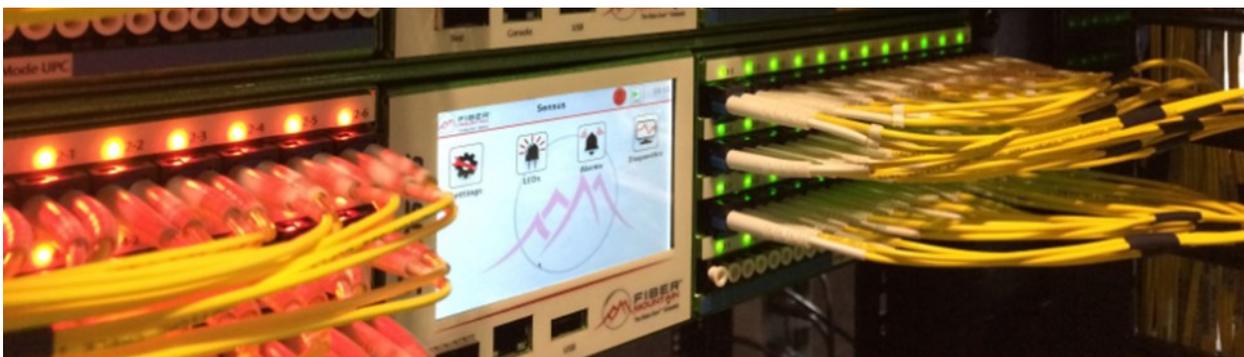


## Introduction

There is little joy in running and terminating cables in a data center or large network. Looking at miles of cables running through conduits, drop ceilings, crawl spaces, rack rails and patch panels can make even the most organized technician cringe. It is not the cables themselves that cause this reaction, but the time and effort it takes to manage an ever-changing sea of cables and connections, where the documentation can become out of date within days or even hours of making a change.

Over the last two decades, everything from phones to cars to the factory floor has been upgraded with software, sensors and new levels of functionality and user-enablement. Levi Strauss & Co. even teamed up with Google to make a connected commuter jacket that lets you play music, make phone calls and listen to the news. Yet, patch panels and cables within the data center have lacked the same pace of innovation. While whole ecosystems of new high-tech products have been created, physical layer elements of the data center have remained relatively unchanged. There have been incremental improvements, such as structured cabling, denser cables/patch panels and rudimentary smart management systems. However, the core of the problem remains. Technicians still use spreadsheets to track cables and connections. When the spreadsheets are found to be out of date, it takes hours of tracing cables, and a lot of old-fashioned elbow grease, to get the job done. The physical layer and the tools we use to manage it are badly in need of an upgrade!

If time is money, then managing cables in a network is an endless money pit – and as the world becomes more connected, the pit keeps getting deeper. People and their devices are getting more connected, big data is getting bigger and datacenters need more and more cable connections. We need a better way to manage them! That's where Fiber Mountain's Sensus™ and the Glass Core™ come in.



## Fiber Mountain's Sensus™

At first glance, Sensus might look like just a modular patch panel with an attitude, but it is so much more.

To understand the ambition of the solution, it helps to understand the genesis of the name. A census is a survey of a population, generally run by a government to understand who is living and working in their territory. Similarly, Fiber Mountain's Sensus enables surveys of the connections within a datacenter or large network. These surveys show the people running the network what's connected where – and when. Knowing what is in your datacenter at any given time is useful but relatively easy to achieve. Seeing the connections between network devices in real time, and knowing when and why each connection was established, is transformative.

Sensus is a key component in the next generation of physical layer intelligence. There have been many previous attempts at implementing intelligence at the physical layer, but excessive complexity and lower-than advertised accuracy have kept them from becoming the transformative solution the industry needs.

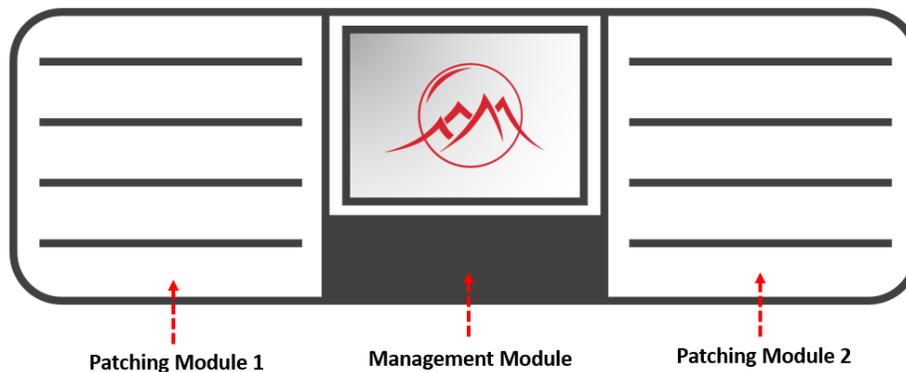
Now, Fiber Mountain has simplified the implementation of physical layer intelligence by developing hardware and software innovations in tandem. These innovations work together to form an integrated system solution called the Glass Core. Sensus, combined with Fiber Mountain's AllPath Director (APD) central orchestration software, allows network infrastructure professionals to have capabilities not yet seen in the physical layer. It even provides a path to endless software enhancements through its Application Programming Interface (API).

Here are just a few of the questions that can be answered in seconds with a Glass Core network using Sensus, APD and Intelligent Connection ID (ICID):

- Want to know how many free ports are in your patch panels? **Checked**
- Want to know all the patching points from server A to switch B? **Checked**
- Want to know why your data center keeps running out of 10M cables? **Checked**

## What's Under the Hood?

Sensus is a 2RU modular unit. Each chassis has a central management module with an LCD screen, which provides local management and diagnostic tools. To either side of the management module there are spaces for hot-swappable patching modules, which can support single-mode or multimode fiber with UPC or APC connectors.

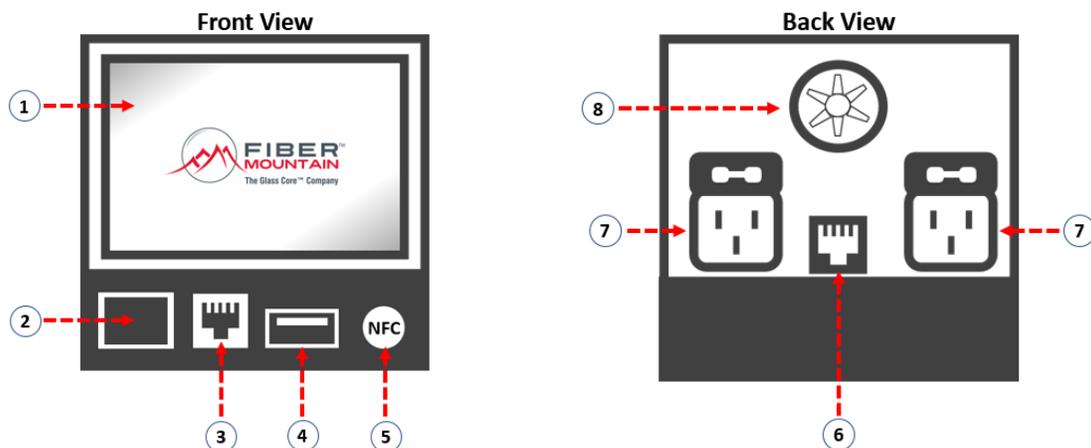


The patching modules are 100% passive for user traffic. If the unit loses power of the management module is disconnected, user traffic will continue without disruption, and only management data will be affected. Sensus can be used in place of any passive patch panel without risking loss of connectivity in the event of a power failure. Business continuity and disaster recovery planning are improved by the addition of management functionality to passive connectivity. Supported configurations include, but are not limited to:

- Duplex LC (Front) – MPO-8 Fiber (Rear)
- Duplex LC (Front) – MPO-12 Fiber (Rear)
- Duplex LC (Front) – MPO-24 Fiber (Rear)
- Duplex LC (Front) – Duplex LC (Rear)
- MPO-8 Fiber (Front) – MPO-24 Fiber (Rear)
- RJ-45 (Front) – 110 style punch down (Rear)

Each port is equipped with a tri-state LED that can be controlled by the management module or APD. These LEDs are used for communication between on-site technicians and the management software or remote administrators. They can be used to draw attention to a specific panel or port, or can be illuminated across devices to indicate a specific end-to-end connection path. In addition to the LED, each port is fitted with sensors to detect the physical presence of cable connectors and the additional information available from ICID-enabled cables.

The management module, and its integration with APD, transform Sensus from a simple modular patch panel into a software-controlled, automatically documented network device. It gives the panel an identity that can be located and managed. It also provides technicians and administrators with access to port information such as real-time port usage or availability. The management module also provides enhanced capabilities with various interfaces available on the front and back of the module.



1. LCD touch screen – access to local config file
2. SFP+ port for diagnostics – Loopback/PRBS
3. RJ-45(front) – craft port for local configuration
4. USB port – third party integrations (i.e. audio)
5. NFC reader – used to read smart cable IDs
6. RJ-45(back) – management (POE capable)
7. Dual AC power
8. Fan

## Why Sensus?

Sensus is more than an “intelligent patch panel.” Sensus and APD can provide real-time knowledge of a data center’s physical infrastructure, including dynamically mapping out the topology of connections through the sea of cables. Using Near Field Communications (NFC), each ICID-enabled cable connector is given an identification that can be read by Sensus. Moves, adds and changes (MAC) are made easier and errors are reduced, providing a more secure and available network.

Different data center professionals will focus on different aspects of the value Sensus provides. Data center architects will be excited by the chance to know how many patching ports are free, and where each one is located. Data center technicians will enjoy the ease of LED-guided MACs that show exactly which port to plug each cable connector into. Data center operations teams will save hours of time and effort by knowing exactly when and where each connection was established.

Sensus and the Glass Core provide solutions to the physical layer challenges that these people face every day: visibility, MACs, documentation, auditing, and central management.

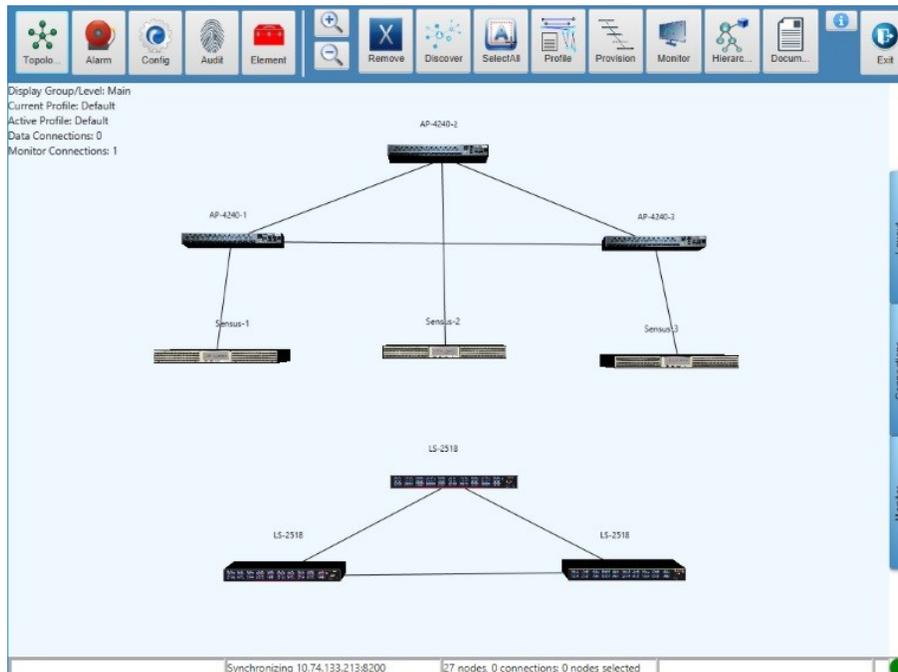
**Visibility** – Each Sensus unit is equipped with dozens of sensors, which allow it to detect the presence of physical cables in each port. In addition, if the cable is ICID-enabled, Sensus can read the cable’s identifier, physical properties (i.e. length, manufacture, glass type, polarity, etc.) and any custom data that may be associated with it. Existing cables can be retrofitted with ICID clip sets. This simplifies the process of integrating Sensus into an existing data center or network.

**MACs** – Moves, adds and changes have traditionally been done in the dark. Technicians are given instructions based on documentation that is guaranteed to have some degree of inaccuracy. They are then sent to find their way through a maze-like array of rows and racks full of servers, switches, patch panels and cables. Sensus simplifies locating the correct panel and port, and it enables automatic confirmation that the MAC was completed correctly. The LEDs can be used to guide the technician through each step of the process and can provide immediate feedback if something is done incorrectly. For example, the Sensus can be configured to blink a fast red LED if a cable is plugged into the wrong port. Although LED guidance won’t eliminate all the potential errors with cable patching, ICID makes it obvious when a mistake is made and easy to make corrections on the spot.

**Documentation** – Most technicians will agree that all documentation is wrong to some extent. This is a testament to the adage that no manual documentation is safe from change. Sensus addresses this problem with automated documentation. All ICID-enabled cables, whether Fiber Mountain brand or retrofitted with ICID clip sets, are automatically documented when plugged into a Sensus port. Say goodbye to Excel spreadsheets!

**Auditing** – When was the last time someone told you “Nothing changed,” or “I didn’t unplug that cable?” One of the challenges with standard physical layer cabling is the fact that changes are invisible unless someone manually tracks them – and manual documentation is as subject to human error as MACs. Sensus addresses this problem by detecting cable presence and logging all port changes of ICID-enabled cables. The Sensus log provides a record of all cable activities. This record includes when and where each cable was plugged/unplugged, how many times it was plugged/unplugged, what kind of cable it was, etc.

**Central Management** – Each Sensus module comes with a standalone management module, which can be accessed locally or remotely. Sensus units are easily connected to APD for central management. This is beneficial even for small deployments of one to three units. For deployments of tens, hundreds or thousands of units, central management with APD simplifies implementation and provides critical visibility into the network.



## Higher Availability

When it comes to high availability, it is understood that 100% uptime is seldom possible. Even the best-run business will be struck by an outage at some point in time. Outages cannot be escaped completely, but it is still important to strive for the highest possible availability.

Human error continues to be one of the largest reasons for data center outages.<sup>1</sup> No matter how diligent technicians are with documentation and implementing MACs, mistakes happen – and the impact can sometimes be disproportionate to the error. For example, in May 2017, British Airways grounded over 1,000 flights at Heathrow and Gatwick airports due to an IT failure. It was later determined that the wrong power cord was pulled. Reconnecting it in an uncontrolled manner caused catastrophic damage to a server, which cascaded into an infrastructure-wide failure.<sup>2</sup>

Although the British Airways issue was power related, the same kind of mistakes happen with network cables. With poor documentation and little guidance, all cables in a datacenter start to look alike. The immediate impact may not be as dramatic as the British Airways example, but it's still a problem. Lack of urgency can make it harder to track down cabling errors once the network starts to suffer, allowing small problems to accumulate over time. In addition, IT staff members are always being asked to do more with less. This makes human errors more likely, and at the same time the team has fewer resources with which to track down and fix mistakes.

Documentation is usually accurate at the time of the initial installation. As errors and oversights accumulate, however, the documentation becomes less and less reflective of the actual network. Documentation errors can be as simple as forgetting to enter a change because something more urgent distracted the technician, or as problematic as a program crashing right before the backup and losing critical data.

Sensus and the Glass Core bypass that problem by making the current physical layer discoverable in real time. They also automatically document and log all changes to physical connectivity within the Glass Core network as they occur.

<sup>1</sup> What is behind most data center outages, February 9, 2016 Kathleen Hickey - <https://gcn.com/Articles/2016/02/09/data-center-outages.aspx>

<sup>2</sup> Human Error to Blame..., July 10, 2017 Renee Harper - <https://cloudscene.com/news/2017/07/datacenterdowntime/>

## Technician/Engineer Efficiency

Reliable accuracy of documentation also increases the potential efficiency of MACs. Imagine a technician who is sent out to add a connection to a specific patch panel to gain access to another row. The technician goes to the panel and every port is in use, even though the spreadsheet indicated that multiple ports were free. Where did the additional cables come from, and what do they connect to? They cannot be pulled without risking an unplanned service outage. The technician on site has to report back to operations with this new information, instead of completing the patch and moving on to the next task. Regardless of the resolution, this situation will delay the establishment of the patch the technician was originally dispatched to make. In remote locations that are only serviced periodically, this problem is even more difficult and time-consuming to resolve.

There are three basic approaches to this problem:

- Ideally, the operations team will have the mystery cables traced to see what they were installed for and update the documentation. This process can take hours, however, and is likely to require additional skilled technicians to be scheduled for the work. Resolving the problem could take days or weeks.
- A simpler approach is to assume the mystery connections are valid. From there, you would either select another panel for the patch that does have open ports or order a new panel. This process is simpler, but it may also take days or weeks. The extra cables remain a mystery, and another potential problem to deal with in the future.
- If the source and destination are close enough together, a cable could be run directly. This is only possible if there is a long enough cable available and if there is room in the cable trays along the route. In many data center patching scenarios, however, this isn't even an option.

Now imagine a data center where Sensus patch panels are used with ICID-enabled cables and managed via APD. The operations team knows exactly which ports specific cables are plugged into, when the cables were plugged in, and where the other ends are connected. When the on-site technician arrives at the panel, there are no surprises. A remote operator can even illuminate the appropriate LEDs to walk an inexperienced technician through the patching process. The remote operator can also identify and correct errors as soon as they occur, which greatly reduces the time to completion. The technician doesn't need to manually document the new connection because Sensus and APD do so automatically. With the appropriate applications, Sensus and APD can even communicate with the data center's ticketing program to identify who made the connection.

## Optical Integrity

The integrity of a signal may be compromised as it passes through patching fields. An optical signal will lose strength as it passes through one or more patch panels. The optical budget outlines the number of patches permitted in a path from end to end, as well as the total cable length. Sensus helps manage optical budgets by providing an accurate picture of the cable lengths and connections along a signal path. It also simplifies troubleshooting. For instance, impairments caused by a mix of multimode OM3 and OM4 cables along a path can be one of the most challenging and time-consuming types of problem to troubleshoot. Sensus managed by APD can easily reveal these kinds of anomalies, avoiding physical layer impairments that are normally difficult to identify and resolve.



## Security/Compliance

Although the physical layer is the most tangible part of the network, it is also the least visible part. From a network administration point of view, physical connections are a matter of blind trust. Troubleshooting physical connectivity between switches, servers and other devices requires hours of work from skilled on-site technicians. A Glass Core network uses Sensus, APD and ICID-enabled cables to change all of that. It enables data center architects, network operations teams and on-site technicians alike to “see the invisible.”

This enables a new level of security and compliance functionality. Sensus, with its ability to detect removals and insertions, keeps track of everything in its event log. It becomes easy to see anomalies and investigate their causes, whether it’s a case of someone accidentally knocking a cable loose, or something more malicious. Custom alarms can be defined to bring attention to activity likely to indicate specific problems. A rapid disconnect and reconnect, for instance, can be set to raise a potential “man in the middle” alarm to trigger immediate investigation. Logs can always be reviewed for historical and compliance purposes.

## Conclusion

Layer One infrastructure has historically resisted all attempts at digital transformation. Previous promises of physical layer intelligence were more of a gimmick than a useful tool for technicians, operations teams and data center architects. With Sensus and APD, Fiber Mountain is introducing a new generation of physical layer intelligence. This new generation is tailored to how data center personnel work and integrated into existing systems in ways that make it easy to implement according to your business needs.

Sensus provides 100% passive patching, with the added benefits of software visibility and management. ICID-enabled cables provide detailed information on the cables and connections within a network, and they enable integration with inventory and maintenance systems. ICID clip sets introduce the ability to retrofit existing cabling with ICID capability for use with Sensus patch panels. APD ties it all together into a discoverable physical layer network. It provides the ability to display real-time topology diagrams, automatically log and document all changes to the network, and blink LEDs for technician guidance and assistance. Digital transformation is finally available to the physical layer, and your network will never be the same.