TEKNILLINEN KORKEAKOULU

Verkkokerros ja Internet Protocol

kirja sivut 190-222

Verkkokerros

- Internet-protokolla (IP) toteuttaa verkkokerroksen
  - Tietoliikennepaketit välitetään erilaisten fyysisten kerrosten ylitse koneelta koneelle
  - IP tarjoaa "best effort"-tyyppisen epäluotettavan välityspalvelun
  - Ylemmät kerrokset välittävät datan oikealle sovellukselle, IP tuo sen vain koneelle
  - Tällä luennolla ei käsitellä muita verkkokerroksen protokollia (esim. X.25, IPX)
- Verkkokerroksen osoiteavaruus on globaali

IP

- Internet Protocol
- Alunperin määritelty standardissa RFC 791
- IP välittää *datagrammeja* koneelta toiselle
- 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 jätetään yksinkeratisesti ottamatta huomioon
  - Kukin IP-paketti on IP-tasolla uniikki viesti, joka käsitellään erikseen
- Tällä kurssilla käsitellään IP-protokollan versio 4
  - Versio 6 on tulossa hitaasti käyttöön, sen olennaisin merkitys on suurempi osoiteavaruus

TEKNILLINEN KORKEAKOULU

End-to-end -argumentti

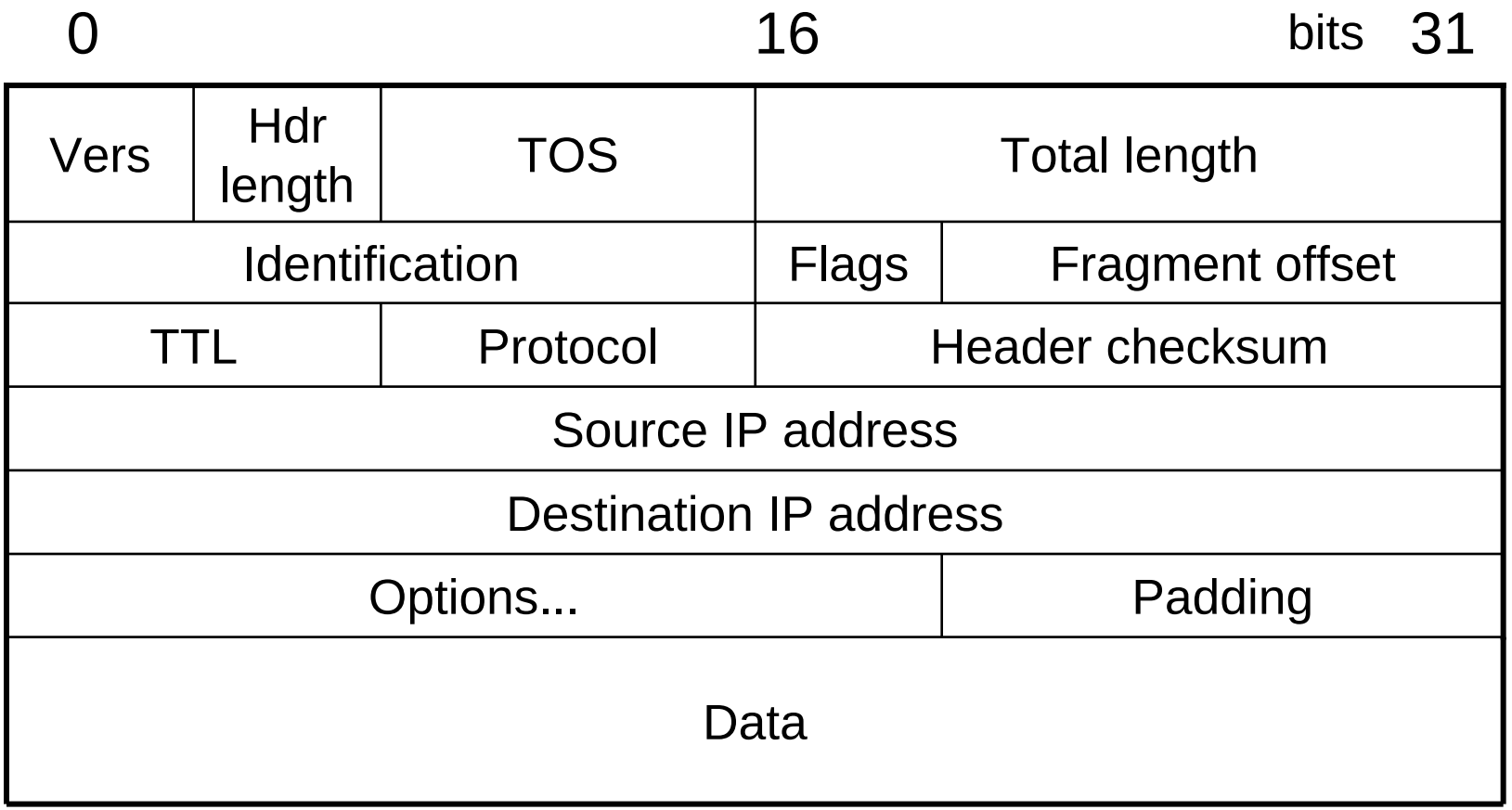
- Internet-teknologioiden suunnittelussa johtoajatus oli *tilattomasta pakettivälitteisestä* verkosta
  - Tilaton: itse reititinverkko ei ole tietoinen yhteyksistä
  - Pakettivälitteinen: kaikki tietoliikenne toteutetaan välittämällä datagrammeja eli viestejä
- Kaikki tieto kahden olion välisestä yhteydestä on siis näissä olioissa ja ne kommunikoivat viestein
  - Verkko tarjoaa vain paketinvälityspalvelun
  - Olennaisesti erilainen ratkaisu kuin esim. puhelinverkko
- Nykyään tämä ei täysin toimi, mm. palomuurien ja NAT/PAT-muunnoksen takia

TEKNILLINEN KORKEAKOULU

IP ja linkkikerros

- Toimiakseen IP tarvitsee:
  - Kehystyksen linkkikerrokselta
  - Reititystiedot, jotka kuvaavat IP-tason osoitteet linkkikerrokseen
    - Lähiverkoissa muunnos IP-osoitetta vastaavaan MAC-osoitteeseen (ARP)
    - Point-to-point -yhteyksien kohdalla tieto linkkien takana sijaitsevista IP-verkoista
- Reititystiedot voidaan saada
  - Asettamalla kiinteästi (tyypillistä verkon reunareitittimille)
  - Hakemalla DHCP:llä (työasemat)
  - Keskustelemalla reititysprotokollilla verkon muiden reitittimien kanssa ja muodostamalla kokonaiskuva (runkoverkon reitittimet, ei käsitellä tällä kurssilla)

IP-otsikkotiedot



- Normaali koko on 20 tavua, optiot saattavat kasvattaa

...IP-otsake

- Versio on 4, IPv6-paketeissa 6 (v6-otsakkeen rakenne erilainen)
- Type of Service -kenttä sisälsi alunperin määriteltyjä laatuparametreja, joita ei ole koskaan käytetty ja ko. tavu on kierrätetty erilaisten siirron laatua tarjoavien ratkaisujen käyttöön
- Identification on uniikki pakettikohtainen tunniste duplikaattien havaitsemiseksi, yleensä nouseva laskuri
- Flags (liput) sisältävät tietoa paketin *fragmentoinnista*
- Fragment offset kertoo mihin kohtaan alkuperäistä pakettia tämän paketin data sijoitetaan

...IP Packet Format

- Time to Live (TTL) -kentän arvoa vähennetään yhdellä jokaisessa reitittimessä, kun kenttä saa arvon 0, paketti hylätään ja lähettäjälle lähetetään "Time exceeded" -viesti
- Protocol-kenttä kertoo ylemmän tason protokollan
  - TCP (6), UDP (17), ICMP (1) jne.
- Optioilla voidaan lisätä toiminnallisuutta IP-tasolle
  - Näitä on määritelty koko joukko, mutta useissa niistä on nykyään suorituskyky- ja turvaongelmia, joten ne ovat käytännössä harvinaisia
  - Esim. loose ja "strict source routing", "route recording", "time stamping" ja "military security options"

Fragmentointi

- Eri linkkikerroksen protokollilla on usein kokorajoitus siirrettävälle segmentille
  - Mitä tehdään, jos IP-paketin lähettäjä lähettää 64 kB paketin ja vastaanottajan kokorajoitus on 1,5 kB
- IP-protokolla antaa reitittemelle mahdollisuuden jakaa tuleva paketti osiin, ja lähettää nämä erillisinä *fragmentteina*, jotka kootaan vastaanottajapäässä kokonaiseksi IP-paketiksi
- Fragmentointi aiheuttaa vastaanottajalle huomattavia suorituskykyongelmia
  - Vastaanottajan on säilytettävä muistissa vastaanotetut fragmentit, kunnes koko paketti saadaan koottua
  - Vastaanottajan on selvittävä yksittäisen fragmentinpalasen (joka on omassa IP-paketissaan) katoamisesta
- Lisäksi fragmentoinnissa on tietoturvaan liittyviä ongelmia
  - Väärinrakennettuja fragmentteja
  - Mahdollisuus palvelunestohyökkäyksiin
- Joten fragmentointia ei käytännössä käytetä
  - Sen sijaan selvitetään suurin sallittu segmentin koko

TEKNILLINEN KORKEAKOULU

Path MTU Discovery

- Fragmentoinnin välttämiseksi on selvitettävä suurin sallittu IP-paketin koko
- Lähetetään suurehko IP-paketti, jossa on "Don't Fragment" -lippu päällä
  - Koska pakettia ei saa fragmentoida, reititin vastaa "Fragmentation Needed" ICMP-viestillä
  - Toistamalla pienemmillä paketeilla voidaan luodata sopiva paketin koko
- Lisäksi käytettäessä TCP-yhteyksiä IP:n ylitse, kumpikin osapuoli lähettää oman lähiverkkonsa salliman segmentin maksimikoon, TCP:n Maximum Segment Size-optio
  - Ei tarjoilla UDP-liikenteeseen
- Käytännössä Ethernet rajaa IP-paketin maksimikoon 1500 tavuun, ja viestinnän jompikumpi tai molemmat osapuolet ovat yleensä Ethernet-verkossa

IP-osoitteet

- IP-osoite on verkkoliittymän (interface) tunniste
  - Verkossa olevalla koneella voi olla useita samanaikaisia verkkoliittymiä
    - Reitittimet
    - Luotettavuus
    - Erillinen varmuuskopioverkko
- IPv4-osoitteet ovat 32-bitin mittaisia
  - IPv6 tarjoaa 128-bitin osoitteet
- Yleisin esityssyntaksi
  - 4 pisteiden erottamaa tavua desimaalinumeroina ("dotted quad")
  - Esim: 130.233.240.9
- Alkuosa osoitteesta kertoo verkon (network id), loppuosa viittaa koneeseen verkossa (host id)
  - Esim. lähiverkko tai yrityksen koko verkko
  - Reitittimet välittävät paketteja verkko-osan perusteella

TEKNILLINEN KORKEAKOULU

IP-verkon esittäminen

- Nykyään yleisin tapa kuvata verkko on CIDR
  - Classless Inter-Domain Routing
- 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 tämän perusteella runkoverkossa
  - Raja on bittiraja, ei tavuraja
- TKK:n verkon sisällä voi olla aliverkkoja, esim. 130.223.236.0/22
  - Tämän verkon *verkkomaski* (netmask) on 255.255.252.0
    - Verkkomaski saadaan suoraan CIDR-notaatiosta
  - Osoitteet 130.223.236.0-130.223.239.255 kuvaavat tätä verkkoa
  - Huomaa että 130.223.237.0/22 ei ole toimiva aliverkko, bittirajaa on seurattava tarkasti
- RFC 1518, 1519

Vanhat IP-osoiteluokat

- Alunperin Internetin osoitteet jaettiin kiinteästi verkko- ja koneosaan
- Nykyään tätä jakoa käytetään viittaamaan tietynkokoisiin verkkoihin
  - C-luokka on 256 osoitetta
  - Vanhojen A-allokaatioiden purkamisesta yleiseen käyttöön puhutaan

Class	netID bits	host bits	first byte	first bits	use
A	7	24	0-127	0	large organizations
B	14	16	128-191	10	medium -"-
C	21	8	192-223	110	small -"-
D	28	0	224-239	1110	multicast addresses
E	27	0	240-247	11110	reserved

TEKNILLINEN KORKEAKOULU

Internetin osoitteet fraktaalikarttana

- IPv4-osoiteavaruuden käyttö on poliittinen kiista
- Vihreät osoitteet ovat allokoimatta
- Lähde ja tarkempi selitys: http://www.xkcd.com/195/

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, vrt. "./" Unixin hakemistoissa
- Koneen osoite -osan kaikki bitit 0
  - Verkon osoite
  - Esim. 222.1.16.0/24

TEKNILLINEN KORKEAKOULU

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
  - Näitä osoitteita voi siis käyttää vapaasti, mutta niistä ei voi viestiä suoraan Internetiin
  - Käytetään lähiverkoissa, koska julkisen verkon osoitteista on pulaa, myös testiverkoista
- Liikennöinnin Internetiin mahdollistaa NAT/PAT (Network/Port Address Translation)

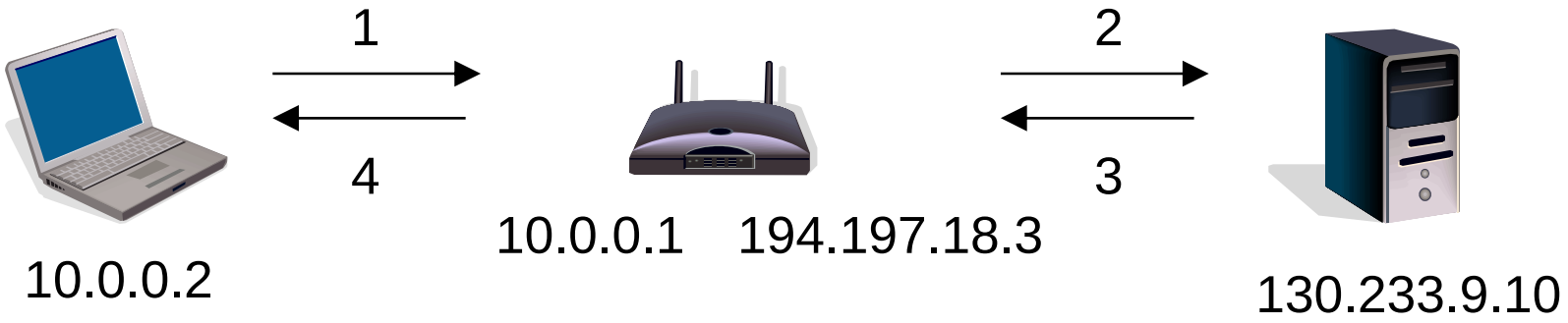
TEKNILLINEN KORKEAKOULU

Network/Port Address Translation

- NAT (NAT/PAT)
- Reititin käyttää yhtä (tai muutamaa) julkista IP osoitetta ja sisäverkossa yksityisosoitteita
  - Lähtevän paketin lähettäjän osoite muutetaan ja reititin kirjaa mikä ulkoinen IP/portti -osoite vastaa mitä sisäistä osoitetta
  - Nyt reitittimessä on verkkoyhteyden tila
- NATin takaa voi ottaa yhteyksiä Internetiin, mutta Internetistä ei voi ottaa yhteyksiä NATin taakse
  - Voidaan tehdä kiinteä NAT-muunnos ja saada NATin takana oleva palvelin näkymään julkisessa verkossa
  - Kaksi NAT-muunnoksen takana olevaa tietokonetta eivät pysty kommunikoimaan keskenään ilman apua
    - STUN, ICE ja muita ratkaisuja

NAT/PAT

- IP-paketin muuttuminen matkalla



	From IP	From Port	To IP	To Port
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

ICMP

- Internet Control Message Protocol
- Standardi RFC 792
- Yksinkertainen viesti IP-paketin sisällä
  - Kahden koneen TCP/IP-pinojen välillä
  - Ei sovelluksien välillä
- Toteuttaa
  - Verkon virheilmoitukset
  - Ping
  - Traceroute
- Turvasyistä käyttö usein rajoitettu
  - "Route redirect", "router advertisement" mahdollistavat yhteyksien kaappaamisen
  - Pelkkä ping mahdollistaa verkon koneiden kartoituksen

ICMP-viesti

Type	Code	Checksum
Data		

- Type määrittelee viestin: echo request, echo reply, destination unreachable, jne.
- Code määrittelee syyn: host unreachable, port unreachable, jne.
- Data sisältää virheviesteissä virheen aiheuttaneen IP-paketin oleelliset osat
- Parametrien määrittely
  - http://www.iana.org/assignments/icmp-parameters

IP lähiverkossa

- Yleensä yksi lähiverkkosegmentti on myös yksi IP-verkko
  - IP-verkolla on verkon osoite ja yleislähetysosoite
- Ongelma: lähiverkko ei ymmärrä mitään IP-osoitteista
- Jotta IP toimisi lähiverkossa, on IP-osoitteet kuvattava lähiveron osoitteisiin
  - ARP tarjoaa tämän palvelun
- Lisäksi kullekin verkon koneelle on kerrottava sen IP-osoite
  - DHCP ratkaisee tämän nykyään
  - Voidaan myös asettaa käsin
- Jotta verkosta voisi viestiä muihin verkkoihin, on koneen tiedettävä yhdyskäytävän (reitittimen) osoite ja pystyttävä erottamaan lähiverkon osoitteet runkoverkon osoitteista

TEKNILLINEN KORKEAKOULU

...IP lähiverkossa

- Koneen verkkoliittymät määritellään (Unix)
- Loopback:

```
ifconfig lo 127.0.0.1
```

- Ethernet:

```
ifconfig eth0 194.197.118.42 broadcast \
194.197.118.255 netmask 255.255.255.0
```

- Muut verkkoliittymät
- Default route on yhdyskäytävä kaikelle, mikä ei mene lähiverkkoon

```
route add default 194.197.118.1
```

ARP

- Address Resolution Protocol
- Yhdistää IP-osoitteet ja lähiverkon MAC-osoitteet
- Kysyjä lähettää lähiverkkoon yleislähetyksen, jossa on vastaanottajan IP-osoite
- Oikean IP-osoitteen omistaja vastaa MAC-osoitteellaan
- Kysyjä tallettaa ensimmäisen saamansa vastauksen dynaamiseen ARP-taulukkoon
  - APR:ssä on tiettyjä turvaongelmia
- Jos koneella on liittymässä enemmän kuin yksi IP-osoite, se vastaa kuhunkin kysymykseen samalla MAC-osoitteella
- RFC 826

TEKNILLINEN KORKEAKOULU

ARP paketin formaatti

hardw type	prot type	hardw size	prot size	OP	sender MAC address	sender IP address	target MAC address	target IP address
2	2	1	1	2	6	4	6	4 bytes

- Kapseloidaan suoraan linkkikerroksen kehykseen
- Data on aina 28 tavua
  - hardw type = MAC-osoitteen tyyppi (0x0001 = Ethernet)
  - prot type = verkkoprotokollan typpi (0x0800 = IP)
  - OP = operation (ARP request/reply)

DHCP

- Dynamic Host Configuration Protocol
  - Automaattien IP-osoitteiden jakelu lähiverkossa
  - Pysyvät IP-osoitteet asiakkaan MAC-osoitteen perusteella
  - Dynaamiset IP-osoitteet poolista
  - Korvaa vanhemmat BOOTP:n ja RARP:n
- Edellyttää palvelimen tai proxy-palvelimen lähiverkkoon
- RFC 2131, 2132

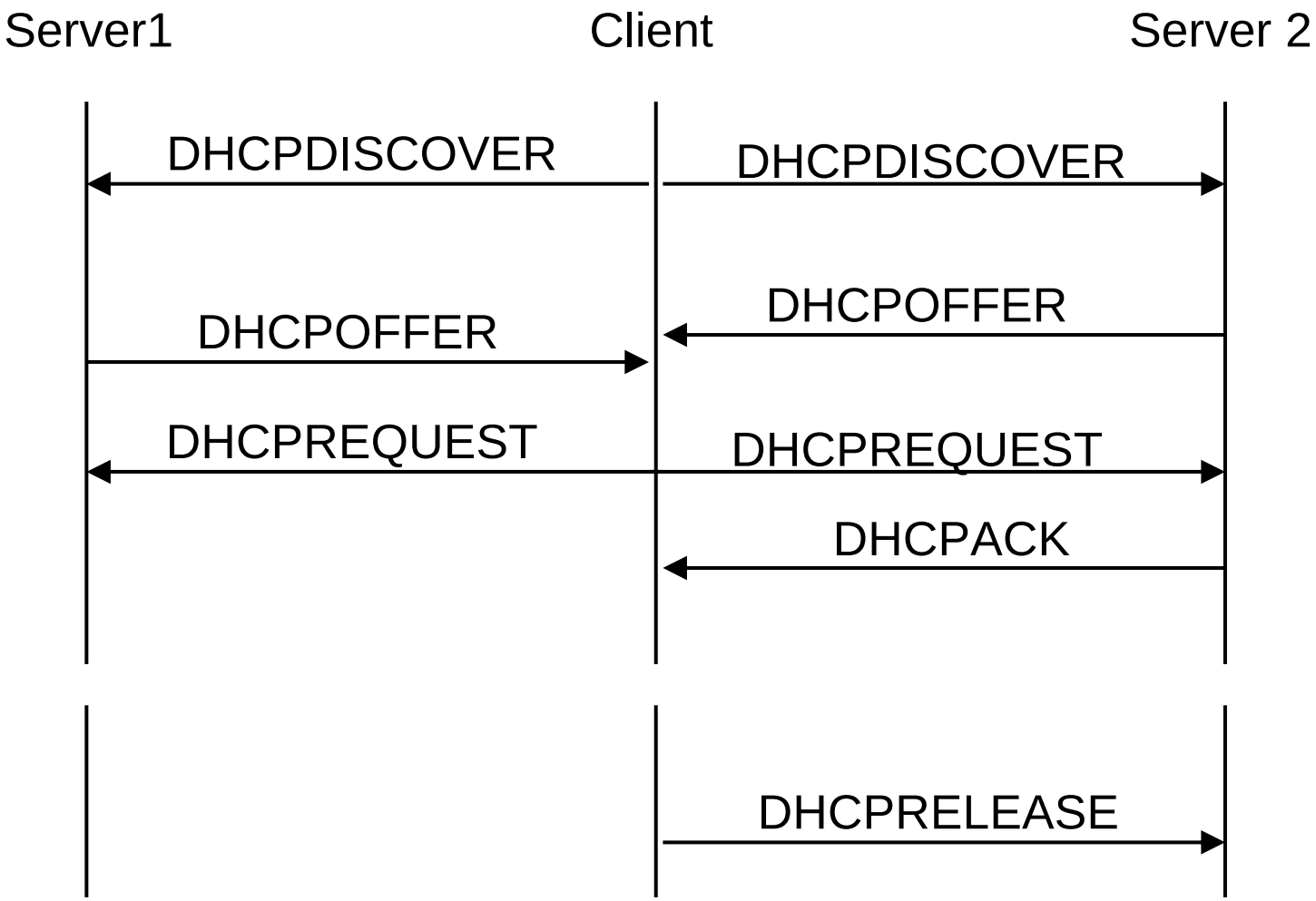
TEKNILLINEN KORKEAKOULU

…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.

TEKNILLINEN KORKEAKOULU

DHCP MSC-kaavio



Reititys

- Jotta verkko olisi verkko, sen on tarjottava useita vaihtoehtoisia reittejä pisteiden välille
  - Internet on suuri ja dynaamisesti muuttuva verkko
  - Yritysten ja muiden organisaatioiden verkot muuttuvat myös melko usein
  - Vaihtoehtoisten reittien tarkoitus on vikasietoisuus, staattisessakin verkossa on dynaamisia tapahtumia
- Reitittimet välittävät tietoa verkon tilasta ja tarjoamistaan verkko-osoitteista reititysprotokollien välityksellä
- *Reititys* tarkoittaa päätöksentekoa paketin edelleenvälittämiseksi verkossa
  - Reitityspäätös tehdään reititysprotokollien välityksellä saadun tiedon perusteella
  - Tieto talletetaan reititystauluun

Reititin

- Reititin on verkkojen välillä liikennettä välittävä tietoliikennekomponentti
  - Kaksi tai useampia verkkoliittymiä
- Reititin pystyy tekemään edelleenlähettämispäätöksen kutakin IP-osoiteavaruuden osoitetta kohden
  - Päätös saattaa myös olla "en lähetä minnekään"
  - Tämä edelleenlähettämispäätös koskee myös työasemia ja palvelimia, vaikka niillä olisikin vain yksi verkkoliittymä
    - Esim. Unix "`route`" ja Windows "`route print`"
- Päätös tehdään reititystaulun perusteella
  - Tietorakenne, jossa on tietoa eri IP-osoitteista ja tietoliikennepakettien kohtelusta
  - Päivitetään reititysprotokollien avulla (dynaaminen reititys)

Staattinen reititys

- Työasemissa ja verkon reunareitittimissä reititystaulu on yleensä staattinen
  - Reititysprotokollia ei käytetä
- Paketin tullessa reitittimelle tehdään paketissa olevan vastaanottajan osoitteen ja reititystietojen perusteella päätös edelleenlähettämisestä
  - Työasemassa verrataan lähtevän IP-paketin vastaanottajan osoitetta koneen omaan osoitteeseen verkkomaskin puitteissa
  - Reunareititin (esim. kotiverkossa) tietää lähiverkon verkko-osoitteet ja ohjaa kaiken muun oletuslinkille (default)

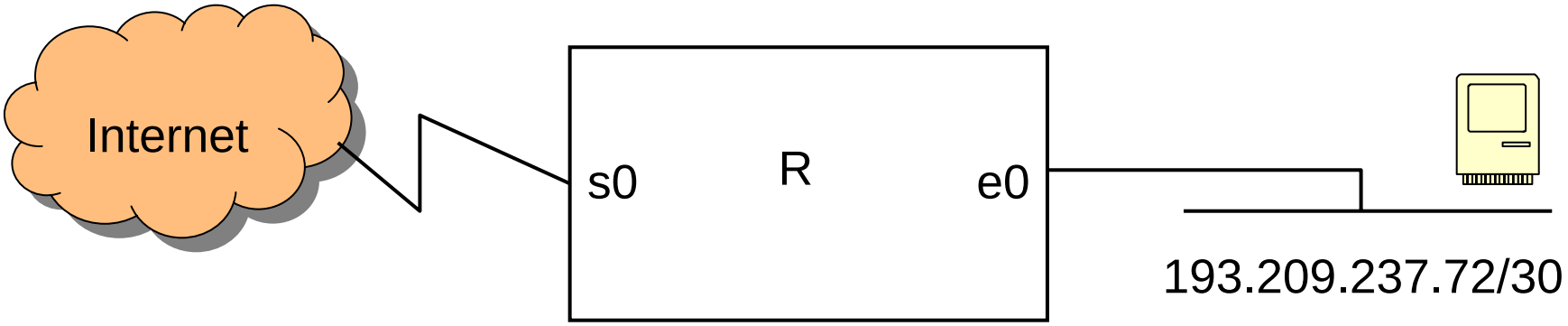
TEKNILLINEN KORKEAKOULU

Dynaaminen reititys

- Reitittimille asetetaan käsin paikalliset (lähi)verkot ja niiden osoiteavaruudet
- Reitittimet mainostavat reititysprotokollilla muille reitittimille omia verkkojaan ja ottavat vastaan muiden reitittimien mainostamia yhteyksiä
- Vastaanotetusta tiedosta rakennetaan dynaamisesti päivittyvä reititystaulu
- Käsitellään tarkemmin kurssilla T-110.4100 Tietokoneverkot

TEKNILLINEN KORKEAKOULU

Yksinkertainen reititystaulu



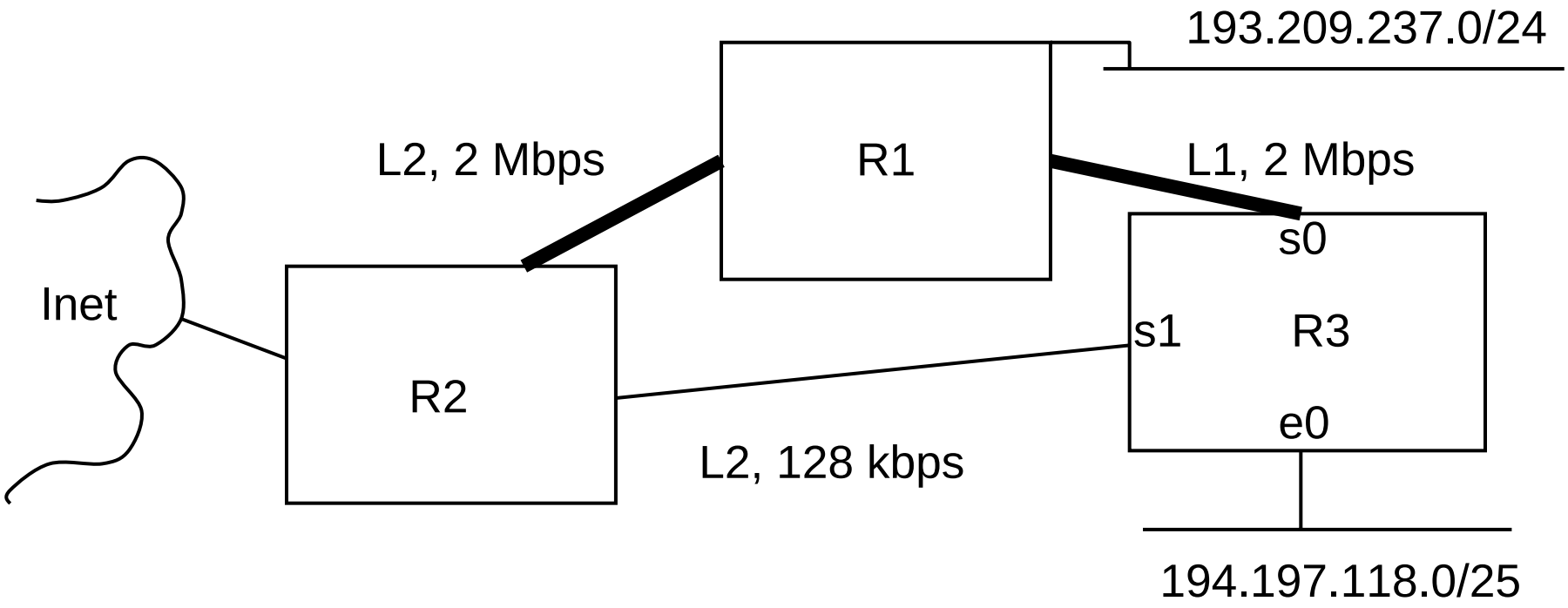
- Tyypillinen pieni kotiverkko
- Reititystaulu:

Destination	Next hop	Comment
193.209.237.72/30	e0	Local LAN (Ethernet)
*	s0	Serial line to Internet (default route)

TEKNILLINEN KORKEAKOULU

Vähän monimutkaisempi reititys

- Tässä tarvitaan jo dynaamisia ominaisuuksia
  - Toimipisteellä on 2 Mbps linkki Internetiin toisen toimipisteen kautta ja 128 kbps varalinkki (esim. ISDN)



...Reititystaulu

- Edellisen esimerkin reitittimen R3 reititiystaulu

```
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

Runkoverkko

- Verkko jolla on Internet-yhteys ei vielä ole runkoverkkoa
- Runkoverkon verkot välittävät muiden verkkojen välistä liikennettä
- Runkoverkon reitittimillä ei ole oletusreittejä, vaan niiden on tiedettävä kaikkien maailman IP-osoitteiden reititys
  - N. 100 000 alkiota taulukossa
  - Kunkin reitittimen tarvitsee vain tietää mihin linkkiin se ohjaa paketin, ei tuntea koko polkua yksityiskohtaisesti

Reititysprotokollat

- Reititysprotokollia on erikseen runkoverkolle ja pienemmille verkoille
- Internetin runkoverkko käyttää BGP4:ää (Border Gateway Protocol)
- Sisäiseen reititykseen on tarjoilla joukko vaihtoehtoja
  - IGRP (Interior Gateway Routing Protocol)
  - EIGRP (Enhanced Interior Gateway Routing Protocol)
  - OSPF (Open Shortest Path First)
  - RIP (Routing Information Protocol)
  - IS-IS (Intermediate System to Intermediate System)
- Protokollat välittävät tietoa, lisäksi reitittimen on toteutettava reititysalgoritmi (yleensä protokollat määrittelevät myös käytetyn algoritmin), jolla tiedosta rakennetaan reititystaulu

IPv6

- IP:stä on tulossa käyttöön uusi versio
- Tärkein etu on suuri osoiteavaruus
  - 128 bittiä
  - Laskettu riittävän huonostikin utilisoiden n. 1500 osoitetta per m2 maapallolle
- Muita etuja
  - Parempi autokonfiguroituvuus
  - Varsinaisessa otsakkeessa ei ole optioita -> tehokkaampi
  - IPsec mukaan rakennettuna
- IPv4:n ja IPv6:n samanaikainen käyttö on mahdollista, siirtymä on määritelty
- Muutos on alkanut
  - Aasian operaattoreilla on oikeasti pulaa IPv4-osoitteista
  - 3GPP R5 määrittelee operaattorille IPv6 runkoverkon
  - Tuki on olemassa (saatavilla) jo tavallisimmissa käyttöjärjestelmissä

Yhteenveto

- Verkkokerros on nykyään Internet-arkkitehtuurissa käytännössä IP
  - Versio 4 tällä hetkellä, versio 6 tulossa
- Ylemmät protokollat (TCP, UDP) olettavat verkkokerroksen onnistuvan riittävän hyvin pyrkimyksessään välittää paketteja koneelta toiselle
  - Ei tarvita täydellistä onnistumista, "enimmäkseen" riittää
- IPv4-osoitteet ovat hallinnoitu luonnonvara, joita voidaan jakaa aliverkoiksi bittirajojen kohdalta