Fiber Mountain Solution
WP-00102.05.01

Fiber Mountain's Secure & Intelligent Physical Layer Solution

As companies embrace digital transformation to maintain their competitive edge, their demands on the datacenter continue to grow. Increasing data demand and pressure for lowering operational costs on the datacenter infrastructure has historically caused systems and network engineers to continually reevaluate their architectures

Evolving Architectures

In the 80's and 90's, datacenters were typically designed with central switching locations/racks. As servers were added, connections would be run from their network ports across the datacenter to attach directly to the central switch. This worked efficiently since most servers hosted both application and associated storage. Traffic was predominantly north-south (in and out of the datacenter), rather than east-west (between servers).

As connection density increased, the volume of cabling from each rack became too large to manage via this kind of direct cabling connections. It created operational issues and made troubleshooting connectivity in the thick web of cables on the switch side almost impossible, often causing outages for neighboring services.

From the late 90's into the early 2000's, this problem was addressed by distributing the switching throughout the datacenter. Each row (or pod) was given an End of Row (EoR) switch to aggregate the connections from all servers within the row. The EoR switch then connected to a core router or switch in order to provide north-south connectivity as needed.

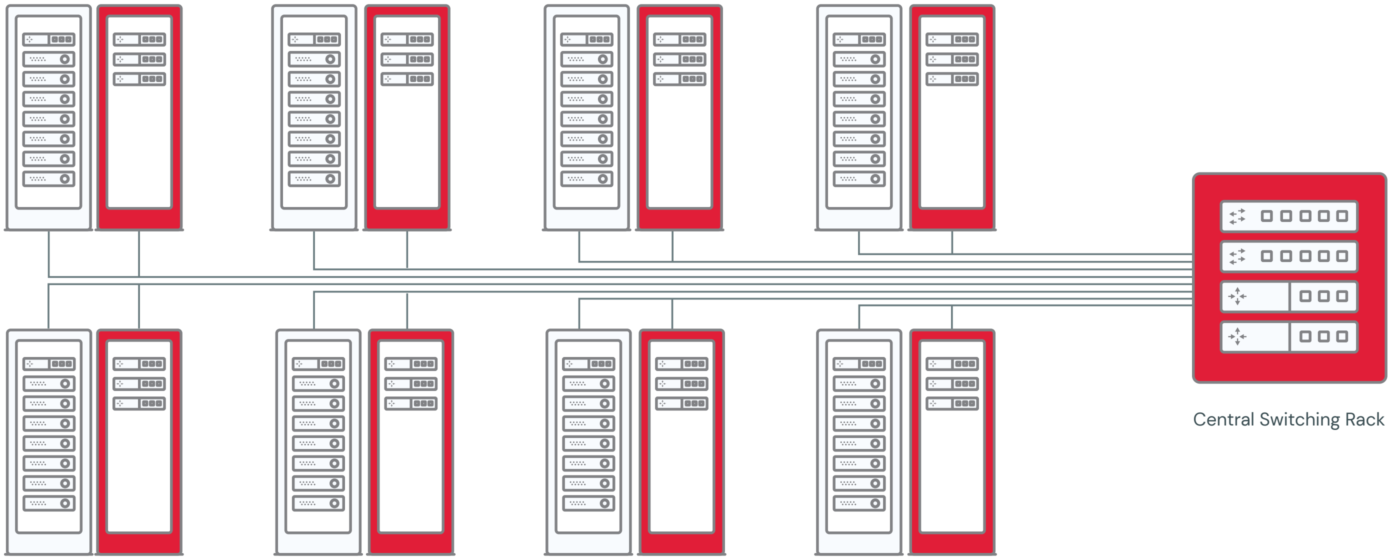
Reconfiguring the physical layer connections can be one of the most challenging tasks from a labor perspective, especially if documentation is poorly maintained.

Fiber Mountain's solution was conceived to address these issues and provide additional operational benefits to help reduce cost.

For more information, visit:
www.fibermountain.com

This aggregation reduced the volume of cabling going into the central switching rack. At the same time, data center operators started deploying cabling in a more structured manner, in order to simplify planning, installation, and troubleshooting. Cables from servers were terminated on patch panels between devices, and cables were run between patch panels instead of direct point-to-point runs.

As rack densities continued to increase, the volume of cables once again became a problem, and many data centers added another switching tier at the top of each rack (ToR) to aggregate the connections from the servers before connecting them to EoR and then to the core. This common three-tier switching architecture is still being used today in a lot of enterprise networks.



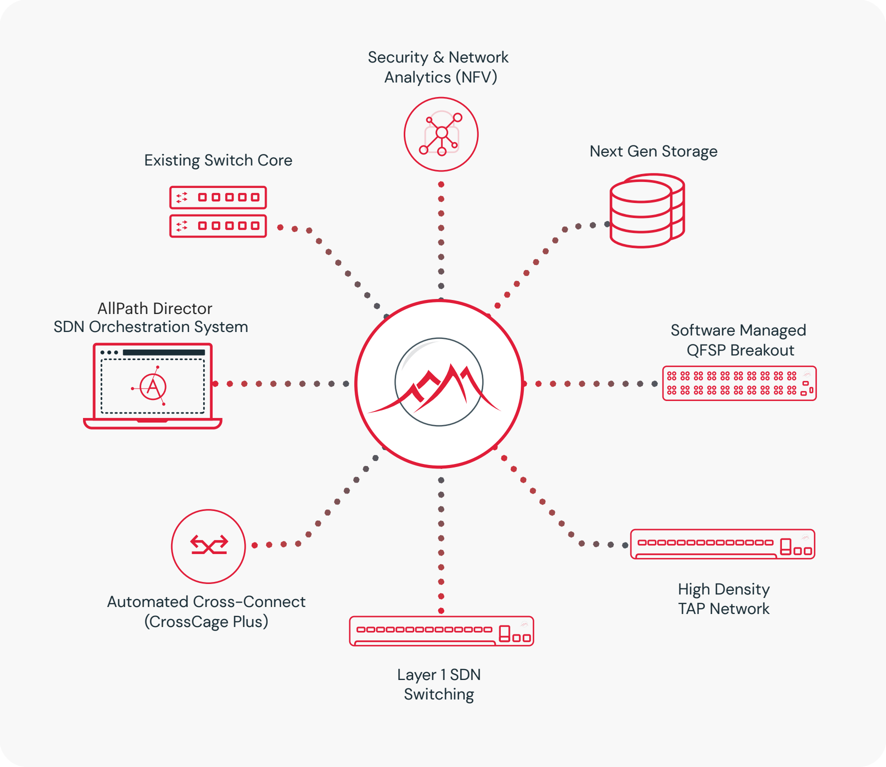
With traffic and server loads continually growing, network designs evolved further, with centralized storage and databases emerging as the preferred design. That centralization meant that the majority of network traffic was now east-west (server-to-server) instead of the predominantly north-south traffic patterns the established network architectures were optimized for. The architectures which had been designed to streamline traffic and simplify troubleshooting were now introducing bottlenecks and limiting growth. It was to address this problem that spine and leaf architecture was conceived and became widely deployed, although both approaches introduce challenges as well as benefits. Distributed switching architectures reduced the volume of cabling to the core switching locations, but at the cost of increasing the number of switches in the network. An alternate approach to the problem focused on standardizing the ways in which cables were run, an approach known as Structured Cabling.

In addition to standardized cabling processes, Structured Cabling made use of patch panels at each aggregation point or Intermediate Distribution Frame (IDF). Manual patches allowed for the completion of connections throughout the data center, but without strict adherence to the guidelines by every employee or contractor, these IDFs quickly became just as difficult to maintain and manage as switch-based aggregation methods. In both cases, manual moves, adds and changes (MACs) introduce the factor of human error, both in making the connections themselves and in documenting those connections once the work is done.

Introducing Fiber Mountain's Secure & Intelligent Physical Layer

Imagine a network where every device can be given a high-speed fiber optic connection to any other device at any time, via software. How is that possible? Wouldn't a full mesh of cable connections from every rack to every other rack be completely unmanageable?

Fiber Mountain set out to address the problem of managing ever-increasing demand for data center connectivity in a different way.


Security & Network Analytics (NFV)
Existing Switch Core
Next Gen Storage
AllPath Director SDN Orchestration System
Software Managed QFSP Breakout
Automated Cross-Connect (CrossCage Plus)
High Density TAP Network
Layer 1 SDN Switching

Fiber Mountain solves that problem in two ways. First, we use today's high density fiber cable to bring hundreds of fiber strands out of each rack via small-dimension cables connecting to distribution points within the datacenter, which are equipped with an intelligent optical cross-connect called the OPX® (Optical Path Exchange). The OPX® combines the first part of the solution (high density fiber optic cable) with the second part of the solution: software control of physical connectivity via Fiber Mountain's AllPath® Director (APD) orchestration software. Servers, storage and other devices can be given programmable connections, through a network equipped with OPX®s and APD, to anywhere else in the network without the need to manually plug or unplug cables.

Transforming the Physical

Fiber Mountain transforms the physical layer from a very static asset into an agile and dynamic component of the network. Reconfiguring the network to meet evolving needs becomes a task that can be achieved via software, with a fraction of the time and expense that standard approaches require. Some Fiber Mountain benefits can also be realized when components are incorporated into existing network architectures.

Fiber Mountain allows devices to be cabled once. Connectivity between devices becomes software defined, and MACs can be accomplished with a keystroke.

Software Controlled

In the structured cabling environment, cables are brought to Intermediate Distribution Frames (IDFs), where racks of patch panels are required to establish connectivity from device to device within the datacenter.

These patch panels usually start nicely dressed and organized, but each move, add and change requires the cables to be undone and redressed – unless technicians pressed for time take short-cuts and skip those steps. Human errors tend to accumulate in both the physical connectivity and the documentation of those connections.

In contrast, Fiber Mountain's solution allows devices to be cabled once. Connectivity between devices becomes software defined, and MACs can be accomplished with a keystroke. For further flexibility, extra fiber can be installed during installation to "future-proof" the infrastructure and enable responsiveness to unexpected demands and requirements.

This ability has many benefits, including:

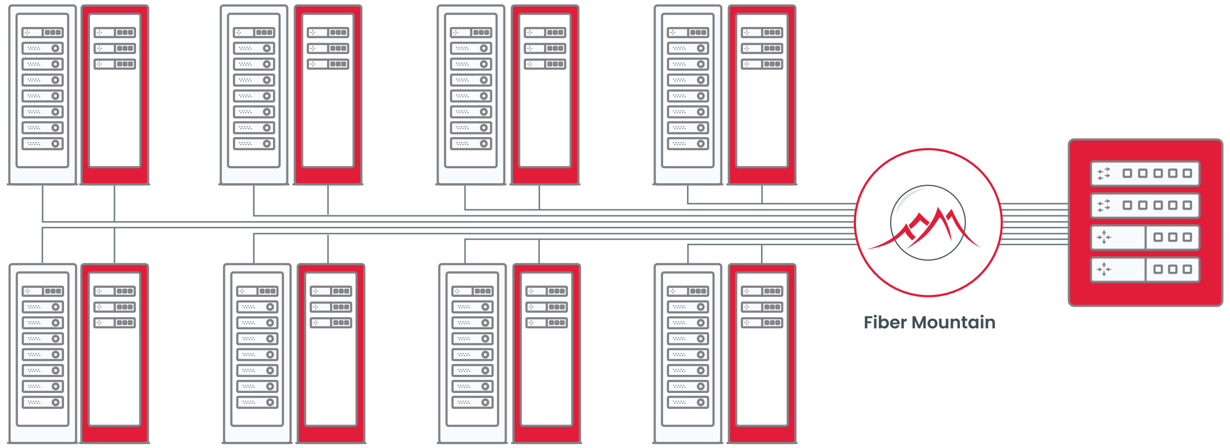
- Moves, adds and changes can now be accomplished remotely, enabling a "lights out" data center environment that meets operational uptime and security objectives.
- Fiber Mountain solution functionality simplifies disaster recovery, whether maintaining backup systems, testing disaster recovery procedures, or reacting instantly to loss of service in the main location.
- Fiber Mountain's customers can use the API to automate their processes, writing applications to control the physical infrastructure to fit their needs.

The API allows endless possibilities for applications that can be written to control the infrastructure. For example, the infrastructure team might automate bandwidth changes in support of recurring events such as data backups, or write an application to authenticate and authorize specific end users to call up additional bandwidth between two devices in support of one-time events, all without additional human intervention.

Flexibility of Virtual Connectivity

Every network architecture topology has benefits and flaws, and the question of which is best for a specific network depends on the current needs and challenges. Historically, changing from one topology type to another has been a labor-intensive and expensive undertaking, incentivizing network administrators to work around the existing architecture for as long as possible.

When all network ports are connected to the Fiber Mountain solution, however, topologies can be virtualized and reconfigured as needed through AllPath® Director. Network administrators can easily switch between topologies such as hub-spoke, three-tier and spine- leaf without having to re-run cables, and new dynamic topologies can be invented, tested and implemented with minimal expense.



Reducing Switches

By virtualizing connectivity, Fiber Mountain tintroduces a new level of flexibility when it comes to the physical location of devices within a data center. The functionality of a three-tier or leaf-spine distributed architecture can be provided via software, while the necessary switches can be physically located in a centralized location to optimize port utilization and simplify maintenance and upgrades.

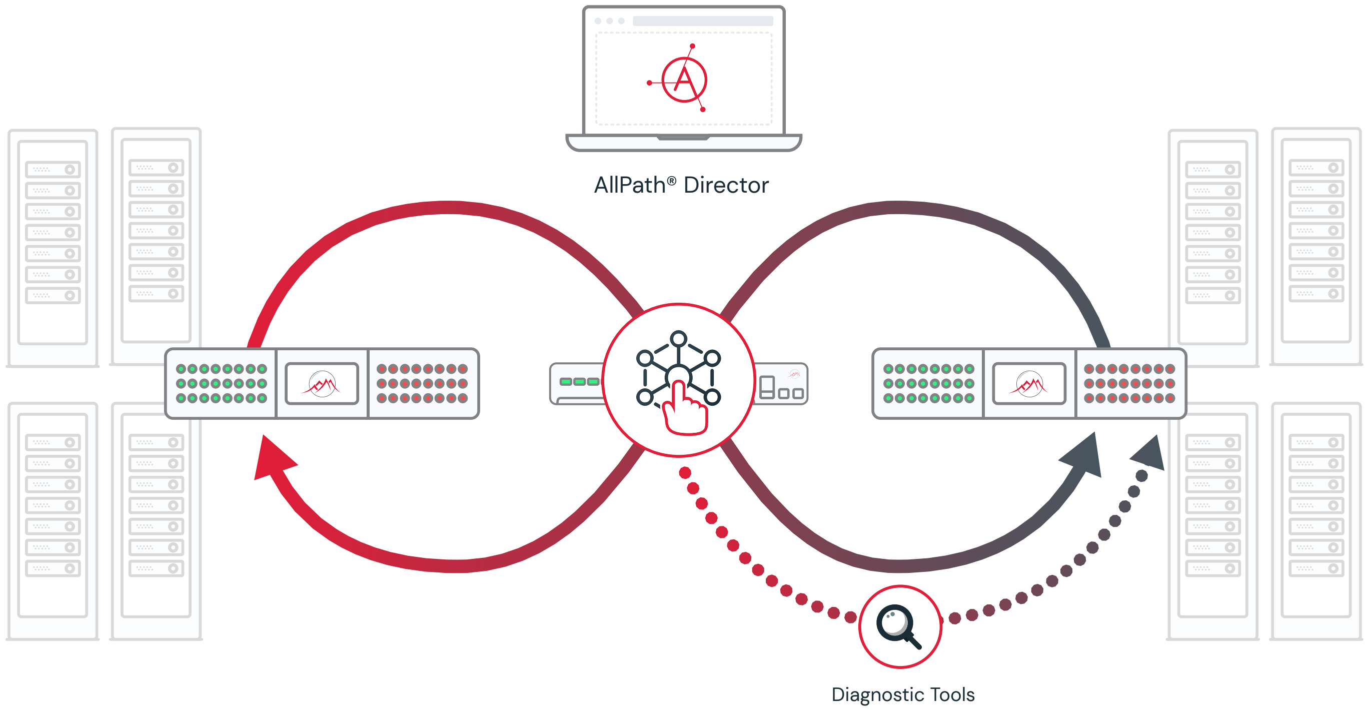
This ability provides many benefits. For example, standard distributed architectures require leaving a subset of switch ports unused in each top of rack switch (ToR). With our solution, the ToR aggregation is performed by Fiber Mountain's Fiber Port Aggregators (FPAs). The FPAs connect to the network of OPX®s and allow AllPath® Director to groom connections to efficiently use all available ports on centrally located switches. Since FPAs cost significantly less per unit than switches, this structure reduces expenses while increasing the agility and responsiveness of the network.

Monitoring/Tapping

Fiber Mountain also simplifies network monitoring. For security reasons and troubleshooting, the demand for monitoring of network traffic has increased. In the standard approach, passive TAPs are deployed in order to monitor traffic, but because these TAPs are expensive, limited numbers are purchased.

Rather than monitor every connection, TAPs are strategically deployed within the network to monitor as much as possible with limited resources, focusing on the most important or most vulnerable traffic. As needs change, the TAPs must be relocated, a manual process which causes service disruptions, impacts scheduling and introduces new opportunities for human error.

In contrast, the our solution makes use of the OPX®'s high-density connections and multicast functionality, combined with AllPath® Director's ability to recognize and configure traffic from individual fibers or fiber groupings within each connector, to enable software-controlled configuration of one-to-many connections. In short, network administrators gain the ability to TAP any connection made through an OPX® and extend that TAP to any number of monitoring applications connected to the solution, regardless of physical location.



Fiber Mountain revolutionizes tapping by allowing monitoring of any device connected to the solution on-demand, at any time, without disruption, and with no need for expensive additional inline TAPs.

Documentation

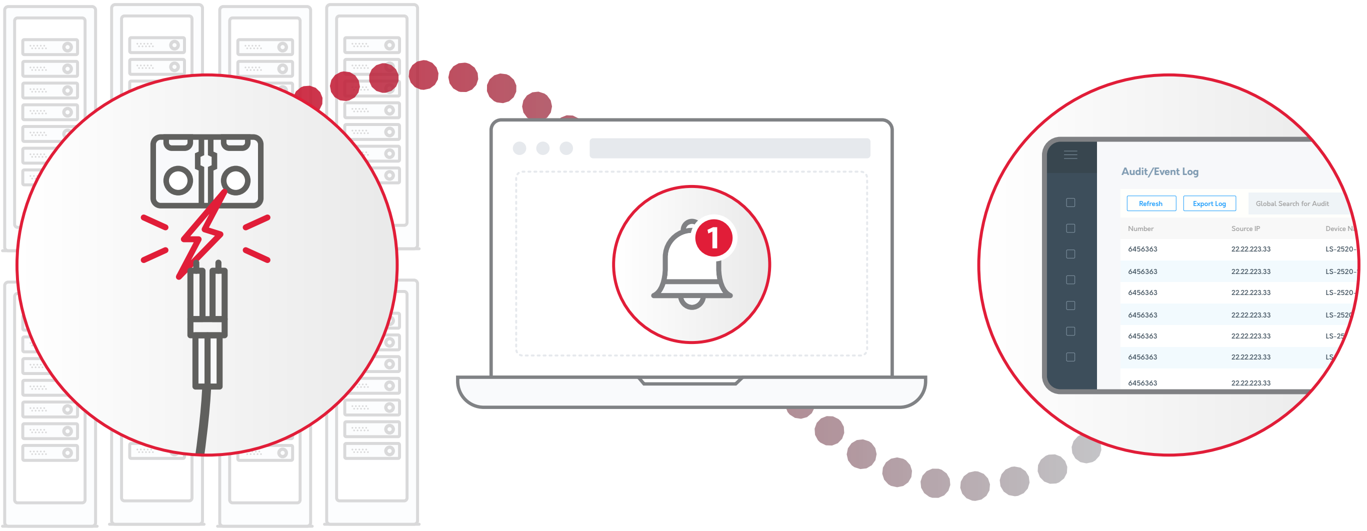
One of the longstanding challenges faced by data center operations is documenting the cabling. Standard practice for documentation requires manual entry of MACs into a database or spreadsheet. More advanced systems tag cables with a barcode that can be scanned manually and entered into a database. In both cases, the documentation can only be as accurate as the last time it was updated, and errors in the process can go undetected for months or years. With the volume of fiber optic cable used in Fiber Mountain architectures, how does Fiber Mountain address this problem?

In addition to OPX and AllPath® Director, the solutionincludes Fiber Mountain's AllPath® Connect. AllPath® Connect cables and panels are designed to be assembled into an intelligent cabling infrastructure that interfaces with AllPath® Director via ICID® (Intelligent Connection Identification).

Why go to the trouble of making physical cable connections software-discoverable? One benefit is the creation of a self-documenting physical infrastructure. APD discovers the identities of panels and cables to draw a real-time topology map of physical connections and polls the network at regular intervals to discover moves, adds and changes.

ICID®

AllPath® Connect cables and panels are designed to be assembled into an intelligent cabling infrastructure that interfaces with AllPath® Director via ICID® (Intelligent Connection Identification).



Each ICID® enabled cable connector has a unique, discoverable identity which is visible to APD when plugged into an AllPath® Connect panel. APD can discover the location of both sides of the cable, including the panel and port. This information is automatically recorded upon discovery, allowing the generation of current and historical reports. Once cable connections are discovered, APD can display the real-time topology of the cabling infrastructure, including the end-to-end routing of any specific connections through all AllPath® Connect panels between two devices.

Security

Security, both physical and virtual, must always be in the forefront of a data center or network manager's mind to ensure regulatory compliance and maintain business systems availability. To date, however, physical infrastructure security has been primarily focused on measures designed to control who can physically enter the data center. While advanced biometrics can be effective in keeping out unauthorized personnel, once someone is inside there are limited ways to track their activities and any accidental or intentional impact they may have.

With AllPath® Connect, however, the Fiber Mountain solution introduces the ability to view physical infrastructure and track connectivity changes via software. AllPath® Director communicates directly with all of the AllPath® Connect panels and cables to monitor the physical layer in real-time. Changes, such as a cable being pulled to introduce an unauthorized monitoring device, will trigger an event or alarm in AllPath® Director and identify the exact location and time of the disconnect. Network operators can act upon this knowledge immediately, minimizing the damage that can be inflicted by either accidental disconnects or "man in the middle" type attacks initiated by an insider. Events and alarms are also logged, and can provide a secure audit trail for use in support of security incident investigations.

Conclusion

Managed and dynamic physical infrastructure is certainly a new concept, but it has the potential to transform the industry. The benefits go much further than just configuring connections via software, although that alone will provide significant cost savings and competitive advantages. The ability to provide enhanced security, always accurate documentation, on-demand TAP of any port in the network and reduced operational costs with the same solution just scratches the surface of the value Fiber Mountain's solution can offer. Fiber Mountain creates a software-defined infrastructure that empowers everyone from data center and infrastructure architects to network operations personnel with real-time visibility and software control of the physical layer.

Fiber Mountain provides a variety of value added services, including hands-on training, on-site installation, and 24x7 technical support. Contact Fiber Mountain for a schedule of available services. **Warranty:** Return to factory hardware repair or replacement for one year.