

Bei der Vernetzung von Standorten im stadtnahen Bereich (MAN) und im WAN verdrängt **Ethernet** immer mehr die traditionellen Punkt-zu-Punkt Verbindungen. Durch die direkte Koppelung der Ethernet Strukturen entsteht meist ein über mehrere Standorte verteiltes LAN. Da dieses LAN über öffentliche Leitungswege geführt wird besteht die Gefahr, dass Daten mitgelesen und manipuliert werden können. Zusätzlich können Dritte Zugriff auf die interne Infrastruktur des Netzes erlangen.

Darum muss der über öffentliche Leitungswege geführte Teil des LANs gegen solche Angriffe geschützt werden. Eine hohe Akzeptanz der Sicherheitslösung wird erreicht, wenn keine Änderungen der Netzwerkstruktur und der Betriebsabläufe notwendig sind.

Der **ATMedia Ethernet Verschlüsseler** ermöglicht dies durch einfaches Einschleifen in die vorhandene Ethernet Netzwerkstruktur (bump in the wire). Aufgrund der **Hardware-Verschlüsselung auf Netzwerkebene 2** arbeitet das Gerät transparent bzgl. höheren Netzwerkprotokollen und ohne messbaren Einfluss auf das LAN.

ATMedia Ethernet Verschlüsseler



Highlights des Ethernet Verschlüsselers

- Voll-Duplex Verschlüsselung mit Leitungsgeschwindigkeit
- Transparent für VLAN, CoS, MPLS
- Verschlüsselung von Unicast, Multicast und Broadcast Traffic
- Unterstützung von Jumbo Frames
- Unabhängig von den verwendeten Endgeräten und Applikationen
- Keinerlei Änderung in der Netzwerkinfrastruktur notwendig
- Kein Einfluss auf vorhandene Redundanzszenarien
- Zugelassen für Verschlusssachen

Anwendungsszenario



Technische Daten

Leistungsdaten

- Punkt-zu-Punkt Ethernet Verschlüsselung
- Echtzeit Verschlüsselung der Ethernet Payload (IEEE 802.3)
- Durchsatz: Leitungsgeschwindigkeit, unabhängig von der Paketgröße
- Schlüsselwechsel ohne Unterbrechung des Links
- Latenz: 100M: $\leq 0,040\text{ms}$, 1G $\leq 0,008\text{ms}$, 10G: $\leq 0,004\text{ms}$ je Gerät

Verschlüsselungstechnologie

- AES (256 Bit) Verschlüsselungsverfahren mit CBC Block Modus
- Schlüsselerzeugung durch Hardware Zufallszahlengenerator
- Schlüsselaustausch über Diffie-Hellman ECC Verfahren (DH-ECKAS)
- Konform zu den Anforderungen von FIPS 140-2 L3 und CC EAL3

Schlüsselmanagement

- Ad-hoc Authentifizierung
- Manipulationsgeschützte Schlüsselspeicherung
- Automatischer Wechsel der Verbindungsschlüssel nach konfigurierbarem Zeitintervall
- Autonomer Betrieb ohne externes Schlüsselmanagement

Systemmanagement

- Konfiguration über serielle Konsole (RS-232/V.24) oder Secure Shell (SSH) Netzwerkzugang (Out-of-Band Ethernet RJ45-10/100BT)
- Integrierte Leitungs- und Betriebsüberwachung
- Audit und Event Logging
- Abfrage des Betriebszustandes über SNMP (V2c/V3 authpriv)
- Überwachung des Linkstatus mittels ATMedia CryptMon

Netzwerk

- Kompatibel mit E-Line, E-Tree, E-Lan, VPLS, VPWS und anderen Ethernet Services
- Unterstützung von Jumbo Frames
- Transparent bzgl. VLAN (auch Q-in-Q), CoS, MPLS, Fibre Channel over Ethernet (FCoE)
- Optical Loss pass-through (Link Loss Carry Forward)
- Line Interfaces

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

Hardware

- Arbeitstemperatur: 1°C - 40°C
- Luftfeuchtigkeit: 10% - 85%, nicht kondensierend
- 10M/100M: 482,6mm (19") 1HE, H: 44mm, B: 430mm, T: 230mm, G: 4kg
Redundante Stromversorgung: 110-240V AC 50-60Hz, 11W
- 1G: 482,6mm (19") 1HE, H: 44mm, B: 430mm, T: 320mm, G: 7kg
Redundante Hot-Swap Stromversorgung
110-240V AC 50-60Hz oder -48V DC, 90W
- 10G: 482,6mm (19") 2HE, H: 88mm, B: 430mm, T: 370mm, G: 10kg
Redundante Hot-Swap Stromversorgung
110-240V AC 50-60Hz oder -48V DC, 115W
- Gehäuse: Tamper resistentes Design
- Konformität: CE, FCC

Die ATMedia Systeme sowie die zugehörige Dokumentation werden ständig auf dem neuesten Stand der Technik gehalten. ATMedia behält sich daher vor, entsprechende Änderungen jederzeit und ohne vorherige Ankündigung durchzuführen.