MRV | EMPOWERING THE OPTICAL EDGE

Encryption in high-speed optical networks

Enabling a Reliably Connected Digital World With Solutions to Make Networks Smarter, Faster and More Efficient

MRV 25 Years EMPOWERING THE OPTICAL EDGE

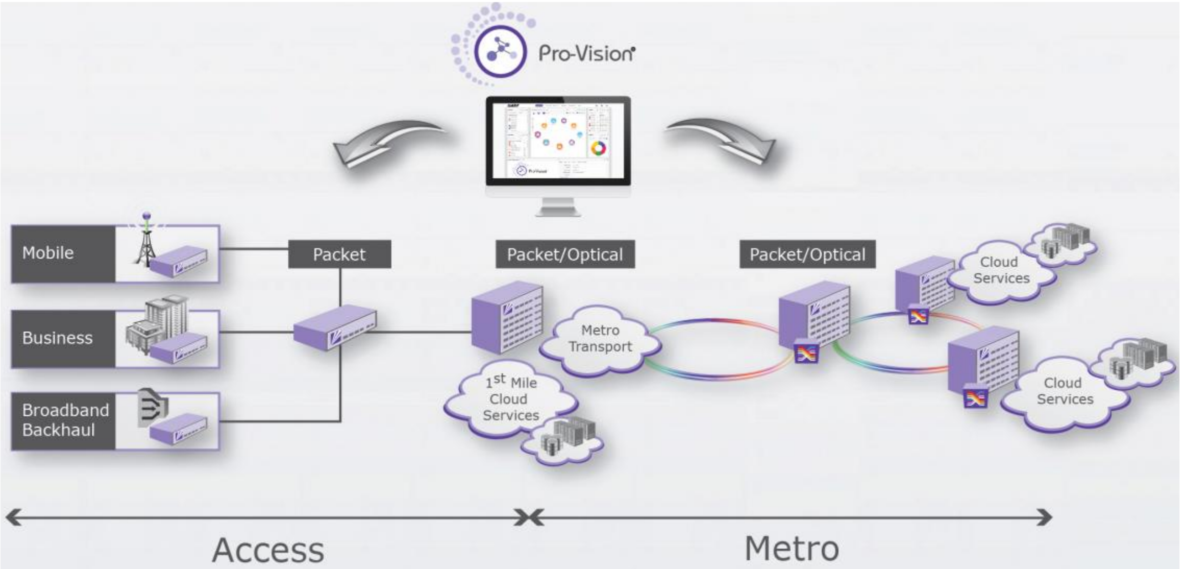
MRV at a Glance

Designing and providing metro packet-optical solutions that power the world’s largest networks

Over $2B

of field-proven

installed base



1000+ GLOBAL CUSTOMERS

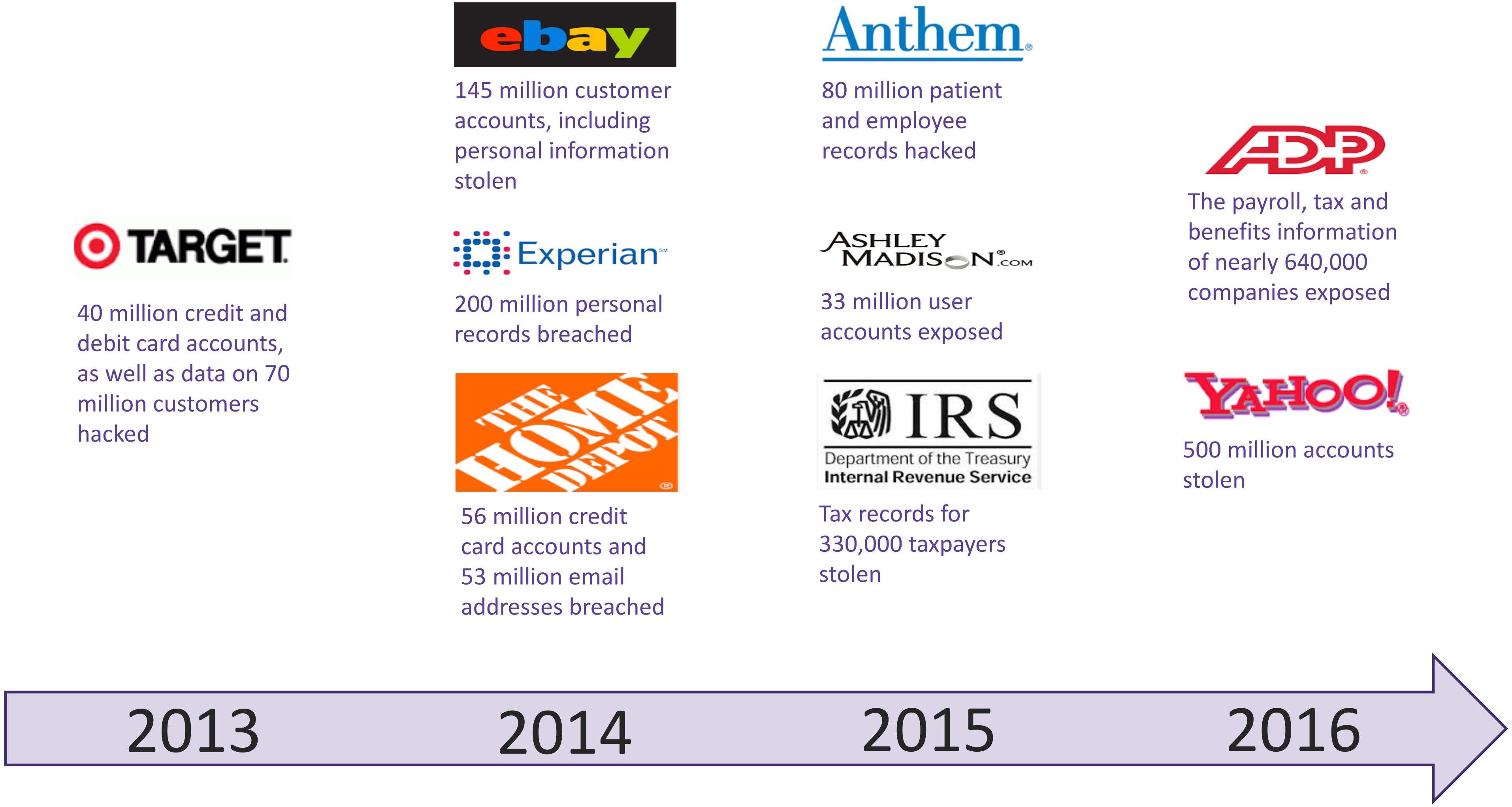
Serving Metro networks: high-capacity cloud & data center connectivity, mobile backhaul and virtualized & programmable networks

GLOBAL PRESENCE

Founded in 1988 (NASDAQ: MRVC)

- R&D centers in USA and Israel
- HQ in Chatsworth, CA, USA

High profile data breaches in recent years



2013

TARGET

40 million credit and debit card accounts, as well as data on 70 million customers hacked

2014

ebay

145 million customer accounts, including personal information stolen

Experian

200 million personal records breached

THE HOME DEPOT

56 million credit card accounts and 53 million email addresses breached

2015

Anthem

80 million patient and employee records hacked

Ashley Madison.com

33 million user accounts exposed

IRS Department of the Treasury Internal Revenue Service

Tax records for 330,000 taxpayers stolen

2016

ADP

The payroll, tax and benefits information of nearly 640,000 companies exposed

YAHOO!

500 million accounts stolen

Data breach statistics

Data breach statistics

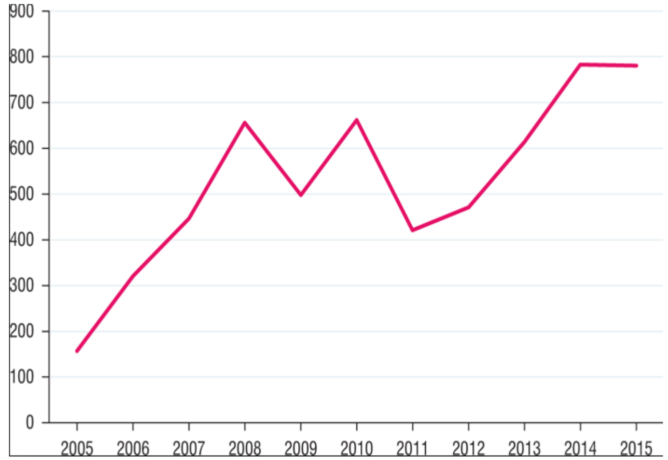
- Almost 800 U.S. data breaches reported in 2015
- U.S. government has spent $100 billion on cybersecurity over the past decade, and has $14 billion budgeted for cybersecurity in 2016
- In 93% of breaches, attackers take minutes or less to compromise systems
- Only 38% of global organizations feel prepared for a sophisticated cyberattack

Security breach notification laws

- Who must comply with the law
- Definitions of “personal information” (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.)
- What constitutes a breach (e.g., unauthorized acquisition of data)
- Requirements for notice (e.g., timing or method of notice, who must be notified)
- Exemptions (e.g., for encrypted information)

Data breach cost statistics

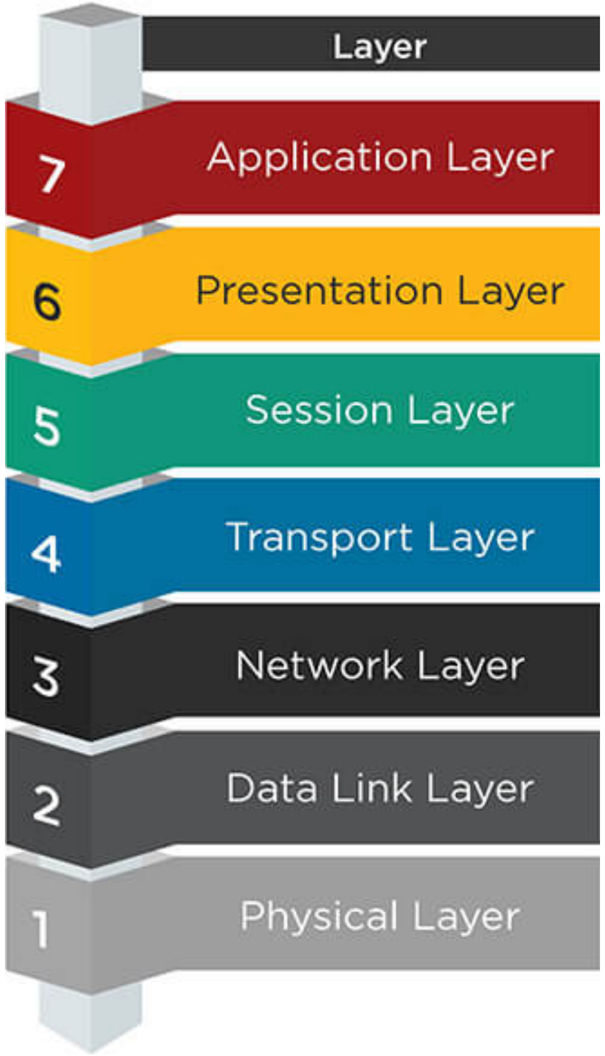
- 80% of analyzed breaches had a financial motive
- Impact from trade secret theft ranges from 1% to as much as 3% of a nation’s GDP
- 68% of funds lost as a result of a cyber attack were declared unrecoverable
- Damaged reputation/brand
- Lost opportunities
- Average organizational breach cost $3.79M



Almost 800 U.S. Data Breaches Reported in 2015

Data encryption at different network layers

- Application level encryption – the end to end data encryption process is completed by the application that is used to generate or modify the data that is to be encrypted
- IP level encryption: Internet Protocol Security (IPsec) is a protocol suite that provides network (IP) layer security by authenticating and encrypting each IP packet of a communication session
- Ethernet level encryption: 802.1AE is the IEEE MAC Security standard (MACsec) that provides link layer security. Key management and the establishment of secure associations is specified by 802.1X-2010
- Transport level encryption: when implemented within OTN frame is payload agnostic. Main advantages of L1 encryption include
  - Directly integrated into the NE
  - Low latency
  - Wire speed data throughput

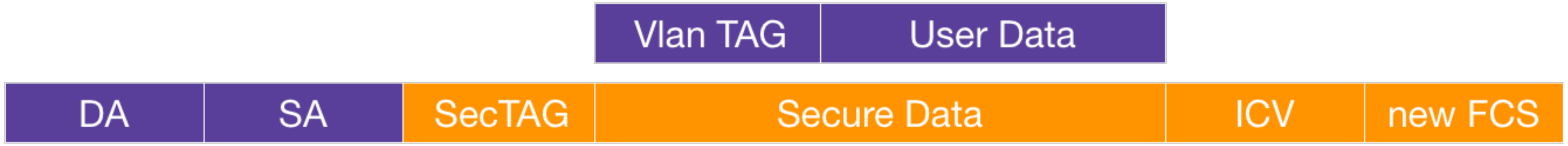


IPsec (Layer 3) Encryption

- IPsec enables the encryption of individual packets that make up traffic flows in the IP domain. Authentication headers are added on a per packet basis and are used to validate access to the encrypted data
- IPsec offers a true standards-based end-to-end encryption solution that is agnostic to the underlying physical network equipment in place—routers, optical transport equipment, etc.

- IPsec has several potential limitations
  - IPsec by definition does not support non-IP traffic flows, including datacenter storage protocols such as Fiber-Channel and Infiniband
  - There is also a performance vs. cost and power trade off related to incremental processing (CPU) and associated memory resources
  - The additional overhead necessary to secure each packet results in packet size expansion which in turn results in increases in network latency and wasted bandwidth on optical fiber networks

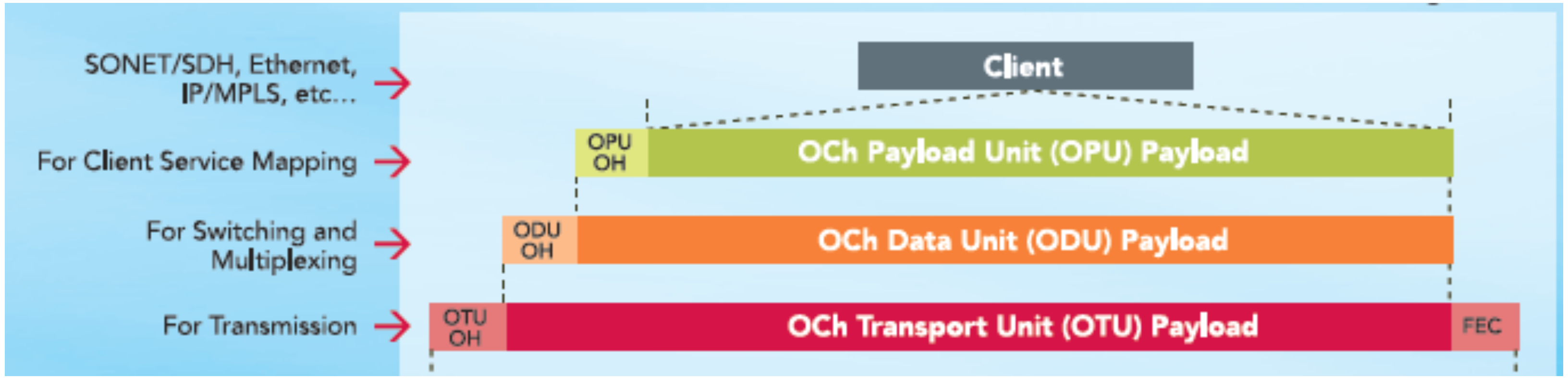
MACsec (L2) Encryption



ICV: Integrity
Check Value

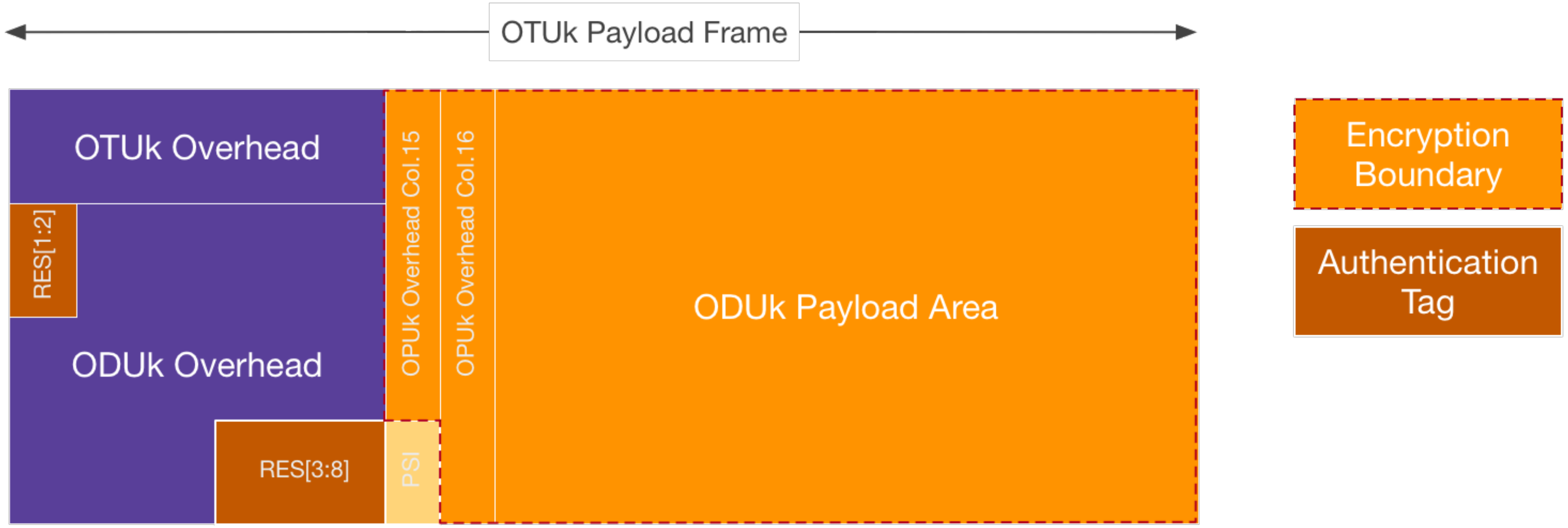
- MACsec security architecture comprises two components:
  - A control plane that provides an authenticated key agreement protocol as defined in 802.1X
  - A data plane for secure transport of payloads (802.1AE compliant) in order to protect the upper protocol data
- Hop-by-hop security architecture (this puts some constraints on its applicability)
- Excludes native support for non-Ethernet client types
- Connectionless data integrity
- Data origin authenticity
- Confidentiality

OTN Terminology


SONET/SDH, Ethernet, IP/MPLS, etc...
For Client Service Mapping
For Switching and Multiplexing
For Transmission
Client
OPU OH
OCh Payload Unit (OPU) Payload
ODU OH
OCh Data Unit (ODU) Payload
OTU OH
OCh Transport Unit (OTU) Payload
FEC

- If it is a signal being transmitted between two points on a wavelength, it’s an **OTU**
- If it’s the payload within the OTU that’s being switched, multiplexed, or otherwise moved around, it’s an **ODU**
- You will probably never hear the term **OPU**

OTN (L1) encryption

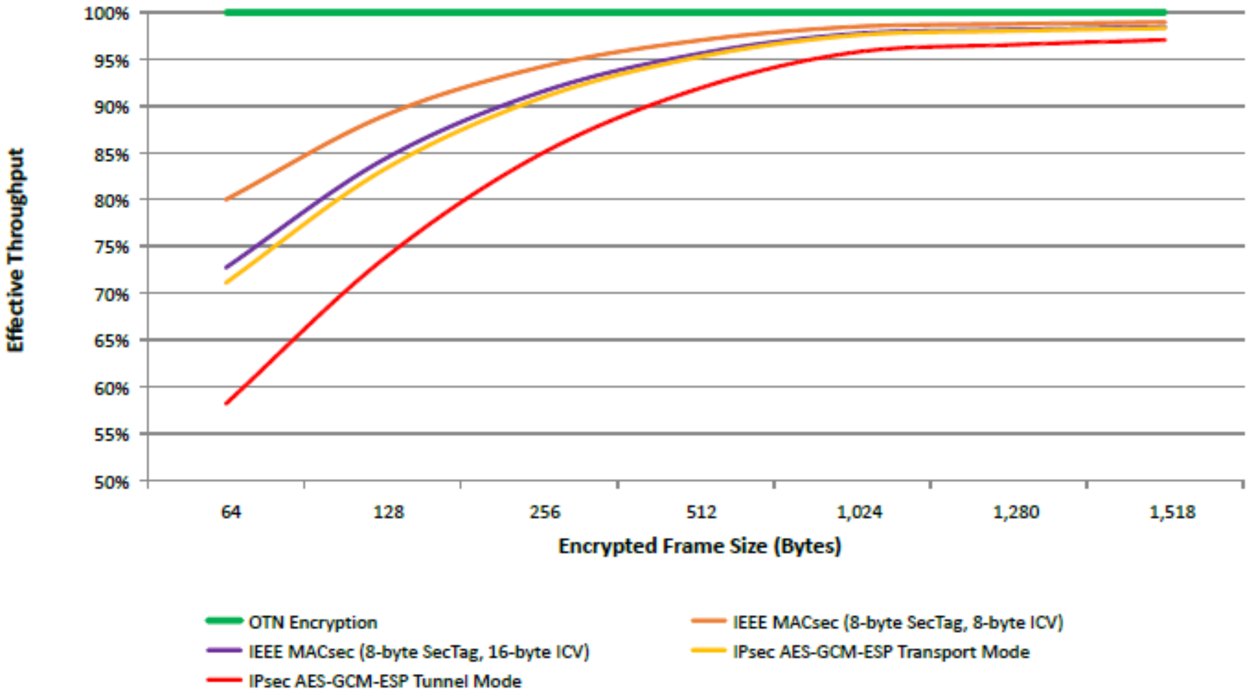


- OTN encryption refers to encrypting the OPUk payload
- OTN encryption does not change the ODUk frame format
- Optimized network efficiency & latency
- OTN encryption offers 100% throughput regardless of the underlying client type or frame-size of packet-based traffic
- Multi-service capability
- Maximum network deployment flexibility and scalability

Throughput versus Encryption Methods

- OTN encryption offers 100% throughput regardless of the underlying client type or frame-size of packet-based traffic

- L2/L3 solutions on the other hand increase latency considerably which has negative impact on user experience



- IPsec (L3) encryption offers a granular, per device or per user policy. Enterprises can leverage more traditional Layer 3 IPsec encryption utilizing high-speed switching technology and fast pipes

- MACsec (L2) encryption is a high-performance security option that offers some advantages over Layer 3 in some scenarios, particularly in network environments that require low-latency, high-volume data transmission of voice, video and other latency sensitive traffic

- OTN (L1) encryption offers 100% throughput regardless of the underlying client type or frame-size of packet-based traffic.

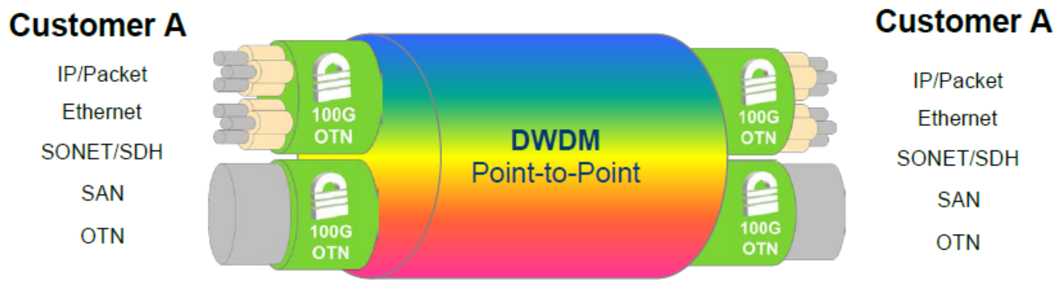
Line side OTN encryption

- IPsec (L3) encryption offers a granular, per device or per user policy. Enterprises can leverage more traditional Layer 3 IPsec encryption utilizing high-speed switching technology and fast pipes

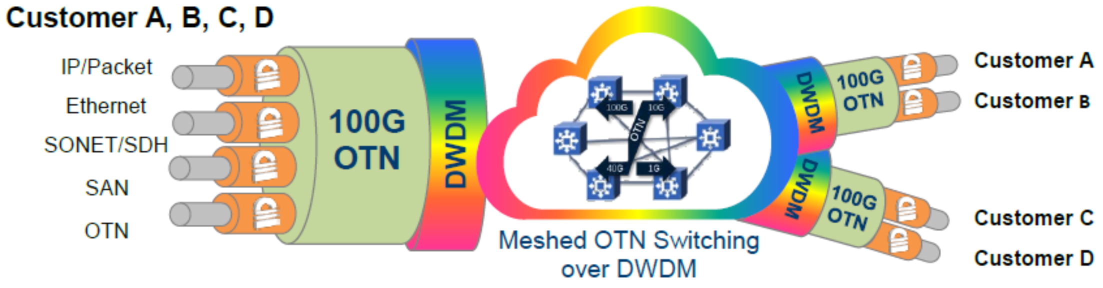
- MACsec (L2) encryption is a high-performance security option that offers some advantages over Layer 3 in some scenarios, particularly in network environments that require low-latency, high-volume data transmission of voice, video and other latency sensitive traffic

- OTN (L1) encryption offers 100% throughput regardless of the underlying client type or frame-size of packet-based traffic.

Line-side versus Client-side (service) OTN encryption



100G Bulk OTN Encryption



Sub-Wavelength OTN Encryption, Multiple Customers, OTN Switched Network

OTN Trunk encryption

- encryption at the wavelength level, such as 10G, 100G or 200G wavelengths
- Typically deployed in point-to-point WDM network configurations and single end-customer deployment scenarios
- Example: leased wavelength encrypted transport service or an encrypted Datacenter Interconnect (DCI) service

SUB-Wave OTN encryption

- encrypting lower-rate clients prior to multiplexing into higher-rate unencrypted wavelengths
- traffic flows are encapsulated into encrypted OTN containers and traverse the network independently, addressing the requirement for end-to-end security of individual data traffic sources
- individual sub-wavelength traverse the networks independently, without the need to decrypt higher-rate wavelengths and therefore compromise the security of sub-wavelength traffic

MRV Encryption enabled transport

OD-TXP-QC2D

- OptiDriver® 100G transponder
- 100GE & OTU-4 transponder
- Access: QSFDP28 Line: CFP2

OD-1MXP200-QC2D

- 200G muxponder - 2x100G over 200G
- Single height/Dual wide module
- Line: CFP2 Digital Optical Line Interface
- Access: 2 x 100G QSFP28

OD-3MXP200-QC2D

- Triple 200G muxponder
- 3 200G muxponders on a single module
- Access: QSFP28 Line: CFP2

Encryption features

Encryption latency	AES256 @ 180ns
Block Cipher mode supported	Counter mode (CTR), Galois/Counter mode (GCM)
Authentication mode	Galois (GMAC)
Encryption facilities	Sub-wave Encryption / Trunk Encryption
Payload Encryption supported	OPUflex/0/1/2/3/4
Key Exchange Facilitation	Support for Current and Next key per engine
Key Life Time	User configurable (by # of frames)

MRV®

NASDAQ: MRVC

Thank you

www.mrv.com

benelux@mrv.com