Case Study

Protect Fiber Uptime, QoS and Security

ONMSi Remote Fiber Test and Monitoring for Outside Plant Fiber Lines and Data Centers

Challenge: Data Centers powered by vast fiber networks serve almost every computerized transaction today, from our commerce, work, entertainment, and social interactions. We are highly dependent on reliable, secure fiber network connectivity. According to 2021 annual Uptime Institute survey results, more than one-third of data centers suffered an outage in the last three years with IT outages increasing in frequency in general. Nineteen percent were caused by software/IT failures and security failures/attacks, 17% were due to network failures, and 37% were due to power outages. There are millions of fiber disruptions a year causing outages and errors. ONMSi provides real time intelligence to reduce and avoid disruptions and troubleshoot underlying causes by optimizing the physical fiber performance for improved reliability, Quality of Service (QoS) and security.

How do fiber outages affect business operations?

- Lost customer business and reputational damage
- Disruptions to dependent operations and life
- Steep SLA violations and penalties
- Expensive network repairs that increase with longer MTTR

Proactively track and transform network performance with remote visibility

- Ensure uptime and performance
- Detect fiber security tapping intrusion
- Maintain bandwidth with low latency
- Identify flash attenuations that cause physical network flapping error conditions and poor user experience
- Drive down OPEX through a 30–50% reduction in resolution time (MTTR)

Proactive Fiber Management Yields Performance Results, Reduces Outages and Protects Security

Fiber plant degradation impacts reliability, speeds, and reduces throughput with increased retransmits and bit error rates. Poor fiber management impacts performance, reduces bandwidth capacity, and increases OPEX expenses and risk to operations.

Outages cost $16,000 to 30,000 per minute in from various surveys and according to Ponemon Institute's 2020 Cost of a Data Breach Report, an annual compendium of data breach trends shows the average data breach costs $3.86M. Data synchronization recovery efforts often takes days of remediation and security breaches take months.

Auto Detect Vulnerabilities in a Data Center Network
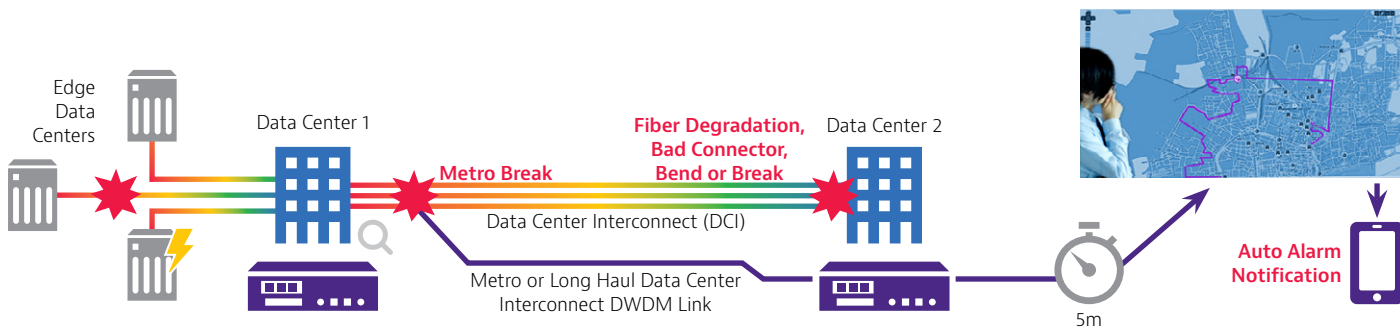
The VIAVI ONMS (Optical Network Management System) transforms your Data Center Operations by proactively protecting the Data Center Interconnect (DCI). Constant monitoring of DCI fiber links will push automatically alerts of fiber degradation, intrusion, and a cut or break. It can take days to identify and locate a cut without a diagnostic system. Often taps go undetected causing data and trust breaches for customers. Finally, accidental, intermittent connector disconnections, and poor connector handling introduces performance issues. The longer the resolution period, the more data synchronization required after a restoration. Minimizing MTTR will save millions in OPEX over time.

The VIAVI ONMS family with the OTU-5000 or the OTU-8000 test heads provide automatic alarms and visibility. You can often avoid outages altogether and restore service after an outage event by accelerating problem diagnostics and the requalification of repaired fiber links. This process detects:

1. Malicious physical vandalism such as tapping and destruction of fiber cables

2. Accidental network outages due to physical degradation, fiber attenuation flapping, cable cuts and breaks

The figure on page one illustrates a multi-data center network in which there are two primary centers along with some smaller edge computing datacenters in a campus setting, connected by redundant links. An optical test head is placed at each datacenter to rapidly scan and report on the fiber health against a baseline of the same fiber. Using a Google street view map overlay with GPS coordinates, pinpoint fiber events and dispatch to fix, not to find the problem.

Case 1: Avoiding Outages

Most fiber problems are crushes, bends, taps, and bad connectors that have failed or degraded due to poor handling. Fibers are frequently impaired by temporary bends that can be remediated before an outage occurs. A loss of bandwidth throughput is often present, but a cause cannot be located without visibility to physical fiber plant faults. Once an alarm hits the system, one can investigate, remove the bend, and prevent traffic outage. If a connector has become dislodged or contaminated when re-connected, proactive maintenance can eliminate this signal impairment. Recertify the fiber under maintenance remotely in minutes instead of sending someone to a center that may be unmanned. **Our customers report eliminating roughly 20% of outages.**

Case 2: Improve MTTR with Demarcation When an Outage Occurs

Determine the cause of an outage and rule out a fiber break or a power outage. If it is a fiber issue, an automatic alert allows immediate action. If the fiber is leased, a trouble ticket can be logged with the service provider. The MTTR (Mean Time To Restore) can be reported to manage the SLA. **Customers report a 30-50% MTTR improvement which has cascading savings associated due to less transaction/ data loss, less repair and resynchronization time.**

Natural Disaster
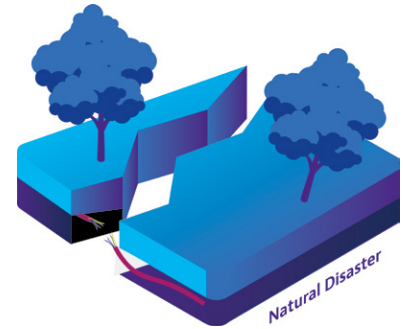
Case 3: Enhance Data Security Preventing Physical Hacking & Tapping cannot be seen by monitoring the data layer.

Inexpensive fiber taps give access to 100% of in-flight data. VIAVI Systems detect the tapping signature with an ultra- sensitive anti-tapping algorithm that can detect a tap that is not disrupting traffic. **Customers report finding taps frequently using the VIAVI solution.**

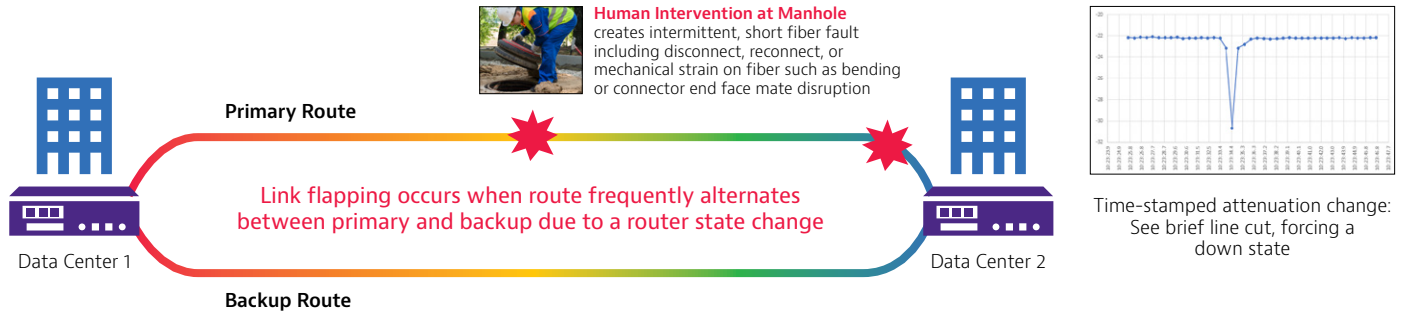## Case 4: Network Flapping Caused by Flash Fiber Attenuation Faults

Network route flapping is caused by pathological network conditions, including errors caused by hardware, software, configurations, and intermittent link "flash" connectivity loss. A physical layer flash attenuation flap can be caused by a connection with mechanical movement on it, causing intermittent connector end face misalignment due to high wind cable galloping conditions, or unintentional human interference. These are also known as intermittent, short duration faults or ISDFs. Such conditions cause router destination information to be repeatedly broadcast and withdrawn as the router state changes from up to down, thereby preventing the network routers from converging or agreeing on router topology. Flapping retransmits cause packet back up leading to a burst of errors that can be experienced by users as quality of service (QoS) issues including multi-media delay or video pixilation or sound issues. Frequent bursts of errors are costly when terabytes of data are not reaching their destination smoothly.

The new VIAVI Flash Fiber Monitoring Diagnostics option is 100 to 300 times faster than traditional fiber monitoring. Until now, operators have been unable to see or locate physical ISDF because the measurement time of traditional OTDR measurements exceeds the fault duration. Thus, now you can detect a flash optical attenuation event in .1 second and continuously monitor for this condition to locate the cause. The Flash Monitoring flapping detection option can be remotely engaged when needed or run 24 hours a day on one, in-service line for maximum flexibility and troubleshooting success.

Use case include identifying:

1. Human intervention causing a route flap such as disconnects/reconnects or short bending at a splice enclosure

2. Connector end face mate misalignment due to intermittent mechanical cable pulling

3. Intermittent cable bending that blocks light transmission

4. Potentially faulty elements causing insufficient laser power levels

Flash Fiber Monitoring System Detection in a Network

Human Intervention at Manhole creates intermittent, short fiber fault including disconnect, reconnect, or mechanical strain on fiber such as bending or connector end face mate disruption

Primary Route

Link flapping occurs when route frequently alternates between primary and backup due to a router state change

Data Center 1

Data Center 2

Backup Route

Time-stamped attenuation change: See brief line cut, forcing a down state

1 Apply Flash Fiber Monitoring 100 to 300x faster to detect and locate the transient fiber events causing errors.

2 Receive instantaneous notification with time-stamped attenuation change and loss metric.

3 Address physical root cause of fiber flapping events to improve service SLA to over five 9s.

4 Select best, most competitive service provider for reliability and obtain compensation from the responsible party.

This innovative, VIAVI patented feature is uniquely designed to assist in troubleshooting network flapping. It provides a time stamp of the attenuation event to be correlated to route flapping or error events in your NMS or router topology table. **Customers are able to see the location of these events and advance the troubleshooting process dramatically by detecting and locating ISDFs caused by flash attenuation events, which is especially critical for high-speed rates.**

Case 5: Network Diagnostics and Fiber Aging Using NITRO BI Fiber Insight for ONMSi

Monitoring to accelerate fault detection, location and correction is the goal of the above monitoring use cases, but NITRO enables proactive manage of fiber plant aging. Trends and tracking the impact of network improvement initiatives is incredibly helpful. The NITRO BI Fiber Insight extension to the ONMSi portfolio gives customers the ability to perform big data analysis on current and past network trace events, outages, repairs and to correlate that with network data. By automating the analysis of all the insight hidden in thousands of network fiber events, we can grade each monitored network cable section, provide a trend, and identify the events causing attenuation alarms and changes. **This enables you to prioritize network maintenance down to the optical faults per cable to get the most out of your entire network asset base.**

Nitro Fiber Insight for ONMSi Helps Operators in 3 steps:

1. Access hidden insights from thousands of fiber events

2. Utilize diagnostics and prioritize actions

3. Track results, trend improvements, manage initiatives

| INSTALLATION / ACTIVATION | QUALITY ASSURANCE | CONSTRUCTION | MAINTENANCE | EXPANSION PLANNING | TECHNOLOGY UPGRADES |

Applying network diagnostics, we can quickly inform key decisions and answer questions:

Fiber network diagnostics organize reporting for customer network domains to grade every fiber down to the fault level. Using a global view, fiber certification quality standards can be maintained by targeting the most urgent network hot spots.

Global Optical Network Quality Diagnostics:
Which customers are impacted by the highest priority cable faults?
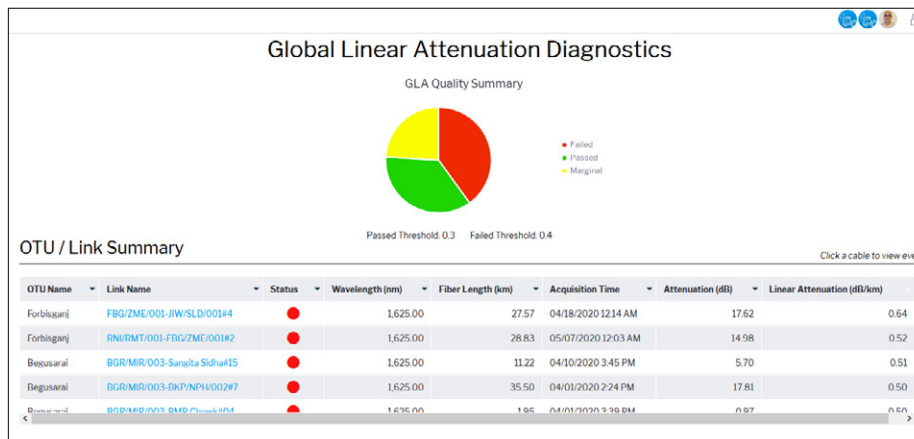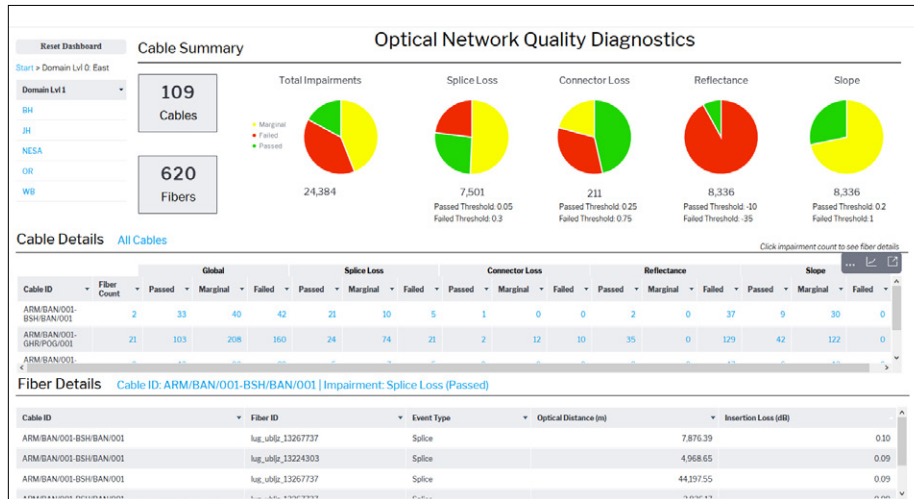
Process Improvement and Acceptance Decisions:

- What remediation should you prioritize to improve service?

- Which cables / KPIs are in trouble?

- Which teams need improvement/training?

- Should this workmanship be accepted or reworked?

Revenue Turn Up Decisions:

- Are optical budgets ready for service upgrades to higher speeds?

- Which lines qualify for exacting SLAs?

- What dark fibers can we offer for customer service?

Summary Overview: The ONMSi RFTS Solution Family Scales to Any Network

The ONMS family provides scalable tools, with several rack-mounted Optical Test Heads containing OTDR and switch combinations. We offer two hardware and two software configurations that scale for a single point location or up to 550 test heads across multiple network domains and teams.

Designing Your Monitoring System

The key to designing your system is to identify your use cases, select the optimal OTDR with help from VIAVI and match your fiber scan time to your network needs so that you can build out your port density plan. One fiber can be scanned in either 10-30 seconds with traditional OTDR tracing or .1 seconds using dedicated VIAVI Flash fiber monitoring. For example, in construction use cases, where the network is not yet in-service, it is optimal to maximize the number of fibers per test head to ensure all fibers can be tested on demand remotely when full coverage of every fiber is required at the lowest cost per fiber. For rapid, repeated monitoring on mission critical fibers, opt for low fiber count in the routine to create a very short scan time that will deliver high monitoring coverage per fiber in the routine.

The scan routine length is determined by the number of fibers in the scan routine set, the fiber length (distance), and the fiber scan algorithm: Many long fibers using a traditional OTDR trace with a rich data set, will generate a longer time before the test unit switch returns to fiber number 1, than a routine with only two, short fibers that are monitored using Flash fiber monitoring.

Software: Either software option, point monitoring SmartOTU or network and test option, ONMSi provide effective alarming, notification, location, and easy recertification after a repair. When a fiber event occurs, it alerts users within minutes (email, SMS, or SNMP).
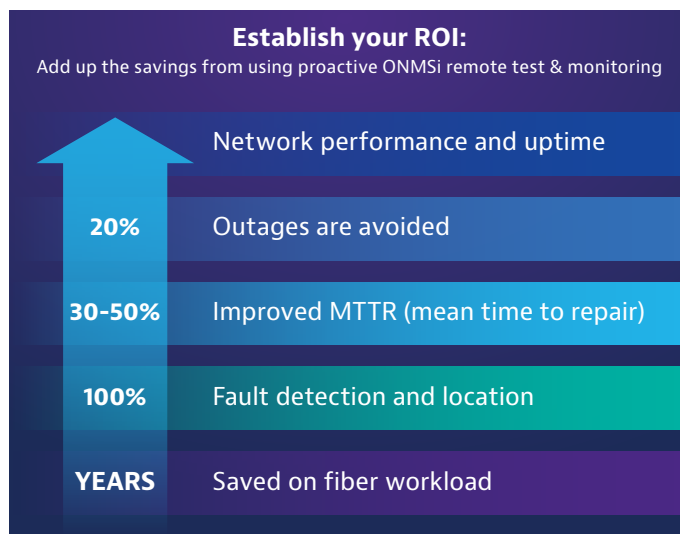
S**martOTU software** is for point-to-point (P2P) monitoring use cases. It can be run right out of the box, on the Optical Test Head with no training or IT configuration.

ONMSi RFTS software adds a database, test head management tool, domain and organizational permissions, and a reporting tool that charts impacts, MTTR, locations of issues and history in the network over time. ONMSi enables the management of the network by domains, network monitoring policies, integration into your ticketing system or GIS, NMS system, corporate sign in process, as well as the NITRO BI Fiber Insight Diagnostics. ONMSi allows integration into other network systems with an API. It supports all VIAVI use cases, including fiber sensing, fiber construction certification, P2P and PON/DAA P2MP monitoring.

NITRO BI Fiber Insight for ONMSi adds a fiber analytics database, and diagnostics reporting, with standard dashboards and reporting capabilities.

Both ONMSi and NITRO Fiber Insight each require a server or two if high availability is required.

Hardware: Both optical test heads support in-service monitoring or dark fiber monitoring depending on the wavelength you select. The tunable DWDM OTDR module, high resolution modules, multi-wavelength or PON optimized modules for the modular 8000 units, there are many in service troubleshooting options that are available for networks using diverse wavelengths.

Establish your ROI:
Add up the savings from using proactive ONMSi remote test & monitoring

	Network performance and uptime
20%	Outages are avoided
30-50%	Improved MTTR (mean time to repair)
100%	Fault detection and location
YEARS	Saved on fiber workload

Two Flexible Choices: Which hardware and which software is right for me?

OTU-5000 Small, Fixed OTDR Form Factor

Up to 16 ports 1/3 RU wide and 1RU high

Optimized for rapid scan Data Center use cases or small PON exchanges, short and medium distances with 1625nm or 1650nm OTDR. Small footprint and low power consumption. Test over 4000 fibers per unit based on switch configuration.

Or

OTU-8000 Modular OTDR Form Factor

1 RU wide and 2RU high with 36 or 48 ports

Modular platform with multiple OTDRs to choose from, including the new tunable DWDM OTDR and high dynamic range OTDRS for long-haul and P2MP networks. Test over 4000 fibers per unit based on switch configuration.

+

SmartOTU Software for single point P2P fundamental monitoring use cases, no server needed.

or

ONMSi Software for or advanced construction, activation, security, and monitoring, including PON/DAA P2MP network use cases. Offers network wide mapping, history, policy control, trending, network domains and permissions.

and

NITRO BI Fiber Insight for ONMSi for network wide diagnostics and reporting

Server(s) required. Optional high availability setup using a redundant server in another location.

VIAVI Solutions

viavisolutions.com