Ongelmallinen Ethernet

Kari Seppänen
Kari.Seppanen@vtt.fi

Sisältö

- Johdanto
- Mikä Ethernet oikeastaan on?
- Toimisto-Ethernet
- Skaalautuvuus, vikasietoisuus ja tietoturva
- Spanning tree protocol -parannukset
- Hierarkkiaparannukset
- Käytännön ongelmia
- Tietoturvauhkat
- Suositukset
- Yhteenveto

Johdanto

- Ethernet:iä pidetään halpana tulevaisuuden siirtoverkkotekniikkana
- Sen oletetaan olevan luotettavaa, koeteltua ja helppokäyttöistä
- Ethernet-termi kätkee taakseen monta erilaista järjestelmää
  - reitittimien ja MPLS-kytkimien välitset linkit
  - Ethernet-palvelut, kuten E-Line ja E-LAN käyttäen esim. EoS tai EoMPLS -ratkaisuja
  - Ethernet-pohjaiset siirtoverkot
- keskitymme näistä viimeiseen

Mikä Ethernet oikeastaan on?

- Kytkentäistä Ethernettiä pidetään usein lähes verkkokerroksen tekniikkana
- Ethernet on kuitenkin linkkikerroksen tekniikka ja Ethernet-kytkimet eivät ole perinteisessä mielessä kytkimiä
  - jaettu siirtotie edelleen taustalla
  - monet apuprotokollat olettavat broadcast palvelun
  - Ethernet-kytkin $\sim$ moniporttinen silta tai joukko siltoja, joita yhdistää nopea sisäinen "kaapeli"
- Vaarallinen virhekäsitys: Ethernet voi korvata ATM:n tai MPLS:n suoraan

Toimisto-Ethernet

- Tarjoaa broadcast palvelun
- Siltojen (kytkimien) avulla verkko voidaan jakaa useaan "törmäysalueeseen" (collision domain)
- Ei-hierarkkinen osoitteistus $\Rightarrow$ sillan on opittava millä puolella kukin osoite on
- Verkossa ei saa olla silmukoita
  - MAC-oppiminen muuten mahdotonta
  - silmukkaan jääneiden pakettien tunnistaminen mahdotonta
- Spanning tree protocol (STP) huolehtii silmukoiden estämisestä
- Virtuaaliset LAN:t (VLAN) mahdollistavat liikenteen erottelun verkkosegmentin sisällä

Skaalautuvuus, vikasietoisuus ja tietoturva

- MAC-oppiminen: yhdessä verkkosegmentissä jokaisen sillan (kytkimen) on opittava kaikkien kohdekoneiden Ethernet MAC osoitteet
- STP toimii varman päälle: toipumisaika pahimmillaan muutamia minuutteja
  - Yksi vika vaikuttaa koko verkkosegmenttiin
  - Vika kytkimien välisissä linkeissä vaatii opittujen MAC-osoitteiden unohtamisen
- Vikatilanteissa voi syntyä lyhytaikaisia silmukoita $\Rightarrow$ broadcast strom
- Verkon vapaata kapasiteettia ei hyödynnetä; juurisillan linkit pullon kauloina
- Etähallinta perustuu ylemmän kerroksen protokolliin
- VLAN ei takaa tietoturvaa: se on vain yksi suodatussääntö verkon toiminnan tehostamiseksi

Spanning tree protocol -parannukset

- Rapid STP (RSTP): jokainen silta voi käsitellä topologiamuutoksia
  - normaaleista linkkivioista toipuminen yleensä < 1s
  - kuollut juurisilta -tilanne; toipuminen pahimmillaan luokkaa 10s
  - nykyään osa päästandardia; ei kuitenkaan taaksepäin yhteensopiva
- Multiple STP (MSTP): verkossa voi olla ≤ 64 ST:a
  - vikojen vaikutukset rajoitetumpia
  - verkon kapasiteetin parempi hyödyntäminen
- Ethernet renkaat
  - Ethernet Automatic Protection Switching (EAPS), RRSTP
  - reduntantit kytkennät "aliverkkoihin"ongelmallisia

Hiearkkiaparannukset yms.

- Provider bridges (PB) perustuen VLAN stacking:in (Q-in-Q)
  - MAC-oppiminen edelleen ongelmana
- Provider backbone bridges (PBB), MAC-in-MAC
- Provider backbone transport (PBT): Ethernet ilman MAC-oppimista
- Hallittavuus:
  - Ethernet local management interface (ELMI)
  - Connectivity fault management (CFM), Eth.OAM
  - Suoritustason seuranta (performance monitoring) puuttuu IEEE:n määrittelyistä

Käytännön ongelmia

- Fail open -käytös
  - ylikuormitustilanteessa kytkin taantuu toistimeksi ⇒ VLAN-määrittelyt yms. menettävät tehonsa
  - broadcast liikenne kasvaa ⇒ suorituskyky laskee
- Yksinkertaiset hallintamodulit
  - monoliittinen hallintaohjelmisto: helppo tehdä DoS-hyökkäys
  - ei muistinsuojauksia ⇒ taulukoiden ylikirjoittaminen
- Kloonatut MAC-osoitteet ⇒ MAC-rewrite tarvitaan tilaajaverkoissa
- Epäyhteensopivat STP-toteutukset
- Tunnettuja bugeja
- ”Kaikki auki kaikille” -oletusasetukset

Tietoturvauhkat

- Kytkimeksi tekeytyminen (STP, CDP, DTP, HSRP, VTP, 802.1q, 802.1x, ISL)
  - kaiken liikenteen kierrättäminen oman koneen kautta
  - VLAN:ien muuttaminen
  - DoS, jne.
- MAC flooding: kytkimen pakottaminen fail open -tilaan
- Apuprotokollien heikkoudet: ARP spoofing, DHCP spoofing
- Valmiit työkalut kaikkien saatavilla
  - Yersinia, dsniff, THC-Parasite
  - SSH ja SSL -yhteyksien MiM -hyökkäykset

Suositukset

- Asiakkaan ja operaattorin Ethernet-laitteiden välillä ei ikinä saisi olla kytkinta-son peering -yhteyttä
  - Vähintään STP, CDP, yms. disabloitava
  - Jos halutaan tukea asiakkaan VLAN:ja, pitäisi käyttää esim. PB (Q-in-Q) tai VLAN:t konfiguroitava manuaalisesti
  - ...toisaalta — kuinka sitten estetään tahalliset tai tahattomat silmukat?
- Vain PBB (MAC-in-MAC) tai PBT turvaavat siirtoverkon MAC-tulvitukselta
- Kattava hallinta
  - STP:n toiminnan aktiivinen seuranta
  - toimiviksi havaittujen ja turvallisten oletusarvojen ajaminen laitteisiin ennen asennusta
  - ELMI:n, CFM ja/tai Eth.OAM käyttöönotto
  - Laitevalmistajien turvallisuuslaajennukset eivät yleensä skaalaudu

Yhteenveto

- Ethernet-tekniikkaa käyttäen voidaan periaatteessa rakentaa siirtoverkko
  - Vaatii huolellisen suunnittelun
  - Tiukka hallinta- ja käyttöönottokuri
  - Uusimmat laajennukset (hierarkkia ja hallinta) käyttöön
- Ei ole enää plug-and-play; katoavatko kustannusedut
- Huolimattomasti rakennettu ja ylläpidetty verkko antaa mahdollisuudet
  - Estää tai muuttaa verkon toimintaa
  - Vakoilla tai muuttaa muiden asiakkaiden liikennettä
- Ilman kunnon hallintaa vikojen paikannus hankalaa

Kysymyksiä?