Support for MACsec

Software Supported MACsec

All existing Cisco IOS XE based routers use special transceivers to perform MACsec encryption and decryption. The software MACsec uses CDAL infrastructure in QFP to perform crypto operations. Compared to the hardware supported MACsec, the process of configuration, status and datapath is performed, it is different which creates certain limitations in the functionality when used.

MACsec is supported only on L2 interfaces. The MACsec port must be put into access mode. As the encryption happens on the egress switch virtual interface (SVI), the VLAN used for the port should be unique, and no other interface must use that VLAN. This is because the QFP does not have the MAC table information.

Note

- Since MACsec is being done through software, performances are not line rate on L2 interfaces.
- Cisco supports only the *shouldsecure* MACsec mode for IR1800, which allows unencrypted traffic even in a secured state.

  The IR1800 does not support the *mustsecure* mode.

For an egress packet, the SVI is aware that the packet needs to be sent out on a VLAN without information about any specific interface. It is the switch chip that decides which port to send it to. All the packets without the MACsec tag are processed without any changes. The outgoing L2 packets will also egress without encryption or modification.

For this feature, the Network Essentials and Network Advantage license support GCM-AES-128. This feature is not available running the NPE image.

Limitations

- MACsec is not supported in controller mode.
- There must be a unique vlan id for a MACsec interface.
- Only gcm-aes-128 is supported

- Both explicit and non-explicit SCI are supported on ingress side. The IR1800 sends out only explicit SCI packets as it is not an end system.
- The IR1800 does not support confidentiality offset.
- Integrity only is not supported.
- For gcm-aes-128, up to 32 bytes are added to an encrypted packet compared to a plain packet. So the MTU setup should add 32 for it to work properly.
- The MACsec key is managed by the MKA module. For that device, it requires a static key for MKA to negotiate MACsec key.
- There is no MIB support.
- Jumbo Frame is not supported.
- MACsec is not supported on the WAN port.
- IP Device Tracking (IPDT) is not supported on Host to switch MACsec