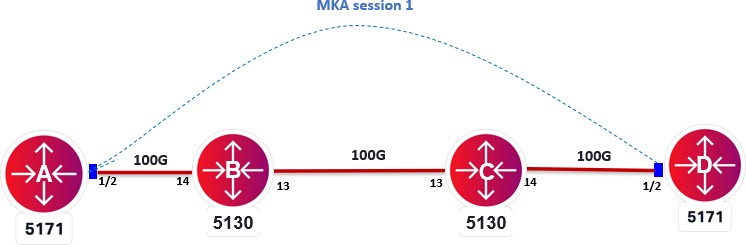
###### End-to-end mode on 5171

Starting from 10.7.1, MACsec feature is supported on 5171 platforms using 100G interfaces on FRU modules.

The only difference on 5171 in 10.7.1 compared to 3926 is that we are adding a l2-transform on the FD only for **FP-based end-end mode**. At the opposite of XGS, control frames are sent untagged on DNX. When MACsec is configured, MKA frames should have the same VLAN tag configured on the classifier of the FP on which the feature is configured.



***Objective***

The objective of this test is to establish FP-based end-to-end MACsec connection-association between the two 5171s over a L2 switched circuit.

***Procedure:***

* Go to the configuration terminal
  + config
* Setup the Forwarding Domains, classifiers and flow points in CLI
  + fds fd fd-Msec5171 mode vpls
  + fds fd fd-Msec5171 initiate-l2-transform vlan-stack 1 push- vid 10
  + classifiers classifier cvid-10 filter-entry classifier:vtag-stack vtags 1 vlan-id 10
  + fps fp p5171-NNI logical-port 1/2 fd-name fd-Msec5171 classifier-list cvid-10
* Create a **key-chain** for authentication and key establishment, it’s used to generate SAK keys to be used to program hardware. It can use both 128 and 256 cryptographic algorithms. The pre-shared key must match on both MACsec devices for the session to be established
  + macsec key-chains key-chain kc10 mka-keys mka-key 01 key 0123456789abcdef0123456789abcdef0123456789abcdef0123456789a bcdef

macsec key-chains key-chain kc10 mka-keys mka-key 01 cryptographic-algorithm AES\_128\_CMAC

exit

* Create a **profile** that combines various user configurable parameters for security
  + macsec macsec-profiles profile pf1 encryption-on true

key-server-priority 10 **(On the server only to generate the SAK)**

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

sak-rekey-interval 30

* Enable MACsec on interface. We can exclude L2 protocols not to be MACsec encrypted when configuring the interface
  + macsec config interfaces interface 1/2 strict-mode-on false
* Create a **connection-association** which is a security relationship, established and maintained by key agreement protocols
  + macsec config connection-association CA10 macsec-admin-state enabled

key-chain kc10 macsec-profile pf10 flow-point fp5171-NNI

The above commands need to be configured at both MACsec nodes to perform encryption.

Once the configuration is performed at both nodes and CA connection is setup, MACsec configuration can be verified using below commands.

* + show macsec key-chains key-chain kc10

+ KEY-CHAIN +

| Key-Chain | KC1 |

+ + +

| MKA Name | 01 |

| MKA Crypto Algo | AES\_128\_CMAC |

+ + +

* + show macsec profiles profile pf10

+ MACSEC-PROFILES +

| KEY | VALUE |

+ + +

| Profile Name | pf10 |

| Cipher Suite | GCM\_AES\_128 |

| Conf Offset | 0\_BYTES |

| Replay Window Size | 2 |

| Additional Bytes In Clear | 0 |

| Encryption | True |

| Key Server Priority | 10 |

| SAK Rekey Interval | 30 |

+ + +

* + show macsec connection-associations

+ CONNECTION-ASSOCIATION +

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

+ + + + + + +

| CA10 | **enabled** | **enabled** | Flow Point | pf10 | kc10 |

+ + + + + + +

* + show macsec connection-associations connection-association CA10

+ CONNECTION-ASSOCIATION +

| Parameter | Value |

+ + +

| CA Name | CA10 |

| Admin State | enabled |

| Oper State | **enabled** |

| Oper State Reason | Operational Up. |

| Key Server | True |

| Destination Address | 01:80:C2:00:00:03 |

| Mka Ethertype | 0x888e |

| Macsec Profile | **pf10** |

| Key Chain Name | **kc10** |

| Service Type | **Flow Point** |

| Service Name | fp5171-NNI |

+ + +

| Peer Secure Channel | |

+ + +

| Mac Address | d0:19:6a:c9:6c:80 |

| Port Identifier | 01-00 |

+ + +

| MKA Statistics | |

+ + +

| In EAPOL MKA invalid CKN Len Frames | 0 |

| In EAPOL MKA invalid Frames | 0 |

| In EAPOL MKA Frames | 338534 |

| Out EAPOL MKA Frames | 321587 |

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

Test Case Results:

Passed: Yes No Verified by Date/Time Comments