

Cisco Discovery Protocol och Link Layer Discovery Protocol

Två protokoll som utför (nästan) samma funktion. Ena är propriärt och andra inte.

Det händer att sårbarheter hittas i CDP och LLDP, ex. har switchar kraschat vid mottagande av LLDP-frames konstruerade på ett visst sätt. Därför anser jag att det är bra att stänga av CDP och LLDP på portar där det inte behövs.

CDP och LLDP bör alltid vara avstängt på interface som går till nätverksutrustning utanför en egen organisations kontroll, såsom partners och internetleverantörer.

Cisco Discovery Protocol (CDP)

CDP är ett protokoll som tillåter Cisco-enheter att upptäcka andra Cisco-enheter. Som namnet antyder så används det av Cisco-enheter men andra leverantörer har implementerat stöd för att ta emot och förstå CDP-meddelanden, ex. äldre HPE Aruba switchar har den möjligheten.

Ett CDP paket skickas var 60 sekund som ett L2 multicast meddelande ut på varje interface där CDP är påslaget. Per default är CDP påslaget på alla interface. `show cdp` visar hur ofta CDP-paket skickas. Timers kan konfigureras globalt med `cdp timer x` och `cdp holdtime x`.

Följande information finns i ett CDP-paket:

- Hostnamn enligt konfigurerad hostname
- IOS mjukvaruversion
- Hårdvaruförmågor, såsom routing, switching och bridging
- Hårdvaruplattform, ex. 2960, 9300
- Enhetens L3-adresser
- Namn på interfacet som CDP skickades via
- Duplex-information från interfacet som CDP skickades via
- VTP domän, om relevant
- Native VLAN, om relevant

CDP kan stängas av globalt med `no cdp run`. Det kan stängas av per interface med `no cdp enable`. Det går att att stänga av globalt och sen aktivera på interface. `show cdp neighbors [ detail ]` visar information om grannar.

Link Layer Discovery Protocol (LLDP)

LLDP är inte propriärt och har implementerats hos många olika tillverkade, exempelvis hos andra nätverksfabrikat men återfinnes i nästan allt som har ett nätverkskort, såsom skrivare, mötesplattor och datorer. LLDP är definierad i IEEE standarden IEEE 802.1AB.

LLDP skickas över L2. LLDP-frames innehåller Type Length Value fält (TLVs). Följande är tvingande fält i TLVerna:

- Portbeskrivning
- Systemnamn
- Systembeskrivning
- Systemförmågor
- Management IP-adress

LLDP aktiveras genom globala kommandot `lldp run` och sedan `lldp receive` och/eller `lldp transmit` i interface-konfigurationsläge. Timers kan konfigureras globalt med `lldp holdtime x`, `lldp reinit x` och `lldp timer x`.

Verifieringar kan ske med ex. `show lldp`, `show lldp interface` och `show lldp neighbors`.

Revision #1

Created 26 April 2025 11:56:52 by Jehrlander

Updated 26 April 2025 11:56:56 by Jehrlander