



Aalto-yliopisto
Teknillinen korkeakoulu

Kuljetus- ja verkkokerrokset

Jyry Suvilehto

T-110.1100 Johdatus tietoliikenteeseen ja
multimediatekniikkaan
kevät 2011

Luennon sisältö

1. Johdantoa

- Kertaus, motivointi
- Yhteys, yhteydettömyys
- Best effort

2. Kuljetuskerros

- UDP
- TCP

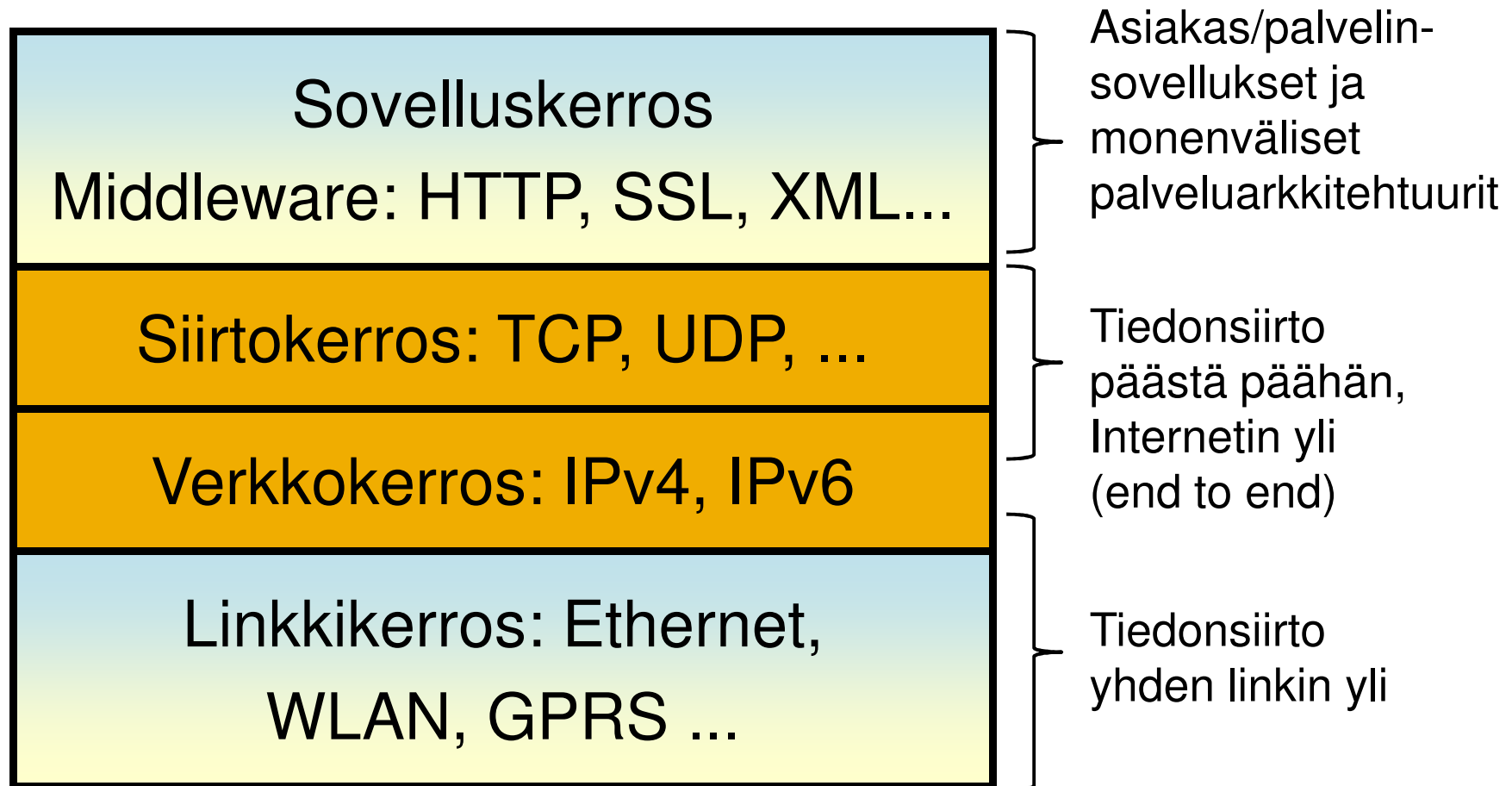
3. Verkkokerros

- Internetin rakenne
- Reititys
- IP
 - IPv4 ja IPv6
 - Lähetystyypit: Unicast, Anycast, Multicast

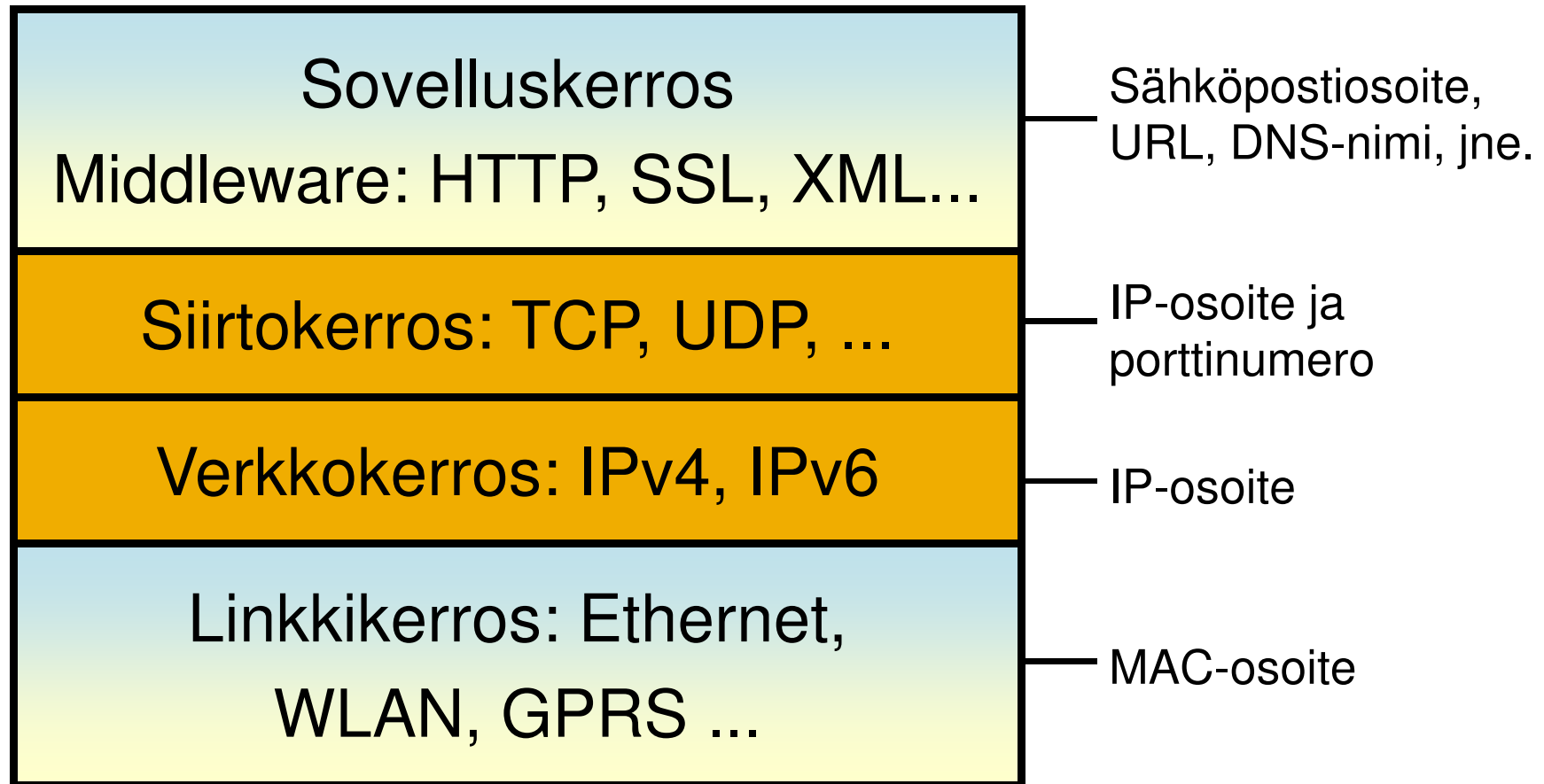
Luennolla eilisen uutisia

- <http://www.uusisuomi.fi/ulkomaat/108945-maailman-nettiosoitteet-loppuivat>

TCP/IP-protokollapino



Nimiavaruudet



JOHDANTO

Internet

- a computer network consisting of a worldwide network of computer networks that use the TCP/IP network protocols to facilitate data transmission and exchange (Princeton WordNet)
- The Internet is a system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide. ...(wikipedia)
- An international network, consisting of independently managed networks using the TCP/IP protocols and a shared naming system. A successor to the ARPAnet.(Cornell University digital library glossary)

Yhteys

- Viime luennolla esitetyt protokollat käyttivät TCP-protokollan tarjoamaa kaksisuuntaista luotettavaa tavuvirtaa (yhteyttä) tiedon siirtoon
 - Kaksisuuntainen: molemmat osapuolet voivat kirjoittaa ja lukea
 - Luotettava: korkeammalla tasolla ei tarvitse huolehtia siirtovirheistä (tai ainakin alemman tason protokolla ilmoittaa niistä)
 - Tavuvirta: voi siirtää mitä tahansa, (vrt. merkkivirta pelkän tekstin siirtoon)

Yhteys

- Merriam-webster connection:

2 a : something that [connects](#) : [link](#) <a loose connection in the wiring> **b** : a means of communication or transport <a telephone connection>

- Paljon kysymyksiä ja vastauksia saman yhteyden yli

- Esim. Keskustelu, puhelu

- Minä: “Haloo, Jyrä puhelimesta”
- Opiskelija: “Kuule, mulla on tällanen ongelma sun kurssis kanssa.”
- Minä: “No minkä ongelma?”
- Opiskelija: “....”

- Jos aloittajaosapuolen yhteys ei mene läpi, tämä huomaa sen

Yhteydettömyys

- Esimerkiksi DNS on yhteydetön tiedonsiirtoprotokolla
- Analogia reaaliaikailmassa: postikortit
 - ”Rakas Tilly-täti, mikä oli Bill-sedän osoite”
 - ”Hei Richard, Bill-setä asuu osoitteessa One Microsoft Way, Redmond, WA 98052-6399”
- Postikortit ja UDP-paketit voivat kadota matkalla

Verkkokerros

- Internet-Protokolla tarjoaa ”best effort” pakettien siirtoa koneelta A koneelle B
 - Best effort: ei takeita oikein mistään, mutta luvataan edes yrittää
 - moni hyökkäys perustuu lupauksen pettämiseen
- TCP/IP:n kanssa kilpailevat mallit (mm. EU:n tukema OSI) pyrkivät tarjoamaan luotettavuutta (ja maksutietoja) verkkokerroksessa
- Lopulta TCP/IP:n käytännöllinen lähestyminen levisi

KULJETUSKERROS

UDP

- UDP: Universal Datagram Protocol
 - Datagrammi on paketti erityisesti epäluotettavassa yhteydessä
- RFC-768

Lähdeportti (ohjelma)	Kohdeportti (ohjelma)
Paketin pituus	Tarkastussumma
Sisältö	

- Tarkastussumma (hash, checksum) lasketaan koko paketista ennaltamäärätyllä tavalla koko paketista

UDP

- UDP tarjoaa epäluotettavan yhteydettömän tiedonsiirron
- UDP:ta käyttävät mm. DNS, VoIP, IPTV, NTP, SNMP
- UDP:ssä pienempi yleiskustannus (overhead) kuin TCP:ssä

TCP

- TCP: Transmission Control Protocol
- RFC-793
- Yhteydellinen, luotettava, kaksisuuntainen tavuvirta
 - Eri suunnat eivät riipu toisistaan
- Ohjelman lähettämä virta pilkotaan palasiin ja palaset lähetetään IP-paketeissa

TCP

Lähdeportti (ohjelma)		Kohdeportti (ohjelma)	
Sekvenssinumero			
Vastausnumero			
Otsikon pituus	Varattu	Lippuja	Ikkunan koko
Tarkastussumma		Kiireellisyys	
Optioita			
Data			

- Portti identifioi ohjelman
- Sekvenssinumeron avulla paketit puretaan (ensimmäinen tavu)
- Vastausnumero kertoo seuraavan odotetun paketin aloitustavun
 - Ikkunan koko on $\text{max sekvenssinumero} - \text{vastusnumero}$

Liput

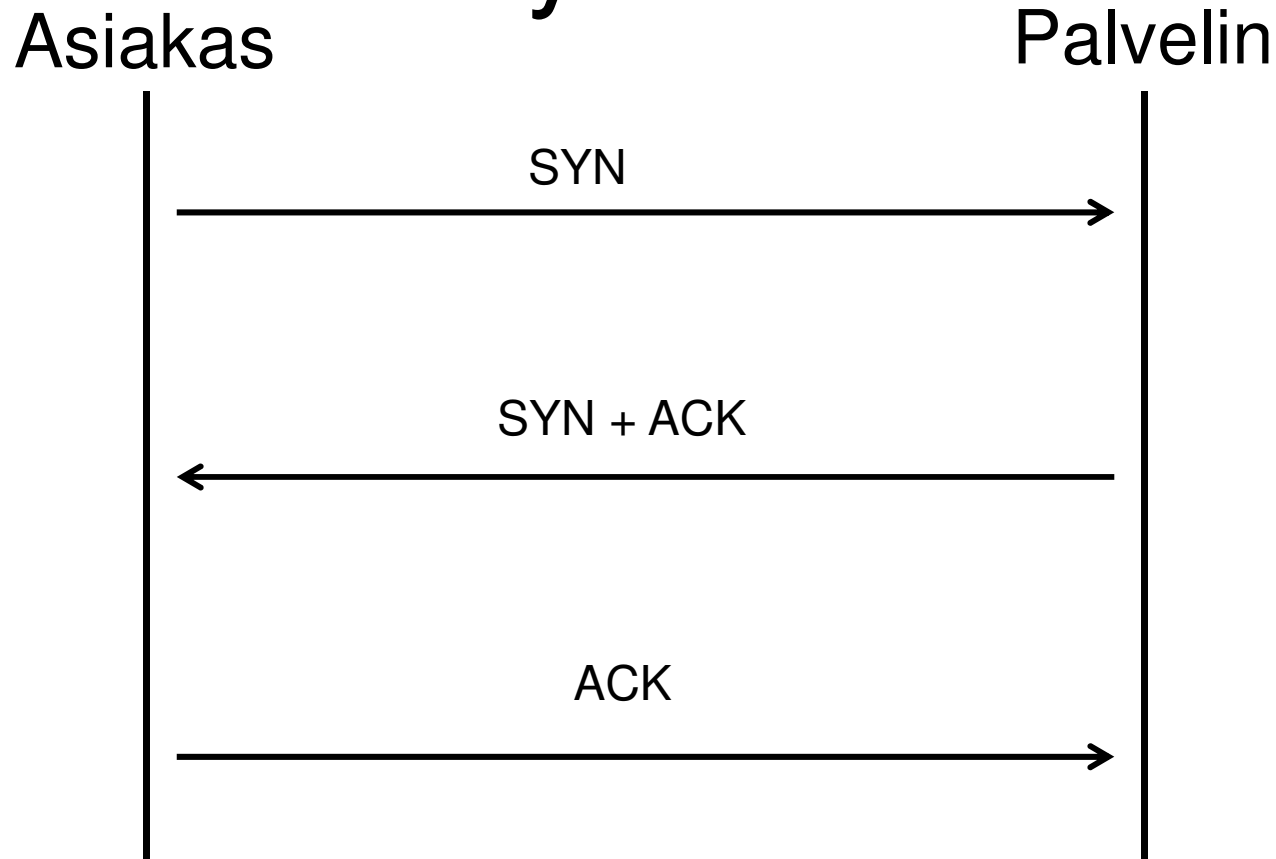
RST	ACK	PSH	URG	SYN	FIN
-----	-----	-----	-----	-----	-----

Liput

RST	ACK	PSH	URG	SYN	FIN
-----	-----	-----	-----	-----	-----

- Liput kertovat mikä viestityyppi on kyseessä
 - RST: Reset Connection
 - ACK: Acknowledge
 - PSH: Push
 - URG: Urgent
 - SYN: Synchronize sequence numbers
 - FIN: I have no more data to send

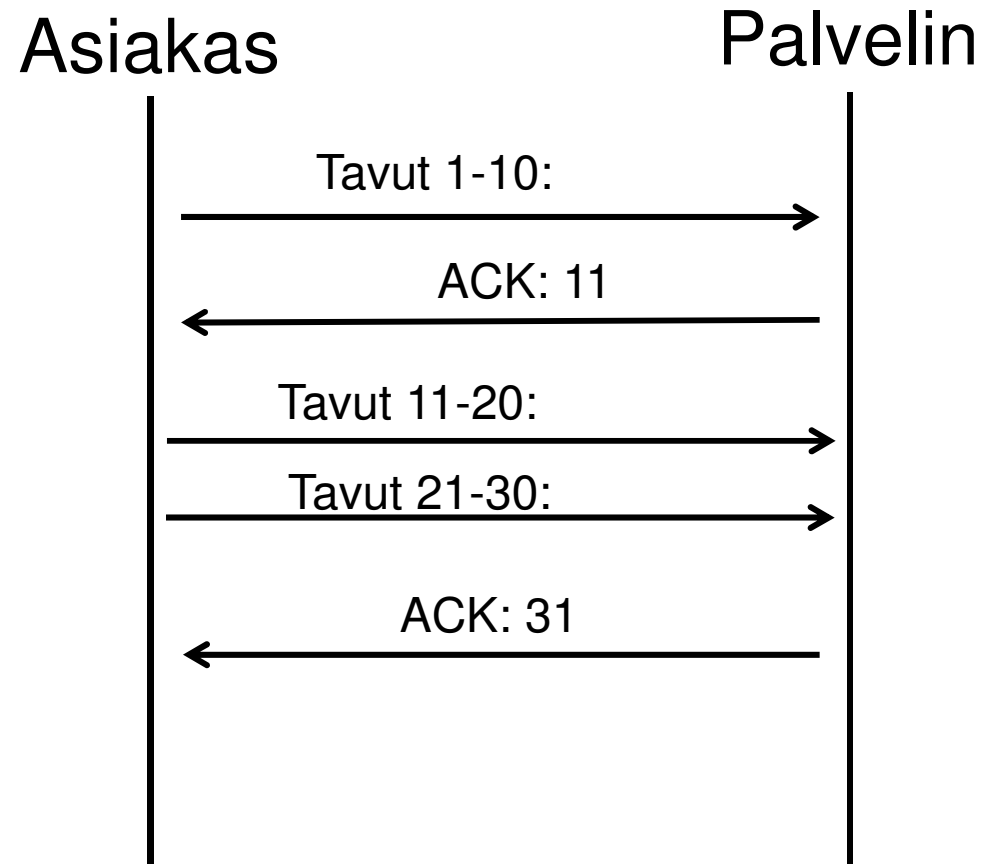
Yhteyden avaus



- Kaksi roolia, aloitteentekijä ja vastaaja
- Sovitaan sekvenssinumeroista (arvottuja)
- Ikävä palvelin (smtp.hut.fi) saattaa kenkkuilla ja vastata RST

Kuittaaminen

- Vastaanottava osapuoli kertoo mitä tavua se odottaa seuraavaksi

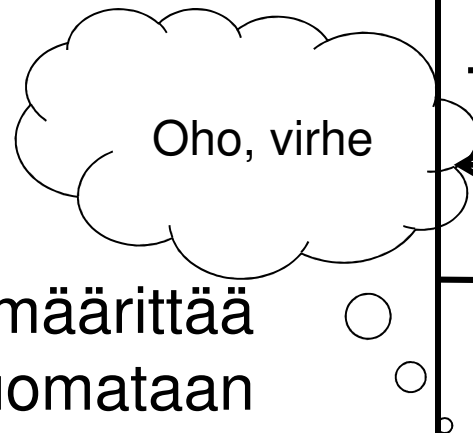


Syn + Ack



Virhe

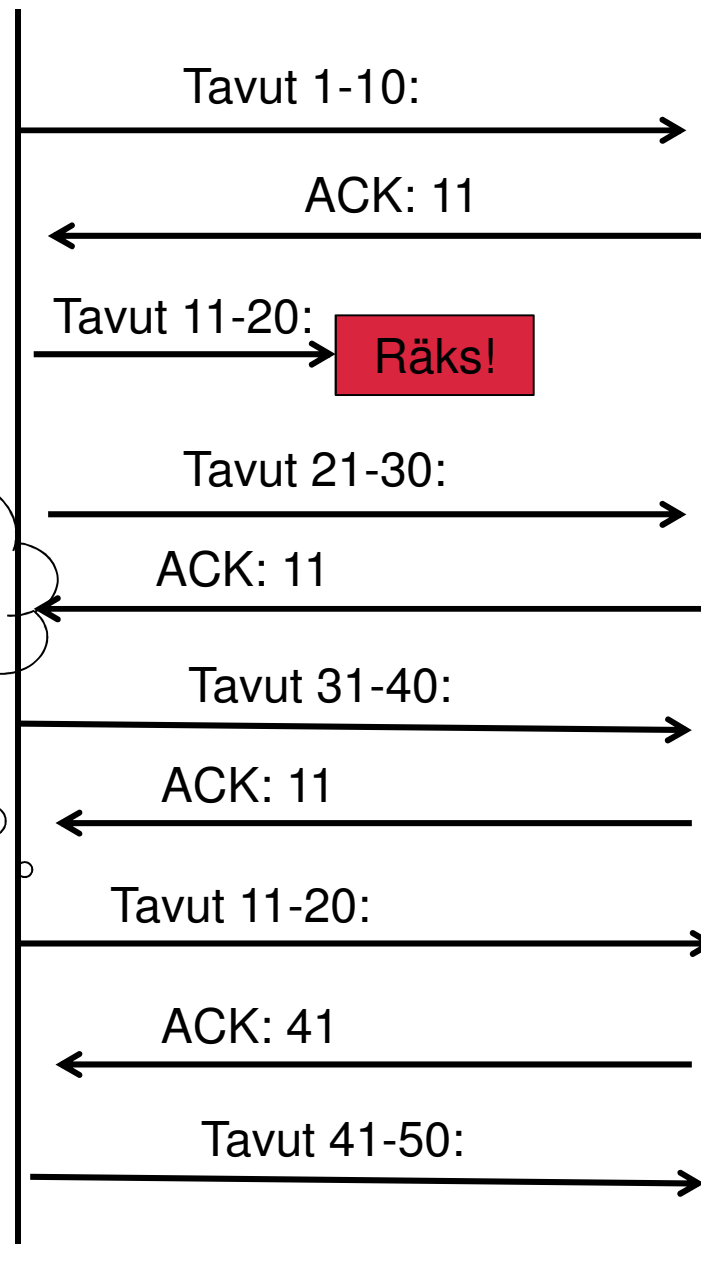
- Toinen osapuoli jättäpäisesti pyytää seuraavaa näkemätöntä pakettia



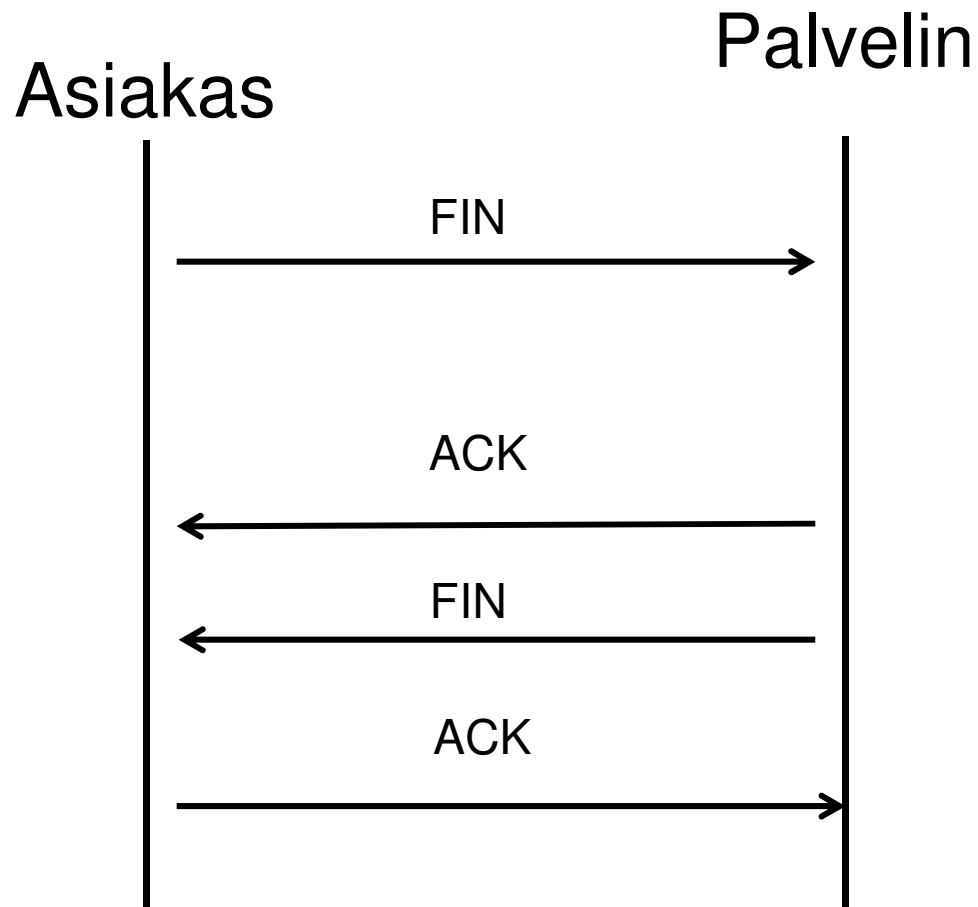
- Ikkunan koko määrittää koska virhe huomataan
- TCP osaa sopeuttaa ikkunan kokoa virheiden tiheyden mukaan

Asiakas

Palvelin



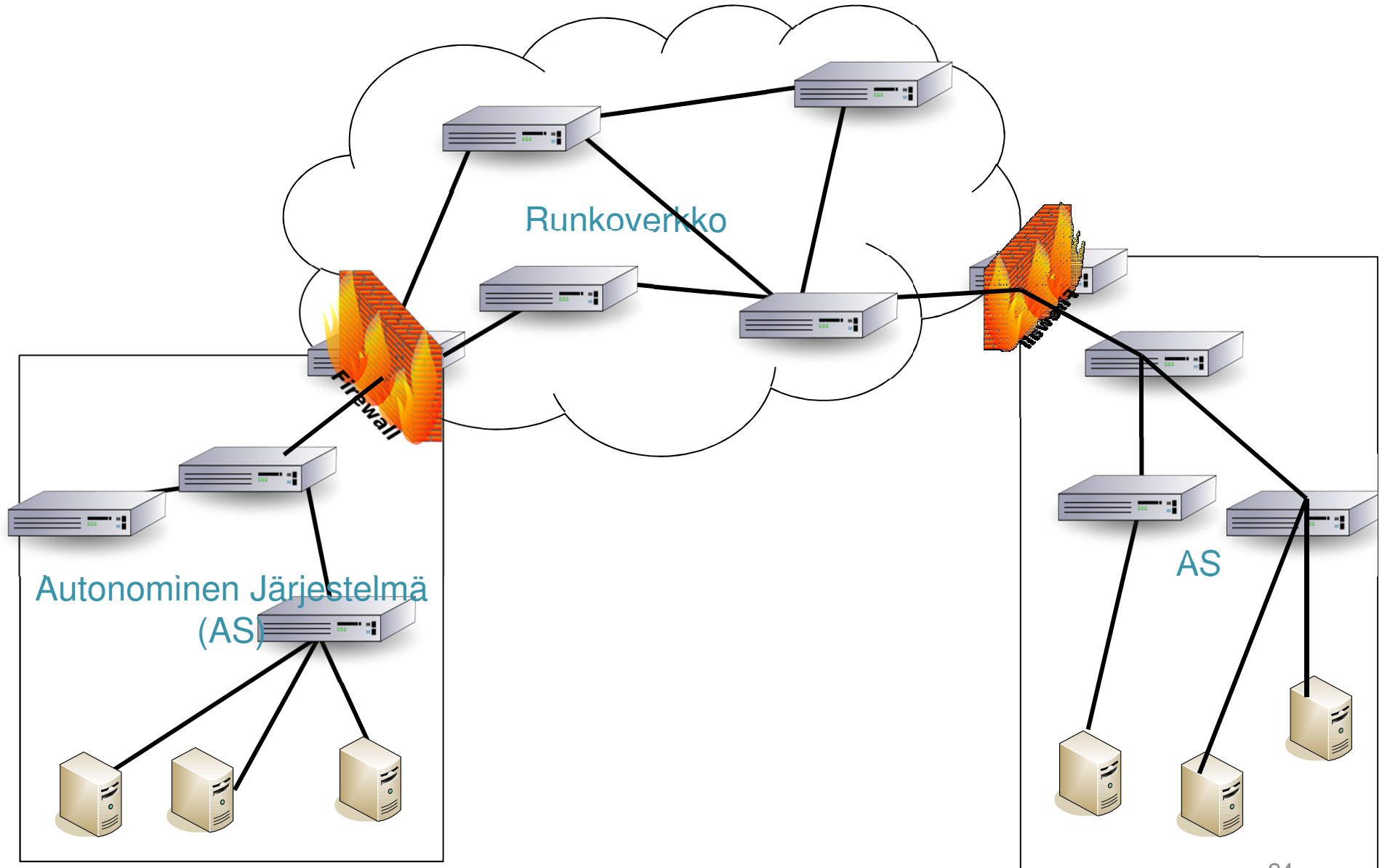
Yhteyden sulkeminen



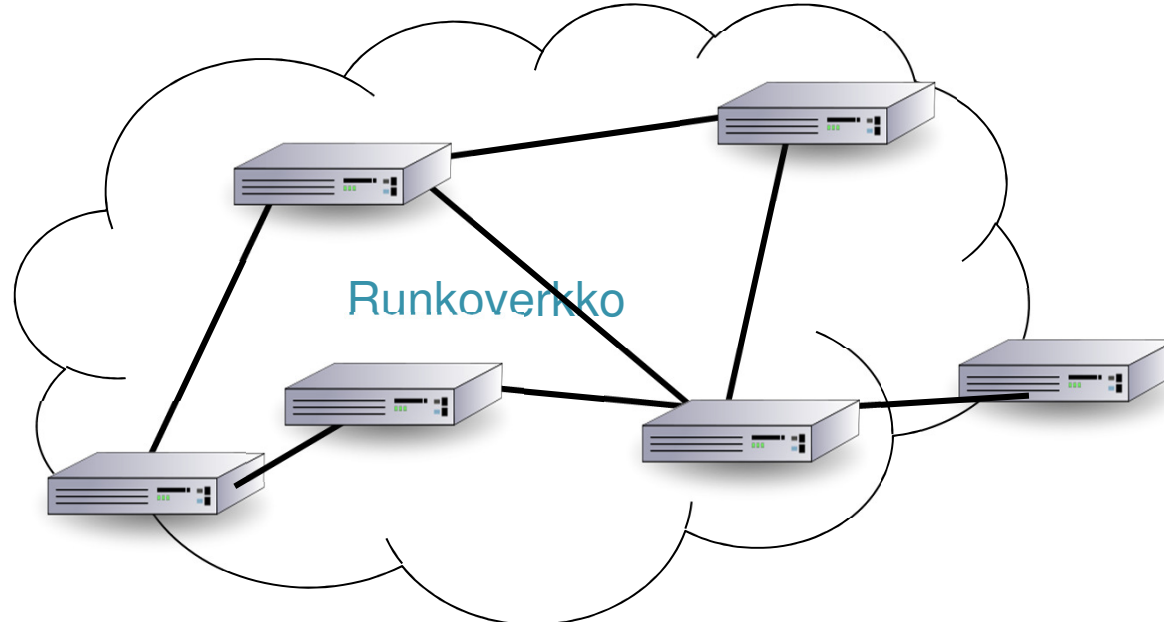
- Kumpi tahansa voi ilmoittaa **FIN** eli "en aio lähettää enää tavuja virtaan"
- Toinen puoli ilmoittaa "**FIN**" kun on itse valmis
- Yhteys voi jäädä puoliksi auki

VERKKOKERROS

Internetin rakenne

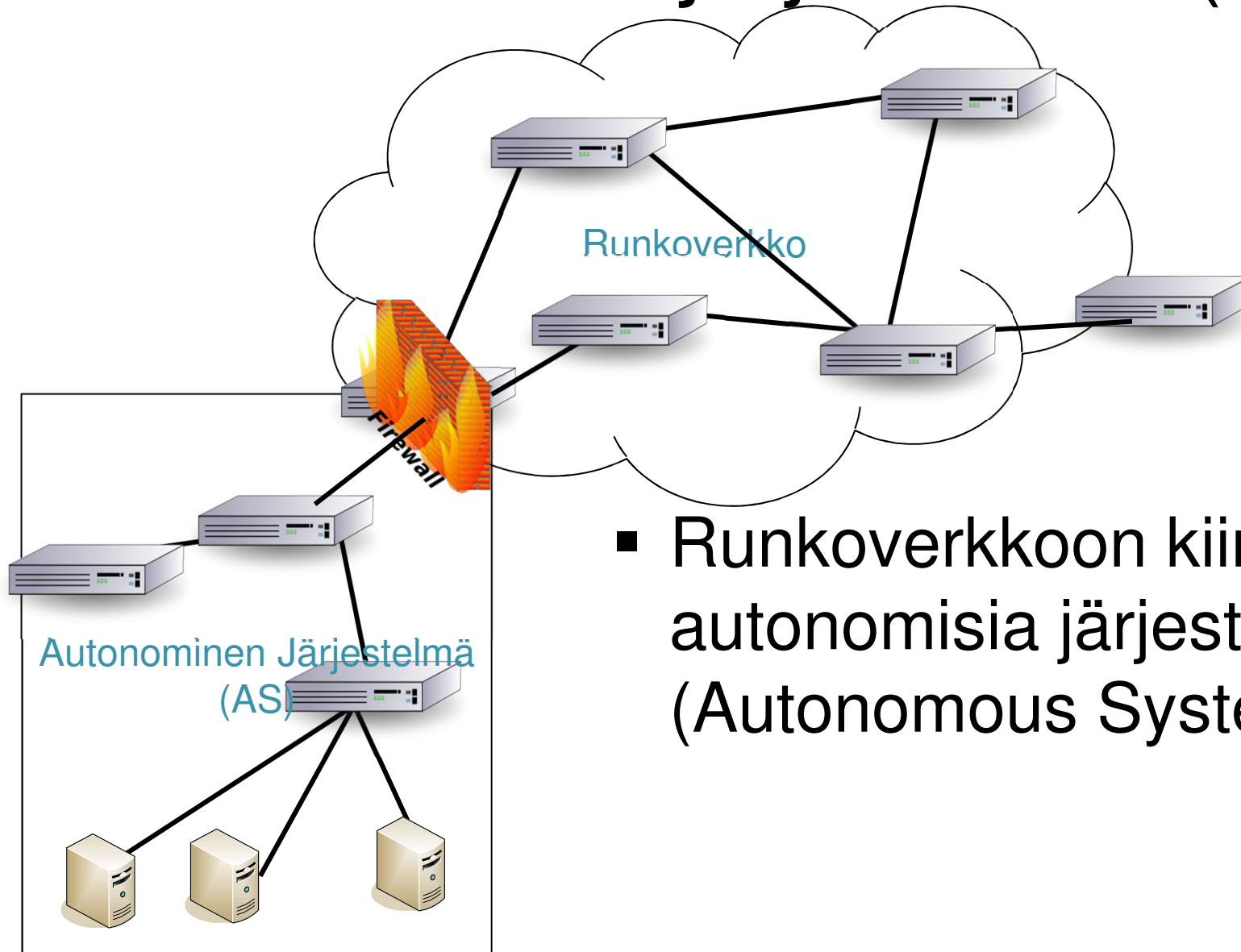


Runkoverkko



- Internet on rakennettu ARPANETin päälle
 - **Advanced Research Projects Agency Network** suunniteltiin 1960-luvulla kestäämään rauhaa rakastavan Neuvostoliiton ydinisku
- Ei keskitettyä hallintaa, ei keskitettyä hallitsijaa
 - Voi pojat mikä sotku
 - → Internet kestää ydiniskun, muttei välttämättä töpeksivää adminia (Esim. Pakistan ja YouTube)

Autonomiset järjestelmät (AS)



- Runkoverkkoon kiinnittyy autonomisia järjestelmiä (Autonomous Systems)

Autonomiset järjestelmät (jatkoa)

- Autonomiset järjestelmät ovat hallinnollisesti yhtenäisiä järjestelmiä, jotka ovat liittyneet kiinni runkoverkkoon
 - Harvardin yliopisto, Sonera, TKY, Vatikaani
- AS voi olla
 - Multihomed: kiinni runkoverkossa monesta kohtaa
 - Stub: Kiinni vain yhden toisen AS:n kanssa
 - Transit: suostuu välittämään muille verkoille viestejä (ISP)

IP(v4)

- IP = The Internet Protocol
- RFC 791
- Lähettää datagrammeja verkon yli (vs. Paketit)
- Epäluotettava, yhteydetön
- Pakettikoko vaihtelee, paketteja saatetaan hajoittaa ja koota siirtäessä
- Internet Control Message Protocol (ICMP) virheiden välittämiseen takaisin lähettäjälle

IPv4

- Osoitteet muotoa a.b.c.d, missä a, b, c ja d ovat lukuja välillä 0-256 (4 tavua muistissa)

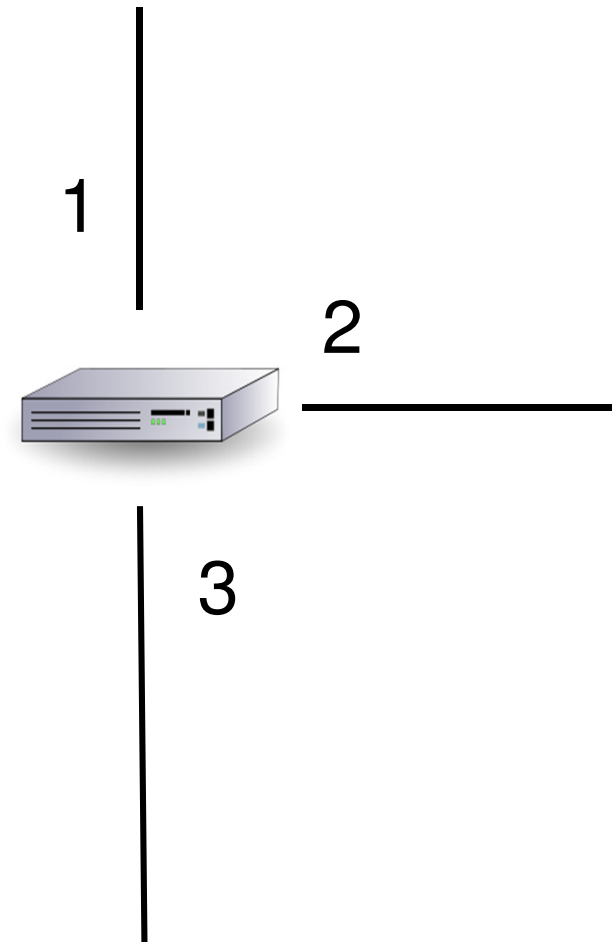
Versio	Otsikon pituus	TOS	Kokonaispituus	
ID			Lippuja	
TTL	Protokolla		Otsakkeen tarkistussumma	
Lähdeosoite				
Kohdeosoite				
Optioita			Täytettä	
Data				

IP-reititys

Jokainen reititin osaa reitittää sille tulevat IP-paketit reititystaulunsa perusteella

Reititystaulun muodostamiseen käytetään reititysprotokollia ja -algoritmeja.

Yksittäisen koneen täytyy tietää vain oletusreitittimen osoite



Reititystaulu	
IP-osoitealue	Suunta
82.130.0.0-82.130.63.255	1
62.237.152.0-62.237.159.255	2
130.233.0.0 - 130.233.255.255	3
...	...

- Jokaisella reititysaskeleella reititin vähentää IP-datagrammin TTL-kentän arvoa yhdellä
- Jos TTL:n arvoksi tulee 0 -> virheviesti lähettäjälle
- Estää pakettia jäämästä ikuisiksi ajoiksi verkkoon

IP-verkkojen määrittäminen

- **IP-osoitteiden reititys ja verkkojen määrittäminen perustuu binäärilukuesitykseen**
- **62.237.153.157 =
111110.11101101.10011001.10011101**
- **Ensimmäiset X bittiä ovat osoitteen verkko-osaa, loput määrittelevät koneen osoitteen**
- **Monta tapaa ilmoittaa verkko:**
 - **62.237.152.0-62.237.155.255**
 - **62.237.152.0/22**
 - **62.237.152.0 netmask = 255.255.252.0**

IP-verkon määrittäminen

- Kaksi jälkimmäistä jakavat osoitteen verkko-osaan ja laiteosaan
- **11110.11101101.10011001.10011101**
- Esimerkissämme ensimmäiset 22/32 bittiä ovat verkko-osaa eli samat kaikille verkon laitteille
- Loput 10/32 identifioivat yksittäisen laitteen verkon (Aalto Open) sisällä
- Verkkoon mahtuu $2^{10} = 1024$ laitetta
- Verkkojen jako tällä tavoin tekee reitityksestä helppoa (ref: Tietorakenteet ja Algoritmit)

IPv4 varatut osoitteet

Osoitealue	Varauksen aihe
10.0.0.0/8	Yksityiset verkot
127.0.0.0/8	Loopback
169.254.0.0/16	Zero config -verkot
172.16.0.0/12	Yksityiset verkot
192.168.0.0/16	Yksityiset verkot
224.0.0.0/4	Multicast
255.255.255.255	Broadcast

- Yksityisiä verkkoalueita voi käyttää sisäverkossa. Reitittimen on tällöin suoritettava verkko-osoitteen muunnos (Network Address Translation) NAT sisäverkon rajalla
- Muitakin varattuja on

MAP OF THE INTERNET THE IP4 SPACE, 2006



THIS CHART SHOWS THE IP ADDRESS SPACE ON A PLANE USING A FRACTAL MAPPING WHICH PRESERVES GROUPING -- ANY CONSECUTIVE STRING OF IP₄ WILL TRANSLATE TO A SINGLE COMPACT, CONTIGUOUS REGION ON THE MAP. EACH OF THE 256 NUMBERED BLOCKS REPRESENTS ONE /8 SUBNET (CONTAINING ALL IP₄ THAT START WITH THAT NUMBER). THE UPPER LEFT SECTION SHOWS THE BLOCKS SOLD DIRECTLY TO CORPORATIONS AND GOVERNMENTS IN THE 1990s BEFORE THE RIRs TOOK OVER ALLOCATION.

0	1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20	21
22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43



 = UNALLOCATED BLOCK

■ <http://xkcd.com/195/>

Localhost = 127.0.0.1



IPv6

- Pidemmät osoitteet: 128 bittiä (vs 32)
- fe80:0:0:0:e91a:6df0:a982:217b (nollat voi jättää pois ja merkata "::")
fe80::e91a:6df0:a982:217b

Versio	Liikenneluokka	Vuon nimi	
Datan pituus		Seuraava otsikko	Hyppyraja
Lähdeosoite			
Kohdeosoite			

IPv4 vs IPv6

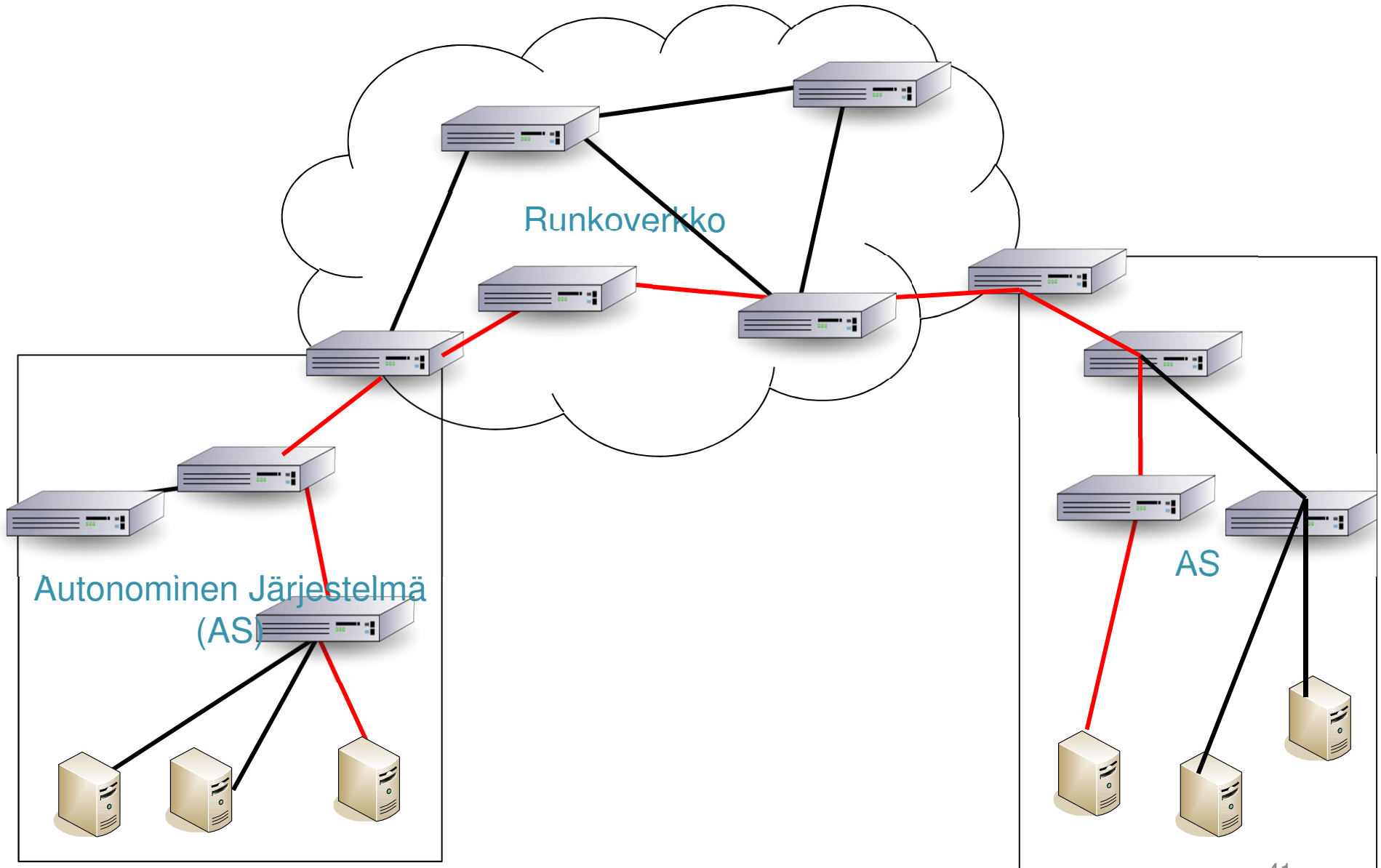
- IPv4:n osoiteavaruus 2^{32} on täynnä
 - NAT vähentää ongelmia
- Kotien päätelaitteet (ADSL-modeemit, jne) eivät tue IPv6:sta laajalti
- Kankea moneen teknisesti hienoon juttuun
- ”Pomminvarma”
- IPv6:n osoiteavaruus 2^{128} riittää kaikille maailmankaikkeuden alkuhiukkasille
- Käytössä runkoverkossa käytännössä kaikkialla
- Taipuu kaikkeen tosi siistiin
- Kaikkea ei ole hiottu loppuun

Network Address Translation

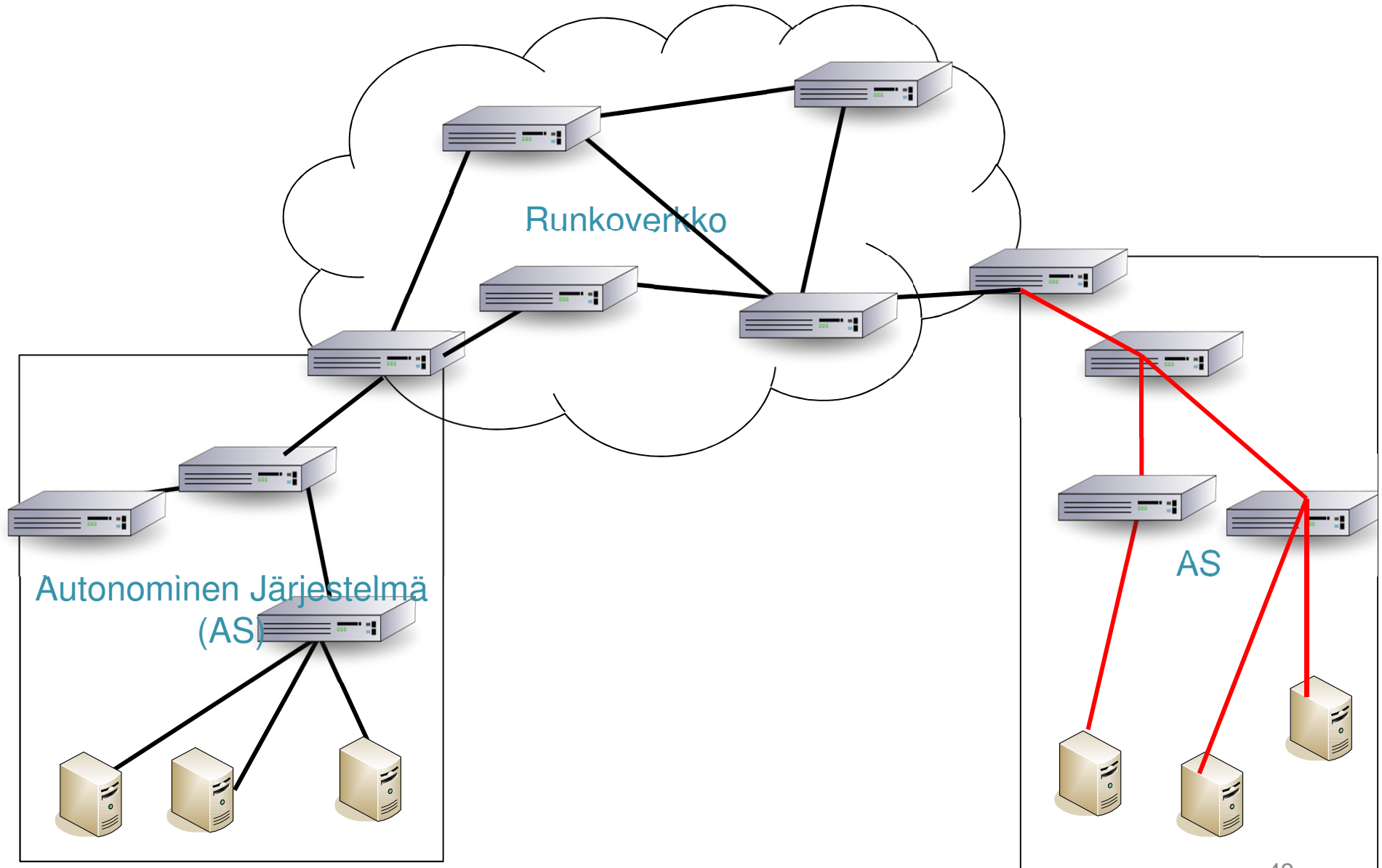
- Idea: portteja on paljon, IP-osoitteita vähän
 - Jokainen kone ei tarvitse jokaista mahdollista porttia
 - Jokaiselle haluavalle ei riitä IPv4-osoitetta
 - Kuluttajat saavat yleensä yhden palveluntarjoajalta
- Laitetaan väliin laite, joka piilottaa sen takana olevan rakenteen
 - Pitää kirjaa mikä portti ulkomaille vastaa minkä sisäverkon IP+portti-yhdistelmää
 - Käyttävät varattuja osoiteavaruuksia
- Asiakas-palvelin –paradigman palvelimena olo NATin takana vaatii lisävaivaa
 - Myös peer-to-peerin vertaisena

LÄHETYSTYYPIT

Unicast



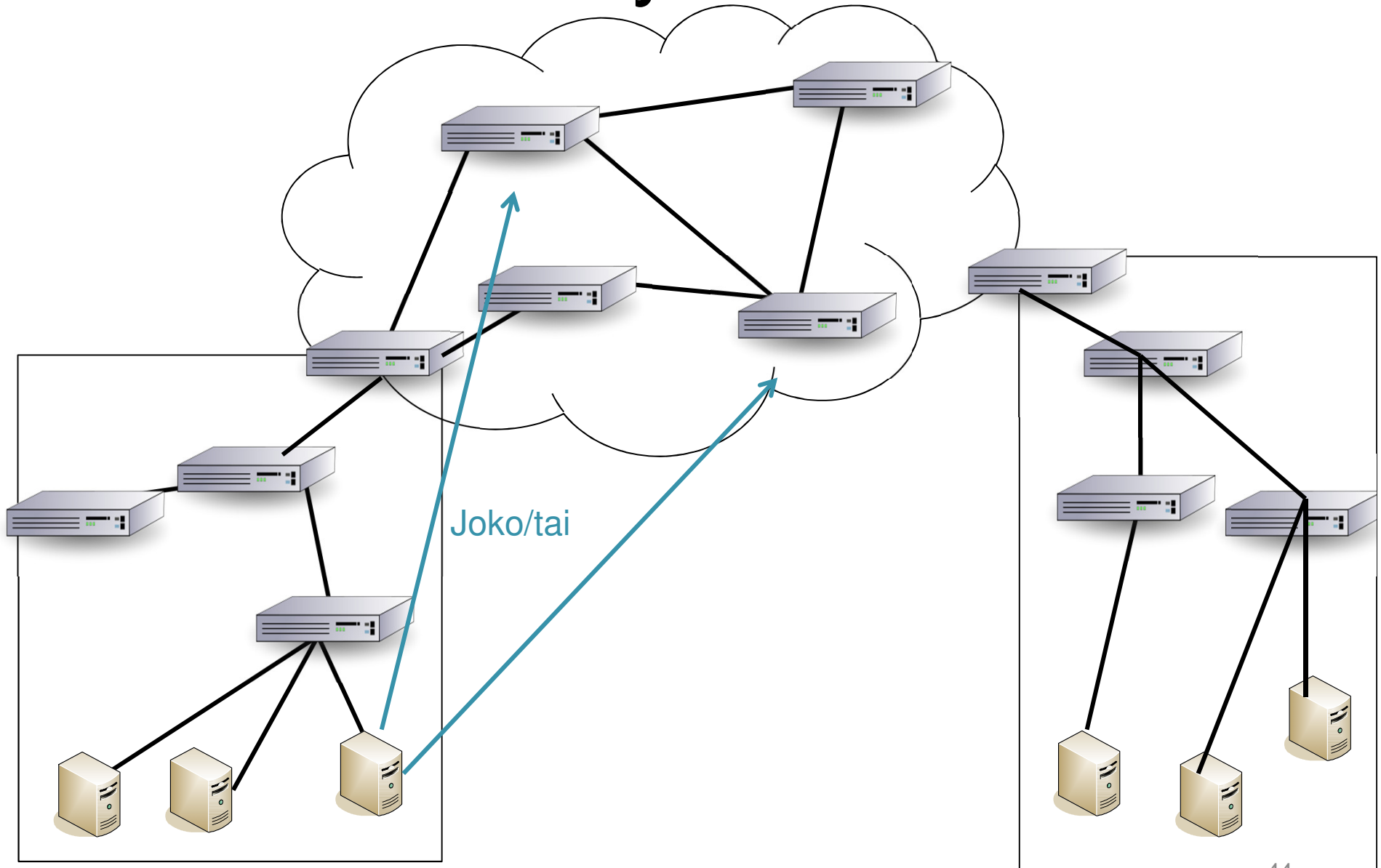
Broadcast



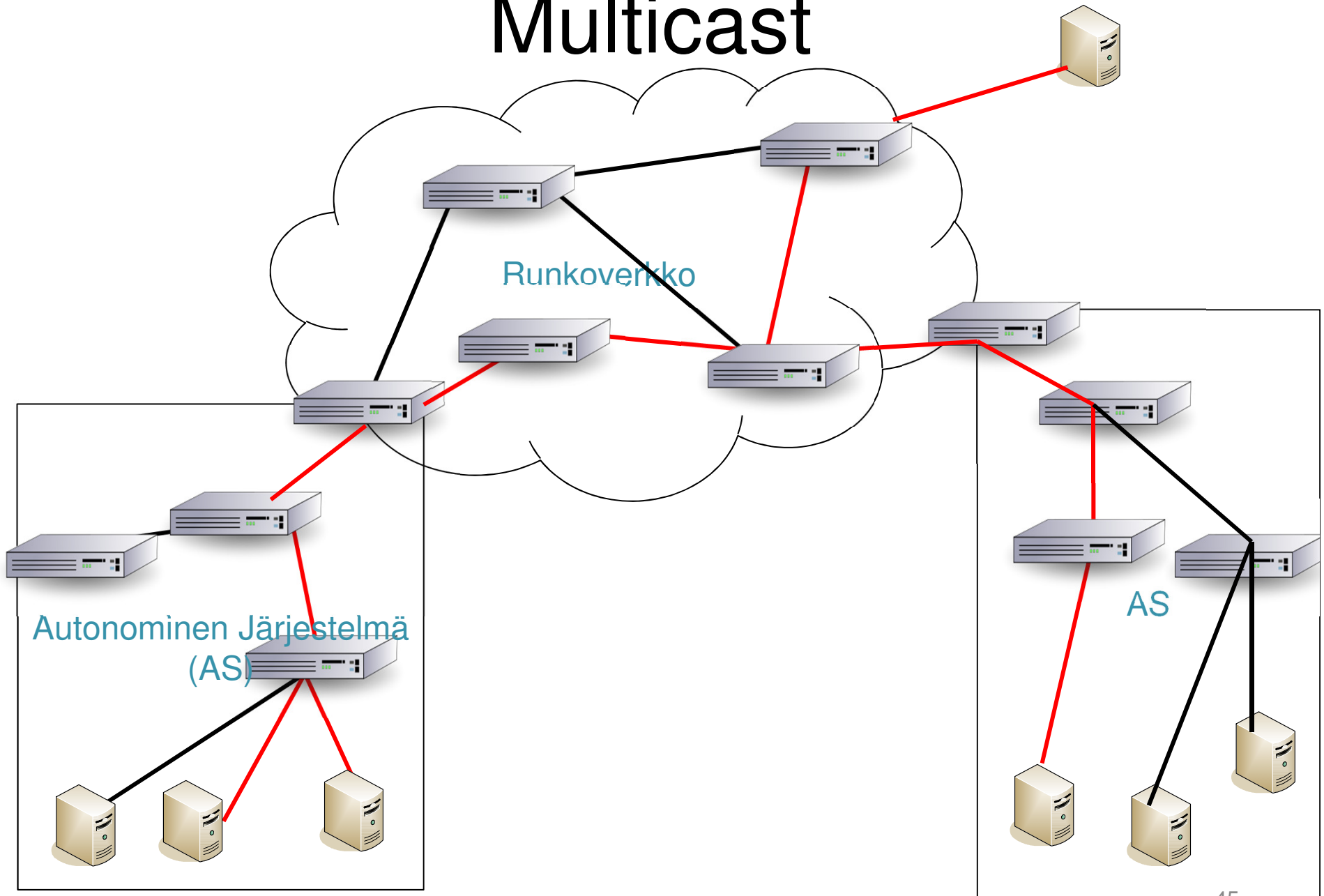
Lähetystyypit

- IP tukee useampaa eri tapaa lähettää tietoa
- Unicast on tavallinen lähetys yhdelle hengelle
- Broadcast on lähetys kaikille verkon laitteille
 - Käytetään mm. DHCP-protokollan ensimmäisessä viestissä
 - Voidaan lähettää verkon hallintadataa yms
 - Jokaisen aliverkon viimeinen IP on varattu sen Broadcast-osoitteeksi

Anycast



Multicast



Lähetystyypit

- Anycastissa monella koneella on sama IP-osoite ja viesti riittää saada mille tahansa niistä
 - Mm. Osa DNS-juuripalvelimista tukee tätä
 - Ei oikein tue yhteyksien rakentamista
- Multicastissa sama paketti viedään usealle sitä pyytäneelle vastaanottajalle
 - Paketin kopioiminen tai monistaminen ei maksa mitään
 - IGMP-protokollalla liitytään multicast-osoitteen vastaanottajaksi

TCP/IP

- TCP/IP:ssä hienoa on luotettava tavuvirta best effort –siirron päällä
- Perustuu kuitenkin kaikkien osapuolien hyväntahtoisuuteen

Ensi viikolla

