Aalto-universitetet
Tekniska högskolan

Reititys 3

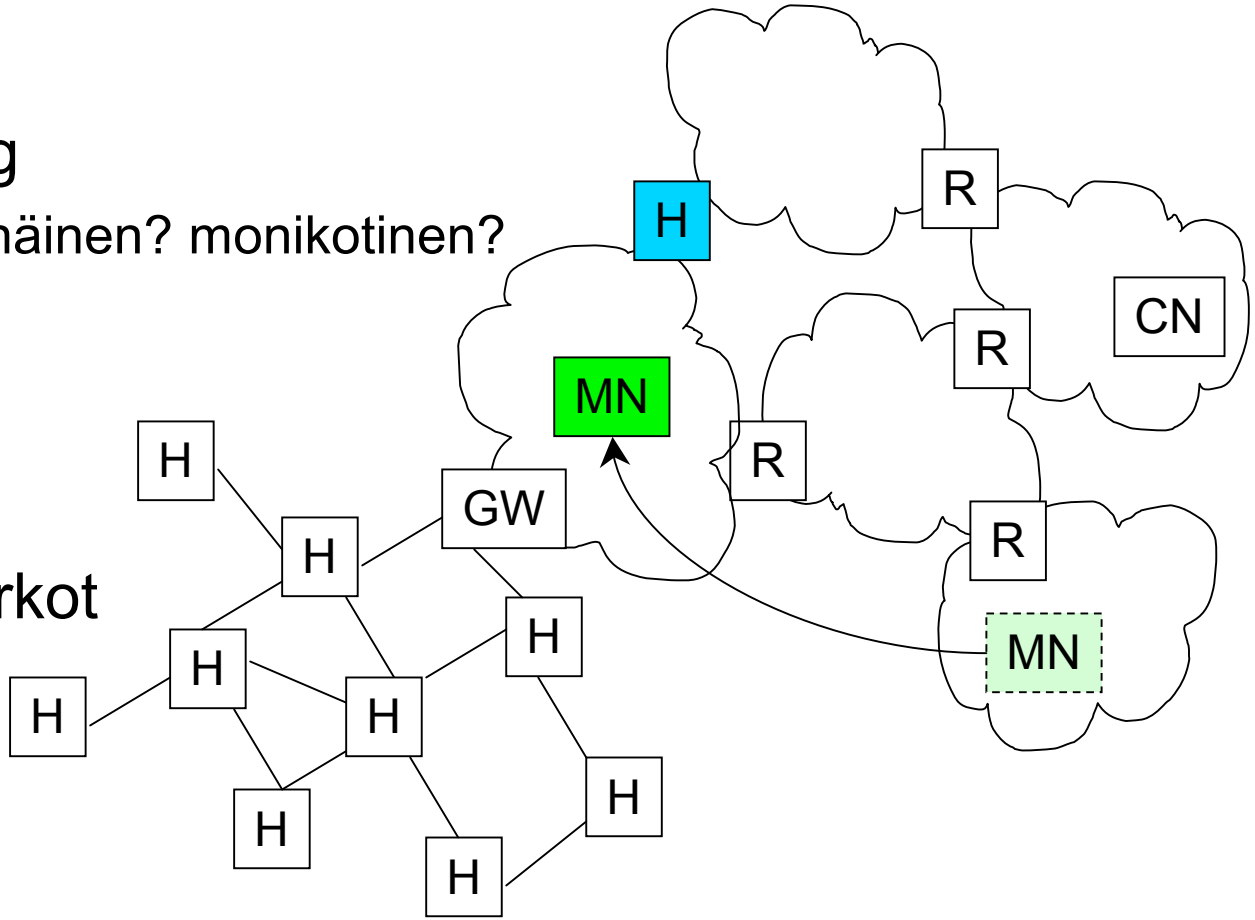
Multihoming, liikkuvuudenhallinta ja vielä vähän muutakin reitityksestä

luvut 18 ja verkkolähteet

Sanna Suoranta
https://noppa.tkk.fi/noppa/kurssi/t-110.4100

Luennon sisältö

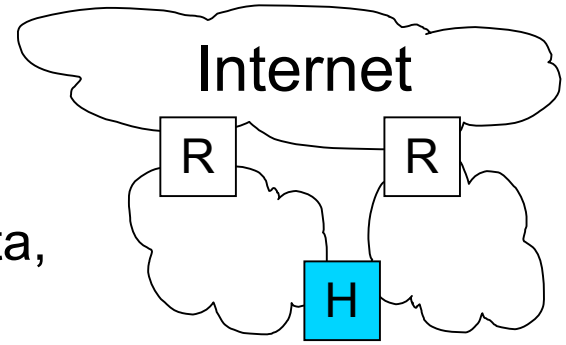
- Multihoming
  - moniliitännäinen? monikotinen?
- Mobile IP
- Ad Hoc -verkot (MANET)



Liikkuvuus ja saavutettavuus

- Liikkuvuus (mobility): tapa vaihtaa verkkoa ja olla silti saavutettavissa
  - laitteella useampi ajan kuluessa vaihtuva yhteys verkkoon
  - Liikkua voi yksittäinen kone tai koko verkko
- ?? (multihoming): tapa olla yhteydessä verkkoon useampaa eri reittiä
  - useampi yhteys verkkoon yhtä aikaa samalle “laitteelle”
  - tavoitteena luotettavuus: (tässä, 3. määritelmä tällä kurssilla ;) taatua saavutettavuutta
- Ongelmana osoitteen duaaliluonne, eli sen toimiminen sekä tunnisteena että osoitteena

Multihoming



- Lisää koneen saavutettavuuden luotettavuutta, kun sillä useampia reittejä verkkoon
  - Tarkoitetaan tässä yksittäisen koneen, esim. serverin yhteyttä,
  - ei esim. operaattoreiden tapaa kahdentaa esim. kaikki verkon reitittimet varmuuden vuoksi
- Jotta oikeasti yhteys kahdentuisi, pitää eri reittien olla
  - eri verkkojen kautta
  - ei yksittäistä muuta pistettä (esim reititin), joiden kautta reitit myöhemmin yhdistyisivät matkan varrella
- Pitää olla yhtenäinen reittiriippumaton tapa löytää palvelu
  - esim. mitä mainostetaan DNS:ssä ja miten vaihdetaan osoite virheen sattuessa

Multihoming - yksittäinen kone

- Yksi verkkokortti - useampi IP-osoite
  - jos verkkokortti hajoaa, ei oikeasti sitten toimi verkko
- Useampi verkkokortti, joista jokaisella omat IP-osoiteet
  - jos yksi korteista hajoaa, kone on yhä tavoitettavissa, mutta
  - käynnissä olleet yhteydet katkeavat, sillä istuntojen päätepisteitä ei voi esim. TCP:ssä vaihtaa (SCTP:ssä voi)
  - (multi-attached eli useampi yhteys samaan verkkoon)
- Käytössä voi olla eri verkkoteknologia
  - eli koneella voi olla sekä IPv4- että IPv6-osoite
- Palvelimen kahdentaminen/virtualisointi on jotain aivan muuta

Multihoming - aidosti useampi yhteys (IPv4-multihoming, RFC 4116)

- Aidosti useampi yhteys verkkoon eri autonomisten järjestelmien kautta
  - yksi multihomed-AS, jolla useammalta ISP:ltä yhteys muualle Internetiin
  - kun yksi verkkoyhteyksistä pettää, voidaan liikenne ohjata toisen verkkoyhteyden kautta, eli toinen yhteyksistä varalla
- Verkkoliikenteen jakaminen kulkemaan eri verkkoyhteyksien kautta (eri transit-ASien kautta)
  - BGP:ssä kohdeverkkokohtaisilla poluilla
  - kovin pieniä verkkoja ei kuitenkaan mainosteta (/24 verkko-osan pituus ainakin) yksittäin, vaan niistä koostetaan mainos (aggregate)

IPv4-multihoming - ominaisuudet

- Redundanssi - useampi yhteys mahdollista
- Kuormanjako - ulosmenevälle liikenteelle mahdollista
- Politiikka - joskus mahdollista määritellä eri protokollille erilainen kohtelu eri reittien kautta
- Verkkokerroksen ongelmista toipuminen kuljetuskerroksella mahdollista - tosin vaatii erikseen tukea kuljetuskerroksen protokollilta
- DNS toimii kuten ennen
- Reititystaulujen kasvaminen ongelmista

IPv6-multihoming

- Useita eri tapoja ja ratkaisuja, jotka on hyvinkin erilaisia
  - osa uusia, osa mukana jo alusta alkaen, esim:
- IPv6-osoitteet, joiden verkko-osa on vaihdettavissa (network provider independent addresses)
  - erikseen sovittava reitityksestä operaattorin kanssa, mutta operaattorin vaihtaminen ei muuta osoitetta
  - 2001:678::/29
  - kuljetuskerroksen yhteydet säilyvät, sillä osoite ei ole sijaintiriippuva
- Automaattinen uudelleennumerointi, kun verkko-osa vaihtuu
  - Rikkoo kyllä olemassaolevat yhteydet

Protokollapohjaisia ratkaisuja: Shim6

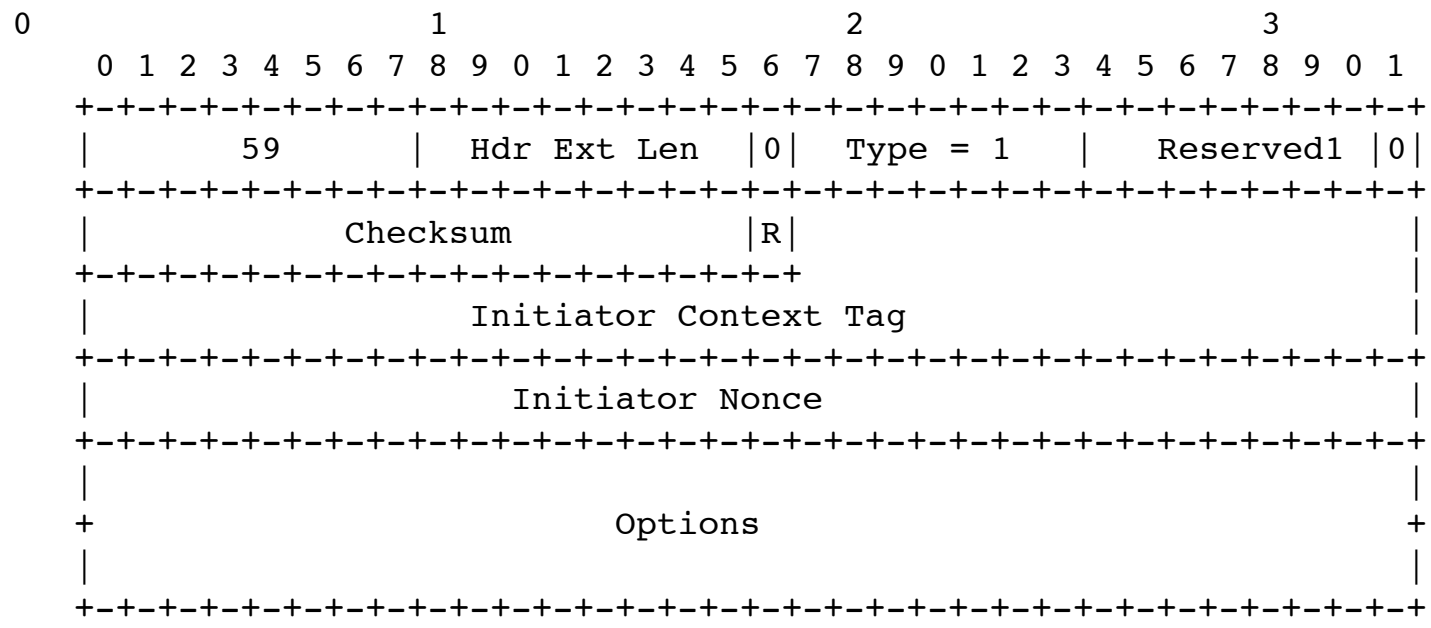
Shim6 (RFC 5533)
Site Multihoming by IPv6 Intermediation

- Kuormantasaukseen ja “lokaatio”- virheistä (=verkkoyhteyden katkeaminen) toipumiseen ilman käynnissäolevien yhteyksien katkeamista
  - ilman operaattorittomia osoitteita
  - Uusi lisäotsake IPv6een (next header = 140)
- Kun ihan tavallinen kuljetuskerroksen (TCP-)yhteys (=konteksti) on ollut hetken käytössä (esim 50 pakettia lähetetty), päätellään, että yhteys kannattaa suojata ja neuvotellaan Shim6-yhteys
  - jos vastaanottaja ei reagoi mitenkään, päätellään, ettei se tue menettelyä
  - jos ongelmia ei esiinny, liikenne jatkuu kuten ihan tavallisesti

Shim6 - Kun yhteys verkkkoon katkeaa

- Sovellusyhteyden lisäksi testataan välillä naapurin saavutettavuutta
  - eli että IP-osoite (paikan tunniste) on yhä sama
- Jos havaitaan katkos, selvitetään uusi osoite ja
  - tai jos halutaan käyttää toista osoitetta
- Pakataan paketit IP-in-IP-tunneliin, eli “alkuperäisen” paketin eteen lisätään Shim6-lisäotsake ja uusi IP-otsikko
  - yhteydet tunnistetaan kummassakin päässä tripleteillä <peer ULID, local ULID, local Context Tag>
  - mahdollista yhdistää useampi yhteys samaan kontekstiin
  - lisäotsikko sijoitetaan reititys- ja lohkomisotsikoiden väliin

Shim6-yhteyden avaus (neljä viestiä)



- Ensimmäisessä viestiparissa kerrotaan vastaanottajalle kontekstin tunniste (tag) ja nonssi tuoreuden takaamiseksi
  - Optioissa ULID-pari, jos toivutaan virheistä (IP-osoite vaihtunut)
  - Vastausviestissä lähettäjän ja vastaanottajan luomat nonssit

Shim6-yhteyden avaus (2)

- 3. viesti sisältää
  - nonssit takaavat molemmille osapuolille, että yhteys on tuore
  - Lista osoitteista ja mahdollisesti niiden preferenssijärjestys
  - Allekirjoitus
- 4. viestissä alkuperäisen lähettäjän nonssi, ja samoin lista osoiteista ja mahdollisesti niiden järjestys sekä allekirjoitus
- Nopeutettua yhteydenmuodostusta käytetään, jos pyydetään vaihtamaan osoitetta yhteydelle, jota ei ole

Shim6 - Muut viestit

- Update-viestillä päivitetään osoitelista
  - viesti kuitataan sen sisältämällä nonssilla
- Keepalive-viesti pitää auki oikeastaan yksisuuntaisia yhteyksiä myös toiseen suuntaan
- Probe-viestiä käytetään, kun yhteydellä toimii eri osoitteet eri suuntiin
- Virheviesti kertomaan ongelmatilanteista

- Yhteyden turvaamiseen voi käyttää IPseciä

Shim6 - Yhteenveto

- Shim6 luo kontrollikanavan datakanavan rinnalle
  - mekanismit huomata IP-osoitteiden muutokset
  - normaalitilanteessa liikenne kulkee ihan kuten ennenkin
  - IP-osoitteen muututtua tunneloidaan IP-kerroksen liikenne uuteen osoitteeseen
- Shim6 vaatii muutoksia kummankin osapuolen IP-pakettien lähetykseen
- Ei vaadi verkolta lisälaitteita tai toiminnallisuuksia
- Ei vaadi muutoksia kuljetuskerrokseen (TCP) tai sovelluksiin

Toinen protokolla/ arkkitehtuuri-ratkaisu: HIP

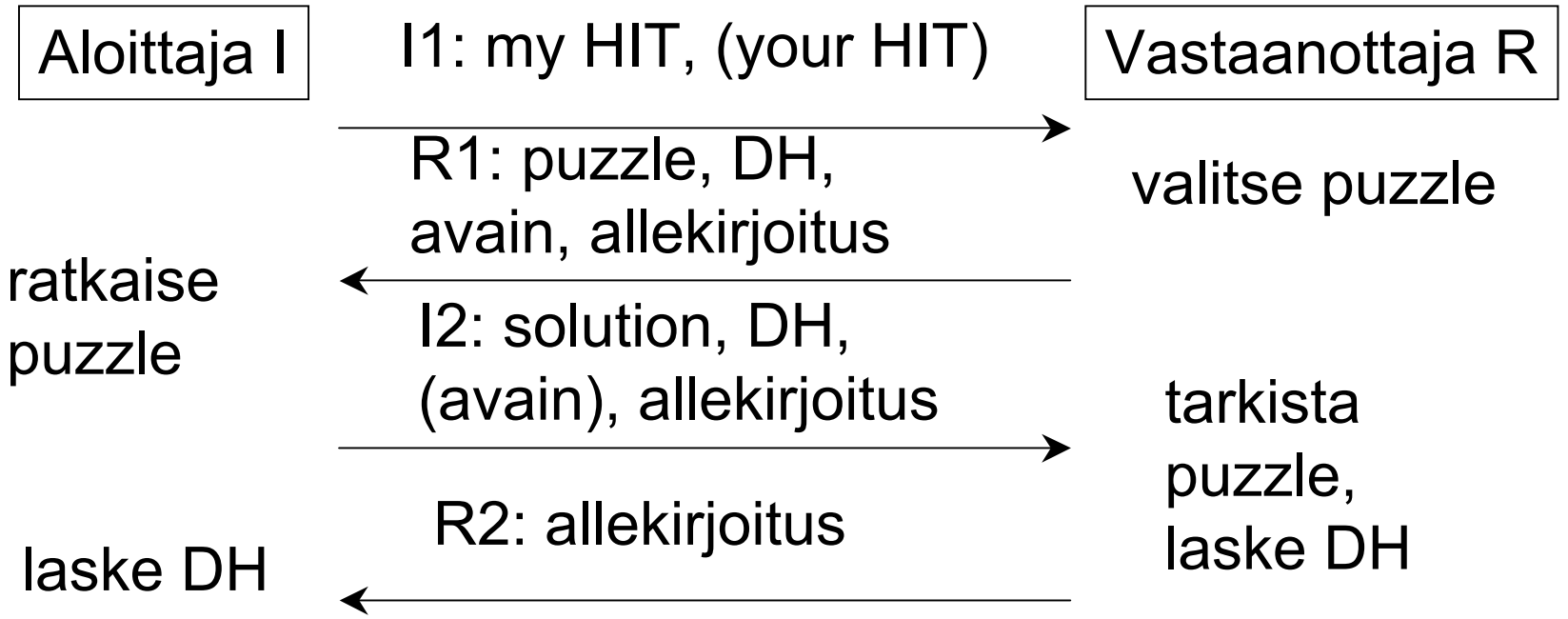
HIP (RFC 4423 et co)
Host Identity Protocol

- HIP tuo uuden kerroksen verkko- ja kuljetuskerrosten väliin eli IP:n ja TCP/UDP:n väliin
- IP-osoitetta käytetään pelkkänä osoitteena, sen tunnisteosan korvaa Host Identity (HI)
  - ylemmän kerroksen protokollissa IP-osoite korvataan HI:llä, eli TCP-yhteyden päätepisteenä <HI, portti>-pari
- HI on julkinen avain
  - siitä lasketaan 128-bittinen tiiviste, jota kutsutaan HIT:ksi
  - kone voi generoida itse avaimen, tai
  - avain voi olla jonkin varmennepalvelun (CA) sertifioima

HI-tunnisteiden käsittely

- IP-osoite voi vaihtua, kun ylemmän kerroksen protokolla käyttää tunnisteena HI:tä
  - olemassaolevat yhteydet säilyvät (multihoming)
  - jopa allaolevan IP:n versio voi vaihtua, tarvitaan vain mekanismi sitoa osoite HI:hin
- Uuden yhteyden avaus tapahtuu rendezvous-mekanismin avulla
  - myös jos molemmat osapuolet vaihtavat paikkaa samanaikaisesti
- HI-tunnisteet tallennetaan joko DNSään tai DHTeen
  - hajautettu tiivistetaulu DHT (Digital Hash Table) on tapa tallettaa tieto hajautetusti useammalle palvelimelle, joista jokaisella osittainen tieto ja tapa ohjata kyselijä eteenpäin

HIP-basic exchange



- Aloitusviesti voi kulkea rendezvous-palvelimen kautta
- DH = Diffie-Hellman-avaintenvaihto

HIP ja turvallisuus

- Kryptografisten avainten käytöstä tunnisteena saa sivutuotteena paremman turvallisuuden
  - voidaan käyttää suoraan IPsec ESP-suojausta, koska avaimet on jo valmiiksi tarjolla
  - voidaan laskea istunnolle symmetrinen avain turvallisesti
- Suoja palvelunestohyökkäyksiä vastaan
  - voidaan vaatia yhteyden avaajaa ratkaisemaan tehtävä (puzzle) ennen kuin yhteys oikeasti avataan
  - asiakas osoittaa käyttämällä omaa laskentatehoaan oikeasti haluavan yhteyden
  - hyökkääjän ei kannata hyökätä, koska laskentatehoa kuluu

HIP - Yhteenveto

- Multihoming, liikkuvuus, IPv4-v6-yhteentoiminta ja turvallisuus yhdessä paketissa
  - uusi tunniste HI, IP-osoite ilmaisee vain sijainnin
  - uusi kerros IP:n ja kuljetuskerroksen väliin
  - toimii kummankin IP-version kanssa
- Tarvitsee todella paljon muutoksia
  - koneiden TCP/IP-pinot, TCP-pseudo-otsikko
  - DNS, NAT, jne
  - sovelluksiin ei tarvi muutoksia, jos ne käyttävät nimiä eikä IP-osoitteita

Multihoming - Yhteenveto

- Useampi eri yhteys verkkoon tuo luotettavuutta saavutettavuudelle
- Aiheuttaa ongelmia olemassaoleville protokollille
  - osoitteiden vaihtumisen vuoksi
- Monet ratkaisut lähinnä tutkijoiden puuhastelua eivätkä käytössä operaattoreiden verkoissa
  - ei ainakaan vielä :)
- Ratkaisuja kehitteillä myös ylemmillä kerroksilla
  - SCTP (Stream Control Transmission Protocol, RFC 4960,3286) -yhteydellä päätepisteellä voi olla useampi IP-osoite

Lähteet - multihoming

- RFC 4116 IPv4 multihoming practices and limitations, 2005
- Site Multihoming by IPv6 Intermediation (shim6) WG: http://datatracker.ietf.org/wg/shim6/charter/
- RFC 3582 Goals for IPv6 site-multihoming architectures, 2003
- RFC 3178 IPv6 multihoming support at site exit routers, 2001
- RFC 4219 Things multihoming in IPv6 (MULTI6) Developers should think about, 2005
- RFC 4218 Threats relating to IPv6 multihoming solutions, 2005
- RFC 5533 Shim6: Level 3 Multihoming Shim Protocol for IPv6, 2009
- RFC 5534 Failure Detection and Locator Pair Exploration Protocol for IPv6 Multihoming, 2009
- RFC 5535 Hash-Based Addresses (HBA), 2009
- RFC 4423 - Host Identity Protocol (HIP) Architecture, 2006
- RFC 5201 - Host Identity Protocol, 2008
- RFC 5202 - Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP), 2008
- RFC 5203 - Host Identity Protocol (HIP) Registration Extension, 2008
- RFC 5204 - Host Identity Protocol (HIP) Rendezvous Extension, 2008
- RFC 5205 - Host Identity Protocol (HIP) Domain Name System (DNS) Extension, 2008
- RFC 5206 - End-Host Mobility and Multihoming with the Host Identity Protocol, 2008
- RFC 5207 - NAT and Firewall Traversal Issues of Host Identity Protocol (HIP) Communication, 2008

Näistä lisää kurssilla T-110.5116 Tietokoneverkot II

Seuraavaksi liikkuvuus (mobility)

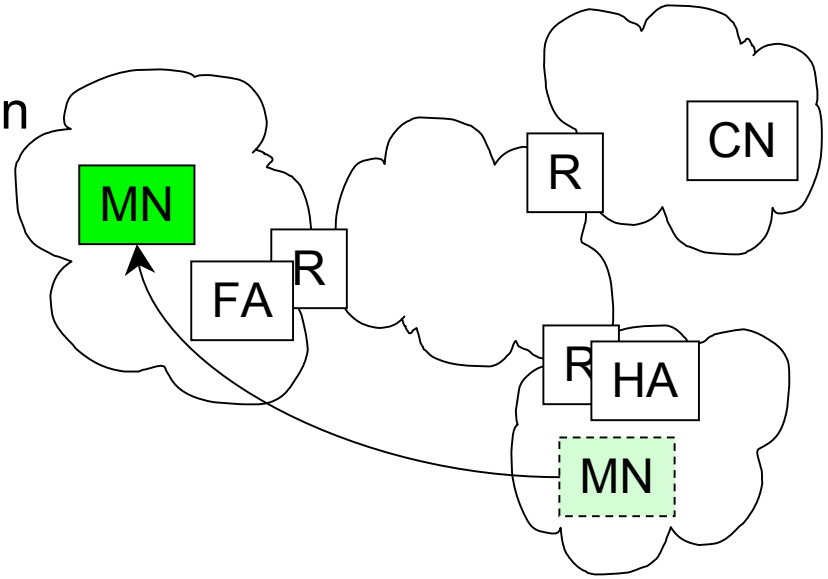
Näistäkin lisää kurssilla T-110.5116 Tietokoneverkot II :-)

Liikkuvuudenhallinta

- Liikkuvuudenhallinnan tavoitteena on säilyttää yhteys verkkoon siten, että sovellusten yhteydet eivät katkea, vaikka verkkoyhteyden päätepiste muuttuu
  - yksi yhteys kerrallaan
- Mikromobility: paljon nopeita siirtymiä verkosta toiseen lyhyellä aikavälillä
- Makromobility: liikutaan verkosta toiseen, mutta uudessa verkossa pysytään kauemmin
  - Mobile IP on ratkaisu tähän

Mobile IP

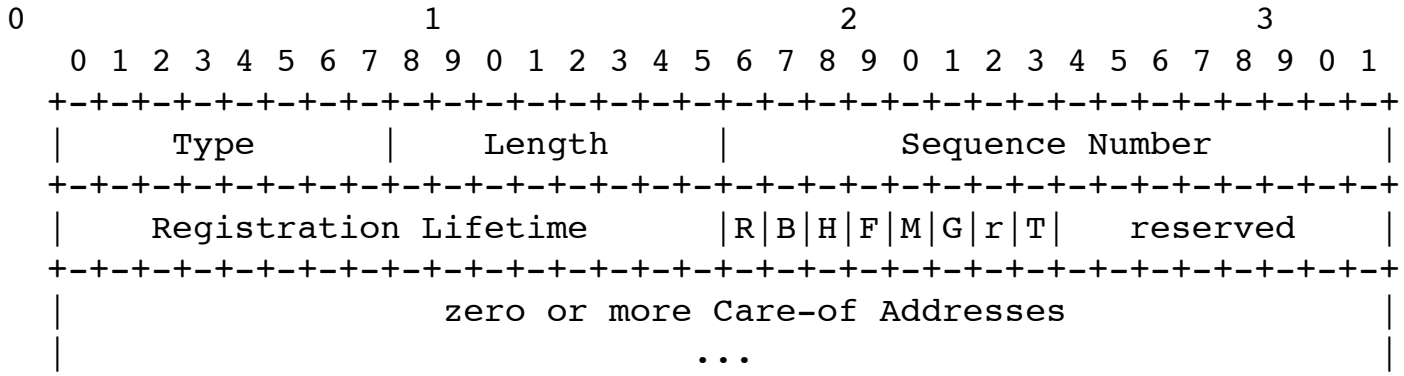
- Jokaisella koneella on kotiverkko ja siellä IP-osoite
- Kone voi kuitenkin liikkua toiseen verkkoon siten, että
  - se on edelleen tavoitettavissa kotiosoitteensa kautta
  - yhteydet säilyvät
- Liikenne tunneloidaan koneen senhetkiseen osoitteeseen
- Kaksi versiota: Mobile IPv4 ja Mobile IPv6



Mobile IP - osoitteet

- Kotiosoite (home address) on pysyvä osoite, josta liikkuvan koneen (mobile node, MN) tavoittaa aina
  - koneen ollessa kotiverkossa se käyttää osoitettaan kuten tavallinen liikkumaton kone (ensisijainen osoite)
  - koneen ollessa muualla, kotiagentti (home agent, HA) vastaanottaa viestin ja lähettää sen edelleen (tunneloi) koneen nykyiseen sijaintiin
- Vierailuosoite (care-of address)
  - Vierailuverkon normaalilla osoitteenjakotavalla saatu osoite (co-located care-of address), ka liikkunut kone huolehtii itse tunneloinnista (vierailuverkon ei tarvi tietää asiasta mitään)
  - Vierailuverkossa voi olla myös vierailuagentti (foreign agent, FA), joka huolehtii tunnelista liikkuneen koneen puolesta (foreign agent care-of address), ja voi jopa kätkeä kaikki NATin yhden osoitteen taa

Mobile IPv4 - Verkon vaihtaminen



- Kone huomaa verkon vaihtuneen agentin etsintämenettelyssä (agent discovery)
  - Laajennus ICMP:n reitittimenlöytämisviestin laajennus, eli mobiiliagentin ilmoitusviesti (Mobile Agent Advertisement Extension)
  - lisätään tavallisen reititinilmoitusviestin perään ilman erillisiä otsikoita

Mobile IPv4 - Uuden sijainnin ilmoitus

- Kun kone on saanut vierailuverkosta osoitteen, se ilmoitetaan kotiagentille
  - joko kone hoitaa rekisteröinnin itse suoraan kotiagentin kanssa (co-located care-of address)
  - tai vierailuagentti hoitaa koneen puolesta (fa-co-address), jolloin pyyntö lähetään vierailuagentille
- Vierailuosoite on voimassa viestissä ilmoitetun ajan
  - kun kone palaa kotiverkkoon, ajaksi ilmoitetaan nolla
- Koti- ja/tai vierailuagentti lähettää kuittauksen, jolloin luodaan tunneli kotiverkosta koneelle (mahdollisesti vierailuagenin kautta)

Mobile IPv4 - Viestin lähetys ja vastaanotto

- Viesti joko lähetetään suoraan
  - lähettäjäosoitteena käytetään kotiosoitetta
- tai viesti tunneloidaan vierasagentilta kotiagentille, joka lähettää sen edelleen vastaaanottajalle
  - vierailuverkon palomuuri saattaa muuten hylätä viestin (ingress filtering)
- Vastaanottajan (correspondent node, CN) ei tarvitse tietää mitään Mobile IP:stä
  - paluuviestit kiertävät aina kotiagentin kautta
- Kolmioreititys tai kaksinkertaisen reitin ongelma
  - erittäin tehotonta, jos viestitään vierailuverkon laitteen kanssa

Mobile IPv6 - Parannuksia v4-versioon

- Erillistä vierasagenttia ei tarvita lainkaan
  - vierasverkon reititin kertoo osoitteidenhankkimistavan, jota käytetään
  - liikkuva kone ilmoittaa itse kotiagentille sijaintinsa
- Tuki reitinoptimoinnille
  - ratkaisee kolmireitityksen luoman ongelman
- Kevyempi tunnelointimenetelmä
  - Käyttää IPv6:n reitityslisäotsikkoa eikä IP-in-IP-tunnelointia

Mobile IPv6 - Binding Update (BU)

- Liikkuva kone lähettää sijainnin päivityksen kotiagentin lisäksi myös koneelle, jonka kanssa se on viestimässä (correspondent node)
  - Kotiagentin kanssa yhteys suojataan IPsec ESP:llä
- Vastaanottaja tarkistaa BU:n todenperäisyyden takaisinreititysproseduurin (return routability) avulla
  - testiviestit lähetetään samanaikaisesti sekä koti- että vierailuosoitteisiin
  - vastauksessa liikkuva kone todistaa saamansa kummatkin ja pystyvänsä viestimään molempia reittejä käyttäen myös takaisin

Mobile IP - yhteenveto

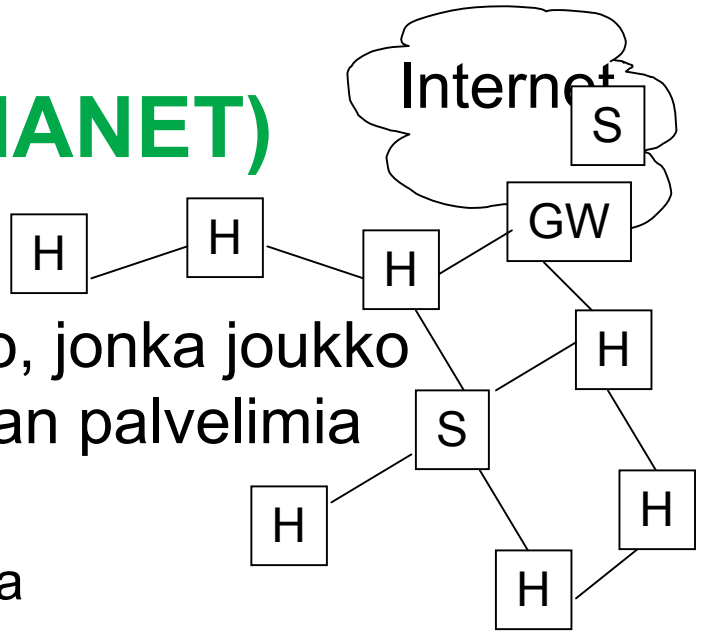
- Kone voi vaihtaa verkkoa ilman, että sovellusten yhteydet katkeavat
- Käytetään koti- ja vierailuosoitteita
- Vaatii ainakin kotiverkkoon kotiagentin (reititin)
  - IPv4-versio vaatii muutoksia ARP-protokollaan, jotta kotiverkon koneet voivat viestiä joko liikkuvan koneen kanssa suoraan tai kotiagentin kautta

Mobile IP - lähteet

- RFC 3344 IP Mobility Support for IPv4, 2002
- RFC 4721 Mobile IPv4 Challenge/Response Extensions (Revised), 2007
- RFC 3775 Mobility Support in IPv6, 2004

Seuraavaksi hieman Ad Hoc -verkoista

Mobile Ad-Hoc Network (MANET)



- MANET on infrastruktuuriton verkko, jonka joukko langattomia laitteita muodostaa ilman palvelimia keskenään
  - laitteet voivat tarjota toisilleen palveluita
  - laitteet voivat olla yhteydessä toisiinsa toistensa kautta
- Verkon linkit muuttuvat taajaan, sillä jokainen laite voi liikkua itsenäisesti
- MANET voi olla yhteydessä Internetiin yhdyskäytävän (gateway) avulla
  - palveluita voi etsiä esim SLP:n avulla
  - jokin laitteista voi siis tarjota palveluna yhteyttään Internetiin

MANET - Reititys

- Jos laitteet eivät ole yhteydessä suoraan toisiinsa, tarvitaan reititystä
- Proaktiivinen (tauluohjattu; proactive, table-driven)
  - laitteet selvittävät verkon yhteydet etukäteen
  - kun yhteyttä tarvitaan, se on nopeasti käytettävissä
  - OLSR, TBRPF ja monta muuta ehdotusta
- Reaktiivinen (tarveohjattu; reactive, on-demand)
  - laite selvittää reitin toiseen vasta kun yhteyttä siihen tarvitaan
  - ei turhaa työtä, mutta yhteyden avaus kestää kauemmin
  - AODV, DSR ja monta muuta ehdotusta

MANET - Lähteet

- RFC 2608 Service Location Protocol, Version 2, 1999
- RFC 2501 Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, 1999
- RFC 3561 Ad hoc On-Demand Distance Vector (AODV) Routing, 2003
- RFC 3626 Optimized Link State Routing Protocol (OLSR), 2003
- RFC 3684 Topology Dissemination Based on Reverse-Path Forwarding (TBRPF), 2004
- RFC 4728 The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4, 2007
- RFC 5444 Generalized Mobile Ad Hoc Network (MANET) Packet/Message Format, 2009
- IETF:n MANET-työryhmä http://datatracker.ietf.org/wg/manet/charter/

Seuraavaksi ensi viikolla

- TkT Matti Siekkinen kertoo tiistaina kuljetuskerroksesta
  - sitten kaikki 1. osatentin asiat on käyty läpi
- Torstaina harjoitustyöstä
  - Huom! Luento alkaa vasta yhdeksältä!