ADVA™
Optical Networking

Lässt sich Glasfaser abhören?

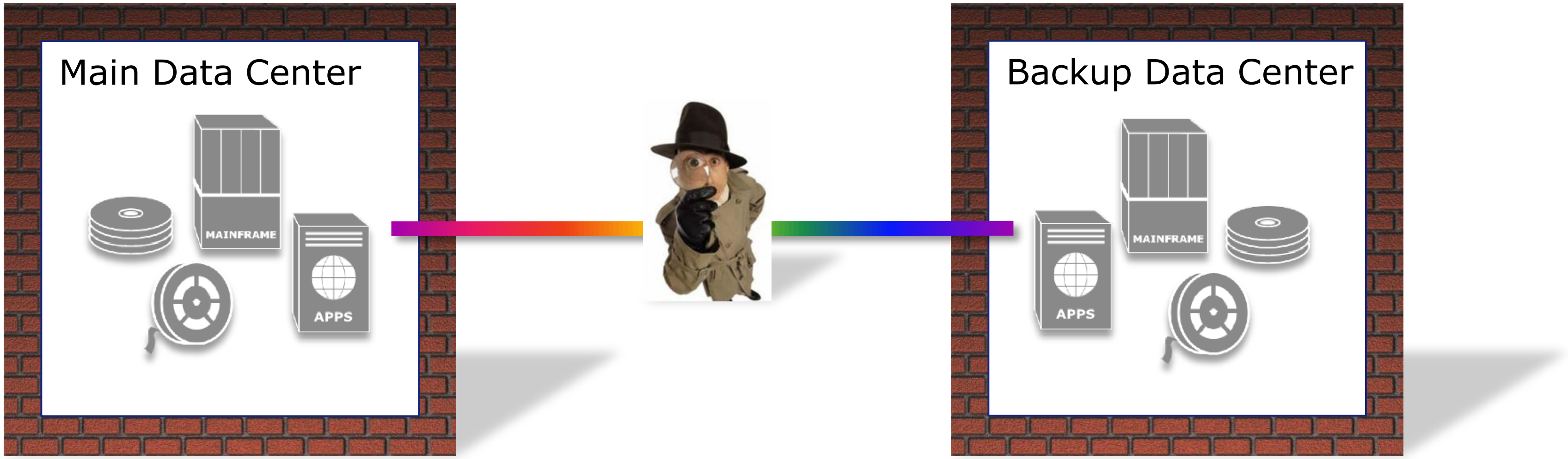
Wie sicher ist die Datenübertragung über Glasfaser und wie kann man sich durch Verschlüsselung schützen?

Christian Illmer

September 2013

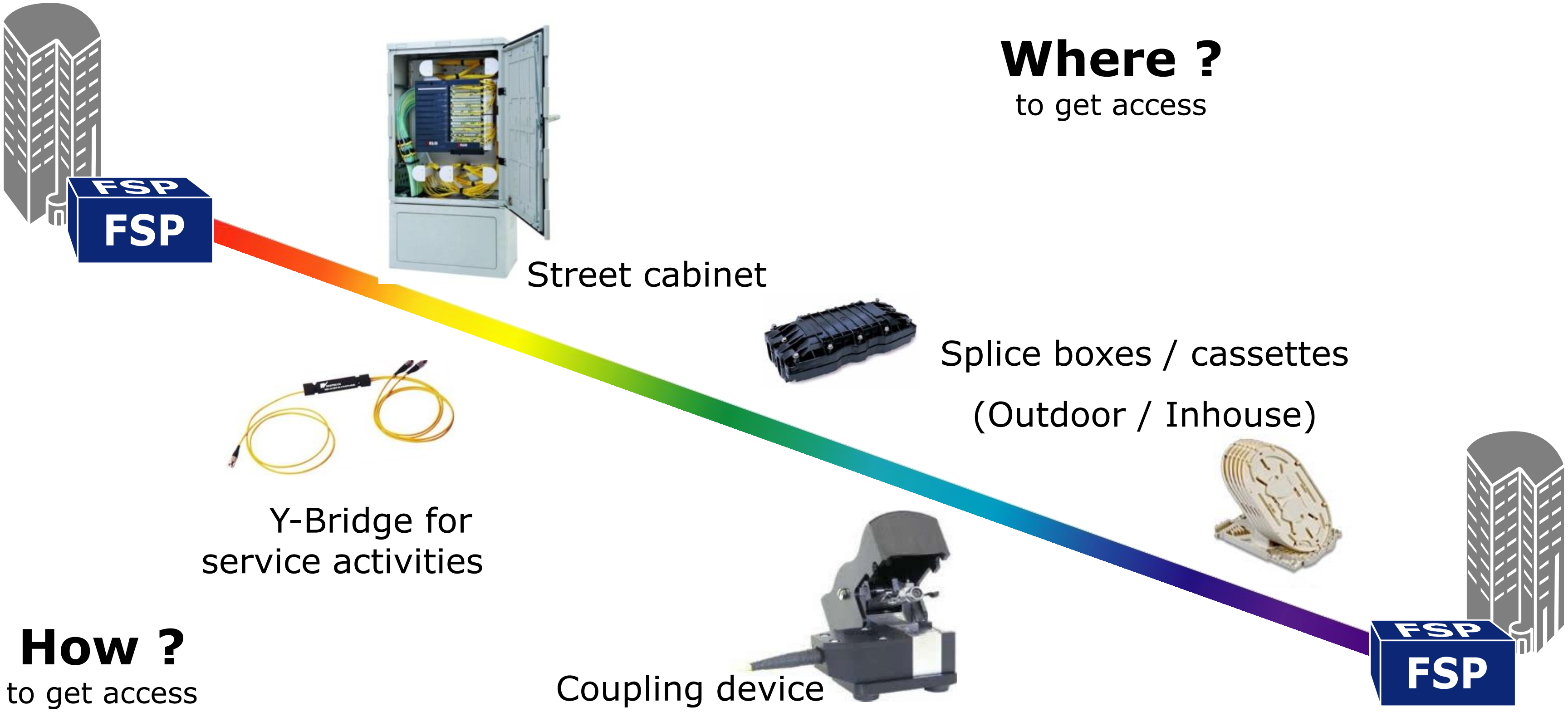
Why security matters

Data Center Security Today



Need to protect information flow between data centers

Fibre optics networks
tapping possibilities



Where ?
to get access

Street cabinet

Splice boxes / cassettes

(Outdoor / Inhouse)

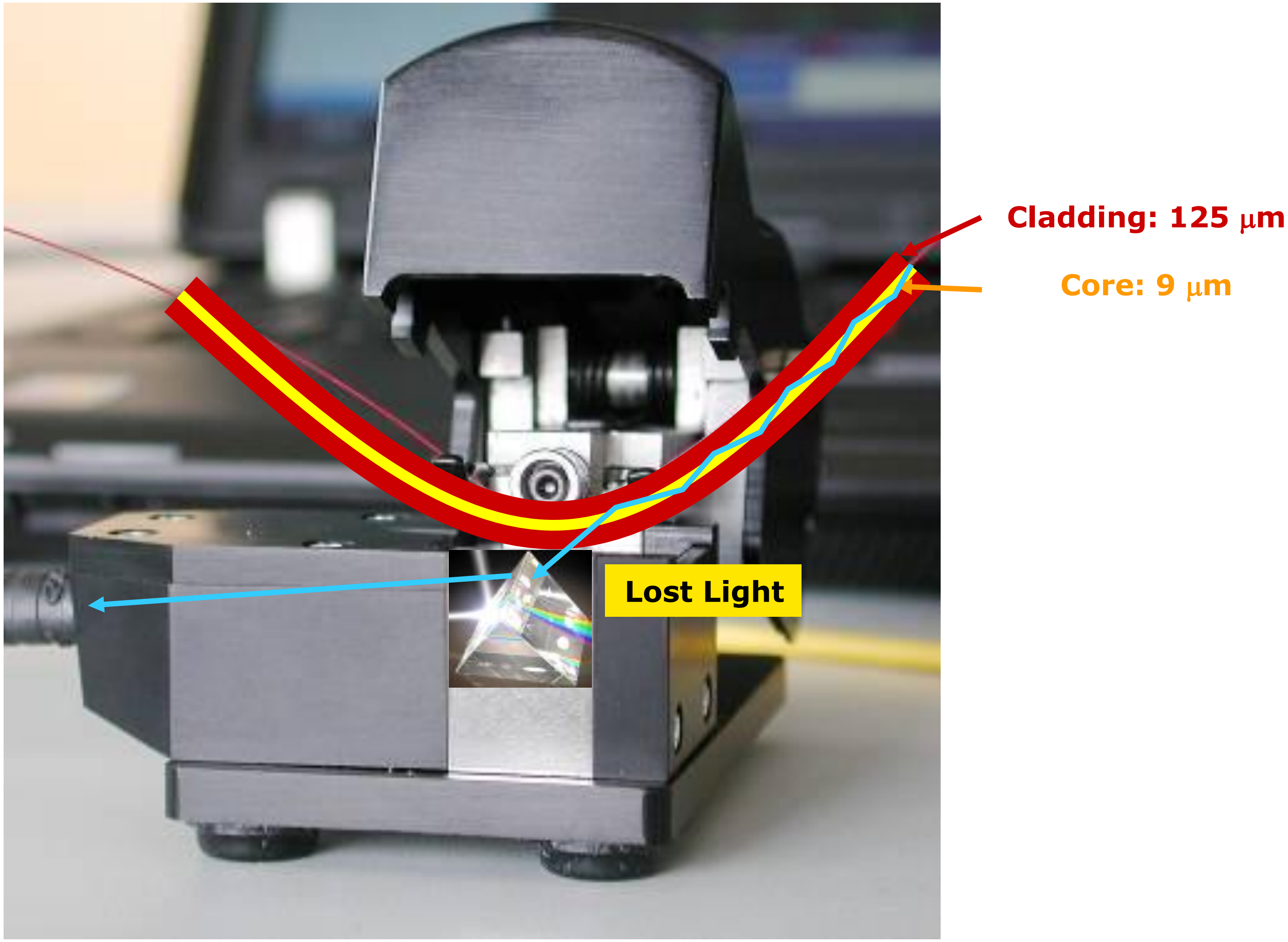
Y-Bridge for
service activities

Coupling device

How ?
to get access

There are multiple ways to access fiber

Fibre optic networks
„optical tapping“ methods



Fibre optic networks
Analyzing the data

- Data analysers and test tools are commonly used by equipment manufacturers to test their product quality

- Optical power meters and spectrum analysers can help to select the right WDM wavelengths

- Data and protocol analysers allow an in-depth reading of all communication protocols used today: Ethernet, SONET/SDH,FC
- Designed for common use by the Telco industry these devices are freely available
- All data traffic can easily be monitored, recorded and replayed!

Commercial splitter, coupler, splicing- and analysis tools are freely available at relatively low cost

How to protect your data in transit

FSP 3000 Security Suite

Physical layer monitoring

Power tracking

Intrusion detection

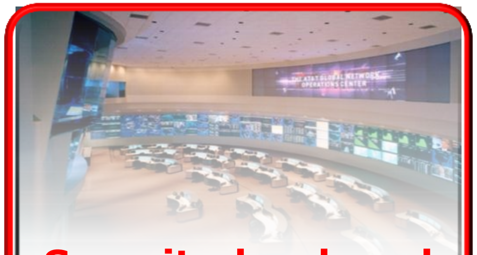
OTDR

Encryption

AES-256

Authentication

Diffie-Hellman



Security-hardened software

RADIUS

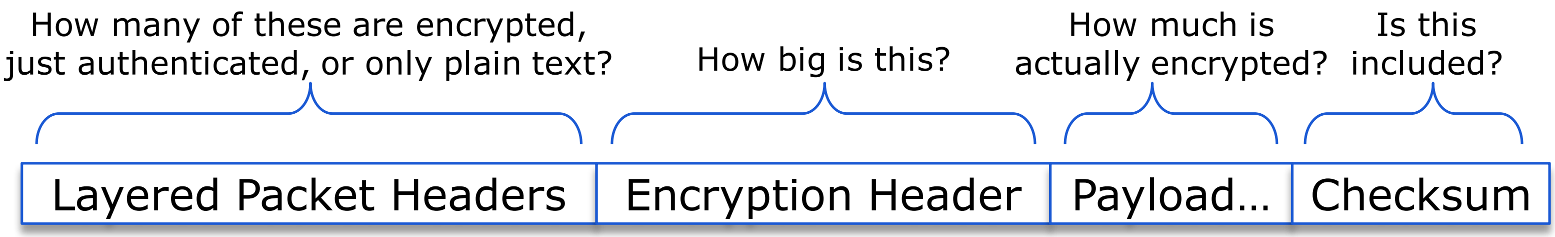
Secure Shell

SNMPv3

A complete and integrated solution leveraging advanced technology

Encryption in transport systems

Encryption Method vs Layer



How many of these are encrypted, just authenticated, or only plain text?

How big is this?

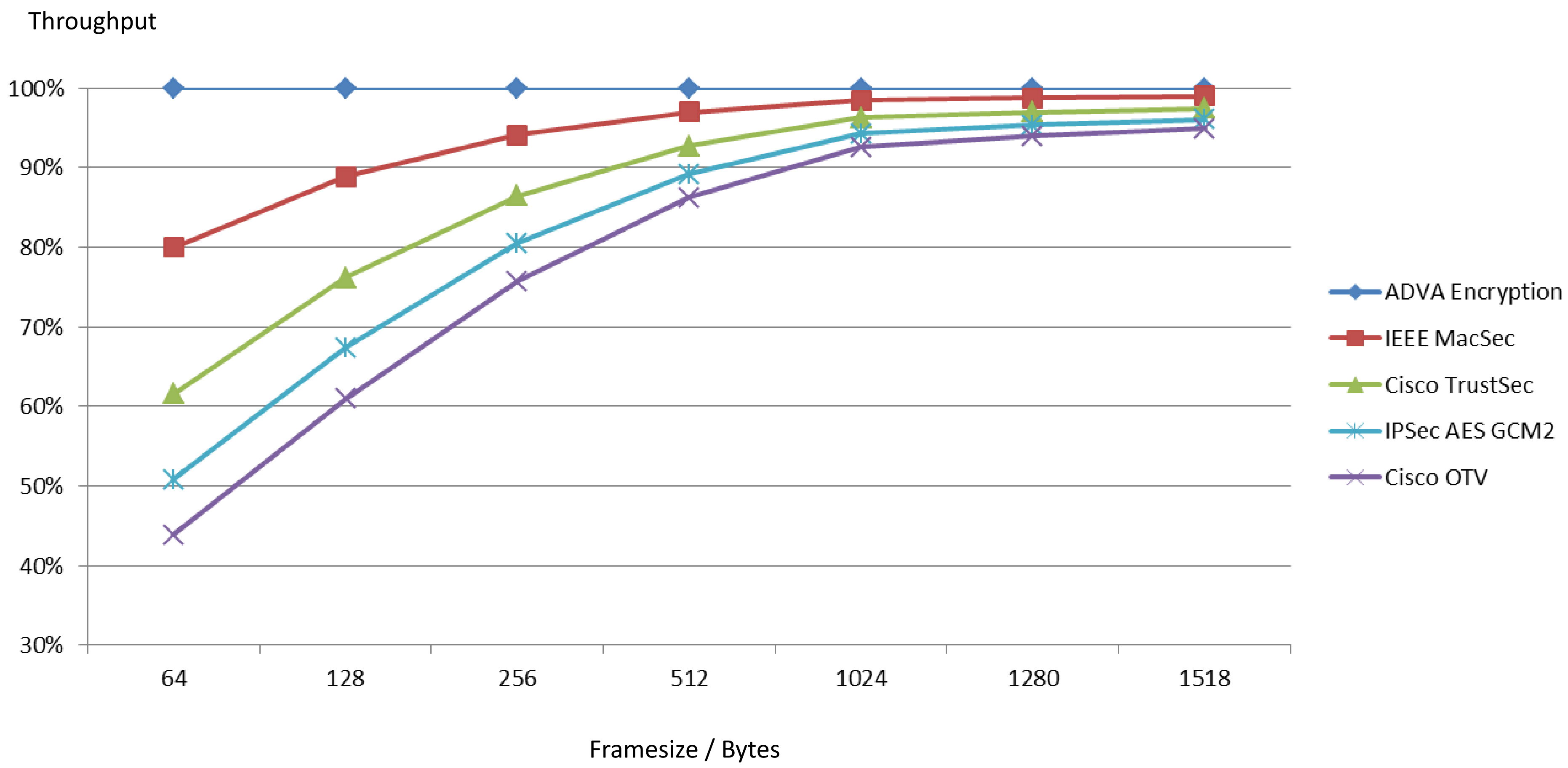
How much is actually encrypted?

Is this included?

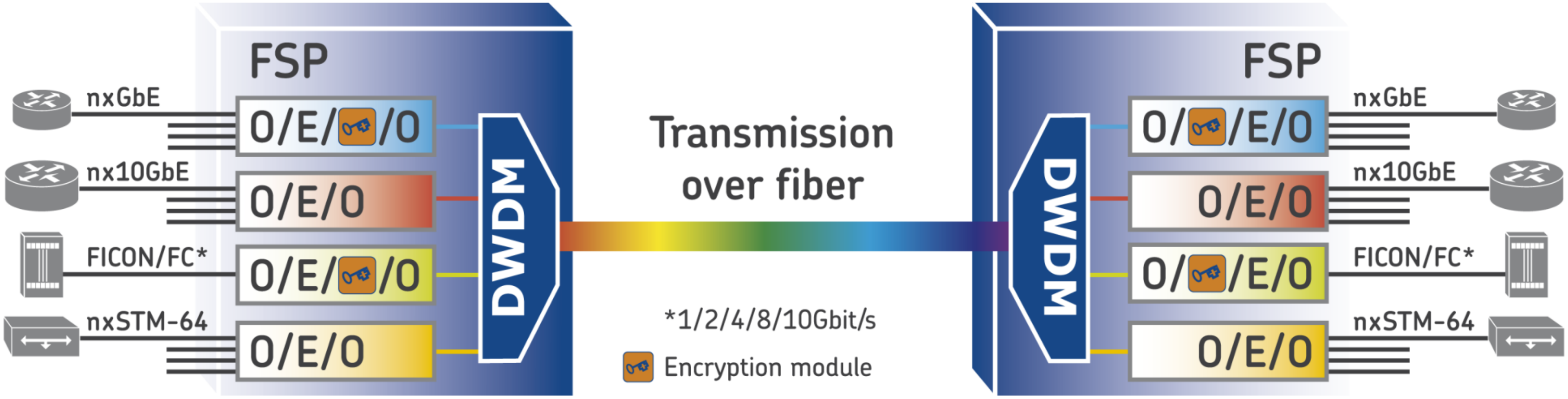
Layered Packet Headers | Encryption Header | Payload… | Checksum

- Overlay Transport Virtualization (OTV)
  - Traditionally used for VPN services
  - 82 Bytes overhead
  - Only select Bytes in header encrypted and authenticated.
- MACsec/TrustSec
  - Point-to-Point Ethernet encryption
  - 32/40 Bytes overhead, respectively
  - Only select Bytes in header encrypted and authenticated.
- Traditional Transport
  - Point-to-point and multipoint
  - Zero bytes overhead, so no loss of throughput with shorter packets.
  - Only select Bytes in header encrypted and authenticated.
- Bulk Transport Encryption
  - Point-to-point
  - Zero bytes overhead, so no loss of throughput with shorter packets.
  - Protocol/ I/F agnostic (Ethernet, FC, IB, Sonet/SDH)
  - All Bytes in header and checksum are encrypted with payload.

Maximum Throughput a Comparison



WDM transmission with encryption

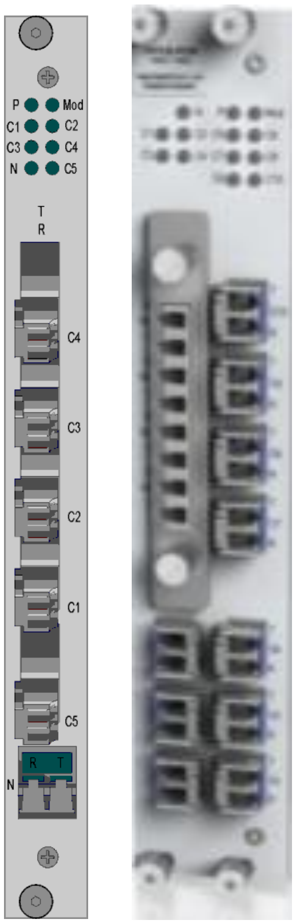


*1/2/4/8/10Gbit/s

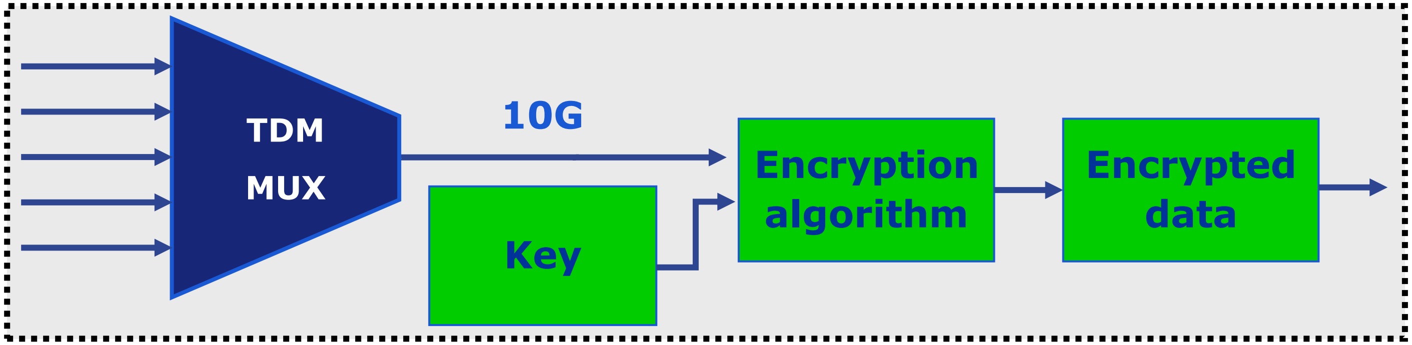
🔑 Encryption module

Modular approach, can be added per channel on an as-needed basis

FSP 3000 encryption overview
5TCE and 10TCE with encryption



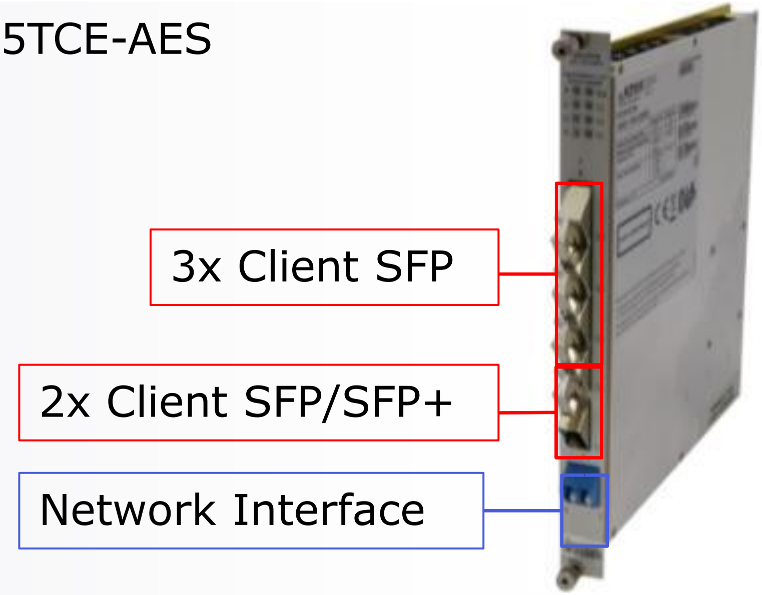
Data encryption on 5TCE and 10TCE muxponder card

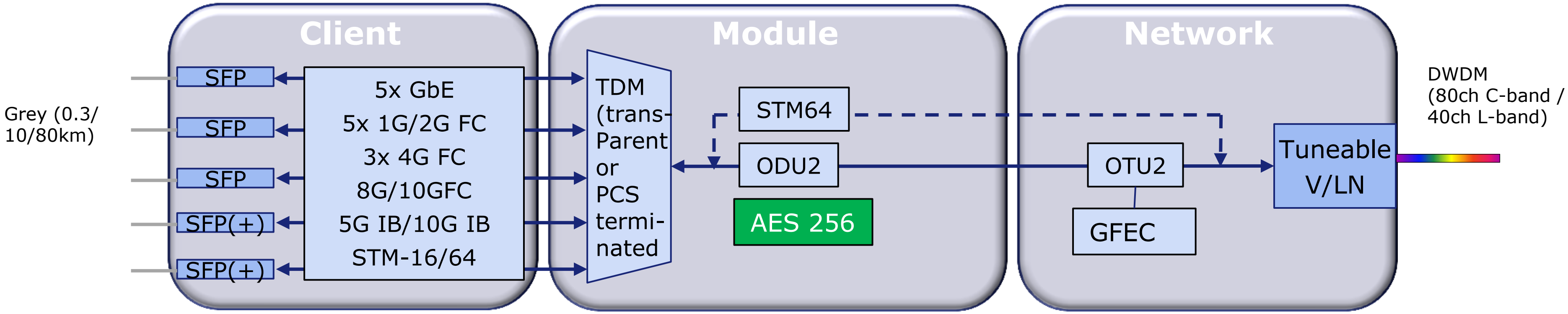


- Encryption applied to the multiplexed data (support of **all** data center protocols)
- AES-256 encryption on the lowest possible layer (latency 100ns)
- Automatic key exchange every 10 mins (5TCE) every 1 min (10TCE) using Diffie-Hellman Algorithm
- Using existing FPGA core PLUS add. encryption specific HW
- Fully tested and qualified with all DC vendors (JNP, BRCD, IBM, EMC…)

Encryption
10G Muxponder with Encryption

- Universal 10G Enterprise Muxponder: 5TCE-AES
- AES256 encryption
- Dynamic key exchange every 10 mins
- 5 x Any Multi-service
- GbE/10GE/FC1/2/4/8/10/Infiniband
- STM-64 network variant

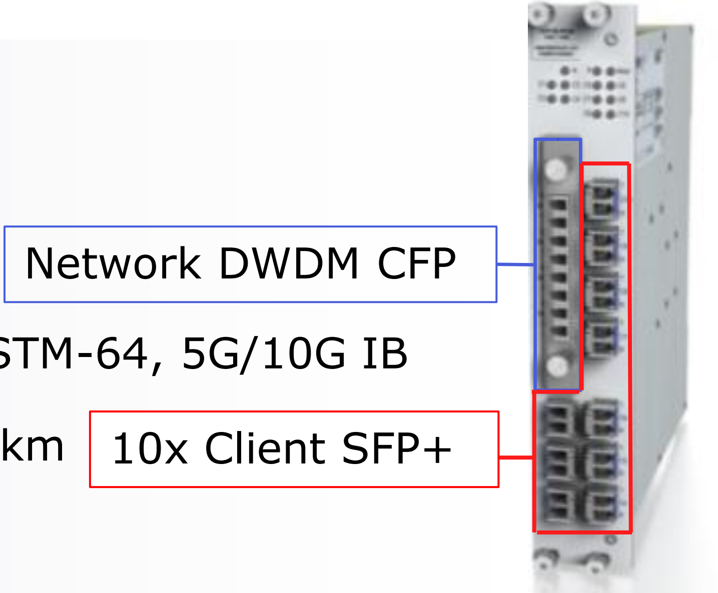


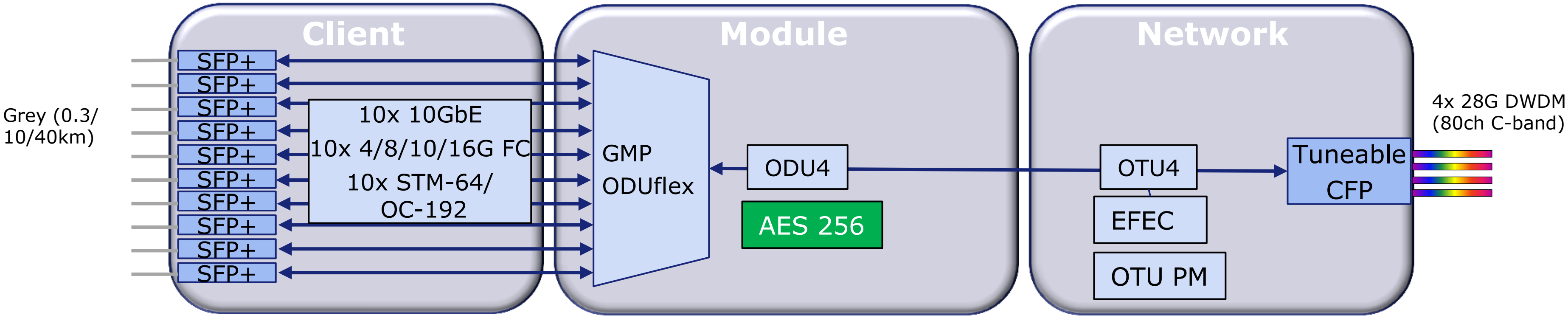


Next Gen 100G Metro

Metro 100G with encryption

- Universal 100G Metro Muxponder
- AES256 encryption with 2048bit key
- Dynamic key exchange every 1 min
- 10GE/40GE/100GE, 4G/8G/10G/16G FC, STM-64, 5G/10G IB
- Cost breaking 100G solution for up to 500km
- Available Q1 of 2014 (R12.3)





Implementation on 5TCE

5TCE-AES Key Definitions

- **Authentication Key**
  - Initial key that must be provided to both systems in order to authenticate them as entitled party for this communication
  - Will be used to encrypt a random number that is required to calculated the final key
  - Will be stored in the non-volatile memory
  - If lost or otherwise destroyed no new key can be generated

- **Private Key**
  - Will be generated by each party and not shared with other side
  - New private key will be generated for each key exchange (no storing)
  - Is required to calculate the shared secret

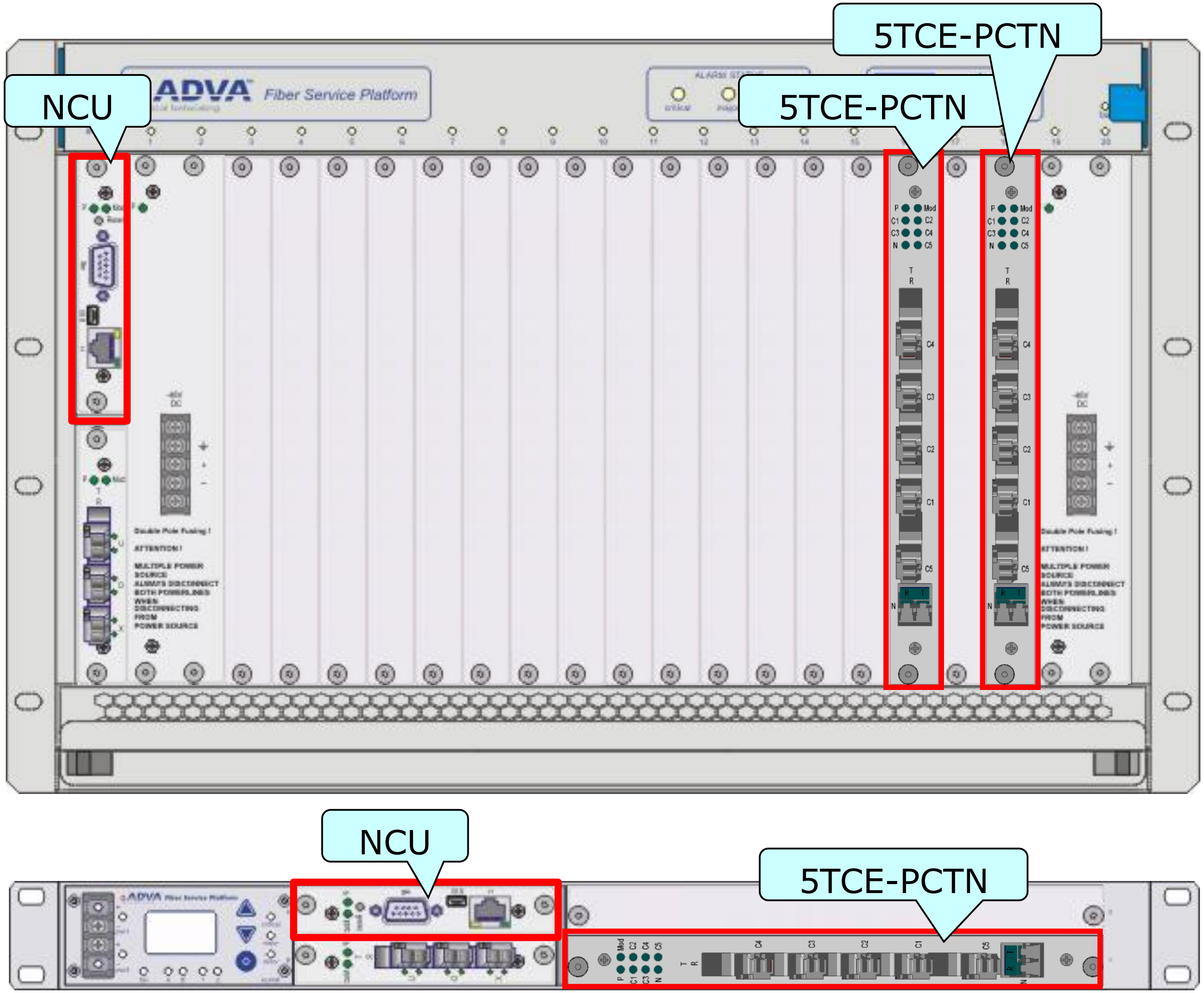
- **Public Key**
  - Will be generated out of the private key and sent over to other side
  - New public key will be calculated for each key exchange (no storing)

- **Shared secret**
  - Will be calculated using public and private key as shared secret between both parties
  - Will be used to generate the final session key

- **Session key**
  - Will be derived from shared secret
  - Is used to encrypt the data
  - Has limited (programmable) lifetime of up to 42 days

WDM Encryption

Required components



Standard Encryption
Step-by-step process

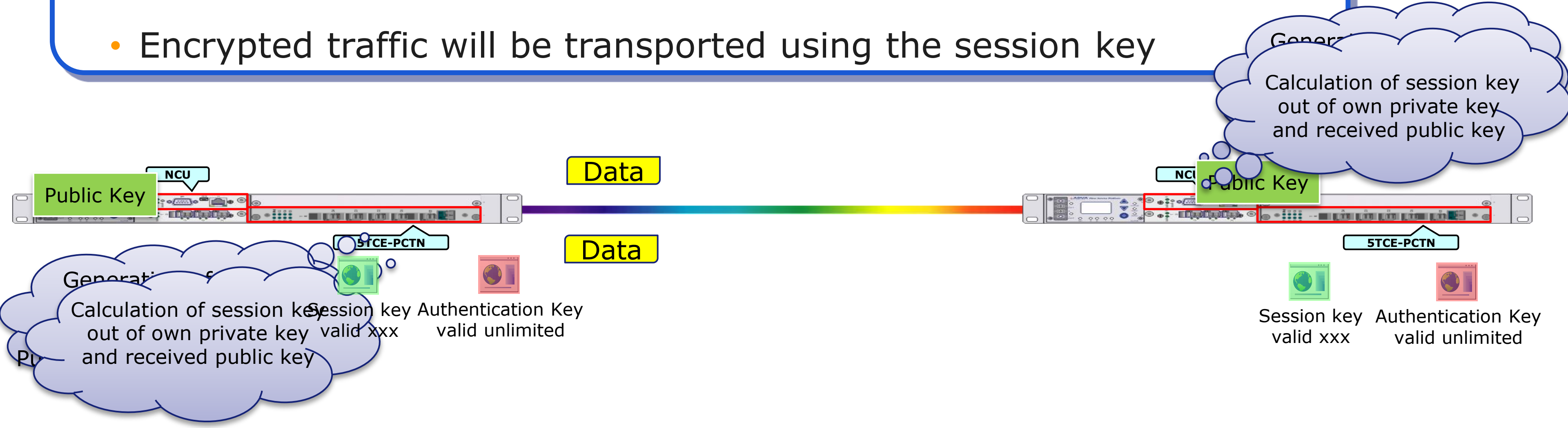
Steps to setup encryption:

- User has to provide Authentication key

- Cards will use Authentication Key for Diffie Hellman process
- Private and public key will be generated (acc. to DH)
- Public key is sent to other side encrypted with Auth. key

- Session Key will be generated out of own private and received public key (acc. to DH)

- Encrypted traffic will be transported using the session key


Calculation of session key out of own private key and received public key
Public Key
NCU
Data
Data
NCU
Public Key
5TCE-PCTN
5TCE-PCTN
Calculation of session key out of own private key and received public key
Session key valid xxx
Authentication Key valid unlimited
Session key valid xxx
Authentication Key valid unlimited

FSP 3000 Security Suite

… for Enterprise customers

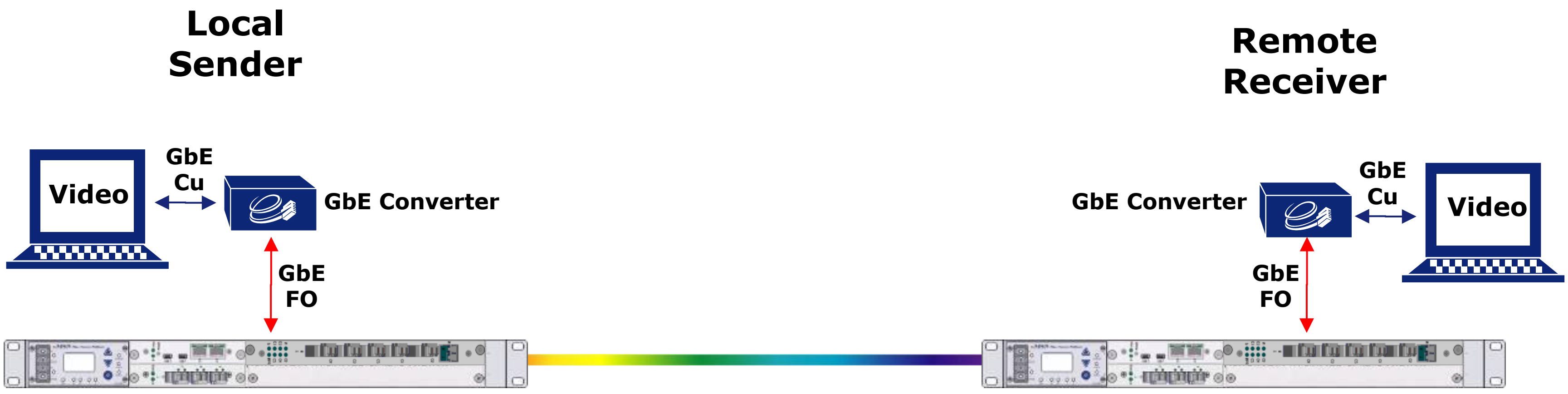
- Helps to effectively protect critical information
- Superior low-latency performance
- Enables compliance with laws and regulations

… for Carriers and Service Providers

- Attract new customers in key verticals
- Differentiate service offering and increase margins
- Enable new encryption service offering through separate transmission and encryption management

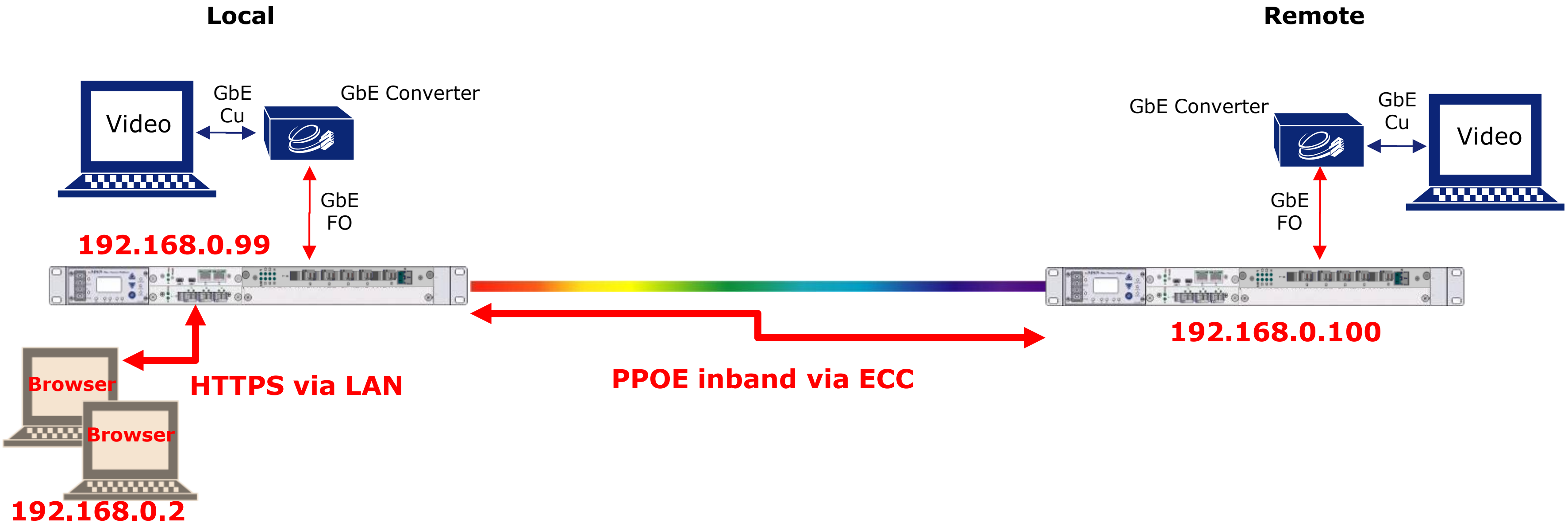
Live Demo

Starting Test Setup



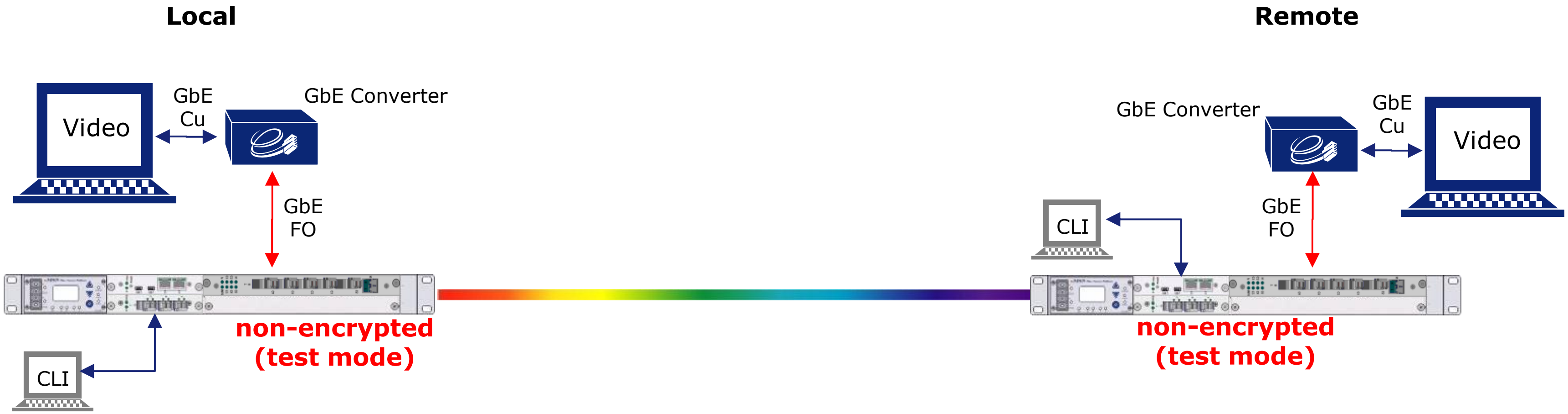
- Notebook streaming Video via GbE port to other side
- GbE converter to convert from copper to fiber
- 5TCE with GbE I/F transports signal to other side
- Receiving end converts back from fiber to copper and feeds into notebook
- Video stream using UDP

Starting Test Setup
Management



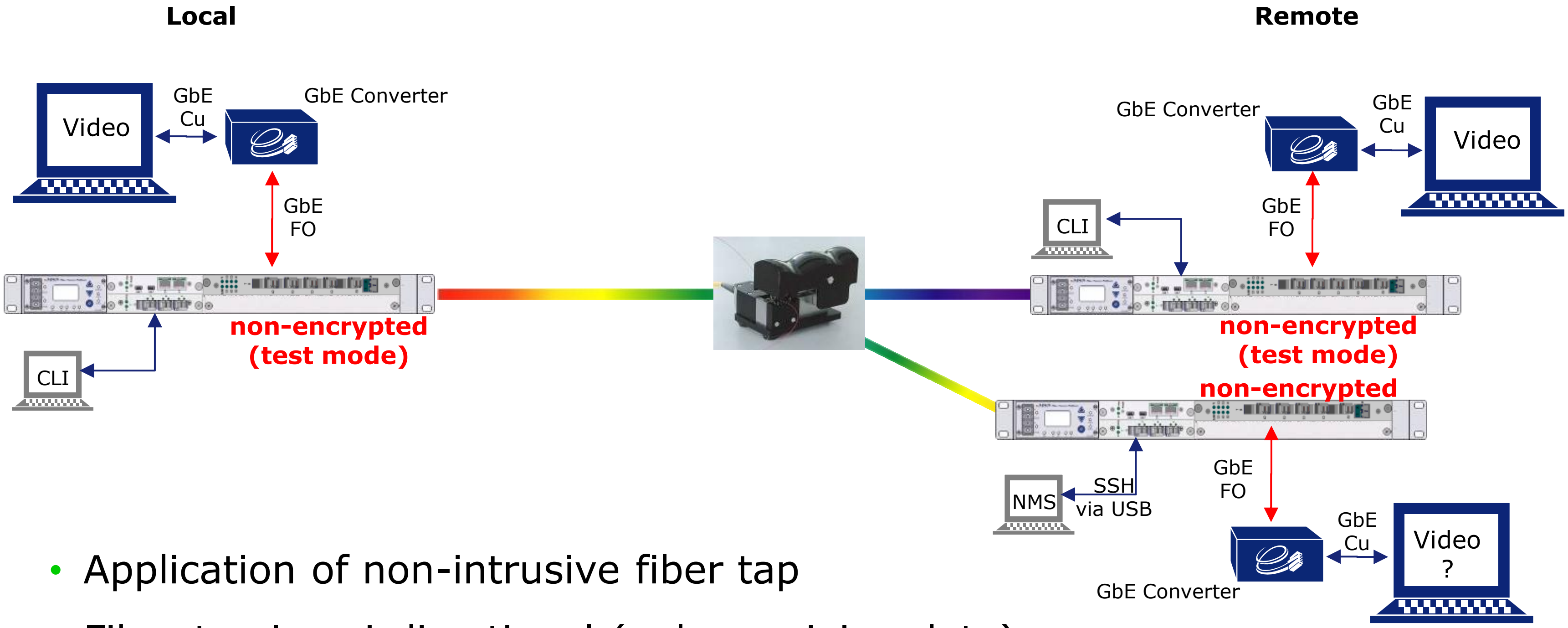
- Management via browser and HTTPS
- LAN/Ethernet cable to connect to local network element
- Inband communication used to access remote network element
- ECC using overhead (not part of the 5TCE encryption but SSH encrypted)
- User can be off-site (but must use HTTPS)

Starting Test Setup
turn on test mode



- Connect to 5TCE via local craft interface
- Login to CRYPTO MENU
- 1st login -> change password
  - Enable test mode
- Repeat activity on remote end
- After correct setup data should be transported and video should be displayed

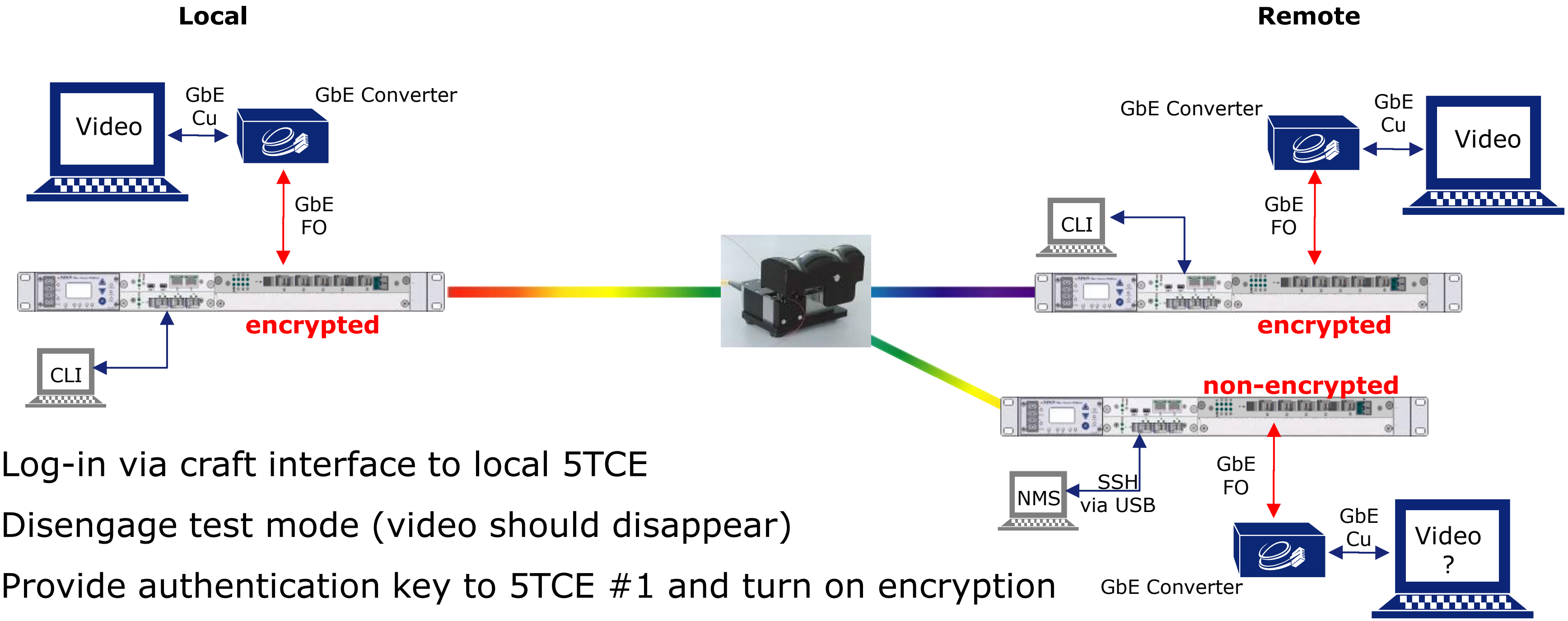
Link with fiber tap



- Application of non-intrusive fiber tap
- Fiber tap is uni-directional (only receiving data)
- Tapped signal gets feeded into 3rd 5TCE (non encryption) card
- Video can now be seen on 3rd notebook (and still on 2nd notebook)
- Simulation of non-intrusive tap into fiber link

Link with fiber tap

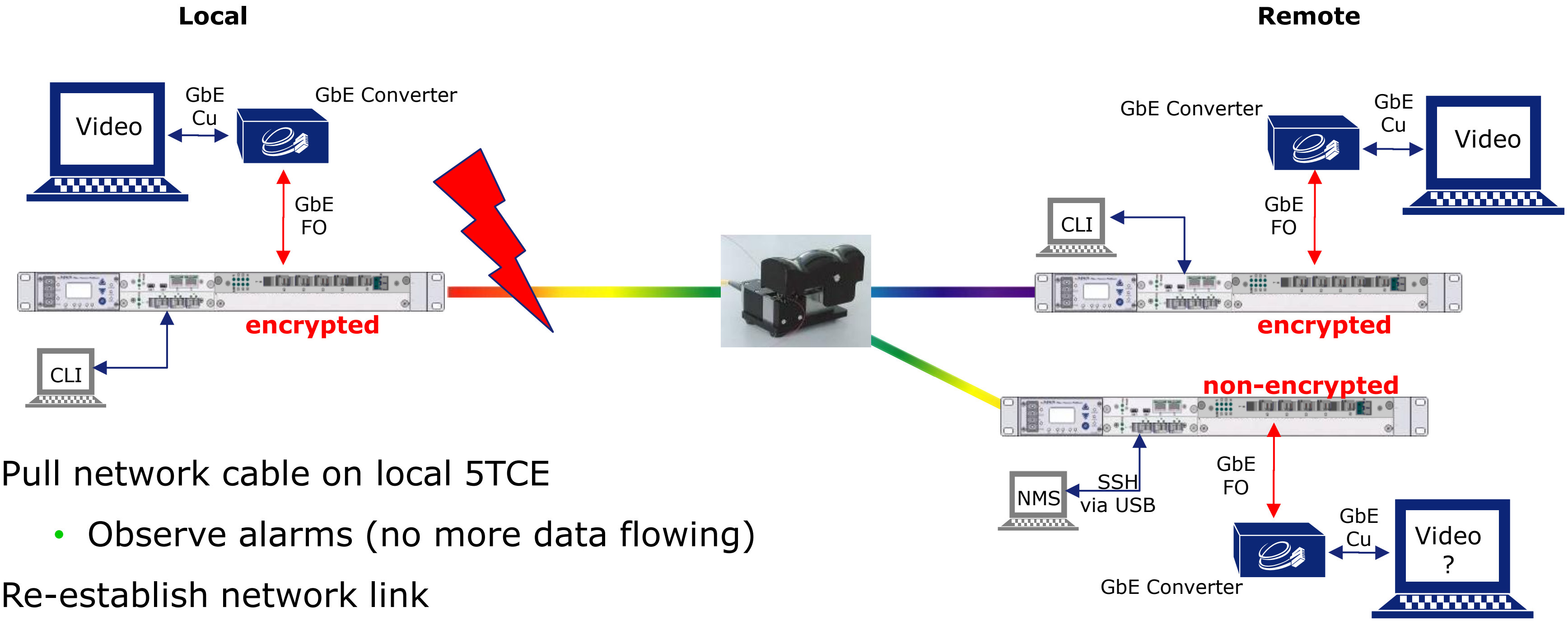
Provisioning of authentication key on 5TCEs



- Log-in via craft interface to local 5TCE
- Disengage test mode (video should disappear)
- Provide authentication key to 5TCE #1 and turn on encryption
- Card now ready to start running encryption (waiting for remote side)
- Repeat activity on remote side
- After authentication key has been provided and encryption turned on cards will generate session key and traffic will be encrypted
  - Video on intruder’s notebook should disappear

Link with fiber tap

Simulation of link failure



- Pull network cable on local 5TCE
  - Observe alarms (no more data flowing)
- Re-establish network link
  - Link should come up again
  - No session key will be generated if life time is still valid (<10 min)
  - Key exchange counter should not have changed

ADVA™
Optical Networking

Thank you

cillmer@advaoptical.com