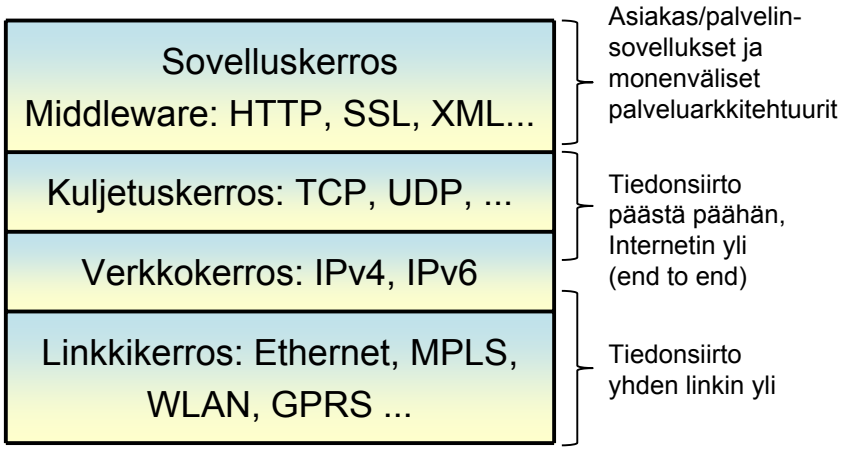
Verkkokerros ja Internet-protokolla

Matti Siekkinen

T-110.2100 Johdatus tietoliikenteeseen
kevät 2010

TCP/IP-protokollapino



Viime luennolla…

- Kuljetuskerros tarvitaan yhdistämään sovelluksia verkon yli
  - Monia aktiivisia sovelluksia yhtäaikaa päätelaitteen sisällä
- Erityyppisiä palveluita
  - UDP: epäluotettavan viestinvälitys
  - TCP: luotettavan tavuvirta

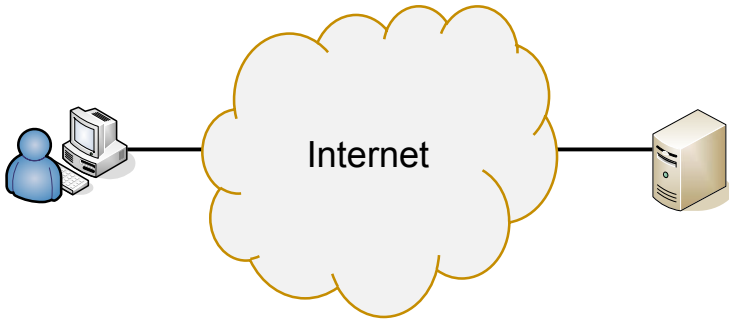
Sisältö

- Verkkokerroksen tehtävä ja ominaisuudet
- Internet-protokolla
  - Osoitteet
- NAT
- DHCP
- ICMP
- Reititin ja reititys

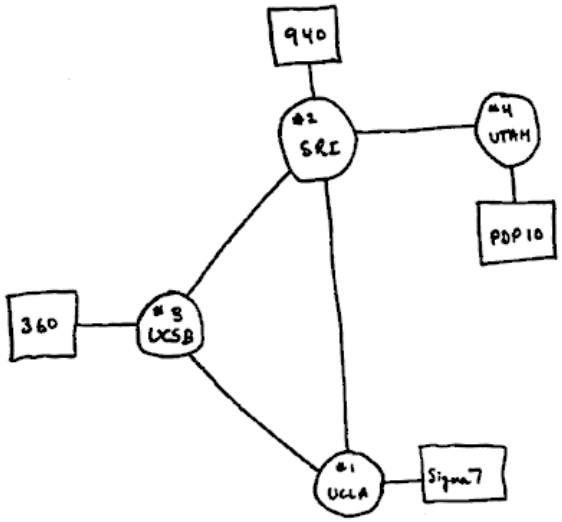
Tämän luennon jälkeen…

- Ymmärrätte:
  - Verkkokerroksen tehtävän ja toiminnan
  - Internetin verkkokerroksen toiminnan
    - Internet protokolla
    - DHCP, NAT, ICMP
  - Mikä on reitin ja mitä se tekee
- Tiedostatte:
  - Mitä reititys on
  - Internetin globaalin rakenteen

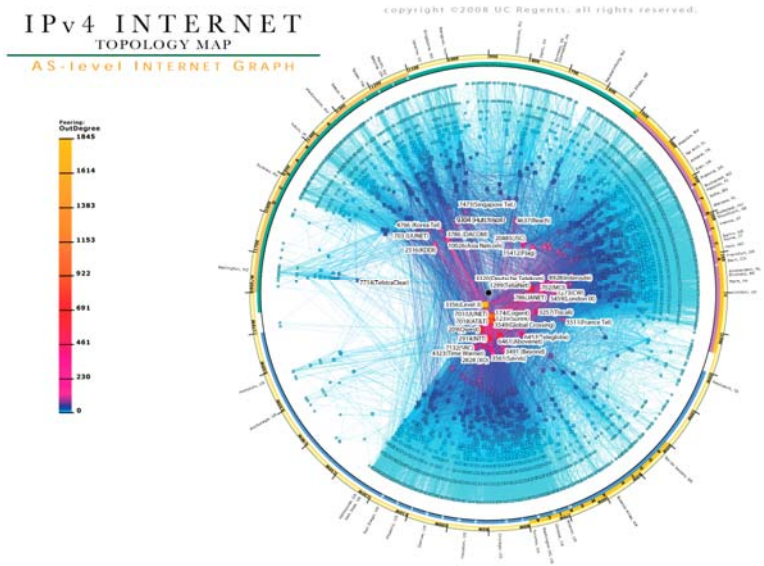
Mikä toi pilvi on?



ARPANET 1969

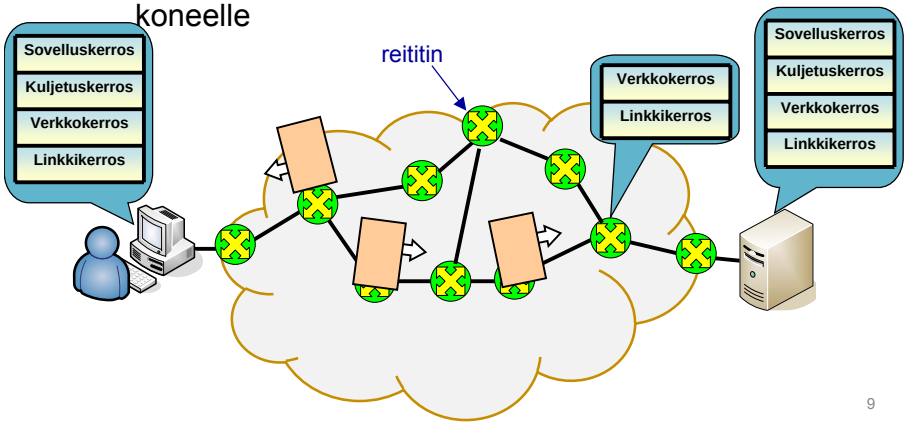


Internet 2008



Verkkokerroksen tehtävä

- Mahdollistaa päätelaitteiden yhdistämisen
- Liikuttaa dataa pisteestä toiseen
  - Useiden erilaisten fyysisten kerrosten ylitse koneelta koneelle



Verkkokerroksen ominaisuuksia

- Pakettikytkentä eli pakettien välityspalvelu
- Myös verkkokerros voi tarjota erilaisia palveluita
  - Luotettava tai ei, min. kaistanleveys, max. viiveen vaihtelu (jitter), tiedonsalaus, etc.
- Virtuaalipiiri (virtual circuit) vs. datagrammi
  - Virtuaalipiiriverkko tarjoaa yhteydellisen palvelun
    - Yhteyden muodostus (virtuaalipiiri) ennen datan lähetystä
    - Hyvää: helpompi toteuttaa parempi palvelu (esim. max jitter)
    - Huonoa: reitittimet joutuvat pitämään lukua yhteyksistä
    - Esim. ATM ja x.25
  - Datagrammiverkko tarjoaa yhteydettömän palvelun
    - Paketteja liikutellaan kohdeosoitteen avulla
    - Reitittimet ei joudu pitämään tilaa yhteyksistä (niitä ei ole!)
    - Esim. Internet Protokolla (IP)
- Tällä luennolla käsitellään jatkossa vain IP:aa

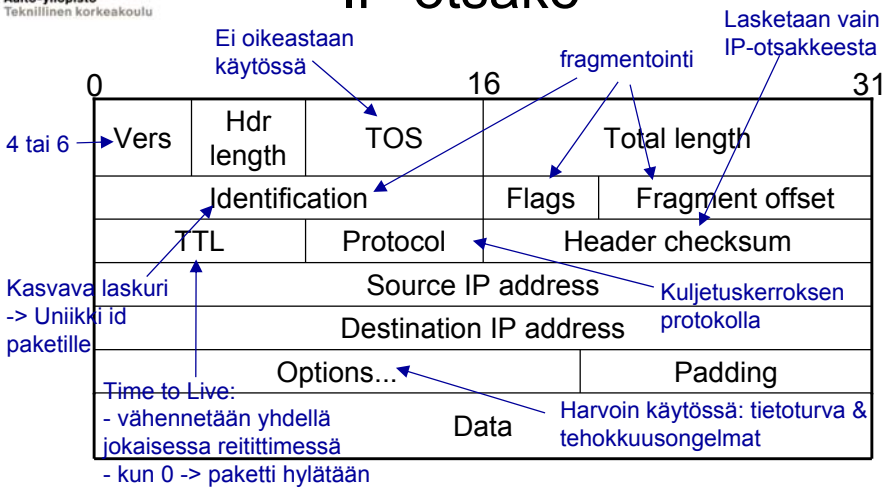
Internetin verkkokerros

- Internet-protokolla (IP) toteuttaa Internetin verkkokerroksen
  - Epäluotettava ja yhteydetön välityspalvelu
    - "best effort"
  - IP tuo datan päätelaitteeseen, kuljetuskerros välittää sen oikealle sovellukselle
  - Kuljetuskerroksen segmentti paketoidaan IP-paketin sisälle
    - Lisätään IP-otsake
- Jokaisella päätelaitteella on IP-osoite
  - Osoiteavaruus on globaali

IP

- Internet Protocol
- Alunperin määritelty standardissa RFC 791
- Se tarjoaa **epäluotettavan** ja **yhteydettömän** palvelun
  - Viestin perillemenoa ei varmenneta
    - Lähettäjä saa virheilmoituksen vain jos IP-kerros ei tiedä miten toimittaa viesti perille
    - Esim. jos reitittimen puskurimuisti on täynnä, tuleva data vain hylätään
  - Reitittimet käsittelevät jokaisen IP-paketin erikseen
- Tällä kurssilla IP-protokollan versio 4
  - IPv6 on tulossa hitaasti käyttöön
  - Olennaisin parannus on suurempi osoiteavaruus

IP-otsake



Fragmentointi

- Linkkikerroksella usein maksimikoko siirrettävälle segmentille
  - Vaihtelee eri tyyppisillä linkkikerroksilla
- Mitä tehdään, jos IP-paketin lähettäjä lähettää 64 kB paketin ja vastaanottajan kokorajoitus on 1,5 kB?
  - Vastaus: Fragmentointi
- Reititin jakaa paketin osiin (fragmentit) ja lähettää ne erillisinä IP-paketteina
- Vastaanottaja kokoaa taas yhdeksi IP-paketiksi

Fragmentointi

- Tehokkuusongelmat
  - Pitää lähettää enemmän otsakkeita (overhead)
    - Riippuu valitusta fragmentin koosta
  - Vastaanottaja puskuroi vastaanotetut palaset kunnes voidaan kasata koko paketti
  - Kaikki paketin palaset pitää uudelleenlähettää jos yksittäinen palanen katoaa
- Myös tietoturvaongelmia
  - Palvelunestohyökkäys väärinrakennetuilla fragmenteilla
    - Jolt2 hyökkäys
- Pyritään välttämään
  - Selvitetään ennemmin suurin sallittu segmentin koko

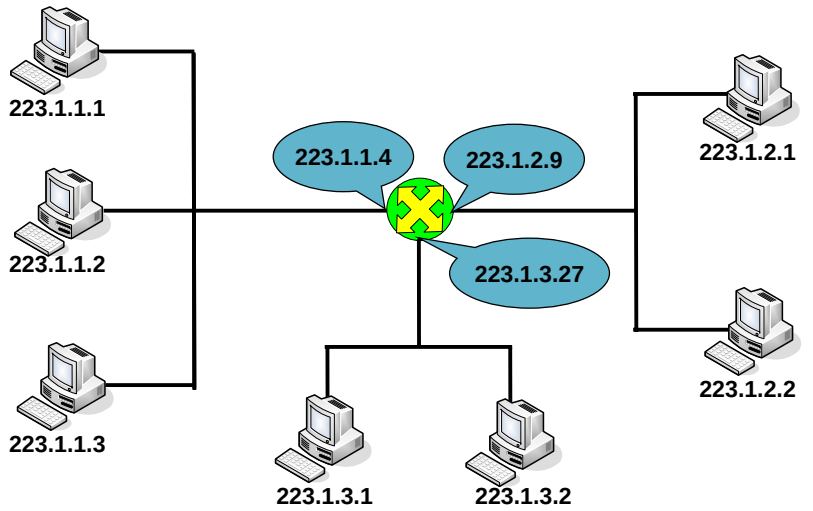
Path MTU Discovery

- Fragmentoinnin välttämiseksi selvitetään suurin sallittu IP-paketin koko
- Lähetetään suurehko IP-paketti, jossa on "Don't Fragment" -lippu päällä
  - Reititin vastaa "Fragmentation Needed" viestillä
  - Etsitään sopiva koko toistamalla pienemmillä paketeilla
- Ethernetissä MTU on 1500 tavua
  - Usein rajoittava tekijä kun jompikumpi osapuoli on Ethernet-verkossa
  - WiFi MTU on suurempi (>2Kt)

IP-osoitteet

- IP-osoite on verkkoliittymän (interface) tunniste
  - Päätelaitteella voi olla useita samanaikaisia verkkoliittymiä
    - Reitittimet
    - Luotettavuus (eräänlainen multihoming)
    - Erilaiset linkit (esim. kännykän WLAN, UMTS)
- IPv4-osoitteet ovat 32-bitin mittaisia
  - IPv6 tarjoaa 128-bitin osoitteet
- 4 pisteiden erottamaa tavua desimaalinumeroina
  - Esim: 130.233.240.9
- Alkuosa osoitteesta kertoo verkon (network prefix), loppuosa viittaa koneeseen verkossa (host id)
  - Esim. lähiverkko tai yrityksen koko verkko
  - Reitittimet välittävät paketteja verkko-osan perusteella

IP-verkko ja osoitteet



IP-verkko ja osoitteet

- Nykyään yleisin tapa kuvata verkko on CIDR
  - Classless Inter-Domain Routing
  - Aiemmin oli käytössä osoiteluokat eri kokoisille organisaatioille
- Kerrotaan verkko-osoite ja merkitsevien bittien määrä
  - Esim. 130.223.0.0/16 on TKK:n verkko runkoverkon tasolla
    - Kaikki 130.223 -alkuisiin osoitteisiin matkaavat paketit ohjataan tässä verkossa
  - Raja on bitteinä, ei tavuina

IP-verkko ja osoitteet

- TKK:n verkon sisällä voi olla aliverkkoja, esim. 130.223.236.0/22
  - *Verkkomaski* (netmask) tässä on 255.255.252.0

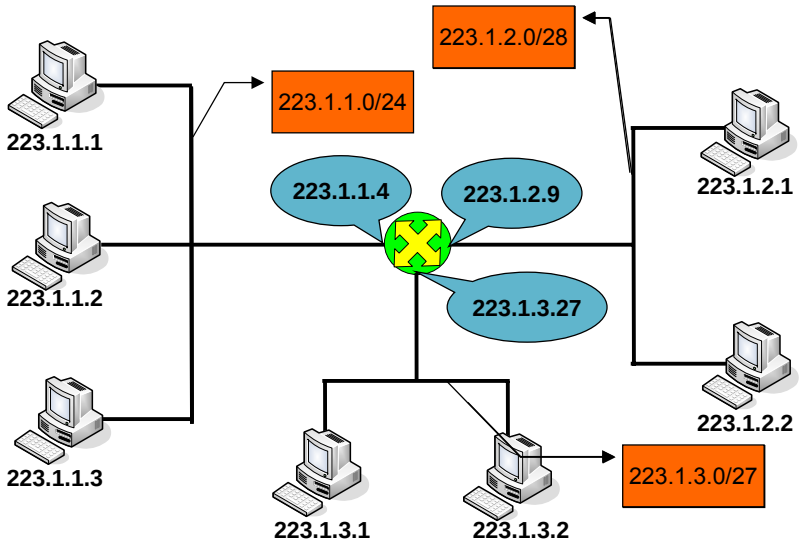
130.223.236.0	10000010 11011111 11101100 00000000
verkkomaski	11111111 11111111 11111100 00000000
130.223.236.0/22	10000010 11011111 111011

  - Osoitteet 130.223.236.0-130.223.239.255 kuuluvat tähän verkkoon
- Onko 130.223.237.0/22 toimiva aliverkko? Ei.

Sama!

130.223.237.0	10000010 11011111 11101101 00000000
verkkomaski	11111111 11111111 11111100 00000000
130.223.237.0/22	10000010 11011111 111011

IP-verkko ja osoitteet



Erityiset osoitteet

- 0.0.0.0
  - Mikä/kuka tahansa (any)
  - Lähettäjällä ei ole vielä IP-osoitetta
- 255.255.255.255
  - Paikallinen yleislähetys (broadcast)
- Koneen osoite -osan kaikki bitit 1
  - Verkon yleislähetys
  - Esim. 222.1.16.255/24
- 127.*.*.*
  - Loopback, viittaa ko. liittymään
  - Yleensä. 127.0.0.1
  - Erittäin käytännöllinen
    - Asiakas ja palvelin samassa päätelaitteessa

```
#38640 +(911)- [X]
<Myren> someone ping flood this bastard please: 127.0.0.1
<darthv> ok
*** darthv has quit IRC (Ping timeout)
```


Yksityiskäyttöön varatut osoitteet

- Tietyt osoitteet on määritelty vain paikalliseen käyttöön
  - 10.0.0.0/8
  - 192.168.0.0/16
  - 172.16.0.0/12
- Runkoverkko kieltäytyy reitittämästä niitä
  - Voi käyttää vapaasti, mutta niistä ei voi viestiä (suoraan) Internetiin
  - Käytetään lähiverkoissa
    - julkisen verkon IPv4 osoitteista on pulaa
- Liikennöinnin Internetiin mahdollistaa NAT (Network Address Translation)

NAT

- Network/Port Address Translation (NAT/PAT)
- Reitittimellä yksi (tai muutama) julkinen IP-osoite ja sisäverkossa yksityisosoitteita
  - Yksityisosoitteet vaihdetaan julkisiin reitittimessä ja päinvastoin
  - Reititin pitää kirjaa yksityinen ↔ julkinen osoite (ja portti) kuvauksesta
  - Nyt reitittimessä on verkkoyhteyden tila

NAT

- IP-paketin muuttuminen matkalla

	lähdeosoite	Lähdeportti	Kohdeosoite	kohdeportti
1	**10.0.0.2**	**8890**	**130.233.9.10**	**80**
2	**194.197.18.3**	**3498**	**130.233.9.10**	**80**
3	**130.233.9.10**	**80**	**194.197.18.3**	**3498**
4	130.233.9.10	80	10.0.0.2	8890

NAT:n huono puoli

- Internetistä ei voi aloittaa yhteyttä NATin taakse
  - Kiinteä NAT-muunnos saa NATin takana olevan palvelimen näkymään julkiseen verkkoon
- Kaksi NATin takana olevaa päätelaitetta eivät pysty viestimään keskenään ilman apua
  - Ratkaisuina STUN, ICE, TURN
  - Pyritään tunnistamaan NAT:n toimintatapa
    - Esim. viestimällä STUN-palvelimen kanssa
  - Viimeisenä konstina välityspalvelin eli relay (TURN)
    - Molemmat päätepisteet ottavat yhteyden palvelimeen

Miten IP-osoite saadaan?

- Blokki osoitteita
  - Internet-yhteydentarjoajalta (ISP)
  - ICANN hallinnoi globaalisti
  - Kohta ei mistään kun ne loppuvat...
- Yksittäisen päätelaitteen osoite
  - Manuaalisesti konfiguroimalla
  - Dynamic Host Configuration Protocol (DHCP)
    - Erittäin käytännöllistä (esim. läppärit)

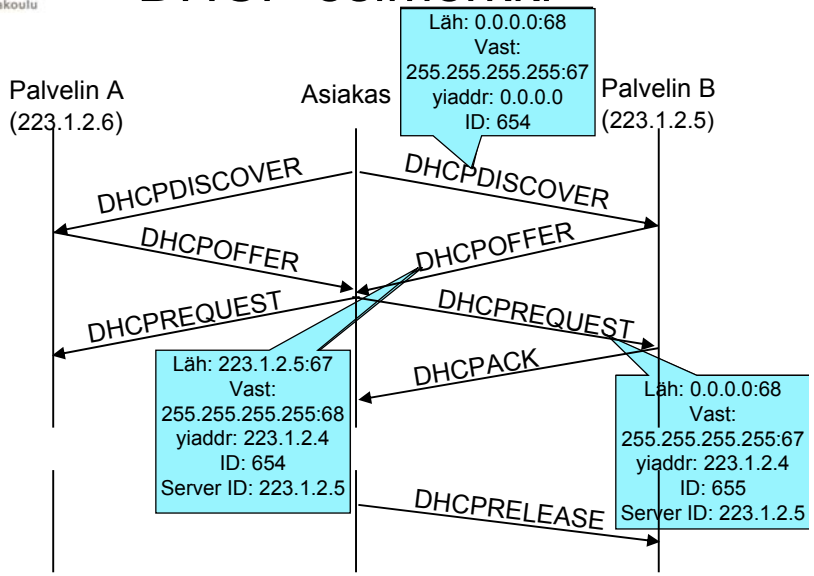
DHCP

- Dynamic Host Configuration Protocol
  - Automaattinen IP-osoitteiden jakelu lähiverkossa
- Eri toimintatapoja
  - Staattinen allokointi
    - Pysyvät IP-osoitteet asiakkaan MAC-osoitteen perusteella
    - Vaatii manuaalisesti MAC-osoitteiden konffaamisen serverille
  - Automaattinen allokointi
    - Ei manuaalista MAC-osoitteiden konffaamista
    - Ensimmäisen kerran jälkeen staattinen allokointi
  - Dynaaminen allokointi
    - IP-osoitteet täysin dynaamisesti poolista
    - Sama asiakas voi saada joka kerta eri osoitteen
- Edellyttää palvelimen tai proxy-palvelimen lähiverkkoon
- RFC 2131, 2132

DHCP

- Viestit kapseloitu UDP:nä IP:n yli
  - Palvelin portissa 67, asiakas portissa 68
- Palvelin löydetään yleislähetyksellä
  - Ensimmäinen paketti osoitteeseen 255.255.255.255 osoitteesta 0.0.0.0
- Viestityypit
  - DISCOVER, OFFER, REQUEST, DECLINE, ACK, NAK, RELEASE
- Palvelin antaa lähiverkon työaseman tarvitseman perusinformaation
  - IP-osoite, verkkomaski, yhdyskäytävä
  - DNS-palvelimen osoite
  - Yms.

DHCP esimerkki



ICMP

- Internet Control Message Protocol
- RFC 792
- Yksinkertainen viesti IP-paketin sisällä
  - Luodaan IP-kerroksella
  - Kahden koneen IP-kerroksien, ei sovelluksien, välillä
  - Viestin ilmoitus usein kuitenkin välitetään sovellukselle
- Toteuttaa
  - Verkon virheilmoitukset
  - Ping
  - Traceroute
- Turvasyistä käyttö usein rajoitettu
  - Esim. yhteyden kaappaus tai DoS perustuen "Route redirect", "router advertisement" -viesteihin
  - Pelkkä ping mahdollistaa verkon koneiden kartoituksen

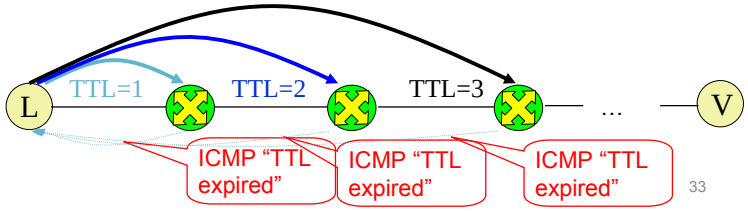
ICMP-viesti

Type	Code	Checksum
Data		

- Type määrittelee viestin: echo request, echo reply, destination unreachable, jne.
  - Esim. Ping = ICMP ”echo request” + ICMP ”echo reply”
- Code määrittelee syyn: host unreachable, port unreachable, jne.
- Data sisältää virheviesteissä virheen aiheuttaneen IP-paketin oleelliset osat

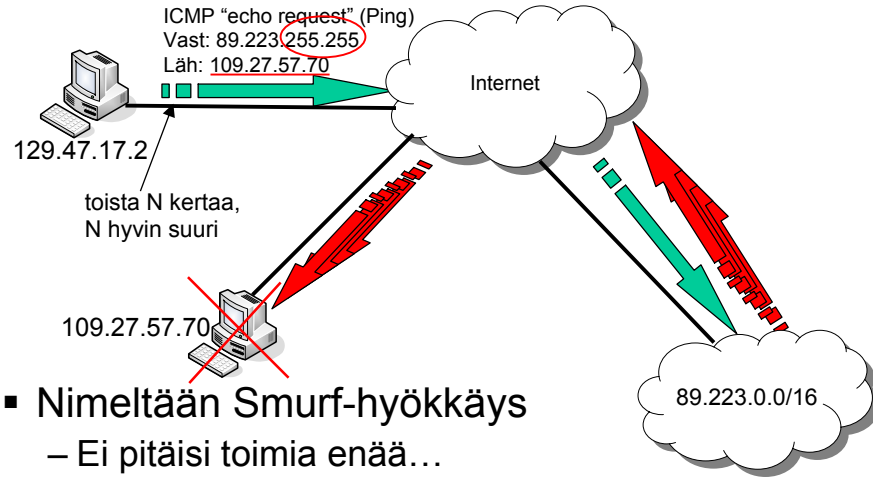
traceroute

- Mahdollistaa IP-tason polun selvittämisen
- Lähettäjä lähettää UDP-segmenttejä
  - Kohdeosoite on polun päätepiste
    - Kohdeportiksi joku epätodennäköisesti auki oleva
  - Aluksi TTL=1, kasvatetaan yhdellä peräkkäisissä segmenteissä
  - Myös ajastin käynnistetään jokaista segmenttiä lähetettäessä
- Kun TTL=0
  - Reititin hylkää segmentin
  - Lähettää ICMP TTL expired viestin lähettäjälle
- ICMP viestit paljastavat polun reitittimien osoitteet ja viiveen



ICMP esimerkki

- Mitä tapahtuu?



- Nimeltään Smurf-hyökkäys
  - Ei pitäisi toimia enää…

Reititys

- Verkossa useita vaihtoehtoisia reittejä pisteiden välille
  - Vikasietoisuus
  - Sopimukset liikenteen siirtämisestä ISP:n välillä
- *Reititys:* Polkujen löytämistä osoitteesta toiseen
- *Reititysprotokolla:* Tapa jolla reitittimet vaihtavat tietoa verkon tilasta ja tarjoamistaan osoitteista
- *Reititystaulu:* Reititysprotokollan avulla selvitetty tieto osoitteiden sijainneista

Reititin

- Kaksi tehtävää:
  - Reititys
    - Ei välttämätöntä
      - Esim. manuaalisesti konfiguroitu reititystaulu
  - Edelleenlähetys (Forwardointi)
    - Siirretään paketti sisääntulevasta portista ulosmenevään (linkistä toiseen)
      - Reititystaulun perusteella
      - Prefix-haku
    - Tehdään siis jokaiselle paketille
    - Erittäin aikakriittinen tehtävä
      - Miljoonia paketteja sekunnissa nopeissa reitittimissä

Prefix-haku (lookup)

- Kohdeosoitetta verrataan reititystaulun sääntöihin

Destination	Next Hop
200.223.0.0/16	R2
200.16.0.0/13	R4
200.22.0.0/15	R1

Kohdeosoite: 200.223.146.51

- *Longest prefix matching rule*
  - Aina haetaan pisin soveltuva sääntö reititystaulusta

Longest Prefix Matching Rule

Destination	Next Hop
200.223.0.0/16	R2
200.16.0.0/13	R4
200.22.0.0/15	R1

- Mihin tämä paketti lähetetään?

Kohdeosoite on: 200.23.146.51

11001000 00010111 10010010 00110011

Miksi longest prefix matching?

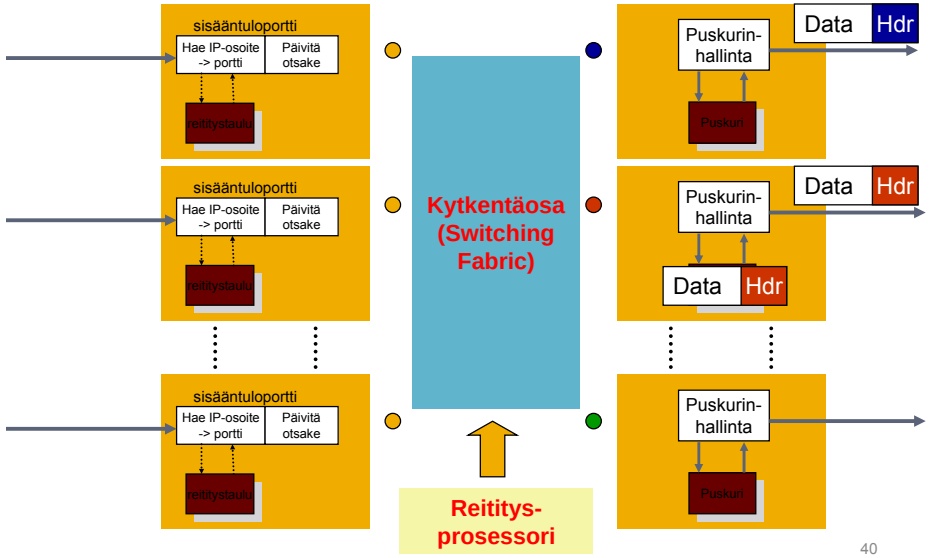
- Vastaus on route aggregation (a.k.a. address aggregation)
  - Voidaan esittää useita aliverkkoja yhdellä säännöllä

Destination	Next Hop
10.1.0.0/24	R3
10.1.2.0/24	direct
10.2.1.0/24	direct
10.3.1.0/24	R3
20.2.0.0/16	R2
20.1.1.0/28	R2

Destination	Next Hop
10.1.0.0/24	R3
10.1.2.0/24	direct
10.2.1.0/24	direct
10.3.1.0/24	R3
20.0.0.0/8	R2

- Vähennetään reititystaulujen kokoa

Reitittimen arkkitehtuuri



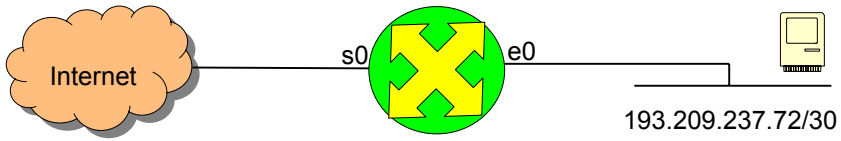
Reititin

- Haasteita suunnittelussa
  - Mikä on oikea puskurien koko?
    - Viime aikoina ymmärretty ettei vieläkään tiedetä ☺
    - Liian suuret:
      - Kallista
      - TCP ei reagoi
        - » Mieti esim. liian vetelä auton jousitus
    - Liian pienet:
      - TCP reagoi heti -> turhan paljon uudelleenlähetyksiä
  - Suuret nopeusvaatimukset
    - Prefix-haku pitää olla todella nopeaa
    - Useita eri ratkaisuja keksitty esim. kytkentäosioon
    - Optiset reitittimet myös tulossa...

Staattinen reititys

- Työasemissa ja verkon reunareitittimissä reititystaulu on usein staattinen
  - Reitityksprotokollia ei käytetä
  - Eli ei oikeastaan reititystä ollenkaan
- Forwardointi
  - Työasema vertaa lähtevän paketin kohdeosoitetta omaan osoitteeseen verkkomaskin puitteissa
  - Reunareititin (esim. kotiverkossa) tietää lähiverkon verkko-osoitteet ja ohjaa kaiken muun oletuslinkille (default)

Esimerkki: kotiverkko



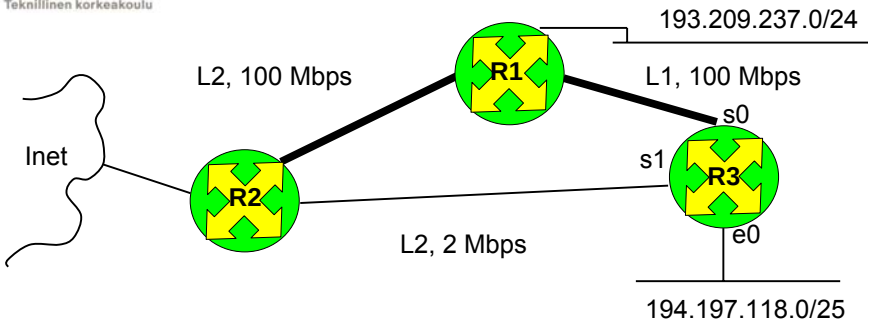
- Tyypillinen pieni kotiverkko
- Reititystaulu:

Destination	Next hop	Comment
193.209.237.72/30	e0	Local LAN (Ethernet)
*	s0	WAN (default route)

Dynaaminen reititys

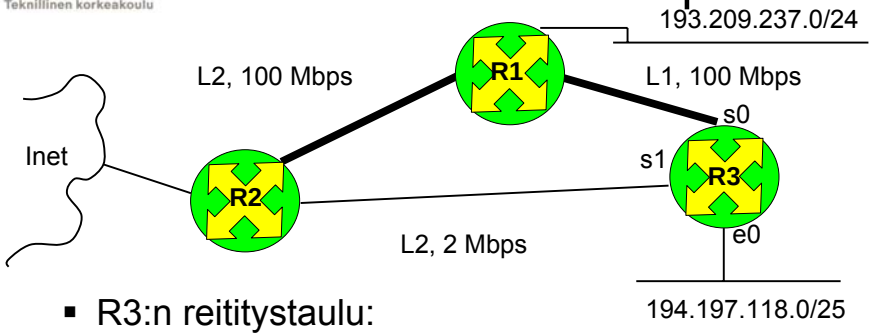
- Reitittimille asetetaan käsin paikalliset (lähi)verkot ja niiden osoiteavaruudet
- Reitittimet ”mainostavat” toisilleen omia verkkojaan
  - Reitityksprotokollat
- Vastaanotetusta tiedosta rakennetaan reititystaulu
  - Päivitetään jatkuvasti
- Protokollat käsitellään tarkemmin kurssilla T-110.4100 Tietokoneverkot

Toinen esimerkki



- Toimipisteellä on 100 Mbps linkki Internetiin toisen toimipisteen kautta ja 2 Mbps varalinkki

Vähän monimutkaisempi...



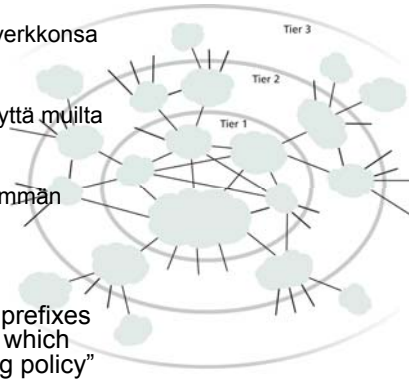
- R3:n reititystaulu:

Destination	Next hop	Cost	Comment
194.197.118.0/24	e0	0	Directly connected
193.209.237.0/24	s0	1	Fastest route
193.209.237.0/24	s1	10	Backup via R2
*	s0	1	Fastest route via R1
*	s1	10	Slower

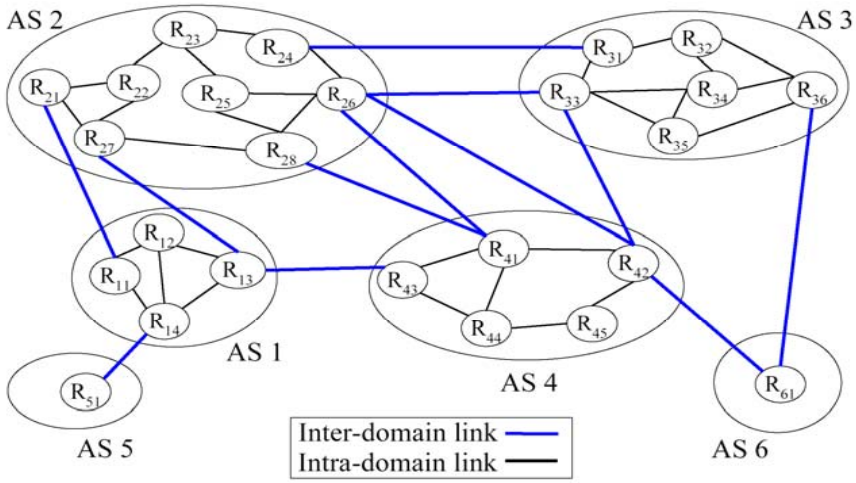
- "Cost" ei ole rahallinen kustannus vaan ohjaa priorisointia

Internetin rakenne

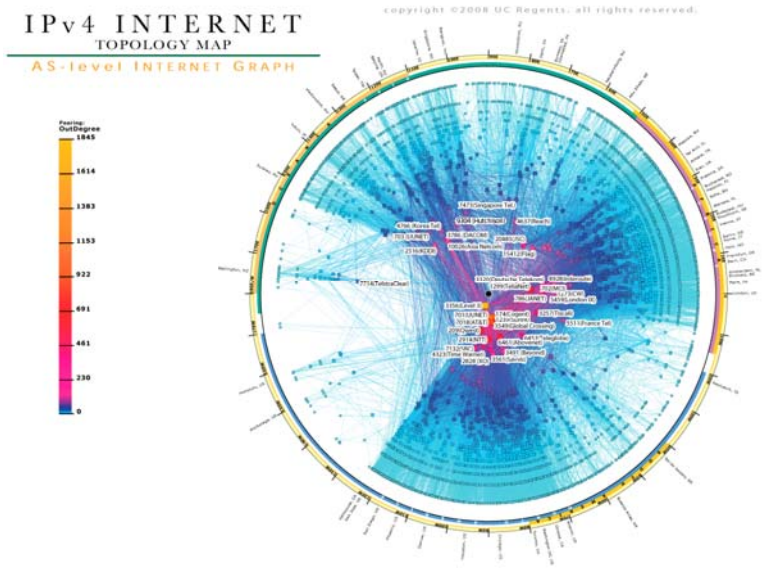
- Internet-yhteydentarjoajat (ISP) jaoteltu kolmeen luokkaan
  - tier 1: globaali
    - Vähän yli kymmenen kappaletta
    - Internetin "selkäranka" eli runkoverkko
    - Sallivat toistensa liikenteen maksutta verkkonsa kautta (a.k.a. settlement free peering)
  - tier 2: alueellinen
    - Myös peering, lisäksi myös ostaa yhteyttä muilta (transit palvelu)
  - tier 3: lokaali
    - Yksinomaan ostaa yhteyttä muilta (ylemmän kategorian) ISP:lta
- Internet koostuu Autonomisista järjestelmistä (AS)
  - "a connected group of one or more IP prefixes run by one or more network operators which has a single and clearly defined routing policy" [RFC 1930]
  - Usein yhteydentarjoaja



Internetin rakenne



Internet 2008

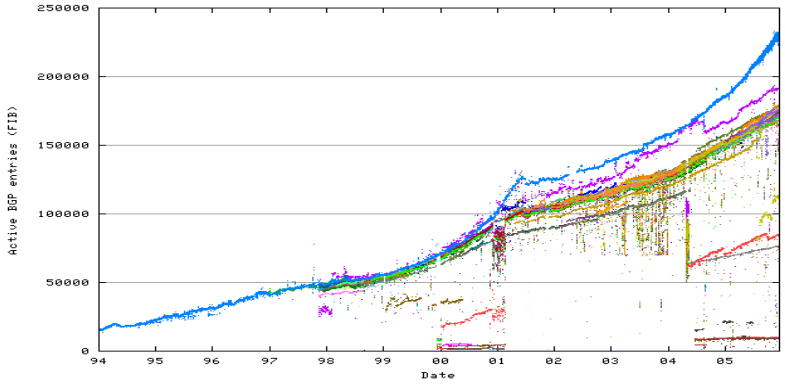


Reititysprotokollat

- Internetissä on käytössä erilaisia reititysprotokollia
  - AS:n välille eli inter-domain routing protokollat
  - AS:n sisällä eli intra-domain routing protokollat
- AS:n välillä käytetään BGP4:ää (Border Gateway Protocol)
  - Myös suurempien AS:n sisällä
- Sisäiseen reititykseen on tarjoilla joukko vaihtoehtoja
  - EIGRP, OSPF, RIP, IS-IS, ...
- Protokollat välittävät tietoa
- Reititin toteuttaa myös reititysalgoritmin
  - Rakennetaan tiedosta reititystaulu
  - Yleensä protokolla määrittää myös käytetyn algoritmin

Runkoverkon reititys

- Runkoverkon reitittimillä ei oletusreittejä
  - Tiedettävä kaikkien maailman IP-osoitteiden reititys
  - Ei tietenkään koko polkua, vain seuraava pysäkki
  - Muista route aggregation



IPv6

- IP:stä on tulossa käyttöön uusi versio
- Tärkein etu on suuri osoiteavaruus
  - 128 bittiä
  - Laskettu riittävän huonostikin käytettynä
- Muita etuja
  - Parempi autokonfiguroituvuus
  - Optiot toteutettu eri tavalla
  - IPsec mukaan rakennettuna
- IPv4 ja IPv6 samanaikaisesti
  - dual stack –tyyliin
  - Tunnelointi

Yhteenveto

- Verkkokerros on nykyään Internet-arkkitehtuurissa käytännössä IP
  - Versio 4 tällä hetkellä, versio 6 tulossa
- IP toteuttaa epäluotettavan ja tilattoman kuljetuspalvelun Internetissä
  - Ylemmät protokollat hoitaa tarvittaessa luotettavuuden ym.
- IPv4-osoitteet ovat hallinnoitu luonnonvara
  - Voidaan jakaa aliverkoiksi bittirajojen kohdalta
  - NAT helpottaa hyödyntämällä yksityisiä osoiteavaruuksia
- Reitittimet siirtelevät IP-paketteja verkossa
  - Forwardointi
  - Reititys

Ensi luennolla

- Linkkikerros
  - Miten IP paketti siirretään päätelaitteesta/reitittimestä toiseen
  - Ethernet
  - WLAN

Jatkokursseilla…

- Reititysalgoritmit
  - Distance vector
  - Link state
- Reititysprotokollat
  - Inter-domain: BGP
  - Intra-domain: RIP, OSPF
- Monilähetys eli multicast
- NAT traversal -ratkaisut
- Liikkuvuudenhallinta
  - Miten IP osoitteet hoidetaan kun liikutaan?
- Kerroksia TCP:n ja IP:n väliin…?
  - Esim. Host Identity Protocol (HIP)
- TCP/IP romukoppaan…?
  - Tulevaisuuden Internet-arkkitehtuurit
  - Esim. PSIRP: Publish-Subscribe Internet Routing Paradigm

Kysymyksiä

- Onko 196.199.356.17 toimiva IP-osoite?
- Reititin muuttaa kunkin paketin IP-osoitteen seuraavaa linkkiä vastaavaksi, kyllä vai ei?
- Reititin muuttaa kunkin paketin linkkikerroksen osoitteen seuraavaa linkkiä vastaavaksi, kyllä vai ei?
- Vastaanottajan IP-toteutus asettaa IP-paketit oikeaan järjestykseen?
- Mitä tapahtuisi jos TTL (Time To Live) kenttä poistettaisi IP-otsakkeesta?