Hewlett Packard Enterprise

HPE aruba networking

AOS-CX 10.13 Update: MACsec Extensions for WAN

Shobana Nandakumar , Technical Marketing Engineer

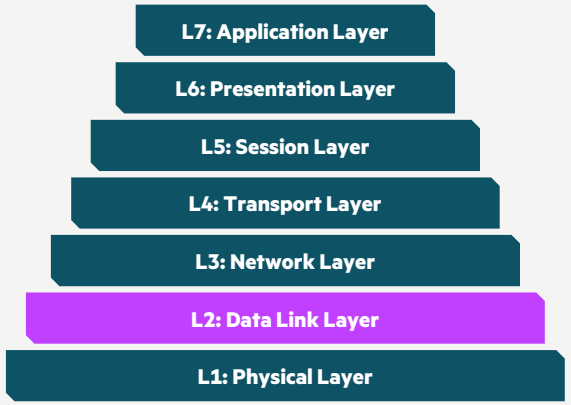
Nov, 2023

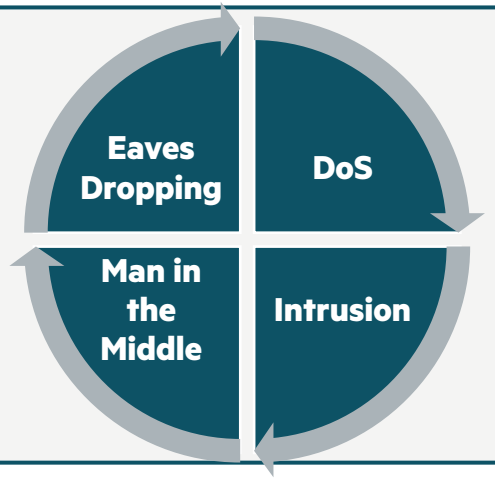
Acronyms

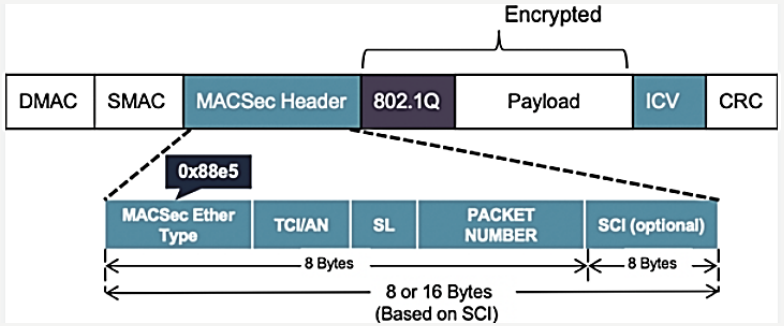
MACsec	**M**edium **A**ccess **C**ontrol **sec**urity
MKA	**M**ACsec **K**ey **A**greement
LAN	**L**ocal **A**rea **N**etwork
WAN	**W**ide **A**rea **N**etwork
EAPoL	**E**xtensible **A**uthentication **P**rotocol **o**ver **L**AN
CAK	**C**onnectivity **A**ssociation **K**ey
CKN	**C**onnectivity Association **K**ey **N**ame
PE	**P**rovider **E**dge
CE	**C**ustomer **E**dge
CFR	**C**ode of **F**ederal **R**egulations
ENC	**E**ncryption **C**ommodities
CSfc	**C**ommercial **S**olutions **f**or **C**lassified
COTS	**C**ommercial **o**ff the **S**helf
MPLS	**M**ulti **P**rotocol **L**ayer **S**witching

Overview

MACsec Overview







Media Access Control security (MACsec) provides L2 hop-by-hop encryption on point-to-point Ethernet links.

- Protects against network data breaches.
- L2 security establishes foundation for security for entire network stack.

MACsec appends a header and tail to all Ethernet frames, and encrypts data payload within the frame.

MACsec Terminologies

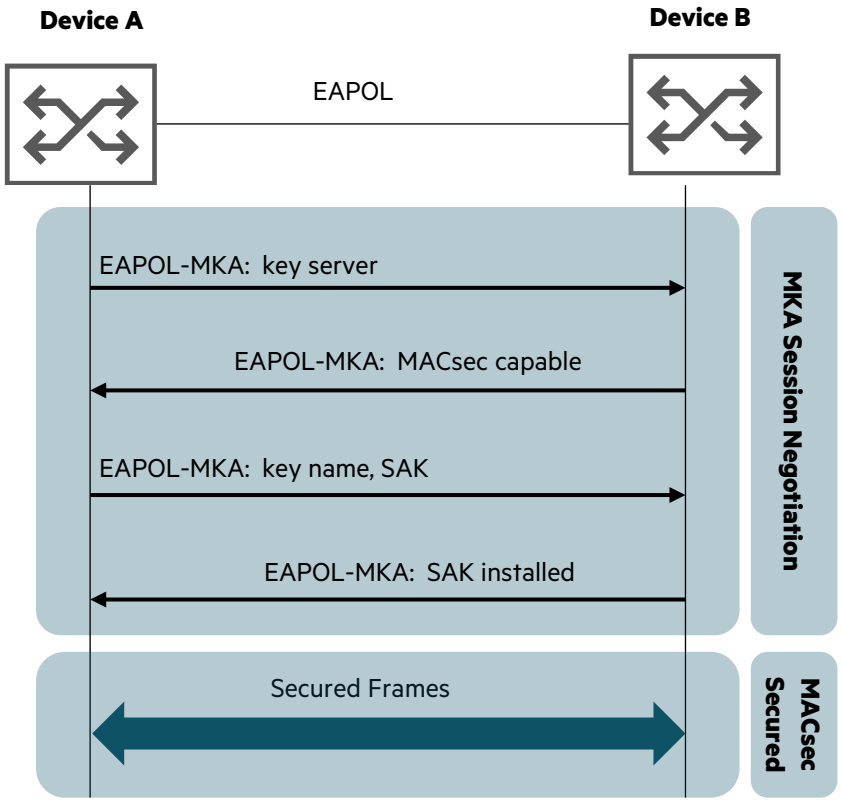
MKA – MACsec Key Agreement Protocol – discovers peers, negotiates keys, and provides session keys.

CAK – Connectivity Association Key – used by MKA to derive a transient session key called the **SAK** (Secure Association Key). SAK used by the network device ports to encrypt traffic for a given session

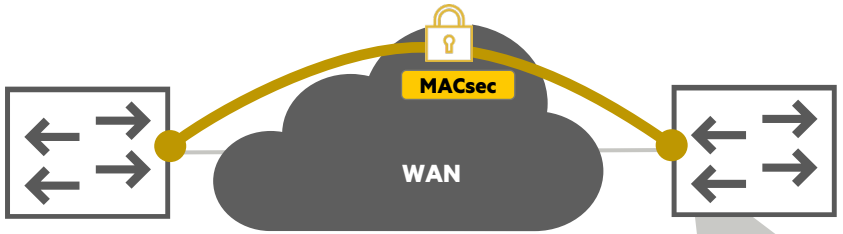
CA – Connectivity Association - A secure relationship between MACsec-capable devices. Endpoints that share CAK are part of same secure CA

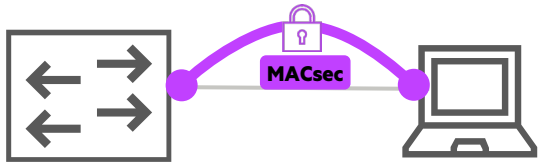
CKN – Connectivity Key Name – used as a container for storing the CAK.

Key Server - One of the MACsec peers in the CA becomes the Key Server. Main role is creation and distribution of SAKs, which are used in actual data encryption



HPE Aruba Networking CX MACsec Journey





- ✓ YouTube TOI

- ✓ PSK
  - ✓ YouTube TOI
- ✓ EAP-TLS
  - ✓ YouTube TOI

LAN MACsec

- PSK :– 10.06.0001
- EAP-TLS :– 10.10.0002

Switch to Host MACsec

- EAP-TLS :- 10.11.0001

WAN MACsec

- PSK :- 10.13.0005

WAN MACsec

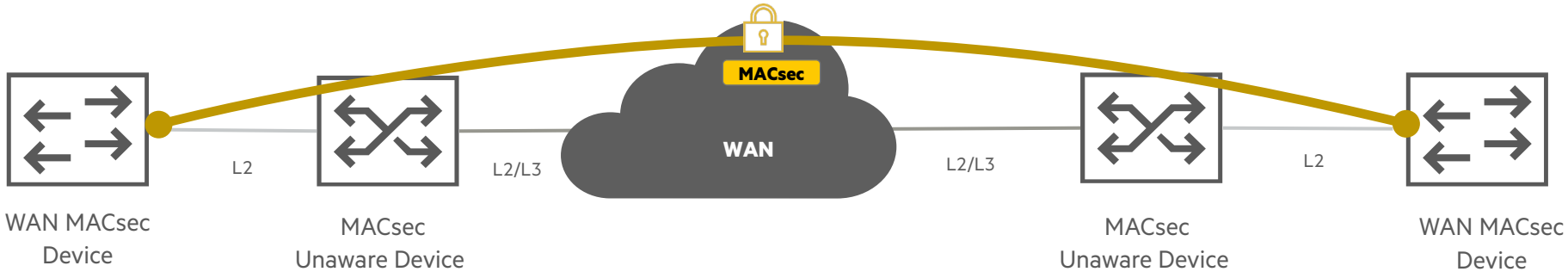
Application of MACsec Encryption standard to encrypt Layer 2 connections over WAN to guarantee:

- Connectionless data integrity
- Data origin authenticity
- Confidentiality
- Replay protections

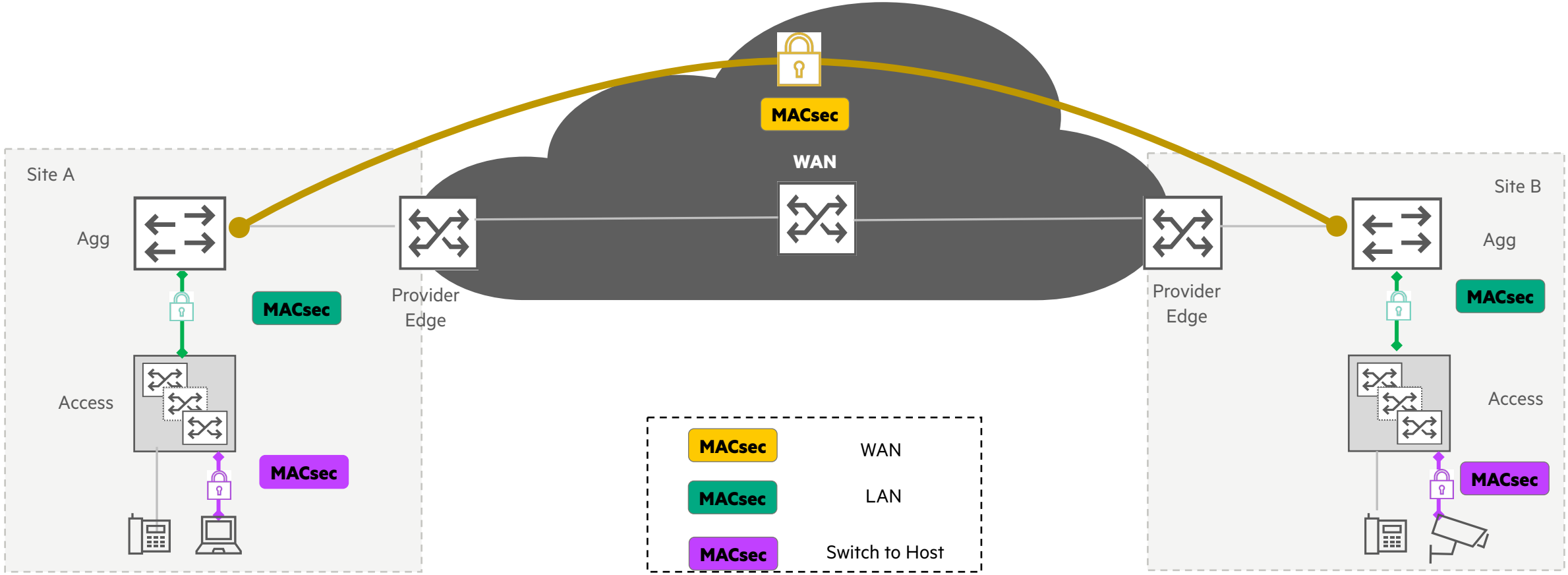
IEEE 802.1AE Standard Based , extensions to MACsec to support WAN . Supported in Physical L2 Ports.

Part of CX Advanced Feature Pack

Platforms Supported – 8360 and 6300



MACsec – End to End Protection



MACsec Extensions for WAN

EAPoL Destination MAC

- Configurable MKA-EAPoL Custom Destination Mac Address
- Enabling MACsec deployment between Non directly connected devices

Tagged EAPoL Frames

- 802.1Q Tag for MKA - EAPoL Frames
- Enabling QinQ Deployments with CVLAN transport (Control Plane)

WAN MACsec

Bypass BPDU

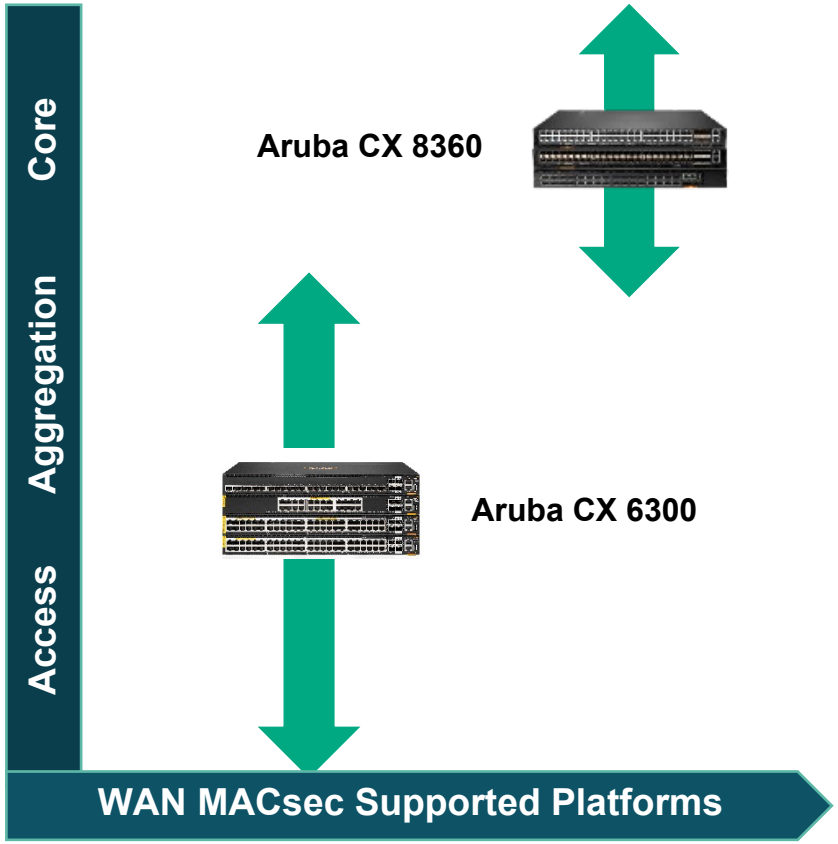
- MACsec Bypass for IEEE BPDUs
- Support for LLDP , flow-control , MVRP and Spanning Tree etc

Clear Tag Mode

- 802.1Q Tag in Clear
- Enabling QinQ Deployments with CVLAN transport (Data Plane)
- 802.1p bit in Clear - Qos Service Offerings

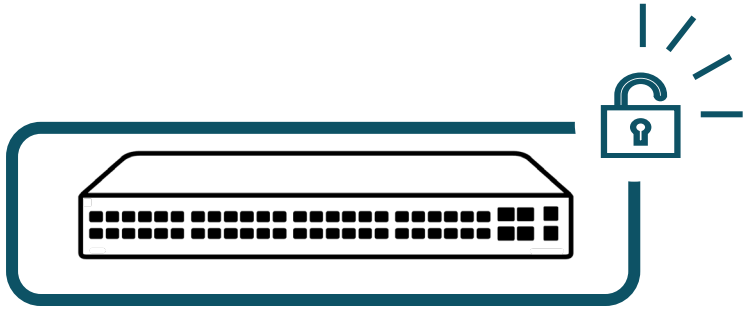
Platform Support Matrix

Platform	SKU	Description	Supported Interfaces *
8360	JL717A	Aruba 8360-32Y4C Switch	1-4
	JL717C	Aruba 8360-32Y4C v2 Switch	1-4
	JL719C	Aruba 8360-48Y6C v2 Switch	1-4 53-54
6300	R8S89A	Aruba 6300M 24SR CL6 PoE 2p50G 2p25G Switch	27-28
	R8S90A	Aruba 6300M 48SR5 CL8 PoE 2p50G 2p25G Switch	51-52
	R8S91A	Aruba 6300M 48SR5 CL6/CL8 2p50G 2p10G Switch	51-52
	R8S92A	Aruba 6300M 24p SFP+ LRM 2p50G 2p25G Switch	1-24 27-28



* Note - MACsec is not supported in ASIC in any of the platform, requires specific PHY for the MACsec enablement on particular port group

Why WAN MACsec part of CX Advanced Feature-Pack ?



Enhanced Security – Over WAN

Adhere to the “Code of Federal Regulations (CFR) - Export Administration Regulations “

Code of Federal Regulations (CFR)

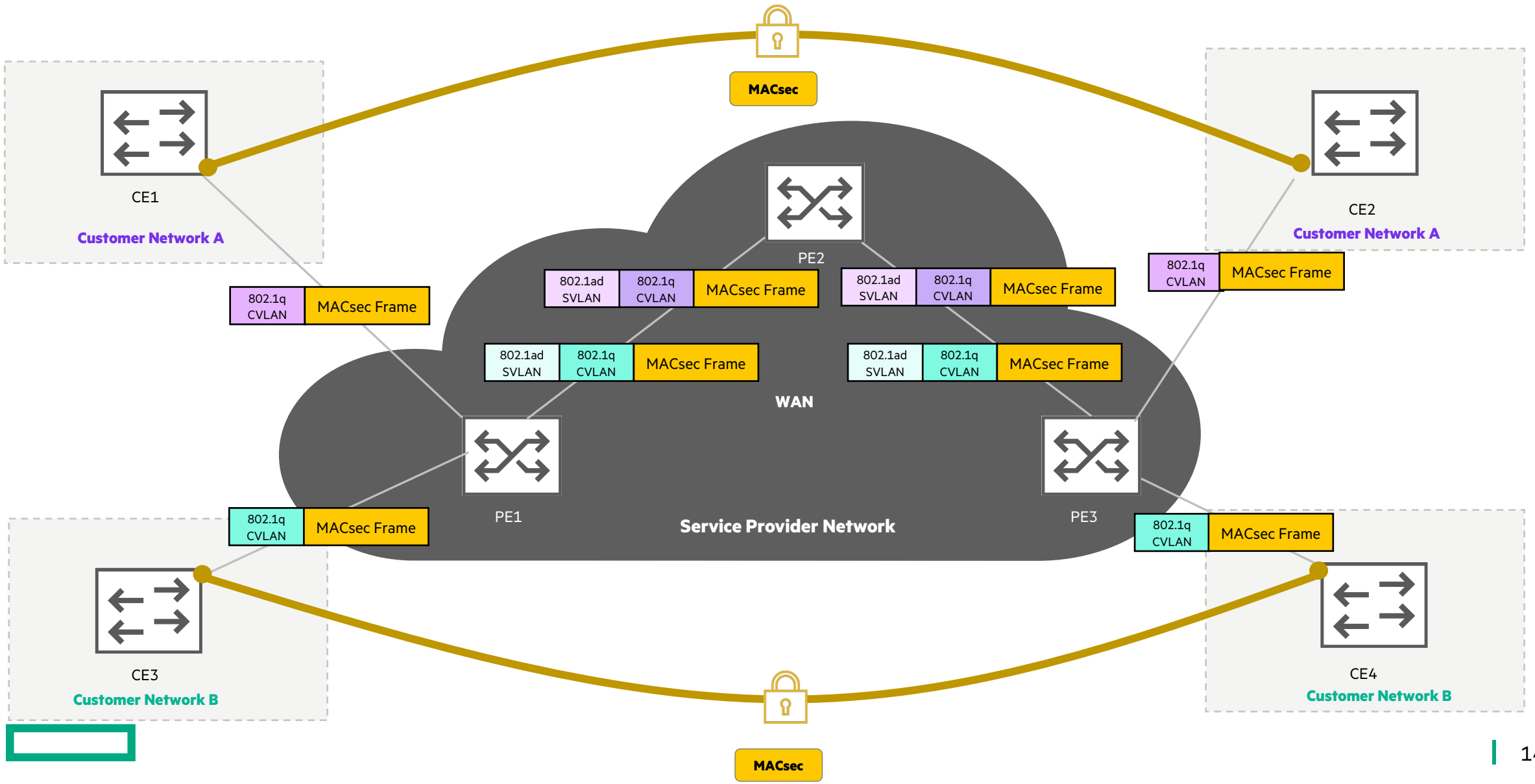
- **CFR**
  - Arrangement of the general and permanent regulations promoted by the executive departments and agencies of the federal government of the United States.
  - It is divided into 50 titles that represent broad areas subject to Federal regulation.

▼ **Title 15** Commerce and Foreign Trade
▼ **Subtitle B** Regulations Relating to Commerce and Foreign Trade
▼ **Chapter VII** Bureau of Industry and Security, Department of Commerce
▼ **Part 740** License Exceptions
§ 740.17 Encryption commodities, software, and technology (ENC).

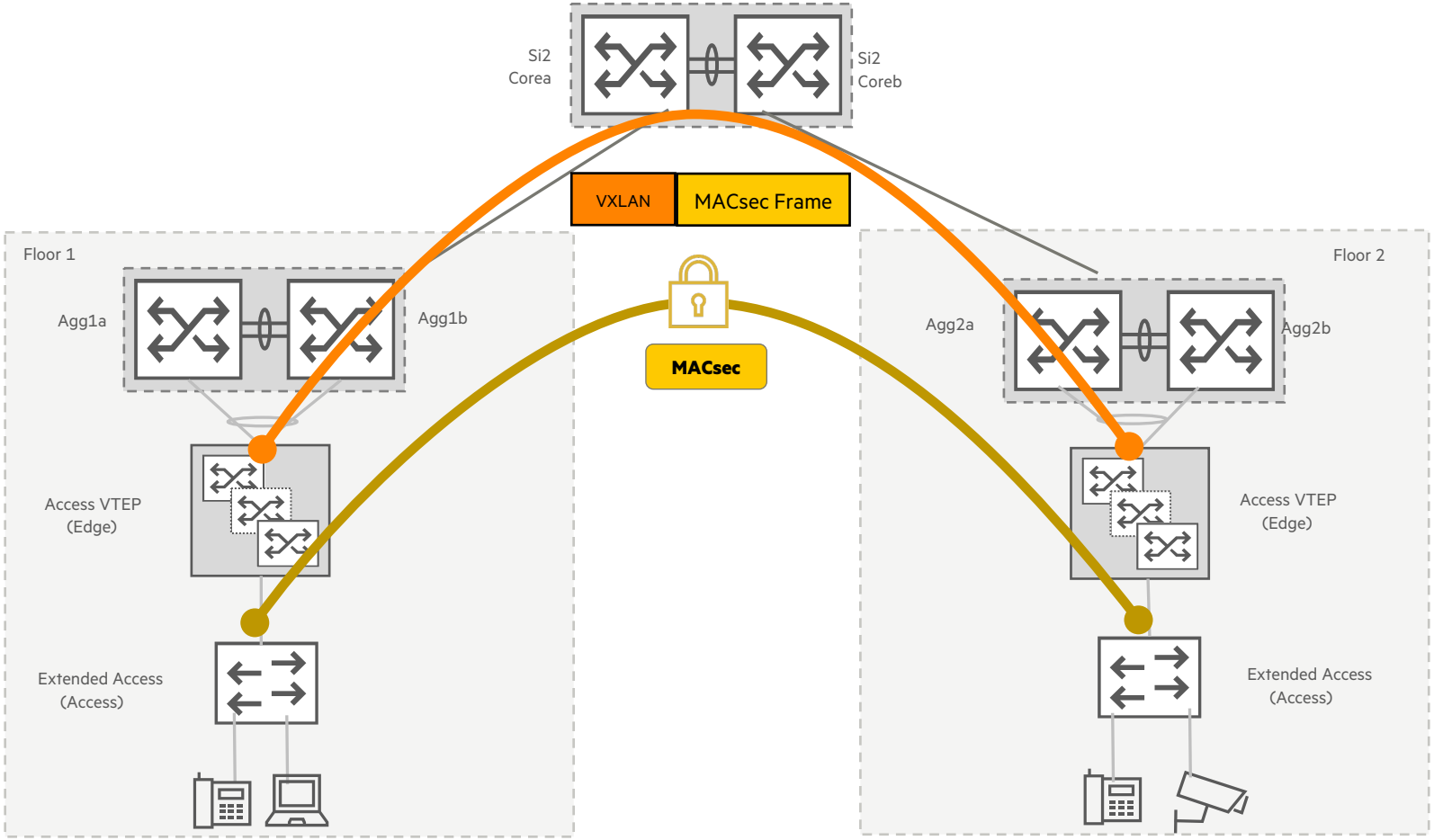
  - License Exception ENC authorizes export, reexport, and transfer (in-country) of systems, equipment, commodities, and components that have encryption features enabled by default.
  - License Exception ENC does not authorize **distributors/partners** to export or reexport to, transfer (in-country) in, or provision of any service in any country **not** listed in **Country Groups** **without Feature Subscription**.

Use Cases

QinQ – Service Provider Bridging



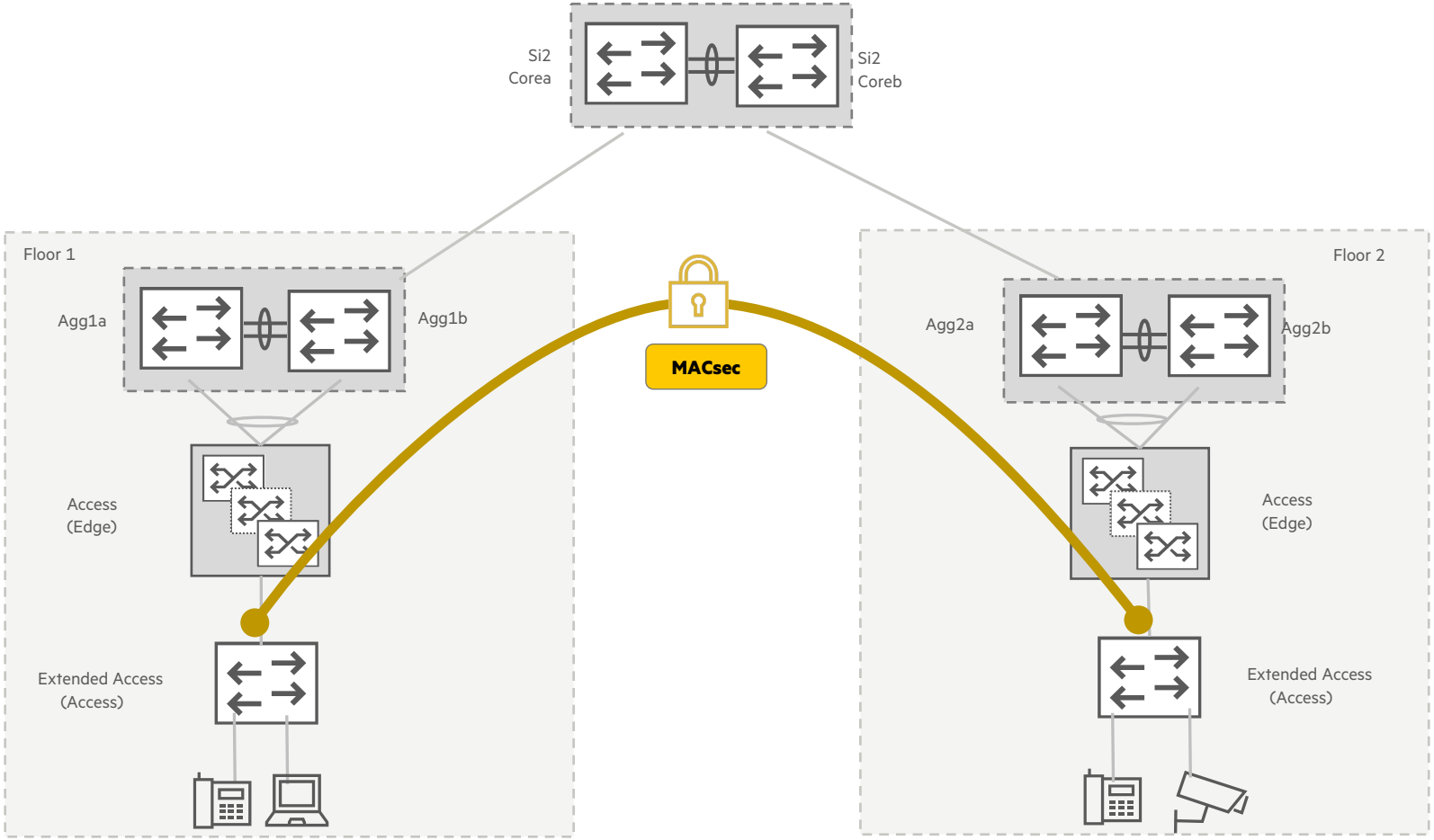
Interconnect using VXLAN



- Two Floors are interconnected over VXLAN
- Access VSF switches will act as VTEPs
- WAN MACsec tunnel is established between the Extended access edge switches of different floors.
- Scalable*
  - Campus to DC Interconnect
  - DC to DC Interconnect

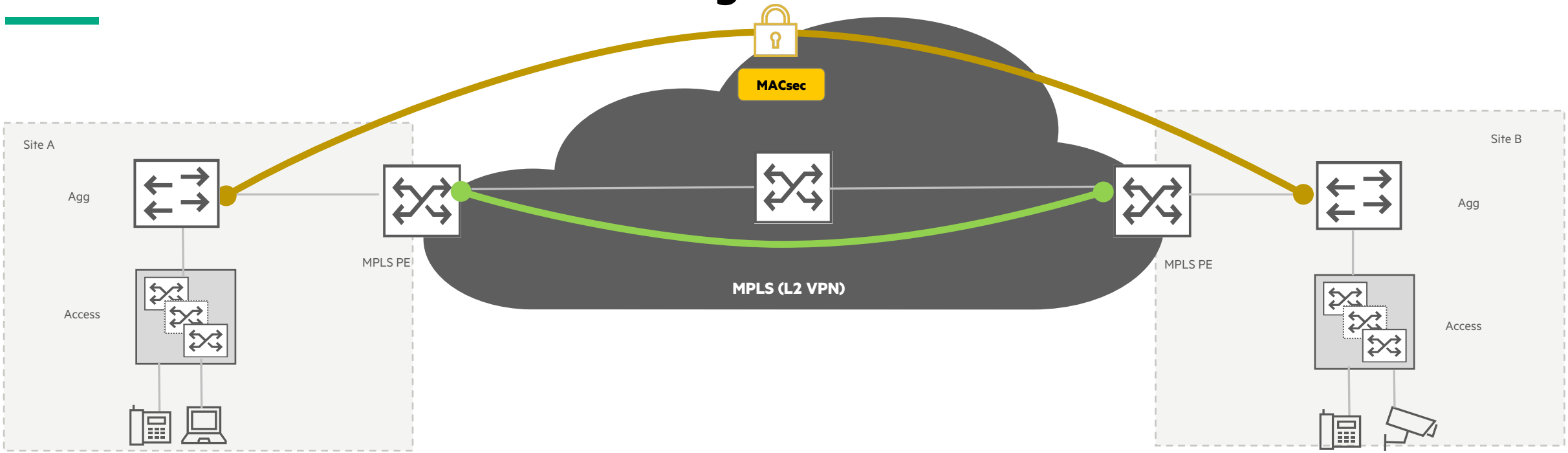
* Validation planned in Future Software Release

Interconnect – L2 Only



- Some of the legacy deployments are purely L2.
- Two Floors are interconnected over L2 Only interfaces.
- Access VSF switches will be connected to extended access standalone switches.
- WAN MACsec tunnel is established between the Extended access edge switches of different floors.

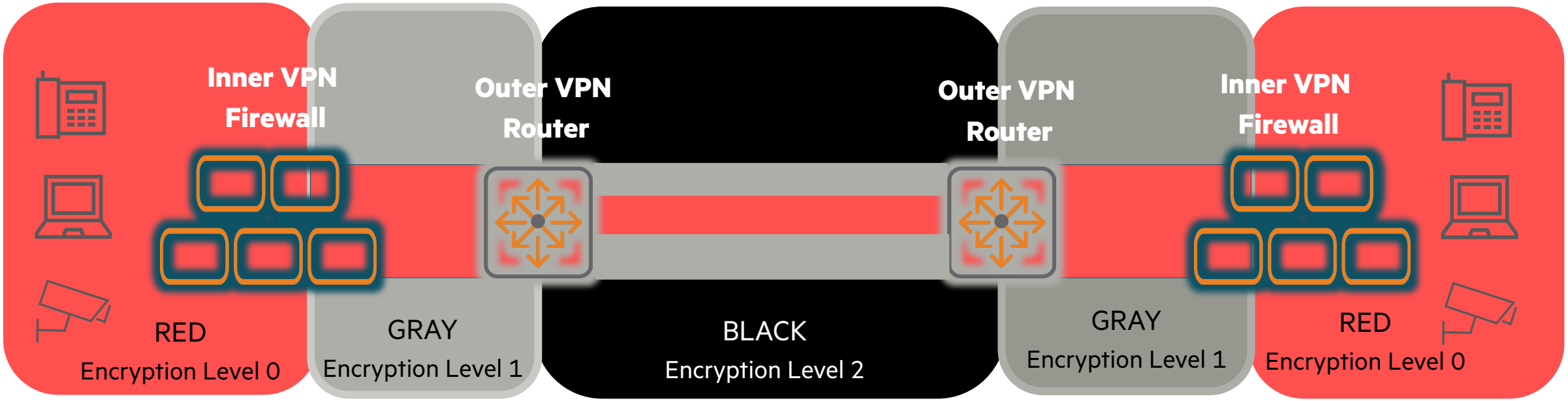
Pseudo Wire – Site Interconnect using MPLS



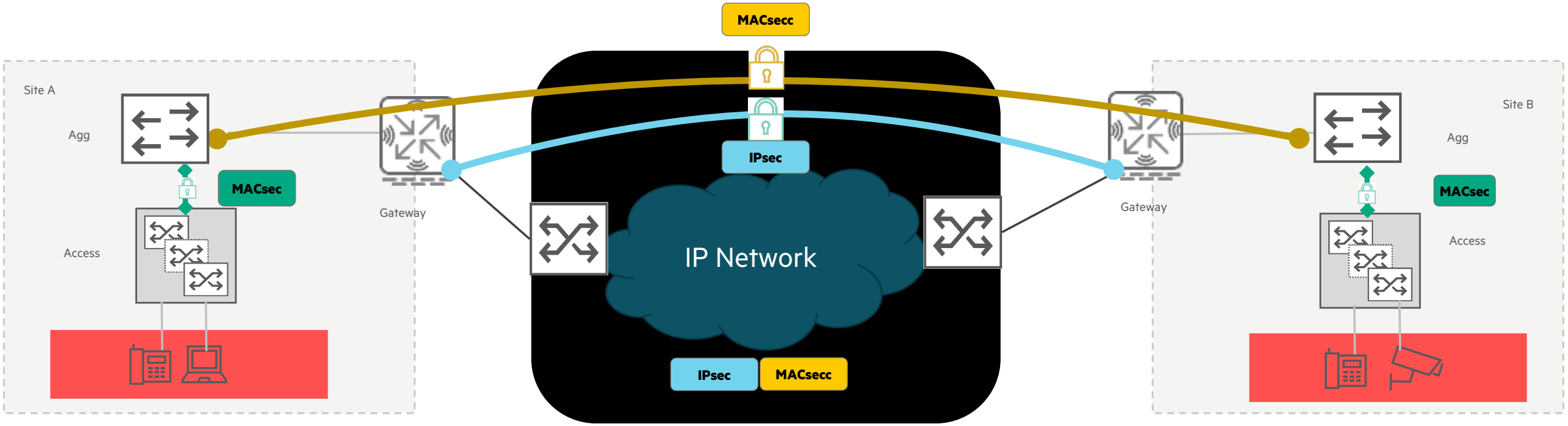
- Two different sites Site A and Site B are connected using MPLS.
- WAN MACsec tunnel is established between MACsec tunnel End-Points over MPLS cloud.
- MPLS PE should be 3rd party device which supports L2VPN.

CSfC – Multisite Connectivity Package

- Commercial Solutions for Classified (CSfC) is an important part of National Security Agency(NSA)'s commercial cybersecurity strategy to quickly deliver secure cybersecurity solutions that leverage commercial technologies and products.
- NSA program using **two layers of encryption** on Commercial off the Shelf (COTS) products



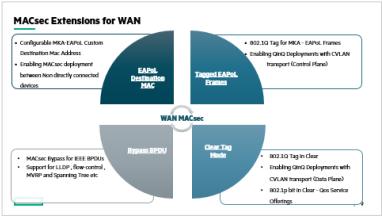
CSfC Dual Encryption – MACsec over IPsec



- Two different sites Site A and Site B are protected using IPSec.
- LAN MACsec channels are established between Access and Aggregation
- WAN MACsec tunnel is established between MACsec tunnel End-Points over IPSec.
- Gateways are used to established IPsec tunnels and achieve L2 extension between the sites.
- Gateways would need to have an L2 GRE tunnel across the IPsec.

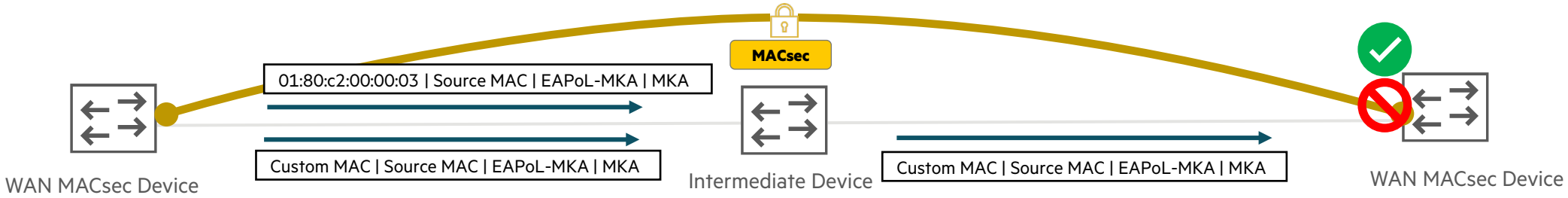
Details

Configurable EAPoL destination MAC



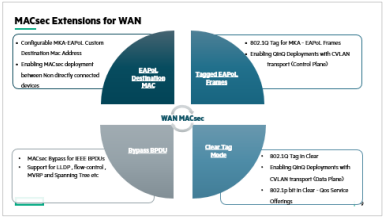
- MKA uses EAPoL as the transport protocol to transmit MKA messages
- LAN MACsec MKA Packet Format -

- The default EAPoL destination MAC is a BPDU MAC and is always **consumed by the directly connected L2 next-hop device**.



- To extend MKA beyond a directly connected device, MKA Policy is being extended with a new configuration option to configure the destination MAC to be used for EAPoL.
- Adding the capability for the user to configure a different MAC (ex: unicast/broadcast/multicast) will enable MKA frames to cross the next hop L2 boundary.
- WAN MACsec MKA Packet Format –

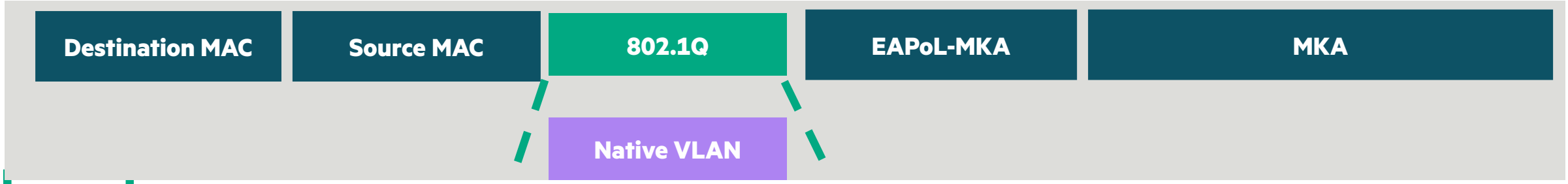
802.1q Tagged EAPoL-MKA



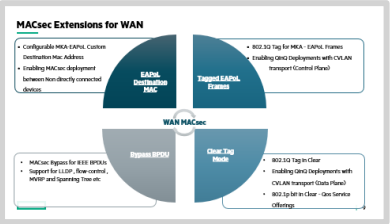
- By default, MKA Control packets are untagged –

- Support for Single 802.1Q tag for MKA Packets to traverse over WAN links , especially for QinQ Transport –

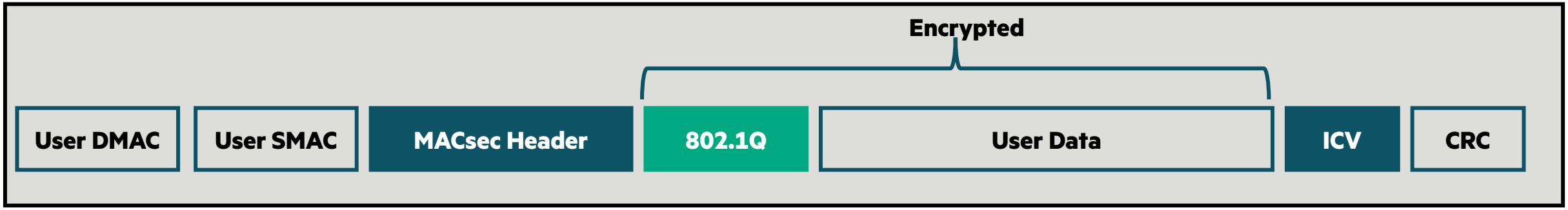
- Configurable option in MKA policy to force EAPoL frames to be tagged with the VLAN used as native VLAN on the port



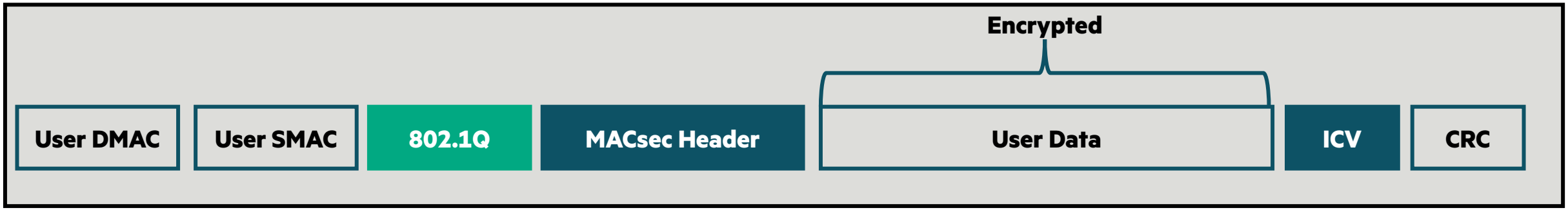
802.1q Tag in Clear



- LAN MACsec encrypts the 802.1Q header along with the data –

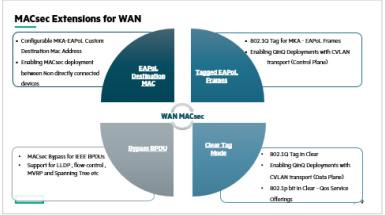


- The clear-tag mode enables 802.1Q tag of a MACsec protected frame to be sent in clear text and placed before the MACsec header.



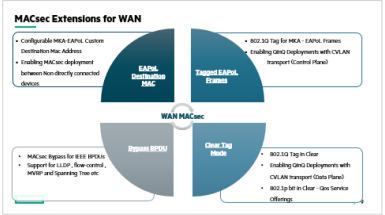
- Enables MACsec tunnel to be established between 2 MACsec endpoints over a non MACsec Layer 2 network

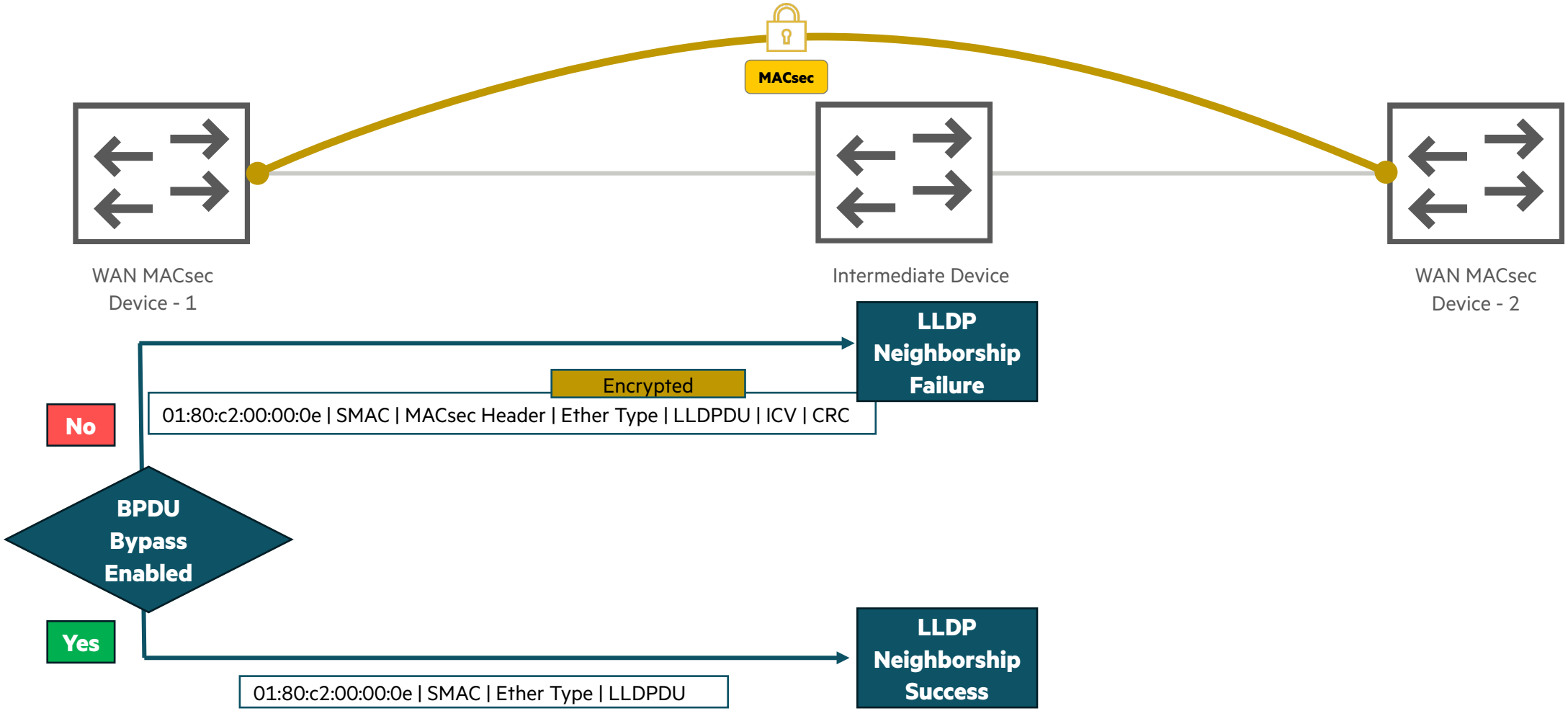
MACsec bypass for BPDUs



- When MACsec is enabled on an interface, by default all BPDU frames except EAPoL are protected by MACsec.
- In case of the interface configured to start a MACsec tunnel, the BPDU frames that are essential to the next hop device are sent with MACsec protection.
- Results in below protocols to fail on the local link since the next hop device would fail to read the MACsec protected frames.
  - LLDP
  - Spanning Tree
  - Flow Control
  - MVRP
- To enable these protocols to operate on such links, the BPDU bypass must be enabled in the MACsec policy
- The BPDU packets with destination MAC as **01:80:c2:00:00:0*** will be transmitted without MACsec protection

MACsec Bypass for LLDP Negotiation





Configuration

MACsec Policy

- List of WAN MACsec CLIs introduced in MACsec Policy -

```
switch(config)# macsec policy <policy-name>
switch(config-macsec-policy)#
  bypass                    Configure MACsec bypass.
  cipher-suite              Configure the cipher-suite to use in the MACsec policy
  clear-tag-mode            Configure the clear-tag mode in the MACsec policy.
                            (Default: none)
  confidentiality           Enable confidentiality in this MACsec policy
  data-delay-protection     Enable data delay protection. (Default: Disabled)
  end                       End current mode and change to enable mode.
  exit                      Exit current mode and change to previous mode
  include-sci-tag           Include Secure Channel Identifier (SCI) tag
                            information in the Security TAG (SecTAG) field
  list                      Print command list
  no                        Negate a command or set its defaults
  replay-protection         Enable replay protection in this MACsec policy
  secure-mode               Configure the MACsec protection behavior on the
                            interface (Default: "must-secure")
  show                      Show running system information
```

MACsec Policy Contd..

- To enable bypassing of IEEE BPDUs -

```
switch(config)# macsec policy <policy-name>
switch(config-macsec-policy)# bypass ieee-bpdu
switch(config-macsec-policy)# exit
```

- To enable clear tag mode for dot1q -

```
switch(config)# macsec policy <policy-name>
switch(config-macsec-policy)#  clear-tag-mode
  dot1q  Encode a single 802.1q tag in clear before SecTAG
  none   The SecTAG directly follows the Ethernet addresses
```

```
switch(config)# macsec policy <policy-name>
switch(config-macsec-policy)#  clear-tag-mode dot1q
switch(config-macsec-policy)# exit
```

MKA Policy

- List of WAN MACsec CLIs introduced in MKA Policy -

```
switch(config)# mka policy <policy-name>
switch(config-mka-policy)#
  eapol-destination-mac  Configure the destination MAC in EAPoL frames for MKA.
  eapol-dot1q-tagged     Enable 802.1q tag in EAPoL frames for MKA. (Default:
                         Disabled)
  end                    End current mode and change to enable mode.
  exit                   Exit current mode and change to previous mode
  key-server-priority    Configure the MKA key server priority
  list                   Print command list
  no                     Negate a command or set its defaults
  pre-shared-key         Configure the pre-shared key for this MKA policy
  show                   Show running system information
  transmit-interval      Configure the MKA transmit interval
```

MKA Policy Contd..

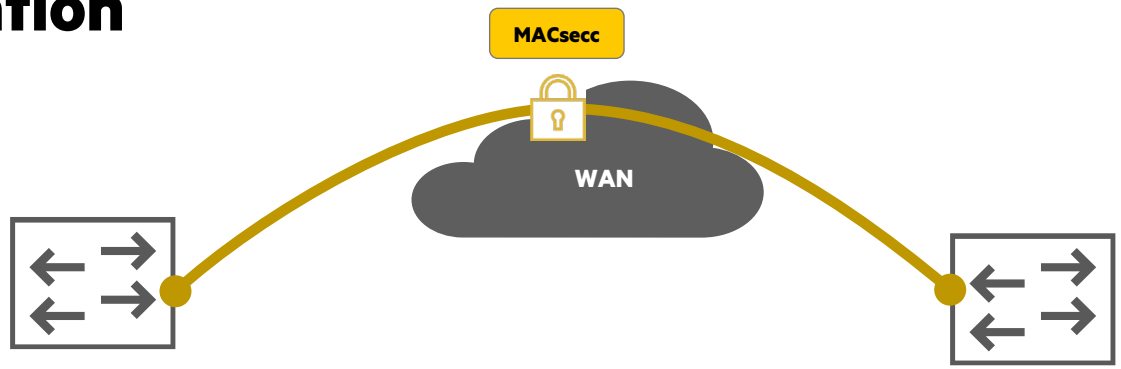
- To configure EAPoL-Destination Mac Address –

```
switch(config)# mka policy <policy-name>
switch(config-mka-policy)# eapol-destination-mac
  MAC-ADDR  The EAPoL destination MAC address (Default: 01:80:c2:00:00:03)
switch(config-mka-policy)# eapol-destination-mac <MAC-ADDR>
switch(config-mka-policy)#exit
```

- To enable 802.1Q tag for MKA EAPoL Frames -

```
switch(config)# mka policy <policy-name>
switch(config-mka-policy)#eapol-dot1q-tagged
switch(config-mka-policy)#exit
```

Sample Configuration




```
vlan 1,10,20
macsec policy <macsec-policy-name>
      bypass ieee-bpdu
      clear-tag-mode dot1q
mka policy <mka-policy-name>
    pre-shared-key ckn <ckn> cak plaintext <cak>
    eapol-destination-mac <>
    eapol-dot1q-tagged
interface 1/1/1
    no shutdown
    no routing
    vlan trunk native 10 tag
    vlan trunk allowed all
    apply mka policy <mka-policy-name>
    apply macsec policy <macsec-policy-name>
```

```
vlan 1,10,20
macsec policy <macsec-policy-name>
      bypass ieee-bpdu
      clear-tag-mode dot1q
mka policy <mka-policy-name>
    pre-shared-key ckn <ckn> cak plaintext <cak>
    eapol-destination-mac <>
    eapol-dot1q-tagged
interface 1/1/1
    no shutdown
    no routing
    vlan trunk native 10 tag
    vlan trunk allowed all
    apply mka policy <mka-policy-name>
    apply macsec policy <macsec-policy-name>
```

Configuration – REST API

- To configure **MKA Policy** via REST API –

POST /system/mka_policies

Parameters Cancel

No parameters

Request body application/json

```
{
  "cak": "abc123456",
  "ckn": "abc123",
  "eapol_destination_mac": "01:01:01:01:01:01",
  "eapol_dot1q_tagged": true,
  "key_server_priority": 0,
  "keychain": null,
  "mode": "psk",
  "name": "mka2",
  "origin": "static",
  "transmit_interval": 2
}
```

Execute Clear

Configuration – REST API Contd..

- To configure **MACsec** Policy via REST API –

POST /system/macsec_policies

Parameters Cancel

No parameters

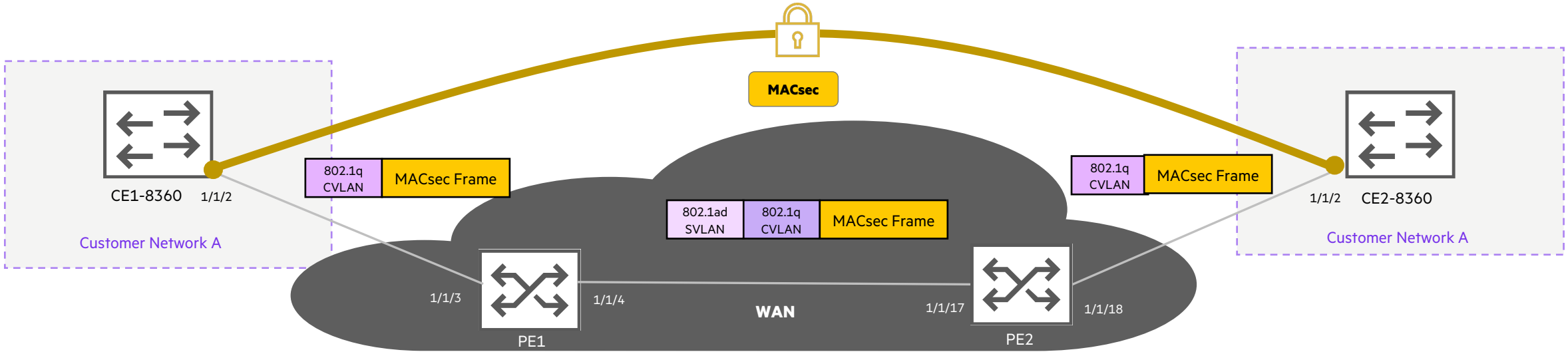
Request body application/json


```
{
  "bypass": {
    "ieee_bpdu_enabled": true
  },
  "cipher_suites": {
    "gcm_aes_128_enabled": true,
    "gcm_aes_256_enabled": true,
    "gcm_aes_xpn_128_enabled": true,
    "gcm_aes_xpn_256_enabled": true
  },
  "clear_tag_mode": "none",
  "confidentiality_disable": true,
  "confidentiality_offset": "byte_0",
  "data_delay_protection_enable": true,
  "include_sci_disable": true,
  "name": "policy1",
  "origin": "dynamic",
  "replay_protect_disable": true,
  "replay_window": 0,
  "secure_mode": "should-secure"
```


Execute

Demo

QinQ – Service Provider Bridging Demo




```
vlan 1,70,80
macsec policy macsec1
    bypass ieee-bpdu
    clear-tag-mode dot1q
mka policy mka1
    pre-shared-key ckn abcd123 cak
ciphertext AQBapcJdUGQF7tXY
eapol-destination-mac
00:00:00:00:00:01
    eapol-dot1q-tagged
interface 1/1/2
    no shutdown
    no routing
    vlan trunk native 70 tag
    vlan trunk allowed all
    apply mka policy mka1
    apply macsec policy macsec1
interface vlan 70
    ip address 70.1.1.1/24
interface vlan 80
    ip address 80.1.1.1/24
```

```
vlan 100
    svlan
interface 1/1/3
    no shutdown
    no routing
    vlan access 100
interface 1/1/4
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 100
```

```
vlan 100
    svlan
interface 1/1/17
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 100
interface 1/1/18
    no shutdown
    no routing
    vlan access 100
```

```
vlan 1,70,80
macsec policy macsec1
    bypass ieee-bpdu
    clear-tag-mode dot1q
mka policy mka1
    pre-shared-key ckn abcd123 cak
ciphertext AQBapcJdUGQF7tXY
eapol-destination-mac
00:00:00:00:00:02
    eapol-dot1q-tagged
interface 1/1/2
    no shutdown
    no routing
    vlan trunk native 70 tag
    vlan trunk allowed all
    apply mka policy mka1
    apply macsec policy macsec1
interface vlan 70
    ip address 70.1.1.2/24
interface vlan 80
    ip address 80.1.1.2/24
```

Packet Capture from Provider Edge

- **MKA Packet –**

No.	Time	Source	Destination	Protocol	Length	Info
2	20:38:12.369876	ArubaaHe_1b:7c:b4	00:00:00_00:00:01	EAPOL-…	138	Key Server, Live Peer List, MACsec SAK Use

```
> Frame 2: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface eth1, id 0
> Ethernet II, Src: ArubaaHe_1b:7c:b4 (18:7a:3b:1b:7c:b4), Dst: 00:00:00_00:00:01 (00:00:00:00:00:01)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 70
> 802.1X Authentication
> MACsec Key Agreement
```

- **MACsec Packet -**

No.	Time	Source	Destination	Protocol	Length	Info
210	20:39:22.037924	ArubaaHe_1b:7c:80	ArubaaHe_f7:de:40	MACSEC	178	MACsec frame

```
> Frame 209: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface eth1, id 0
> Ethernet II, Src: ArubaaHe_1b:7c:80 (18:7a:3b:1b:7c:80), Dst: ArubaaHe_f7:de:40 (ec:02:73:f7:de:40)
> IEEE 802.1ad, ID: 100
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 80
> 802.1AE Security tag
> Data (130 bytes)
```

Thank you

© 2023 Hewlett Packard Enterprise Development LP

License Exception ENC Favourable Treatment Countries

Supplement No. 3 to Part 740 License Exception ENC Favourable Treatment Countries

Code of Federal Regulations (CFR)

- CFR
- Arrangement of the general and permanent regulations promoted by the executive departments and agencies of the federal government of the United States.
- It is divided into 50 titles that represent broad areas subject to Federal regulation.

Title 15 Commerce and Foreign Trade
Subtitle B Regulations Relating to Commerce and Foreign Trade
Chapter VII Bureau of Industry and Security, Department of Commerce
Part 740 License Exceptions
§ 740.17 Encryption commodities, software, and technology (ENC).

- License Exception ENC authorizes export, reexport, and transfer (in-country) of systems, equipment, commodities, and components that have encryption features enabled by default.
- License Exception ENC does not authorize distributors/partners to export or reexport to, transfer (in-country) to, or provision of any service in any country not listed in Country Groups without Feature Subscription.

§ 32

- Australia.
- Austria.
- Belgium.
- Bulgaria
- Canada NLR
- Croatia
- Cyprus.
- Czech Republic.
- Denmark.
- Estonia.
- Finland.
- France.
- Hungary
- Germany
- Greece.
- Iceland
- Ireland.
- Italy.
- Japan.
- Latvia.
- Lithuania.
- Luxembourg.
- Malta.
- Netherlands.
- New Zealand.
- Norway.
- Poland.
- Portugal.
- Romania
- Slovakia.
- Slovenia.
- Spain.
- Sweden.
- Switzerland.
- Turkey
- United Kingdom.
- USA