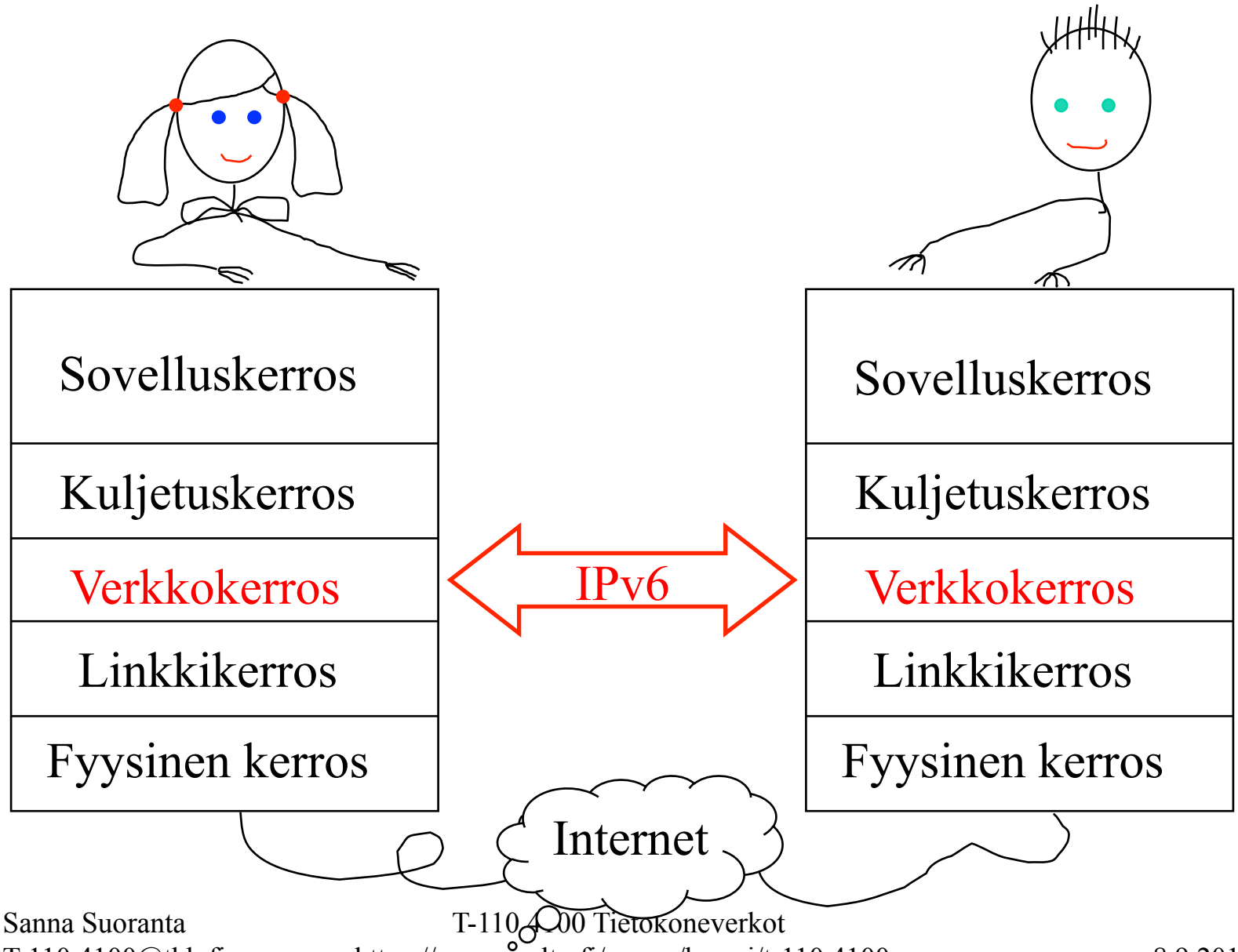
Internet-protokolla versio 6

Comer luku 31, 30

(vanha kirja ss. 257-278+...)


Sovelluskerros
Kuljetuskerros
Verkkokerros
Linkkikerros
Fyysinen kerros
IPv6
Sovelluskerros
Kuljetuskerros
Verkkokerros
Linkkikerros
Fyysinen kerros
Internet

Luennon sisältö

- Internet Protocol (IPv6)
  - Miksi vaihtaa?
  - Osoitteet
  - Otsakkeet
- Internet Control Message Protocol (ICMPv6)
  - osoitteiden määrittäminen
- IPv4/IPv6-yhteistoiminta

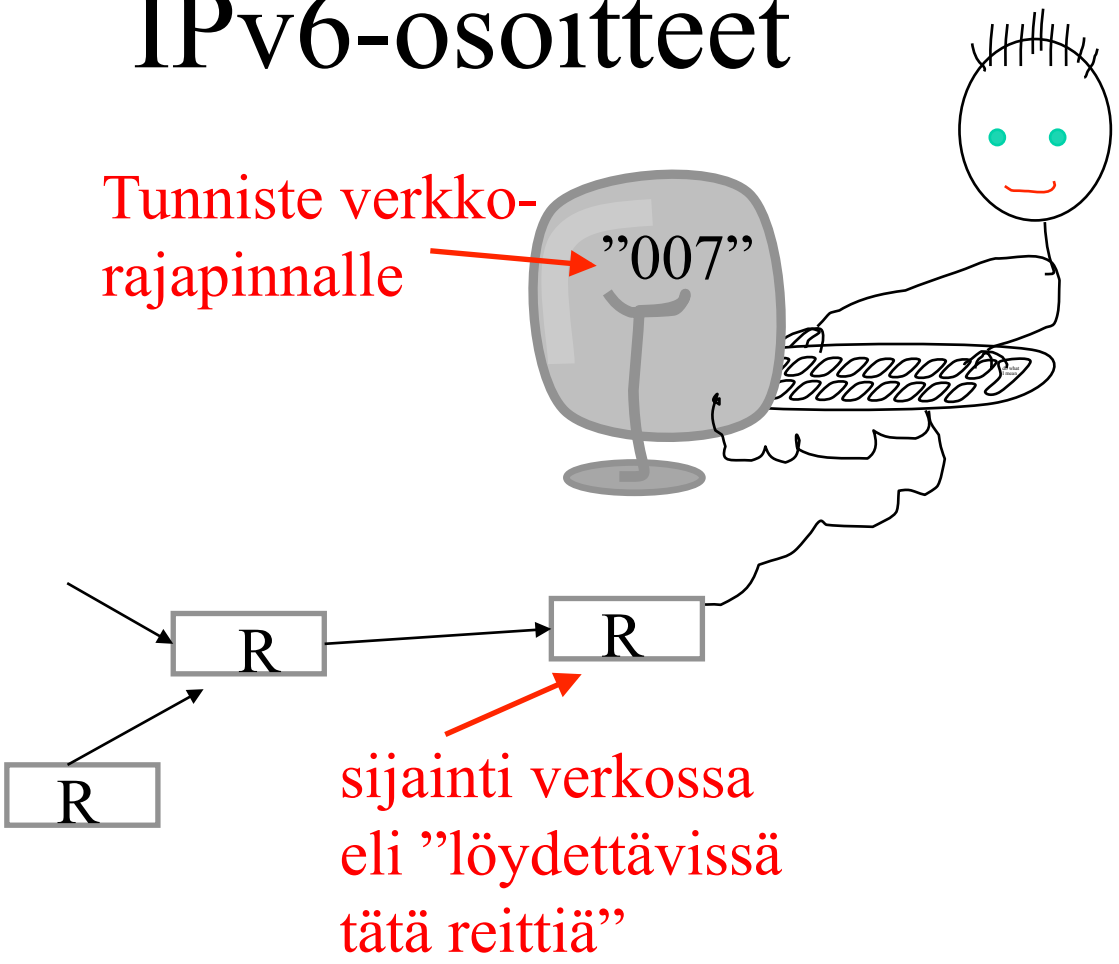
Miksi vaihtaa?

- Internet-verkon koko on kasvanut
- Uudenlaiset sovellukset
  - Esim. Tosiaikainen tiedonsiirto tarpeen
- Uudet päätelaitteet ja verkkoteknologiat
- Kansalliset verkot ja kansainväliset yritykset

IPv6:n ominaisuudet

- Pidemmät osoitteet
- Laajennettu osoitehierarkia
- Joustava otsakeformaatti
- Paremmat optiot
- Protokollan laajentamiseen varautuminen
- Tuki automaattisille asetusmäärityksille ja uudelleennumeroinnille
- Tuki resurssien varaamiselle

IPv6-osoitteet



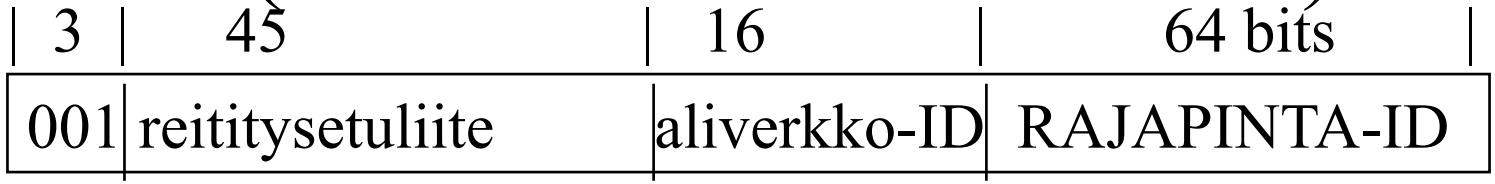
IPv6-osoitteet

- Pituus 128 bittiä
- Käytetään kaksoispistein erotettua heksadesimaalimuotoa (colon hex)
  - 68E6:8C64:FFFF:FFFF:0:1180:95A:FFFF
  - (104.230.140.100.255.255.255.255.0.0.17.128.150.10.255.255)
- Nollat voidaan jättää pois
  - 0:0:0:0:0:0:13:1:68:3 = ::13:1:68:3
  - vain osoitteen yhdestä osasta

Kolme osoitetyyppiä

- Unicast – Yksilähetys
  - Vastaanottaja on yksittäinen verkkorajapinta (esim. isäntäkone tai reititin)
- Anycast - ??
  - Vastaanottaja on joukko verkkorajapintoja
  - Tietosähke vain yhdelle joukon jäsenelle
- Multicast – Monilähetys, ryhmälähetys
  - Vastaanottaja on joukko verkkorajapintoja
  - Tietosähke kaikille joukon jäsenille
  - 1111 1111 monilähetysosoitteet (multicast)

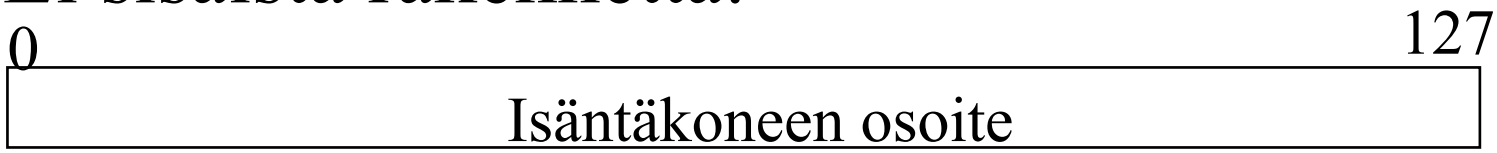
Maailmanlaajuinen yksiosoite (Global Unicast Address) unicast



- Tarkoitus tehdä reitityksestä tehokasta
  - etuliite 001, mutta voi olla jotain aivan muutakin
  - Reititysetuliite (Global routing prefix) = toimipaikka (Vaihtuvankokoinen kenttä)
  - Aliverkon tunniste, vaihtuvanmittainen
  - Rajapinnan tunniste EUI-64-formaatissa (yleensä 64 bittiä)

Yksilähetysosoite isäntäkoneen näkökulmasta

- Ei sisäistä rakennetta:



- Yksinkertainen rakenne (aliverkon peite):

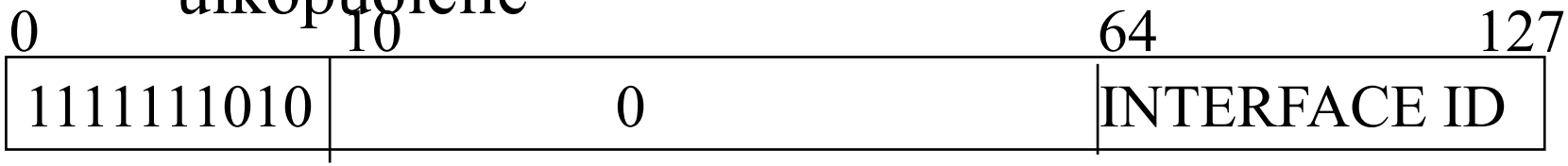
- Rajapinnan tunnisteen pitää olla yksilöivä tietyn linkin alueella (voi olla myös laajemmin)

Yksilähetysositteiden hierarkia

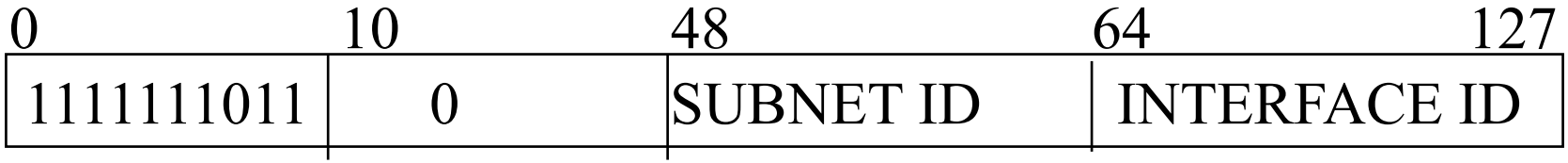
- Yksittäinen verkkorajapinta
  - Yksi yhteys verkon ja tietokoneen välillä
- Toimipaikka (site)
  - Joukko tietyn organisaation tietokoneita
- Maailmanlaajuisesti tunnettu julkinen verkko
  - Julkisesti saavutettavissa oleva “osa” Internetiä
  - Kahdenlaisia: ISP ja “vaihde” (exchange)

Paikalliset osoitteet

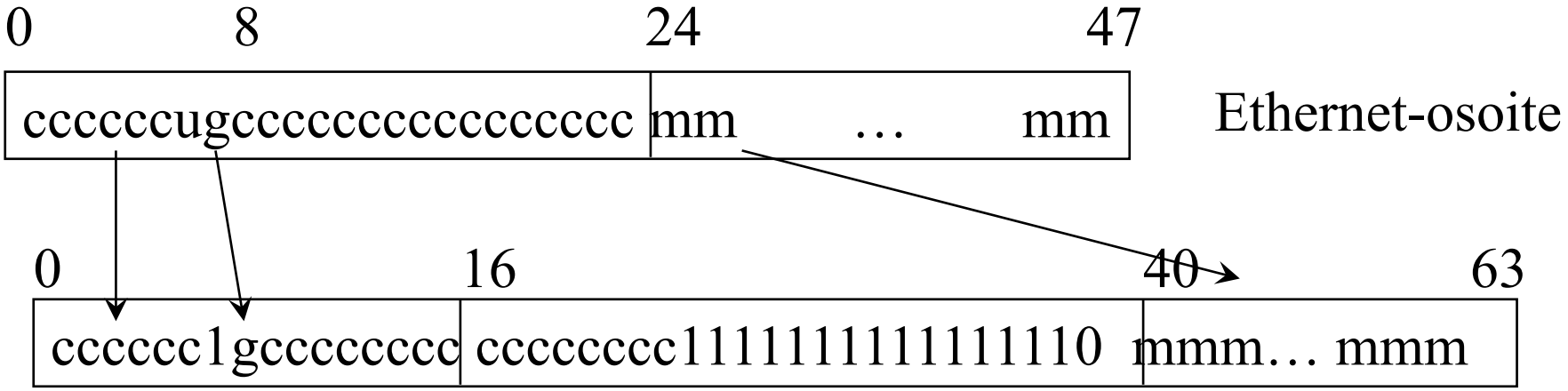
- Paikalliset yksilähetysosoitteet
- Linkkikohtainen osoite
  - Tietosähkettä ei lähetetä ko. fyysisen verkon ulkopuolelle



- Toimipaikkakohtainen osoite
  - Tietosähkettä ei lähetetä toimipaikan ulkopuolelle

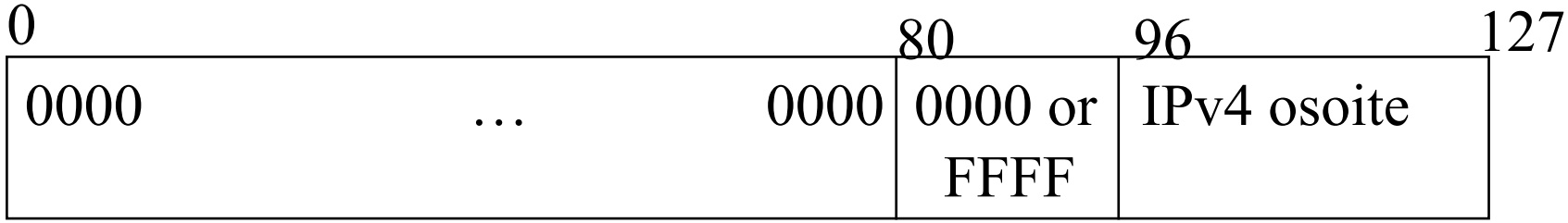


IPv6-osoite Ethernet-osoitteesta



- Rajapinnan tunniste
  - c = verkkokortin valmistajan ID
  - g = yksilö/ryhmä-bitti (monilähetystä varten)
  - u = universaali (= 1) / paikallinen (= 0) bit
  - m = valmistajan valitsema tunniste

Sulautetut IPv4-osoitteet



- Käytetään, kun tunneloidaan IPv6-paketteja IPv4-verkon läpi, tai viestitään IPv4-koneen kanssa (ei vaikuta pseudo-otsikon laskemiseen)
  - 0000 = IPv4-yhteensopiva IPv6-osoite
  - FFFF = IPv4-osoite muunnettu IPv6-osoitteeksi (vain IPv4 osaava noodi)

Erikoisosoitteet

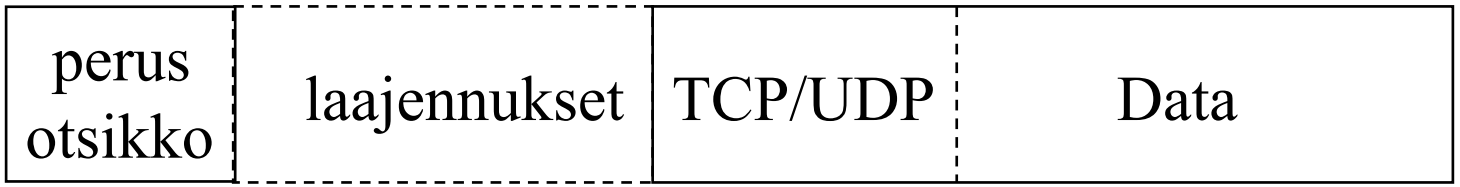
- Määrittämätön osoite
  - 0:0:0:0:0:0:0:0 (= ::)
  - Voidaan käyttää lähettäjän osoitteena, kun oma osoite on tuntematon
- Loopback-osoite
  - 0:0:0:0:0:0:0:1 (= ::1)
  - Testaukseen, ei välitetä verkkoon
  - Paketti palaa takaisin samaan koneeseen

Anycast-osoitteet

- Sama osoite useammalla rajapinnalla
  - Rajapinta tietää osoitteen olevan anycast-osoite
- Käytetään yksiosoitteiden avaruudesta (001 alku)
- (Topologisella) alueella, jossa anycast-osoitetta käytetään, jokaisella oikealla vastaanottajalla on erillinen tietue reititystaulussaan osoitteelle
- Vähän kokemusta
  - Nyt käytössä lähinnä tietyn organisaation reittimien löytämisessä

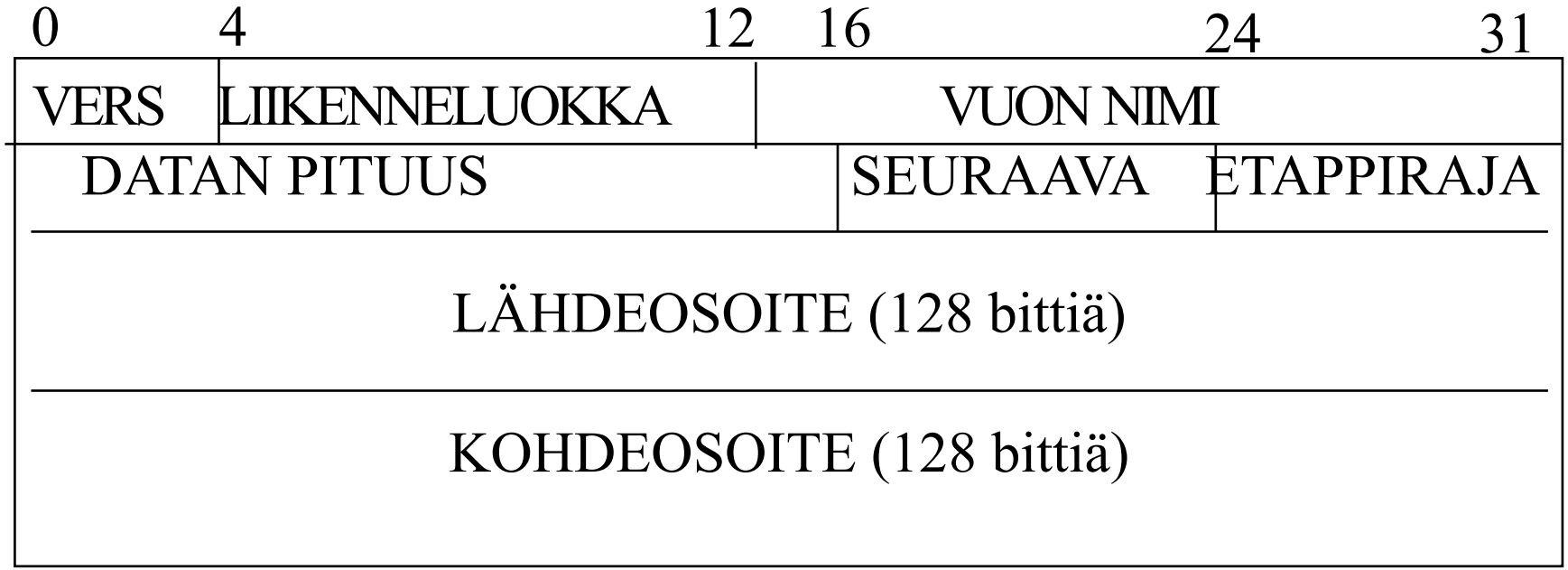
Monilähetysosoitteista reititysluentojen yhteydessä ja multimediatekniikan kurssilla lisää

Tietosähkeen rakenne



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

IPv6-perusotsikko



- Versio = 6
- Etappiraja (Hop Limit)
  - Jokainen reititin vähentää etappirajaa yhdellä
  - Jos etappiraja on 0, paketti hylätään

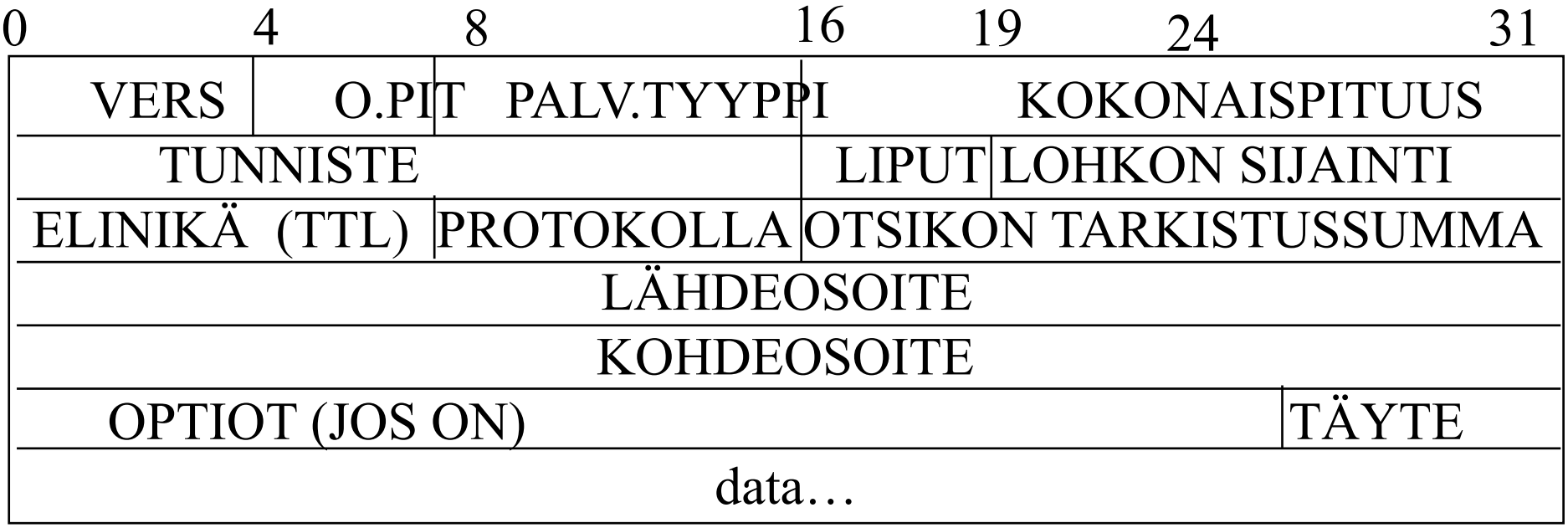
Perusotsikko (2)

- Liikenneluokka
  - Koekäytössä (palvelunlaatu)
  - Kertoo IP-paketin luokan tai prioriteetin
- Vuon nimi – pseudosatunnainen tunniste
  - Koekäytössä (palvelunlaatu)
  - Yhdessä lähettäjän IP-osoitteen kanssa on vuon tunniste
  - 0, jos paketti ei kuulu vuohon
  - Vuot tarvitsevat erikoiskäsittelyä reittimissä

Perusotsikko (3)

- Seuraava otsikko
  - Mikä otsikko tulee IPv6:n perusotsikon jälkeen
  - Voi olla laajennusotsikko tai ylemmän kerroksen otsikko, kuten TCP
  - Käytetään samoja protokollanumeroita kuin IPv4:ssä, määritelty www.iana.org (RFC3232)
- Otsikkoa seuraavan datan pituus oktetteina
  - perusotsikko on vakiomittainen

Kertaus: IPv4-otsikko



- Mikä näyttäisi siis muuttuneen?

Ylemmän kerroksen tarkistussumma

- 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)
- UDP:n pitää käyttää tarkistussummaa IPv6:n kanssa

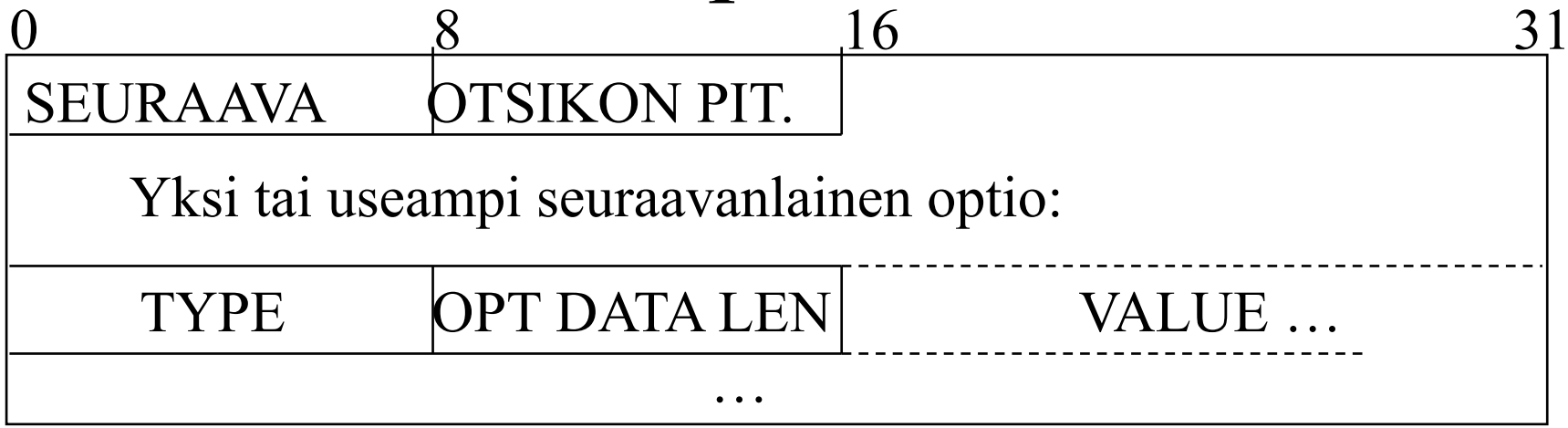
Laajennusotsikot

- Laajennusotsikot tarjoavat
  - Lohkomisen
  - Lähdereitityksen
  - Optiot
  - Väärentämättömyyden ja luottamuksellisuuden
- Laajennusotsikot tuovat tehoa ja joustavuutta
- Edellisen otsikon “seuraava otsikko”-kenttä kertoo seuraavan laajennusotsikon sisällön

Laajennusotsikot (2)

- Suositeltu järjestys
  - Hop-by-Hop-optiot (matkanvarren reittimille)
  - Määränpään optiot (matkanvarren reitittimille)
  - Reititysotsiko
  - Lohkomisotsikko
  - Todennusotsikko (IPsec)
  - Salausotsikko (IPsec)
  - Määränpään optiot (jotka prosessoidaan vastaanottajalla)

Optiot



- Edellisen otsikon “seuraava otsikko”-kenttä kertoo tämän otsikon tyypin
- Voi olla useampia TLV-koodattuja optioita

Optiot (2) - Option tyyppi

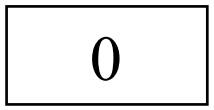
- Tyyppi-kenttä on kahdeksanbittinen
- Option tyypin rakenne on seuraava:
- Ensimmäiset kaksi bittiä kertoo, mitä tehdä tuntemattomalle optiolle
  - 00 = ohita ja jatka otsikon prosessointia
  - 01 = hylkää paketti
  - 10 = hylkää paketti (vastaanottajana monilähetysosoite, lähetä ICMP-viesti tuntemattomasta optiosta)
  - 11=hylkää paketti (ei-monilähetys, lähetä ICMP-viesti)

Optiot (3) - Option tyyppi

- Kolmas bitti
  - 0=ei muutu matkan varrella
  - 1=saattaa muuttua matkan varrella
- Loput biteistä määrittelevät option
- Jos optio voi muuttua matkalla, sitä ei lasketa mukaan todennusotsikkoon

Optiot (4) - Täyte

- Pad1 optio



  – Ei pituus- eikä arvokenttiä
- PadN optio

  – Option data-osa on nollia
- Täytettä tarvitaan tietosähkeen järjestämiseen

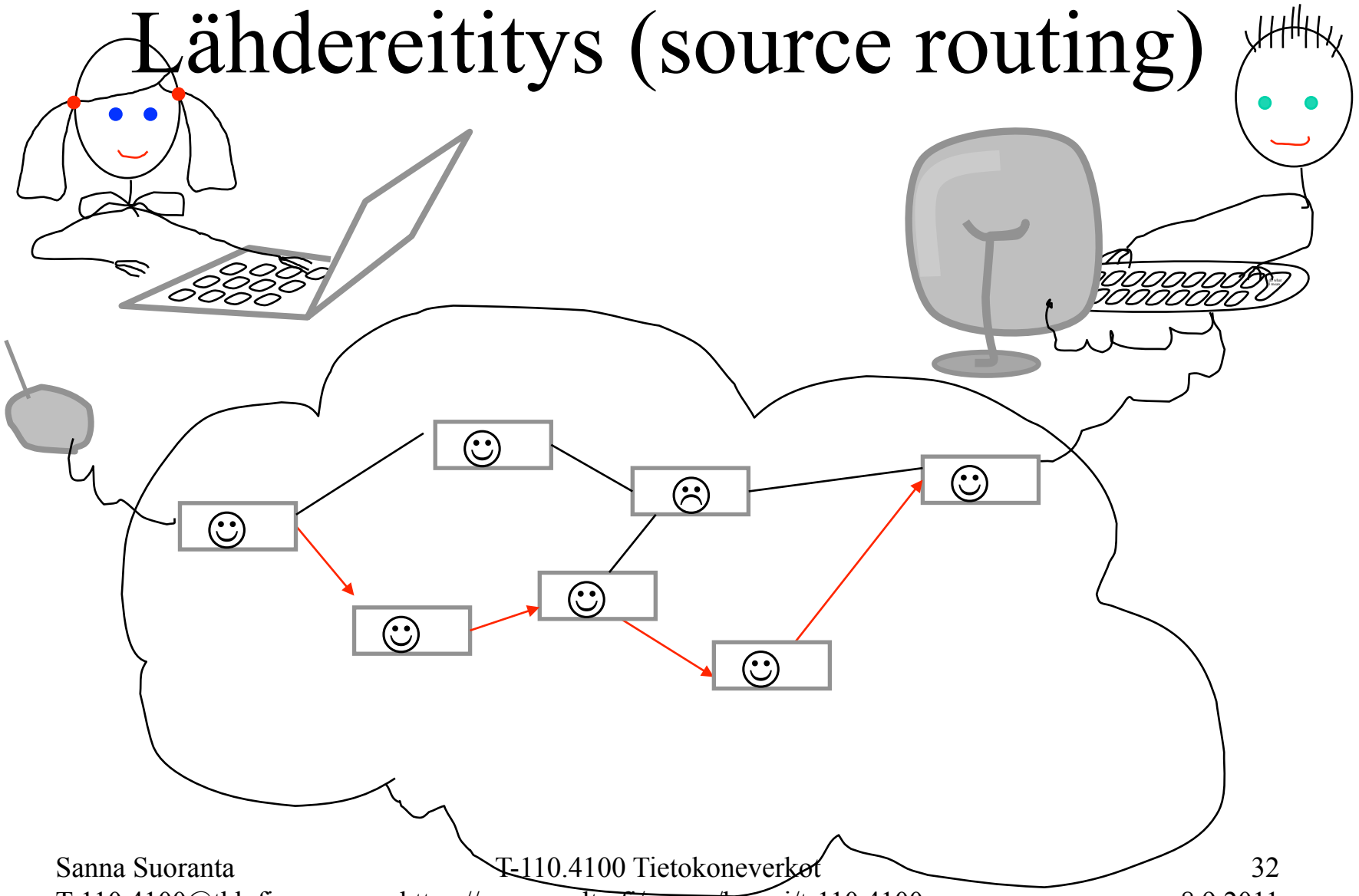
Hop-by-Hop Optio

- Tietoa, joka pitää tarkistaa jokaisessa noodissa, jonka kautta paketti kulkee
- Seuraavan otsikon tyyppi = 0
- IPv6's RFC 2460 määrittelee vain kaksi optiota: Pad1 ja PadN

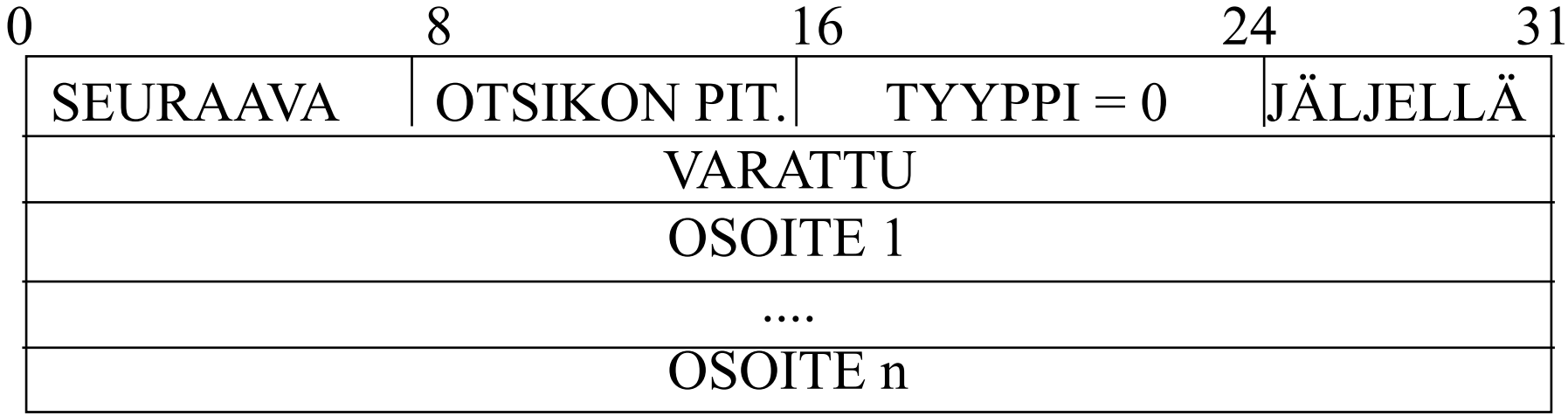
Määränpääoptiot

- Tietoa, jonka vastaanottaja tarkistaa
- Seuraavan otsikon tyyppi = 60
- RFC2460 määrittelee vain Pad1 ja PadN

Lähdereititys (source routing)



Ohjeellinen lähdereititys -otsikko

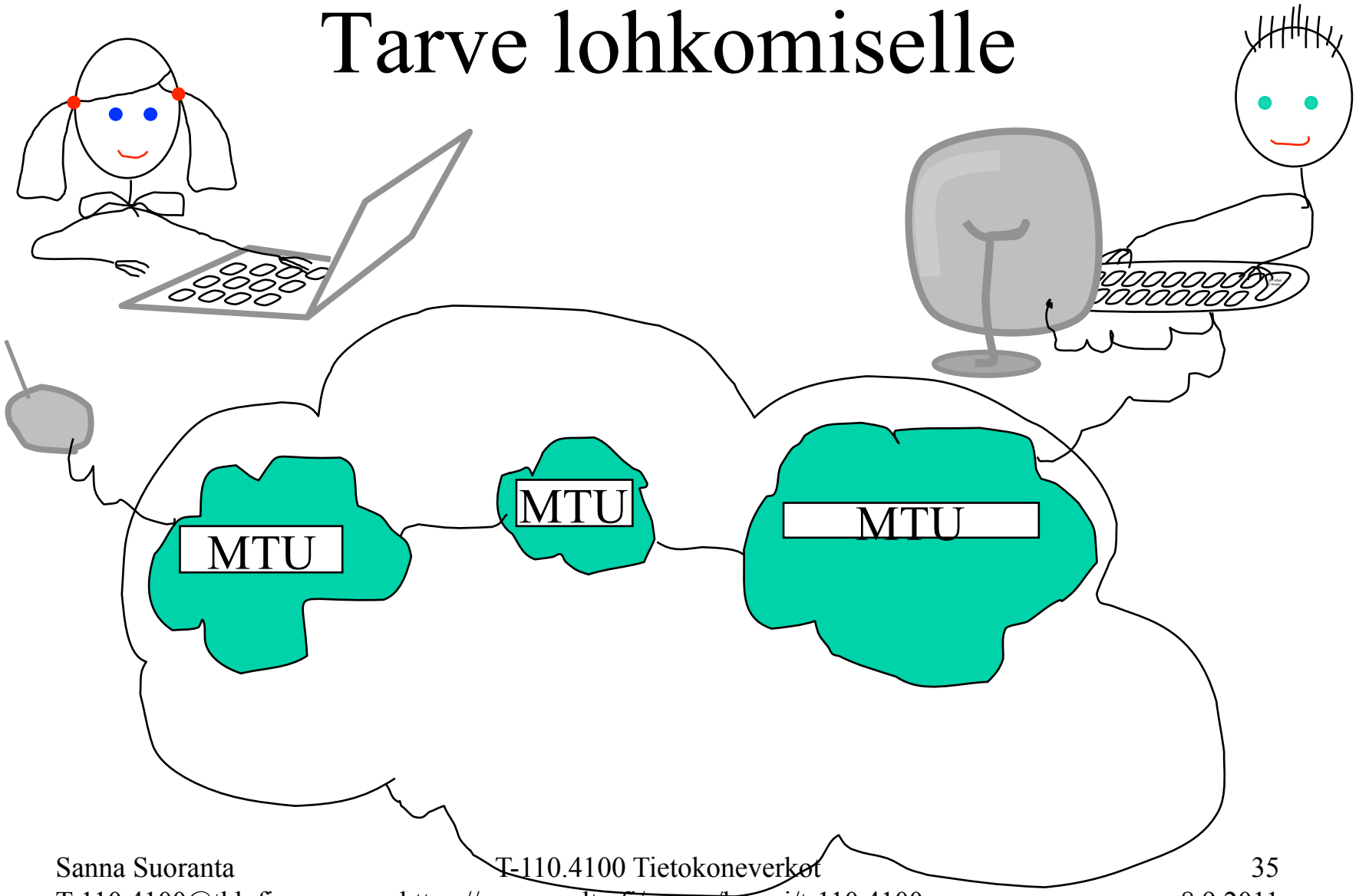


- Seuraava otsikko tälle otsikolle = 43
- Otsikon pituus = 2*osoitteiden määrä (mukaan ei lasketa ensimmäistä kahdeksaa oktettia)
- Monilähetysosoitteita ei voi olla noodilistassa

Reititysotsikko (2)

- Tyyppi kertoo reititysotsikon tyypin (määritelty vain 0=ohjeellinen lähdereititys)
- Jäljellä-kenttä kertoo kuinka monta osoitetta otsikossa on jäljellä, eli minkä noodien kautta viestin pitää vielä kulkea
  - Jos tyyppiä ei tunnisteta ja jäljellä=0, jatka seuraavasta otsikosta
  - Muuten lähetä ICMP-viesti parametriongelmasta

Tarve lohkomiselle



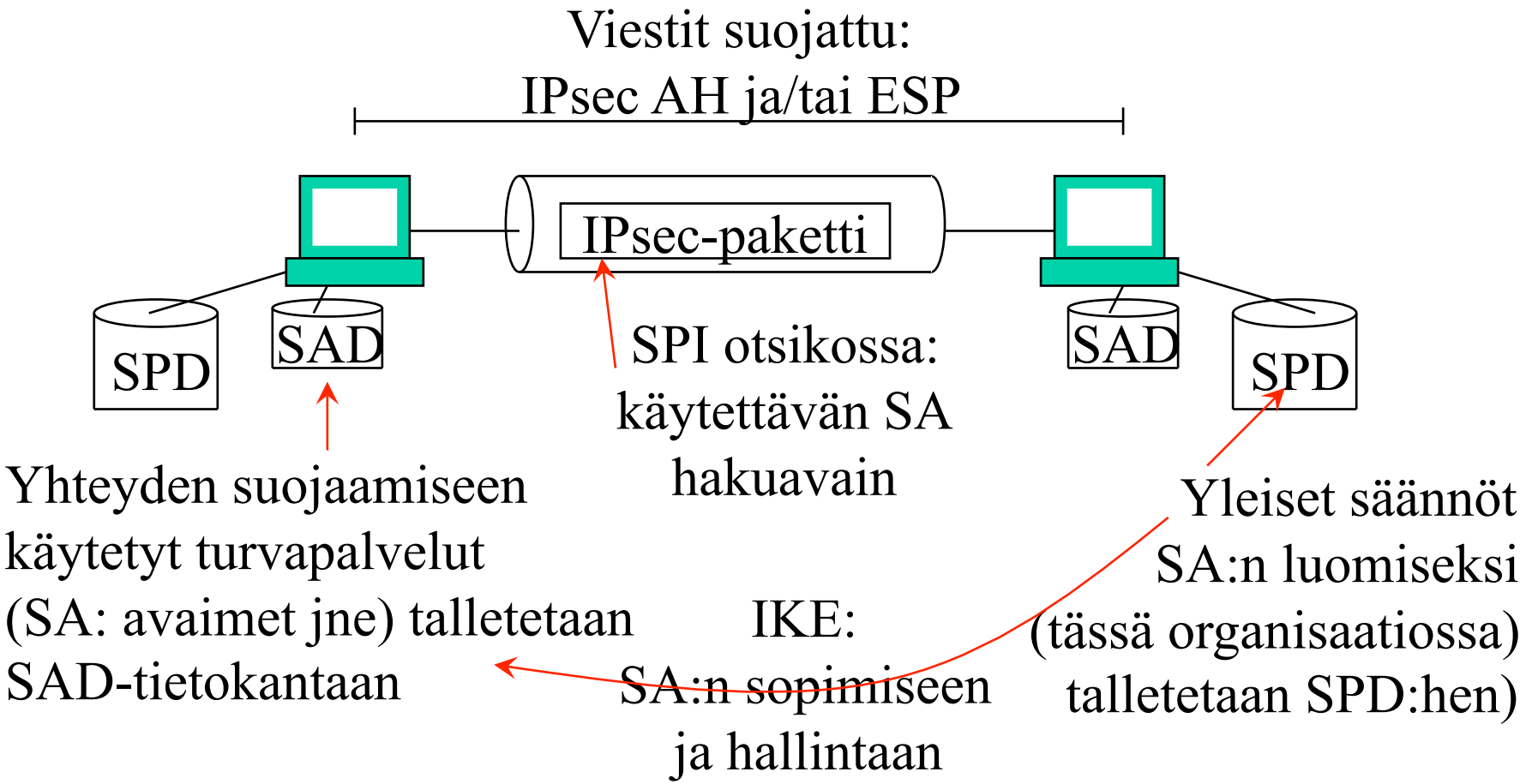
Lohkomisotsikko

- Päästäpäähänlohkominen nopeuttaa reititystä
  - Taattu pienin MTU (1280 oktettia)
  - ICMP tarjoaa polun MTU löytämismenetelmän (path MTU discovery)
- Kun lohkomista tarvitaan, lohkomislisäotsikko on perusotsikon lisäksi paketissa
  - Next header = 44

Lohkomisotsikko (2)

- Lohkon sijainti (fragment offset)
  - Kahdeksan oktetin pätkissä
  - Tiedon paikka “alkuperäisessä” paketissa
- (RS on käyttämätön eli 0)
- M-bitti
  - 1 = lisää lohkoja
  - 0 = viimeinen lohko
- Tunniste
  - Sama kaikissa “alkuperäisen” paketin osissa

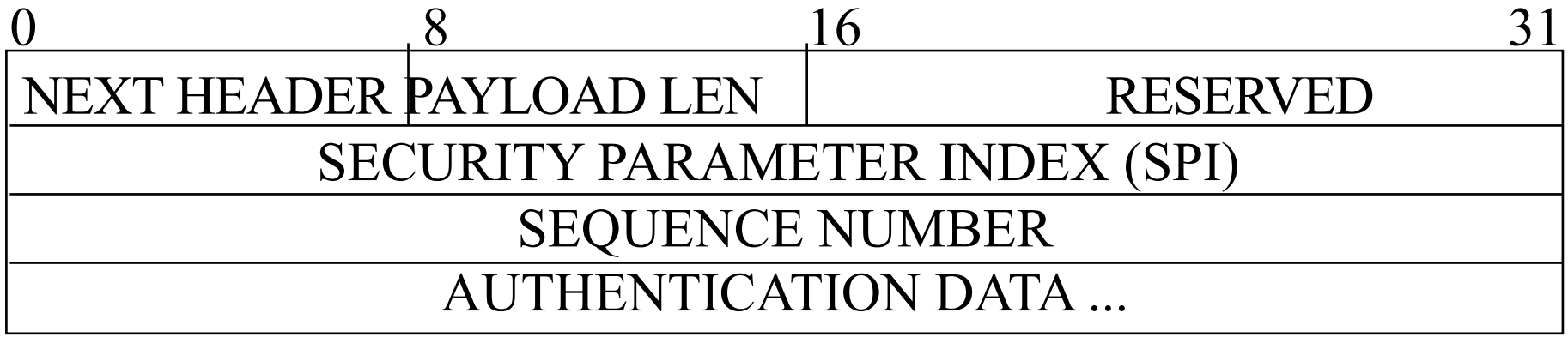
IPsec kokonaisuutena (framework)



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
- SPD: Turvapolitiikkatietokanta (security policy database)
- SAD:Turva-assosaatiotietokanta (security association database)
- IKE: Avaintenhallinta (key management) ja SA:sta sopiminen

Todennusotsikko (IPsec AH)

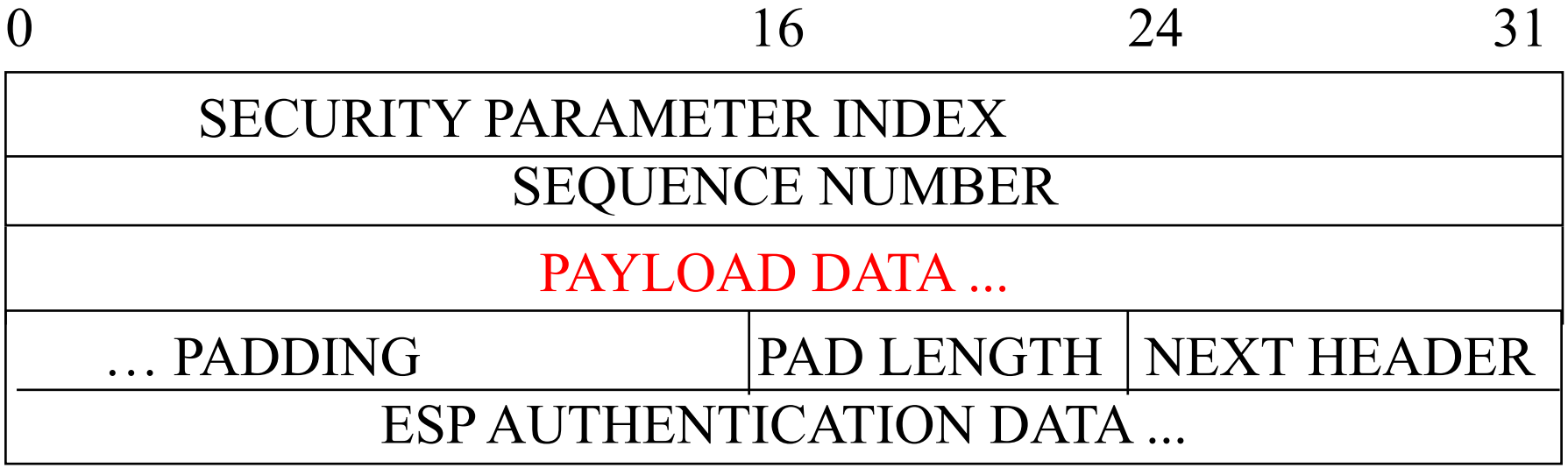


- IPsec Authentication Header (AH)
- Yhteydetön eheys ja tiedonlähteen todennus
- Todentaa IP-otsikon muuttumattomat kentät (myös perusotsikon) ja tietosähkeen sisällön

Todennusotsikko (2)

- Security parameter index (SPI) = käytettävän turva-assosiaation tunniste vastaanottajalla
- Sekvenssinumero = paketin järjestysnumero alkaen satunnaisesta
- Todennusdata = tiiviste laskettu SA:n määrittämällä tiivistealgoritmilla (kentän pituus riippuu algoritmista)

Salausotsikko (IPsec ESP)



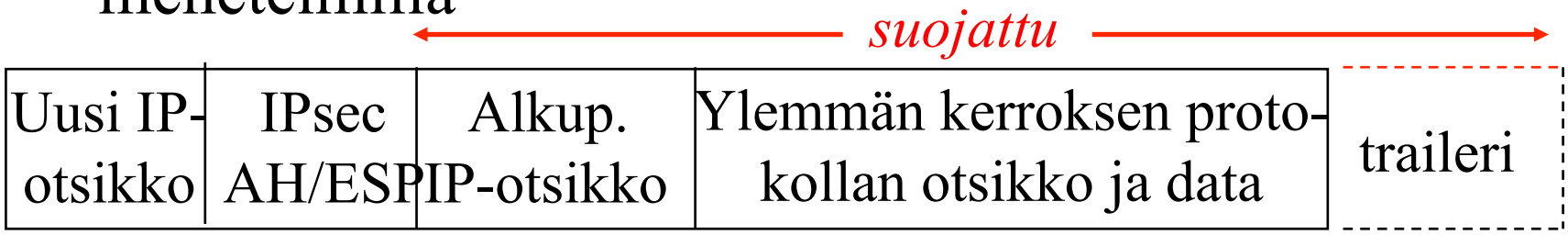
- IPsec Encapsulating Security Payload (ESP)
- Yhteydetön eheys, tiedonlähteen todennus, ja/tai luottamuksellisuus (=salaus)
- Sisältää sekä otsikon että ”trailerin”

Salausotsikko (2)

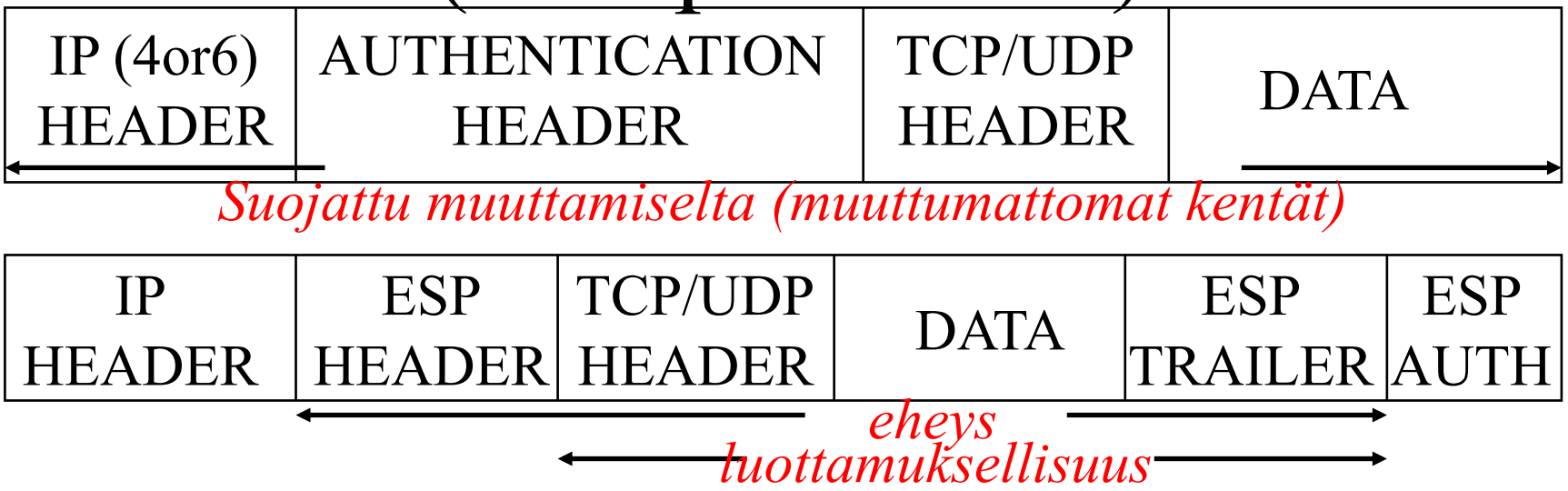
- SPI ja sekvenssinumero kuten AH:ssa
- Täytettä tarvittaessa: 0, 1, 2, 3, 4,… jne - ei siis nollia kuten yleensä! + täytteen pituus
- Seuraavan otsikon (paketin sisällä) tyyppi
- Todennusdata samoin kuin AH:ssa, eli SA määrittää käytetyn algoritmin ja sen tuottaman tiivisteen pituuden

IPsec-tunnelointi

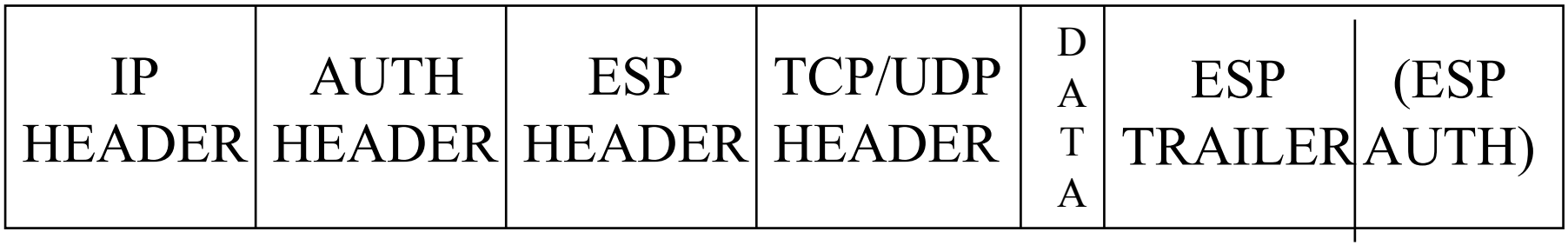
- Tunnelointia käytetään kun toinen tai molemmat yhteyden päätepisteet ovat turvayhdyskäytäviä
- Uusi IP-otsikko lisätään kokonaan suojatun alkuperäisen IP-otsikon (ja IPsec-otsikoiden) eteen
- Koko alkuperäinen paketti on suojattu sovituilla menetelmillä



Pakettikohtainen suojaus (transport mode)



Yhdessä:



IPsec tarjoaa

- Sama protokolla toimii sekä IPv6 että IPv4 kanssa
- Pääsynvalvonta (access control)
- Yhteydetön eheys (connectionless integrity)
- Tiedon alkuperän todennus (data origin authentication)
- Suojaus toistoa vastaan
- Luottamuksellisuus (confidentiality)
- Rajoitettu vuon luottamuksellisuus
  - Mitä nämä oikeasti tarkoittavat IPsecin kohalla?

Ei seuraavaa otsikkoa

- Arvo 59 seuraavan otsikon kertovassa kentässä
- Tämän otsikon jälkeen ei ole enää otsikkoa
  - huom: ylemmän tason otsikolle on myös omat numerot, joita käytetään niitä merkitsemään
- Jos pituuden mukaan paketissa olisi vielä jotain, se jätetään huomioimatta
  - Jos paketti lähetetään vielä eteenpäin, sille ei silti tehdä mitään, eli ylimääräiset bitit jätetään

Yhteenveto IPv6:sta

- IPv6 tarjoaa yhteydettömän, best-effort -paketinvälityspalvelun
- Tietosähke sisältää perusotsikon, laajennusotsikot ja (ylemmän kerroksen) datan
- Yksi- ja monilähetys- ja, anycast-osoitteet
- Edellyttää muutoksia myös muihin protokolliin
  - ICMP ja DNS, sekä UDP (tarkastussumma)
- Yhteensopivuus IPv4:n kanssa
  - lisää tästä kohta

Lähteet

- RFC 4291 - IP Version 6 Addressing Architecture, 2006
  - RFC 2462 IPv6 Stateless Address Autoconfiguration
- RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification, 1998
- 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

Lisää tietoa

- RFC 3587 Aggregatable Global Unicast Address Format
- RFC3177 IAB/IESG Recommendations on IPv6 Address Allocations to Sites
- RFC 1546 Host Anycasting Service
- RFC 2375 IPv6 Multicast Address Assignments
- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks

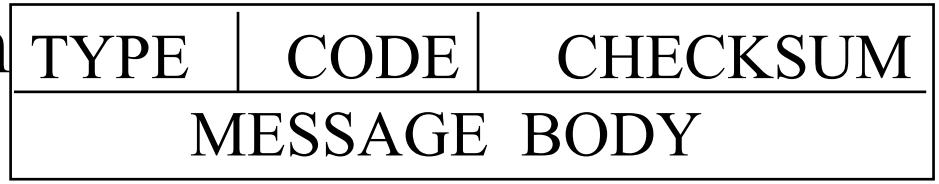
Siinä kaikki IPv6:sta.
Seuraavaksi ICMPv6
ja lopuksi IPv4-IPv6.

Internet Control Message Protocol version 6 (ICMPv6)

-ICMPv6-viestit
-Naapureiden löytäminen
-Osoitteen automaattinen määrittely
-Polun MTU:n selvittäminen

ICMP for IPv6 (RFC 4443)

- Kuten IPv4, IPv6:lla on oma pakollinen ICMP
  - Virheviestit
  - Tiedotteet
- Paketin rakenne on samanlainen kuin vanhan ICMP:n

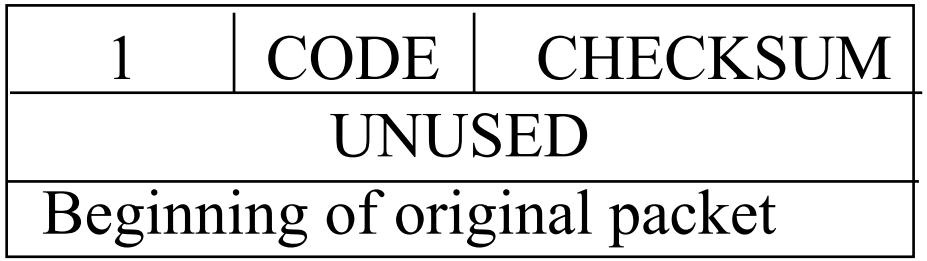


- Enemmän käyttötarkoituksia kuin IPv4:ssä

ICMPv6

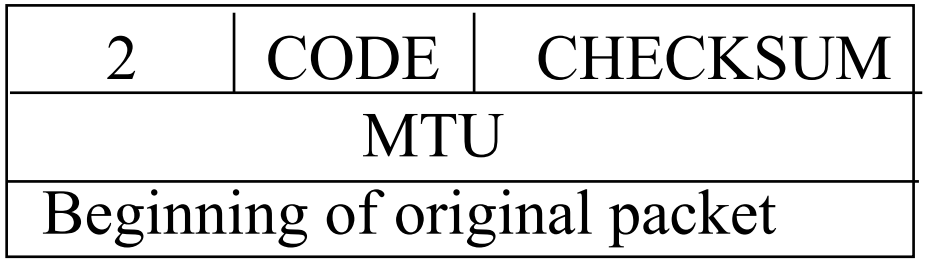
- Jokaisen noodin pitää toteuttaa viestit, ja lisäksi tarjota ylemmälle kerrokselle rajapinta viestien lähettämiseen ja vastaanottamiseen
- Tarkastussummaan lasketaan ICMPv6-viestin lisäksi myös lähde- ja kohdeosoitteet
- Tyypit 0-127 ovat virheviestejä ja 128-255 tiedotteita varten
- Uusi protokollanumero on 58

Kohde tavoittamattomissa



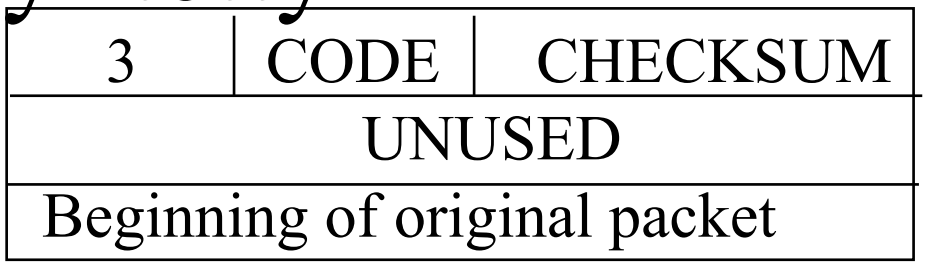
- virhekoodit:
  - 0=ei reittiä kohteeseen
  - 1=hallinnollisesti estetty
  - 3=osoite tavoittamattomissa
  - 4=portti tavoittamattomissa
- Alkuperäisestä paketista niin paljon dataa kuin mahdollista siten, että ICMP-viesti mahtuu minimimittaiseen pakettiin (MTU=1280 octets)

Paketti liian suuri



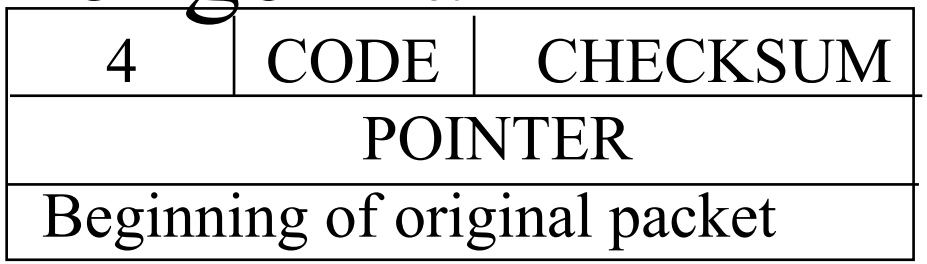
- Koodi käyttämätön
- MTU = seuraavan linkin MTU
- Alkuperäistä pakettia ei voida edelleenlähettää
- Osa polun MTU:n selvittämisprosessia
- Ongelma ratkaistaan ylemmällä kerroksella
- Lähetetään myös monilähetyksen ongelmista

Aika ylitetty



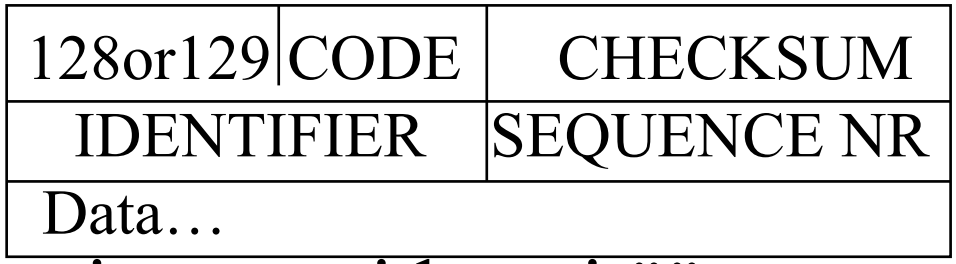
- Koodi
  - 0 = etappiraja saavutettu
  - 1= lohkojen kokoamisen aikaraja saavutettu
- Ylemmän kerroksen ratkaistava ongelma

Parametriongelma



- Koodi
  - 0 = virheellinen otsikon kenttä
  - 1 = tuntematon seuraavan otsikon arvo
  - 2 = tuntematon IPv6-optio
- Osoitin (Pointer) kertoo ongelmakohdan sijainnin

Echo-pyyntö ja -vastausviestit



- koodi = 0
- Tunnisteen ja sekvenssinumeroiden pitää täsmätä pyynnön ja vastauksen toisiinsa
- Data: nolla tai useampi oktetti satunnaista dataa

- Perus-ICMPv6-viestit käyty läpi

- ICMPv6-tyylisiä viestejä käytetään myös
  - Naapureiden löytämiseen
  - Osoitteiden automaattiseen määrittämiseen
  - Polun MTU:n selvittäminen

Naapurinlöytämisprotokolla Neighbor Discovery (ND) Protocol

- IPv6 ei käytä ARP:ia eikä yleislähetystä
- Naapurinlöytämisprotokollaa käytetään linkkikerroksen osoitteiden ja reitittimien etsimiseen
- ICMP:n laajennus eli sama viestiformaatti

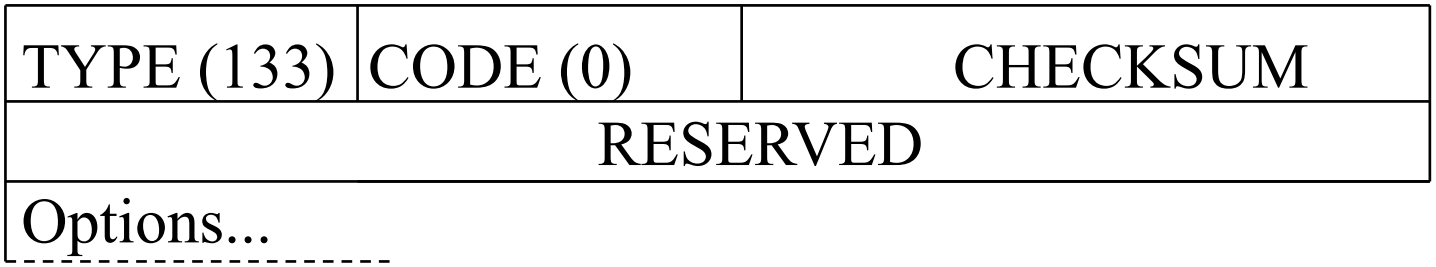
Naapurinlöytämisviestit

- Reitittimen etsintä- (solicitation) ja ilmoitusviestit (advertisement)
  - Lähetetään säännöllisesti tai kun kone on juuri käynnistetty
- Naapurin etsintä- (solicitation) ja ilmoitusviestit (advertisement)
  - Linkkikerroksen osoitteiden etsiminen ja tavoitettavuus
- Uudelleenohjaus
  - Parempi ensimmäinen hyppy kohteeseen

Reitittimen löytäminen

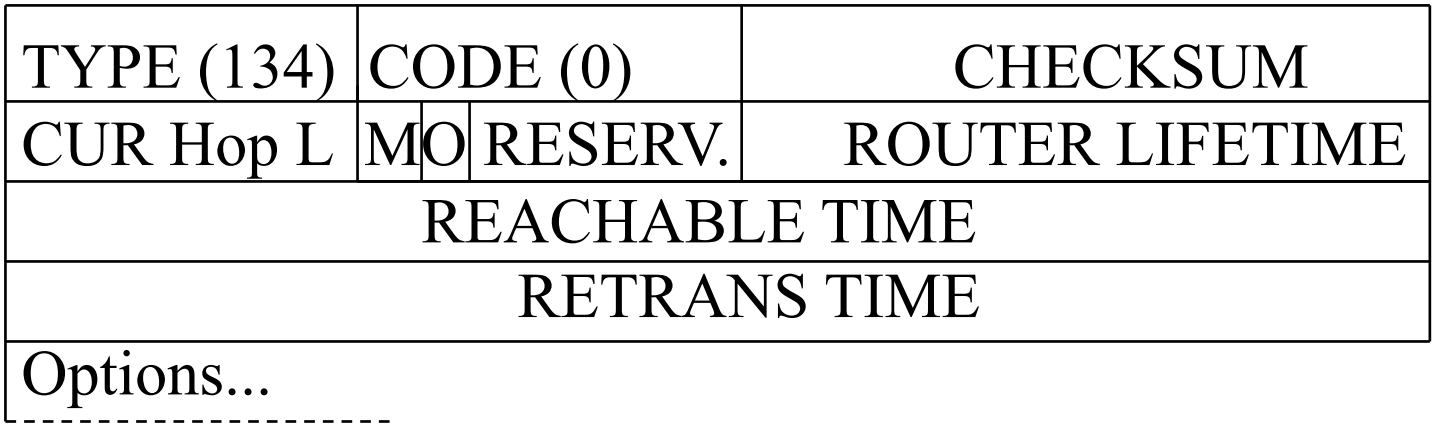
- Isäntäkone tarvitsee tietoa
  - Verkosta, esim. IP-osoitteen verkko-osan
  - Oletusreitittimen osoitteen
  - jne
- Kaksi viestiä
  - Reitittimen etsintäviesti (Router Solicitation)
  - Reitittimen ilmoitusviesti (Router Advertisement)

Reitittimen etsintäviesti



- Pyyntö lähettää reitittimen ilmoitusviesti
- Lähetetään, kun verkkorajapinta otetaan käyttöön
- Optio-kentässä on lähteen linkkitason osoite, jos se on tunnettu

Reitittimen ilmoitusviesti



- Reitittimet lähettävät tämän viestin säännöllisesti tai vastauksena reitittimen etsintäviestiin
- Current Hop Limit: oletusarvo lähetettäville IP -paketeille (0 = määrittelemätön tässä reitittimessä)

Reitittimen ilmoitusviesti (2)

- M=1=Hallinnoitu osoitteidenmääritys
  - Käytetään tilallista protokollaa osoitteen määrittämiseen (esim DHCP)
- O=1=Toinen tilallinen määrittely
  - Käytetään tilallista protokollaa muun tiedon (kuin osoitteen) selvittämiseen
- (RES=varattu tulevaan käyttöön eli 0)

Reitittimen ilmoitusviesti (3)

- Reitittimen elinikä (Router Lifetime)
  - 0 = tämä ei ole oletusreititin
  - muu = tämän reitittimen elinaika oletusreitittimenä (max 18.2 tuntia)
- Aika (Reachable Time, millisekunteina), jonka naapurin oletetaan olevan tavoitettavissa
  - Naapurin tavoittamattomissaolon havaitsemisen (Neighbor Unreachability Detection) algoritmi
- Ilmoitusviestien uudelleenlähetysväli (Retrans Timer) millisekunteina

Reitittimen ilmoitusviesti (4): optiot

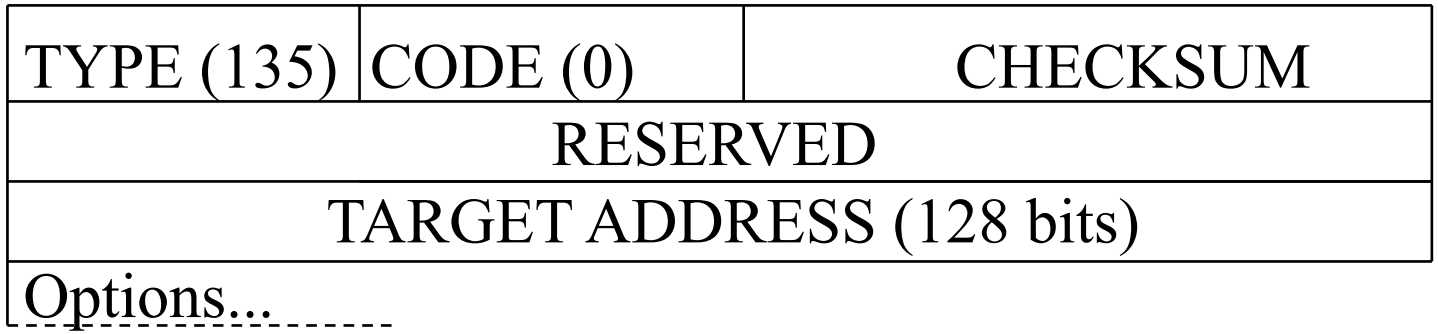
- Lähteen linkkitason osoite
- MTU (jos saatavissa)
- Tieto verkon etuliitteestä
  - Käytetään osoitteen automaattisessa määrityksessä

- Reitittimien ilmoitusviestit lähetetään monilähetyksenä “kaikki verkon koneet” -osoitteeseen

Naapurit

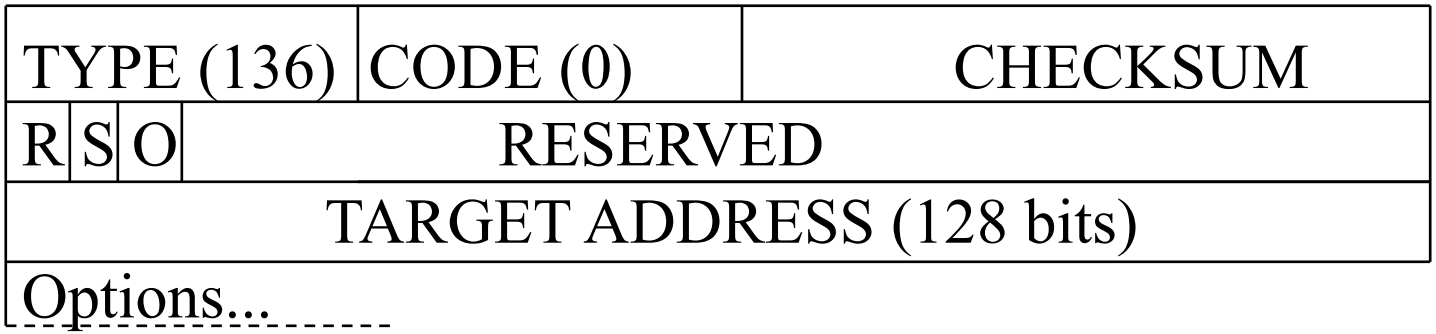
- ARP-protokollaa ei käytetä linkkikerroksen osoitteiden ja IPv6-osoitteiden yhteyden selvittämiseen
- Naapurinetsintäviestillä (Neighbor Solicitation) kysytään noodin linkkikerroksen osoitetta
- Vastaus on naapuri-ilmoitusviesti (Neighbor Advertisement message)

Naapurinetsintäviesti



- Kysytään kohteen linkkikerroksen osoitetta
  - Jos vastaanottaja tuntematon, käytetään monilähetystä
  - Jos tarkistetaan saavutettavuutta, käytetään yksilähetystä
- Optiossa linkkikerroksen osoite, jos se tunnetaan

Naapuri-ilmoitusviesti

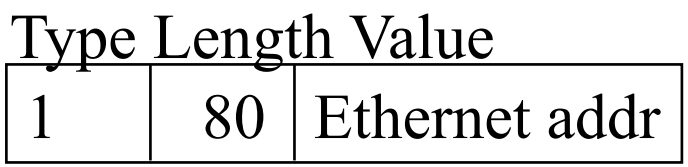


- Liput: R=1= reititin, S=1= vastaus ja O=1=ylikirjoita vanha tieto
- Kohteen linkkikerroksen osoite on optio -kentässä

Optiokenttä ND-viesteissä

esimerkiksi:

- TLV-tyyppiset optiot
- Tyypit:
  - 1 = lähteen linkkikerroksen osoite
  - 2 = kohteen linkkikerroksen osoite
  - 3 = verkon etuliitetietoa (automaattiseen osoitteenmääritykseen)
  - 4 = uudelleenlähetetty
  - 5 = MTU



Uudelleenohjausviesti (Redirect)

TYPE (137)	CODE (0)	CHECKSUM
RESERVED		
TARGET ADDRESS (128 bits)		
DESTINATION ADDRESS (128 bits)		
Options...		

- Kertoo paremman reitin (seuraavan hypyn osoite on kohdeosoite-kentässä) tai että kohde on naapuri (osoitteet samat)
- Optiot: linkkikerroksen osoite, alkuperäinen viesti

Isäntäkoneeseen talletettavat tiedot

- Isäntäkoneissa pidetään tietoa naapureista
  - IPv6- ja linkkikerroksen osoitteet
  - Tieto, onko naapuri reititin
  - Tietoa naapureiden tilasta
- Tietoa päivitetään ja ylläpidetään seuraavalla algoritmilla

Naapurin tavoittamattomuuden havaitsemisalgoritmi

- (Neighbor Unreachability Detection Algorithm)
- Syy tavoittamattomuuteen voi olla polussakin
- Käytetään isäntäkoneiden välillä ja isäntäkone -reititin-välillä
- Jos vastaanottaja on tavoittamaton
  - Isäntäkoneelle: selvitä osoite uudestaan
  - Reitittimelle: etsi toinen reititin
- Käytetään vain yksilähetyspaketteja lähetettäessä

Automaattinen asetustenmäärittely

- Linkkikohtaisen osoitteen luominen koneelle
  - (ei reitittimelle!)
  - Isäntäkone “keksii” koneosan tunnisteen itselleen
  - Tarkistetaan, että se on yksilöllinen (linkille)
- Reititin kertoo, käytetäänkö tilallista vai tilatonta automaattista osoitteenmääritystä
  - Ajastin kertoo, kuinka kauan verkko-osaa voi käyttää (suositeltava elinaika ja voimassaoloaika)

Automaattinen asetusmäärittely (2)

- Reitittimeltä selvitetään, josko käytetään?
  - tarkkaillaan ilmoitusviestiä tai kysytään
- Yksilöllisyys selvitetään naapurin etsintäviestillä
  - Lähetetään kaikki noodit –monilähetysosoitteeseen
- Jos tunniste on jo käytössä, vastaanotetaan naapuri-ilmoitusviesti
  - Osoite asetetaan käsin

Vertailu

- Tilaton automaattinen osoitteenmääritys
  - Paikalliselle verkolle (linkkikohtainen)
  - Reititintä tarvitaan kertomaan käytettävä verkko -osa
- Tilallinen automaattinen osoitteenmääritys
  - DHCPv6
  - Tiukempi kontrolli verkossa
- Molempia voi käyttää yhtäaikaa:
  - Ensin tilaton tunnisteen luomiseksi, sitten tilallinen muiden tietojen saamiseksi

Polun MTU:n selvittäminen

- IPv6 käyttää päästä-päähän lohkomista
- Lähettäjän pitää tietää polun pienin MTU
  - Ensin käytetään ensimmäisen hypyn MTU:ta
  - Jos ei onnistu, vastaanotetaan ICMP-virheviesti liian suuresta paketista
  - Pienennetään paketteja, kunnes lähetys onnistuu
- Toinen vaihtoehto: käytetään vain minimimittaisia paketteja (ei hyvä)

Polun MTU (jatkuu)

- Polun MTU voi vaihtua
  - Paketit eivät kulje aina samaa polkua
  - Testattava aika-ajoin lähettämällä suurempi paketti
- Monilähetyksessä valitaan se MTU, jota käyttäen viesti menee perille kaikille vastaanottajille

ICMPv6-yhteenveto

- ICMP:lle on uusia käyttökohteita
  - ARP:n sijaan naapureiden osoitteiden selvittämisessä
  - DHCP:n lisäksi oman osoitteen selvittämisessä
  - IP:n käytön tueksi mm lohkomisen tarpeen selvittäminen
- Enemmän tietoa alkuperäisestä paketista ICMP-virheviestiin

Lähteet

- 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

Miten IPv4 ja IPv6 voivat toimia yhteen?

IPv4-IPv6 yhteentoimivuus (interoperability)

- IPv6 over IPv4
  - tuplapino (dual stack)
- IPv4-IPv6 muunnokset
  - Stateless IP/ICMP Translation Algorithm (SIIT)
  - Network Address Translation – Protocol Translation (NAT-PT)
- IPv4 over IPv6

Perustelu yhteentoimivuuden tarpeellisuudelle

- Länsimaissa käytetään edelleen IPv4ää
  - NAT ratkaissut osan osoitteiden riittämättömyydestä
  - Jonkun pitää olla ensimmäinen
  - Yhteentoimivuus pitää taata, ja ratkaisut vielä kehitteillä
- Kuitenkin IPv6 tarjoaa monia etuja IPv4:än verrattuna
  - IPv6 on laajalti käytössä mm. Kiinassa, koska IPv4-osoitteita ei sinne ole jaettu (paljon)

Tuplapino (dual stack) RFC 4213

- Tuplapinoa käytetään kahden IPv6-koneen viestiessä yli (väliin sattuvan) IPv4-verkon
  - Rajakoneessa on tuplapino
- Kahdenlaisia koneita verkossa:
  - Koneita, jotka käyttävät vain IPv4:ä
  - IPv6-koneita, jotka ovat yhteensopivia IPv4:n kanssa
- IPv6:n tunnelointi IPv4:n sisällä
  - router-to-router, host-to-router, host-to-host
  - Tunneleita käsitellään yksittäisenä hyppynä

Tuplapino (2)

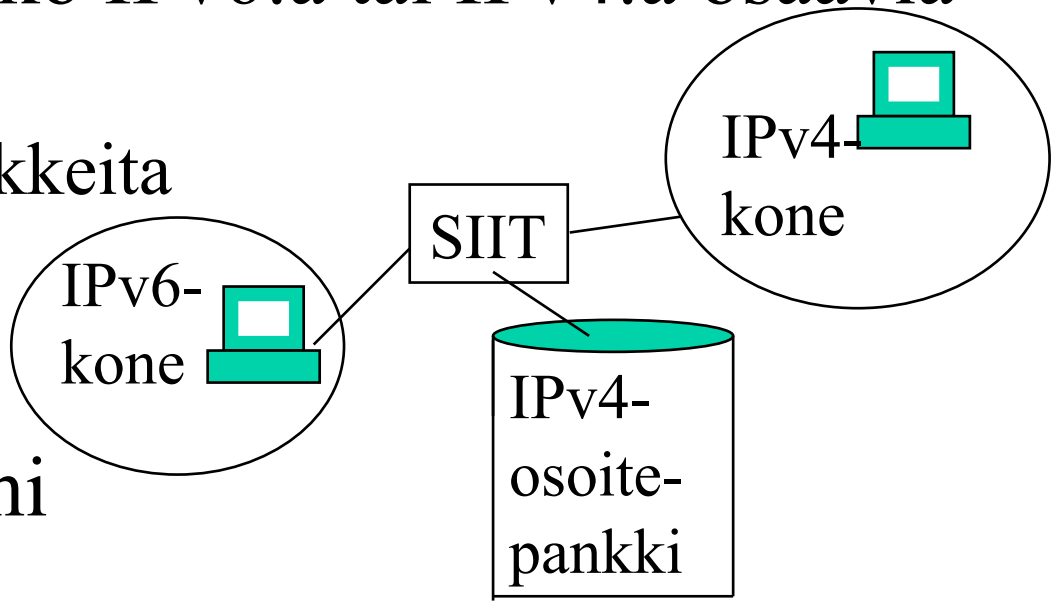
- Tunnelointi voi olla automaattista tai säädettävää
  - IPv4- ja IPv6-osoitteet eivät välttämättä riipu toisistaan
  - Automaattinen tunnelointi käyttää IPv4 -yhteensopivia IPv6-osoitteita
- MTU ja lohkominen
  - Lohkomista vältetään IPv4:n polun MTU:n löytämismenetelmän avulla

Tuplapino (3)

- IPv4:n ICMP-virheviestien käsittely
  - Paketti liian suuri: tunnelin päätepiste hoitaa
  - Muut riippuvat virhetilanteesta
  - Jos alkuperäisessä paketissa tapahtuu virhe, sen havaitseminen voi olla hankalaa
- Nimipalvelua pitää muuttaa
  - Mikä osoitteista palautetaan: A vai/ja AAAA?

SIIT (RFC 2765)

- Stateless IP/ICMP Translation Algorithm (SIIT)
  - IPv6-kone voi viestiä IPv4-koneen kanssa
- Verkko sisältää joko IPv6:a tai IPv4:ä osaavia koneita
  - Pieniä IPv6-saarekkeita
  - IPv4-osoitepotti
- Kaksisuuntainen käännösmekanismi



SIIT (2)

- Muutetaan IP-otsikko versiosta toiseen
  - Lohkominen aiheuttaa ongelmia
- Pitää myös muuttaa ylemmän kerroksen protokollan otsikoita
  - UDP:n tarkastussumma (jos nolla)
  - ICMP-viestien muuttaminen (tiputetaan, jos tuntematon)

NAT-PT (RFC 2766+3596)

- Network Address Translation – Protocol Translation (NAT-PT)
  - IPv6-kone voi viestiä IPv4-koneen kanssa
- ”yhdistelmä” SIIT:sta ja NAT:sta
  - Usempi IPv6-kone voi käyttää yhtä yhteistä IPv4-osoitetta (NAT:n avulla)
  - SIIT:ä käytetään pienin muutoksin

IPv4 over IPv6 (RFC 5754)

- IPv4-liikenteen tunnelointi IPv6-verkon yli
- MP-BGP-reititysprotokolla apuna
  - automaattiset tunnelit, ei tarvi konfiguroida
  - tietoa reitittimen takana olevista IPv4-verkoista toisille IPv4-verkoille

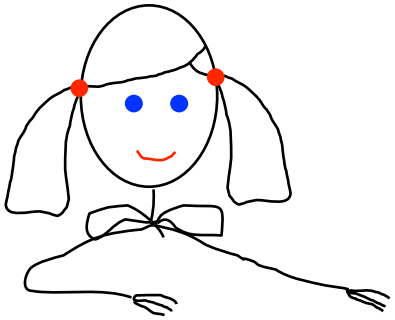
Yhteenveto

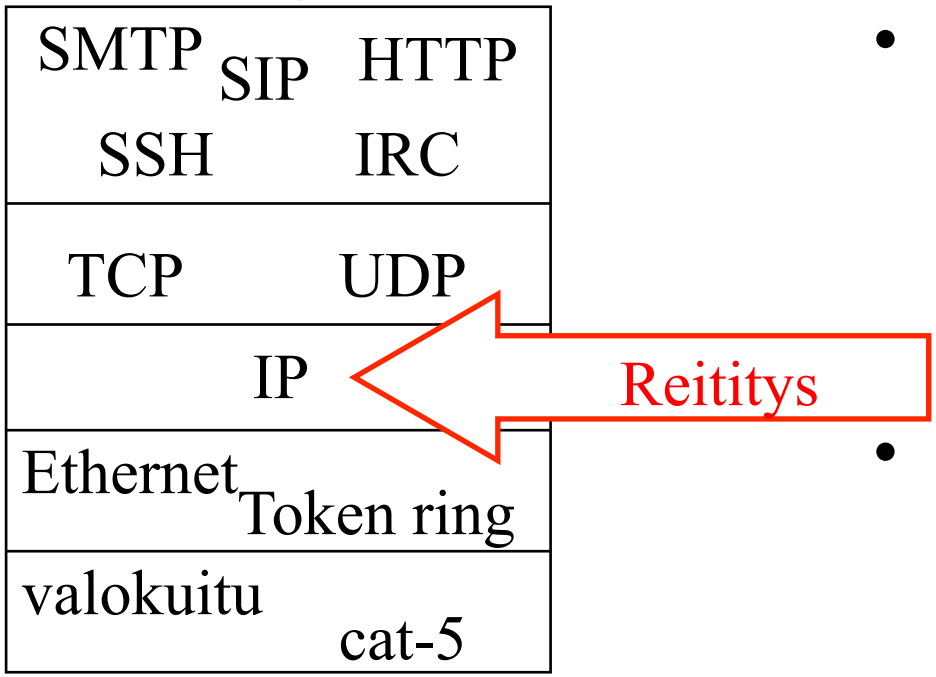
- Yhteentoimivuutta tutkitaan yhä
  - Tuplapinot ja tunnelointi yli sekä IPv4- että IPv6-”saarien”
  - Yhteentoimivuusprotokollat (Interoperability protocols)
- Vaatii muitakin muutoksia verkossa
  - esimerkiksi nimipalveluun (DNS)

Lähteet

- IETF Next Generation Translation workgroup http://www.ietf.org/html.charters /ngtrans-charter.html
- IETF Softwire workgroup https://datatracker.ietf.org/wg/softwire/charter/
- RFC 5747 4over6 Transit Solution Using IP Encapsulation and MP-BGP Extensions, 2010
- Jianping Wu, Yong Cui, Xing Li, Chris Metz. The Transition to IPv6, part I. IEEE Internet Computing, May-June 2006
- Yong Cui, Jianping Wu, Xing Li, Mingwei Xu, Chris Metz. The Transition to IPv6, part II. IEEE Internet Compuring, September-October 2006
- RFC 4760 Multiprotocol Extensions for BGP-4, 2007
- RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers, 2005
- RFC 3596 DNS Extensions to Support IP Version 6, 2003
- RFC 3142 An IPv6-to-IPv4 Transport Relay Translation, 2001
- RFC 3056 Connection of IPv6 Domains via IPv4 Clouds, 2001
- RFC 2765 Stateless IP/ICMP Translation Algorithm (SIIT), 2000
- RFC 2766 Network Address Translation – Protocol Translation (NAT-PT), 2000
- RFC 2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels, 1999
- RFC 2473 Generic Packet Tunneling in IPv6 Specification, 1998

Ensi viikolla





- Reititys autonomisen järjestelmän sisällä
  - Reititysprotokollat
  - Reitityksalgoritmit
- Reititys autonomisten järjestelmien välillä