Oct 2020

MACsec on 8360 Switch

SPEAKERS:

- Steve Baker
- B. Abhay

aruba
a Hewlett Packard Enterprise company

Agenda: MACsec

1 Overview

2 Use Cases

3 Configuration

4 Best Practices

5 Troubleshooting

6 Resources

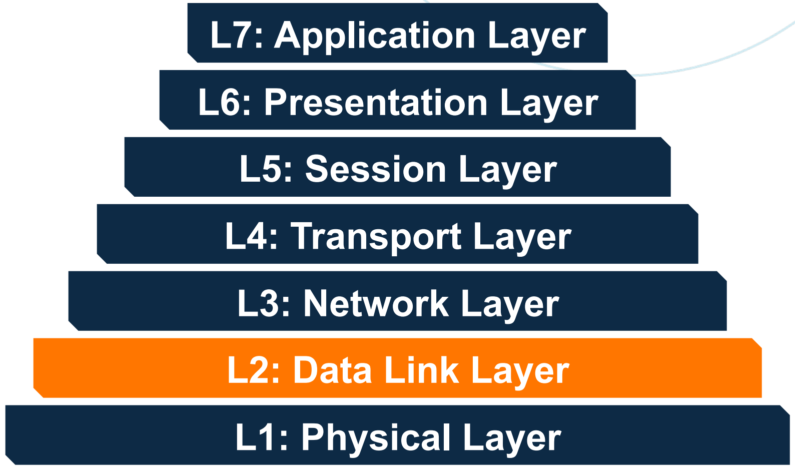
7 Demo

Overview

a Hewlett Packard
Enterprise company

Overview MACsec

- Media Access Control security (MACsec) provides Layer 2 hop-by-hop encryption on point-to-point Ethernet links.
  - MACsec is intended for wired Local Area Networks; wireless networks use different set of protocols (like WEP,WPA2).
- Enables a bi-directional secure link after an exchange and verification of security keys between two connected devices.
  - Secures switch to switch infrastructure using the (MACsec Key Agreement) protocol and Static CAK (Connectivity Association Key).
  - A combination of data integrity checks and encryption is used to safeguard the transmitted data.
- Provides Layer 2 security protecting network communications against a range of attacks including - denial of service, intrusion, man-in-the-middle and eavesdropping
  - These attacks exploit Layer 2 vulnerabilities and often cannot be detected



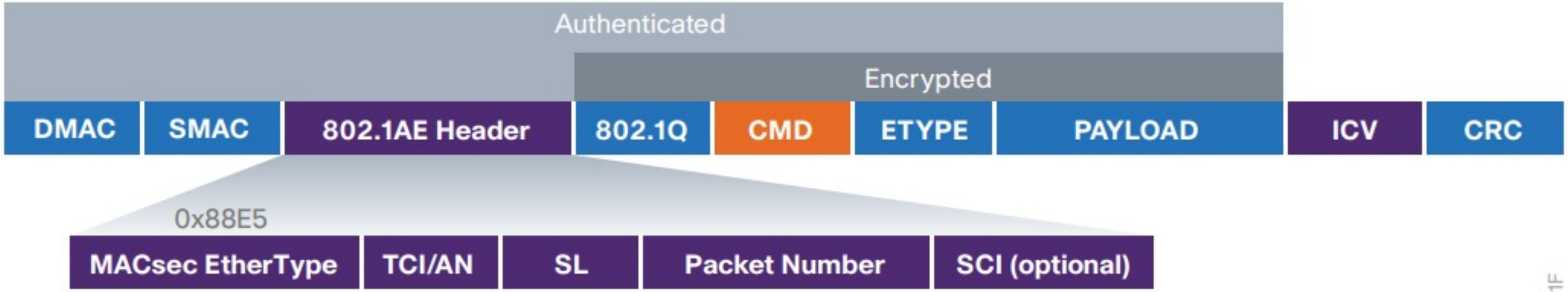
L7: Application Layer
L6: Presentation Layer
L5: Session Layer
L4: Transport Layer
L3: Network Layer
L2: Data Link Layer
L1: Physical Layer

L2 is where communication begins, security here establishes the foundation for security for the entire network stack

- **Connectionless data integrity** – Unauthorized changes to data cannot be made without being detected. Each MAC frame carries a separate integrity verification code
- **Data origin authenticity** – A received MAC frame is guaranteed to have been sent by the authenticated device.
- **Confidentiality** – The data payload of each MAC frame is encrypted to prevent it from being eavesdropped by unauthorized parties.
- **Replay protection** – MAC frames copied from the network by an attacker cannot be resent into the network without being detected.
- **Bounded receive delay** – MAC frames cannot be intercepted by a man-in-the-middle attack and delayed by more than a few

MACsec Details

- MACsec appends a header and tail to all Ethernet frames, and encrypts data payload within the frame. Receiving device checks header and tail for integrity.
  - If check fails, traffic is dropped.
  - Successful check, the frame is decrypted.
- MACsec frame format includes an additional 32-byte MACsec header, which includes a well-known EtherType field (0x88E5), while allowing the Ethernet source/destination MAC addresses to be left in the clear for Ethernet frame forwarding
- MACsec encrypts all fields behind the source/destination MAC addresses, so unless the ability to offset the encrypted field exists, fields such as MPLS labels and 802.1Q tags are encrypted and not able to be used when the Ethernet frame traverses the underlying transport between encrypted stations.



MACsec Details (cont.)

- MACsec secures switch to switch infrastructure using the MACsec Key Agreement (MKA) protocol and Static Connectivity Association Key (CAK).
- The pre-shared key (PSK) includes a connectivity association name (CKN) and a connectivity association key (CAK).
  - The CKN and CAK are configured by the administrator and must match on both ends of the link to operate
  - Connectivity Association & Pre-shared Key:
    - A Connectivity Association (CA) is a logical association between two or more MACsec participating entities.
    - Each CA has a root key known as the CA-Key(CAK).
    - Uses EAPoL as a transport protocol to transmit MKA messages.
    - During negotiation process, port with higher MKA key server priority becomes key server. The Key server generates and distributes an SAK (Secure Authentication Key).
- By default CX will use the most secure cipher suite “gcm-aes-xpn-256” for establishing MACsec secure link. CX supports the following cipher suites:

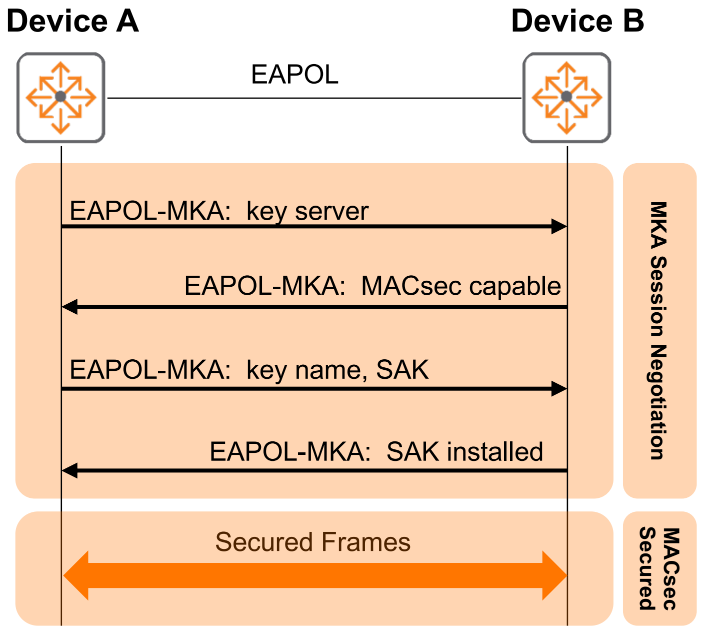
– gcm-aes-128	Use AES-128 encryption with Galois/Counter mode
– gcm-aes-256	Use AES-256 encryption with Galois/Counter mode
– gcm-aes-xpn-128	Use AES-128 encryption with Galois/Counter mode and extended packet numbering
– gcm-aes-xpn-256	Use AES-256 encryption with Galois/Counter mode and extended packet numbering

- Key-server priority on CX is ‘0’ by default so unless modified it should become the key-server

MACsec Details (cont.)

The following shows device to device MACsec process:

1. The devices use configured pre-shared key as the CAK to exchange EAPOL-MKA packets.
2. They exchange MACsec capability and required parameters for session establishment. Parameters include MKA key server priority and MACsec desire.
3. During negotiation process, port with higher MKA key server priority becomes key server. Key server generates and distributes an SAK.
4. Devices use the SAK to encrypt packets
5. When device receives logoff request from peer, it immediately deletes the associated secure session.

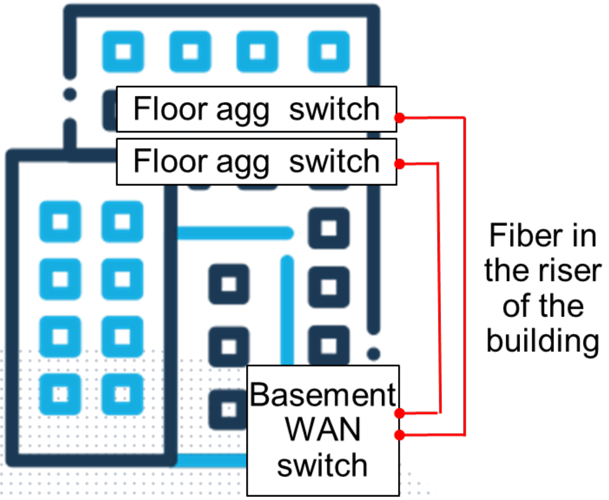


Use Cases

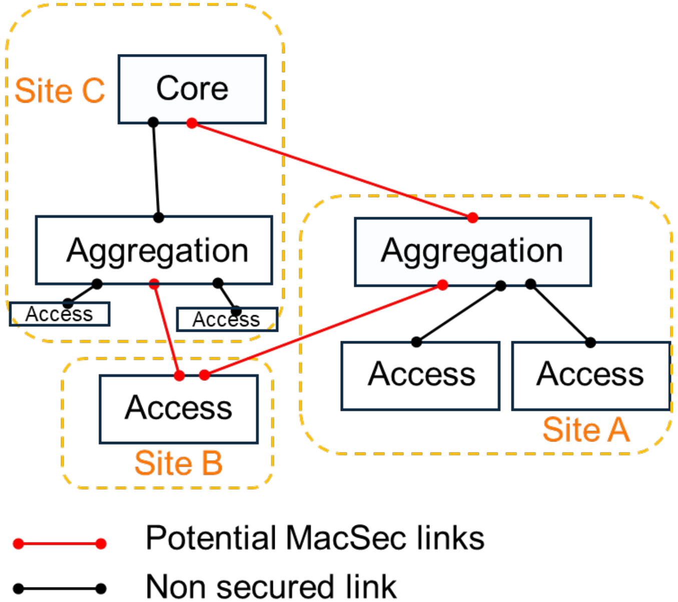
aruba
a Hewlett Packard Enterprise company

MACsec Targeted Use Cases

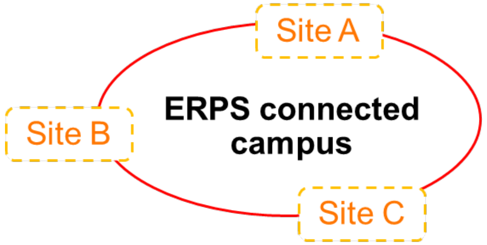
Point-to-Point links between directly connected MACsec capable devices.

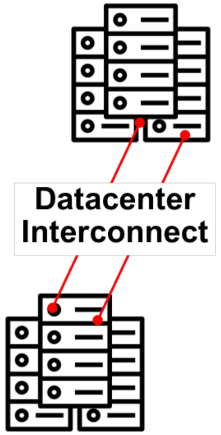


Customer leasing on several floors of a building (financial vertical)



Distributed campus (Low density)





Configuration

MACsec Policy Commands

Creating a MACsec Policy

- A MACsec policy can be associated with one or more logical ports on the system to turn on the MACsec functionality on the port.
- The no form of the command deletes the MACsec policy. A policy cannot be deleted when it is still attached to one or more ports. All references to the policy must be removed before deleting the policy.

- **Create MACsec policy**
  - `macsec policy <POLICY-NAME>`

Parameter	Status	Description
`macsec`	Required	MAC Security (MACsec) protocol
`policy`	Required	Configure a MACsec policy
`POLICY-NAME`	Variable - Required	A MACsec policy name up to 32 characters long Alphanumeric, '.', '-' and '_' characters only

Example	`switch(config)# macsec policy MACsecP1`
	`switch(config-macsec-policy)#`	

Enabling Confidentiality

- When confidentiality is enabled, the Ethernet frame following the MACsec header is encrypted starting at the offset as dictated in the configuration.
- Confidentiality is enabled by default in a policy with an offset of 0.
- The no form of the command disables confidentiality in the policy and resets the offset to its default value of 0.
- **Enable Confidentiality**
  - `confidentiality [offset {0|30|50}]`

Parameter	Status	Description
`confidentiality`	Required	Enable confidentiality in this MACsec policy
`offset`	Optional	Configure the confidentiality-offset to use in the MACsec policy (Default: 0)
`0`		Encrypt the entire packet
`30`		Encrypt after byte 30 of the packet
`50`		Encrypt after byte 50 of the packet

Example

```
switch(config)# macsec policy MACsecP1 confidentiality offset 30
OR
switch(config)# macsec policy MACsecP1
switch(config-macsec-policy)# confidentiality offset 30
```

Enable Secure Channel Identifier Tag

- The Secure Channel Identifier (SCI) tag in the Security TAG (SecTAG) field of the MACsec header is comprised of a globally unique MAC Address and a port identifier that is unique within the system.
- An explicitly encoded SCI field in the SecTAG is not required on point-to-point links if the transmitting link has only one MACsec peer.
- The no form of the command disables inclusion of the SCI tag in the secTAG field.
- Default: enabled
- NOTE: Asymmetric configuration of include-sci-tag between two ends of a MACsec channel is not supported. With an asymmetric configuration, MACsec frames would be dropped on the switch.
- **Enable SCI Tag**
  - `include-sci-tag`

Parameter	Status	Description
`include-sci-tag`	Required	Include Secure Channel Identifier (SCI) tag information in the Security TAG (SecTAG) field

Example	`switch(config)# macsec policy MACsecP1 include-sci-tag`
	OR
	`switch(config)# macsec policy MACsecP1`
	`switch(config-macsec-policy)# include-sci-tag`	

Enable Replay Protection

- When replay protection is turned on, packets are expected to arrive within the replay protection window.
- Packets arriving outside the window are dropped by the interface.
- The replay protection window of zero enforces strict order of reception.
- The no form of the command disables replay protection in the MACsec policy and resets the window-size to its default value of 0
- Default: enabled
- **Enable Replay Protection**
  - `replay-protection window-size <0-4294967295>`

Parameter	Status	Description
`replay-protection`	Required	Enable replay protection in this MACsec policy
`window-size`	Optional	Configure the replay protection window size (Default: 0)
`WINDOW-SIZE`	Variable - Optional	The replay protection window size between 0-4294967295

Example	`macsec policy MACsecP1 replay-protection window-size 100`
	OR
	`switch(config)# macsec policy MACsecP1`
	`switch(config-macsec-policy)# replay-protection window-size 100`	

Configure the Cipher-Suite

- When one or more cipher-suites are configured, the switch will use the most secure cipher-suite in the list to generate the SAK if it is the key-server.
- If no cipher-suites are configured, all the cipher-suites supported on the interface are considered for MACsec encryption.
- Default: All the cipher-suites supported on the interface are considered for MACsec encryption
- **Enable Cipher-Suite**
  - `cipher-suite {gcm-aes-128|gcm-aes-256|gcm-aes-xpn-128|gcm-aes-xpn-256} [{gcm-aes-128|gcm-aes-256|gcm-aes-xpn-128|gcm-aes-xpn-256}]`

Parameter	Status	Description
`cipher-suite`	Required	Configure the cipher-suite to use in the MACsec policy
`gcm-aes-128`	Optional	Use AES-128 encryption with Galois/Counter mode
`gcm-aes-256`	Optional	Use AES-256 encryption with Galois/Counter mode
`gcm-aes-xpn-128`		Use AES-128 encryption with Galois/Counter mode and extended packet numbering
`gcm-aes-xpn-256`		Use AES-256 encryption with Galois/Counter mode and extended packet numbering

Example	`switch(config)# macsec policy MACsecP1 cipher-suite gcm-aes-256 gcm-aes-xpn-256`
	OR
	`switch(config)# macsec policy MACsecP1`
	`switch(config-macsec-policy)# cipher-suite gcm-aes-256 gcm-aes-xpn-256`	

Configuration

MKA Policy Commands

Create a MKA Policy

- A MKA policy can be associated with one or more logical ports on the system to turn on the MKA functionality on the port.
- The no form of the command deletes the MKA policy. A policy cannot be deleted when it is still attached to one or more ports. All references to the policy must be removed before deleting the policy.
- **Create MKA Policy**
  - `mka policy <`*`POLICY-NAME`*`>`

Parameter	Status	Description
`mka`	Required	Configure the MACsec Key Agreement (MKA) protocol
`Policy`	Optional	Configure a MKA policy
`<POLICY-NAME>`	Optional	A MKA policy name

Example	`switch(config)# mka policy MKA1`
	`switch(config-mka-policy)#`	

Configure an MKA Pre-Shared-Key

- The Pre-Shared Key (PSK) to use for an MKA policy includes the Connectivity Association Key Name (CKN) and Connectivity Association Key (CAK).

- The no form of the command deletes the MKA policy. A policy cannot be deleted when it is still attached to one or more ports. All references to the policy must be removed before deleting the policy.

- **Create MKA Pre-Shared Key**
  - `pre-shared-key ckn <CKN> cak {plaintext [<PLAINTEXT-CAK>] | ciphertext <ENCRYPTED-CAK>}`

Parameter	Status	Description
`pre-shared-key`	Required	Configure the pre-shared key for this MKA policy
`ckn`	Required	Configure the CA Key Name (CKN) of this MKA policy
`<CKN>`	Variable - Required	The CKN as a hexadecimal string of up to 64 characters
`cak`	Required	Configure the CA Key (CAK) of this MKA policy

`plaintext`
`or`
`ciphertext`
	Required	Configure the CAK in plaintext
		Configure the CAK in ciphertext

`<PLAINTEXT-CAK>`	Variable	A hexadecimal string of up to 64 characters in plaintext
`<ENCRYPTED-CAK>`	Variable	The encrypted CAK

Example

```
switch(config)# mka policy MKA1
switch(config-mka-policy)# pre-shared-key ckn abc123 cak plaintext
Enter CAK: abc123
Confirm CAK: abc123
OR
switch(config)# mka policy MKA1
switch(config-mka-policy)# pre-shared-key ckn abc123 cak plaintext 123abc
```

Configure Key Server Priority

- A lower value indicates higher priority. A value of 255 indicates that this participant does not want to become the key server.
- The no form of the command resets the key server priority to the default value.
- Default: 0.
- **Create MKA Key Server Priority**
  - `key-server-priority <PRIORITY>`

Parameter	Status	Description
`key-server-priority`	Required	Configure the pre-shared key for this MKA policy
`<PRIORITY>`	Variable – Required	The MKA key server priority. <0-255>

Example	`switch(config)# mka policy MKA1 key-server-priority 5`
	OR
	`switch(config)# mka policy MKA1`
	`switch(config-mka-policy)# key-server-priority 5`
	`Reset the MKA key server priority.`	

Configure MKA Transmit Interval

- Configure the transmit interval (in seconds) between MKA packets for the MKA policy.
- The no form of the command resets the transmit interval to the default value.
- Default: 2
- **Configure MKA Transmit Interval**
  - `transmit-interval <INTERVAL>`

Parameter	Status	Description
`transmit-interval`	Required	Configure the MKA transmit interval.
`<INTERVAL>`	Variable – Required	The MKA transmit interval in seconds (Default: 2)

Example	`switch(config)# mka policy MKA1 key-server-priority 5`
	OR
	`switch(config)# mka policy MKA1`
	`switch(config-mka-policy)# key-server-priority 5`	

Configuration

Interface Commands

Associate a MACsec Policy to a Port

- When a policy is associated with a port, MACsec is enabled and all data traffic is blocked until a secure channel is successfully established. However, MACsec requires both a MACsec policy and a MKA policy to be associated with the port to function.
- A MACsec policy can be associated with the following types of ports.
  - A physical interface that is not part of any LAG ports.
  - A LAG port.
  - Not all interfaces may support MACsec capability. Unsupported interfaces will show error message when policy is applied. On LAG, any non MACsec capable interfaces part of LAG will be blocked.
- The 32-port 8360 switch (JL700A/JL701A) does not support both MACsec and priority-based flow-control (PFC) on same interface. Applying a MACsec policy to port associated with existing PFC configuration will disable interface. PFC must be unconfigured from the interface before it can be used.
- Only a single MACsec policy can be associated with any port.
- The no form of the command dissociates the MACsec policy from the port.
- **Apply MACsec policy on port**
  - `apply macsec policy <POLICY-NAME>`

Parameter	Status	Description
`macsec`	Required	MAC security (MACsec) protocol
`Policy`	Required	Apply a MACsec policy to the interface
`<POLICY-NAME>`	Variable – Required	The MACsec policy to apply

Example

```
switch(config)# interface 1/1/1
switch(config-if)# apply macsec policy MACsecP1
If PFC was enabled:
MACsec and priority-based flow control (PFC) cannot be configured at the same time on this interface. Applying a
MACsec policy will disable the interface until PFC is removed.
Continue (y/n)?
```

Associate a MKA Policy to a Port

- To start the MKA protocol on the port, a MACsec policy must also be associated to the port. When a MACsec policy is dissociated from a port, any MKA instances running on the port will be destroyed.
- An MKA policy can be associated with the following types of ports.
  - A physical interface that is not part of any LAG ports.
  - A LAG port.
  - Not all interfaces may support MACsec capability. Unsupported interfaces will show error message when policy is applied. On LAG, any non MACsec capable interfaces part of LAG will be blocked.
- Only a single MKA policy can be associated with any port.
- The no form of the command dissociates the MKA policy from the port.
- **Apply MKA policy on port**
  - `apply mka policy <POLICY-NAME>`

Parameter	Status	Description
`mka`	Required	MACsec Key Agreement (MKA) protocol
`Policy`	Required	Apply an MKA policy to the interface
`<POLICY-NAME>`	Variable – Required	The MKA policy name to apply

Example	`switch(config)# interface 1/1/1`
	`switch(config-if)# apply mka policy Agg-To-Agg`	

Configuration

MACsec Execution Commands

Show MACsec Policy

- Display details of a MACsec policy.
- **Show MACsec policy**
  - `show macsec policy [<POLICY-NAME>]`

Parameter	Status	Description
`macsec`	Required	Show MACsec information
`policy`	Required	Show MACsec policy information
`<POLICY-NAME>`	Variable – Required	The MACsec policy to display

Example

```
switch# show macsec policy

MACsec Policy Details
======================

  Policy Name: MACsecP1
  ----------------------------------------------------------------------------------------
    Cipher suite             : GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128, GCM-AES-XPN-256
    Include SCI              : Yes
    Confidentiality          : Enabled
    Confidentiality offset   : 30
    Replay protection        : Enabled
    Replay protection window : 0
```

Show MACsec Status

- Display the MACsec status on each MACsec enabled interface.
- **Show MACsec status**
  - `show macsec status [interface <IFRANGE>] [detailed]`

Parameter	Status	Description
`macsec`	Required	Show MACsec information
`status`	Required	Show MACsec status information
`[interface] [detailed]`	Either required	Interface view or detailed view
`<IFRANGE>`	Variable - optional	Interface to display MACsec information on

Example

```
switch# show macsec status interface 1/1/1-1/1/2

MACsec Protocol Status

 Interface  Port-Id  Policy                    Protection           Status
 ---------- -------- ------------------------- -------------------- ------------
 1/1/1      1        MACsecP1                  IC, Conf, Offset 0   Init
 1/1/2      1        MACsecP1                  IC, Conf, Offset 0   Init
```

Show MACsec Status (cont.)

Parameters

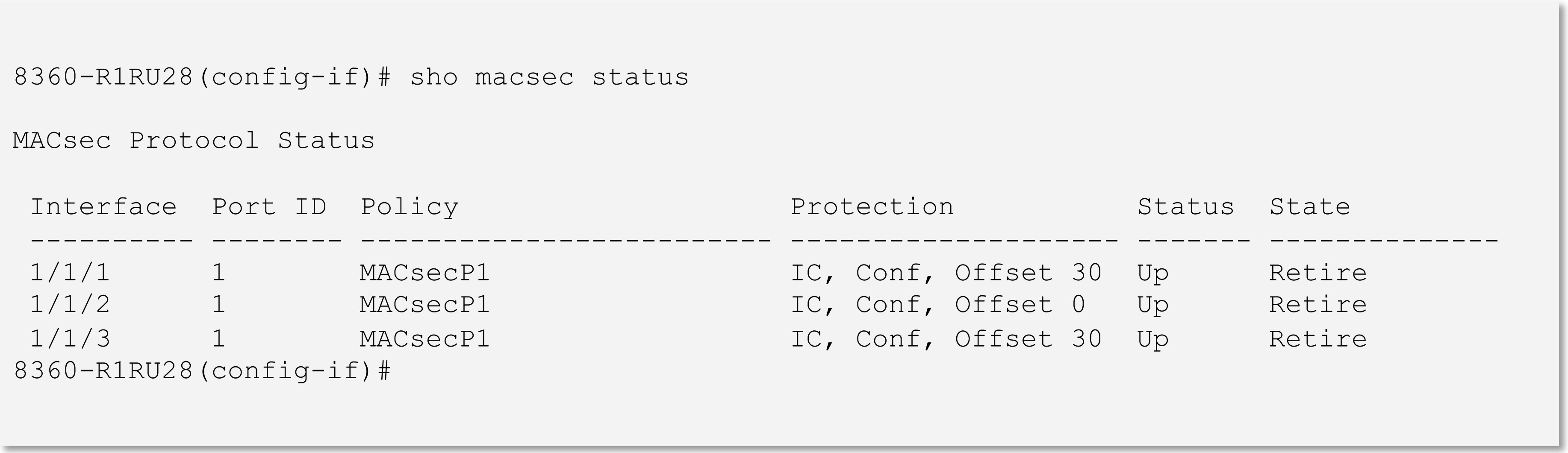
- `show macsec status [interface <IFRANGE>] [detailed]`

Parameter	Status Description
PORT-ID	The identifier associated with an instance of the MAC security entity (SecY) on the interface. ‘0’ for the instance running on the ‘real port’ of the interface. Non-zero values for entities running on a ‘virtual port’ of the interface
STATE	The status of the controlled port (CP) associated with the MACsec link. Possible values for Status • Init = The CP is initialized • Secured = The CP is waiting for a new SAK to be generated. • Receive = A new SAK is generated and the latest receive SAs for the new SAK are created on the CP. • Receiving = The latest receive SAs are in use on the CP. • Ready = The CP is ready to transmit with the latest SAs. • Transmit = The latest transmit SA is enabled on the CP. • Transmitting = The latest transmit SA is in use on the CP. • Abandon = The current SAs are being abandoned on the CP as a result of a new SAK being generated. • Retire = The old SAs are removed and the latest SAs are now the current SAs on the CP
PROTECTION	The possible values for PROTECTION TYPE • Conf = Confidentiality is enabled on the MACsec link. • Offset offset = Confidentiality offset is enabled on the MACsec link. • IC = Integrity Check is enabled on the MACsec link.
STATUS	• Up = Secured • Down = Unsecured

Show MACsec Status (cont.)

Example

- `show macsec status`



```
8360-R1RU28(config-if)# sho macsec status

MACsec Protocol Status

 Interface  Port ID  Policy                    Protection           Status  State
 ---------- -------- ------------------------- -------------------- ------- --------------
 1/1/1      1        MACsecP1                  IC, Conf, Offset 30  Up      Retire
 1/1/2      1        MACsecP1                  IC, Conf, Offset 0   Up      Retire
 1/1/3      1        MACsecP1                  IC, Conf, Offset 30  Up      Retire
8360-R1RU28(config-if)#
```

Show MACsec Statistics

– Display statistics associated with MACsec on each MACsec enabled interface.

– **Show MACsec statistics**

– `show macsec statistics [interface <IFRANGE>]`

Parameter	Status	Description
`macsec`	Required	Show MACsec information
`statistics`	Required	Show MACsec statistics information – for all ports unless interface command is used
`interface`	Optional	Filter statistics by interface
<IFRANGE>	Optional	Shows the statistics associated with mka on the given interfaces.

Example

```
switch# show macsec statistics
MACsec Statistics
Interface 1/1/1
================
  Rx Statistics
  --------------
    Unicast Uncontrolled Packets    : 0
    Multicast Uncontrolled Packets  : 604441
    Broadcast Uncontrolled Packets  : 12
    Rx Uncontrolled Drop Packets    : 0
    Rx Uncontrolled Error Packets   : 0
    Rx Controlled Unicast Packets   : 0
    Rx Controlled Multicast Packets : 2
    Rx Controlled Broadcast Packets : 12
    Rx Controlled Drop Packets      : 0
    Rx Controlled Error Packets     : 0
    Uncontrolled Octets             : 70196985
    Controlled Octets               : 6466885
  Tx Statistics
  --------------
    Unicast Uncontrolled Packets    : 0
    Multicast Uncontrolled Packets  : 744632
```

```
Broadcast Uncontrolled Packets  : 16
    Rx Uncontrolled Drop Packets    : 0
    Rx Uncontrolled Error Packets   : 0
    Unicast Controlled Packets      : 0
    Multicast Controlled Packets    : 448486
    Broadcast Controlled Packets    : 125916
    Rx Controlled Drop Packets      : 0
    Rx Controlled Error Packets     : 0
    Uncontrolled Octets             : 98851304
    Controlled Octets               : 52810544
    Common Octets                   : 169728074
 SecY Statistics
  ----------------
    Port Identifier : 1
    Rx Statistics
    --------------
      Transform Error Packets : 0
      Control Packets         : 3
      Untagged Packets        : 0
      No Tag Packets          : 0
```

Clear MACsec Statistics

- Clear the MACsec statistics associated with the port. If no interface is specified, the statistics is cleared for all MACsec enabled ports.
- The command clears the statistics for all the MACsec related counters in the hardware and not just in the current user session.
- **Clear MACsec statistics**
  - `clear macsec statistics [interface <IFRANGE>]`

Parameter	Status	Description
`macsec`	Required	Clear MACsec information
`statistics`	Required	Clear MACsec statistics
`interface`	Optional	Filter by interface
`<IFRANGE>`	Optional	Clears the MACsec statistics on the given interfaces

Example

```
Clear MACsec statistics on interfaces:
switch# clear macsec statistics interface 1/1/1-1/1/2

Clear MACsec statistics on all interfaces:
switch# clear macsec statistics
```

Configuration

MKA Execution Commands

Show MKA Policy

– Display details of an MKA policy.

– **Show MKA policy**

  – `show mka policy [<POLICY-NAME>]`

Parameter	Status	Description
`mka`	Required	Show MKA information
`policy`	Required	Show MKA policy information
`<POLICY-NAME>`	Variable – Required	The MKA policy to display

Example

```
switch# show mka policy
MKA Policy Details
===================
  Policy Name: MKA1
  ---------------------------------------------------------------------------
    Mode                         : Pre-shared key
    CKN                          : abcdef123456
    CAK (encrypted)              : AQBapXxKjQnKN2KvYeWVIJQ9wmQzgQ3aecN9A0Z6RJR...
    Key-server Priority          : 0
    Transmit Interval            : 2 seconds
```

OR

```
switch# show mka policy MKA1
MKA Policy Details
===================
  Policy Name: MKA1
  ---------------------------------------------------------------------------
    Mode                         : Pre-shared key
    CKN                          : abcdef123456
    CAK (encrypted)              : AQBapXxKjQnKN2KvYeWVIJQ9wmQzgQ3aecN9A0Z6RJR...
    Key-server Priority          : 0
    Transmit Interval            : 2 seconds
```

Show MKA Status

– Display status of an MKA policy.

– **Show MKA policy**

  – `show mka status [interface <IFRANGE>]`

Parameter	Status	Description
`mka`	Required	Show MKA information
`status`	Required	Show the status of MKA on the interface
`interface`	Optional	
`<IFRANGE>`	Variable – Optional	Interface to display MACsec information on

Example

```
switch# show mka status
MKA Protocol Status
Interface 1/1/1
================
MKA Port Identifier : 1
MKA Session Status  : Unsecured
Mode                : Pre-shared key
CKN                 : abcdef123456
CAK (encrypted)     : AQBapXxKjQnKN2KvYeWVIJQ9wmQzgQ3aecN9A0Z6RJRr9IUHBgAAAM73SUN+AQ==
Member Identifier   : 5134f576310aed35fa16dc2b
Message Number      : 1218
Capability          : IC, Conf, Offset 0
Transmit Interval   : 2 seconds
Key Server Priority : 0
Key Server          : Yes
Live Peer List:
MI                       MN       PRI Capability            Rx-SCI
------------------------ -------- --- --------------------- ----------------
Potential Peer List:
MI                       MN       PRI Capability            Rx-SCI
------------------------ -------- --- --------------------- ----------------
```

Show MKA Statistics

- Display statistics associated with MKA on each enabled interface.
- **Show MKA statistics**
  - `show macsec statistics [interface <IFRANGE>]`

Parameter	Status	Description
`mka`	Required	Show MKA information
`statistics`	Required	Show MKA statistics information – for all ports unless interface command is used
`interface`	Optional	Filter statistics by interface
<IFRANGE>	Optional	Shows the statistics associated with MKA on the given interfaces.

Example

```
switch(config)# show mka statistics
MKA Statistics
Interface 1/1/1
================
  KaY
  ----
    SCI : 00fd456704510001
    Statistics
    -----------
      MKPDUs With Invalid Version : 0
      MKPDUs With Invalid CKN     : 0
    Participant
    ------------
      CKN : abcdef123456
      Statistics
      -----------
        Tx MKPDUs                 : 1518
        Rx MKPDUs                 : 0
        SAKs Distributed          : 0
        SAKs Received             : 0
        MKPDUs With Invalid ICV   : 0
        MKPDUs With Duplicate MI  : 0
        MKPDUs With Invalid MN    : 0
```

```
Interface 1/1/2
================
  KaY
  ----
    SCI : 00fd456704520001
    Statistics
    -----------
      MKPDUs With Invalid Version : 0
      MKPDUs With Invalid CKN     : 0
    Participant
    ------------
      CKN : abcdef123456
      Statistics
      -----------
        Tx MKPDUs                 : 1505
        Rx MKPDUs                 : 0
        SAKs Distributed          : 0
        SAKs Received             : 0
        MKPDUs With Invalid ICV   : 0
        MKPDUs With Duplicate MI  : 0
        MKPDUs With Invalid MN    : 0
```

Clear MKA Statistics

- Clear the MKA statistics associated with the port. If no interface is specified, the statistics is cleared for all MACsec enabled ports.
- The command clears the statistics for all the MKA related counters in the software and not just in the current user session.
- **Clear MKA statistics**
  - `clear macsec statistics [interface <IFRANGE>]`

Parameter	Status	Description
`mka`	Required	Clear MKA information
`statistics`	Required	Clear MKA statistics
`interface`	Optional	Filter by interface
<IFRANGE>	Optional	Clears the MKA statistics on the given interfaces

Example	`Clear MKA statistics on interfaces:`
	`switch# clear mka statistics interface 1/1/1-1/1/2`
	
	`Clear MKA statistics on all interfaces:`
	`switch# clear mka statistics`	

Best Practices

aruba
a Hewlett Packard
Enterprise company

Feature/Solution Best Practices

- Enable MACsec on links that have the potential to be compromised (man-in-the-middle, masquerading etc.) a.k.a Dark fiber.
- Avoid MACsec on links that are already (or close to) operating at full capacity. The overhead of a MACsec header can lead to packet drops on a link operating close to full capacity. (~85% and above)
- Use the default values for the following configurations –
  - Confidentiality (Default: Enabled)
  - Confidentiality-Offset (Default: 0)
  - Replay Protection (Default: Enabled, Window-Size 0)
  - Transmit-Interval (Default: 2 seconds)
- Cipher-Suite: Configure the most secure cipher-suite that both the ends of a MACsec channel can support.
- Key-Server Priority: Ensure the device that must be elected as key-server is configured with a lower key-server priority value than the other device of the channel.
- Include-SCI tag: Disable it for a slight improvement in performance due to lower overhead in the MACsec header on point-to-point links.

Feature/Solution Best Practices (cont.)

- MACsec channel is destroyed and re-established on a configuration change in the MACsec or MKA policy in use on the channel.
  - The user is warned with a prompt when a configuration change is attempted on a policy that is currently is use on an interface.
  - Avoid configurations changes in MACsec and MKA policies that are applied on interfaces on a live network to avoid traffic drops for a few seconds.
- Interop
  - Cisco
    - The Cisco device needs to be elected key-server for the MACsec channel to be successfully established. Configure the key-server priority on the AOS-CX device to be higher than the Cisco device to guarantee the Cisco device is elected key-server.
    - It is advised to use a confidentiality-offset value of 0.
    - NOTE: Verified with Cisco Catalyst 9300.
- Comware
  - It is advised to use a confidentiality-offset value of 0.
  - NOTE: Verified with HPE FlexFabric 5940.
- AOS-S
  - AOS-S devices that support MACsec only support the AES-128 encryption for MACsec. Configure the cipher-suite to “aes-gcm-128” on the AOS-CX device.
  - Use confidentiality-offset value of 0 since AOS-S devices don’t support other offset values.
  - NOTE: Verified with Aruba 5400R and 3810.

Troubleshooting

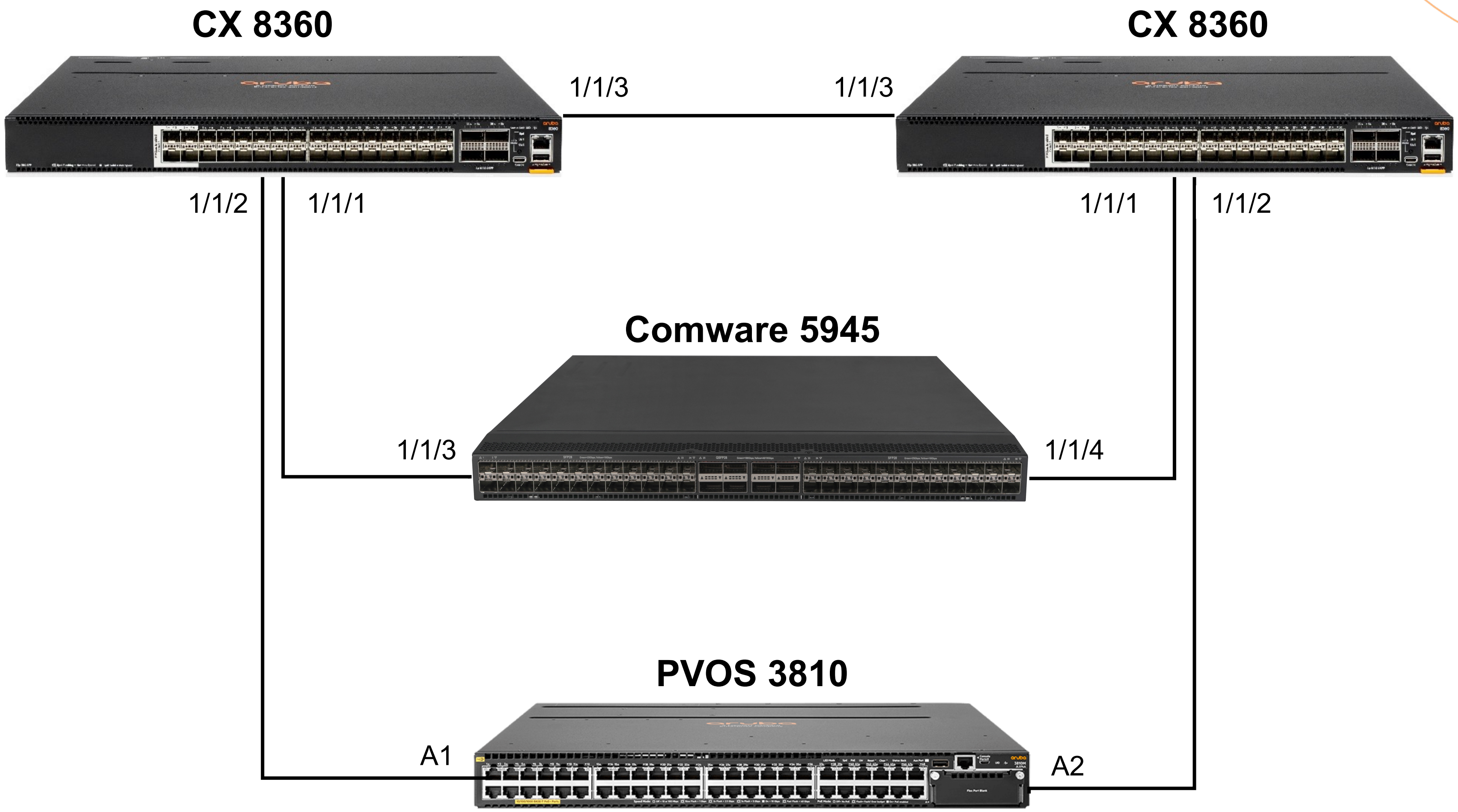
aruba
a Hewlett Packard
Enterprise company

Feature/Solution Troubleshooting

- Use “copy support-files” and “diag-dump” commands with feature as “macsec” to capture diagnostic data specific to MACsec.
  - NOTE: Use “all” when reporting CFDs.
- Debug logs are available for MACsec.
  - Run “debug macsec all” for verbose logs when debugging issues.
- When MACsec does not work between 2 end points.
  - Verify the MKA session is “Secured” on both the sides.
    - When the MKA sessions between the 2 MACsec end points flaps continuously between Secured and Unsecured.
    - Verify the cipher-suite advertised by the elected key-server is supported on the peer.
    - Verify the confidentiality-offset configuration is identical on the MACsec peers.
  - Verify the MACsec status shows “Up” and state shows as “Retire”.
  - Check the MACsec statistics for packets being dropped.
    - Ok packets must increment on the Rx channel.
    - Not Valid packets incrementing on the Rx channel indicates an issue with the key programmed on either side of the MACsec channel.

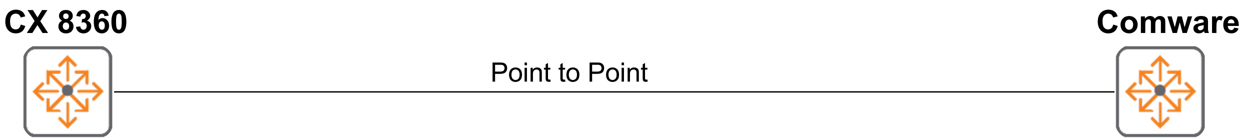
Demo

Demo environment



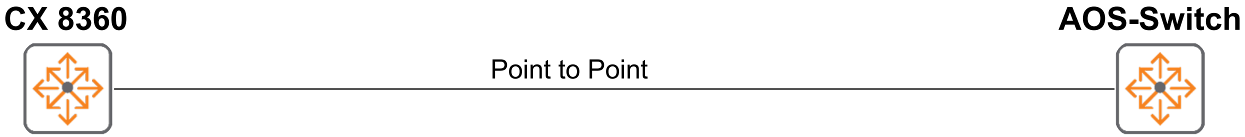
```
8360-R1RU28(config-if)# sho macsec status
MACsec Protocol Status
 Interface  Port ID  Policy                     Protection          Status  State
 ---------- -------- -------------------------- ------------------- ------- --------------
 1/1/1      1        MACsecP1                   IC, Conf, Offset 30 Up      Retire
 1/1/2      1        MACsecP1                   IC, Conf, Offset 0  Up      Retire
 1/1/3      1        MACsecP1                   IC, Conf, Offset 30 Up      Retire
8360-R1RU28(config-if)#
```

MACsec example configuration



```
interface 1/1/1
    no shutdown
    ip address 110.1.1.1/24
    apply mka policy MKA1
    apply macsec policy MACsecP1
macsec policy MACsecP1
    cipher-suite gcm-aes-128
    replay-protection window-size 100
    confidentiality offset 30
mka policy MKA1
    pre-shared-key ckn abc123 cak ciphertext
AQBapUvjDZgUxtTpgA4NLqnsn7CjXzbDch+BOS7y9fcWExLUBgAAAKUmDYdhew==
```

```
interface 1/1/3
    port link-mode bridge
    port access vlan 110
    macsec desire
    macsec confidentiality-offset 30
    macsec replay-protection window-size 100
    mka enable
    mka psk ckn ABC123 cak cipher
$c$3$IOw3GqlAnN7eKO68rp/rMiQlWVSHTd+6qQ==
    lldp compliance admin-status cdp txrx
```



```
interface 1/1/2
    no shutdown
    ip address 111.1.1.1/24
    apply mka policy MKA1
    apply macsec policy MACsecP1
macsec policy MACsecP1
    cipher-suite gcm-aes-128
    replay-protection window-size 100
mka policy MKA2
    pre-shared-key ckn abc123 cak ciphertext
AQBapUvjDZgUxtTpgA4NLqnsn7CjXzbDch+BOS7y9fcWExLUBgAAAKUmDYdhew==
    key-server-priority 24
```

```
aaa port-access mka key-server-priority 5 A1-A2
aaa port-access mac-based 1-2
macsec policy "MACsecP1"
   mode pre-shared-key ckn "abc123" cak "123abc"
   replay-protection 100
   exit
macsec apply policy "MACsecP1" A1-A2
```

Thank you

aruba

a Hewlett Packard
Enterprise company