

Dans le cadre de l'interconnexion de sites dans les régions urbaines (MAN) et le WAN, Ethernet remplace de plus en plus les connexions traditionnelles point-point. Par le couplage direct des structures Ethernet, un LAN est créé qui, dans la majorité des cas, est reparti sur plusieurs sites. A cause du fait que ce LAN est routé à travers des réseaux publics de télécommunications le danger existe que des données soient lues et manipulées par autrui. De plus, d'autres peuvent accéder à l'infrastructure interne du réseau.

C'est pourquoi il s'impose de protéger le segment du LAN qui est routé à travers des réseaux publics contre de telles attaques. Il est possible de parvenir à un haut degré d'acceptation s'il n'y a pas besoin de modifier ni la structure du réseau ni le flux de travaux.

ATMedia Crypteur Ethernet est le meilleur moyen de réaliser tout cela par une simple insertion dans la structure du réseau Ethernet existante, appelé bump in the wire.

Grâce au **cryptage hardware sur la couche 2**, le système fonctionne de manière transparente à l'égard des protocoles réseau du niveau supérieur sans avoir une influence mesurable sur le LAN.

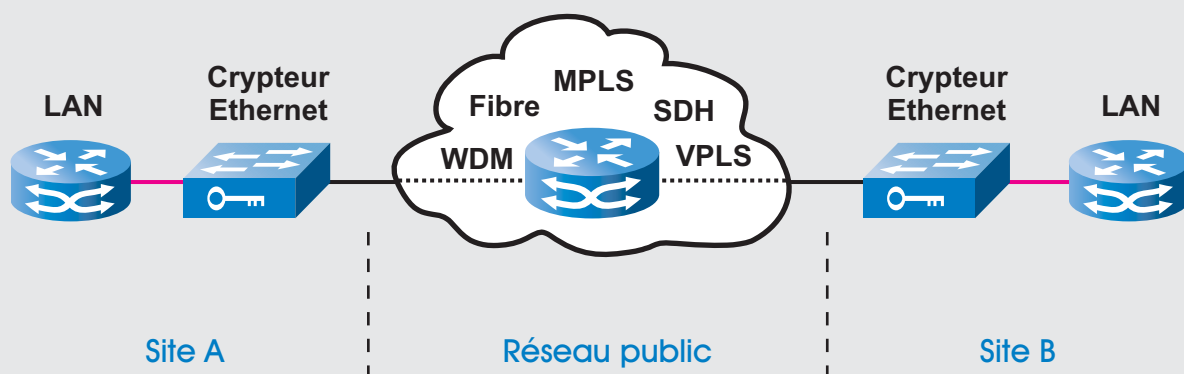
ATMedia Crypteur Ethernet



Avantages principaux du Crypteur Ethernet

- Cryptage full-duplex à la vitesse du câble
- Transparent à l'égard de VLAN, CoS, MPLS
- Cryptage du trafic unicast, multicast et broadcast
- Support de trames jumbo
- Indépendant des équipements terminaux et applications utilisés
- Aucun changement de la structure de réseau nécessaire
- Aucune influence sur les scénarios de redondance existants
- Approuvé pour les informations classifiées

Scénario d'utilisation



Données techniques

Caractéristiques

- Cryptage Ethernet point-point
- Cryptage en temps réel de la charge utile Ethernet (IEEE 802.3)
- Débit: Vitesse de ligne, indépendamment de la taille de trame
- Echange de clé sans interruption de la liaison
- Latence: 100 M ≤ 0,040 ms, 1 G ≤ 0,008 ms, 10 G ≤ 0,004 ms par appareil

Technologie de cryptage

- Procédure de cryptage AES (256 bit) en utilisant le mode CBC Block
- Génération de clé par hardware générateur de nombres aléatoires
- Echange de clé par la méthode Diffie-Hellman ECC (DH-ECKAS)
- Conformité aux spécifications de FIPS 140-2 L3 et CC EAL3

Gestion de clé

- Authentification ad hoc
- Mémorisation de clé protégée contre la manipulation
- Changement automatique des clés de liaison d'après intervalle de temps configurable
- Exploitation autonome sans gestion externe de clé

Gestion du système

- Configuration par une console sérielle (RS 232/V.24) ou accès au réseau par Secure Shell (SSH) (Ethernet hors bande RJ45-10/00BT)
- Supervision intégré de la ligne et de l'opération
- Audit et consignation d'événements
- Interrogation de l'état d'opération via SNMP (V2c/V3 authpriv)
- Supervision de l'état de connexion par ATMedia CryptMon

Réseau

- Compatible avec E-Line, E-Tree, E-Lan, VPLS, VPWS et d'autres services Ethernet
- Support de trames jumbo
- Transparence à l'égard de VLAN (y inclus Q-in-Q), CoS, MPLS, Fiber Channel over Ethernet (FCoE)
- Optical Loss Pass-Through (Link Loss Carry Forward)
- Interfaces de ligne

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

Hardware

- Température d'exploitation: 1° C - 40° C
- Humidité d'air: 10 % - 85 %, non-condensant
- 10M/100M: 482,6 mm (19") 1 U, H: 44 mm, L: 430 mm, P: 230 mm, Poids: 4kg
Alimentation redondante : 110-240 V CA 50-60 Hz, 11 W
- 1G: 482,6 mm (19") 1 U, H: 44 mm, L: 430 mm, P: 320 mm, Poids: 7kg
Alimentation redondante hot swap
110-240 V CA 50-60 Hz ou -48V CC, 90 W
- 10G: 482,6 mm (19") 2 U, H: 88 mm, L: 430 mm, P: 370mm, Poids: 10kg
110-240 V CA 50-60 Hz ou -48V CC, 115 W
- Boîtier: Résistant aux manipulations
- Conformité: CE, FCC

Les systèmes et les documentations afférentes de ATMedia sont toujours maintenus à la pointe de la technologie. ATMedia se réserve donc le droit d'y apporter des modifications à tout moment et sans avis préalable.