Data Security using MACsec

Introduction

Chakri Alluri
Principal FAE

Jan 2023

AGENDA

- Data security overview
- MACsec overview & history
- MACsec protocol & operation
- Sample use cases
- Marvell support & configuration

Data Security

Overview

Need for data security

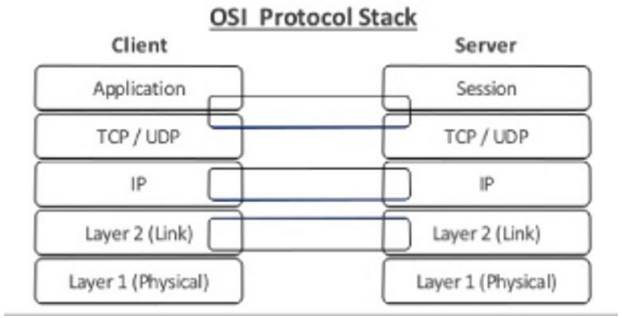
- End-to-end security of data needs security when
  - Data is *at rest*
    - During data processing
    - Stored in a device
  - Data is *in motion*
    - Data is being communicated between devices

Data at rest

- Security provided by ***Hardware root of trust*** anchored in silicon
  - Inherently trusted and secure by design
  - Contains security keys used for cryptographic functions
    - Data encryption
    - Certificate validation
    - Key management
  - Enables a secure boot process
- Can be a standalone security module or within SoC
- Can be a Fixed function or Programmable

Data in motion

- Security anchored in hardware at foundational communication layer
- Done using network security protocols
  - TLS (SSL)
    - For secure communications between applications
  - IPsec
    - For secure IP traffic between Networks & Hosts
  - MACsec
    - Protect Ethernet links between Switches and Hosts



Requirements for security protocols

- Meet line rate throughput
  - Vast proliferation of applications
    - Streaming 4K videos
    - Transmission to the Cloud(s)
    - IoT devices increasing by billions
- Limit latency
  - Applications mandate constant latency
- Support prioritization
  - Prioritization/preemption of packets for applications like TSN
- Cope with network diversity & deployments

MACsec

Overview & History

What is MACsec?

- IEEE standard that provides point-to-point security on Ethernet links
- Defined in IEEE 802.1AE
- The Ethernet connected devices can be
  - Directly connected, and/or
  - Regardless of number of intervening devices or the networks
- Operates at Layer2
- Provides
  - Confidentiality (via data encryption)
  - Integrity (frame integrity check)
  - Authenticity (data origin validation)

What is MACsec? (contd.)

- Encryption/decryption standard that identifies & prevents most security threats, including
  - DoS
  - Intrusion attacks
  - Man-in-the-middle attacks
  - Masquerade attacks (pretending to be someone one is not)
  - Passive wiretapping
  - Playback attacks
- Can be used in combination with other security protocols (IPsec, SSL/TLS) to provide end-to-end network security

What is MACsec? (contd..)

- Leverages onboard encryption/decryption rather than offload to an encryption engine
- Secures an Ethernet link for almost all traffic
- Includes traffic that are not typically secured by other security protocols
  - LLDP
  - LACP
  - DHCP
  - ARP, etc.
- Transparent to higher-level functions that inspect and classify traffic (Firewall)

What is MACsec? (contd…)

- Does not authorize the systems connected to network
  - Done by IEEE 802.1X
  - Enforces prior authentication
    - Valid symmetric key is a must to receive traffic
    - Only way to get a key is via authentication
  - Makes DoS attacks difficult
    - It cannot prevent a device from transmitting
    - But it can prevent a device from lying about its identity
- Enables those systems to encrypt traffic destined for the network
- MACsec is used on wired networks only

MACsec Services

- Data encryption
  - Encrypt outbound frames
  - Decrypt MACsec encrypted inbound frames
- Integrity check
  - Use key negotiated via MKA to calculate ICV for the frame
  - Compare the calculated ICV with ICV in the frame trailer
    - If ICV matches, the frame is legal
    - Otherwise, device determines whether to drop the frame or not based on validation mode
- Replay protection
  - Allows to accept out-of-order packets within replay protection window size
  - Drop out-of-order packets

History of MACsec

- Developed to complement 802.1X-2004 standard
- First standardized in 2006 by IEEE 802.1AE-2006
- Multiple revisions since then have added …
  - Strong cipher suites
  - Extended packet number
  - Provider Network support, etc.
- 2006 standard uses GCM-AES-128bit cipher suite
- Newer standards support GCM-AES-128 & 256-bit keys
  - Required for line-rate encryption performance @ 1G/10G/100G/400G
- Current version is IEEE 802.1AE-2010

History (contd.)

- Innovations are driven by continuously increasing bandwidth demand
  - DCI
  - Branch back-haul
  - Metro Ethernet, etc.
- Evolved from a LAN encryption technology to a much wider area in
  - WAN transport
  - Cloud and Data Center
  - 5G, and
  - Automotive networks

Benefits of MACsec

- Much better encryption performance at higher speed compared to IPsec
- In addition to network security, offers…
  - Scalability
  - No software intervention
  - Full speed operation
  - Device-to-device security
  - Connectionless data integrity
  - Data origin authenticity
  - Confidentiality
  - Replay protection
  - Bounded receive delay

MACsec applications

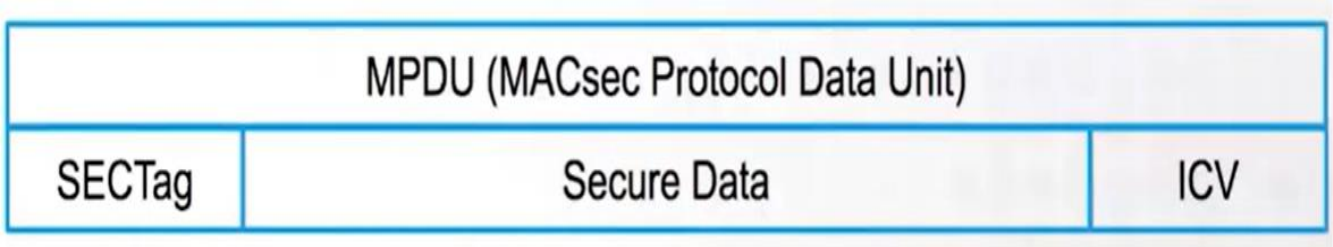
Used in …

- LAN switches
- WAN/MAN routers
- Data Center routers/switches
- Server, storage and ToR switches
- Secure end-points such as
  - Security camera
  - Industrial robots
- 5G
- Automotive, etc.

MACsec

Protocol & Operations

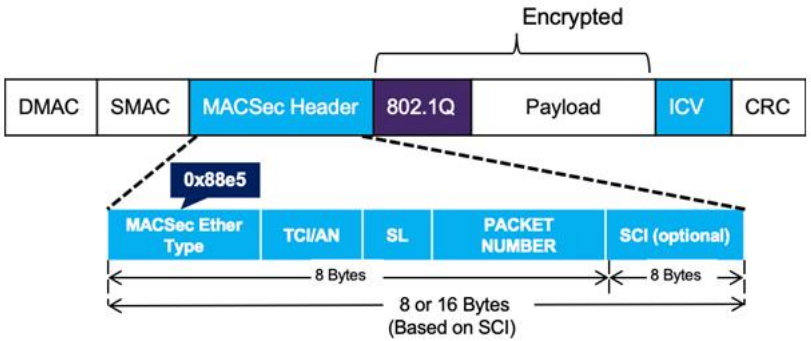
MACsec PDU



SECTag	Security Tag 8-16B in length (16B with SCI) Identifies the key to be used to validate the frame Provides replay protection when frames are received out of sequence
Secure Data	Data in frame that is encrypted by MACsec
ICV	Provides integrity check for the frame Usually 8-16B in length depending on cipher suite Frames that do not match expected ICV are dropped

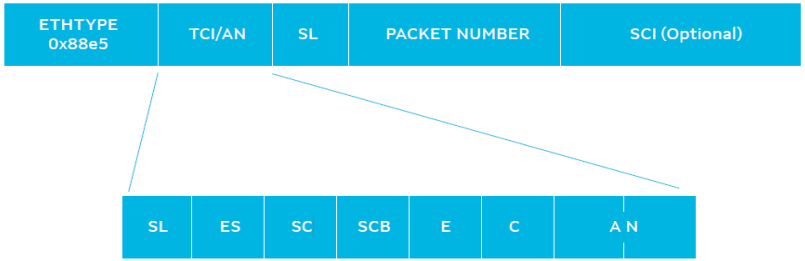
MACsec Frame Format

Based on standard Ethernet frame



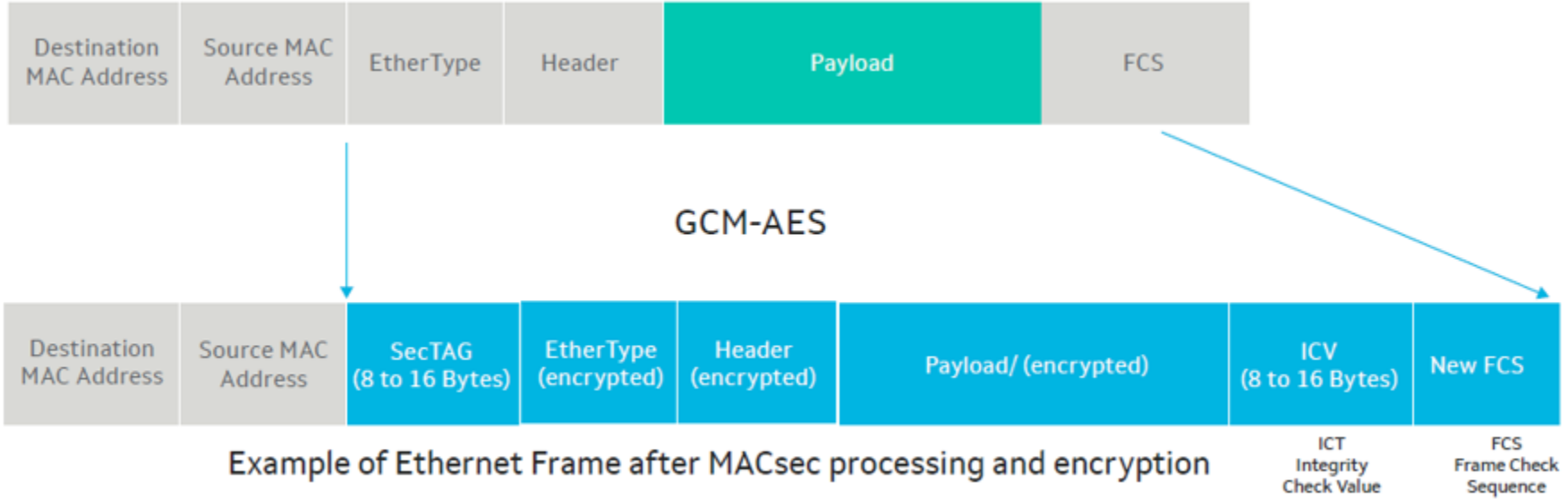
MACsec Ether Type	0x88e5
TCI/AN	TAG Control Information (TCI)/Association Number
SL	Short Length - length of encrypted data
PN	Packet number used for replay protection
SCI	Secure Channel Identifier for a CA Concatenation of MAC address & 16-bit port ID
ICV	16B generated by GCM-AES to ensure source node identify and integrity of the frame

TCI/AN fields



ES	End Station bit
SC	If SC=1, SCI field is present
SCB	Single Copy Broadcast
E & C	Used to determine if packet is encrypted E,C = 1,1 (Encrypted) E,C = 0,0 (Authenticated only)
AN	Used for key rotation

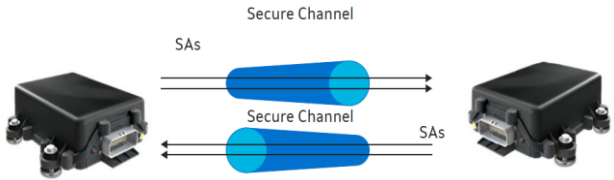
Ethernet frame – before & after MACsec



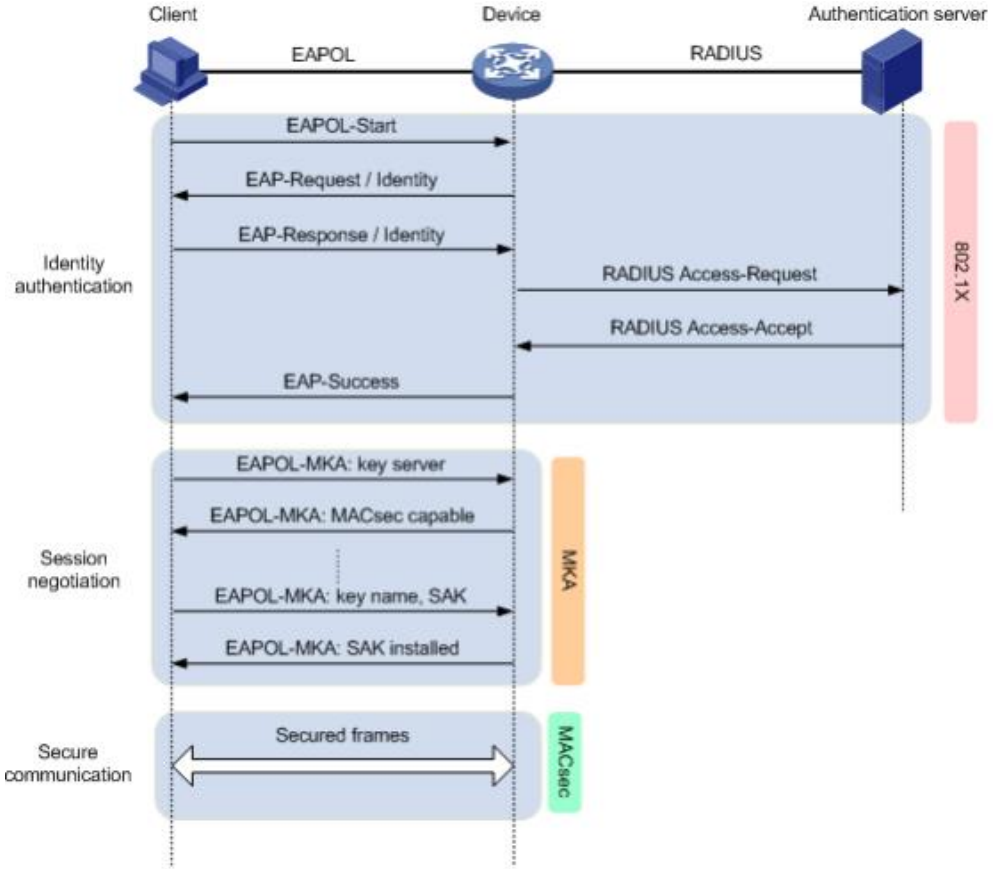
Example of Ethernet Frame after MACsec processing and encryption

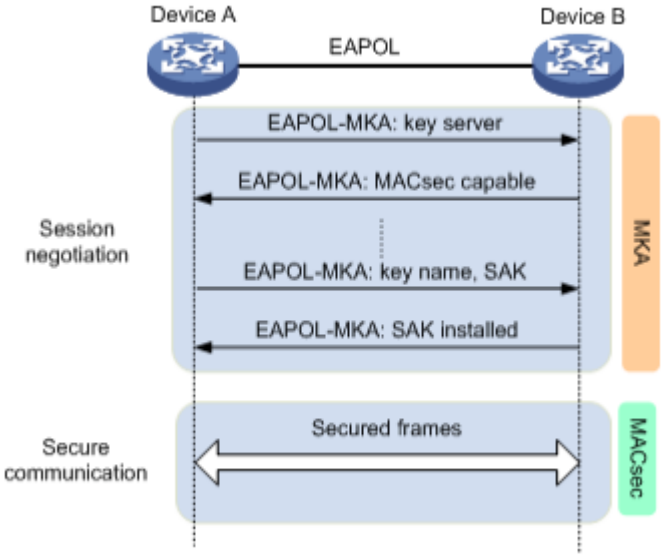
MACsec operation - Overview

- Overall, 2 steps involved in MACsec operation
- Step-1: MKA discover & establish session between potential peers
  - MKA provides a method of discovering peer and negotiating security keys
  - When MACsec enabled interfaces come up, they start exchanging MKA frames
    - If parameters are valid, then peer will be discovered and accepted
  - Depending on KS priority of the device, Key Server is elected
  - On successful session establishment, KS generates SAK and distributes through MKA messages
- Step-2: SAK is used to encrypt/decrypt data traffic
  - All MACsec frames are encrypted using SAK
  - Separate Tx and Rx secure channels created



MACsec operation modes





How MACsec works?

- When MACsec is enabled, a bi-directional secure link is established
  - Exchange and verification of security keys between devices
- Uses combination of data integrity and encryption to safeguard transmitted data
- Sending device
  - Appends a header & tail to all Ethernet frames
  - Encrypts data payload within the frame
- Receiving device
  - Check header & tail for integrity
  - If check fails, packet is dropped
  - On success check, packet is decrypted

MACsec – Terminology

- ***MACsec Key Agreement*** (MKA) protocol is control protocol between MACsec peers
  - Used for peer-discovery and negotiating encryption keys
  - Provides session keys and manages encryption keys
- ***Connectivity Association*** (CA) is a group of participants that use same key and key algorithm
  - Established and maintained by MKA
  - Security relationship between MACsec peers
- The encryption key used by CA participants is called a ***Connectivity Association Key*** (CAK)
  - CAK can be
    - An encryption key generated during 802.1X authentication
    - A user-configured ***Pre-Shared Key*** (PSK)

MACsec – Terminology (contd.)

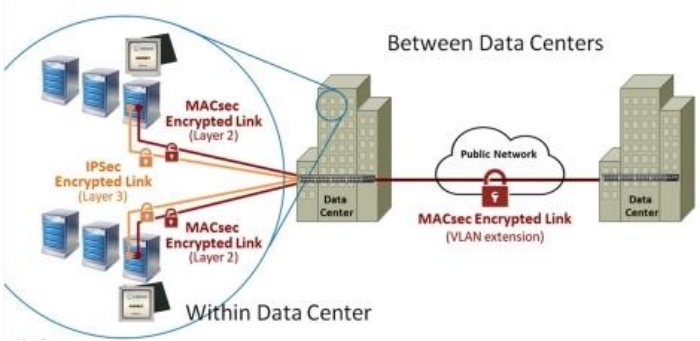
- ***Secure Association*** (SA) is an agreement negotiated by CA participants
  - It includes a cipher suite and keys for integrity check
- A ***Secure Channel*** (SC) uses one or more SAs
  - SC provides a unidirectional point-to-point or point-to-multipoint communication
- Each SA uses a unique ***Secure Association Key*** (SAK)
  - SAK is generated from CAK
  - MACsec uses SAK to encrypt data transmitted along the SC
- **Extensible Authorization Protocol** (EAP) provides the authentication framework via Supplicants (clients), Authenticator and Authentication Server
- **EAPoL** (EAP over LAN) is network port authentication protocol used in IEEE 802.1X

MACsec

Sample Use Cases

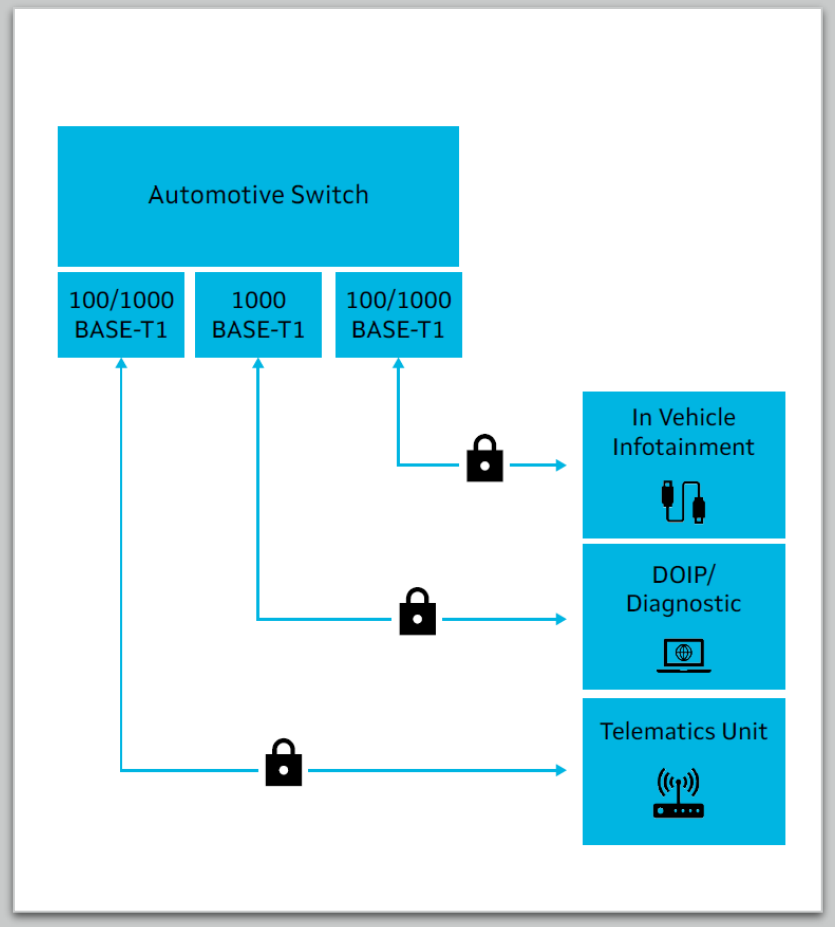
Data Centers

- Enabling secure interconnect for next-gen CSPs
- Hyper Scalers adapting encryption technologies due to
  - ✓ Cost
  - ✓ Overhead on high-speed data links
- Silicon vendors & NEMs support MACsec in their next gen chips/routers/switches etc.



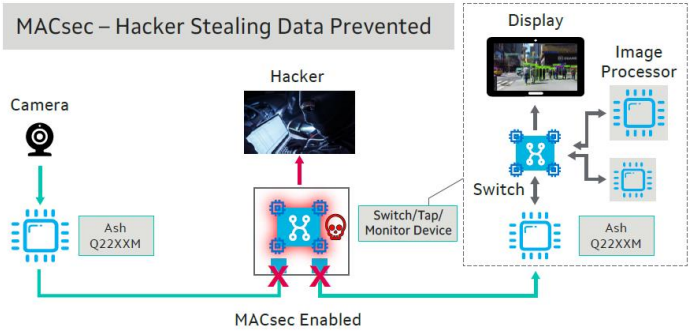
Automotive

- Increased vehicle connectivity & autonomous functionality
- Ethernet becoming essential part of Automotive architecture
- Ethernet links are used between ECUs (Electronic Control Units)
- Need arises to protect data that is transported on such connectivity links



Automotive/IoT

- The inline connectors provide attack opportunities to hackers
- Hackers can steal/disrupt data
- DoS attacks on image processing and jam links
- MACsec based solutions achieve functional safety compliance at system level



Specifications

Standard	Description
IEEE 802.1AE-2006	MAC security
IEEE 802.1X-2010	Port-based Network Access Control MKA protocol specification
IEEE 802.1AEbn-2011	GCM-AES-256 Cipher Suite (Galois Counter Mode – Advanced Encryption Standard)
IEEE 802.1AEbw-2013	Extended Packet Numbering Cipher suites
IEEE 802.1AEcg-2017	EDEs – Ethernet Data Encryption devices Transmission using multiple SCs for strict replay protection
IEEE 802.1Xbx-2014	MKA extensions

MACsec

@ Marvell

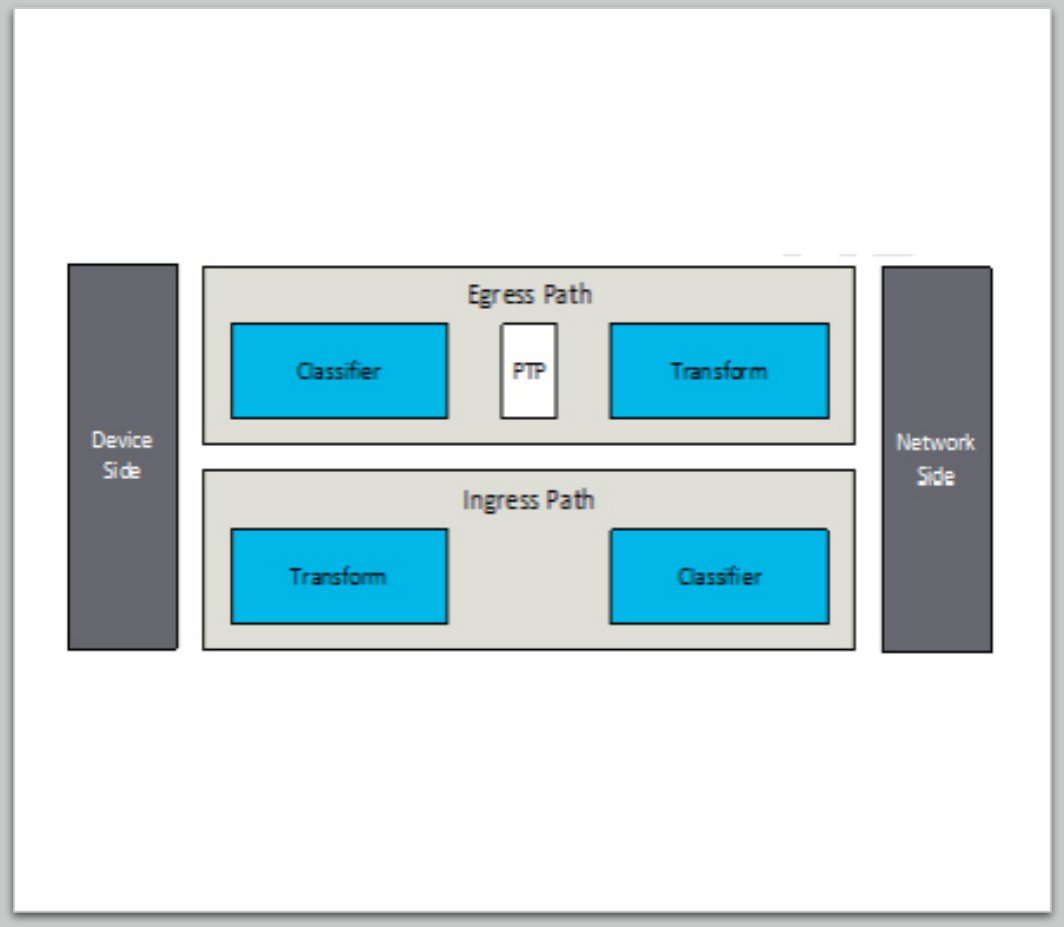
MACsec function

- Contains 2 separate instances of MACsec engines covering both Ingress & Egress traffic, and controlling latency within egress path
- Egress (System -> Line side)
  - Adds SECTag identified by special ether-type 0x88E5
  - Adds ICV
  - Optionally encrypt payload
- Ingress (Line -> System side)
  - Identify and decrypt MACsec packets
  - Check integrity, provides replay protection
  - Remove SECTag/ICV
  - Invalid frames are discarded or monitored

MACsec architecture

MACsec engine is split into 2 main units

- Classifier Unit
- Transform Unit



MACsec architecture - Classifier Unit

- Performs MACsec header classification (multiple channels & vPorts)
- Control packet detector
  - Supports extensive set of programmable rules
  - Control protocols can be configured to bypass MACsec encryption
- Frame header parser
  - Supports 4xVLAN tags before SECtag header
- MACsec header parser
- MACsec header parsing following VLAN headers
  - Supports ClearTags functionality

MACsec architecture - Transform Unit

- High-performance MACsec frame processing engine
- Provides complete MACsec SecY frame transformation for multiple channels & vPorts
- In egress direction
  - Computes SECTag header, ICV and encrypts data if encryption is enabled for that SC
- In ingress direction
  - Decrypts the frame and verifies MACsec matches IEEE 802.1AE standard

Marvell devices support

- Ethernet PHYs
  - Alaska family (88E1340M, 88X7121P,…)
- Packet Processors
  - 98X2220 multi-port 10GbE
- Automotive solutions
  - Brightlane Automotive Ethernet portfolio
    - Switch family supporting MACsec, Trusted boot, DPI, TSN and AVB
    - PHY family supporting 10/100/1000BT1, MACsec, and PTP
    - Bridge family supporting 802.3ch 10/5/2.5GBT1
- Datacenter & 5G solutions
  - 88X7121P (supporting Retiming & Gearbox functionality)
  - Prestera CX-8500 400GbE switch

MACsec configuration on a Prestera switch

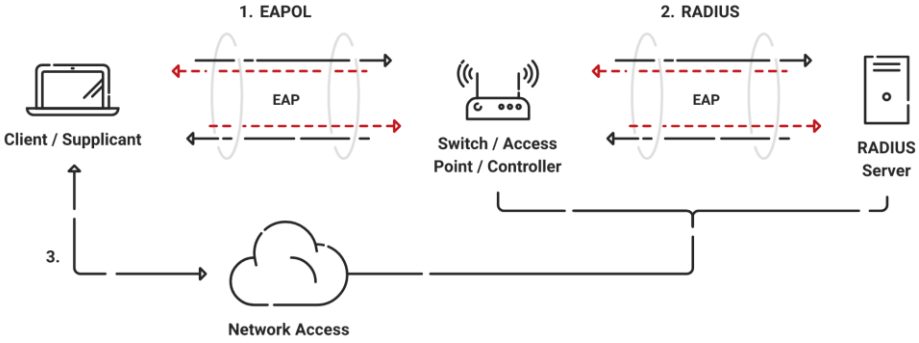
Steps	APIs	Description
Initialize MACsec on the device	cpssDxChMacSecInit	Init MACsec for a device
Enable MACsec for a port	cpssDxChMacSecPortClassifyConfigSet cpssDxChMacSecPortSecyConfigSet	Enable/bypass MACsec for a port to set MACsec mode for Classifier and Transform unit
Installing vPort in Classifier Unit	cpssDxChMacSecClassifyVportAdd cpssDxChMacSecClassifyVportIndexGet	Install and obtain vPort handler for ingress/egress Classifier
Install SA record in Transform Unit	cpssDxChMacSecSecySaAdd cpssDxChMacSecSecySaActiveGet	Install an SA record on TU for both ingress/egress & obtain currently active SAs for a vPort/SCI
Install rules in Classifier Unit	cpssDxChMacSecClassifyRuleAdd cpssDxChMacSecClassifyRuleEnable	Install classifier rules on ingress/egress vPorts & enable

MARVELL

Thank You

802.1X Authentication

- IEEE standard for Port-based Network Access Control (PNAC)
- Allows access to networks with use of RADIUS server
- Gold standard for secure wireless and wired networks
- EAP is standard authentication protocol on encrypted networks
- Uses 802.1X for passing EAP over wired or wireless LAN
  - Provides encrypted EAP tunnel
  - Transfers user's identity info
- 802.1X is encrypted



WPA2 Enterprise Protocols	Level of Emcrption	Authentication Speed	Directory Support	Credentials
EAP-TLS	Public-Private Key Cryptography	Fast - 12 Steps	SAML/LDAP/MFA	Passwordless
PEAP-MSCHAPV2	Encrypted Credentials	Slow - 22 Steps	Active Directory	Passwords
EAP-TTLS/PAP	Non-Encryted Credentials	Slowest - 25 Steps	Non-AD LDAP Servers	Passwords