Aalto-yliopisto
Perustieteiden
korkeakoulu

Verkkokerros 1: IP-protokolla

CSE-C2400 Tietokoneverkot

Kirjasta 4.1-4.2, 4.4. ja 8.7

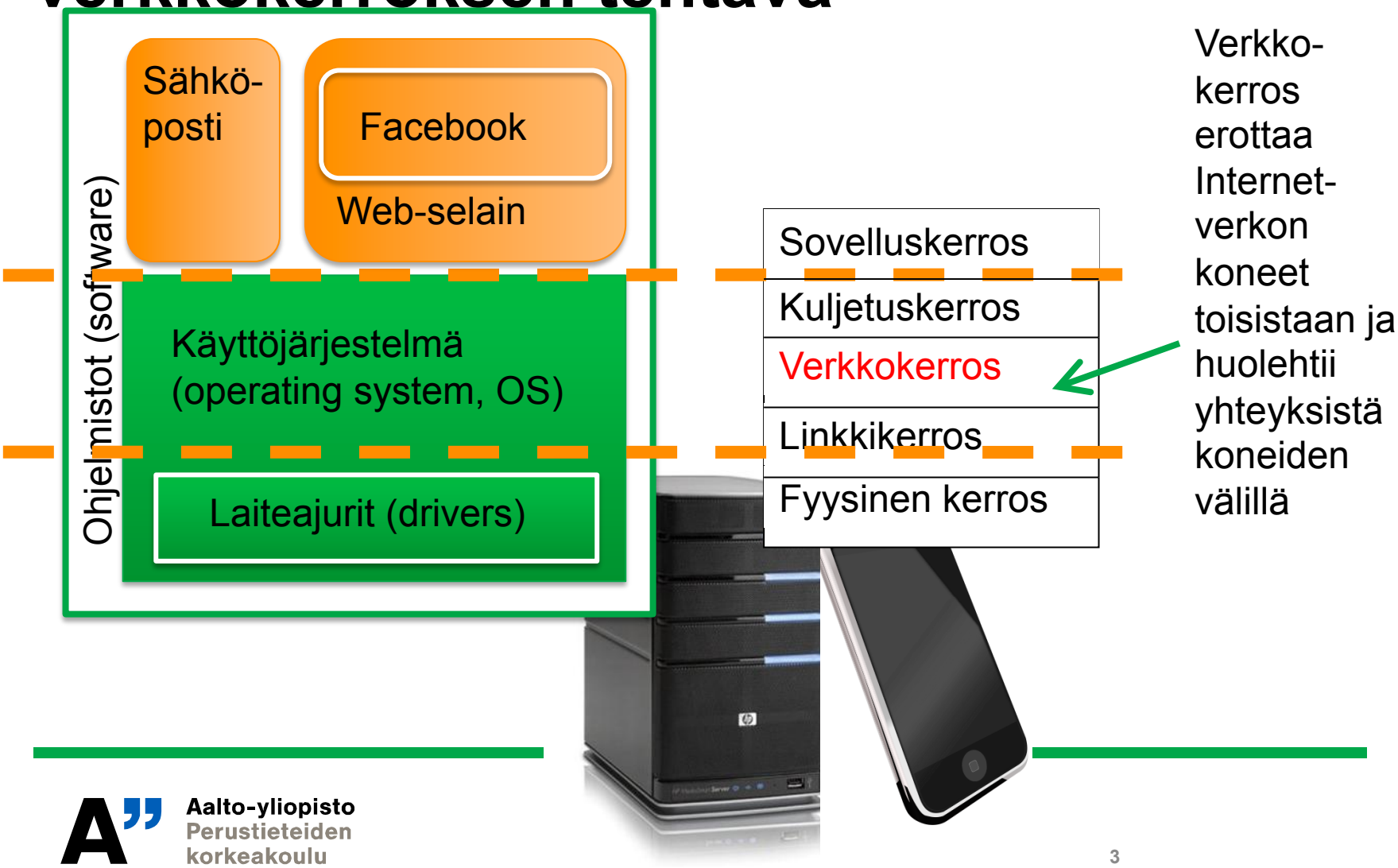
Sanna Suoranta

Verkkokerros

- Tällä luennolla
  - Yleistä verkkokerroksessa erityisesti Internet-verkossa
  - IP-osoitteet, NAT- ja DHCP-protokollat
  - IP-protokolla (versiot 4 ja 6)
  - Virhetilanteet ja ICMP-protokolla
  - Turvallinen IP

- 25.2. luennolla kahden viikon päästä jatketaan
  - Reitittimen toiminta
  - Reititys Internet-verkossa ja internet-verkoissa
  - Yleislähetys (broadcast) ja monilähetyksen (multicast) reititys

Internet-protokollapino ja verkkokerroksen tehtävä



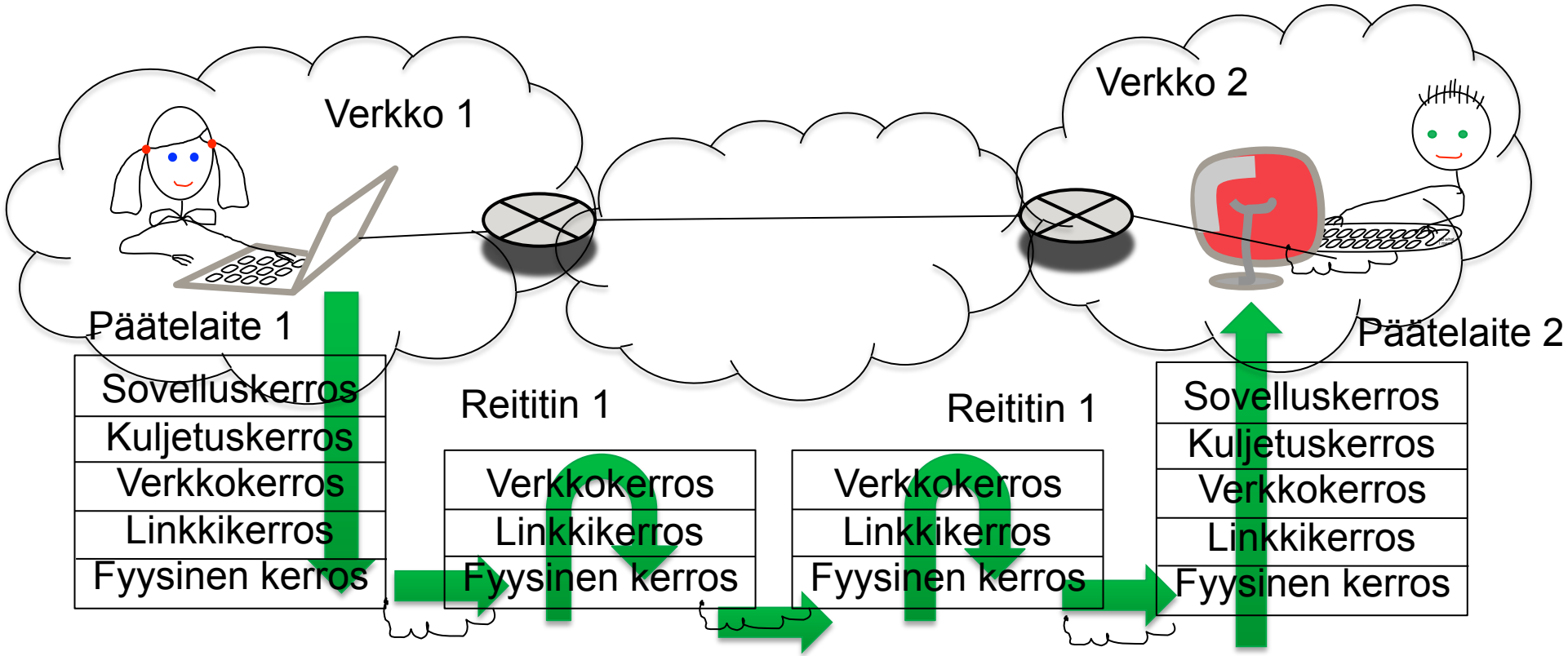
Verkko-kerros erottaa Internet-verkon koneet toisistaan ja huolehtii yhteyksistä koneiden välillä

Verkkokerroksen tehtävä

- (edellisillä luennoilla käsitellyn) kuljetuskerroksen tehtävä on viestien välittäminen eri koneiden eri prosessien (esim. Web-palvelin ja -sovellus) välillä verkon yli
- Verkkokerroksen tehtävä on huolehtia verkossa
  - Pakettien edelleenlähetyksestä (forwarding), eli mitä tehdään, kun yksittäinen paketti saapuu reitittimeen (tällä luennolla) ja
  - Reitityksestä (routing), eli miten reitittimet sopivat keskenään jo ennen pakettien välittämistä, että mihin mikäkin paketti välitetään, jotta se löytää perille mahdollisimman tehokkaasti. Tätä tietoa käytetään sitten hyväksi paketteja edelleenlähetettäessä yllä. (reitityksestä kahden viikon päästä)

Verkkokerroksen ominaisuuksia

- Myös verkkokerros voi tarjota erilaisia palveluita
  - Luotettava tai ei, min. kaistanleveys, max. viiveen vaihtelu (jitter), tiedonsalaus, etc.
- Virtuaalipiiri (virtual circuit) vs. Pakettiverkko (datagram net)
  - 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
  - Paketti(kytkentäinen)verkko tarjoaa yhteydettömän palvelun
    - Paketteja liikutellaan kohdeosoitteen avulla yksittäin
    - Reitittimet ei joudu pitämään tilaa yhteyksistä (niitä ei ole!)
    - Esim. Internet Protokolla (IP)
- Tällä luennolla käsitellään jatkossa vain Internet-protokollaa (IP), joka on pakettikytkentäisen verkon protokolla



- Sovelluskerroksen data pakataan kuljetuskerroksen tietosähkeeseen, joka pakataan verkkokerroksen pakettiin
- Reitittimet katsovat edelleenlähetystaulustaan, mihin rajapintaan paketti lähetetään seuraavaksi
  - Reitittimet ovat siis verkkokerroksen laitteita

Miten tunnistetaan kone, jolle paketti on tarkoitettu?

- Verkkokerroksen tunnisteina käytetään globaalisti uniikkia IP-osoitteita (address)
- Oikeastaan IP-osoite kertoo verkkoliittymän (network interface) osoitteen, sillä joskus yhdellä laitteella voi olla useita IP-osoitteita (eri verkkotekniikoille tai esim. reititin)
  - IPv4-osoite on 32 bittiä pitkä, esim. 130.233.224.196 (minkäniminen kone? ☺)
  - IPv6-osoite on 128-bittinen, esim. 2001:db8::1420:57ab ja 68E6:8C64:FFFF:FFFF:0:1180:95A:FFFF

Sovelluskerros - nimi
Kuljetuskerros - portti
Verkkokerros - IP-osoite
Linkkikerros - MAC-osoite
Fyysinen kerros - ”piuhan” pää

IPv4-osoitteen kaksi osaa: verkko ja rajapinta

10000010 11100000	11011111 11000100

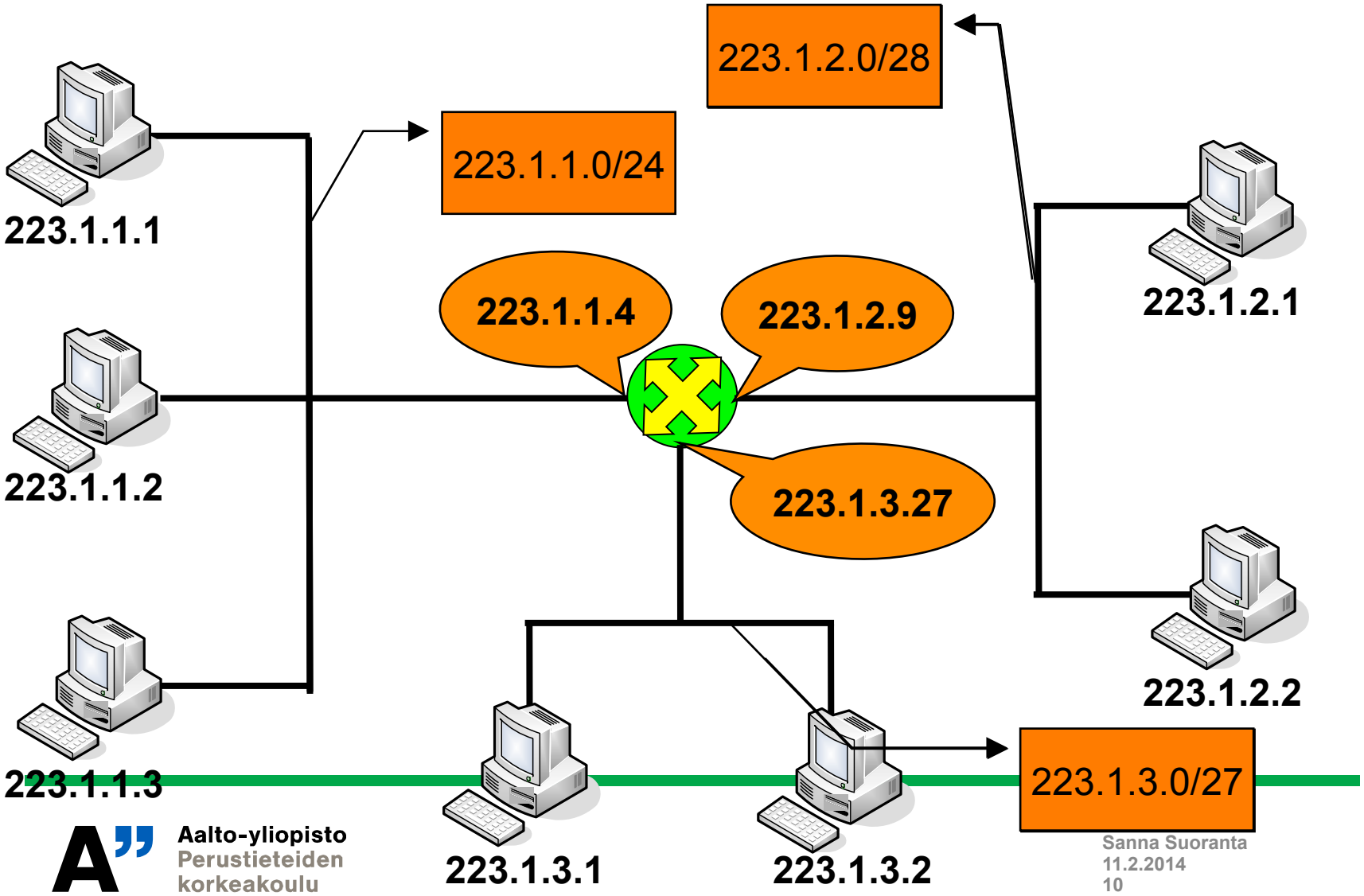
- Alkuosa kertoo verkon (network prefix) ja loppuosa identifioi verkkorajapinnan (host id)
  - Reitittimet välittävät paketteja verkko-osan perusteella
  - Alunperin käytettiin vakiomittaisia luokkia (A, B ja C)
- Nykyään liukuva raja käyttäen CIDR-tekniikkaa (Classless Interdomain Routing): kerrotaan verkko-osoite (ensimmäinen osoite) ja merkitsevien bittien määrä
  - 130.233.0.0/16 on Aallon verkko-osoite (vanha B-luokan verkko)
  - Huom: osoitetta käsitellään binäärinä, vaikka se esitetään ihmiselle helpommin ymmärrettävässä desimaalimuodossa

Aliverkot ja verkkomaski

Kone:	130.233.224.196/22		
Kone:	10000010 11100000	11011111	11000100
Verkko:	10000010 11100000	11011100	00000000
Verkko-maski	11111111 11111111	11111100	00000000

- Verkko voidaan jakaa vielä aliverkkoihin “lainaamalla” kone-osan alusta bittejä aliverkkoa varten
  - Aliverkon osoite: 130.233.220.0/22
  - Aliverkkoon kuuluvat osoitteet: 130.233.220.0-130.233.223.255
  - Alin osoite on verkon osoite ja ylin yleislähetysosoite, loput sopivat isäntäkoneille, eli koneita voi olla 2^10-2=1022 konetta

Esimerkki: IP-verkko ja osoitteet



Erikoisosoitteet

- Mikä tahansa; lähettäjällä ei ole vielä IP-osoitetta
  - 0.0.0.0 (IPv4) ja 0:0:0:0:0:0:0:0 (= ::) (IPv6)
- Paikallinen yleislähetysosoite (reititin ei välitä eteenpäin)
  - 255.255.255.255 (kaikki bitit ykkösiä), IPv6 ei käytä yleislähetystä vaan sen sijaan “kaikki koneet” -ryhmälähetystä
- Verkon yleislähetysosoite (broadcast)
  - Esim. 222.1.16.255/24 (koneosan bitit ykkösiä)
- Loopback-osoite – “takaisin itselle”
  - 127.0.0.1 (mikä tahansa 127-alkuinen osoite, IPv4)
  - 0:0:0:0:0:0:0:1 (=::1, IPv6)
  - Näppärä testatessa omia ohjelmia paikallisesti, ei välitetä lainkaan ulos koneesta

Yksityiskäyttöön varatut osoitteet

- Vain paikalliseen käyttöön (IPv4)
  - 10.0.0.0/8 (alunperin Arpanetille varattu osoiteavaruus)
  - 192.168.0.0/16
  - 172.16.0.0/12
- Linkki- ja toimipaikkakohtaiset osoitteet (IPv6)
  - Alkaa biteillä 1111111010 (linkkikohtainen), ei välitetä ulos fyysisestä verkosta
  - 1111111011 + aliverkko (toimipaikkakohtainen), ei välitetä ulos organisaation verkosta
- Runkoverkko kieltäytyy reitittämästä näitä
  - Voi käyttää vapaasti lähiverkossa, mutta
  - Ei voi viestiä (suoraan) Internet-verkkoon – apuna käytetään NAT-tekniikkaa

IPv6-osoitteet

Yksilähetysosoitteen etuliite on yleensä 001

Toimipaikan tunniste (global routing prefix) (vaihtuvamittainen)

Aliverkon (linkin) tunniste (vaihtuvamittainen)

Koneen tunniste (EUI-64-formaatissa)

- Verkko-osa mahdollista jakaa kahtia: toimipaikka ja sen aliverkot
- Rajapinnan ID voidaan johtaa esim verkkokortin Ethernet-osoitteesta
- IPv4-osoitteen voi “upottaa” IPv6-osoitteeseen: alkuun nollia, juuri ennen osoitetta joko 0000 (molempia tuetaan) tai FFFF (IPv4-noodi)

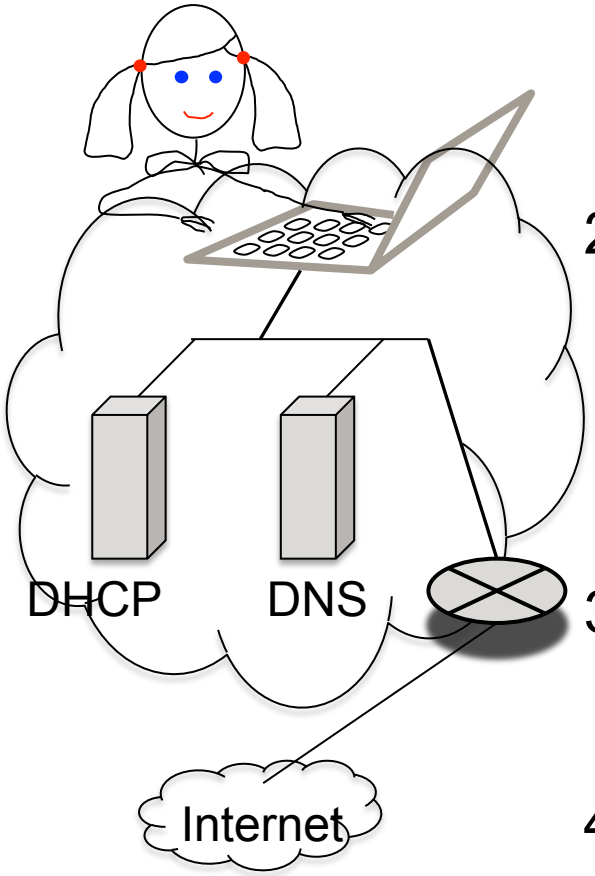
Mistä saa verkolleen osoitteen?

- Organisaation sisällä vastuulliselta taholta oma aliverkko
- Internet-palveluntarjoajalta (ISP) voi ostaa oman verkon
- ISP saa osoitteitaan oman alueensa Internet-rekisteriltä (Regional Internet Registry, RIR) – näitä on viisi
  - Euroopassa Réseaux IP Européens Network Coordination Centre (RIPE NCC)
- Alueen rekisteri saa osoitteet ICANNilta (Internet Corporation for Assigned Names and Numbers)
  - Viimeinenkin IPv4-verkko on jaettu 2011! Eli IPv4-osoitteet ovat käytännössä nyt loppuneet
  - IPv6-osoitteita on joka hiekanjyvälle, joten niitä riittää hyvin
- Miten IPv4 voi vielä olla käytössä? Miten osoitteita yhä riittää?

Miten päätelaite saa osoitteen itselleen?

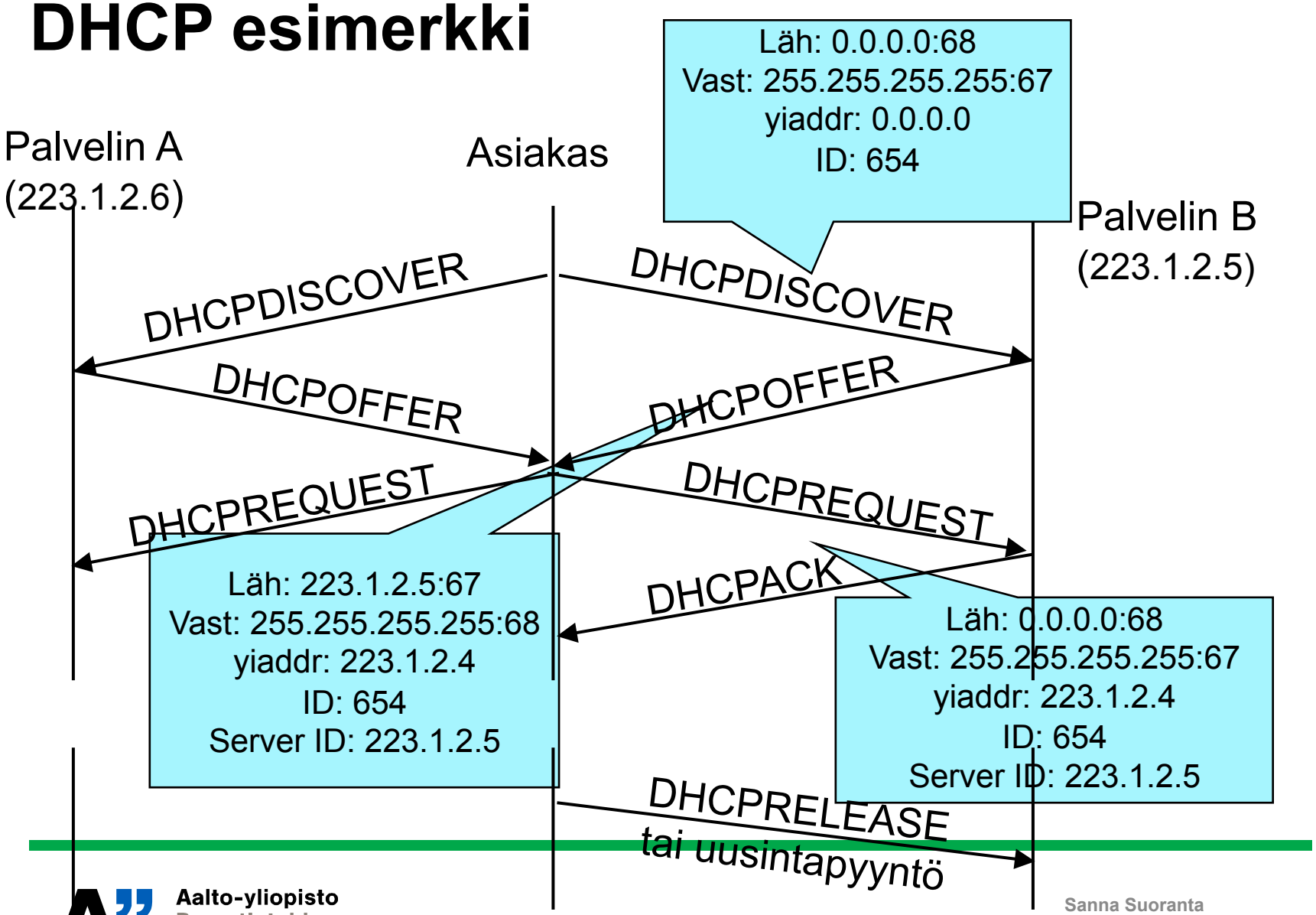
- Päätelaitteelle voidaan asettaa kiinteä osoite verkkoasetuksista käsin (lähinnä palvelimille nykyään)
- Yleensä käytetään DHCP-protokollaa (Dynamic Host Configuration Protocol): kolme tapaa
  - Staattinen allokointi: Aina sama osoite tietylle päätelaitteelle linkkikerroksen MAC-osoitteen perusteella (ylläpitäjä konffaa)
  - Automaattinen allokointi: Joku osoite ekalla kerralla, sitten aina sama MAC-osoitteen perusteella (ei tarvi manuaalista konfausta)
  - Dynaaminen allokointi: Päätelaite saa jonkin osoitteista “lainaan” väliaikaisesti, mutta lainaa voi pyytää jatkettavaksi. Osoite voi vaihtua joka kerta, kun laite liittyy verkkoon
- DHCP tarvitsee palvelimen lähiverkkoon (tai välityspalvelimen)
  - Osoitteen lisäksi päätelaite saa muutakin tietoa verkosta, esim. aliverkkomaskin, oletusyhdyskäytävän (=reititin) ja DNS-palvelimen osoitteet

DHCP



1. Asiakas lähettää DISCOVER-viestin UDP:n porttiin 67 käyttäen yleislähetysosoitetta 255.255.255.255 (lähettäjän osoitteena 0.0.0.0)
   - Transition ID tunnisteeksi
2. Palvelin huomaa viestin ja lähettää UDP:llä porttiin 68 OFFER-viestin yleislähetysosoitteeseen
   - Transition ID, tarjottu IP-osoite (yiaddr), osoitteen laina-aika DHCP-palvelimen IP-osoite, verkkomaski, jne
3. Asiakas lähettää REQUEST-viestin
   - Edelleen yleislähetysosoitteeseen
   - Samat tiedot kuin OFFER-viestissä
4. Palvelin vastaa ACK-kuittauksella
   - Samat tiedot kuin OFFER-viestissä

DHCP esimerkki



Toinen tapa säästää osoitteita: NAT (Network/Port Address Translation)

- Reitittimellä yksi (tai muutama) julkisen verkon osoite
- Sisäverkossa käytetään yksityisosoitteita
  - Yksityisosoitteet vaihdetaan reitittimessä julkisiin ja päinvastoin
  - Reititin pitää kirjaa käytetyistä osoite (ja portti) –pareista
  - Huom! Reitittimessä on verkkoyhteyden tila
  - Päätelaite ei (välttämättä) huomaa, että yhteyden välissä on NAT-laite (eikä sitä, että sillä on käytössä vain yksityisosoite)
- Huonot puolet – NAT rikkoo päästä-päähän-yhteyden
  - Internetistä ei voi aloittaa yhteyttä NATin takana olevalle sisäverkon koneelle (jollei käytetä kiinteää NAT-muunnosta)
  - Kaksi NATin takana olevaa päätelaitetta ei pysty viestimään, vaan avuksi tarvitaan STUN-, ICE-, tai TURN-välityspalvelimia

NAT esimerkki

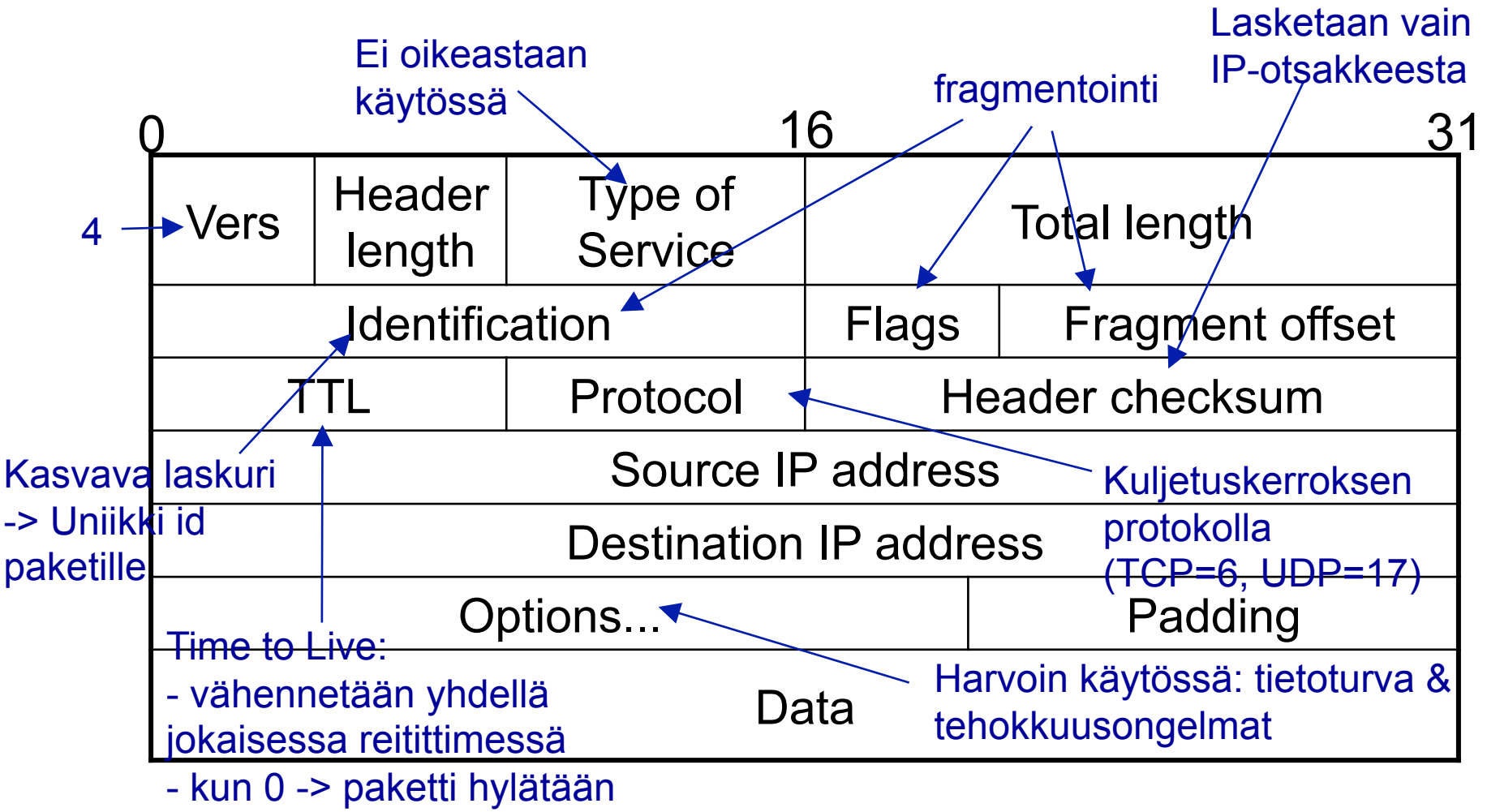
- IP-paketin muuttuminen matkalla: reititin vaihtaa osoitteita ja portteja Internetin ja sisäverkon rajalla

	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

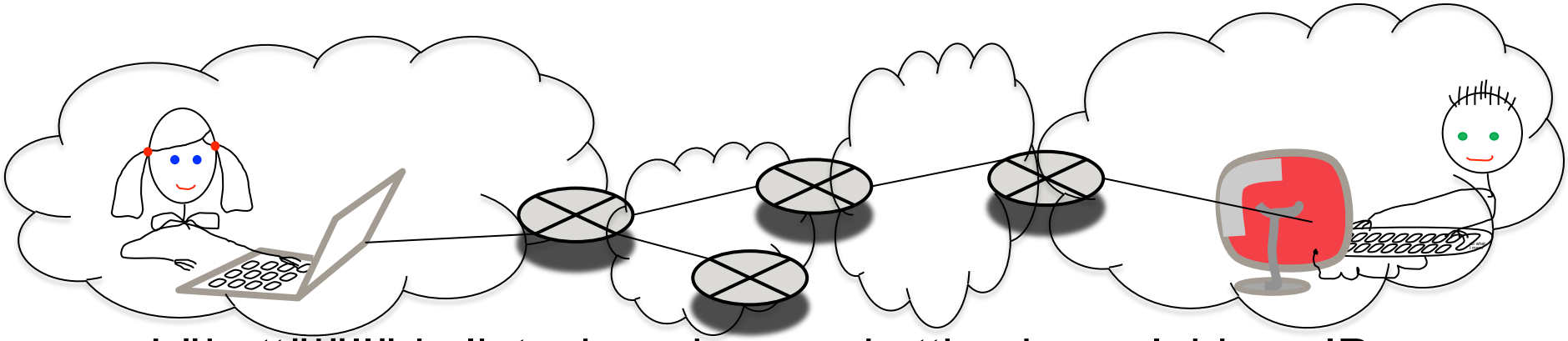
IP-protokollan käyttö ja viestit

- IPv4 alunperin määritelty RFC 791 (vuodelta 1981)
- IPv6 määritelty RFC 2460 (jo vuonna 1998), 2462, 4291
- Epäluotettava ja yhteydetön palvelu, viestien perillemenoa ei varmenneta
  - Reitittimet käsittelevät jokaisen IP-paketin erikseen
  - Lähettäjä saa virheilmoituksen vain, jos IP ei tiedä, miten toimitttaa viesti perille – lähettäjän vastuulle jää, miten sitten toimitaan
- Apuprotokolla ICMP (Internet Control Message Protocol) virhetilanteiden käsittelyyn

IPv4-otsake

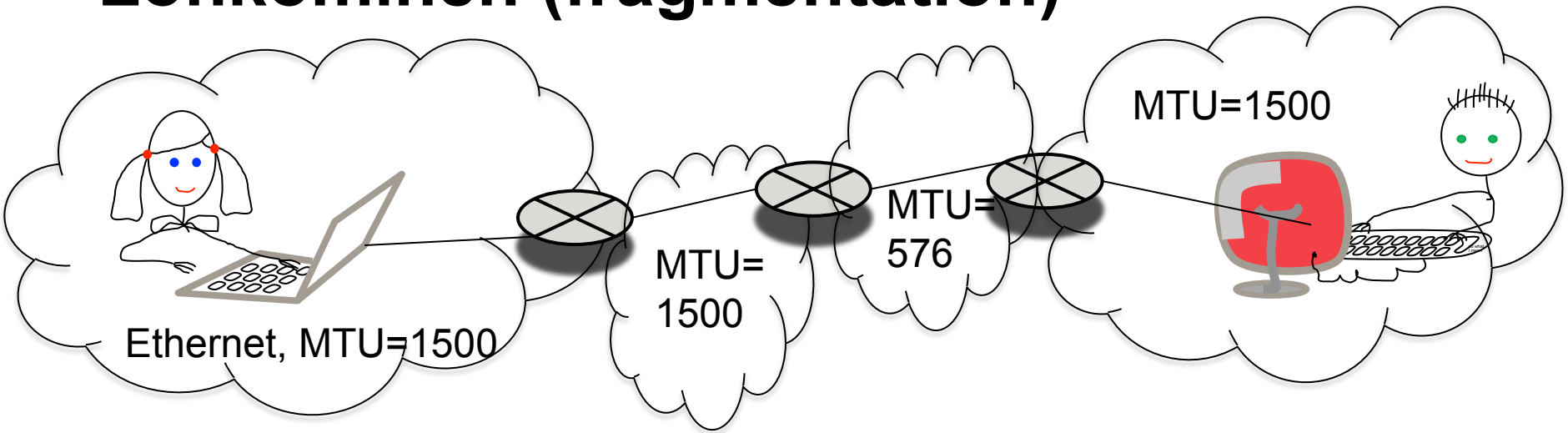

Ei oikeastaan käytössä
fragmentointi
Lasketaan vain IP-otsakkeesta
0
16
31
4
Vers
Header length
Type of Service
Total length
Identification
Flags
Fragment offset
TTL
Protocol
Header checksum
Source IP address
Destination IP address
Options...
Padding
Data
Kasvava laskuri -> Uniikki id paketille
Kuljetuskerroksen protokolla (TCP=6, UDP=17)
Time to Live:
- vähennetään yhdellä jokaisessa reitittimessä
- kun 0 -> paketti hylätään
Harvoin käytössä: tietoturva & tehokkuusongelmat

Paketin lähettäminen ja välittäminen



- Lähettäjällä kuljetuskerroksen paketti enkapsuloidaan IP-pakettiin ja muodostetaan sille IP-otsikko
  - näin saatu paketti enkapsuloidaan linkkikerroksen protokollan kehykseen ja lähetetään oletusreitittimelle
- Reititin tarkistaa otsikon tarkistussumman, ja jos se on ok, katsoo vastaanottajan osoitteen perusteella, mihin rajapinnoista viesti seuraavaksi välitetään,
  - Reititin vähentää TTL-kentän arvoa yhdellä ja laskee uuden tarkastussumman otsikolle ja enkapsuloi viestin seuraavan verkon linkkikerroksen protokollaa käyttäen ja lähettää sen eteenpäin

Lohkominen (fragmentation)



- Reitillä olevien eri linkkikerroksen tekniikoita käyttävien verkkojen kehysten koko vaihtelee
  - MTU – Maximum Transmission Unit; taattu minimi 68 oktettia IPv4 ja 1280 IPv6 (näiden käyttäminen olisi erittäin epätehokasta)
- Reititin voi joutua lohkomaan paketin useampaan fragmenttiin
  - ID jokaisessa sama, fragment offset kertoo palasen sijainnin alkupeäisessä paketissa ja liput kertovat, onko palasia lisää
- Vastaanottaja kokoaa fragmentit yhdeksi IP-paketiksi

Lohkomisen ongelmat

- Epätehokasta; otsikkojen osuus (overhead) kasvaa
- Monimutkaistaa reitittimien ja vastaanottajan toimintaa
  - Vastaanottajan pitää puskuroida palaset kunnes koko paketti saatu perille
  - Kaikki palat pitää uudelleenlähettää, jos yksikin katoaa (kuljetuskerros ei edes tiedä näin tapahtuneen)
- Tietoturvaongelma, esim. Palvelunestohyökkäys pommittamalla kohdetta väärinrakennetuilla fragmenteilla

Lohkomisen välttäminen polun MTU:n selvittämisellä

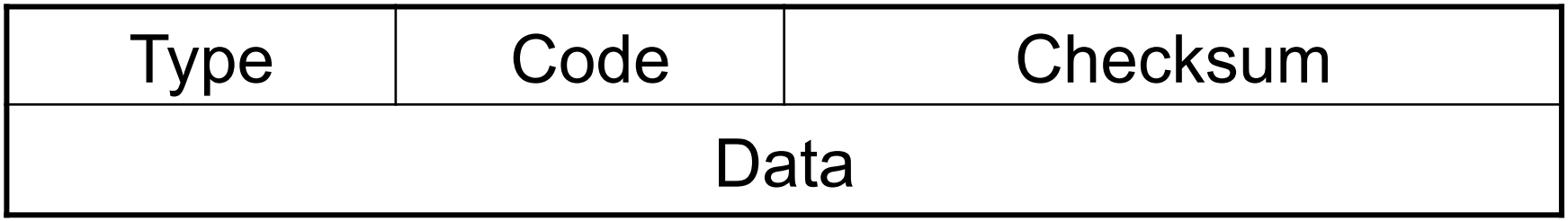
- Lohkomista pyritään välttämään selvittämällä koko polun suurimman sallitun tietosähkeen koko ja lähettäjä tekee alunperin sen kokoisia paketteja
  - Näin toimii esim IPv6, jossa matkan varrella ei lohkota mitään
- Path MTU Discovery: Lähetetään suuri paketti, jossa “do not fragment” –lippu päällä
  - Jos paketti oli liian suuri, vastaanotetaan virheviesti reitittimeltä
  - Kokeillaan pienemmällä paketilla uudestaan (virheviestissä mukana se MTU, johon matka tyssäsi)

- Mitäs nämä virheviestit sitten oikein on?

ICMP (Internet Control Message Protocol)

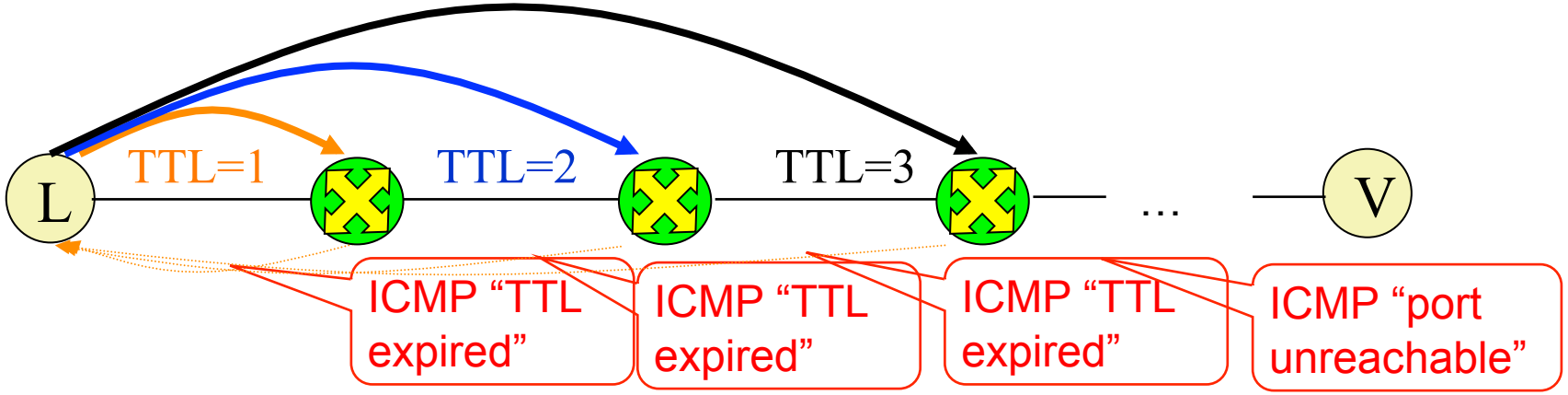
- Kummallekin IP:lle oma: v4 RFC 792 ja v6 RFC 4443
- Virhetilanteista raportointiin (ei niiden korjaamiseen)
  - Lisäksi ping ja traceroute käyttävät ICMPtä
- ICMP-viestit on tarkoitettu verkkokerrokselle
  - Pakataan suoraan IP-paketin sisään
  - Usein ilmoitus välitetään myös sovellukselle
- Käyttö on usein rajoitettu turvallisuussyistä
  - “route redirect” ja “router advertisement” –viestien väärinkäyttö
  - Pingin avulla voi kartoittaa verkon koneet

ICMP-viesti



- Tyyppi määrittelee viestin
  - Esim. 3=tavoittamattomissa (+code); 11=TTL expired, 12=IP-otsikko rikki, 8 = echo request ja 0 = echo reply (pingiä varten)
- Code määrittelee syyn (lisätietoa edelliseen)
  - Esim. 0=verkko, 1=host, 2=protokolla, 3=portti, 6=tuntematon verkko, 7=tuntematon host
- Data sisältää virheviestin aiheuttaneen paketin alun
  - Vakiomittainen viesti: IPv4:ssä mukaan mahtuu 8 oktettia virheen aiheuttaneesta paketista, IPv6:ssa MTU:n verran

ICMP esimerkki: traceroute

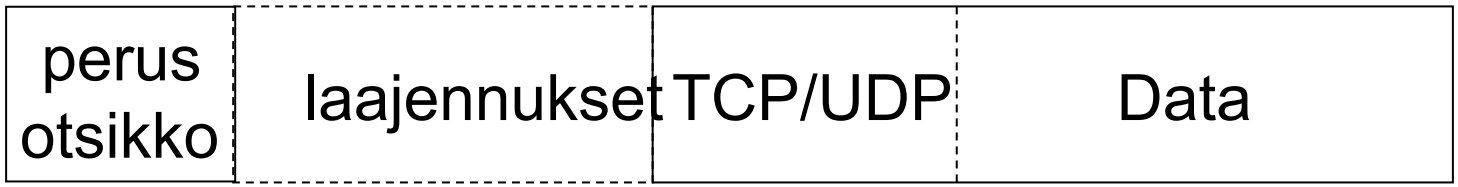


- Mahdollistaa IP-tason polun selvittämisen
- Lähettäjä lähettää UDP-segmenttejä
  - Kohdeosoite on polun päätepiste, portiksi joku epätodennäköisesti auki oleva
  - Aluksi TTL=1, kasvatetaan yhdellä peräkkäisissä segmenteissä
  - Myös ajastin käynnistetään jokaista segmenttiä lähetettäessä
- Kun TTL=0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

Uusi versio IP-protokollasta (IPv6)

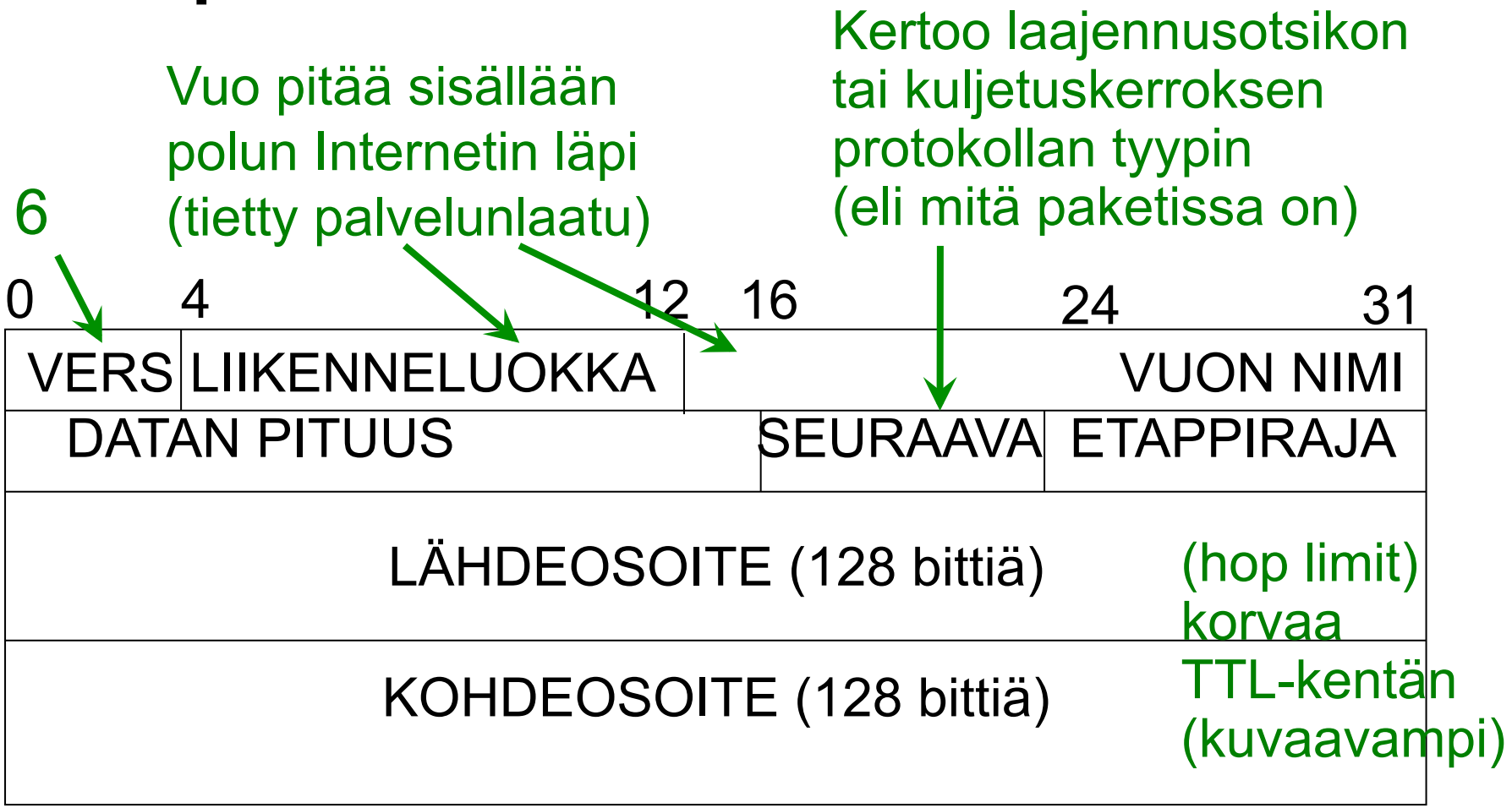
- Aika ajoissa havaittiin IPv4-osoitteavaruuden ongelmat ja osoitteiden loppuminen
- Internet-verkon koko kasvoi ja tarpeet muuttuivat
  - ylikansalliset yritykset, uudet päätelaitteet ja verkkoteknologiat, uudenlaiset sovellukset tosiaikavaatimuksineen
- Erot aiempaan:
  - Pidemmät osoitteet (128) ja laajempi osoitehierarkia, kolme osoitetyyppiä (yksilähetys, monilähetys ja anycast)
  - Joustava otsakeformaatti, jota on helppo laajentaa
  - Tuki automaattiselle asetusten määrittelylle
  - Tuki resurssien varaamiselle (oli jo IPv4:ssä, mut kömpelö)

IPv6-tietosähkeen rakenne



- Perusotsikko on määrämittainen
  - 40 oktettia (eli 40*8 bittiä)
  - Perusotsikko on nopea käsitellä
- Useita laajennusotsikoita

IPv6-perusotsikko



- Mitä puuttuu IPv4ään verrattuna?

Ylemmän kerroksen tarkistussumma

- IPv6-otsikossa ei ole tarkastussummaa!
  - UDP:n pitää käyttää tarkistussummaa IPv6:n kanssa
- Erityisesti TCP- ja UDP-protokollien tarkistussumma
  - 128-bittiset lähettäjän ja (lopullisen) vastaanottajan osoitteet
  - 32-bittinen ylemmän kerroksen tietosähkeen pituus
  - 24 bittiä nollia
  - 8 bittiä seuraava ylemmän kerroksen protokollan tunniste (ei siis esim. IPv6-optio)
- Perusotsikko on vakiomittainen, joten sen pituutta ei tarvita
- Fragmentointi ja optiot tiputettu laajennusotsikoihin
  - Lohkominen tehdään jo lähettäjällä, ei koskaan matkan varrella

Laajennusotsikot

- Laajennusotsikot tarjoavat
  - Lohkomisen
  - Lähdereitityksen (eli minkä verkkojen kautta paketin tulee kulkea)
  - Optiot
  - Tietoturvaa (IPsec): väärentämättömyyden ja lähettäjän (authentication header, AH) ja luottamuksellisuuden (encapsulating security payload, ESP) takaavat otsikot
- Laajennusotsikot tuovat tehoa ja joustavuutta
  - Suositeltu järjestys: matkan varrella muuttuvat optiot, reititys-otsikko, lohkomisotsikko, IPsecin todennus ja salausotsikot, määränpään optiot

Mitä muuta muuttuu? ICMPv6 tarjoaa lisää palveluita

- ARPia ei käytetä naapureiden osoitteiden löytämiseen vaan naapureiden/reititimen etsintä- ja ilmoitusviestit toteutetaan ICMPv6:lla (neighbor discovery protocol)
- DHCP voidaan korvata automaattisella asetusten määrittelyllä ICMPv6:lla
  - Reititin kertoo, käytetäänkö tätä tapaa ja kertoo verkon tiedot (esim. verkkomaskin)
  - Isäntäkone “keksii” koneosan esim. verkkokortin MAC-osoitteen perusteella, ja tarkistetaan sitten tarkistetaan, onko osoite vapaa, lähettämällä kysely kaikillle

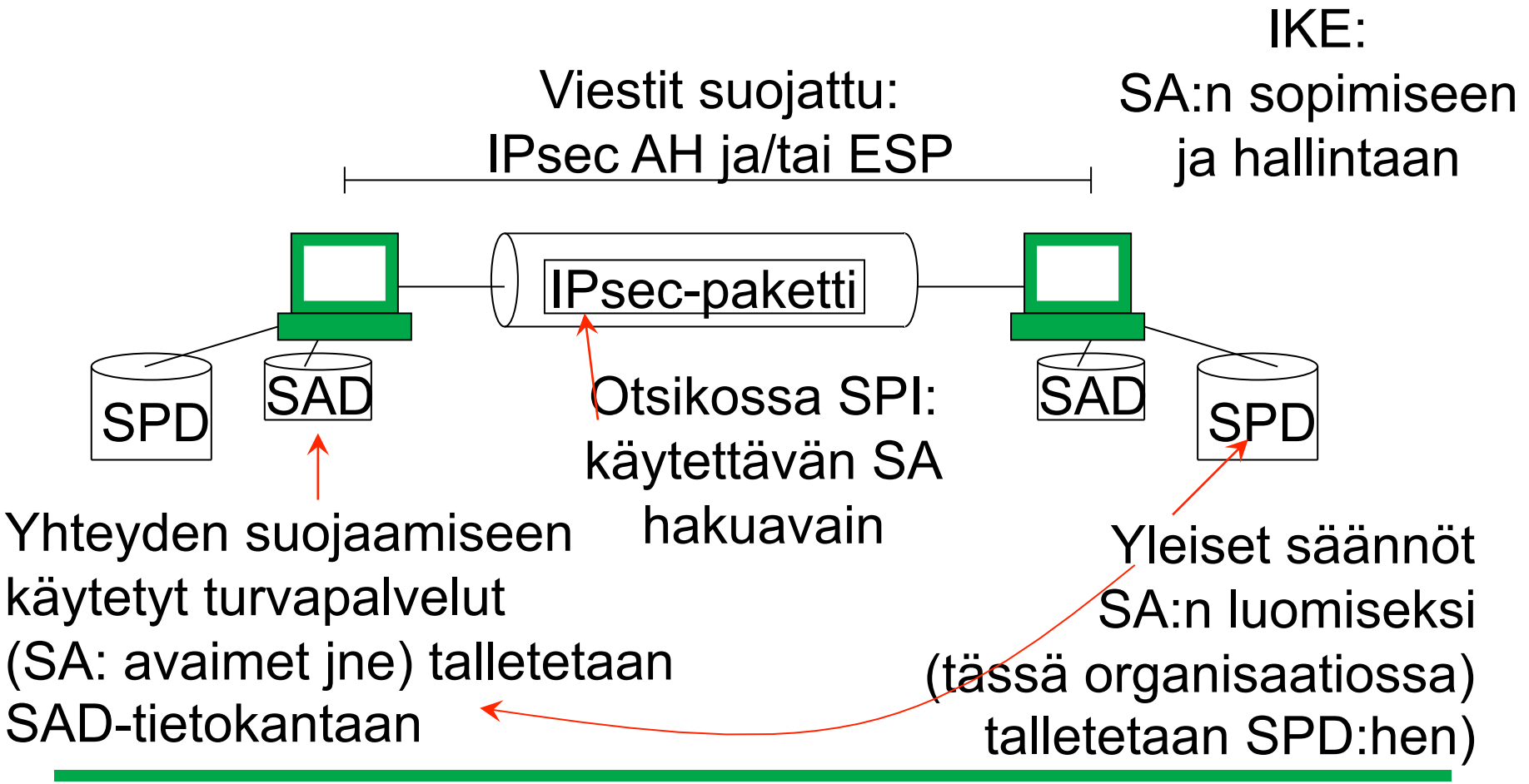
Verkkokerroksen protokollaversion vaihto uuteen versioon

- Tuplapino (dual stack)
  - IPv6-noodeilla myös IPv4-pinosta toteutus,
  - DNS apuna kertomaan, osaako kone kumpaa protokollaa
  - Ongelmia virheviestien ja lohkomisten kanssa
- Tunnelointi
  - IPv6-koneet viestivät IPv4-verkon yli keskenään, välissä IPv6-paketit pakataan IPv4-pakettien sisään
  - Voidaan käyttää NATin tyyliin
- Vaihtaminen on ollut todella hidasta
  - Länsimaissa on riittänyt IPv4-osoitteita
  - Kiinassa käytetään jo IPv6:tta

Verkkokerroksen tietoturva: IPsec

- Käytetään yleensä VPN-tekniikassa (virtual private network)
- Sama protokolla(perhe) toimii sekä IPv6 että IPv4 kanssa
  - IPv4:ssä IP-otsikon jälkeen tulee turvaotsikot
  - IPv6:ssa laajennusotsikoina, toteutus pakollista, käyttö ei
- Kaksi käyttötapaa: tunnelointi ja pakettien suojaus yksittäin
- Tarjoaa monenlaisia tietoturvapalveluita:
  - Luottamuksellisuus (confidentiality)
  - Yhteydetön eheys (connectionless integrity) ja tiedon alkuperän todennus (data origin authentication)
  - Pääsynvalvonta (access control)
  - Suojaus toistoa vastaan (replay protection)
  - Rajoitettu vuon luottamuksellisuus

IPsec kokonaisuutena (framework)

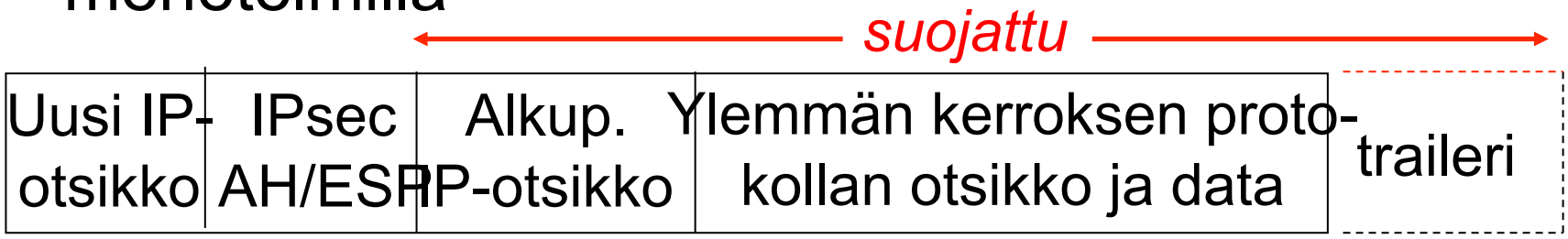


IPsec Framework (2)

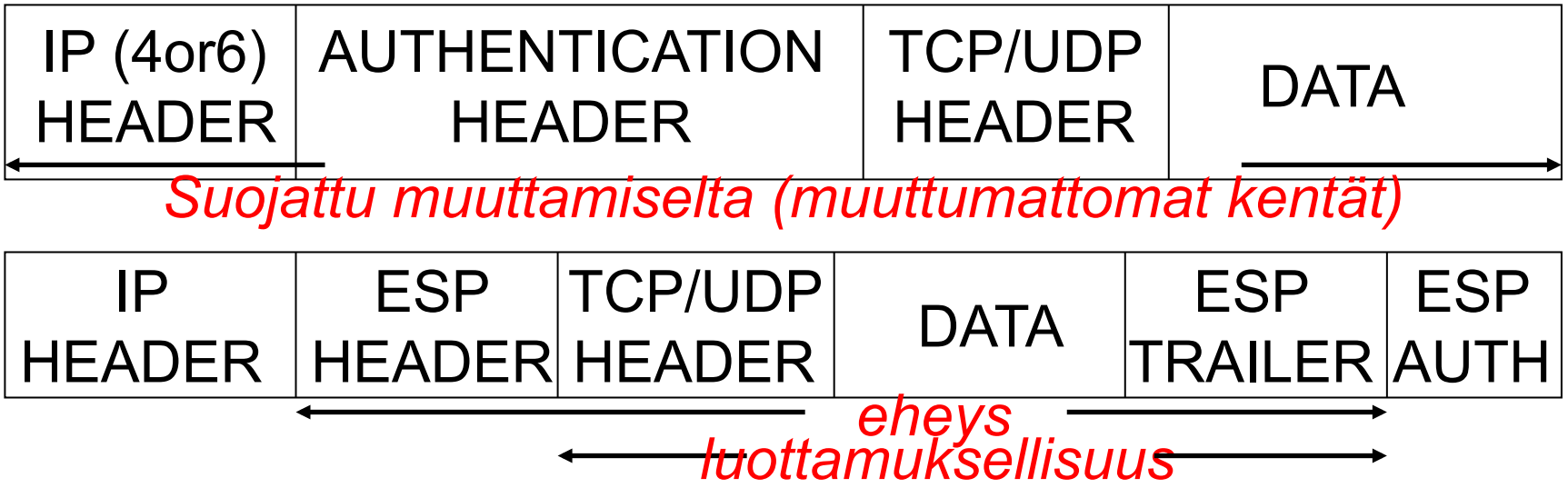
- SA: Turva-assosiaatio (security association)
  - määrittelee yhteydellä käytetyt algoritmit ja avaimet
  - yhteen suuntaan, toiseen suuntaan voi olla erilainen SA
- SPI: tietokanta-avain SA:lle (security parameter index)
  - kertoo käytetyn SA:n
  - vastaanottajan tietokantaan, ei lähettäjän
- SAD:Turva-assosaatiotietokanta (security association database)
  - m.m. mitä algoritmeja olemassaolevilla yhteyksillä on käytössä
- SPD: Turvapolitiikkatietokanta (security policy database)
  - Esim. Mitä algoritmeja saa käyttää ja mihin saa ottaa yhteyden
- IKE: Avaintenhallinta (key management) ja SA:sta sopiminen

IPsec-tunnelointi

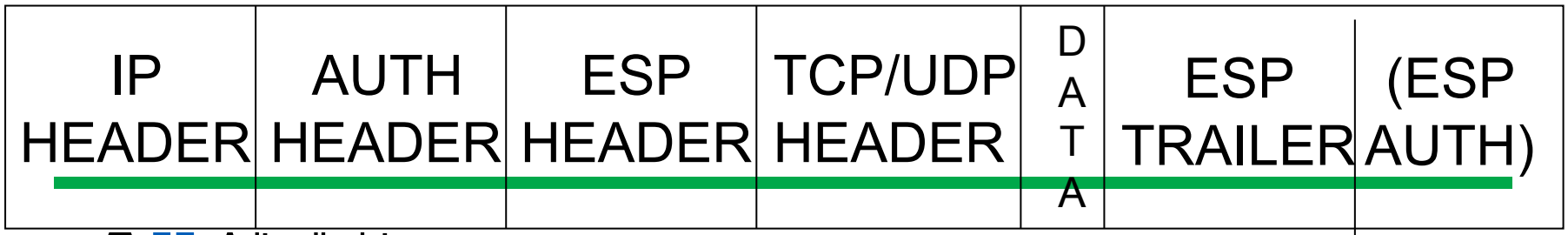
- Tunnelointia käytetään kun toinen tai molemmat yhteyden päätepisteet ovat turvayhdyskäytäviä (esim VPN:n yhteydessä)
- Uusi IP-otsikko lisätään kokonaan suojatun alkuperäisen IP-otsikon (ja IPsec-otsikoiden) eteen
- Koko alkuperäinen paketti on suojattu sovituilla menetelmillä



Pakettikohtainen suojaus (transport mode)



Yhdessä:



Yhteenveto

- Verkkokerroksen IP-protokolla toteuttaa epäluotettavan ja tilattoman kuljetuspalvelun Internetissä
  - Luotettavuus voidaan toteuttaa kuljetuskerroksella (ylempänä)
  - Paketit välitetään perille niissä olevan osoitteen perusteella kukin itsenäisesti
- IPv4 osoitteet ovat lopussa, mutta protokolla yhä käytössä
  - DHCP ja NAT auttavat
  - IPv6 käytössä jo

Olennaisia termejä ja käsitteitä

- Edelleenlähetys (forwarding) ja reititys (routing), edelleenlähetystaulu, reititystaulu, reititin (router), reititysalgoritmi, reitityksprotokolla, kytkin (switch)
- Taattu välitys (guaranteed delivery), viive (delay), viiveen vaihtelu (jitter), kaista (bandwidth), palvelunlaatu (quality of service), paras mahdollinen –palvelu (best-effort service), virtuaalipiiriverkko (virtual circuit network), paketti(kytkentäinen)verkko (datagram network), yhteydellinen (connection-oriented), yhteydetön (connectionless), signalointi (signaling)
- Etuliite (prefix), verkko-osa (network part), osoite (address), tietosähke/paketti (datagram), (verkko)rajapinta (network interface), piste-erotettu esitysmuoto? (dotted-decimal notation)
- Lohkominen (fragmentation), lohko (fragment), suurin mahdollinen linkkikerroksen kehys, suurin mahdollinen lähetysyksikkö (maximum transmission unit),
- Aliverkko (subnet), aliverkkomaski (subnet mask), luokaton osoitteistus (classless addressing), luokallinen osoite (classfull address), väliaikainen osoite (temporary address), lainattu osoite (leased address), laina-aika (lease time), osoiteavaruus (address space), yksityisosoite (private address)
- NATin läpäisy? (NAT traversal)
- Monilähetys (multicast), yksilähetys (unicast), anycast(?), vuo (flow), liikenneluokka (traffic class), etappiraja (hop limit), tuplapino (dual-stack), muunnosalgoritmi, tunnelointi (tunneling),
- Lähteen todennus (origin authentication), tiedon eheys (data integrity), salaus (encryption),

Olennaisia lyhenteitä

- IP Internet protocol
- ICMP internet control message protocol
- TOS type of service
- QoS quality of service
- TTL time to live
- VC virtual circuit
- MTU maximum transmission unit
- CIDR classless interdomain routing
- DHCP dynamic host configuration protocol
- NAT network address translation
- IPsec Internet protocol security

Lähteet

- RFC 791 IPv4
- RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification, 1998
- RFC 4291 - IP Version 6 Addressing Architecture, 2006
  - RFC 2462 IPv6 Stateless Address Autoconfiguration
- IPsec:
  - 4301- Security Architecture for the Internet Protocol, 2005
  - 4302 - IP Authentication Header, 2005
  - 4303 - IP Encapsulating Security Payload (ESP), 2005
  - 4306 - The Internet Key Exchange (IKE), 2005
  - 2411 - IP Security Document Roadmap, 1998

- CIDR: RFC 4632
- DHCP: RFC 2131, RFC 2132
- NAT: RFC 2663, 3022
- RFC 4443- Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, 2006
- RFC 2461 - Neighbor Discovery for IP Version 6 (IPv6), 1998
- RFC 1981 - Path MTU Discovery for IP Version 6, 1996