WDM Encrypted

Encrypted data, the ultimate protection against cybercrime

- Encryption in the optical layer
- Available at excellent speeds up to 100 Gb/s
- Low latency: < 1 msec. per 100 km
- Encryption is protocol-independent
- Certified FIPS 197 for AES-256 encryption
- Certified FIPS 140-2 Level 2 for hardware encryption
- Separated encryption for authentication and encryption based on X.509

Over half of all organizations face a security incident at least once a year, and cybercrime continues to rise steadily. As a result, data protection is a growing concern for most organizations. Governments respond by introducing tougher legislation which ensures that European organizations process as well as protect their data with all due care. You can minimize these security risks with Eurofiber's WDM Encrypted, which provides intrinsic protection for your data transport.

Data encryption is key

A fiberoptic connection is generally used to exchange data between different locations. The Eurofiber fiberoptic network is completely underground, housed in a solid conduit and robust hand-hole. A fiberoptic connection eventually ends up somewhere above the ground – for instance when the cable enters the building via a parking garage or a main or satellite equipment room. It is highly unlikely that this fiberoptic connection can be tapped, but the possibility cannot be excluded entirely. Eurofiber provides demonstrable guarantees that intercepted data cannot be used by anyone tapping the connection. Eurofiber's WDM Encrypted makes it possible to safely encrypt data that is sent across a network.

How does encryption work?

Cryptography techniques are an important part of data protection. The data is encrypted to protect confidential information against threats such as malware abuse and unauthorized access by third parties. Encryption is the procedure used to encode and decode data. An algorithm is used to ensure that the information is no longer in its original form and can no longer be read without a specific encryption key.

eurofiber

Three types of encryption

Encryption on the network is possible in various ways:

1. **Hardware-based encryption**
   If you share a large amount of privacy-sensitive and confidential information, then this is a good method. This solution uses specific hardware to provide the encryption key. If a hacker tries to get into this hardware and opens it, then the key is automatically erased.
2. **Software-based encryption**
   This solution makes it possible to make a specify which data needs to be encrypted and which can be left unencrypted. A downside is that it generates more latency, which will have a negative impact on the speed of the connection.
3. **Encryption via the physical network**
   This encryption solution on the optical layer does not affect speed or performance. In addition, the data is also protected from intercepts during transport.

The benefits of optical encryption

Many encryption solutions operate at the IP layer (OSI layer 3). WDM Encrypted, on the other hand, applies hardware and software encryption in the optical layer (OSI layer 1). The advantage: up to a thousand times less latency, ensuring a faster connection. In addition, the protective security layer is transparent and protocol independent.

Underlying connectivity service

To make the most efficient use of a fiberoptic connection, for instance between datacenter locations, the WDM (Wavelength Division Multiplexing) connectivity service is used, while applying encryption. By using different frequencies, multiple secure connections can be configured across the same fiberoptic connection, e.g. Fiber Channel for storage and Ethernet for servers.

FIPS 140-2 Level 2 and X.509 standard

Eurofiber's WDM Encrypted is FIPS 197 certified for AES-256 encryption and FIPS 140-2 Level 2 for encryption hardware. This is an encryption standard used by the federal government of the USA, which is being adopted by more and more national governments, as well as institutions in the financial and healthcare sectors. It is the highest measurable standard that can be validated (higher than the German BSI). In addition, WDM Encrypted uses the global X.509 certificates for data encryption and authentication. The certificate is authenticated and verified by the internationally accepted digital Public Key Infrastructure (PKI).

Taking control of your key management

For more stringent security, we can facilitate your organization in handling your own key management. You can keep control of issuing and checking your encryption keys based on your own PKI. This eliminates the need for a third party to be involved in key management, thus minimizing the risk that your data will end up in the hands of third parties. Eurofiber will help you get started on software configuration for key management and will provide training for your security officer.

Service Level Agreement

Depending on the configuration, WDM Encrypted has a minimum availability of 99.9% per year. If the service is unexpectedly unavailable, you can contact the Eurofiber Network Monitoring Center 24/7 to report the problem. In the event of a business-critical failure, we guarantee that the problem will be solved within 4 hour

Armed against cybercrime

Hackers continue to develop new ways to get their hands on privacy-sensitive information. Protect your data with encryption using Eurofiber's WDM Encrypted. Arrange better protection from the surge in cybercrime and comply with strict privacy laws.

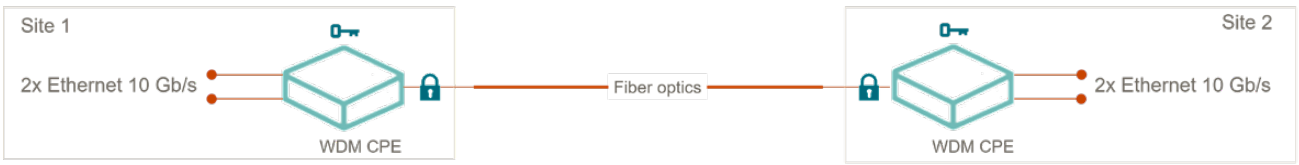
*In case of a ruptured fiber, we guarantee a maximum repair time of 8 hours.

eurofiber

Three solutions tailored to your needs

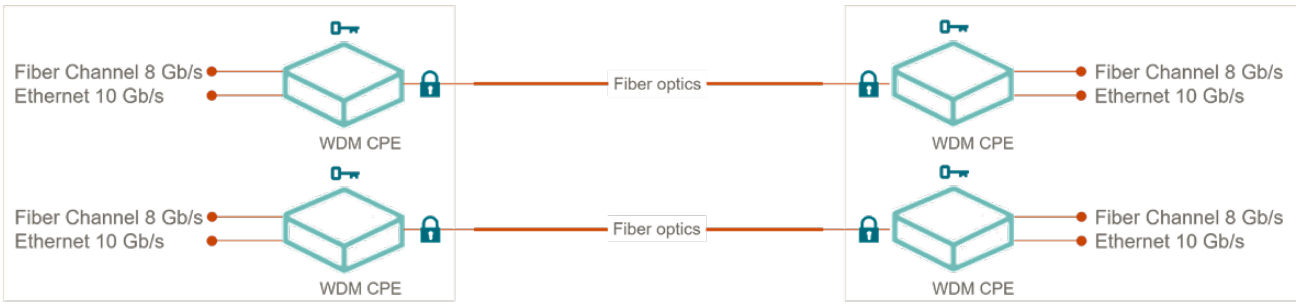
WDM Encrypted is partly determined by its specific application in your situation, but it comes down to three basic propositions

1. Site-to-site connection



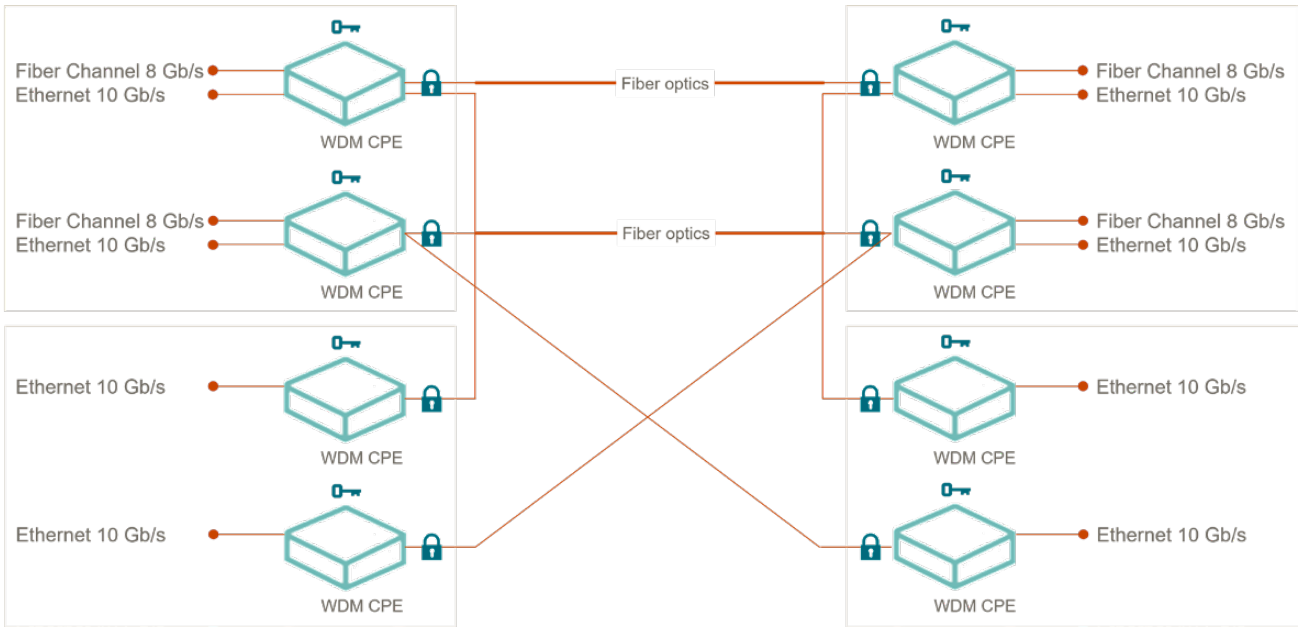
This solution provides a single encrypted LAN connection between two locations, for which you choose a specific protocol and bandwidth. In this example, the connection is configured for two times 10 Gb/s Ethernet. The availability of the connection is 99.9% per calendar year.

2. Twin DCI connection



This solution provides a completely separate, redundant connection between two datacenters for the purpose of data replication. Eurofiber has a wide range of bandwidths available for Ethernet and Fiber Channel protocols. In this example, each route is configured for 1x Fiber Channel with an 8 Gb/s bandwidth and a 1x Ethernet with a 10 Gb/s bandwidth. The combined availability of this solution is 99.98% per calendar year.

3. Twin DCI + Sites



This solution is a combination of the Twin DCI solution (see above) and a redundant connection from two locations to both datacenters. In addition to the above specifications for Twin DCI, both sites are also connected to a datacenter and a 10 Gb/s Ethernet connection. This configuration is often used in a private cloud environment, in which business-critical applications are hosted in the datacenters and accessed from

Contact

For more information about WDM Encrypted, please contact our sales department at +31 (0)30 242 87 00 or info@eurofiber.com.