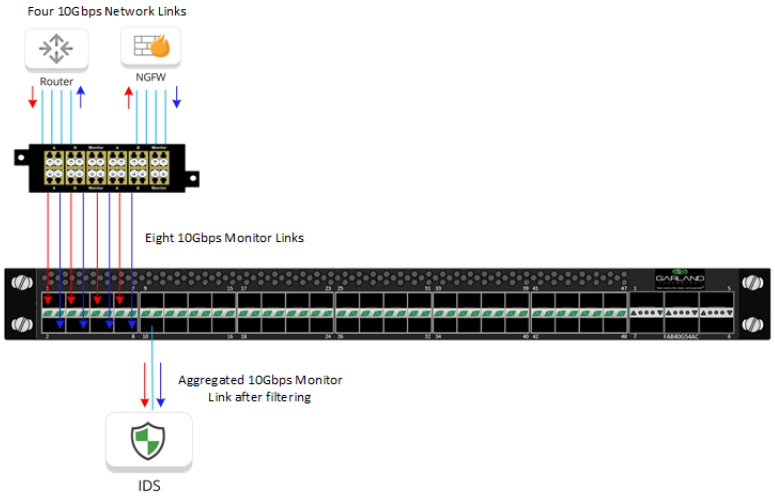
There are four common TAP deployment scenarios in combination with an aggregation layer to add visibility and value to your monitoring and security tools.

1 Aggregate traffic from a single TAP port to a single tool

Most security and monitoring tools currently handle up to 10Gbps of traffic at any given time. When incoming traffic from a network TAP is 40Gbps, that traffic needs to be filtered by a factor of 4 to match monitoring tools. Network Packet Brokers ensure the traffic is filtered properly to meet network speed limitations, providing all necessary packets to guarantee visibility and performance.

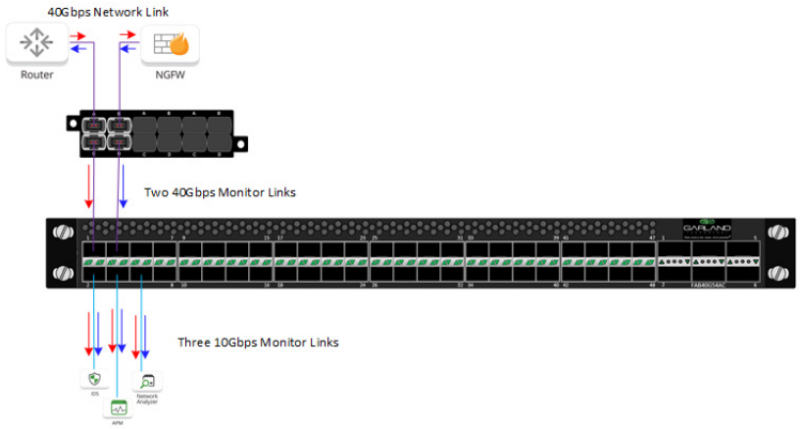
2 Aggregate traffic from multiple TAP ports to a single tool

Now, the network packet broker has to support aggregation in addition to filtering. With aggregation, users can set up individual filters that apply to all incoming traffic, streamlining configuration and simplifying deployment. Aggregating traffic also ensures tools receive packets from multiple data streams.



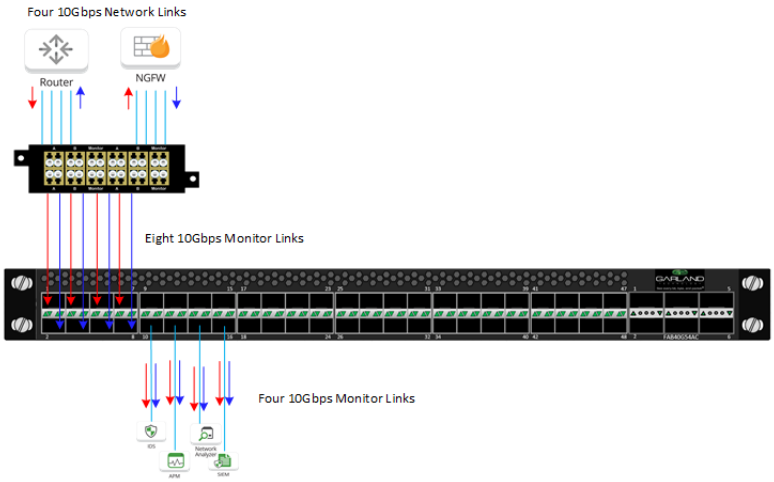
3 Aggregate traffic from a single TAP port to multiple tools

Filtering is still necessary in this use case. But now, the NPB must also replicate and/or load balance traffic. Replication ensures every tool has access to the packets they need. In the case that tools require the same filtered traffic for analysis, load balancing is necessary to avoid oversubscription. Pay close attention to NPBs that support configurable hash-based load balancing in addition to round-robin and weighted round-robin approaches.



4 Aggregate traffic from multiple TAP ports to multiple tools

This use case is essentially a combination of the previous three. Filtering, aggregation, and load balancing combine to guarantee that each connected tool is operating at maximum efficiency with visibility into every bit, byte, and packet® necessary.



Creating an Effective Aggregation Layer

A well-designed aggregation layer has the power to dramatically simplify a data center network. However, the wrong approach can easily lead to just as much complexity and inefficiency as any other design strategy.

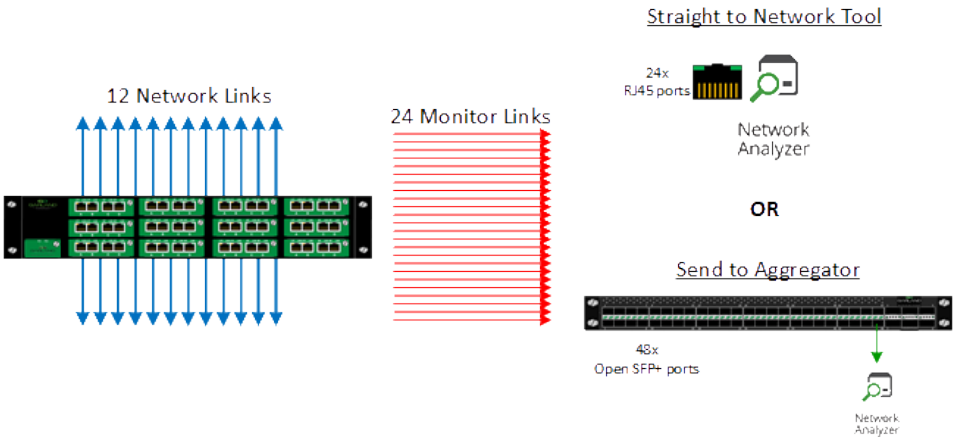
When the access layer is properly connected with network TAPs, you can consider the best ways to build the aggregation layer. There is no one-size-fits-all approach. But with the right devices, you can maximize cost efficiency and performance.

Increasing Visibility to More Links Cost-Effectively

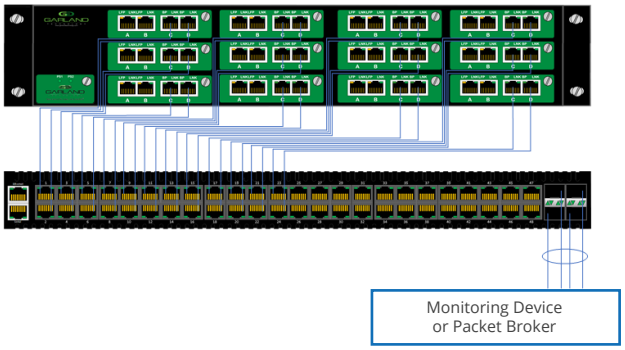
Achieving 100% visibility into network traffic should be a goal for any IT organization. However, challenges like limited rack space, ever-growing port fees, and port limitations on core infrastructure often make it easier said than done. As a result, IT leaders are left to find the most cost-effective ways to increase the number of monitored links in their network designs.

By taking advantage of high-density network TAPs, IT leaders can tap 12 links in just a 2U footprint with only two UPS connections. This initial step saves PDU ports, outlets, and setup time. Using an Advanced Aggregator to aggregate and load balance these tapped links significantly decreases the number of ports necessary on the core network packet broker.

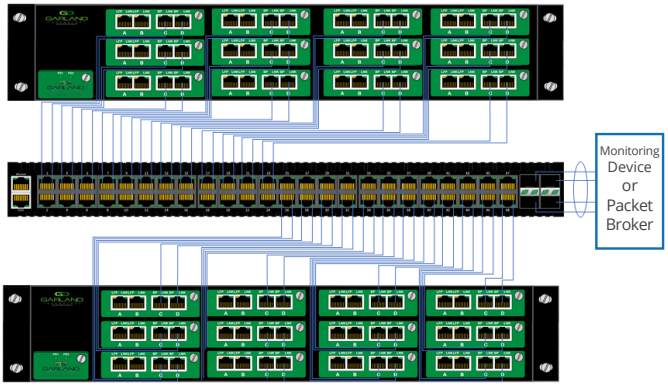
The results are greater network simplicity, increased port efficiency, and overall reduced costs by eliminating the need for so many visibility solutions.



Aggregate 12 1G Links to One



TAP 24 1G Links and Load Balance to 10G



TAP + Aggregation for Gigabit Copper Networks

For all the publicity about 40G and 100G networks, there are still plenty of 1G copper networks that need greater visibility. Copper network TAPs are the best means of guaranteeing traffic visibility. However, as more security and monitoring tools come into play with greater resource demands, it is important to have a design that avoids over-utilization.

When multiple copper network links are tapped, many monitor links could be generated as breakout and aggregation modes alternate to support both high and low utilization links. When there are many monitor links, an aggregator can reduce the number of connections needed to get data to the necessary tools.

Because most network tools do not have many available ports, Advanced Aggregators may be necessary to further reduce the number of monitor links. However, it may not be necessary to purchase a standard aggregation appliance that comes with 10G open SFP+ ports. This hardware would potentially have only 10% utilization because it is deployed on a 1G copper network. As a result, it often makes more sense to deploy smaller Advanced Aggregators that are more suited to the needs of copper networks.

TAP + Aggregation for High Density 10G Passive Fiber Networks

In higher density fiber networks like those commonly found in telcos and other carriers, the need for aggregation is critical. Adding the visibility needed throughout the network to gain complete situational awareness of their extended environment leads to having many tapped ports and not enough tool ports to accommodate.

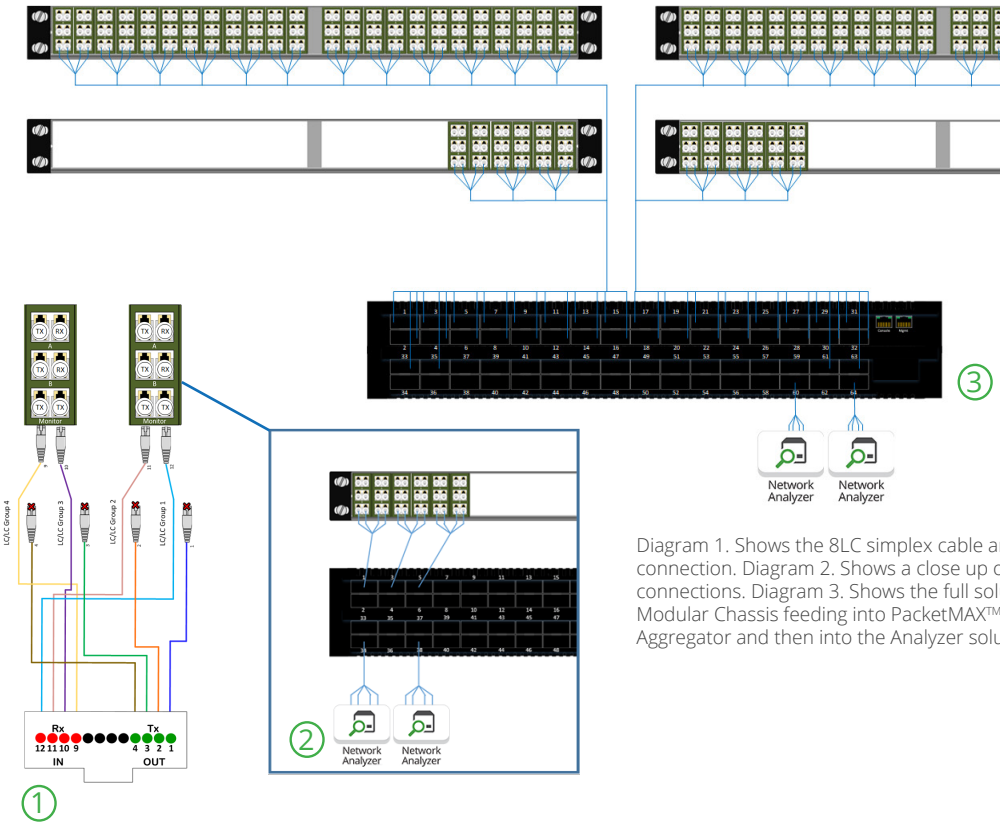


Diagram 1. Shows the 8LC simplex cable and MTP 12 breakout cable connection. Diagram 2. Shows a close up of the TAP and aggregation connections. Diagram 3. Shows the full solution with 4 SelectTAP™ Fiber Modular Chassis feeding into PacketMAX™: 100G 64 Port Advanced Aggregator and then into the Analyzer solution.

Using a passive fiber TAP creates two monitoring ports for each link tapped. Tapping 60 links, gives you 120 10G monitoring ports, and in many cases there may only be 4 ports on a tool.

The ideal situation is to take all 120 links into a single device, at which point you can load balance and filter out traffic that isn't needed, to ensure that all the packets are going to the tool.

Aggregation at The Core

The core layer is where Network Packet Brokers collect and process all traffic flows. Here, you can take advantage of advanced packet processing and send specific data to individual monitoring, forensics, and analysis tools. Advanced processing features at the core include:

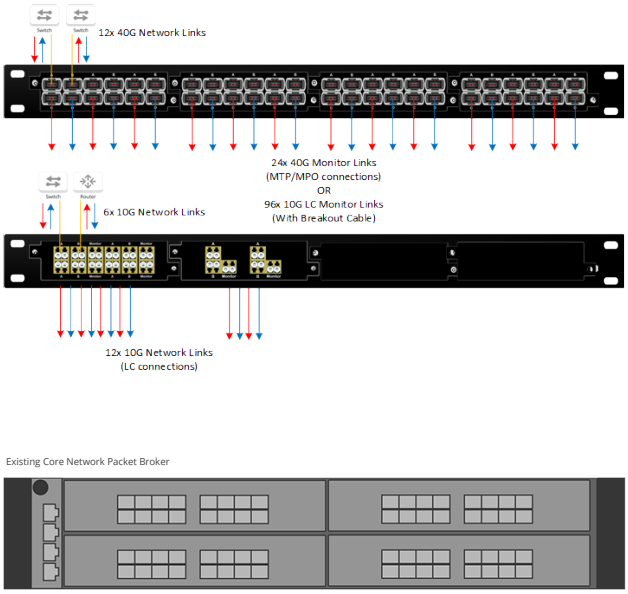
- **Deduplication**
- **Time stamping**
- **Packet slicing**
- **Load balancing**
- **Decryption**

But the only way to take advantage of these features is to guarantee visibility of every packet. With so much traffic to manage, it's important to take advantage of an aggregation layer to more efficiently monitor data packets.

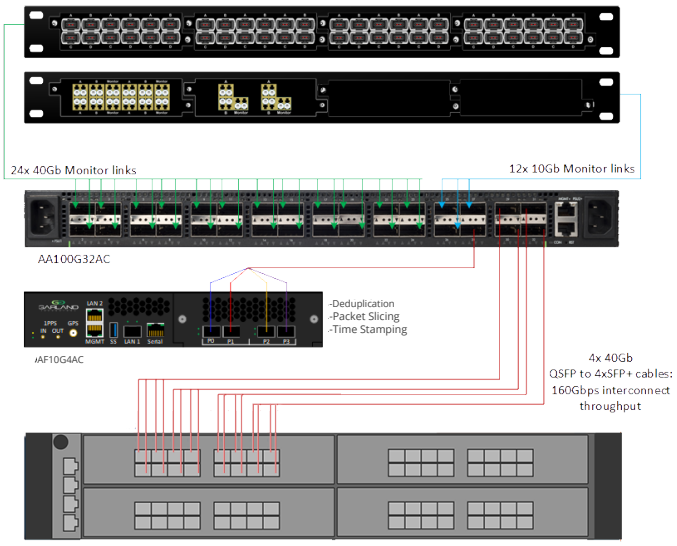
Adding an Aggregation Layer to Existing Infrastructure

In an effort to scale network services to meet business needs, many designs are trending away from 10G uplinks to 40G links between core and distribution switches. But when these links are upgraded, additional visibility is necessary into the core and edge of the network.

TAP Requirements



Adding an Aggregation Layer and Advanced Features



Adding network TAPs into the uplinks between core and distribution switches and from the core switches to the edge ensure visibility into every bit, byte, and packet.® However, the challenge is then to fully utilize each monitor link on the new 40G capacity. Advanced Aggregators can enable packet brokers to make the most of each port, while ensuring that fewer ports are necessary overall.

Conclusion

Aggregating a path to Network ROI

Networking demands are increasing at a rate that IT budgets simply can't keep pace with. It's probably not feasible to continually purchase new TAPs, packet brokers, security appliances, and monitoring tools every time new applications or networking speeds emerge.

Instead, maximizing ROI is all about finding ways to make the most of what you have today. And that means simplifying the network wherever possible.

By building out aggregation at the access layer and creating a more efficient aggregation layer within your data center, you can utilize more of your network resources and reduce the number of ports necessary to provide total visibility to security and monitoring tools. It's the most cost-effective path to add value to the network while also unlocking long-term ROI.

But the ROI hinges on coming up with the right design and deploying the right hardware in the right places. This is where Garland Technology excels.

Securing and monitoring your network is the ultimate goal. Garland's TAP to Tool™ concept is to not lose sight of that goal by architecting to the tool, not competing with them. Garland Technology can help save budget on expensive Network Packet Broker platforms and focus on what's important - getting that wire data to the tool.

Garland Technology ensures complete 360° network visibility by delivering a full platform of network access products including: Breakout TAPs, Aggregator and Regeneration TAPs, Advanced All-In-1 Filtering TAPs, Inline Edge Security Bypass TAPs, Cloud solutions, as well as purpose-built Network Packet Brokers.

Setting Yourself Up for Aggregation Success

If you want to learn more about which visibility solutions and aggregators can best unlock the ROI in your network, contact Garland and tell us about your biggest networking challenges.

Garland's Design-IT team of engineers will work directly with you, as a free consultation, on designing a network connectivity strategy.

Credit - Contributions from Vince Black, Jonathan Devoy, and Greg Zemlin.