Layer 2 Ethernet Link Verschlüsselung

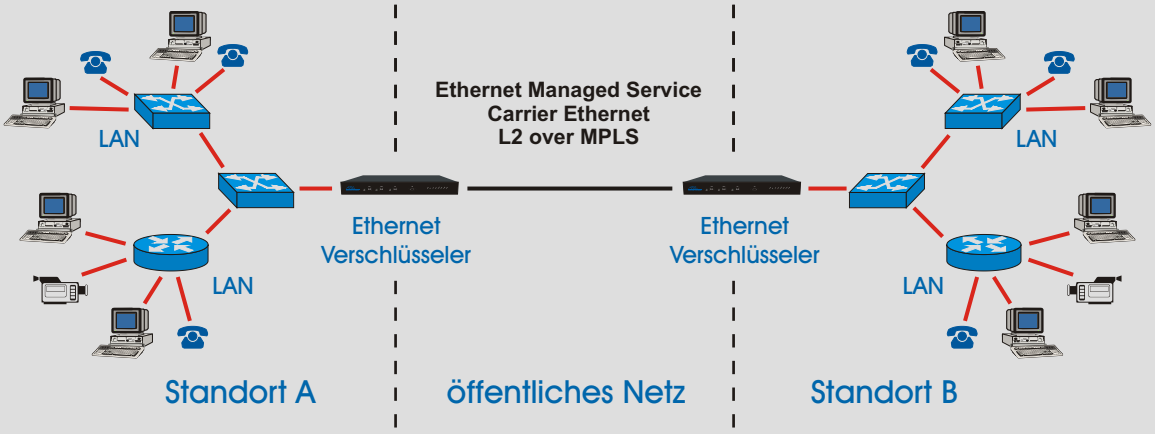
Bei der Vernetzung von Standorten im stadtnahen Bereich (MAN) und im WAN verdrängt **Ethernet** immer mehr die traditionellen Punkt-zu-Punkt Verbindungen.
Durch die direkte Koppelung der Ethernet Strukturen entsteht meist ein über mehrere Standorte verteiltes LAN. Da dieses LAN über öffentliche Leitungswege 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 Encryptor

Highlights des ATMedia Ethernet Verschlüsselers

- Verschlüsselung von 10/100BT Ethernet auf Ebene 2 in Hardware
- Transparent bzgl. VLAN und MPLS
- Full Duplex Verschlüsselung mit Leitungsgeschwindigkeit
- Sehr geringe und konstante Latenz
- Keinerlei Änderung in der Netzwerkinfrastruktur notwendig
- Wartungsfreier Betrieb
- Adhoc Authentisierung

Anwendungsszenario



ATMedia GmbH
Science Park 1
66123 Saarbrücken / GERMANY

Tel: +49 (0) 681 842477
Fax: +49 (0) 681 842481

URL: http://www.atmedia.de
EMail: crypt@atmedia.de

Technische Daten

Leistungseckwerte

- Echtzeit Verschlüsselung der 10/100BT Ethernet Payload (IEEE 802.3)
- Voll-Duplex Durchsatz 10/100 MBit/s unabhängig von der Paketgröße
- Schlüsselwechsel ohne Unterbrechung des Links
- Zusätzliche Latenz kleiner als 37μs je Gerät

Verschlüsselungstechnologie

- AES (256 Bit) Verschlüsselungsverfahren mit CBC Block Modus
- Schlüsselerzeugung durch Hardware Zufallszahlengenerator
- Schlüsselaustausch über Diffie-Hellman ECC Verfahren

Schlüssel Management:

- Geräteauthentisierung über Passphrase/Hostkey
- Adhoc Authentisierung
- Manipulationsgeschützte Schlüsselspeicherung
- Automatischer Wechsel der Verbindungsschlüssel nach konfigurierbarem Zeitintervall
- Autonomer Betrieb ohne externes Schlüsselmanagement

System Management:

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

Hardware:

- Unterstützung von Jumbo Frames
- Transparent bzgl. VLAN, MPLS
- RJ45 10/100BT Kupfer Interfaces
- Tamper Resistentes Gehäusedesign
- 19" 1HE Gehäuse (H: 44mm, B: 430mm, T: 230mm)
- Stromversorgung: 110-240V AC 50-60Hz, ca. 11W

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.

© 2007 ATMedia GmbH. Alle Rechte vorbehalten. Alle erwähnten Markennamen sind eingetragene Warenzeichen ihrer jeweiligen Eigentümer.