CCNP Security - SISAS
Layer 2 Encryption - MACSec

Cisco TrustSec

- Stands for Trusted Security
  - Consists of 802.1x, SGT and MACSec
  - SGT stands for Security Group Tags
  - MACSec stands for Mac Security (layer 2 encryption)
- MACSec offers line-rate layer2 hardware-based encryption on a hop-by-hop basis
  - Host-to-switch
  - Switch-to-switch
- MACSec is 802.1ae standard
  - GCM-AES-128 algorithm
  - EtherType value changed to 0x88e5
  - Supports SGT embedded inside CMD (Cisco Meta Data) – layer 2 header

MACSec Implementation Options

- Host-to-switch (downlink)
  - Requires host to perform 802.1x authentication via EAP-TLS, PEAP or EAP-FAST
  - Native Windows supplicant does not support it
  - AnyConnect offers software based encryption
  - Negotiation and key derivation via MKA (MACsec Key Agreement)
    - Standard per the RFC
- Switch-to-switch (uplink)
  - Manual/static configuration
  - Negotiation and key derivation via SAP (Security Association Protocol)
    - Cisco proprietary based on 802.11i

MACsec Policy Enforcement

- MACsec policy is enforced per port
  - Must-not-secure, do not negotiate MACsec
  - Should-secure (default), negotiate MACsec, if failed allow clear-text traffic
  - Must-secure, negotiate MACsec, if failed do not allow clear-text traffic
- Policy type received from ISE overrides locally configures settings on NAD
  - Local Should-Secure is overridden by ISE Must-Not-Secure
- Based on host port mode, MACsec is
  - Fully supported with single-host and multi-domain
  - Partially supported with multiple-host, only first authenticated MAC address may negotiate MACsec
  - Not supported with multiple-authentication, because MACsec is point-to-point

MACsec Configuration Steps Supplicant

- Requires AnyConnect
  - Configure EAP-FAST with MacSec support

MACsec Configuration Steps on NAD

- Ensure 802.1x authentication requirements are configured
- Enable MACsec on the switch port (downlink)
  - `macsec`
  - `mka default-policy`
- Optionally define MACsec policies on switch port (downlink)
  - `authentication linksec policy`
  - `authentication event linksec fail action authorize vlan <vlan_nr>`
- Enable MACsec on the switch port (uplink)
  - `cts manual`
  - `sap pmk <value> mode-list gcm-encrypt`

MACsec Configuration Steps on ISE

- Ensure 802.1x authentication and authorizations are functional
- Configure MACsec policy in the authorization profile

MACsec Verification and Troubleshooting

- Verification
  - `show macsec summary`
  - `show macsec interface <if_nr>`
  - `show authentication session interface <if_nr>`
  - `show mka sessions interface <if_nr> detail`
  - `show mka default-policy detail`
  - `show cts interface summary`
  - `show cts interface if_nr>`
- Troubleshooting
  - `debug radius authentication`
  - `debug macsec event`

Q&A