Aalto-yliopisto
Perustieteiden
korkeakoulu

Multihoming ja liikkuvuudenhallinta

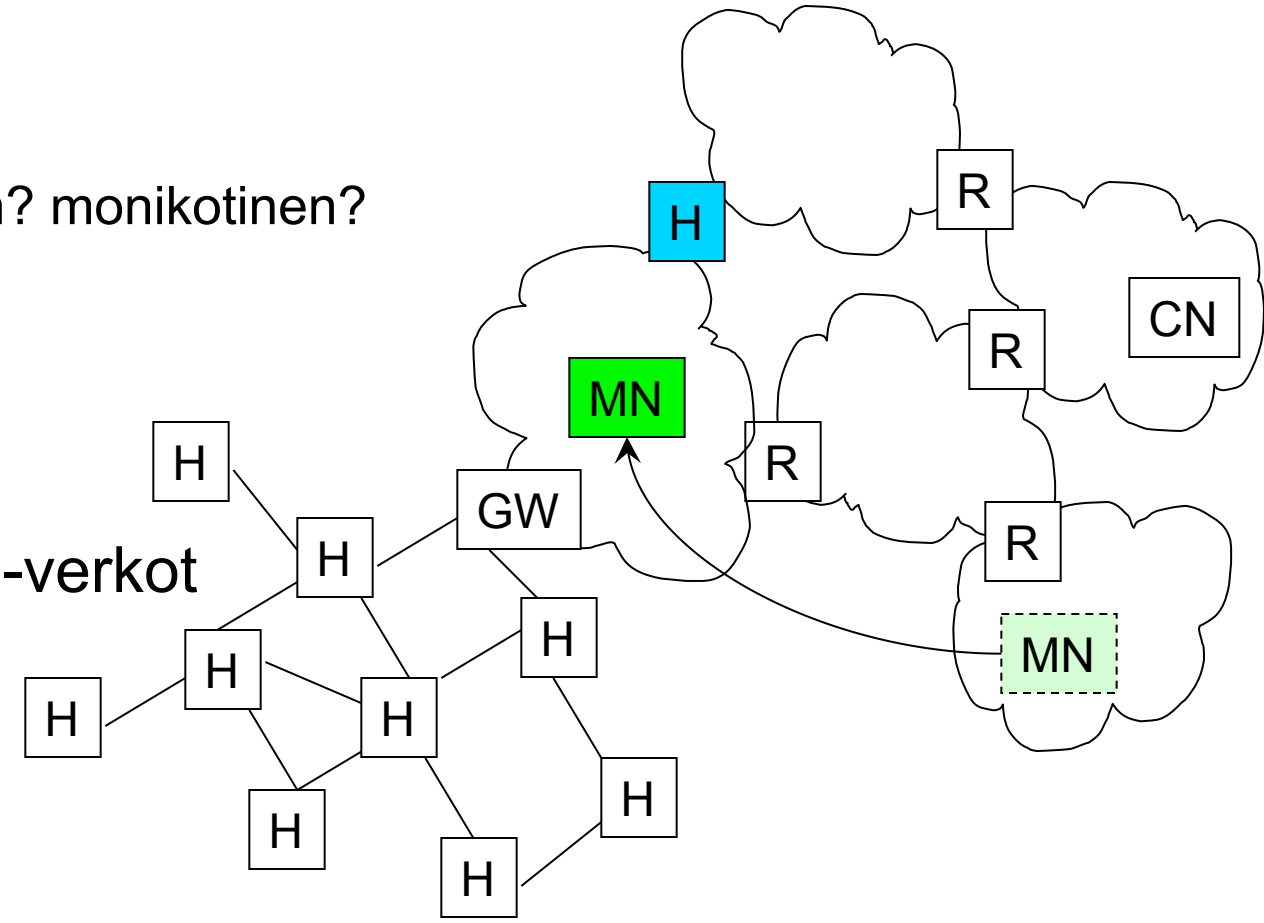
Matti Siekkinen

21.2.2012

Lähteet:
•Sanna Suorannan edellisten vuosien materiaali.
•Nick Feamster: CS 7260 (2007)
•Miika Komu: HIP (110.5111, 2011)
•etc.

Luennon sisältö

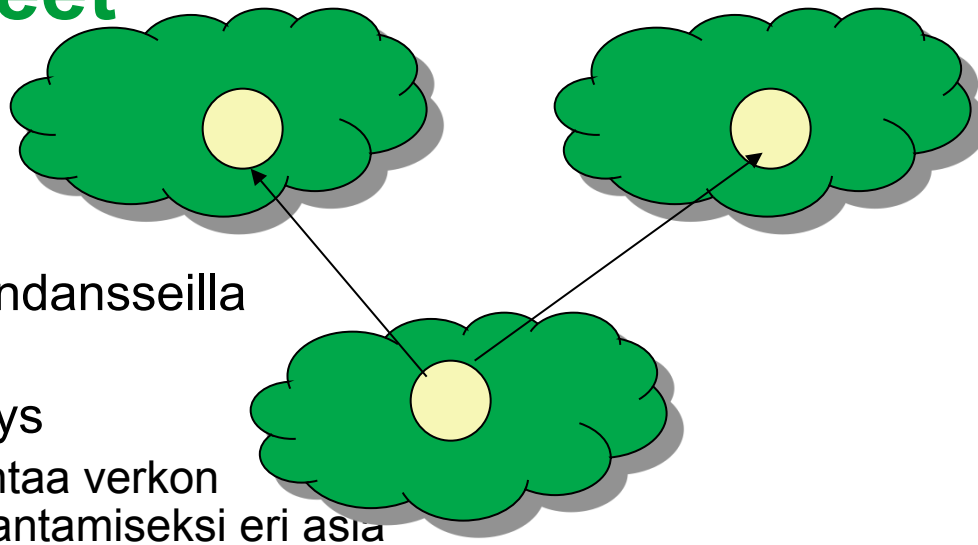
- Multihoming
  - moniliitännäinen? monikotinen?
- Mobile IP
- (Mobiilit Ad Hoc -verkot (MANET))



Multihoming ja liikkuvuus

- Multihoming (monikotisuus?)
  - Päätelaite on yhteydessä verkkoon useampaa eri reittiä
  - Useampi yhteys verkkoon yhtä aikaa samalle “laitteelle”
  - Saman tai eri palveluntarjoajien (ISP) kautta
- Liikkuvuus (mobility)
  - Päätelaite vaihtaa verkkoa ja pysyy koko ajan saavutettavissa
  - Laitteella useampi ajan kuluessa vaihtuva yhteys verkkoon
  - Liikkua voi yksittäinen kone (host mobility) tai koko verkko (network mobility)
- Miksi tämä on vaikeaa?
  - IP-osoitteen kaksijakoinen luonne: tunniste ja osoite

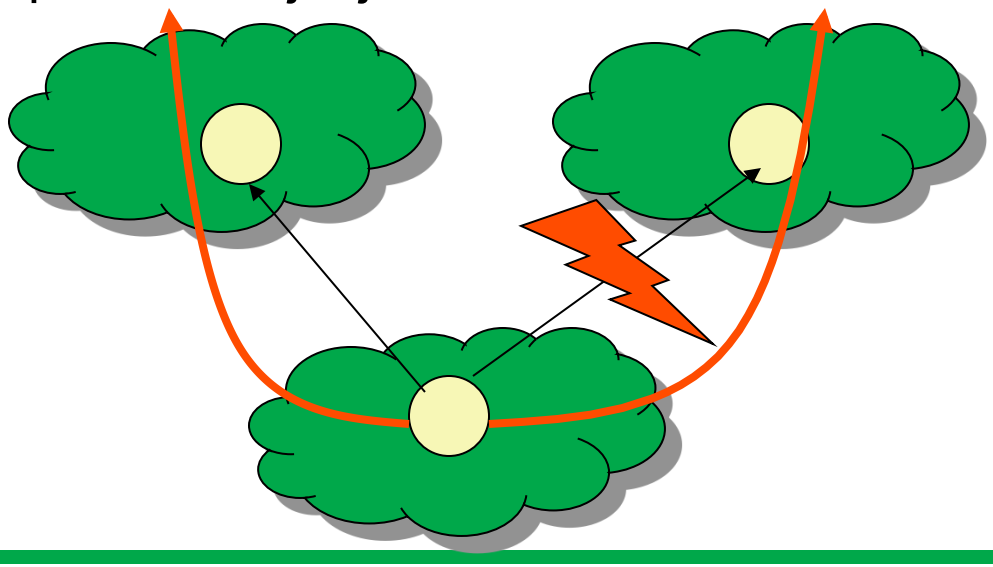
Multihoming: tavoitteet



- Useimmiten luotettavuus
  - Parempi saavutettavuus redundansseilla reiteillä
  - Yksittäisen päätelaitteen yhteys
    - Operaattoreiden tapa kahdentaa verkon reitittimiä luotettavuuden parantamiseksi eri asia
    - Palvelimen kahdentaminen/virtualisointi myös eri juttu
      - T-110.5150 Applications and services in Internet
- Lisäksi suorituskyvyn parantaminen
  - Kuorman tasaus
  - Suurempi läpisyöttö
  - (Parempi energiatehokkuus (mobiililaitteet))

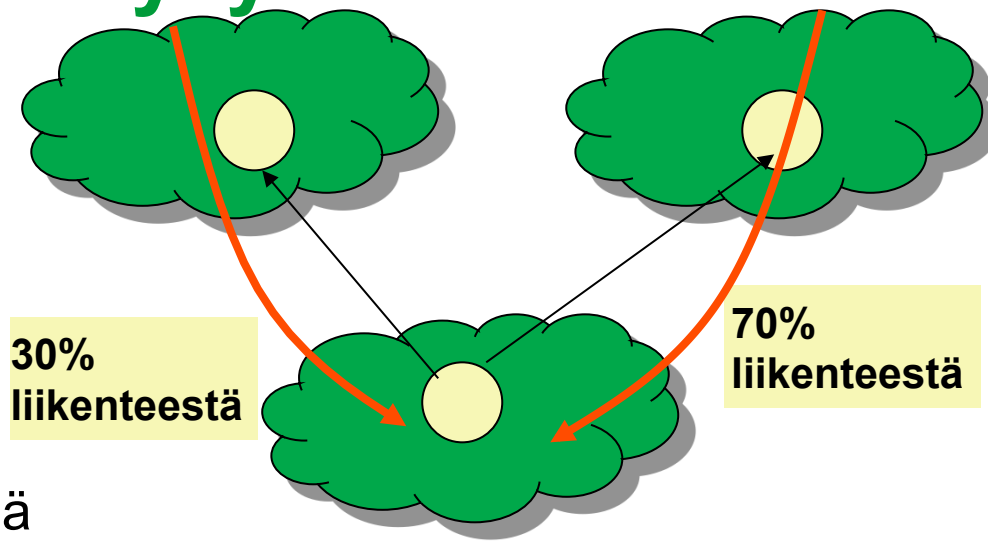
Multihoming: luotettavuus

- Pyritään välttämään keskitettyä vikakohtaa (single point of failure)
- Yhteys Internetiin säilyy vaikka:
  - Paikallisia laiteongelmia (kuitu poikki, verkkolaite kaatuu, jne.)
  - Ongelmia palveluntarjoajalla



Multihoming: suorituskyky

- Edut
  - Kuorman tasaus
  - Suurempi kokonaisläpisyöttö
- Multihoming ja TCP
  - Yleensä yksi yhteys yhtä reittiä
    - Liikenne ohjataan puhtaasti IP tasolla
  - Voi myös olla yksi multihomed yhteys
    - Vaatii erityisratkaisuja kuljetuskerroksella
    - Lisäetuna parempi energiatehokkuus (mobiililaitteet)
      - Linkin energiatehokkuus vaihtelee hetkellisesti sekä eri teknologioiden kesken (Wi-Fi, 3G, LTE, Bluetooth)



Multihoming: toteuttaminen

- Päätelaitteessa
  - Yksi verkkokortti - useampi IP-osoite
    - Single point of failure
  - Useampi verkkokortti, joista jokaisella omat IP-osoitteet
    - Jos yksi korteista hajoaa, kone on yhä tavoitettavissa
      - Jos käytössä TCP, käynnissä olleet yhteydet katkeavat
        - TCP ei osaa vaihtaa päätepisteitä kesken yhteyden
        - Esim. SCTP osaa
    - (multi-attached: useampi yhteys samaan verkkoon)
- IPv4 ja IPv6 mahdollistavat eri ratkaisuja

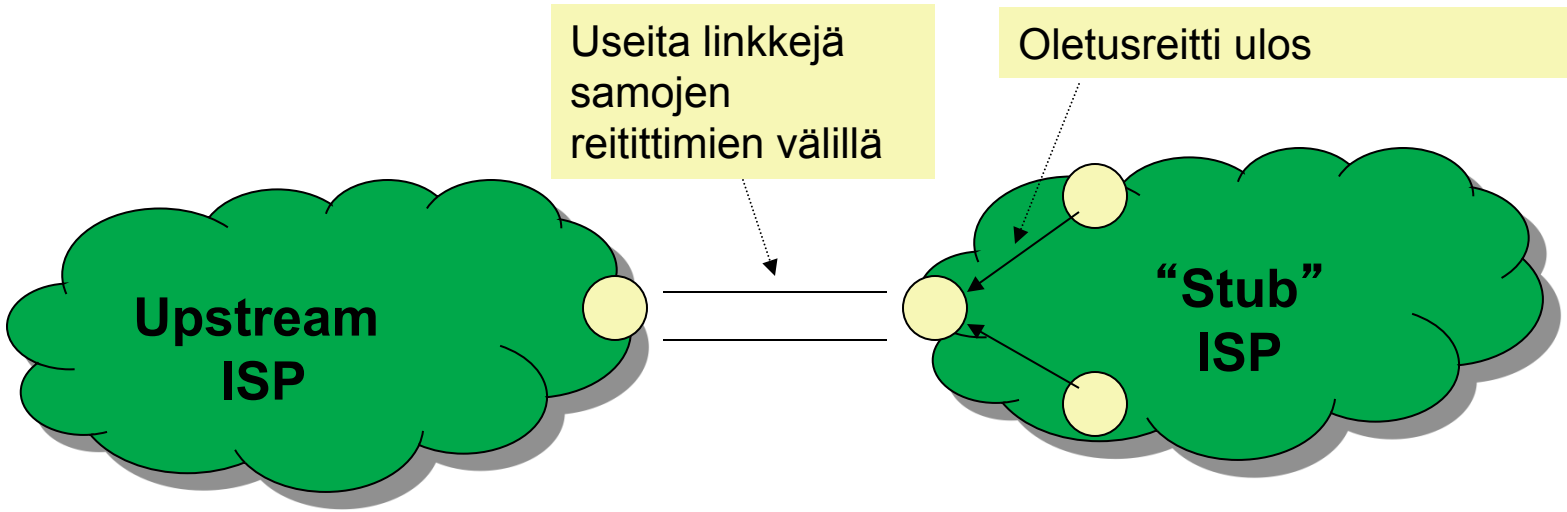
IPv4-multihoming

- Useampi yhteys verkkoon eri autonomisten järjestelmien (AS) kautta
- BGP:aa käytetään eri reittien mainostamiseen
  - Verkkoliikenne jaetaan eri reiteille
- Verkkokerroksen ongelmista toipuminen kuljetuskerroksella mahdollista
  - Vaatii erikseen tukea kuljetuskerroksen protokollilta
- DNS toimii kuten ennen
- RFC 4116: IPv4 Multihoming Practices and Limitations

IPv4-multihoming: eri tyyppiset AS:t

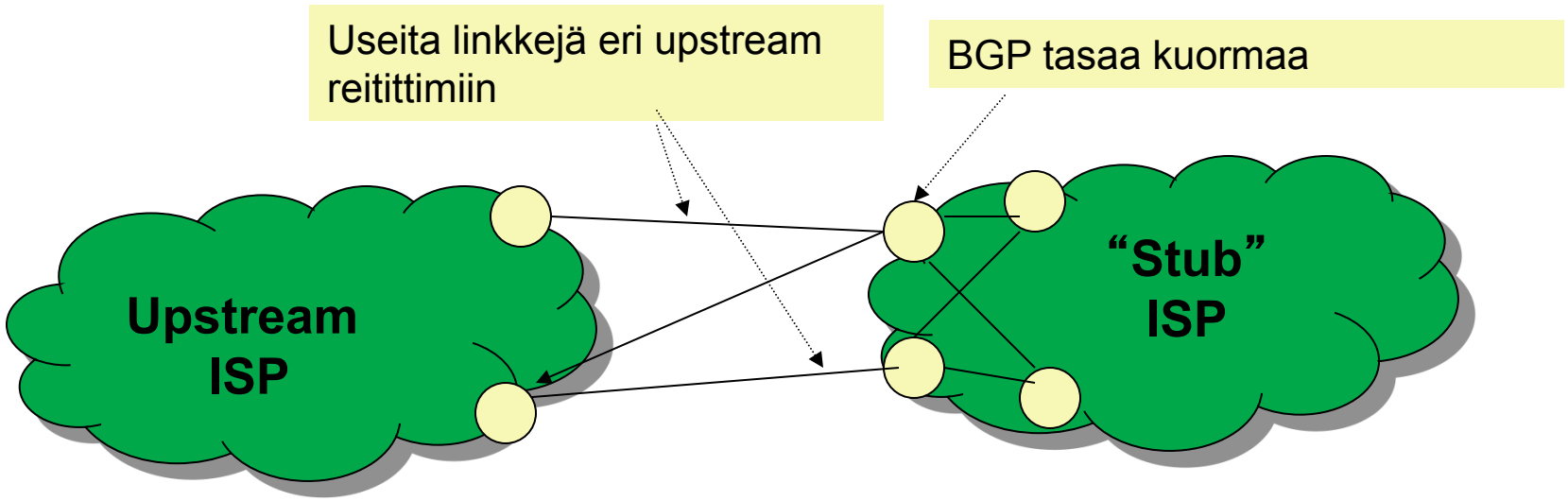
- **Stub AS:** ei transit palvelua
  - Ei tarvitse käyttää BGP:aa ollenkaan
  - Staattinen oletusreitti ulos
- **Multi-homed stub AS:** useampi yhteyspiste yhteen tai useampaan upstream palveluntarjoajaan
  - BGP tarvitaan
  - Hyvä olla julkinen AS numero
  - Ei tarvitse omaa IP prefix allokaatiota (käyttää osaa transitin allokaatiosta)
- **Multi-homed transit AS:** yhteys useampaan AS:iin *ja* transit-palvelu
  - BGP tarvitaan
  - Julkinen AS numero tarvitaan
  - Allokoitu IP prefix tarvitaan

Stub AS: Yksi yhteyspiste



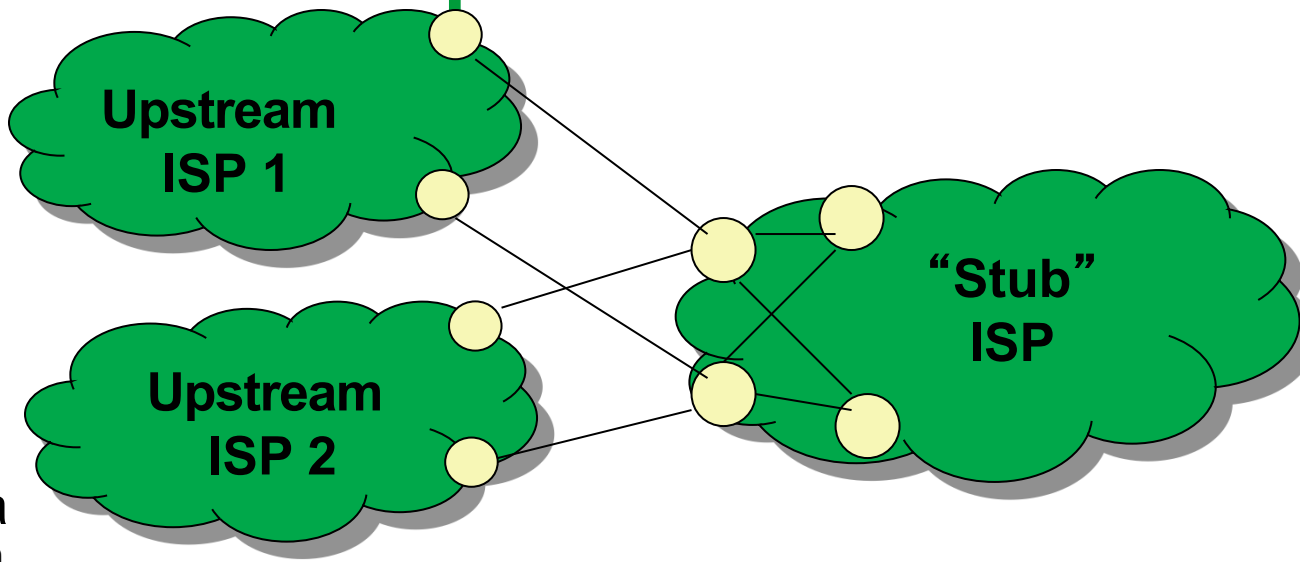
- Staattinen oletusreitti reunareitittimen kautta
- Upstream ISP mainostaa saavutettavuutta
- Ei tarvita BGP:aa

Multihomed Stub: Monta yhteyspistettä



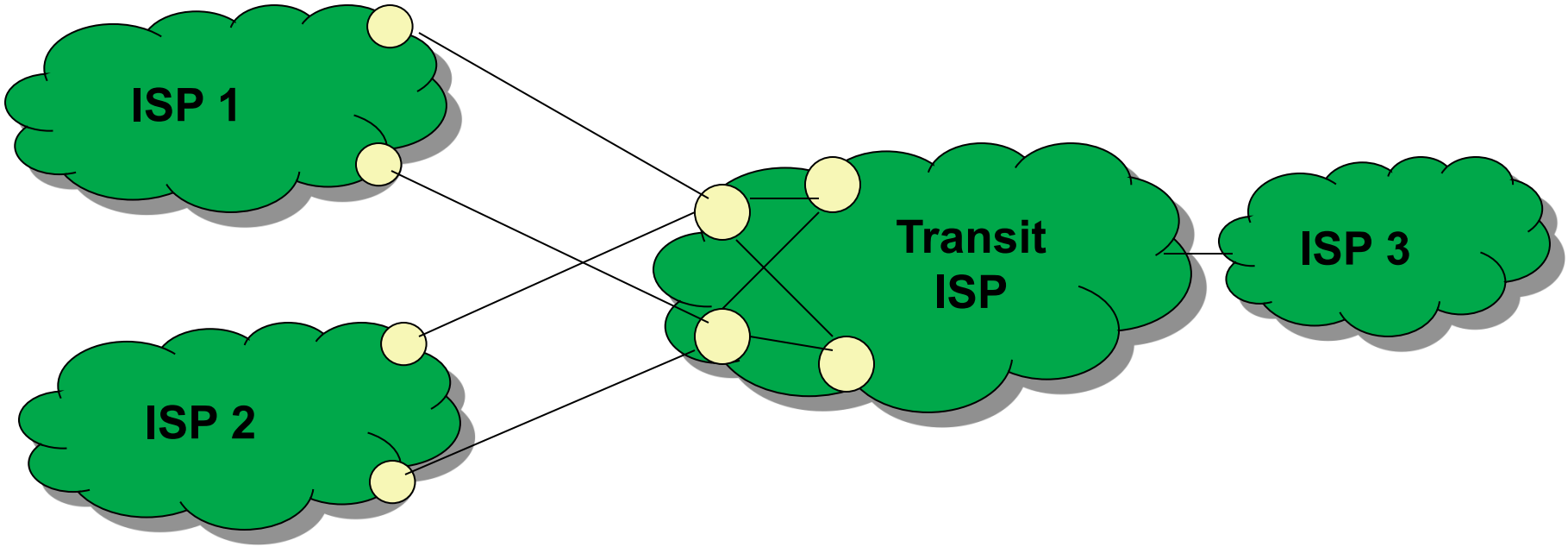
- BGP:lla voidaan tasata kuormaa
- Voidaan käyttää ei-julkista AS numeroa
  - Upstream ISP mainostaa saavutettavuutta omalla numerollaan

Multihomed Stub: Multiple ISPs



- Monta tapaa toteuttaa
  - Kuorman tasaaminen
  - Primary-backup
- BGP tarvitaan toteutukseen
  - Mainostetaan prefixiä niin että saadaan aikaan toivottu palvelu
- Stubilla olisi hyvä olla julkinen AS numero
  - Muuten BGP mainokset voivat olla inkonsistentteja, kun molemmat ISPt mainostavat Stubin prefiksiä omalla numerollaan
- Voidaan käyttää Provider-aggregatable (PA) –osoitteita
  - Eli osa joko ISP1:n tai ISP2:n osoiteavaruutta

Multihomed Transit Network



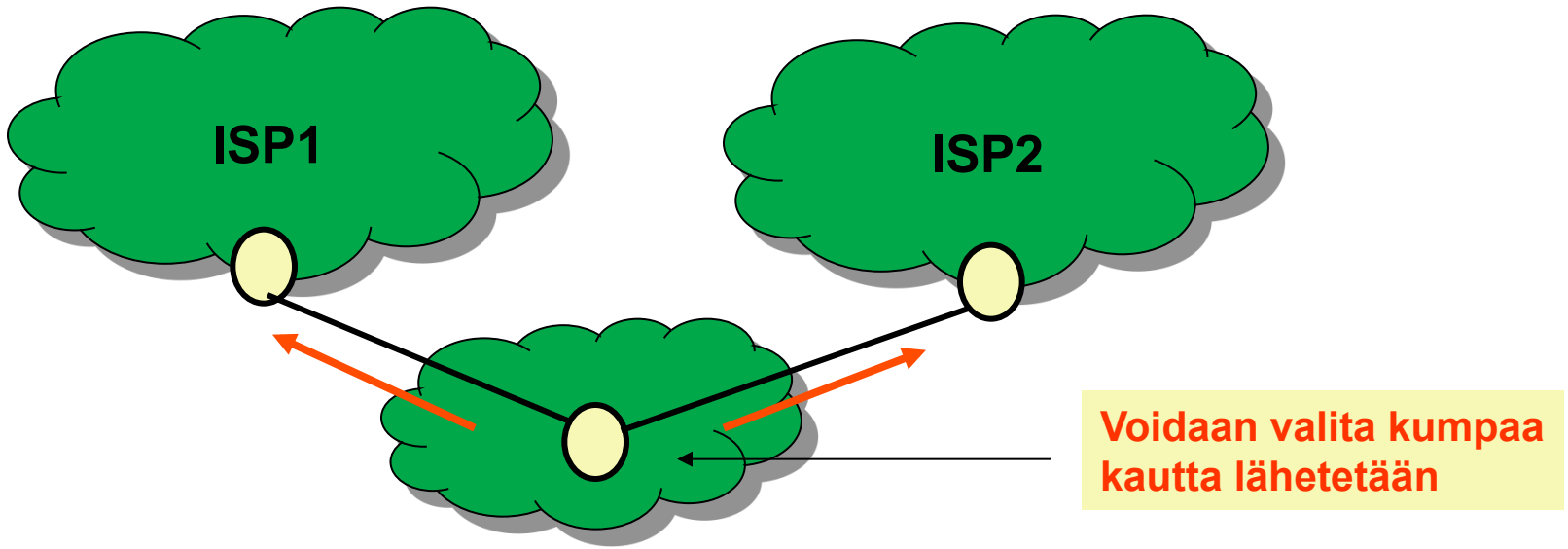
- BGP täysin käytössä
- Pitää olla julkinen AS numero
- Pitää olla oma allokoitu osoiteavaruus

IPv4-multihoming: Miten saavutetaan haluttu palvelutaso?

- Halutaan toteuttaa tietynlainen multihoming-palvelu, esim.
  - Kuormantasaus
  - Redundanssius (primary/backup)
- Kaksi päätehtävää?
  - Ulosmenevän liikenteen kontrollointi
  - Sisääntulevan liikenteen kontrollointi

Ulosmenevän liikenteen kontrollointi

- Helpompaa kuin sisääntulevan liikenteen kontrollointi
  - Lähettäjä voi valita mitä kautta paketit lähetetään
- Mahdollistaa kontrollin vain yhden AS-hypyn verran
  - Ei voida valita koko AS-polkua



Ulosmenevä liikenne: kuormantasaus

- Kontrolloidaan liikennettä *per prefix*
  - Päätetään mitkä kohdeprefiksit lähetetään mitäkin kautta
  - Voidaan dynaamisesti muuttaa preferenssejä
- Tehokkaaseen kuormantasaukseen tarvitaan tilastotietoja
  - Verkkopolkujen suorituskyky
  - Ulosmenevät liikennemäärät per prefiksi
- Tarvitaan myös menetelmä jolla liikennemäärät kuvataan prefikseiksi jotka assosioidaan eri ulosmenolinkkeihin

Sisääntulevan liikenteen kontrollointi

- Hankalaa koska ei voida kontrolloida naapurien päätöksiä
- Yleisiä menetelmiä
  - AS path prepending
    - Keinotekoisesti pidennetään joitain AS-polkuja lisäämällä oma numero monta kertaa
    - BGP suosii lyhyempiä polkuja
  - Communities and local preference
    - BGP:n attribuutteja joita voidaan hyödyntää tiettyjen reittien suosimiseen
  - Prefiksien säätäminen
    - Mainostetaan osia prefiksistä eri kautta
    - Säädetään pituutta: BGP suosii pidempiä prefiksejä (spesifisempiä)

IPv4 Multihoming: ongelmia

- Reititystaulujen koko
  - Provider-independent (PI) -osoitteiden käyttö
    - Jokaisen upstream palveluntarjoajan taulut kasvaa
  - Provider-aggregatable (PA) -osoitteiden käyttö
    - Vain yksi upstream palveluntarjoaja voi aggregoida
- Tulevan liikenteen tarkka kontrollointi vaikeaa
  - PA-osoitteet
    - BGP priorisoi spesifisempää prefiksiä -> liikenne ei jakaudu tasaisesti

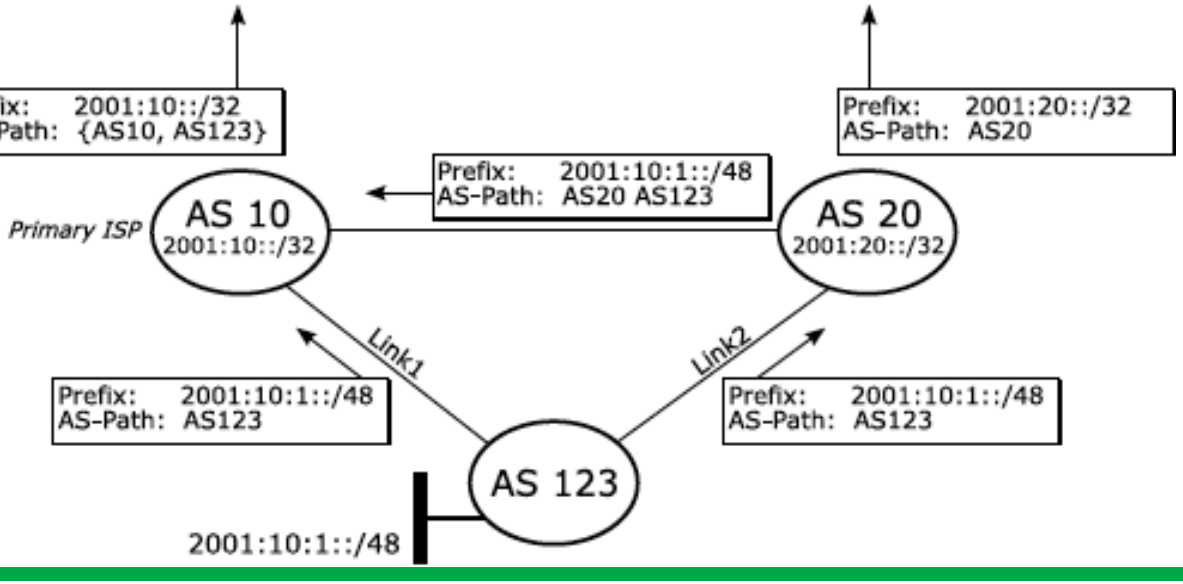
IPv6-multihoming

- “Helppo” ratkaisu: IPv6 provider independent addresses
  - Toimii kuten IPv4 multihoming
  - Operaattorin vaihtaminen ei muuta osoitetta
  - Erityinen osoiteavaruuden osa: 2001:678::/29
  - Kuljetuskerroksen yhteydet säilyvät (Transp. layer surv.)
  - Ongelmana on edelleen reititystaulujen skaalautuvuus
    - Operaattorit eivät voi aggregoida PI osoitteita
- Tarve toteuttaa multihoming paremmin kuin IPv4
  - Reititystaulujen koko pitää pysyä järkevänä (aggregointi)
  - ”Transport layer survivability”
- Useita eri tyyppisiä parempia ratkaisuja
  - Reitityspohjaiset ratkaisut
  - Middlebox-ratkaisut
  - Päätelaitteessa toteutettavat ratkaisut

IPv6-multihoming: reitityspohjaiset ratkaisut

- Palveluntarjoajat voivat tehdä yhteistyötä
  - Toimii yhtä hyvin IPv4:lla
  - ☺ AS20 ei tarvitse mainostaa AS123:a
  - ☺ Toimii vaikka linkki 1 tai 2 menee poikki
  - ☹ AS10 on “single point of failure”

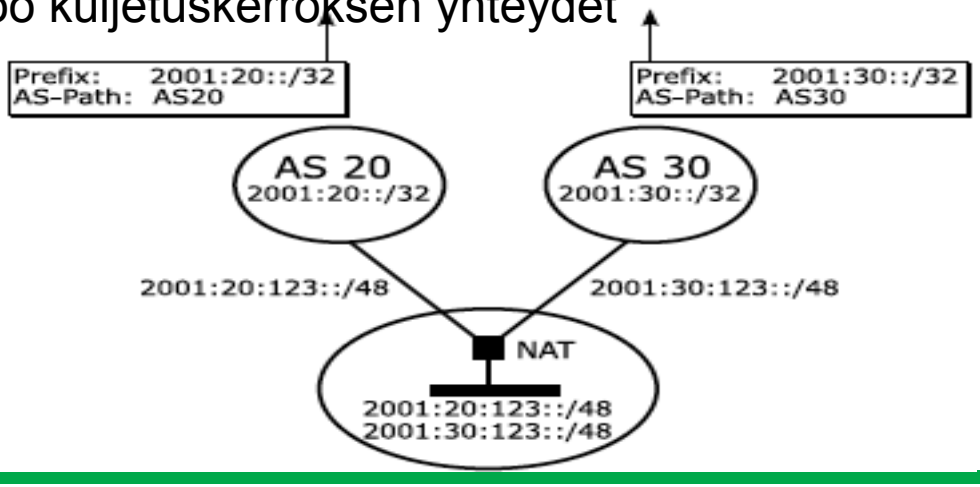
Huono puoli?



IPv6-multihoming: Middlebox-ratkaisut

- Multihoming NAT:n avulla
  - NAT tiedostaa kumpi linkki/ISP toimii ja vaihtaa osoitteen lennosta jos tarpeen
  - Päätelaitteet voi käyttää osoitteita mistä tahansa prefikseistä
  - Soveltuu pienehköille esim. kotiverkoille
  - ☺ Helppo toteuttaa, ei tarvita BGP:aa
  - ☹ NAT on “single point of failure”
  - ☹ Rikkoo kuljetuskerroksen yhteydet

Huono puoli?



IPv6-multihoming: päätelaiteratkaisut

- Monia eri ratkaisuja tässä luokassa
  - Kuljetuskerroksen protokollat (SCTP, DCCP, TCP-MH)
    - Harmina on ettei voida käyttää vanhoja protokollia ja sovelluksia
  - Verkkokerroksen protokollat (SHIM6, HIP)
    - IETF suosii tätä ratkaisumallia
- Yhteisiä piirteitä
  - Useampi eri IPv6 osoite per päätelaite
    - Prefiks per palveluntarjoaja
  - Lähettäjän osoite määrittää upstream palveluntarjoajan
    - Käytetään sen palvelua jolta on osoite
    - Aggregoinnin vuoksi
  - Päätelaitteen tulee havaita vika ja tehdä päätös palveluntarjoajan vaihtamisesta toiseen
    - Eli vaihtaa osoitetta
  - Ei saisi näkyä sovellukselle -> kuljetuskerroksen yhteys säilyy

Shim6: Site Multihoming by IPv6 Intermediation

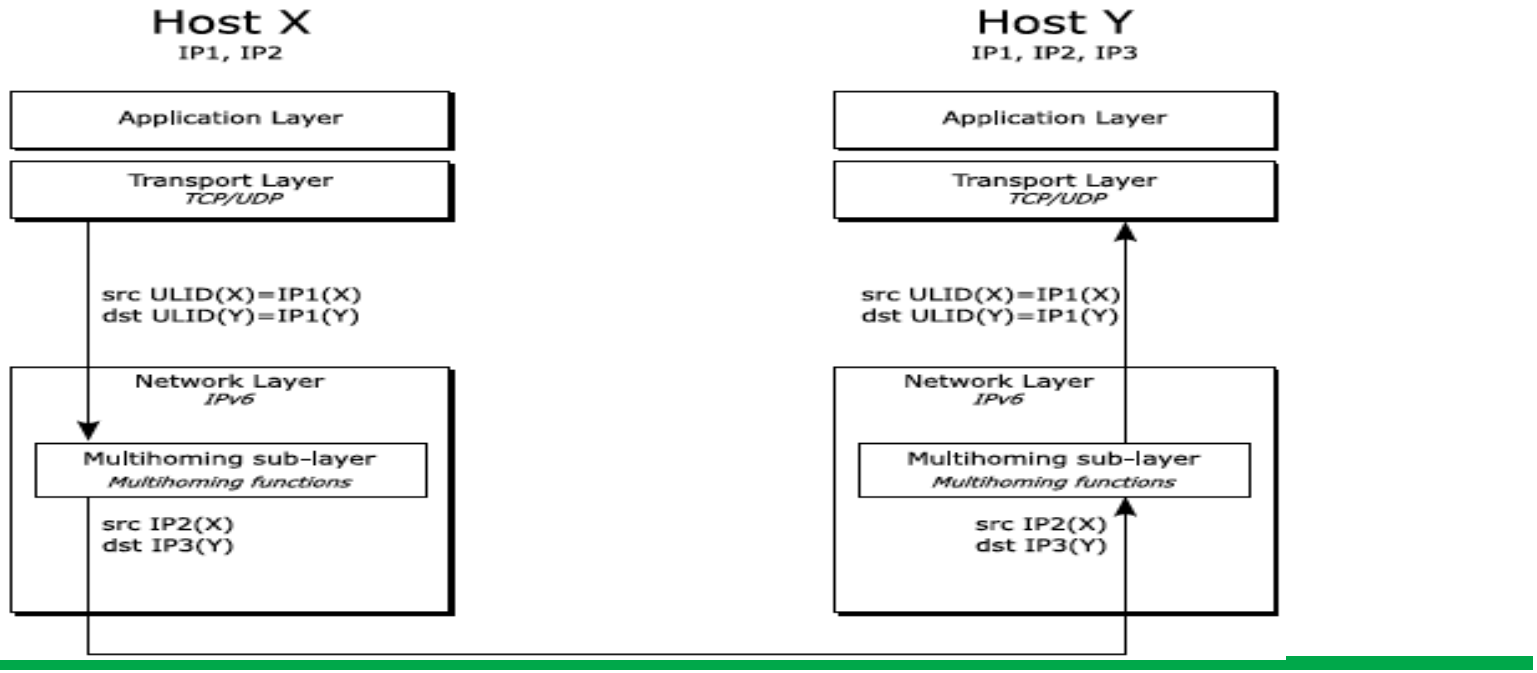
- RFC 5533
- “3.5” kerroksen protokolla
  - Verkkokerroksella IP-reititysalikerroksen ja IP endpoint-alikerroksen välissä
- Ei katkaise käynnissäolevia kuljetuskerroksen yhteyksiä
- Uusi lisäotsake IPv6een (next header = 140)
- Shim6-yhteys neuvotellaan
  - Kun kuljetuskerroksen (TCP-)yhteys on ollut hetken käytössä (esim 50 pakettia lähetetty)
  - Kerrotaan vaihtoehtoiset IP-osoitteet
  - Jos vastaanottaja ei reagoi -> se ei tue protokollaa
  - Jos ei ongelmia ei esiinny, liikenne jatkuu normaalisti

Shim6: kun yhteys 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
  - Alkuperäinen IP-osoite -> upper-layer identifier (ULID)

Shim6: osoitteista

- “Locator – identifier split”
  - Ylemmät kerrokset käyttävät alkuperäistä osoitetta joka ei vaihdu (ULID)
  - Shim-kerros käyttää senhetkistä toimivaa osoitetta
  - Kuljetuskerros ei huomaa osoitteenvaihdosta



Shim6: protokollan ominaisuuksia

- Useita erilaisia viestejä
  - Update-viestillä päivitetään osoitelista
  - Keepalive-viesti pitää auki oikeastaan yksisuuntaisia yhteyksiä myös toiseen suuntaan
  - Probe-viestiä käytetään, kun yhteydellä toimii eri osoitteet eri suuntiin
  - Virheviesti kertomaan ongelmatilanteista
- Myös tietoturvaominaisuuksia
  - Hash Based Addresses (HBA): toinen osapuoli voi varmistaa että uusi osoite tulee oikealta osapuolelta
    - Redirection-hyökkäystä vastaan

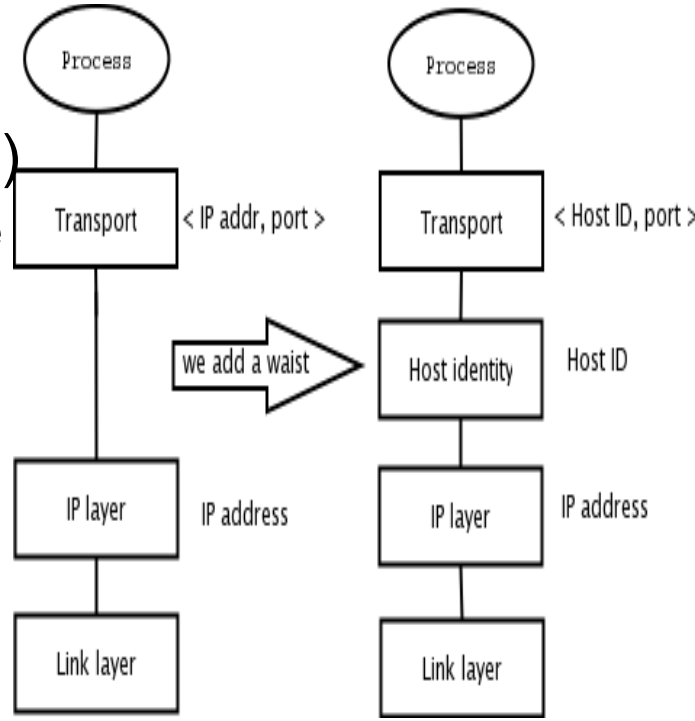
Shim6: Yhteenveto

- 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
- Edut ☺
  - Ei vaadi verkolta lisälaitteita tai toiminnallisuuksia
  - Ei vaadi muutoksia kuljetuskerrokseen (TCP) tai sovelluksiin
    - Vanha osoite pysyy tunnisteena, uusi osoite on vain paikka
- Huonot puolet ☹
  - Shim6 vaatii muutoksia kummankin osapuolen IP-pakettien lähetykseen -> deployment ongelma

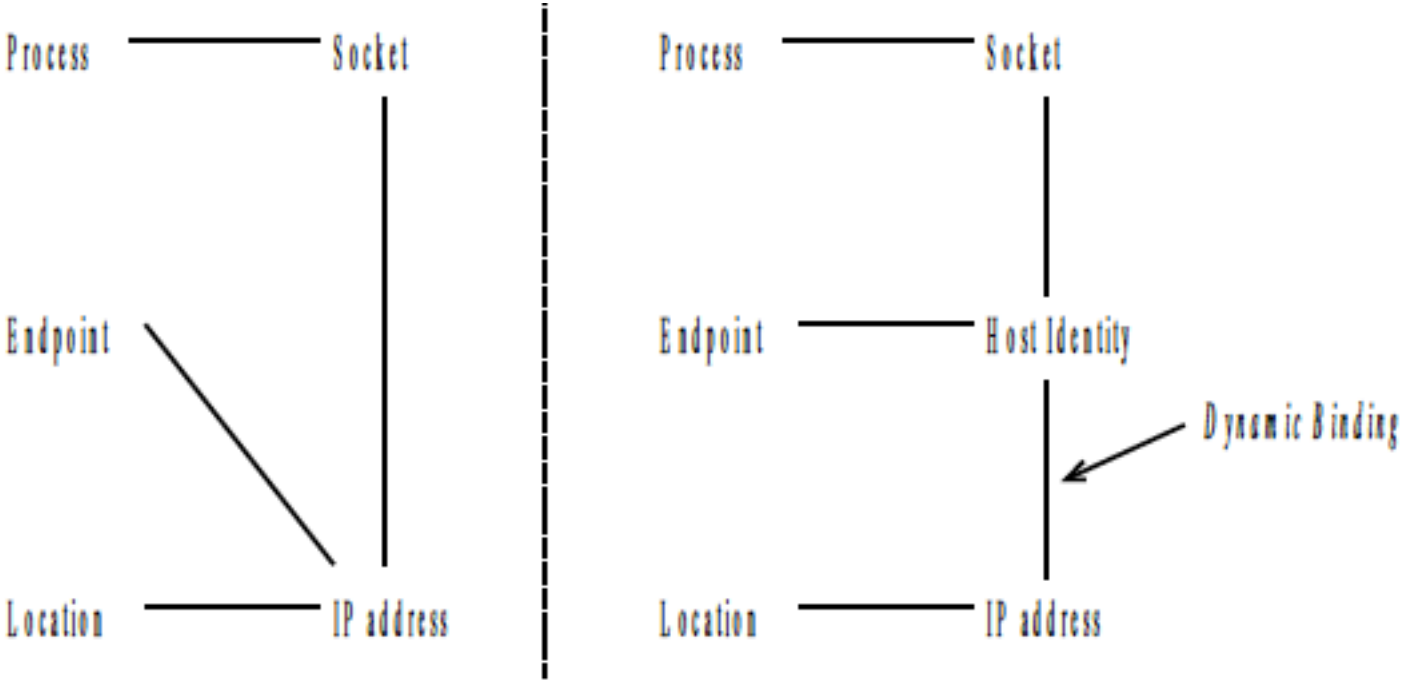
Toinen protokolla/ arkkitehtuuri-ratkaisu: HIP

HIP (RFC 4423 et co)
Host Identity Protocol

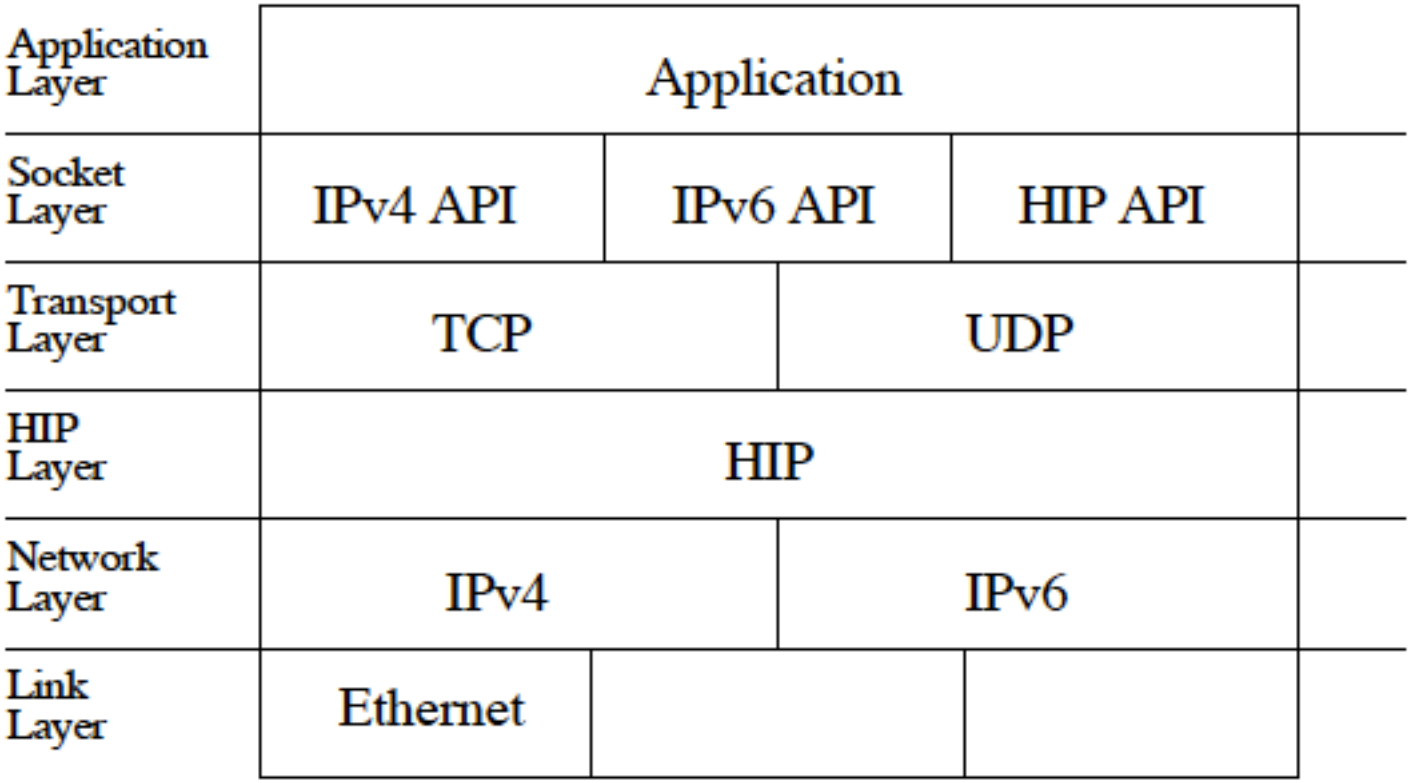
- Kerros IP- ja kuljetuskerrosten väliin
- IP-osoitetta on pelkkä osoite (locator)
- Tunniste (identifier) nyt Host Identity (HI)
  - ylemmän kerroksen protokollissa IP-osoite korvataan HI:llä, eli TCP-yhteyden päätepisteenä <HI, portti>-pari
- HI on julkinen avain
  - siitä lasketaan 128-bittinen tiiviste, jota kutsutaan HIT:ksi
  - kone voi generoida itse avaimen, tai
  - avain voi olla jonkin varmennepalvelun (CA) sertifioima



HIP vs. non-HIP



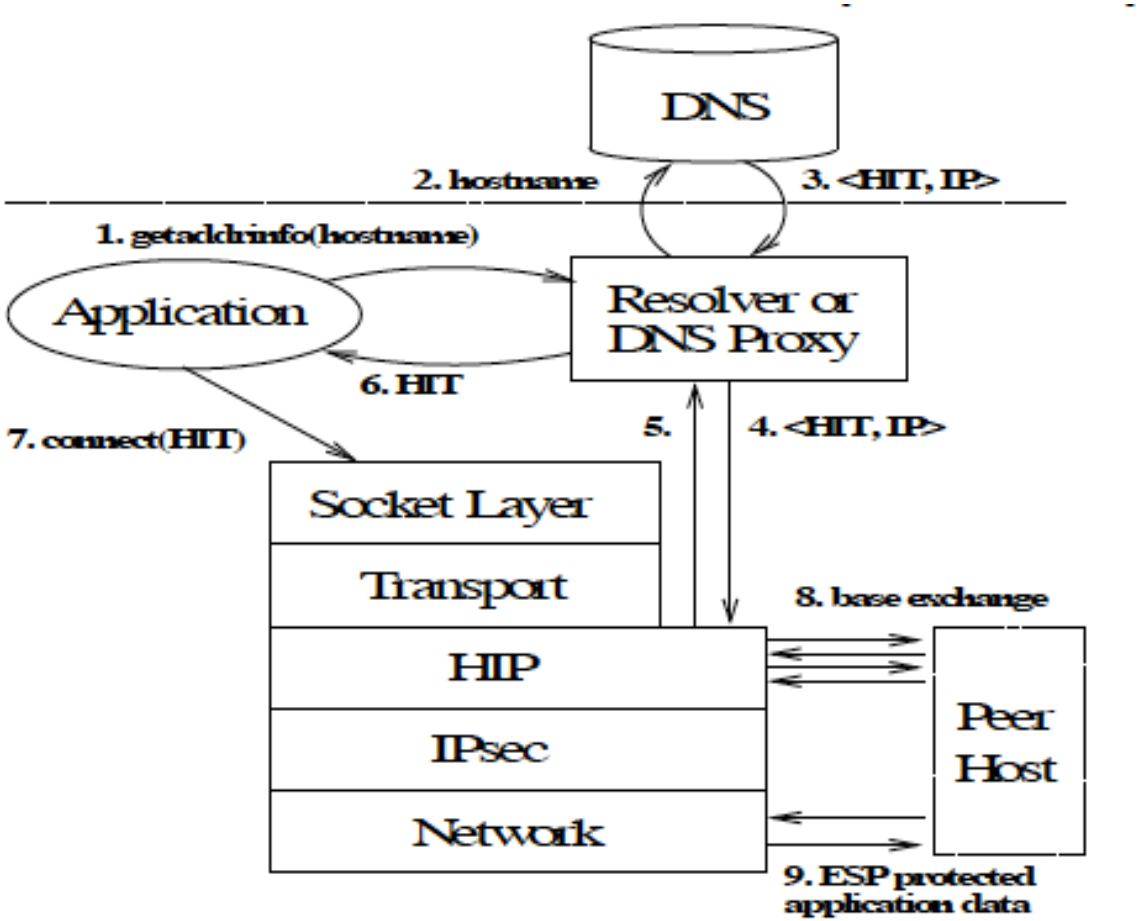
API:t


Application Layer
Application
Socket Layer
IPv4 API
IPv6 API
HIP API
Transport Layer
TCP
UDP
HIP Layer
HIP
Network Layer
IPv4
IPv6
Link Layer
Ethernet

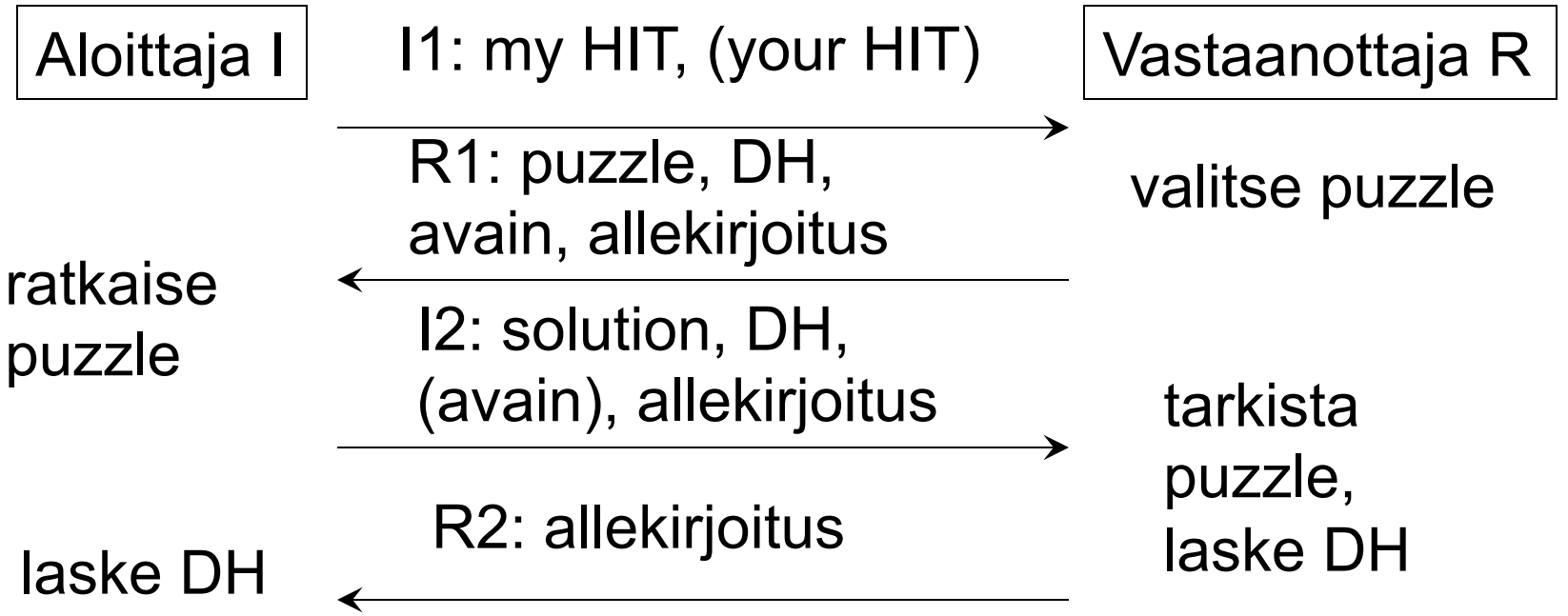
HI-tunnisteiden käsittely

- IP-osoite voi vaihtua, kun ylemmän kerroksen protokolla käyttää tunnisteena HI:ä
  - olemassaolevat yhteydet säilyvät (multihoming)
  - jopa allaolevan IP:n versio voi vaihtua, tarvitaan vain mekanismi sitoa osoite HI:iin
- HI-tunnisteet tallennetaan DNS:een (tai DHT:een)
  - hajautettu tiivistetaulu DHT (Digital Hash Table) on tapa tallettaa tieto hajautetusti useammalle palvelimelle, joista jokaisella osittainen tieto ja tapa ohjata kyselijä eteenpäin

HIP toimintakaavio



HIP base exchange



- Aloitusviesti voi kulkea rendezvous-palvelimen kautta
- Puzzle: DoS-hyökkäysten torjumiseksi
- 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, turvallisuus ja NAT-traversal yhdessä paketissa
  - uusi tunniste HI, IP-osoite ilmaisee vain sijainnin
  - uusi kerros IP:n ja kuljetuskerroksen väliin
- Tarvitsee kohtuu paljon muutoksia
  - koneiden TCP/IP-pinot (käyttöjärjestelmän ydin)
  - DNS, NAT, jne

Multihoming: Yhteenveto

- Useampi eri yhteys verkkoon tuo luotettavuutta saavutettavuudelle
- Aiheuttaa ongelmia olemassaoleville protokollille
  - osoitteiden vaihtumisen vuoksi
- Ratkaisumalleja löytyy erilaisia
  - Reitityspohjaiset ratkaisut (BGP+aggregointi)
  - Middlebox-ratkaisut (NAT)
  - Päätelaitteessa toteutettavat ratkaisut
    - Kuljetuskerroksen protokollat (SCTP, TCP-MH)
    - Verkkokerroksen ratkaisut (Shim6, HIP)

Multihoming: Lähteet

- RFC 4116 IPv4 multihoming practices and limitations, 2005
- C. de~Launois and M. Bagnulo. The Paths towards IPv6 Multihoming. IEEE Communications Surveys and Tutorials. 2006.
- RFC 3582 Goals for IPv6 site-multihoming architectures, 2003
- RFC 3178 IPv6 multihoming support at site exit routers, 2001
- RFC 5533 Shim6: Level 3 Multihoming Shim Protocol for IPv6, 2009
- RFC 4423 - Host Identity Protocol (HIP) Architecture, 2006
- RFC 5201 - Host Identity Protocol, 2008
- RFC 5206 - End-Host Mobility and Multihoming with the Host Identity Protocol, 2008

Seuraavaksi liikkuvuus (mobility)

Liikkuvuudenhallinta

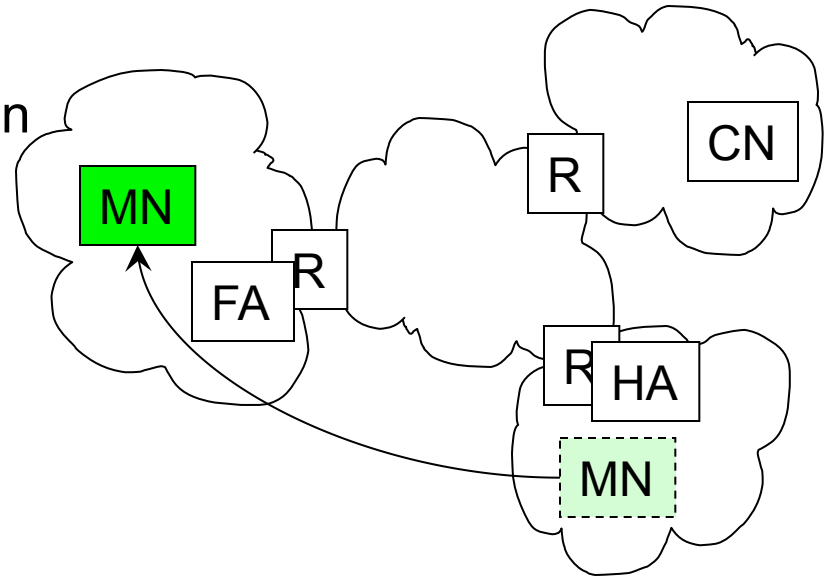
- Liikkuvuudenhallinnan tavoitteena on säilyttää yhteys verkkoon siten, että sovellusten yhteydet eivät katkea, vaikka verkkoyhteyden päätepiste muuttuu
  - yksi yhteys kerrallaan (ei varayhteyttä, kuten edellä)

Kahdenlaista liikkuvuutta:

- Makromobility: liikutaan verkosta toiseen, mutta uudessa verkossa pysytään kauemmin
  - Mobile IP on ratkaisu tähän
- Mikromobility: paljon nopeita siirtymiä verkosta toiseen lyhyellä aikavälillä
  - Tähän on muita ratkaisuja (esim. Hierarchical Mobile IP), joita ei tässä käsitellä

Mobile IP

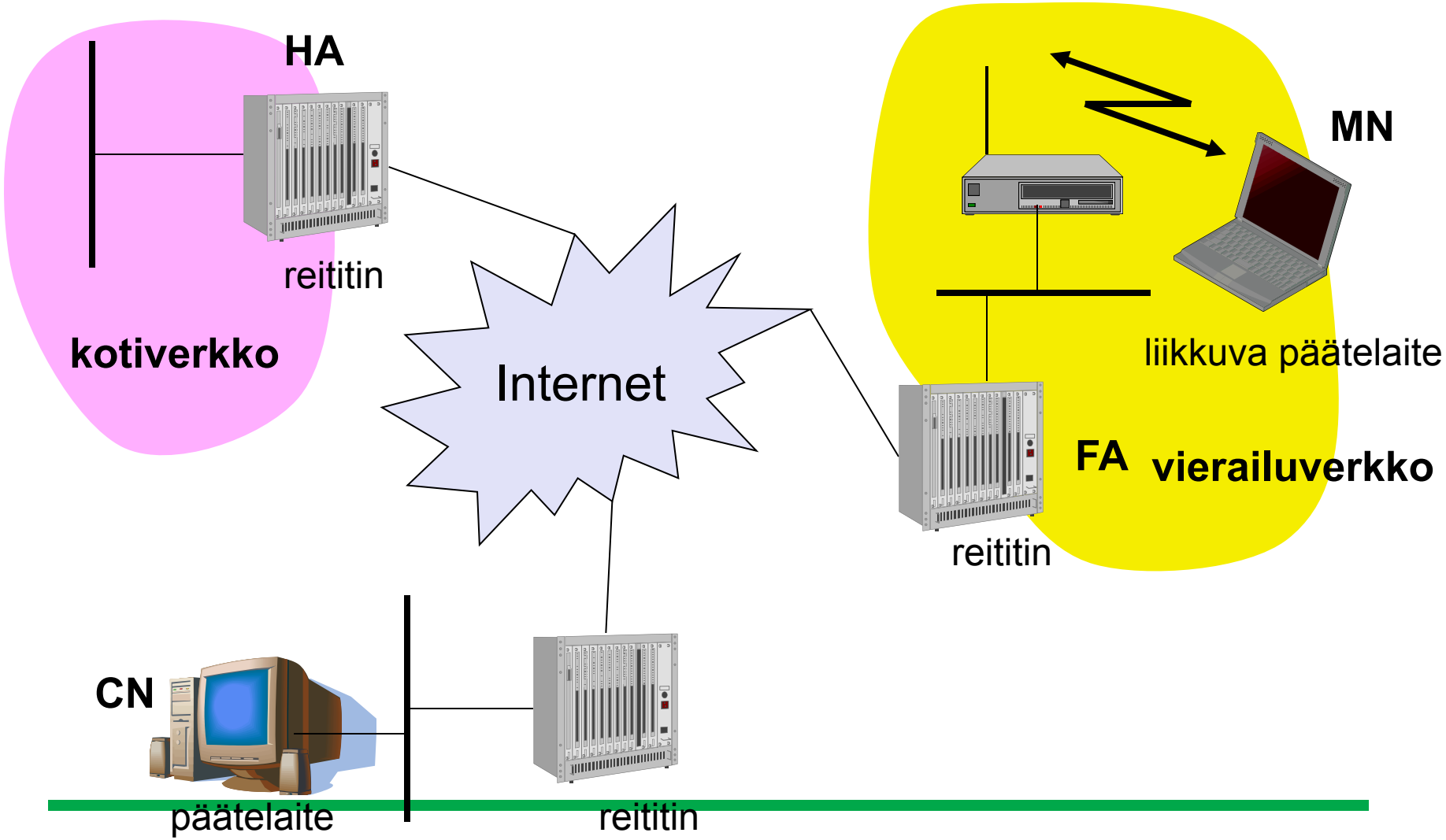
- Jokaisella koneella on kotiverkko ja siellä IP-osoite
- Kone voi kuitenkin liikkua toiseen verkkoon siten, että
  - se on edelleen tavoitettavissa kotiosoitteensa kautta
  - yhteydet säilyvät
- Liikenne tunneloidaan koneen senhetkiseen osoitteeseen
- Kaksi versiota: Mobile IPv4 ja Mobile IPv6



Mobile IP: hieman terminologiaa

- Mobile Node (MN)
  - Päätelaite joka liikkuu ja vaihtaa yhteyspistettä verkkoon vaihtamatta IP osoitettaan
- Home Agent (HA)
  - Laite MN:n kotiverkossa, yleensä reititin, joka pitää kirjaa MN:n sijainnista ja tunneloi IP paketteja MN:n kyseiseen osoitteeseen
- Foreign Agent (FA)
  - Laite verkossa jossa MN tällä hetkellä vierailee, yleensä myös reititin, joka välittää tunneloidut paketit MN:lle
- Correspondent Node (CN)
  - Päätelaite jonka kanssa viestitään

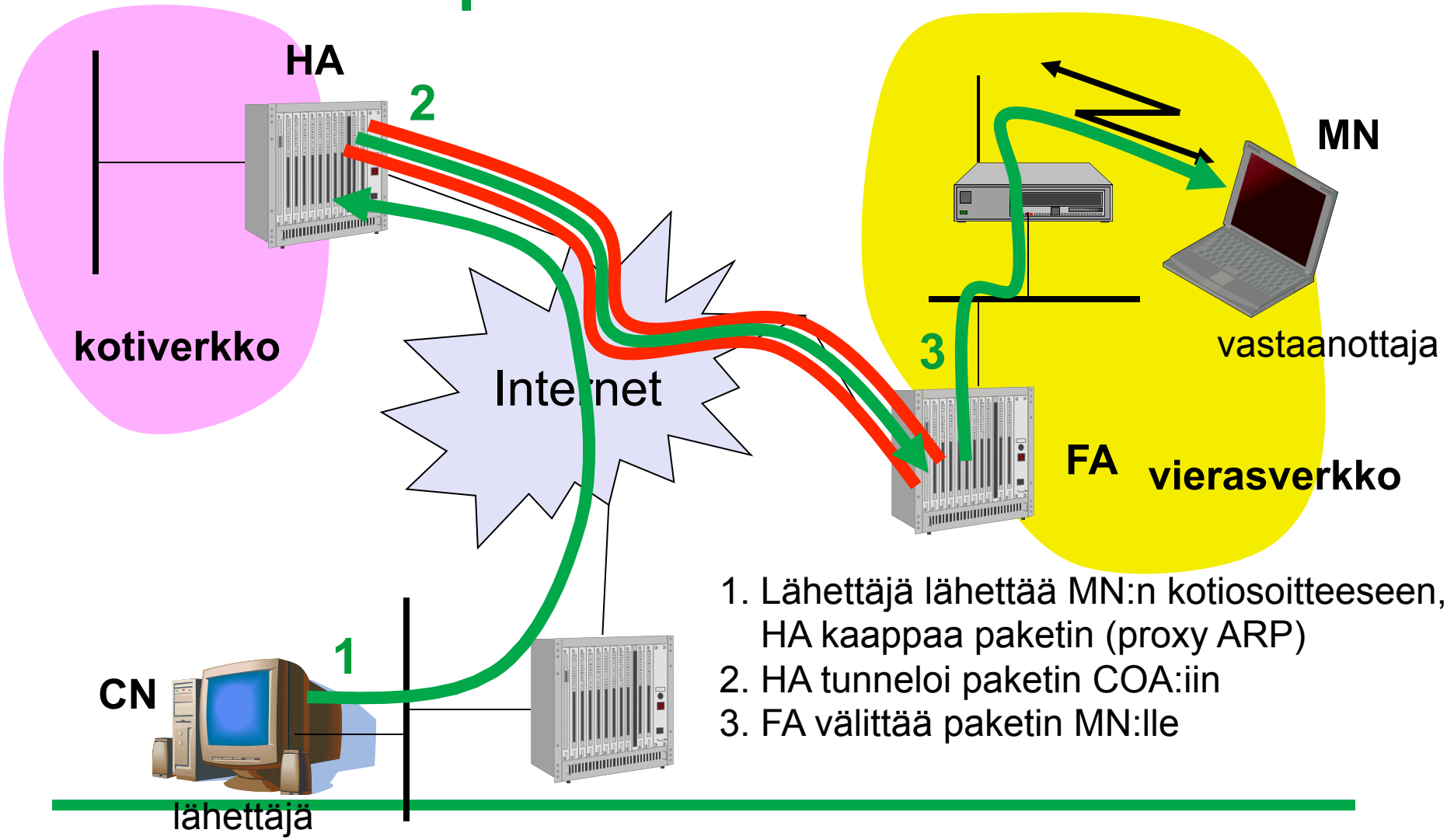
Esimerkki


HA
reititin
kotiverkko
Internet
MN
liikkuva päätelaite
FA
vierailuverkko
reititin
CN
päätelaite
reititin

Mobile IP: osoitteet

- Kotiosoite (home address)
  - Pysyvä osoite, josta liikkuvan koneen (MN) tavoittaa aina
  - Kotiverkossa MN käyttää osoitettaan kuten tavallinen liikkumaton päätelaite
  - Vieraassa verkossa kotiagentti (home agent, HA) vastaanottaa viestin ja lähettää sen edelleen (tunneloi) MN:n nykyiseen sijaintiin
- Vierailuosoite (care-of address eli COA) on *joko*
  - Foreign Agentin (FA) osoite
    - FA toimittaa MN:lle paketit jotka HA on edelleenlähettänyt
  - *Tai* väliaikainen vieraasta verkosta saatu osoite
    - Esim. DHCP:n avulla normaalisti
    - HA tunneloi paketit suoraan tähän osoitteeseen
    - Tässä ei vieraalta verkolta tarvita erityistä tukea

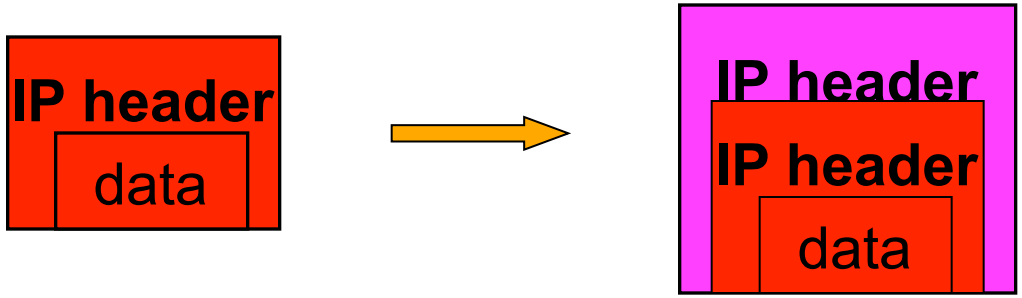
Mobile IPv4: pakettien vastaanotto



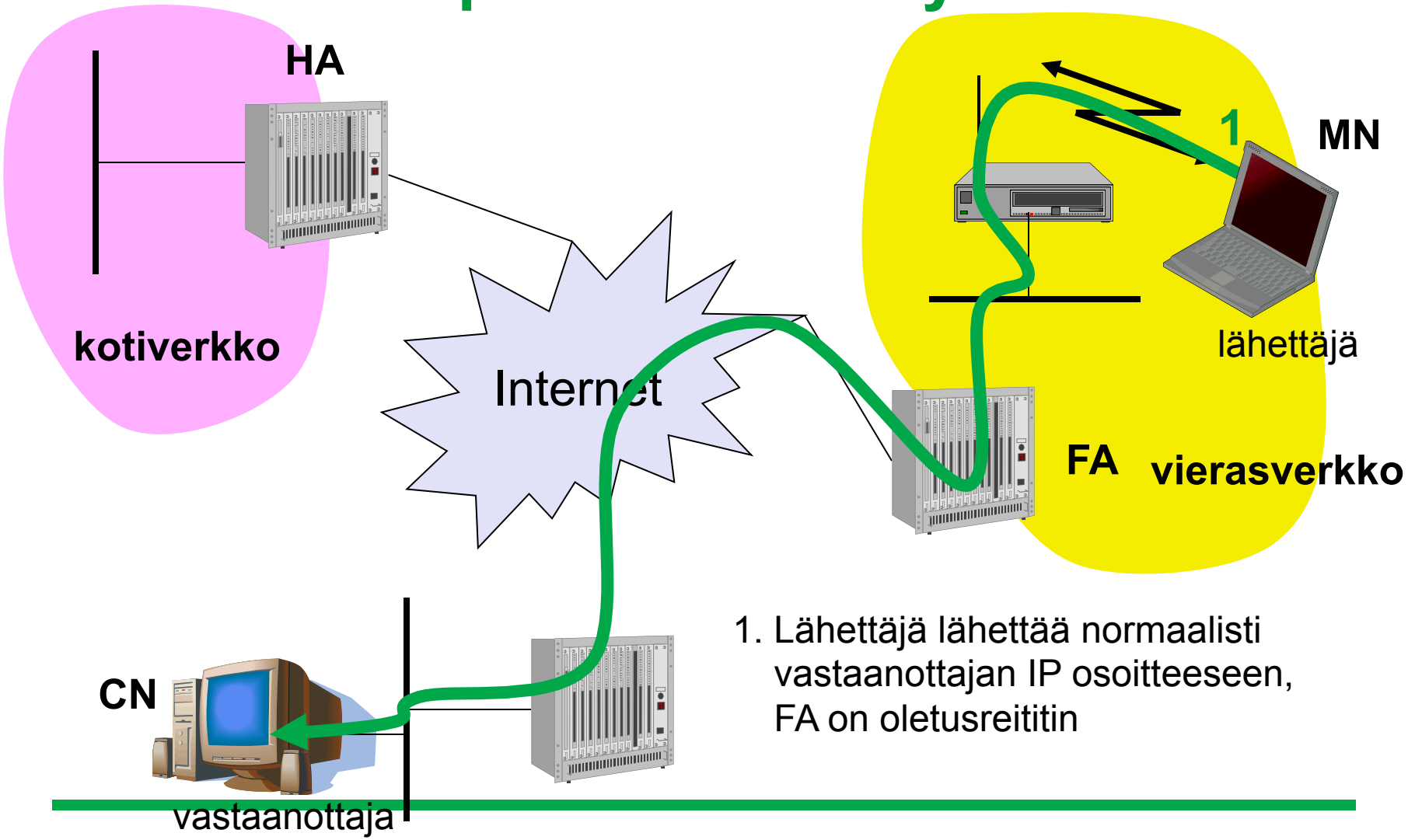
1. Lähettäjä lähettää MN:n kotiosoitteeseen, HA kaappaa paketin (proxy ARP)
2. HA tunneloi paketin COA:iin
3. FA välittää paketin MN:lle

Mobile IP: IP-in-IP Tunnelointi

- Edelleenlähetettävä IP-paketti kapseloidaan uuden IP-paketin sisään
- Uuden paketin otsake:
  - Vastaanottajan osoite = care-of-address
  - Lähettäjän osoite = HA:n osoite
  - Protokollanumero = IP-in-IP



Mobile IPv4: pakettien lähetys



1. Lähettäjä lähettää normaalisti vastaanottajan IP osoitteeseen, FA on oletusreititin

Mobile IPv4: lähetys ja vastaanotto

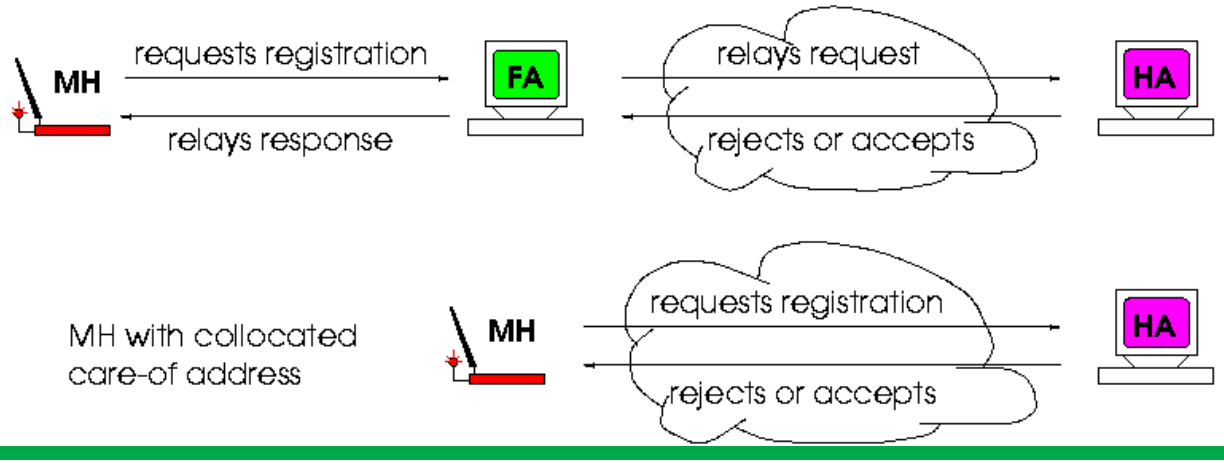
- Äskeisessä esimerkissä MN lähetettää paketin suoraan
  - Lähettäjän osoitteena kotiosoite
- Vaihtoehto: Paketti tunneloidaan vierasagentilta kotiagentille, joka lähettää sen edelleen vastaaanottajalle
  - Syy on Ingress filtering: vierailuverkko hylkää paketin koska se ei tule oman verkon osoitteesta
    - Vaikeuttaa IP osoitteen väärentämistä
- Vastaanottajan (correspondent node, CN) ei tarvitse tietää mitään Mobile IP:stä
  - paluuviestit kiertävät aina kotiagentin kautta
- Mikä ongelma Mobile IPv4:ssa on?
  - Kolmioreititys: erittäin tehotonta -> reitin optimointi

Mobile IPv4: Miten MH tietää vaihtaneensa verkkoa?

- HA:t ja FA:t lähettävät säännöllisesti mainoksia (agent advertisements)
  - Linkkikerroksen broadcast viestejä
  - Sisältää: care-of address, encapsulation type ja lifetime
  - Mainostamisessa käytetään ICMP:n laajennusta
    - Mobile Agent Advertisement Extension
- MH:t kuuntelevat mainoksia
- Oletetaan että ollaan uudessa verkossa
  - jos saadaan mainos uudesta aliverkosta
    - Tässä tapauksessa mainoksessa pitää olla Prefix Lengths Extension
  - jos ei saada mainosta lifetimen indikoiman ajan kuluessa

Mobile IPv4: Uuden sijainnin ilmoitus

- Uusi COA ilmoitetaan kotiagentille
  - joko MN hoitaa rekisteröinnin itse suoraan kotiagentin kanssa (co-located care-of address)
  - tai vierailuagentti hoitaa MN:n puolesta (fa-co-address), jolloin pyyntö lähetään vierailuagentille
- Vierailuosoite on voimassa viestissä ilmoitetun ajan
  - kun kone palaa kotiverkkoon, ajaksi ilmoitetaan nolla
- Rekisteröityessä autentikoidaan



Mobile IPv6: Parannuksia v4-versioon

- Erillistä vierasagenttia ei tarvita lainkaan
  - vierasverkon reititin kertoo osoitteidenhankkimistavan, jota käytetään (kuten tavallisestikin)
- Kevyempi tunnelointimenetelmä
  - Käyttää IPv6:n reitityslisäotsikkoa
- Tuki reitinoptimoinnille
  - ratkaisee kolmireitityksen luoman ongelman
  - Binding Update CN:lle

Mobile IPv6: Binding Update (BU)

- Liikkuva kone lähettää sijainnin päivityksen kotiagentin lisäksi myös CN:lle
  - Kotiagentin kanssa yhteys suojataan IPsec ESP:llä
- Vastaanottaja tarkistaa BU:n todenperäisyyden return routability-prosedurin avulla
  - testipaketit lähetetään samanaikaisesti sekä koti- että vierailuosoitteisiin
  - vastauksessa MN todistaa saaneensa kummatkin ja pystyvänsä viestimään molempia reittejä käyttäen myös takaisin
- Tämän jälkeen CN voi lähettää suoraan paketit MN:n vierailuosoitteeseen
  - Ei tarvitse ”kolmioreitittää”

Mobile IP: yhteenveto

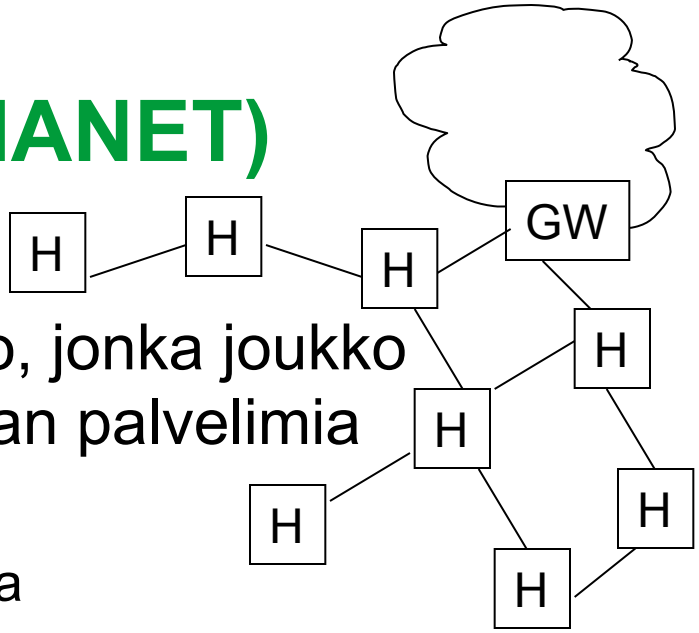
- Kone voi vaihtaa verkkoa ilman, että sovellusten yhteydet katkeavat
- Käytetään koti- ja vierailuosoitteita
- Vaatii ainakin kotiverkkoon kotiagentin (reititin) sekä muutoksia ARP-protokollaan
- HIP toteuttaa myös liikkuvuudenhallinnan

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

Lopuksi 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-protokollan avulla
  - jokin laitteista voi siis tarjota palveluna yhteyttään Internetiin

MANET - Reititys

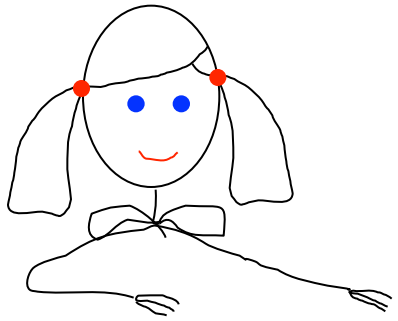
- Jos laitteet eivät ole yhteydessä suoraan toisiinsa, tarvitaan reititystä
- Proaktiivinen (tauluohjattu; proactive, table-driven)
  - laitteet selvittävät verkon yhteydet etukäteen
  - kun yhteyttä tarvitaan, se on nopeasti käytettävissä
  - OLSR, TBRPF ja monta muuta ehdotusta
- Reaktiivinen (tarveohjattu; 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

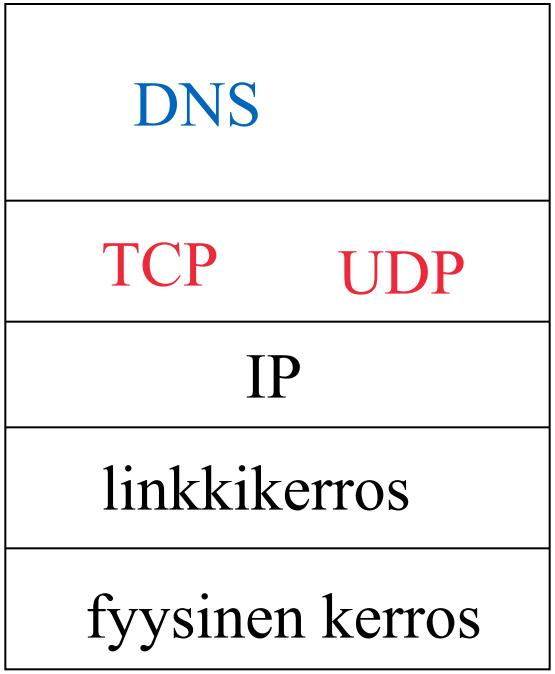
MANET - Lähteet

- 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/

Seuraavat luennot

- Ensi kerralla käsitellään kuljetuskerrosta





Aalto-universitetet
Tekniska högskolan

Aalto-yliopisto
Teknillinen korkeakoulu

Aalto-yliopisto
Teknillinen korkeakoulu

Aalto University
School of Science
and Technology

Aalto-yliopisto
Teknillinen korkeakoulu

Aalto University
School of Science
and Technology

Aalto-universitetet
Tekniska högskolan

Aalto University
School of Science
and Technology