atmedia
secure data communication

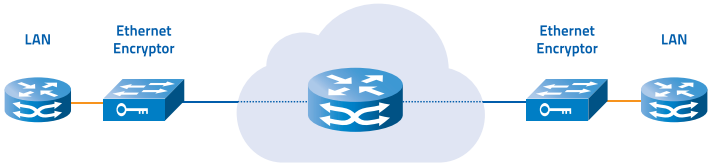
Ethernet Encryption

atmedia Encryptor

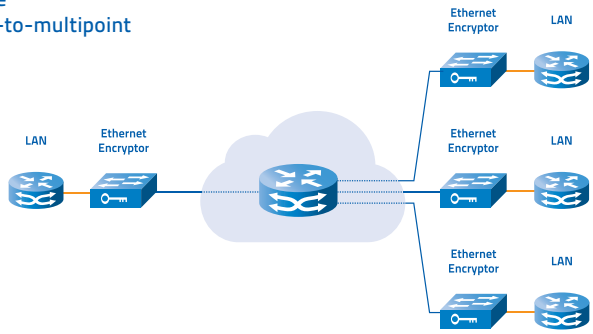
In the area of layer 2 Ethernet networking, a fast-growing number of network providers is offering their customers multi-point enabled WAN services. The technical realization reaches from simple hub-and-spoke solutions to advanced Carrier Ethernet, Metro Ethernet or VPLS technologies. From the customers point of view, these solutions look like a LAN distributed over multiple sites that can be directly connected to Ethernet devices. Unlike traditional point-to-point networks which offer a strong separation between users, this separation is a „virtual" one only. This however results in a substantial risk of unwanted interconnection between the networks of different users and could enable unauthorized third parties to get full access to the internal network. The atmedia Ethernet Encryptor saveguards Ethernet multipoint scenarios as efficient as point-to-point scenarios against tapping and manipulation. The encryptor is working fully transparent at network layer 2 and encrypts the network independent of the network devices and user applications. The deployment of the encryptor does not require any change of network infrastructure or existing redundancy scenarios.

Application scenarios

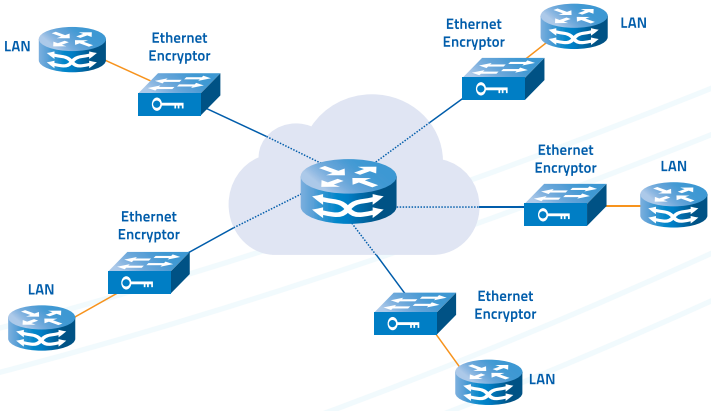
E-Line
point-to-point



E-Tree
point-to-multipoint



E-Lan
multipoint-to-multipoint



Highlights

- Strongest crypto technology available (AES-GCM, ECC)
- Integrity- and replay-protection of transmitted data
- Full-Duplex real-time encryption
- Compatible to E-Line, E-Tree, E-Lan, VPLS, VPWS and other Ethernet services
- Transparent to VLAN/CoS, MPLS and FCoE
- Encryption of unicast, multicast and broadcast traffic
- Interoperable from 10 mbps to 10 gbps
- Network integration without any change of infrastructure (bump in the wire)
- Highly scalable
- No impact on existing redundancy mechanisms
- Compliant to the requirements of FIPS 140-2 L3 and CC EAL4
- Certified for the transmission of classified data by the German BSI (restricted)

atmedia GmbH
Science Park 1
66123 Saarbrücken
GERMANY

Tel: +49 681 84 24 77
Fax: +49 681 84 24 81

crypt@atmedia.de
www.atmedia.de

atmedia
secure data communication

Technical Data

Ethernet Security

Performance
▪ Multi tenant group encryption (max. 1000 peers)
▪ Real-time encryption of the Ethernet payload (IEEE 802.3)
▪ Encryption independent of packet size and packet content
▪ Key changes without interruption of traffic
▪ Latency per device: 100M: ≤ 0,040ms, 1G ≤ 0,008ms, 10G: ≤ 0,004ms

Key Management
▪ Ad-hoc device authentication
▪ Tamper resistant key storage
▪ Built-in key server for the distribution of group keys
▪ Automatic time triggered change of master keys and group keys

Network
▪ Compatible to E-Line, E-Tree, E-Lan, VPLS, VPWS and other Ethernet services
▪ Support of Jumbo frames
▪ Transparent to VLAN (incl. Q-in-Q), CoS, MPLS, Fibre Channel over Ethernet (FCoE)
▪ Optical Loss Pass-through (Link Loss Carry Forward)

Line interfaces	
10 M:	10Base-T TP RJ45 Full-Duplex
100 M:	10/100Base-T TP RJ45 Full-Duplex
1 G:	SFP-modules
	1000Base-T SFP TP RJ45
	1000Base-X SFP MM LC (62,5/125µ)
	1000Base-X SFP SM LC (9/125µ) SR/IR/LR
	1000Base-X SFP DWDM/CWDM
10 G:	XFP-modules
	10GBase-R XFP MM LC (62,5/125µ)
	10GBase-R XFP SM LC (9/125µ) SR/IR/LR
	10GBase-R XFP DWDM/CWDM, tunable DWDM

Crypto Technology
▪ AES (256 bit) encryption
▪ Integrity and replay protection with Galois Counter Mode (GCM)
▪ Key generation with hardware random source
▪ Key exchange with Diffie-Hellman ECC algorithm (DH-ECKAS)
▪ Compliant to the requirements of FIPS 140-2 L3 and CC EAL4

System Management
▪ Configuration via serial console (RS-232/V.24) or Secure Shell (SSH) network access (out-of-band Ethernet RJ45-10 /100BT)
▪ Integrated monitoring of network status and operation
▪ Audit and event logging
▪ Remote monitoring via SNMP (V2c/V3 authpriv)
▪ Link monitoring via atmedia CryptMon

Hardware	
Operating temperature: 1°C - 40°C	
Relative humidity:	10% - 85%, non condensing
10M / 100M:	482,6mm (19") 1RU, H: 44mm, W: 430mm, D: 230mm, Weight: 4kg Redundant PSU: 10-240V AC 50-60Hz, 11W
1G:	482,6mm (19") 1RU, H: 44mm, W: 430mm, D: 320m, Weight: 7kg, Redundant Hot-Swap PSU: 110-240V AC 50-60Hz or -48V DC, 90W
10G:	482,6mm (19") 2RU, H: 88mm, W: 430mm, D: 370mm, Weight: 10kg, Redundant Hot-Swap PSU: 110-240V AC 50-60Hz or -48V DC, 115W
Chassis:	Tamper resistent design

Conformity:
▪ CE, FCC

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

atmedia GmbH
Science Park 1
66123 Saarbrücken
GERMANY

Tel: +49 681 84 24 77
Fax: +49 681 84 24 81

crypt@atmedia.de
www.atmedia.de