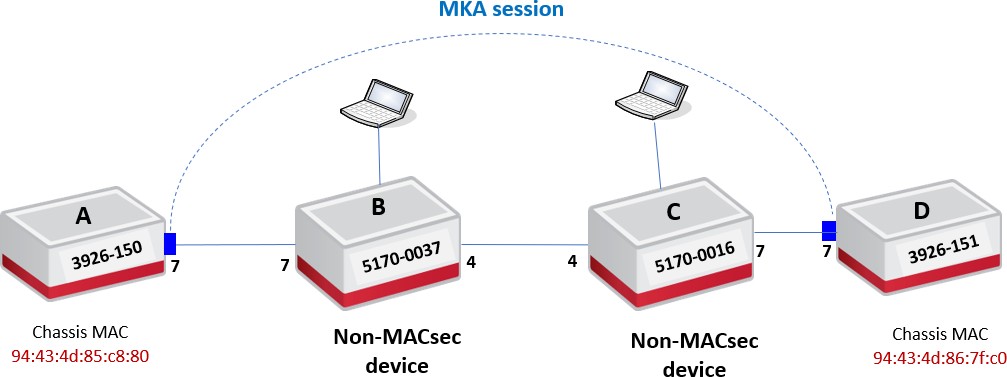
###### End to End Mode on 3926

MACsec end end-to-end is also supported over the WAN and allows transport through non-MACsec intermediate network.

In this mode, we support both ETTP based as well as Flow Point based service. FP-based service allows MACsec and non-MACsec traffic flows to run on same physical interface. We will be covering FP-based service in the following sections.

* Scenario1: Vlan-based



***Objective:***

The objective of this test is to establish end-to-end MACsec connection-association between the two nodes over an L2 switching circuit and verify that the traffic running is being encrypted. 5170s devices used in the topology are not MACsec aware.

***Procedure:***

***On Node A & Node D***

* Go to the configuration terminal
  + Config
* Setup the Forwarding Domains, classifiers and flow points in CLI on nodes A and D
  + classifiers classifier cvid-10 filter-entry classifier:vtag-stack vtags 1 vlan-id 10
  + fds fd FD1 vlan-id 10 mode vpls
  + fps fp fp7.1 logical-port 7 fd-name FD1 classifier-list cvid-10
* Create a **key-chain** for authentication and key establishment
  + macsec key-chains key-chain kc2002 mka-keys mka-key 2002 key 0123456789abcdef0123456789abcdef0123456789abcdef0123456789a bcdef

macsec key-chains key-chain kc2002 mka-keys mka-key 2002 cryptographic-algorithm AES\_128\_CMAC

* Create a MACsec **profile**
  + macsec macsec-profiles profile pf2002 encryption-on true

additional-bytes-in-clear 4 **(Optional, to leave C-tag in clear)**

key-server-priority 10

macsec-cipher-suite GCM\_AES\_128 replay-window-size 2

sak-rekey-interval 30

* Enable MACsec on **interface**
  + macsec config interfaces interface 7 strict-mode-on false

exclude-protocols lldp

exclude-protocols lacp

**Note:** In this case, strict mode needs to be set to false (Lenient mode) to allow MACsec and non- MACsec traffic flows to run over the same PHY.

* Create a **connection-association**

On node A:

* + macsec config connection-association CA2002 macsec-admin-state enabled

destination-address 94:43:4d:86:7f:c0 **(MAC of the peer chassis)**

mka-ether type 0x9001 key-chain kc2002 macsec-profile pf2002 flow-point untag-fp7.1

On node D:

* + macsec config connection-association CA2002 macsec-admin-state enabled

destination-address 94:43:4d:85:c8:80 **(MAC of the peer chassis)**

mka-ether type 0x9001 key-chain kc2002 macsec-profile pf2002 flow-point untag-fp7.1

**Note:** other devices within the provider network can process MKA frames. To avoid this behavior, the MAC@/Ether type for the control frames need to be changed so that they are not consumed when forwarded through the provider’s network.

We support 3 scenarios in end-to-end Flow point-based mode:

* Default multicast destination MAC **(01:80:C2:00:00:03)** and default Ether type **(0x888E).**
* Non-default multicast destination MAC **(01:01:01:01:01:01)** and non-default Ethertype

(0x9001).

* UNICAST destination MAC (**peer Chassis MAC**) and non-default Ethertype **(0x9001).**

***On Node B & Node C***

* + Go to the configuration terminal
    - Config
  + Setup the Forwarding Domains, classifiers and flow points in CLI on nodes A and D
    - classifiers classifier cvid-10 filter-entry classifier:vtag-stack vtags 1 vlan-id 10
    - classifiers classifier cvid-1002 filter-entry classifier:vtag-stack vtags 1 vlan-id 1002
    - fds fd FD1 mode vpls
    - fps fp fp7.1 logical-port 7 fd-name FD1 classifier-list cvid-10

ingress-l2-transform push-svid-1002 vlan-stack 1 push-tpid tpid-8100 push-vid 1002

egress-l2-transform pop-svid-1002 vlan-stack 1 pop-type fps fp fp4.1 logical-port 4 fd-name FD1 classifier-list cvid-1002

MACsec configuration on the nodes can be viewed using below commands.

3926\_0150> show macsec connection-associations

+ CONNECTION-ASSOCIATION +

| CA Name | Admin State | Oper State | Service Type | Macsec Profile | Key Chain |

+ + + + + + +

| CA2002 | enabled | enabled | Flow Point | pf2002 | kc2002 |

+ + + + + + +

3926\_0150> show macsec connection-associations connection-association CA2002

+ CONNECTION-ASSOCIATION +

| Parameter | Value |

+ + +

| CA Name | CA2002 |

| Admin State | enabled |

| Oper State | enabled |

| Oper State Reason | **Operational Up.** |

| Key Server | True |

| Destination Address | **94:43:4d:86:7f:c0** |

| Mka Ethertype | **0x9001** |

| Macsec Profile | pf2002 |

| Key Chain Name | kc2002 |

| Service Type | **Flow Point** |

| Service Name | fp7.1 |

+ + +

| Peer Secure Channel | |

+ + +

| Mac Address | 94:43:4d:86:7f:c0 |

| Port Identifier | 01-00 |

+ + +

|  |  |  |  |
| --- | --- | --- | --- |
| |  + | MKA Statistics | |  + | |  + |
| | | In EAPOL MKA invalid CKN Len Frames | | 0 | | |
| | | In EAPOL MKA invalid Frames | | 0 | | |
| | | In EAPOL MKA Frames | | 220 | | |
| | | Out EAPOL MKA Frames | | 242 | | |

| In Version Mismatch Frames | 0 |

| In CKN Mismatch Frames | 0 |

| In ICV Mismatch Frames | 0 |

+ + +

| Data Statistics | |

+ + +

| In Valid Packets | 0 |

| In Error Packets | 0 |

| In Transform Error Packets | 0 |

| In Control Packets | 0 |

| In Untagged Packets | 0 |

| In No Tag Packets | 0 |

| In Bad Tag Packets | 0 |

| In No SCI Packets | 0 |

| In Unknown Packets | 0 |

| In Decrypted Octets | 0 |

| In Validated Octets | 0 |

| Out Encrypted Packets | 0 |

| Out Protected Packets | 0 |

| Out Control Packets | 0 |

| Out Untagged Packets | 0 |

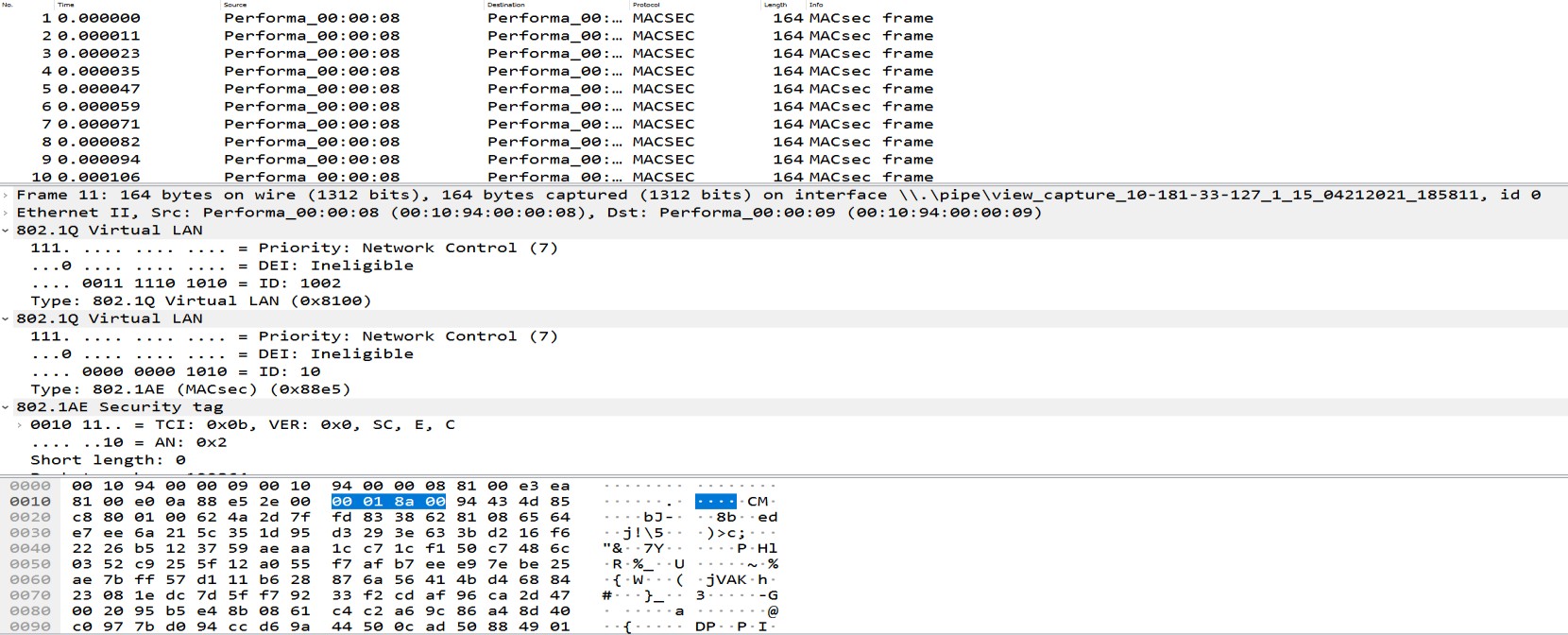
| Out Transform Error Packets | 0 |

| Out Encrypted Octets | 0 |

| Out Protected Octets | 0 |

+ + +

The captured encrypted traffic is depicted below. After configuring the 4 additional bytes in clear, we can see that both C-Tag and S-tag are displayed on the packet capture **(flow-point-based MACsec include the service provider’s S-tag in the clear by default).**



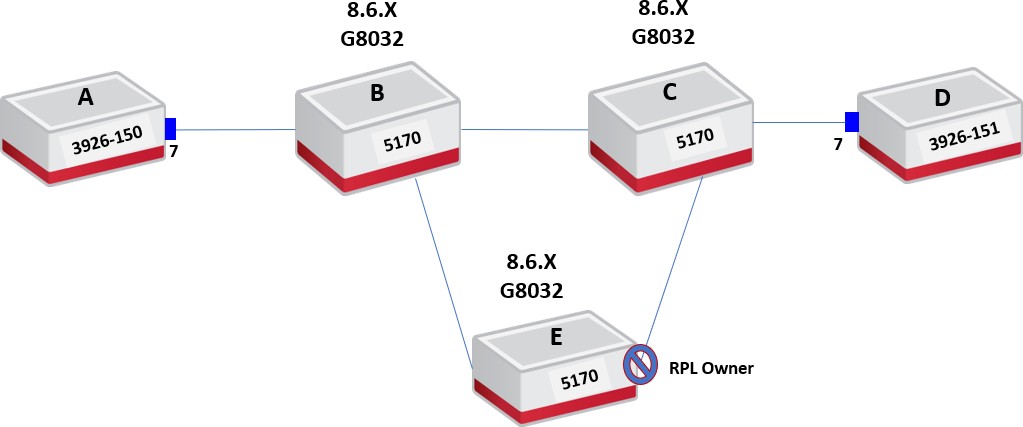
C-TAG

S-TAG

**Test Case Results:**

Passed: Yes No Verified by Date/Time Comments

**Scenario2: Macsec over G8032 ring**



***Objective:***

The objective of this test is to setup end-to-end macsec along with G8032 ring. In this case MACsec devices shouln’t be part of the ring as the ethernet ring protection and the encryption are working independetly.

G8032 as an ecrypted MACsec service is not supported in **SAOS 10.6** and will be introduced in future relases.

***Procedure:***

Here it is assumed that G8032 is already running on 5170 devices running 8.6.x SW.

***On Node A & Node D***

* + Go to the configuration terminal
    - Config
  + Setup the Forwarding Domains, classifiers and flow points in CLI on nodes A and D:
    - classifiers classifier VLAN1000 filter-entry classifier:vtag-stack vtags 1 vlan-id 1000
    - fds fd FD1000 vlan-id 1000 mode vpls
    - fps fp FP7 logical-port 7 fd-name FD1000 classifier-list VLAN1000
  + Create a **key-chain** for authentication and key establishment
    - macsec key-chains key-chain KC1000 mka-keys mka-key 01 key 0123456789abcdef0123456789abcdef0123456789abcdef0123456789a bcdef
    - macsec key-chains key-chain KC1000 mka-keys mka-key 2002 cryptographic-algorithm AES\_128\_CMAC
  + Create a MACsec **profile**
    - macsec macsec-profiles profile pf1 encryption-on true

key-server-priority 10

macsec-cipher-suite GCM\_AES\_128 replay-window-size 2

sak-rekey-interval 30

* + Enable MACsec on **interface**
    - macsec config interfaces interface 7 strict-mode-on false
  + Create a **connection-association On node A:**
    - macsec config connection-association CA1000 macsec-admin-state enabled

destination-address 94:43:4d:86:7f:c0 **(MAC of the peer**

chassis)

mka-ethertype 0x9001 key-chain KC1000 macsec-profile pf1 flow-point FP1

* + Create a **connection-association On node D:**
    - macsec config connection-association CA1000 macsec-admin-state enabled

destination-address 94:43:4d:85:c8:80 **(MAC of the peer**

chassis)

mka-ethertype 0x9001 key-chain KC1 macsec-profile pf1 flow-point FP1

MACsec configuration on the nodes can be viewed using below commands.

3926-150> show macsec connection-associations

+ CONNECTION-ASSOCIATION +

| CA Name | Admin State | Oper State | Service Type | Macsec Profile | Key Chain |

+ + + + + + +

| CA1000 | enabled | enabled | Flow Point | pf1 | KC1000 |

+ + + + + + +

3926-150> show macsec connection-associations connection-association CA1000

+ CONNECTION-ASSOCIATION +

| Parameter | Value |

+ + +

| CA Name | CA1000 |

| Admin State | enabled |

| Oper State | enabled |

| Oper State Reason | **Operational Up.** |

| Key Server | True |

| Destination Address | **94:43:4d:86:7f:c0** |

| Mka Ethertype | **0x9001** |

| Macsec Profile | pf1 |

| Key Chain Name | KC1000 |

| Service Type | **Flow Point** |

| Service Name | FP7 |

+ + +

| Peer Secure Channel | |

+ + +

| Mac Address | 94:43:4d:86:7f:c0 |

| Port Identifier | 01-00 |

+ + +

| MKA Statistics | |

+ + +

| In EAPOL MKA invalid CKN Len Frames | 0 |

| In EAPOL MKA invalid Frames | 0 |

| In EAPOL MKA Frames | 5334 |

| Out EAPOL MKA Frames | 5089 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| | | In Version Mismatch Frames | | | 0 | | |
| | | In CKN Mismatch Frames | | | 0 | | |
| | | In ICV Mismatch Frames | | | 0 | | |

+ + +

| Data Statistics | |

+ + +

| In Valid Packets | 5216 |

| In Error Packets | 0 |

| In Transform Error Packets | 0 |

| In Control Packets | 5334 |

| In Untagged Packets | 0 |

| In No Tag Packets | 0 |

| In Bad Tag Packets | 0 |

| In No SCI Packets | 0 |

| In Unknown Packets | 0 |

| In Unused SA Packets | 0 |

| In Unused SA Discarded Packets | 0 |

| In Overrun Discarded Packets | 0 |

| In Unchecked Packets | 0 |

| In Invalid Packets | 0 |

| In Invalid with Sectag C-bit=1 Packets | 0 |

| In Delayed Packets | 0 |

| In Late Packets | 0 |

| In Decrypted Octets | 563328 |

| In Validated Octets | 563328 |

| Out Encrypted Packets | 3 |

| Out Protected Packets | 3 |

| Out Control Packets | 5089 |

| Out Untagged Packets | 0 |

| Out Transform Error Packets | 0 |

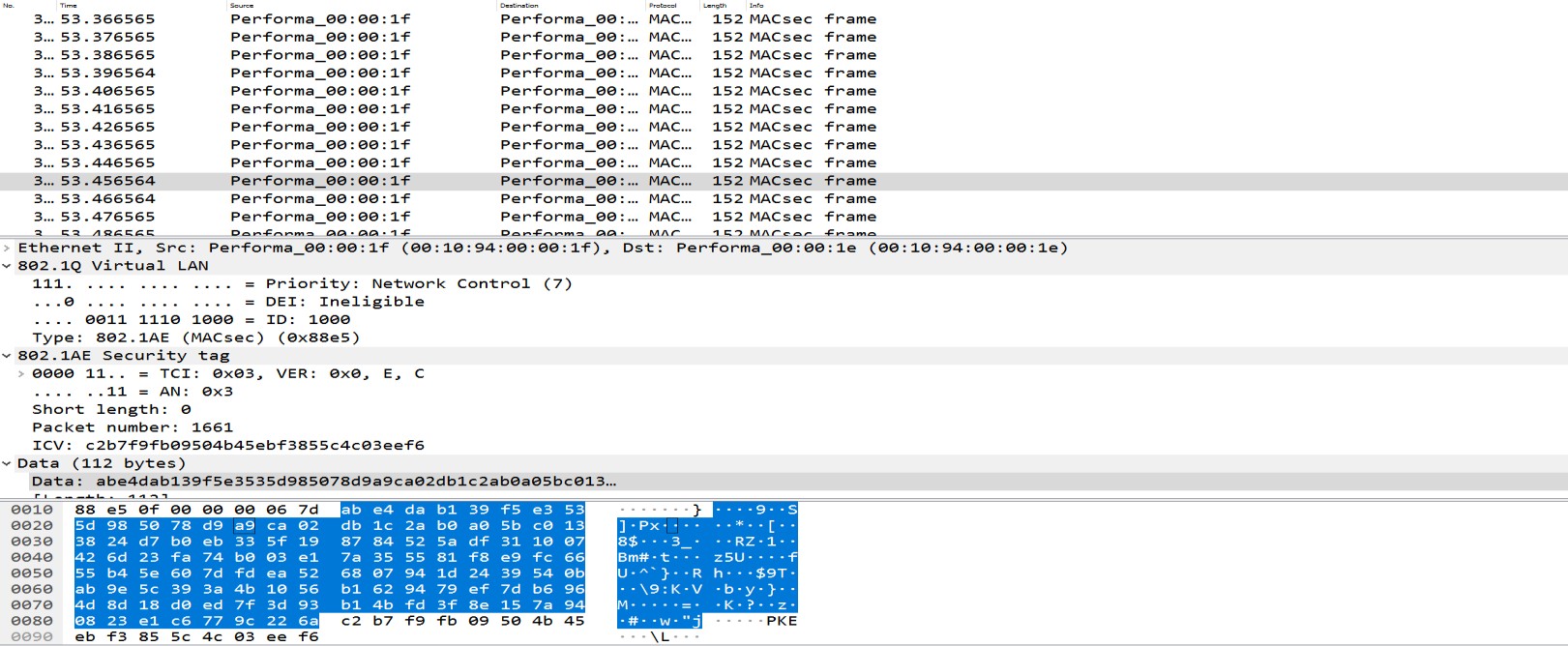
| Out Too Long Discarded Packets | 0 |

| Out Encrypted Octets | 324 |

| Out Protected Octets | 324 |

+ + +

We can see on the capture below that the traffic running end-to-end (NodeA-Node D) is being encrypted. As mentioned previously, the S-tag is left in clear by default.



**Test Case Results:**

Passed: Yes No Verified by Date/Time Comments