PCAP / Packet Capture i IOS-XE

Det är jätteenkelt att skapa en PCAP i en IOS-XE switch. Det finns många filter man kan använda. Här skriver jag hur man gör det per port utan speciella filter. Man är välkommen att fylla på i artikeln.

1. Identifiera vilken port användaren sitter på. (show mac address-table kan väl vara hjälpsam)
2. Definiera namn på monitor session, vilken port, riktning, och filter. Ex. `monitor capture PCAP-NAMN interface gigabitEthernet 3/0/20 both match any`
3. Definiera var PCAP ska sparas med `monitor capture dameware file location flash:PCAP-NAMN.pcap`
4. Starta insamling med `monitor capture PCAP-NAMN start`
5. När du är nöjd avsluta insamling med `monitor capture PCAP-NAMN stop`. **Om du inte vill fylla diskytan på switchen glöm inte detta.**
6. Ladda hem PCAP-fil med SCP och analysera. Det är viktigt att på din klient använda flaggan -O. Pga att du behöver använda scp och inte sftp protokollet.
7. Ta bort pcap fil i flash när du är klar

Verfiering sker med `show monitor capture`. Man kan kolla på en del av insamlingen med `show monitor capture NAMN buffer brief`. Har man inte specifiserat, eller inte kan specifisera, var den ska sparas kan man exportera ut PCAP-en till ex. bootflash med `monitor capture NAMN export bootflash:NAMN.pcap`.

Revision #1
Created 26 April 2025 12:05:03 by Jehrlander
Updated 26 April 2025 12:05:32 by Jehrlander