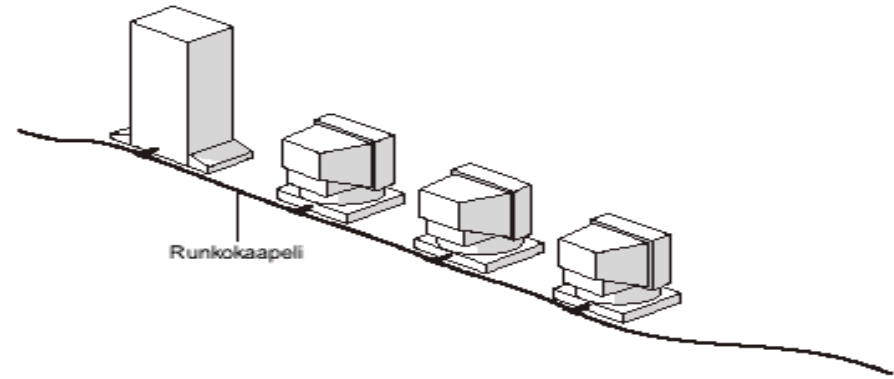


VERKKOTOPOLOGIAT

Verkkotopologialla tarkoitetaan tietokoneverkon perusrakennetta eli tapaa jolla verkon laitteet on liitetty toisiinsa. Verkon perustopologiat ovat väylä, rengas ja tähti.

Fyysisellä topologialla tarkoitetaan sitä, miten koneet on fyysisesti liitetty toisiinsa kaapeleilla. Fyysinen rakenne ei ota kantaa siihen, miten paketit liikkuvat johdoissa. Kun verkon rakennetta aletaan tarkastella siinä liikkuvien pakettien kannalta, tulee eteen verkon looginen rakenne. Verkon fyysinen rakenne voi olla erilainen kuin sen looginen rakenne.

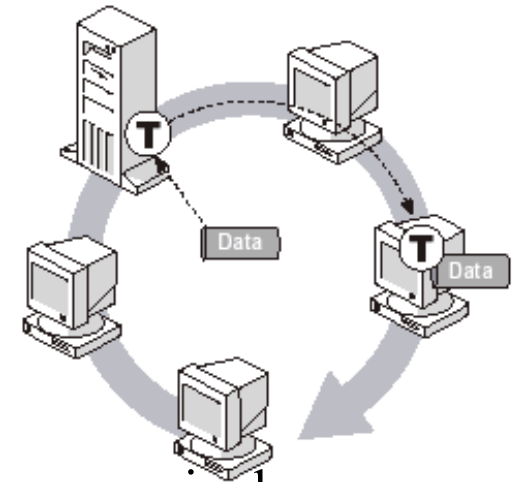
VÄYLÄ



Väylätopologia on vanhin käytössä olevista topologioista. Siinä verkon laitteet on kytketty yhteen yhdistävään kaapeliin, jonka molemmat päät on kytketty terminattoriksi kutsuttuun vastukseen. Esimerkiksi 10Base2 ja 10Base5 ovat väylätyyppisiä verkkoja, joita ei enää rakenneta.

Väylätopologian heikkous on siinä, että sen käyttö perustui kilpavarausmenettelyyn (CSMA/CD), jolloin verkkoa saattoi käyttää vain yksi laite kerrallaan ja jokainen laite joka yritti liikennöidä verkossa yhtä aikaa jonkin toisen laitteen kanssa aiheutti törmäyksen ja ruuhkautti verkkoa. Näin ollen laitteiden määrä oli rajattu. Väylärakenteessa kaikki verkossa olevat koneet saavat sanoman samaan aikaan. Kaapelina käytetään joko koaksiaali- tai valokuitukaapelia. Väylärakenteen ongelmana on, että mikäli kaapeli menee epäkuntoon, on verkko tämän jälkeen kahdessa osassa ja lakkaa toimimasta.

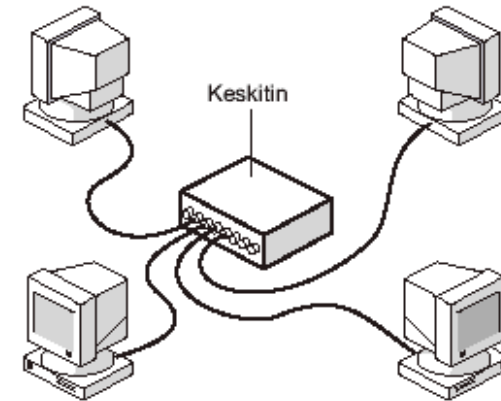
RENGAS



Rengastopologiassa verkosta on muodostettu fyysinen rengas, jonka jokaisessa solmussa on verkkolaite. Verkkolaitteet on yhdistetty verkkoon MAU-yksiköllä (Multistation Access Unit). Tunnetuin esimerkki rengasverkosta on IBM:n Token Ring -verkko, joka on toteutettu fyysisenä tähtenä IBM:n kaapelointijärjestelmällä, joka kytkeytyy renkaaksi. Token Ring -verkkoja ei enää kehitetä, sillä ne eivät olleet kilpailukykyisiä Ethernet-tekniikan kanssa.

Rengasrakenteisessa verkossa kullakin asemalla on kaksi naapuria. Toiselta asemalta saadaan sanoma ja toiselle lähetetään. Vain yksi asema kerrallaan saa sanoman. Token on itse asiassa valtuus puhua (eng. token = valtuus), eli verkossa kiertää ns. token, jonka haltijakone saa puhua, jolloin muut koneet eivät lähetä mitään. Jos koneella ei ole mitään lähetettävää, token siirtyy seuraavalle koneelle. Token kiertää aina myötäpäivään.

TÄHTI

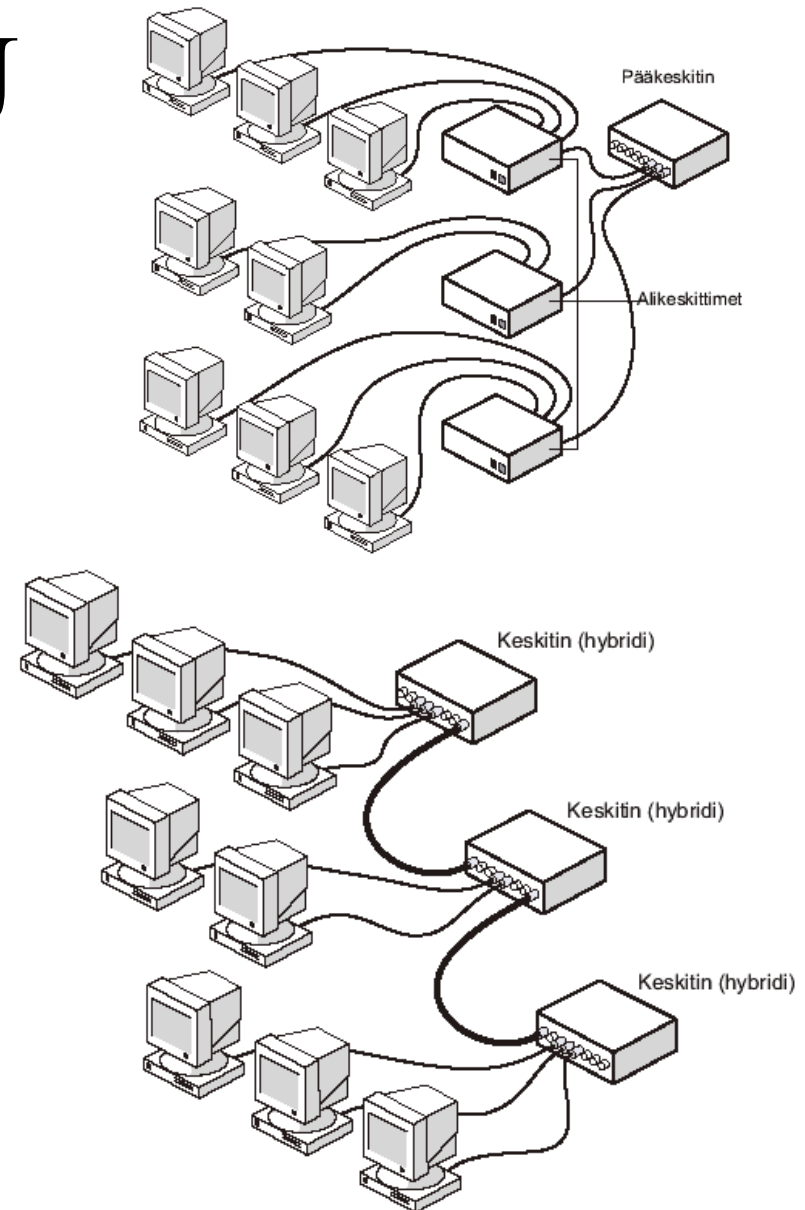


Tähtitopologiassa on keskuslaite, kuten kytkin tai keskitin, johon verkkolaitteet on kytketty. Verkon kaikki tietoliikenne kulkee keskuspuolesta kautta. Kytkin/keskitin on yleensä kytketty joko toiseen kytkimeen tai reitittimeen, josta yhteys jatkuu toisille laitteille. Keskitimien käyttö on vähenemässä, sillä ne kaiuttavat kaiken liikenteen jokaiseen keskitimessä kiinni olevaan verkkolaitteeseen, jolloin liikenne voi ruuhkautua. Kytkin puolestaan ohjaa datan vain siihen osoitteeseen jonne se on tarkoitettu, joten verkko ei ruuhkaudu datapakettien törmäyksistä.

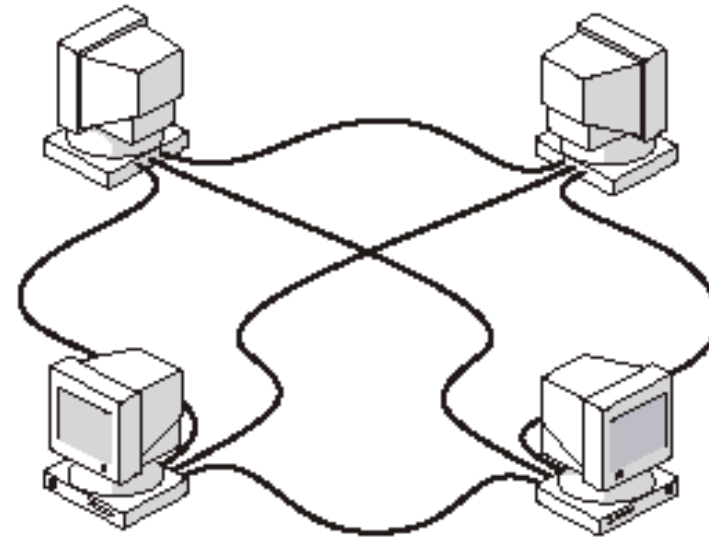
Tähtitopologia on yleisin käytössä olevista Ethernet-verkkotopologioista. Tähtirakenteen huomattava etu on ettei yhden kaapelin rikkoutuminen vaikuta muun verkon käyttöön. Esimerkkinä tähtirakenteisesta verkosta voidaan mainita tavallinen lankapuhelinverkko.

LAAJENNETTU TÄHTI

Laajennettu tähti yhdistää yksittäiset tähdet toisiinsa ja lisää tähtitopologiaan hierarkian käsitteen. Sitä käytetään erityisesti tiukkaa laitehierarkiaa vaativien reititysprotokollien (kuten esimerkiksi OSPF:n) yhteydessä.



MESH



Mesh-topologiassa jokainen tietokone on yhdistetty kaikkiin muihin tietokoneisiin erillisellä kaapelilla. Topologia on usein käytännöllinen langattomissa verkoissa.

OSI-mallit

		Network Devices	Models	Memory rule
Layer 7	Application	Gateway	telnet, SMTP, POP3,IMAP4, HTTP	A
Layer 6	Presentation	Gateway	translation, data encryption	P
Layer 5	Session	Gateway	connecting, establishing, monitoring, terminating	S
Layer 4	Transport	Gateway	TCP, UDP, <i>telnet</i>	T
Layer 3	Network	Router, L3 Switches, Gateway	Ping, tracert, traceroute, pathping	N
Layer 2	Data Link	NIC, Bridges, L2 Switches, Access Point, Gateway	LLC, MAC, hosts, nodes	D
Layer 1	Physical	HUB, MAU, Repeater, Gateway	NIC, Network cabling, voltage and electrical signals	P

All **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing

7. **Sovelluskerros** (*Application layer*), jolle itse käyttäjälle näkyvät sovellukset sijoittuvat.
6. **Esitystapakerros** (*Presentation layer*), joka muuttaa tiedon käyttäjälle sopivaan muotoon, kuten kuvan pikseleiksi tai Unicode-tekstin kiinankielisiksi merkeiksi.
5. **Istuntokerros** (yhteysjakso, *Session layer*), joka huolehtii useiden yhdessä yhteydessä kulkevien istuntojen multipleksoinnista.
4. **Kuljetuskerros** (*Transport layer*), joka huolehtii siitä, että paketit tulevat perille ja että ne järjestetään oikeaan järjestykseen. Myös vuonhallinta on kuljetuskerroksen tehtävä.
3. **Verkkokerros** (*Network layer*), joka hoitaa globaalin reitityksen ja kohdekoneen löytämisen koko Internetistä.
2. **Siirtoyhteyserros** tai siirtokerros (*Data Link layer*), joka hoitaa paikallisen lähiverkon laitteiden välisen liikennöinnin.
1. **Fyysinen kerros** (*Physical layer*), joka käsittelee sähköimpulsseja, valoa tai muuta fyysistä tekniikkaa.

TULEVAISUUS

IPv6

IPv6 on nykyisen IP-protokollan (IPv4) seuraajaksi kehitetty protokolla. IPv6 tunnettiin varhaisessa kehitysvaiheessaan myös nimellä IPng eli IP next generation. Sen tärkein ero IPv4:ään on osoitteen pituus ja osoiteavaruuden laajuus. IPv6:ssa käytetään 128-bittisiä osoitteita, jolloin yhdessä verkossa voi olla yli 340 sekstiljoonaa ($340 \cdot 1036$) solmua, IPv4:n osoitteen pituus on 32 bittiä, ja IPv4-verkossa voi olla noin neljä miljardia (4–109) solmua.

IPv4-osoitteiden puute

Tärkein syy IPv6:n kehittämiseen oli nykyisin käytössä olevan IPv4-protokollan osoiteavaruuden pienuus. IPv4-osoitteiden loppumisesta on esitetty useita arvioita. Euroopassa IP-osoitteita hallinnoivan RIPEn vuonna 2007 esittämän arvion mukaan IPv4-osoiteavaruus loppuu vuoteen 2011 mennessä.

IPv4-osoitteiden loppumista on kyetty siirtämään käyttämällä osoitteenmuunnostekniikoita ja muuttamalla IP-osoitteiden jakamista tehokkaammaksi. Osoitteenmuutoksien avulla suurikin joukko koneita voi jakaa yhtä aikaa yhden IP-osoitteen. Toisaalta juuri osoitteenmuunnostekniikat vaikeuttavat monien uusien palvelujen, kuten IP-puheen tai vertaisverkkojen käyttöä. Osoitteiden jakamista on tehostettu jakamalla organisaatioille entistä sopivamman kokoisia osoitenippuja, mikä on vähentänyt käyttämättömien mutta varattujen osoitteiden määrää. Toisaalta myös muuttamalla verkkojen konfigurointi dynaamisemmaksi esimerkiksi DHCP-protokollan avulla on voitu kierrättää entistä pienempää määrää osoitteita niille jotka sitä sillä hetkellä tarvitsevat.

IPv6:n uusia ominaisuuksia

IPv6:ssa on pyritty siihen, että tietoliikenneverkon perustehtävä - pakettien välittäminen päätelaitteelta toiselle – on mahdollisimman yksinkertainen. Ylimääräisistä tarkistussummien laskemisesta on luovuttu.

Perus-IPv6:n ohella on kehitetty myös muita tekniikoita täydentämään IPv4:n puutteita:

IPsec on Internetin tietoturva-arkkitehtuuri, joka suojaa yhteyksiä salakuuntelulta ja väärinkäytöksiltä

Mobile IPv6 mahdollistaa Internet-laitteiden liikkumisen verkosta toiseen ilman, että yhteydet katkeavat

SSM (*Single Source Multicasting*) on tehokas ja skaalautuva tapa lähettää vaikkapa videolähetettä Internetissä monille vastaanottajille

Tilaton autokonfiguraatio (*stateless autoconfiguration*) on IPv6:n uusi tapa konfiguroida IP-laitteelle osoite ja muut asetukset automaattisesti ilman, että käyttäjän tarvitsee tehdä laitteelle muuta kuin kytkeä se verkkoon

Kaikki näistä tekniikoista on sovitettu myös nykyisen IPv4:n päälle. IPsec on saanut kohtalaisen hyvin suosiota etäkäytössä ja lähiverkkojen yhdistämisessä. Osa salaustarpeista ratkaistaan jo nyt SSL:llä.

MobileIPv6:n käyttö on vielä vähäistä. Osan liikkuvuuden hallinnasta pystytään toteuttamaan verkkokerroksen ratkaisuille (esimerkiksi GPRS).

SSM vaatii sitä, että kaikki reitittimet Internetin rungossa tukevat sitä. Operaattorit eivät ole kuitenkaan nähneet SSM:lle vielä olevan kysyntää eivätkä tue sitä.

Tilaton autokonfiguraatio on toteutettu IPv4:n yhteydessä APIPA-standardina (*Automatic Private IP Addressing*). Niin APIPA kuin IPv6 tilaton autokonfiguraatiokaan ei kykene konfiguroimaan kaikkia verkon ominaisuuksia, kuten DNS-palvelimia, joten automaattiseen konfigurointiin käytetty protokolla DHCP tulee olemaan edelleen tarpeellinen IPv6:n kanssa.