In the area of cross linking locations in a metropolitan region (MAN), **Ethernet over Fiber** increasingly replaces the traditional leased lines or radio based connections. The direct interconnection of Fast- or Gigabit-Ethernet structures results in a LAN spanning across several locations. Since parts of this LAN are linked via public networks, there is the risk of tapping and manipulation. In the worst case, third parties may gain access to the internal structure of the network.

These threats demand for the protection of the public accessible parts of the LAN. If this protection can be achieved without changes in the network infrastructure and workflows, the resulting security solution will be highly acceptable.

The **ATMedia Gigabit Encryptor** realizes this by a very simple integration (bump in the wire) into the existing Gigabit Ethernet structure. The hardware encryption at network layer 2 allows a **fully transparent operation** in respect of higher protocols and does not cause any measurable effect on LAN operation.
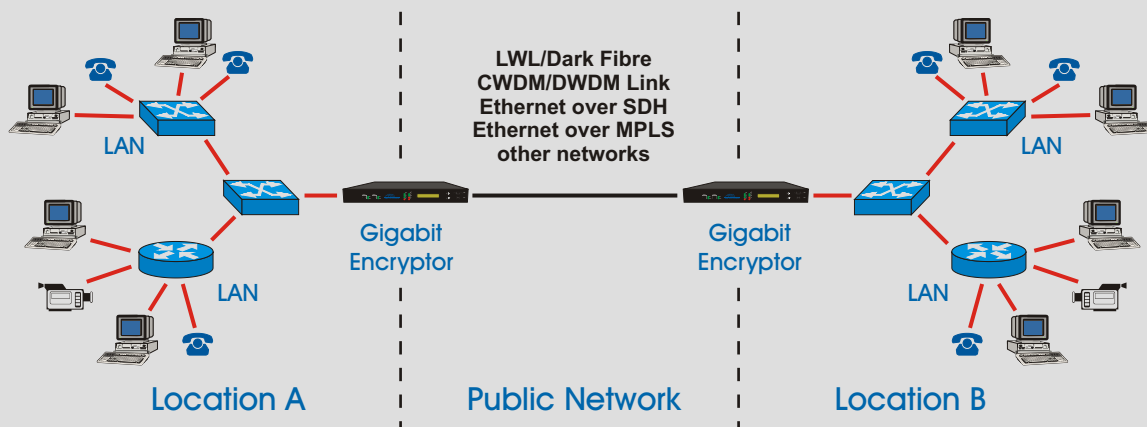
ATMedia Gigabit Ethernet Encryptor

Highlights of the ATMedia Gigabit Encryptor

- Transparent to VLAN and MPLS, support of Jumbo frames
- Full-duplex encryption at Gigabit Ethernet line rate
- No encryption overhead
- Network integration without any change of infrastructure (Bump in the wire)
- Maintenance-free operation
- Exchangeable fibre optics

Application scenario

LWL/Dark Fibre
CWDM/DWDM Link
Ethernet over SDH
Ethernet over MPLS
other networks

LAN

LAN

Gigabit Encryptor

Gigabit Encryptor

LAN

LAN

Location A   Public Network   Location B

Technical Data

Encryption Performance

- Real-time encryption of Ethernet connections (IEEE 802.3)
- 1000 mbps full-duplex throughput independent of packet size, no encryption overhead
- Key change without interruption of traffic
- Additional latency: $< 15\mu s$ per device

Crypto Technology

- AES (256 bit) encryption with CBC block mode
- Key generation with hardware random source
- Key exchange with Diffie-Hellman ECC algorithm

Key management:

- Device authentication with passphrase/hostkey
- Tamper resistant key storage
- Automatic time triggered change of session keys
- Autonomous operation without external key management

System management:

- Configuration via serial console (RS-232/V.24) or SSH network (Ethernet RJ45-10/100BT) access
- Integrated monitoring of network status and operation
- Audit and event logging
- Remote monitoring via SNMP (V2c/V3)
- Link monitoring via ATMedia CryptMon

Hardware:

- Support of Jumbo Frames
- Transparent to VLAN and MPLS
- SFP modules: RJ45-1000BT, Multi Mode 850 nm, Single Mode 1310/1550 nm SR/IR/LR, CWDM, DWDM
- Tamper resistant housing
- 19" 1RU chassis (h: 44mm, w: 430mm, d: 320mm)
- Redundant hot-swap PSU: 110-240V AC 50-60Hz or -48V DC

The ATMedia systems and related documentation are subject to continuos improvement.
Therefore ATMedia reserves the right to change documentation without notice.

ATMedia GmbH - High End Data Communication Made in Germany

20062905G