



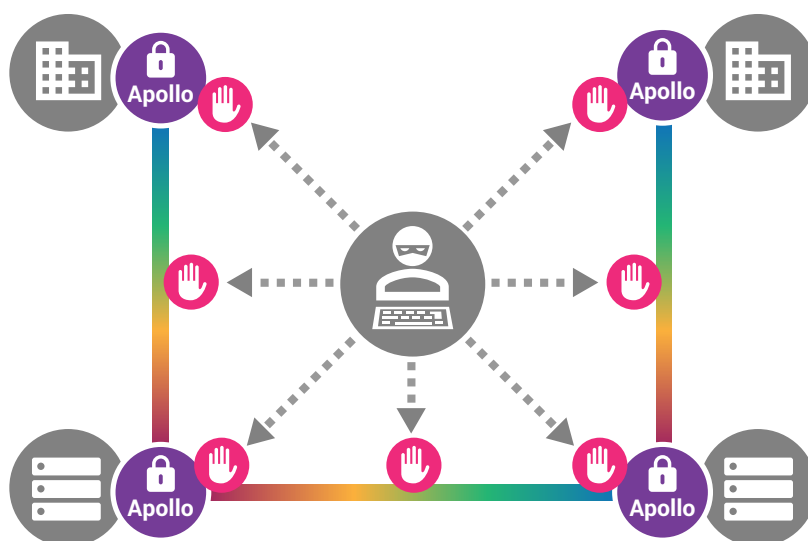
Apollo Optical Encryption



Accelerating Network
Transformation

Apollo Layer 1 Quantum-Safe Optical Encryption

Apollo Layer 1 optical encryption prevents data from being intercepted on wide area optical networks, including attacks like fiber tapping. It provides the highest level of commercial encryption and operates at wire speed with no added latency. To mitigate against threats posed by quantum computing, Apollo strengthens the traditional symmetrical encryption key (SEK) creation process with both post-quantum cryptography (PQC) and quantum key exchange (QKD) techniques.



Value of Optical Encryption

Optical networks, which span large geographic regions, are vulnerable to attacks at multiple locations. The only way to safeguard against data interception through fiber tapping is by employing Layer 1 optical encryption (L1OE). Even if encryption is applied above the optical layer, fiber tapping can still expose unencrypted addressing details, revealing a customer's network structure and communication patterns, along with higher-level OSI stack data that remains unprotected.

Optical encryption is especially appealing since it adds no delay or performance overhead. This advantage is crucial for latency-sensitive applications like synchronous data replication, in which transactions are only completed once data has been mirrored at both sites. Like other multi-layered security systems, optical encryption is now a key part of safeguarding communications networks. It helps ensure data protection for customers and supports compliance with regulations and standards.

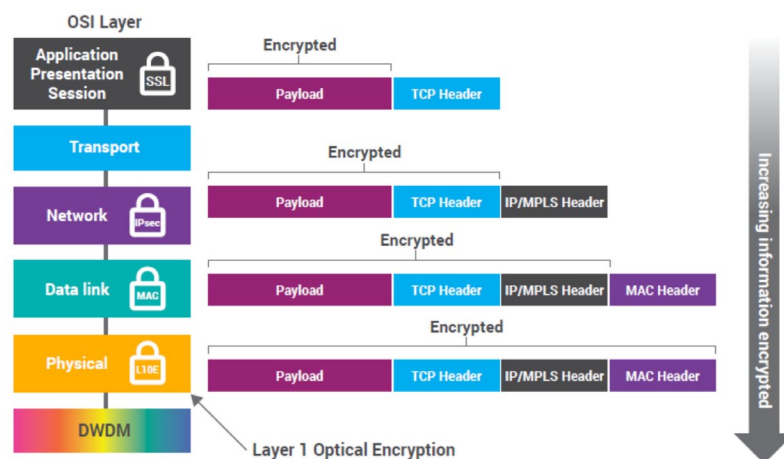


Figure 1 – Positioning of Layer 1 Optical Encryption



Addressing the Quantum Computing Challenge to Encryption

In traditional encryption, the nodes or applications at the ends of a connection use public-private key pairs to algorithmically create a shared secret symmetrical encryption key (SEK). The SEK is then used to encrypt and decrypt data into and from ciphertext.

This can be attacked by using intercepted ciphertext and the known public keys to try and “reverse engineer” the SEK creation algorithm to discover the private keys. However, this is not feasible today using conventional binary computing, as it would require about one hundred years to execute. But the situation changes with the advent of qubit-based quantum computing, where some projections suggest that existing encryption systems could be vulnerable as early as 2030.

The industry is pursuing two approaches to counter this threat, Post Quantum Computing (PQC) algorithms and hardware-based Quantum Key Distribution (QKD). The table below summarizes the main points of the current and new cryptography approaches.

| | Traditional Encryption | Post Quantum Computing (PQC) | Quantum Key Distribution (QKD) |
|--|--|--|---|
| SEK generation method | Established software algorithms like Elliptic Curve Diffie-Hellman are executed at the end nodes | Same as traditional cryptography, but using advanced software algorithms being developed | Specialized hardware that uses principles of quantum mechanics to create and distribute encryption keys |
| Security against quantum computing attacks | Susceptible in a few years | Very high if the algorithms are continuously tested against advances in quantum computing technology | Unbreakable based on physics principles |
| Relative cost | Low | Low | Very high |

Apollo Optical Encryption Solution Overview

Apollo supports all three encryption approaches outlined above. It uses the generated SEKs to encrypt and protect service payloads within OTN-framed signals using AES256-GCM coding, which is the strongest level of commercial encryption. By focusing encryption solely on the OTN payloads, Apollo ensures that encrypted DWDM/OTN networks can carry any client service without causing interoperability problems. Because the unencrypted OTN headers contain no clues about the nature of a service, anyone intercepting the optical line cannot identify the types of services being transmitted—let alone access the actual content.

Apollo Optical Encryption

Figure 2 shows the Apollo L1OE framework for using traditional and PQC algorithmic approaches to creating and using a SEK. The major steps are:

- 1. Authentication** – The Apollo nodes at each end of the encrypted link are authenticated using X.509 certificates in conjunction with the nodes' public-private keys. This can be performed via a trusted partner or a self-signing method that is often used in closed networks.
- 2. Creating Symmetrical Encryption Key (SEK)** – The Apollo nodes employ public key encryption algorithms, using their private and public keys, to create a symmetric “shared secret” encryption key – SEK. Standard Elliptic Curve Diffie Hellman or advanced Post Quantum Computing (PQC) algorithms can be used.
- 3. Message Encryption** – The Apollo nodes use the SEK to encrypt and decrypt data using AES-256.
- 4. Key Rotation** – A primary node (e.g. Node A) sends a “Key ID” over the DCN to the secondary node instructing it which SEK to use next.

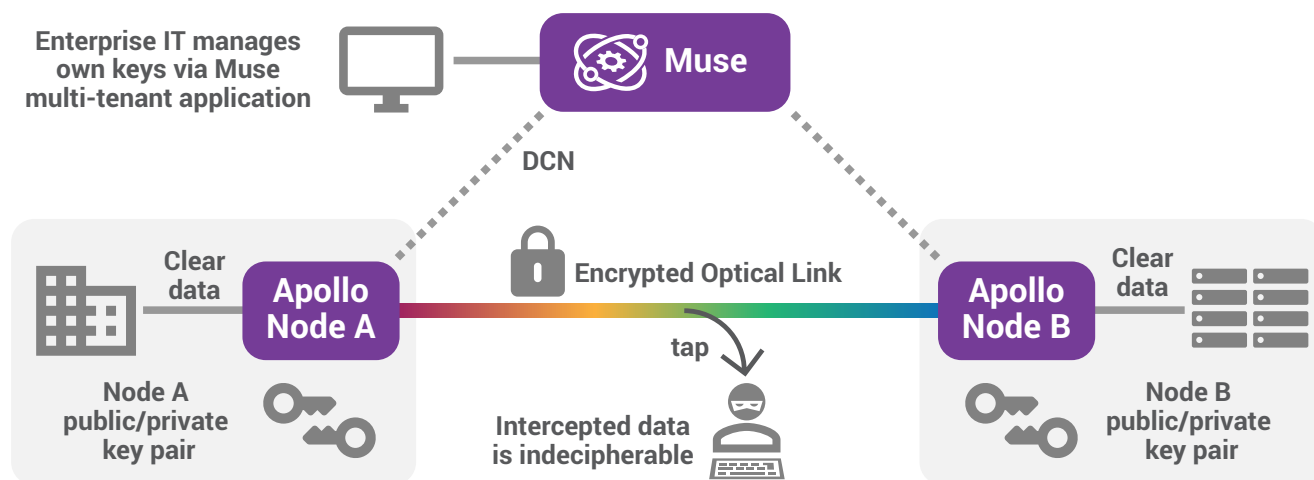


Figure 2 – Apollo Algorithmic Framework for Creating a Symmetrical Encryption Key

Figure 3 shows how Apollo enhances the algorithmic framework to support the creation of SEKs using Quantum Key Distribution. While node authentication is still performed using X.509 certificates, SEK generation is performed by external QKD devices co-located with the Apollo equipment. Apollo communicates with the QKD devices according to the ETSI QKD 014 standard, and Apollo has tested and proved interoperability with multiple QKD device suppliers.

Apollo Optical Encryption

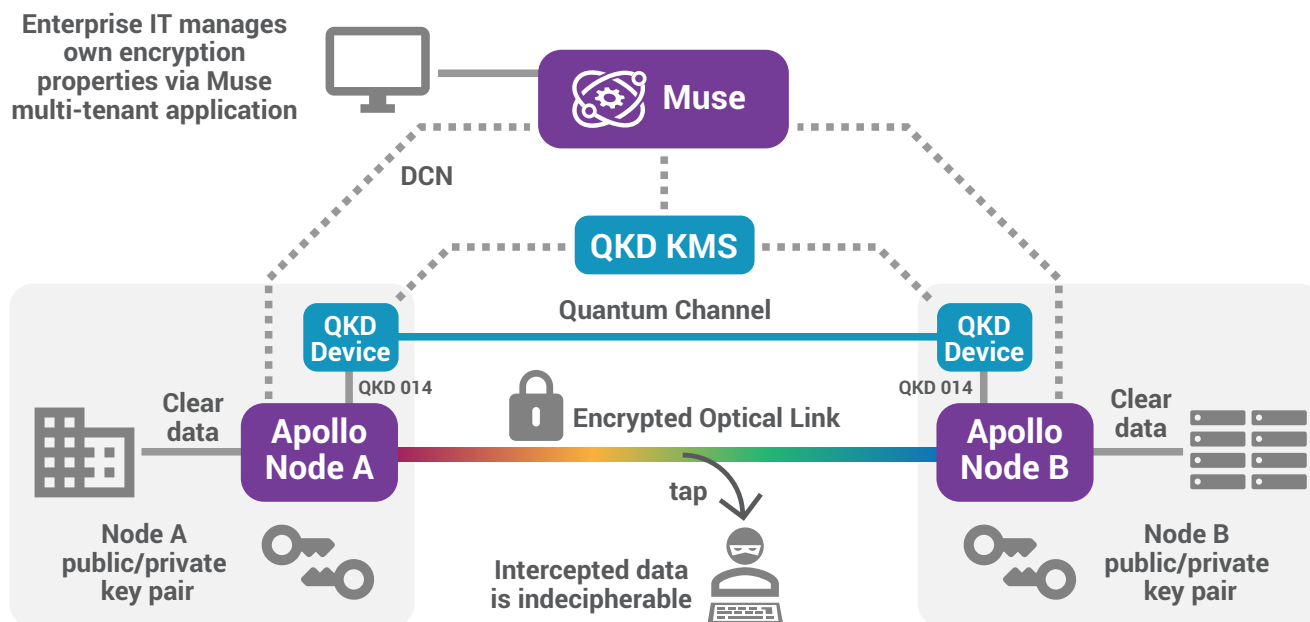


Figure 3 – Apollo QKD Framework for Creating a Symmetrical Encryption Key

Key aspects of Apollo's Layer 1 optical encryption solution are:

- **Service transparency.** All services transported by Apollo can be encrypted. These include 1GbE to 400GbE, as well as Fibre Channel and SDH/SONET services
- **Strongest encryption.** The service payload is encrypted using AES256-GCM coding, which is the highest level of commercial encryption. This is supplemented with an Initialization Vector that ensures no two messages are encrypted the same way, and a Message Integrity Check that safeguards against message tampering.
- **Multiple Symmetric Encryption Key generation methods.** SEKs can be created using traditional, PQC, or QKD approaches. Moreover, the private keys (which are fundamental to the algorithmic approaches and used for authentication with QKD) never leave the Apollo cards at the endpoints of each link.
- **Trusted authentication.** X.509 end-point authentication, which is a part of the key exchange process, can be self-signed, as is often the case in a closed network, or can rely on a trusted 3rd-party.
- **Tampering security.** Apollo provides FIPS 140-3 compliant cards, which show evidence of physical tampering attempts with the encryption and key management mechanisms. This certification is often mandated by government agencies and regulated sectors.
- **Alien wavelengths.** Apollo optically encrypted signals can be transported as alien wavelengths on foreign networks.
- **Third-party management.** The Muse Multilayer Automation Platform manages Apollo NEs. Using a Muse multi-tenant application, the IT departments of Enterprises can oversee their encrypted links without involving a service provider who may be delivering the network. Capabilities include:
 - Selecting which services to encrypt
 - Monitoring the operational status of the encrypted optical services
 - Obtaining security alarms
 - Updating login password/profile
 - Rotating keys on FIPS-140-3 SL3 tamper proof cards

Apollo 9600 Series DWDM/OTN Transport Encryption Solution

The Apollo 9600 series provides highly flexible DWDM/OTN transport of service interfaces based on a family of small (2RU), medium (5RU), and large (15RU) platforms that use a common set of line cards for transponder, muxponder, amplification, and ROADM functions.

The primary line card supporting L1 Optical Encryption is the TM400ENB. As shown in Figure 4, the TM400ENB provides per-service encryption with each service having a unique secure session key for added security. It can support any mix of services up to the 400G limit. The OTN-framed output signal can be transported transparently as a native wavelength over an Apollo DWDM/OTN network or carried as an alien wavelength over a third-party DWDM network.

Using the TM400ENB, service providers can now install the hardware for a high-speed 400G network on day one and offer both encrypted and unencrypted services to their clients. Existing clients can be upsold at any time to an encrypted service without the need to replace any hardware, and the service can be enabled instantly via software commands. There is no need to install expensive hardware that will sit idly in anticipation of future encryption needs, and there is no need to give away encryption for free on a link, just because one client has requested that feature.

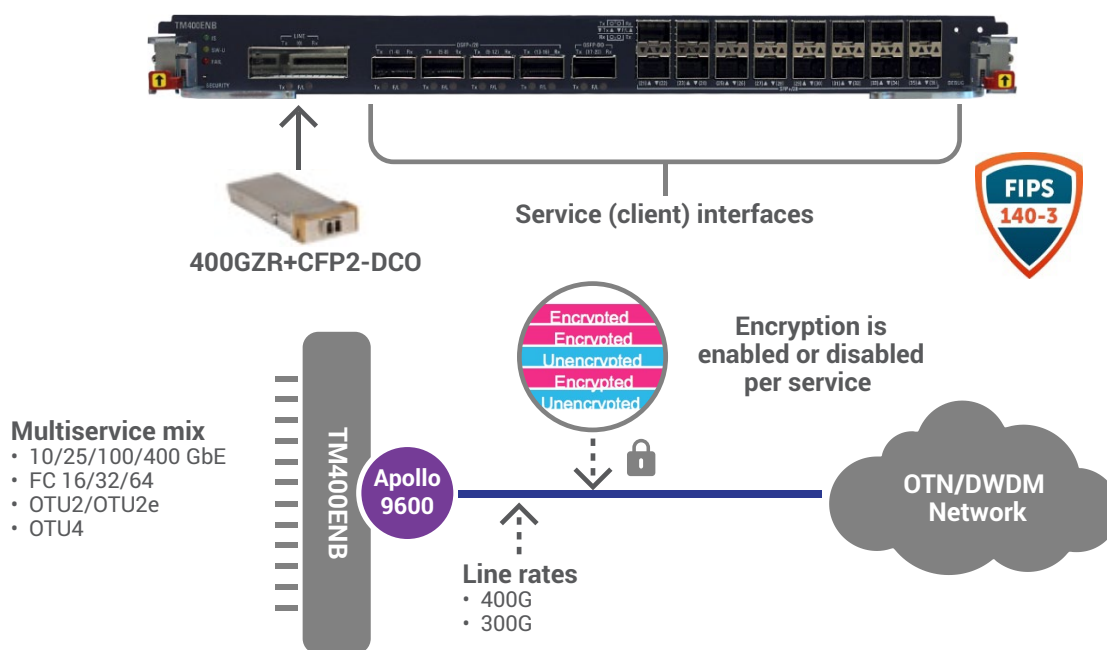





Figure 4 – Apollo TM400ENB 400G Multiservice Encryption Muxponder

Apollo 9600 platforms also support the following cards:

- TM800_2EN with dual 800G uplinks for a mix of 100GbE and 400GbE clients;
- TM200ENB with a 200G uplink for 10/40/100GbE, FC8/32, STM64, and OTU2/e clients.

Apollo 9600 Series
Modular OTN/DWDM

- Rich set of transmission and OLS cards, usable across all platforms without engineering rules
- Telco and data center



96039608/D9624

Apollo 9900 Series OTN Switching Encryption Solution

Apollo provides a scalable access-to-core OTN switching solution that enables automated grooming of services onto wavelengths, rapid service provisioning, and dynamic restoration. As each link within an OTN-switched network aggregates multiple services at high density, the emphasis is on ensuring end-to-end OTN link encryption with seamless interoperability among the OTN switching platforms. This is enabled by:

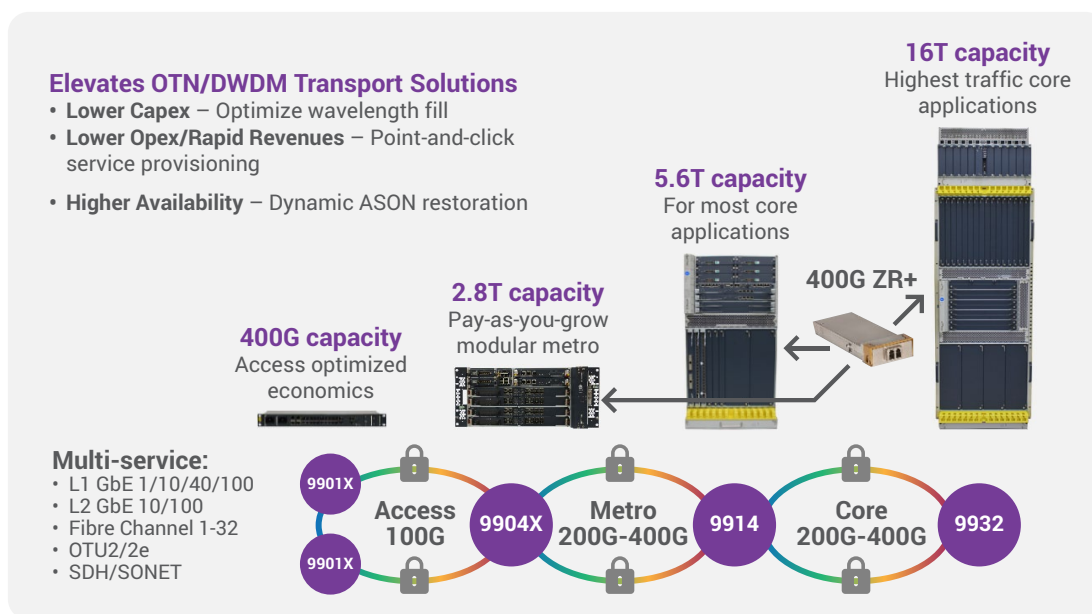


Figure 5 – Apollo 9900 OTN Switching Encryption Solution

- **HIO400EN** – Multiservice card for the OPT9914 and OPT9932 providing 200G encrypted links.
- **MIO200BEN** – Multiservice card for the OPT9904X, providing 100G encrypted links.
- **9901X** – Access OTN switch optimized to replace multiplexers and F-OADM's to flexibly and rapidly provision multiple types of L1 services. The 9901X is a highly versatile platform that supports optical encryption in multiple configurations; both interworking with other OTN switches as well as in a standalone mode. A primary application, illustrated below, is an Add-Drop Multiservice Multiplexer on an Access Ring. This gathers and grooms client traffic onto encrypted 100G wavelengths that can be processed end-to-end by Apollo OTN switches.

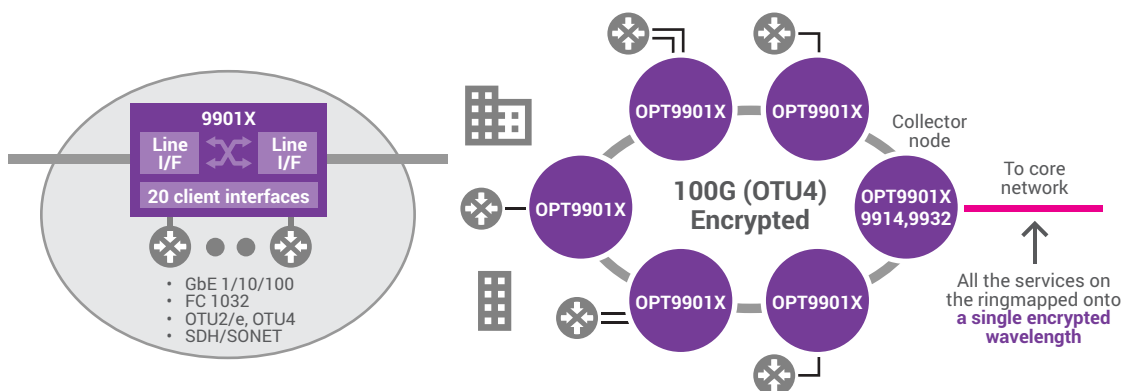


Figure 6 – Apollo 9901X Software Controlled Add/Drop Ring Application

Optical Encryption as a MOFN Service

Managed Optical Fiber Networks (MOFNs) are becoming an important application in response to the rapid growth of data centers. Service providers, who own dark fiber, have an opportunity to build and deliver MOFNs for data center interconnect to cloud and colocation data center companies, as well as to enterprises.

With an increased focus on security and the ease with which optical layer encryption can be added to any optical channel, optical encryption presents service providers with a value-added service offering to their MOFN offerings.

Optical encryption as a service also acts as a differentiator. By providing the same service at a similar price, but with the added security of optical layer encryption enabled by Apollo, service providers can differentiate their services from competitors.

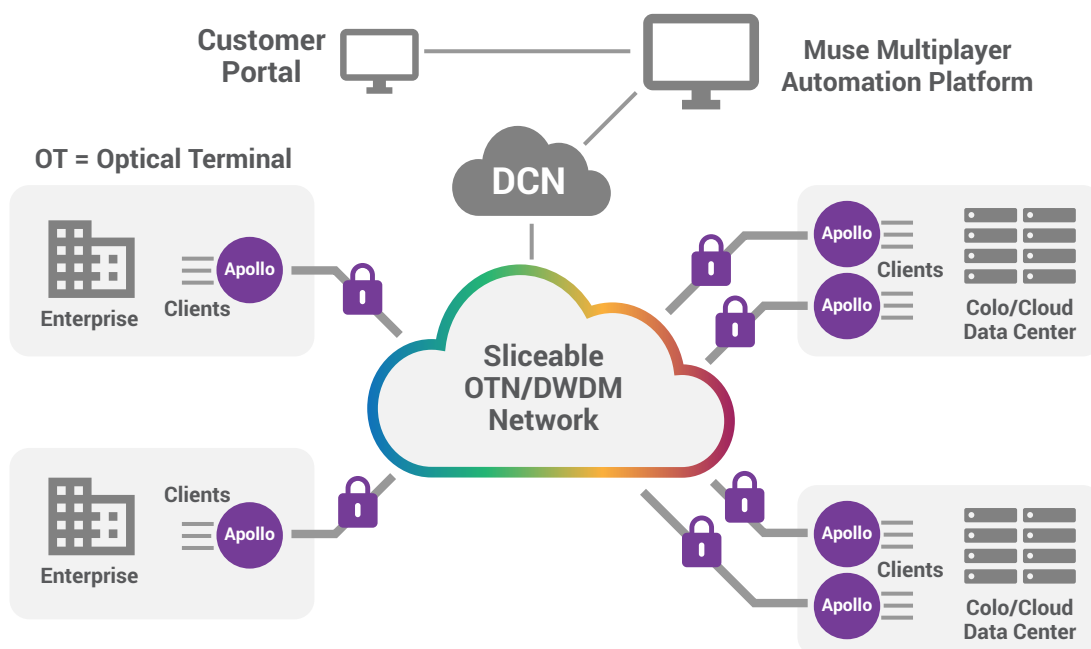


Figure 7 – MOFN with Optical Encryption

It's Time to Optically Encrypt

In a world where network and data security has become a daily concern, optical layer encryption is a powerful tool in the fight against unwanted intrusion. Ribbon's cost-effective and flexible Apollo optical networking system adds layer 1 optical encryption easily to any network, allowing network operators to use it for internal purposes or to extend it as a value-added service to end user customers. Apollo optical layer encryption adds no overhead and virtually zero latency. It blacks out all information about the payload and higher level addressing, and can be applied to any service type.

Contact Us

Contact us to find out how Apollo protects your optical network.

About Ribbon

Ribbon Communications (Nasdaq: RBBN) delivers communications software, IP and optical networking solutions to service providers, enterprises and critical infrastructure sectors globally. We engage deeply with our customers, helping them modernize their networks for improved competitive positioning and business outcomes in today's smart, always-on and data-hungry world. Our innovative, end-to-end solutions portfolio delivers unparalleled scale, performance, and agility, including core to edge software-centric solutions, cloud-native offers, leading-edge security and analytics tools, along with IP and optical networking solutions for 5G. We maintain a keen focus on our commitments to Environmental, Social and Governance (ESG) matters, offering an annual Sustainability Report to our stakeholders. To learn more about Ribbon visit rbbn.com.