In the area of cross linking locations in a metropolitan region (MAN) or in a Wide Area Network (WAN), **Ethernet** technologies increasingly replace the traditional point-to-point connections. The direct interconnection of 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 Ethernet Encryptor** realizes this by a very simple integration (bump in the wire) into the existing 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.
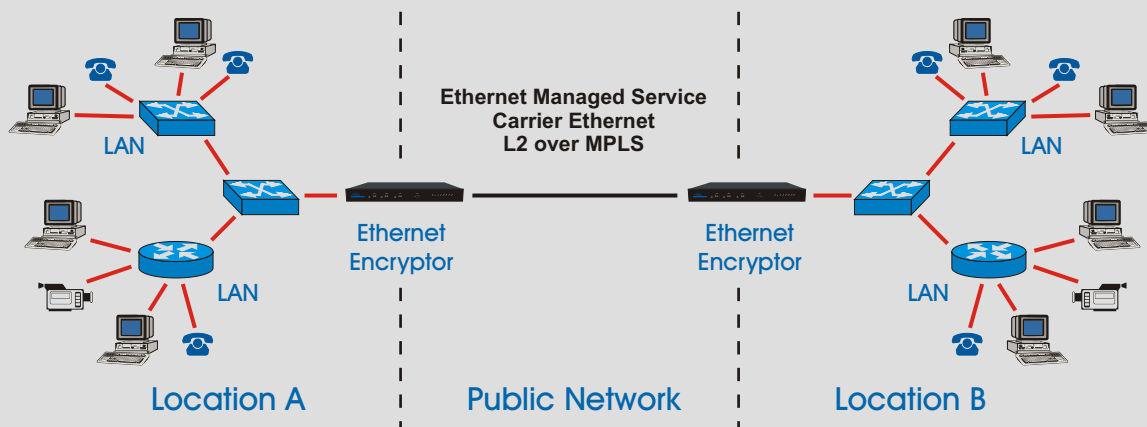
ATMedia Ethernet Encryptor

Highlights of the ATMedia Ethernet Encryptor

- Encryption of 10/100BT Ethernet connections at layer 2 in hardware
- Transparent to VLAN and MPLS
- Full-duplex encryption at line rate
- Low and constant latency
- Network integration without any change of infrastructure (bump in the wire)
- Maintenance-free operation
- Adhoc authentication

Application scenario

Ethernet Managed Service
Carrier Ethernet
L2 over MPLS

LAN LAN LAN LAN

Ethernet Encryptor   Ethernet Encryptor

Location A   Public Network   Location B

Technical Data

Encryption Performance

- Real-time encryption of 10/100BT Ethernet connections (IEEE 802.3)
- Full-duplex throughput independent of packet size
- Key change without interruption of traffic
- Additional latency: < 0,037ms 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
- Complies with the requirements of FIPS 140-2 L3 and CC EAL3

Key management:

- Ad-hoc device authentication
- 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
- Link Loss Carry Forward
- RJ45 10/100BT copper interfaces
- Tamper resistant housing
- 19" 1RU chassis (h: 44mm, w: 430mm, d: 230mm)
- PSU: 110-240V AC 50-60Hz, 11W

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

20081305E