MACSEC

MACSEC (802.11ae) är ett protokoll som innebär kryptering över L2 point-to-point, mellan switch och switch eller från switch till klient.

Komponenterna som ingår är:

- MACSEC Key chain (måste vara i HEX)
- MKA Policy (Macsec Key Algorithm)
- Konfigurering på interface

MACSEC stödjs ej direkt på länkaggregeringar. Interface som ska ingå i port-kanaler, men ändå kryptera trafik via MACSEC, måste först tas ur port-kanalen, konfigureras med MACSEC och sedan konfigureras tillbaka in i portkanalen.

MACSEC mellan switch och klient vid 802.1x innebär att injicering av trafik från tredje part på samma länk omöjliggörs.

För att undvika att länkar går ned oväntat kan man tvinga periodvis omförhandling av nycklar med `sak-rekey interval x`.

Exempelkonfiguration switch till switch

```
key chain MACSEC_KEY macsec
 key 20
   cryptographic-algorithm aes-256-cmac
  key-string 0 xxx....

mka policy MKA_POLICY
 key-server priority 100
 macsec-cipher-suite gcm-aes-256
 confidentiality-offset 30
 sak-rekey interval 300
 ssci-based-on-sci
```

```
interface GigabitEthernet1/0/48
 macsec replay-protection window-size 1000
 macsec network-link
 mka policy SMKA_POLICY
 mka pre-shared-key key-chain MACSEC_KEY
```

Kommandon

- show mka *
- show mka sessions interface te 1/0/34 detail
- show macsec *
- debug mka *
- debug macsec *

Se även Macsec-konfiguration för NXOS.

Revision #1
Created 26 April 2025 11:55:51 by Jehrlander
Updated 26 April 2025 11:56:06 by Jehrlander