



High Speed Encryption Made in Germany

Today's Trends in Network Encryption

Today's Trends in Network Encryption

Contents

- Background ATMedia GmbH
- Why Encryption?
- Which Encryption?
- How to deploy Encryption

ATMedia GmbH

- ATMedia GmbH founded in 1996
- Privately owned and independent German company
- Development, production and distribution of high-speed network security products
- Encryption products up to 10G with a BSI/NATO/EU approvals
- Suisse Partner: DeltaNet AG

Security Risks of WAN-connections

WAN connections are not secure if:

- Value of the data is higher than the costs of getting the data
- Risk of detection is low

A short reminder

Security Risks of WAN-connections

WAN security categories

☺ „real“ WAN network connections

- Dark Fiber
- WDM
- SONET/SDH

☹ „virtual“ WAN networks

- MPLS
- Carrier Ethernet / VPLS
- IP Services

Security of Fiber WAN connections

Low Tech risk analysis

- Physical access to Fibers easy
- Fibre emits light
- Light can be detected

Security of Fiber WAN connections

WDM does not add security

- Coupling out → Spectrum analysis → Filter → Detector
 - Looks like a WDM system (analysis not really needed)
- Analysis of data content
 - Detection of speed and type
- Capturing of „needed“ data
 - Hardware „FPGA“ Filter → disk storage
- Costs ~ 5 digits
- Patents e.g. from DTAG: EP 0915356A1

Security of real Fiber WAN connections

Counteractions

- Fiber monitoring
 - Good for debugging but no reliable detection of attacks
 - “False positive” rate extremely high
- Fiber protection
 - Extremely expensive and not reliable
- Encryption
 - Only reliable measure, no economical worthwhile attacks possible

Security of “virtual” WAN connections

„virtual“ connections

- No physical access needed for eavesdropping
- Data can be rerouted or duplicated by a mouse click
- All members of the group known?
- Is it really “Private”?
- „VPN“ is misleading regarding security risks and resulting liabilities

➔ Encryption is essential

Selection of WAN Security Products

- Firewall, IDS (incl. DPI)
 - Protection against unwanted connections
 - No protection against manipulation and eavesdropping
 - Challenge of „defective“ protocols (VoIP, ...)
 - Additional application gateways needed
 - Works for “known” protocols and applications only

- Encryption (VPN)
 - Cryptographic access control
 - Data protected against manipulation and eavesdropping
 - Offers protection for all protocols and applications

Selection of WAN Security Products

- Firewall, IDS (incl. DPI)



➔ Extensive use of hardware and software

- Encryption (VPN)



➔ Dedicated hardware

Selection of Encryption Equipment

„integrated“ (add-on) Encryption

Firewall, Router, Switch, Director, Multiplexor

- Minor security performance
- High Risk of Denial of Service
- Encryption easily to bypass
- Encryption often at IP level
- Key management?

➔ Combination of many different security functions in one device not optimal

Encryption Checklist

- Encryption „main function” of the device (no giveaway)
- One security level for the whole system
- No „security by obscurity“ arguments
- Use of open and well known algorithms (AES, ECC, ...)
- Perfect Forward Secrecy (long term security)
- Real security reviews by 3rd parties

- Transparency of the whole chain from manufacturer to the integrator

Layer 2 or Layer 3 ?

Layer 3 Encryption = IPSec

- IP
- Universal, high complexity => high overhead
- Low speed IP networks (DSL, UMTS, LTE)
- Most implementations software only
- Impact on QoS, challenge of stream prioritization
- Multicast support difficult
- IP V6, MPLS, VLAN Separation ?

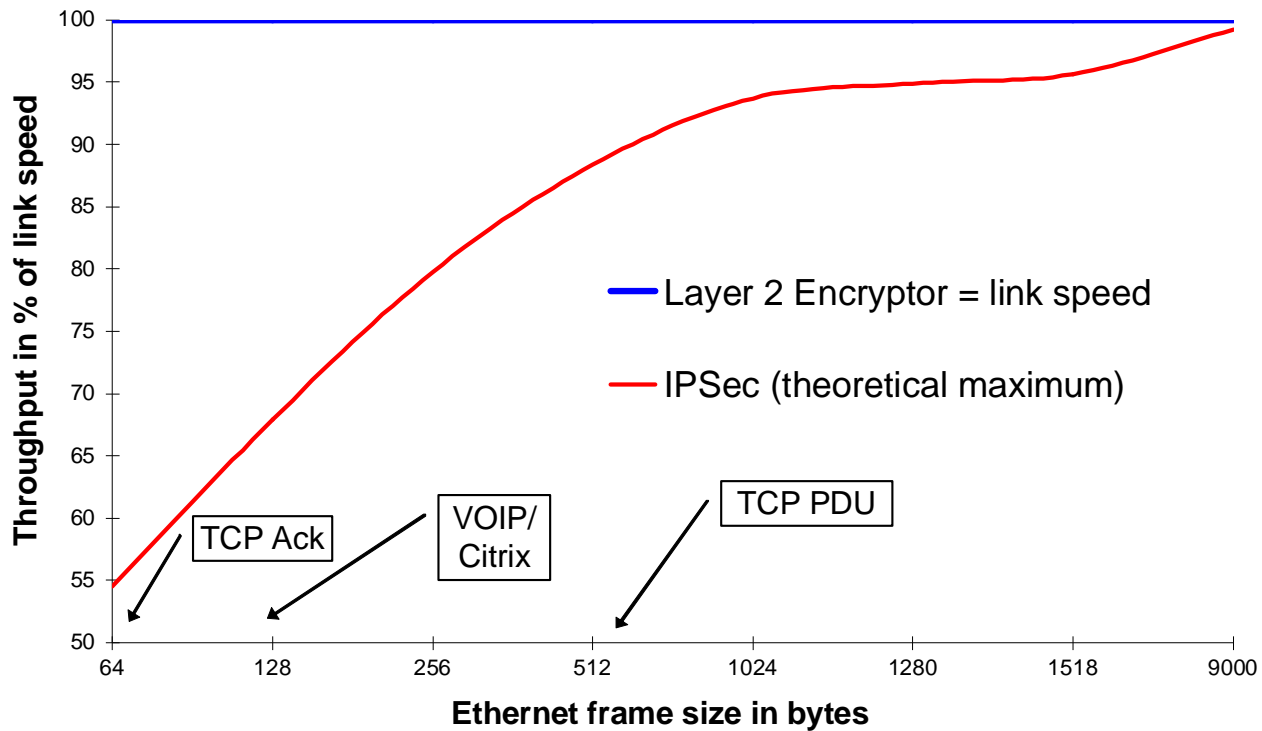
Layer 2 or Layer 3 ?

Layer 2 Encryption

- Network layer below IP and MPLS
- Less complexity => low overhead
- Hardware implementation: minimal Delay and Jitter
- Optimal for real-time communication (VoIP, Video, Terminal-Services)
- QoS and prioritization conserved
- Transparent to IP V4+V6, MPLS, VLAN, ...

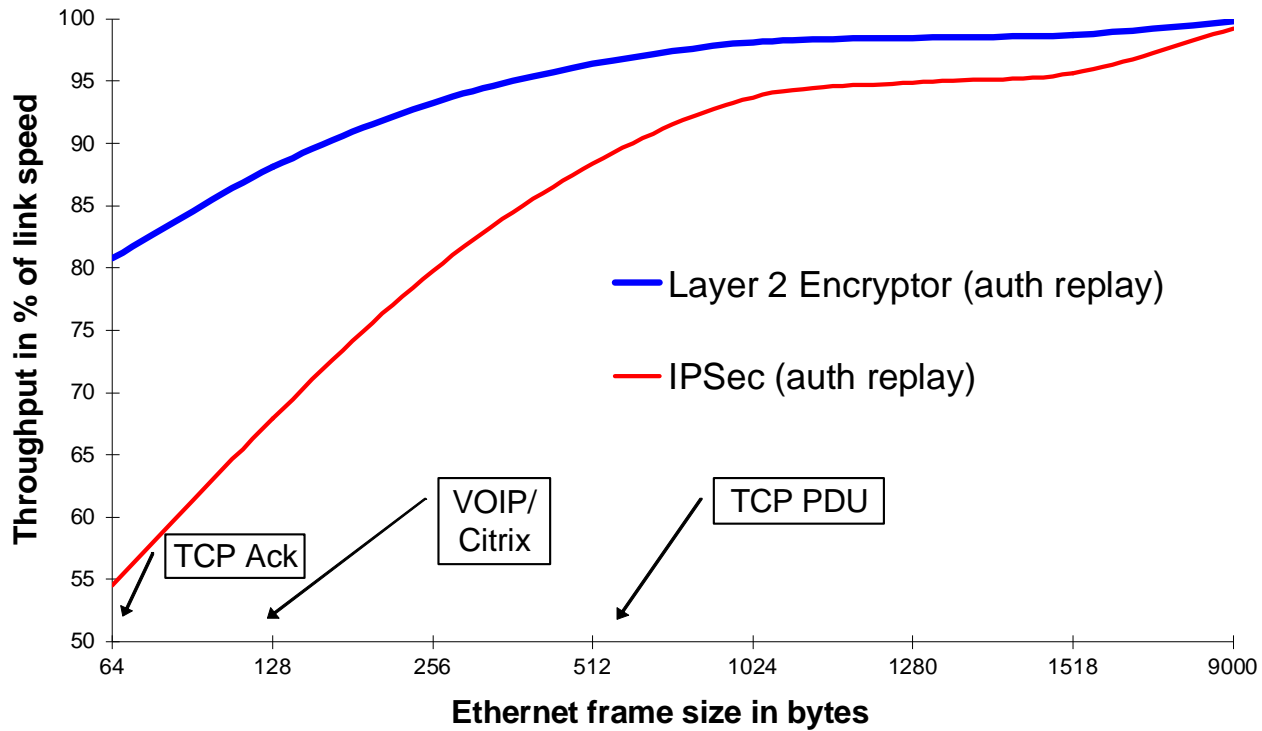
Layer 2 or Layer 3

Marketing:



Layer 2 or Layer 3

Fair comparison:

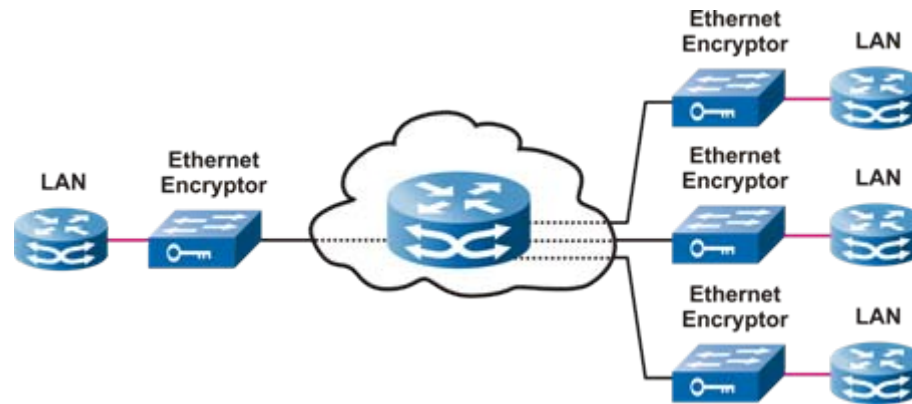


Real Layer 2 VPN: Carrier Ethernet

- Point-to-Point: E-Line

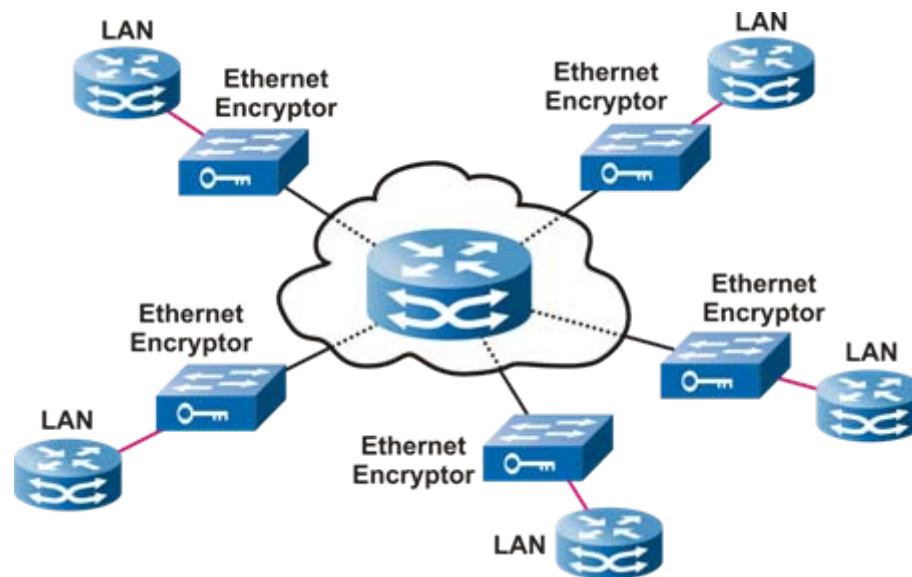


- Point-to-Multipoint: E-Tree



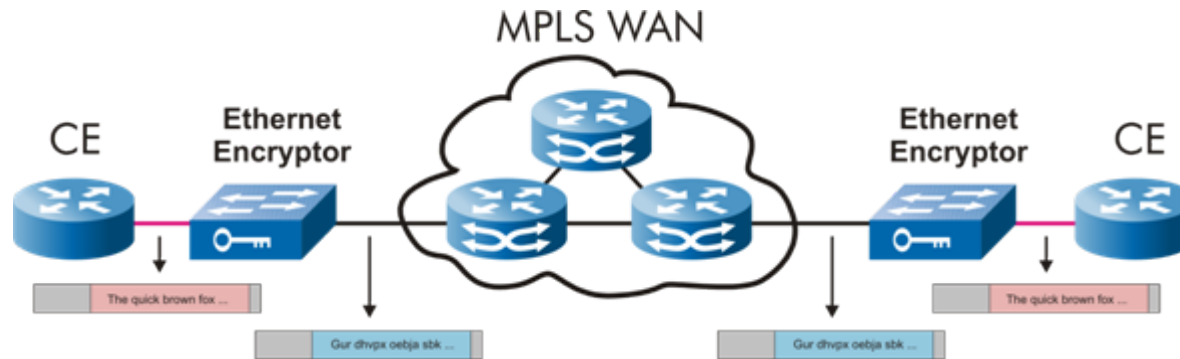
Real Layer 2 VPN: Carrier Ethernet

- Full Multipoint: E-LAN



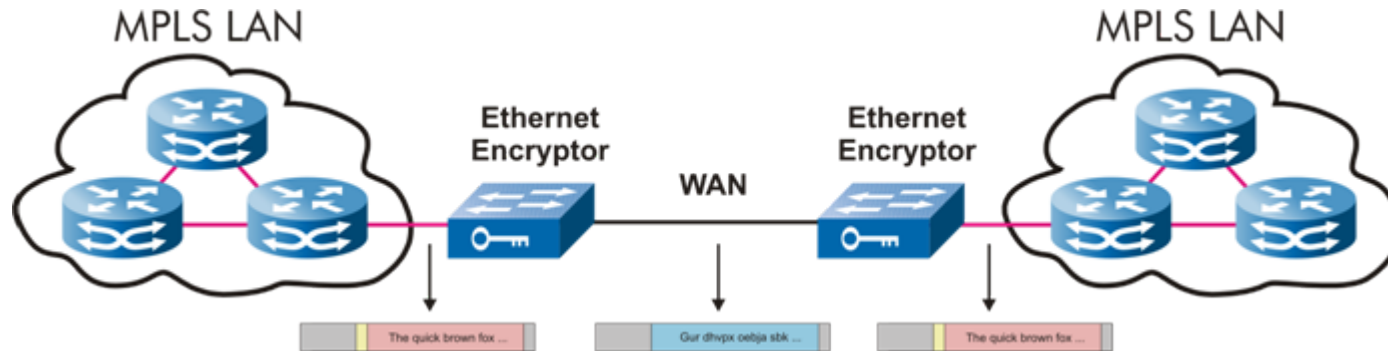
- Offered as “crypto service” by some carriers
(Inside-IT Ethernet Encryption market overview 2010)

Real MPLS VPN: MPLS Layer 2 WAN



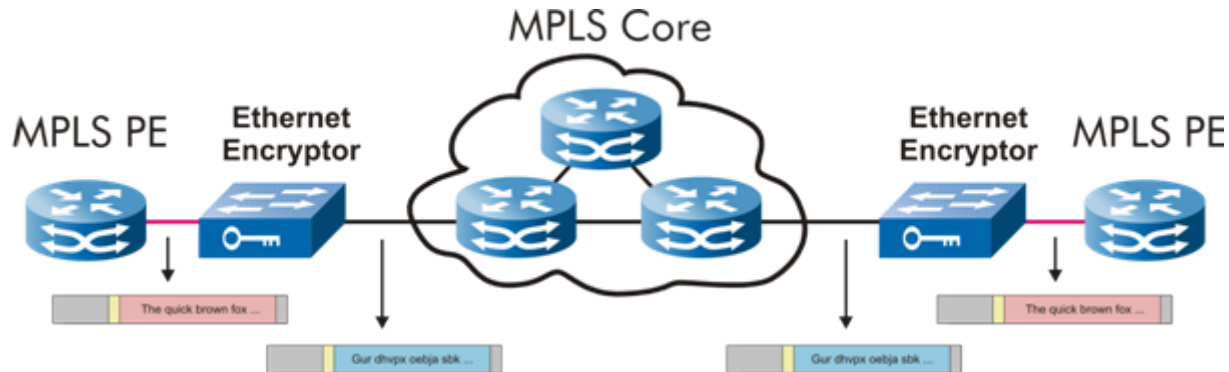
- MPLS used as Layer 2 transport
- VPLS or Pseudo-Wires
- Works for Point-to-Point and Multipoint networks

Real MPLS VPN: MPLS over Layer 2



- Local MPLS networks connected via Layer 2 WAN connections
- Point-to-Point Encryption of the WAN connection
- Special case: “private” MPLS where all P and PE Routers are interconnected by encrypted Layer 2 connections

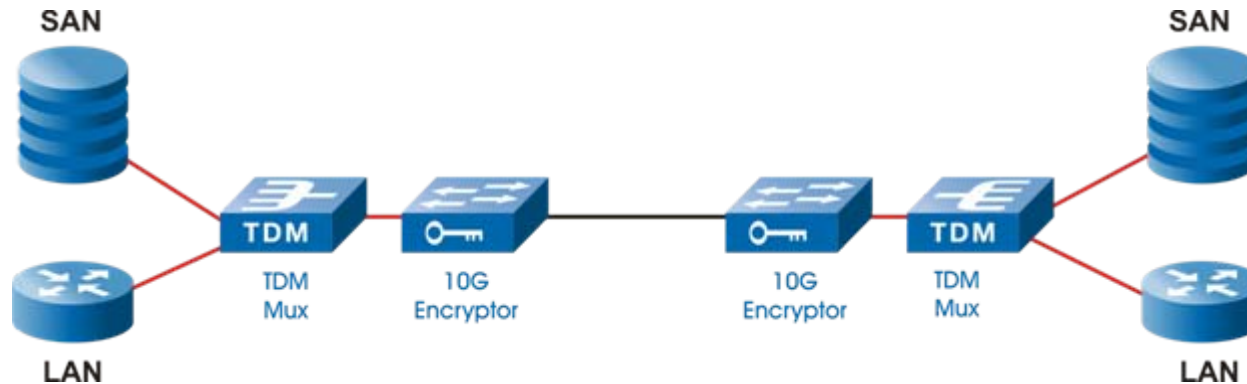
Real MPLS VPN: Full MPLS Encryption



- MPLS services of WAN and LAN connected
- PE serves as “service multiplexor” \Leftrightarrow ATM
- All MPLS data is encrypted
- Works for Point-to-Point and Multipoint scenarios

Important Layer 2 Scenario: Storage

SAN Security often “forgotten”:



- Aggregation of Storage and Data services (1G-4G)
 - TDM System multiplexes services into a 10G SDH link
 - Encryption of the SDH link with a **10G SONET/SDH Encryptor**
- **Certified Secure Data Centre Interconnection**

ATMedia Solutions



10M Ethernet
100M Ethernet



1G Ethernet
155M-2.4G SDH



10G Ethernet
10G SONET/SDH

- 19" chassis
- Redundant power supplies with dual inputs
- Approved by the BSI for VS-NfD, EU and NATO
- OEM versions certified for FIPS 140-2 L3 and CC EAL3

Summary

- Any network communication can be intercepted and manipulated
- Risk depends on the value of content and availability of the data
- Reliable Encryption is the only effective countermeasure
- Encryption solutions for most network scenarios available

Contact

ATMedia GmbH

Science Park 1
66123 Saarbruecken
Germany

phone: +49 681 842477

fax: +49 681 842481

crypt@atmedia.de

www.atmedia.de

DeltaNet AG

Riedstrasse 8
8953 Dietikon
Suisse

phone: +41 43 322 40 50

fax: +41 43 322 40 51

info@deltanet.ch

www.deltanet.ch