

Host Identity Protocol (HIP)

Esityksen sisältö

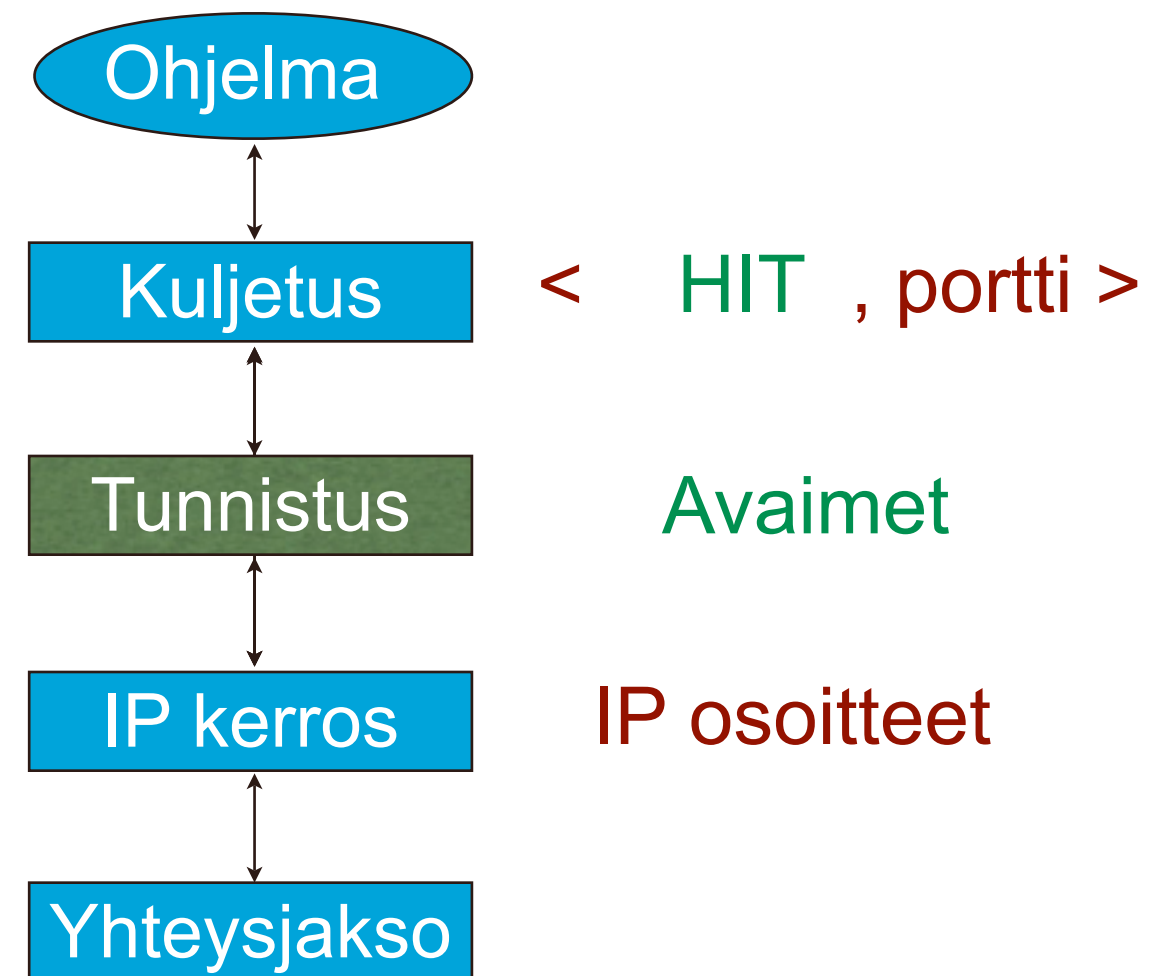
- HIP – Mikä se on?
- Kuinka valmis HIP on?
- Kenelle HIP:istä on hyötyä?
- Yhteenveto

HIP - Mikä se on?

- Ehdotus muuttaa TCP/IP-pinoa
- Työryhmä IETF:ssä
 - Perusprotokolla lähes valmis
- Tutkimusryhmä IRTF:ssä
 - Mitkä olisivat HIP:in vaikutukset?
- Kolme avoimen koodin toteutusta
 - Ericsson Research: FreeBSD (+ Mac OS X)
 - TKK / HIIT: Linux
 - Boeing Phantom Works: Linux / Windows

HIP pähkinäkuoressa

- Uusi “Tunnistus”-kerros TCP/IP:hen
- Laitteet tunnistetaan julkisella avaimella osoitteen asemesta
- Julkinen avain tiivistetään HIT:iksi
 - näyttää osoitteelta
- Tunnistus-kerros tekee muunnoksen



Vaikutusanalogia: Jos yhdistäisimme ihmisiä laitteiden asemesta

Nykyinen IP



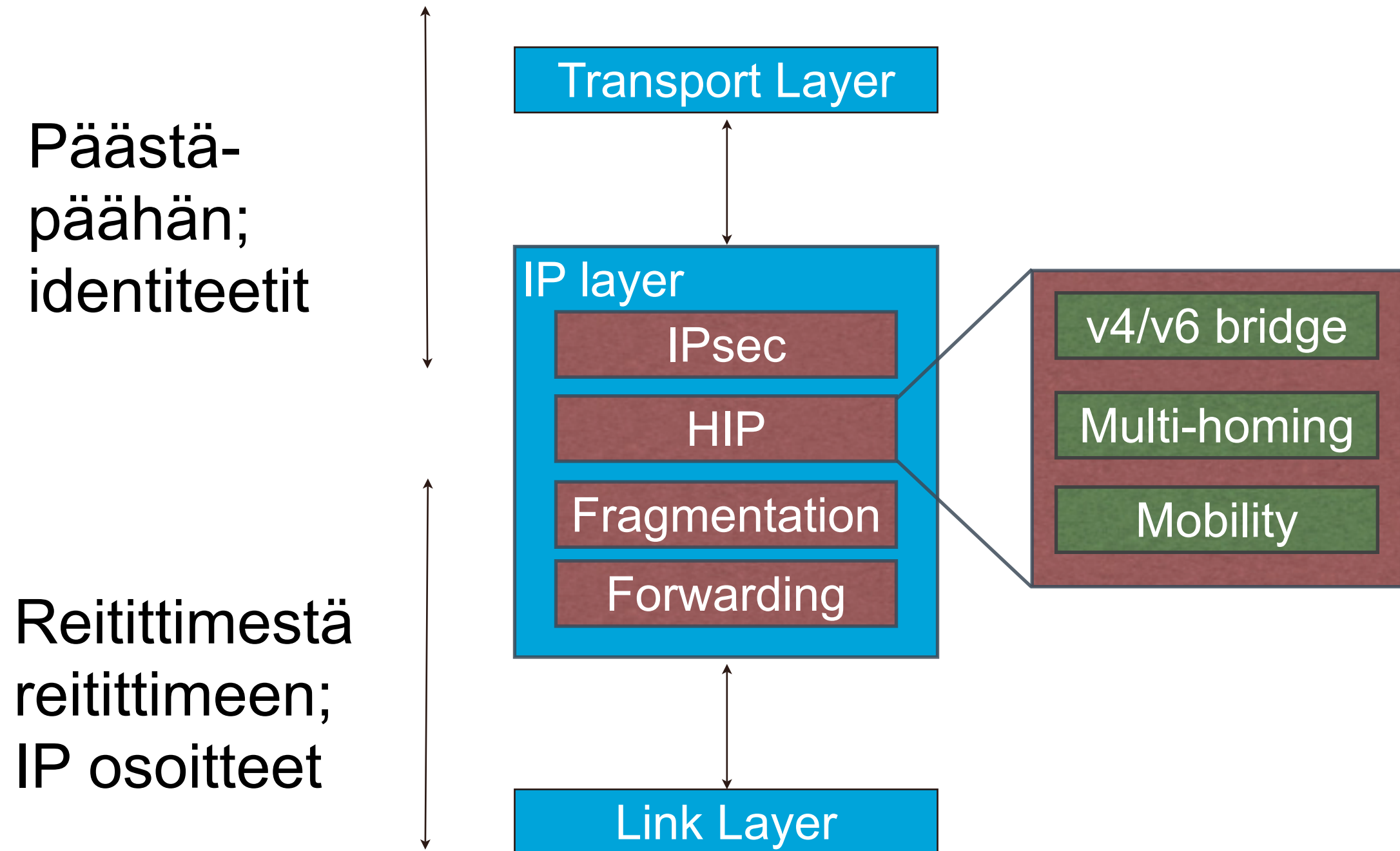
HIP



Julkinen avain \approx Valokuva

Salainen avain \approx Kasvot

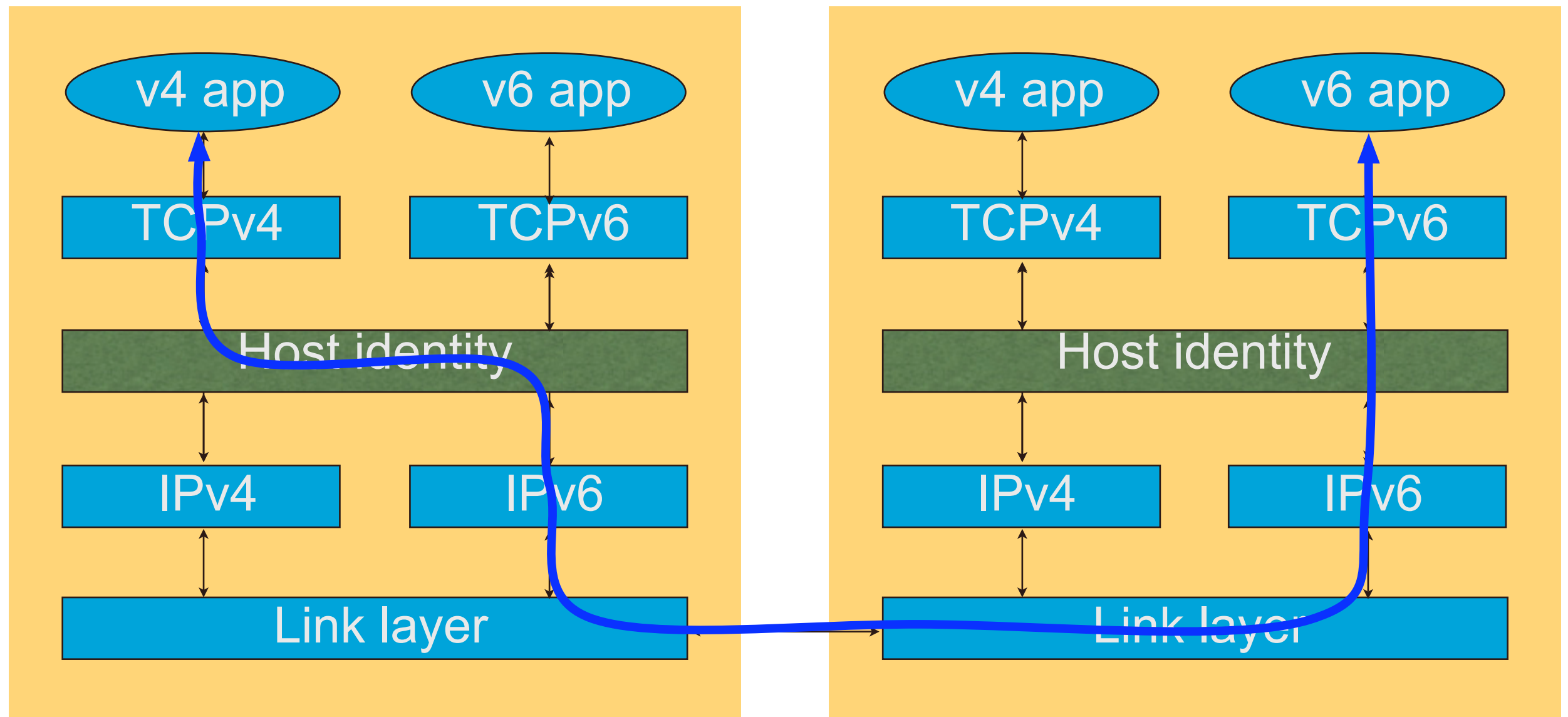
HIP tarkemmin osana pinoa



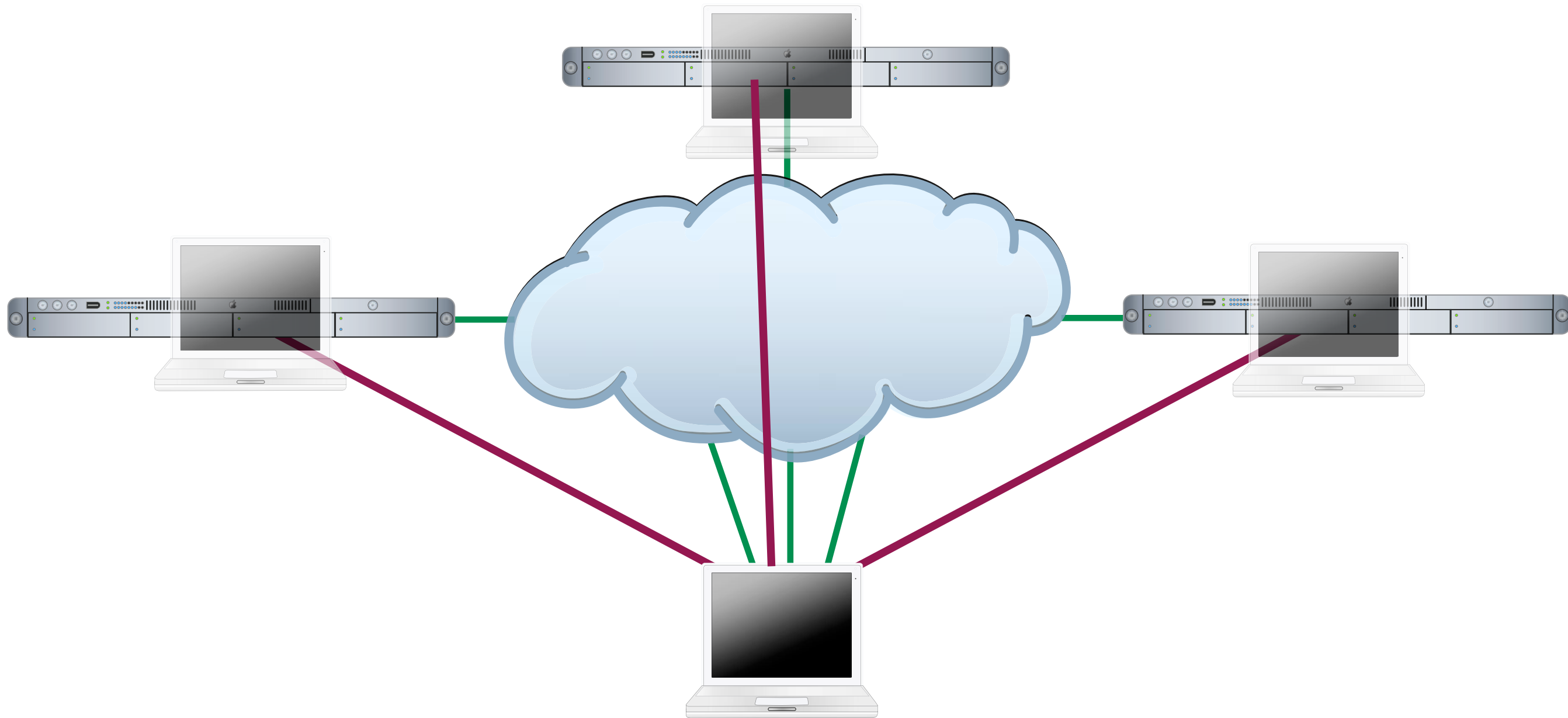
HIP - Mitä sillä saavutetaan?

- Yhdistää samaan pakettiin
 - liikkuvuuden hallinnan (mobilitetti)
 - useamman verkon samanaikaisen käytön (multi-homing / multi-access)
 - perustietoturvan, mukana myös DoS-suojaus
- Kertaluokkaa yksinkertaisempi kuin olemassaolevien standardien yhdistäminen
 - nykyiset (ilman multi-homing): ~60000 LoC
 - HIP (mukana multi-homing): < 15000 LoC
- Mahdollistaa uusia asioita (mm. valtuutus)

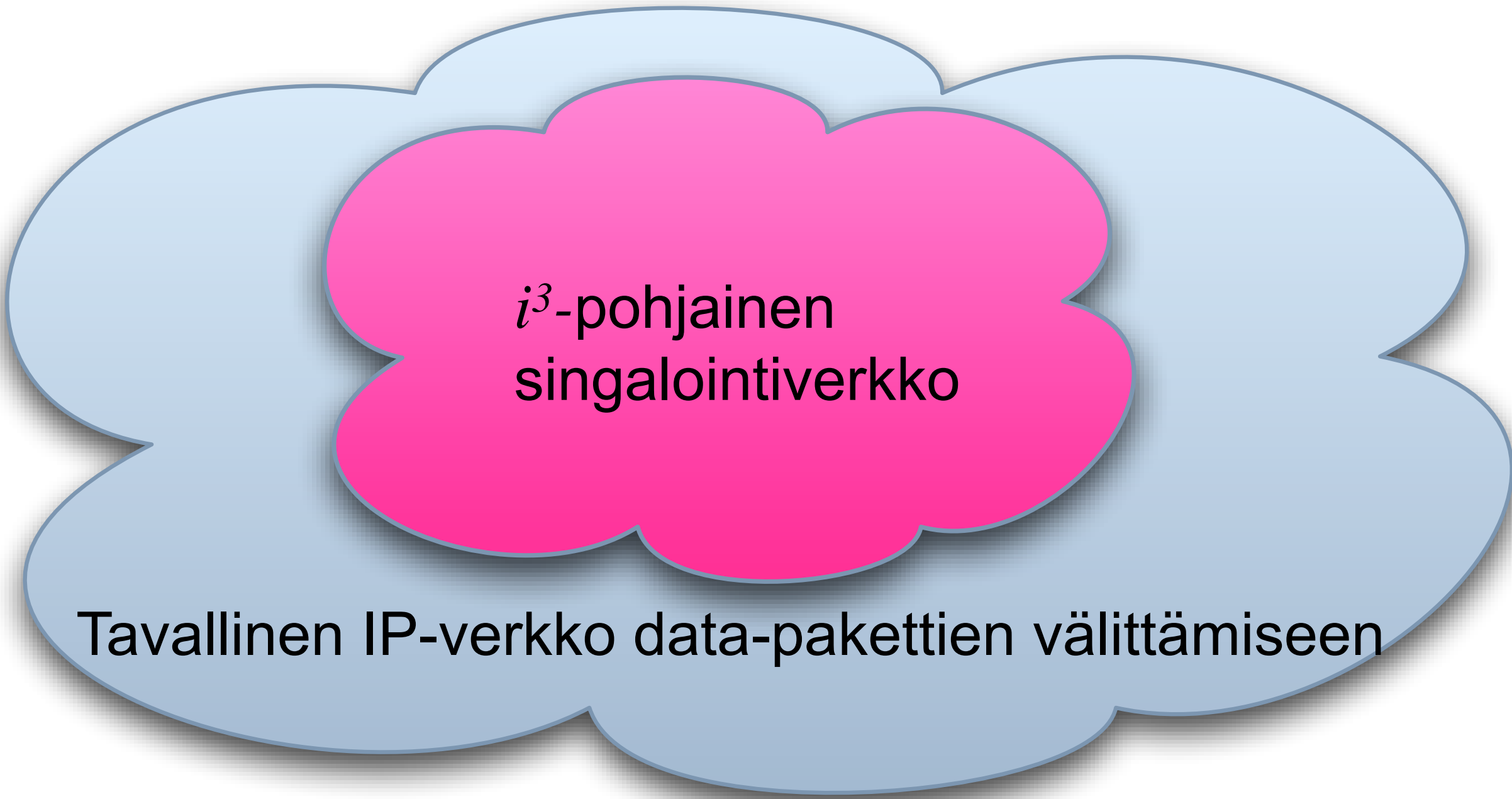
IPv4:n ja IPv6:n yhtäaikainen käyttö



Liikkuvuus ja monien yhteyksien samanaikainen käyttö



H_{i^3} : Signaloinnin ja data erottaminen



i^3 -pohjainen
singalointiverkko

Tavallinen IP-verkko data-pakettien välittämiseen

Kuinka valmis HIP on?

- Tutkimus- ja testikäyttöön valmis nyt
 - Lataa, asenna, ala käyttää
 - Asennus ja konfigurointi ei vielä helppoa
- Perusprotokollan kuvaus (internet draft) lähestulkoon valmis
 - draft-ietf-hip-base-02.txt
- Muut osakomponentit (mobiliteetti, rendezvous, NAT jne) vielä työn alla
- Vertikaalisiin, integroituihin sovelluksiin valmis varsin pian (tänä vuonna?)

Mitä käyttöönotto vaatii?

- Osallistuvat tietokoneet: HIP:in asennus
- Reitittimet ja verkko: ei muutoksia
- DNS ja verkkopalvelut: riippuu tavoitteista
 - alkuun pääsee ilman muutoksia
 - laajassa käytössä joko DNS:ään pitää lisätä uutta tietoa tai tarvitaan uusi verkkopalvelu
- NAT-laitteet: ei muutoksia (ainakaan aluksi)
- Palomuurit: riippuu tavoitteista
- Muut laitteet: ei muutoksia

Kuka hyötyy HIP:istä?

- Verkkoarkkitehtuurin tutkijat
- Uuden teknologian aikaiset omaksujat
- Integroitujen sovellusten kehittäjät
 - Useampaa verkkoyhteyttä samanaikaisesti käyttävät liikkuvat käyttäjät
 - Erilliset hallintaverkot
 - Sotilas- ja kaksikäyttöjärjestelmät (dual use)
 - Korkean käytettävyyden järjestelmät
- Pitkällä aikavälillä toivottavasti kaikki Internet-käyttäjät

Yhteenveto

- Ehdotus muuttaa TCP/IP-arkkitehtuuria
 - Laitteille tunnistettavat “kasvot” (julk.avain)
 - Yhdistää liikkuvuuden, useamman yhteyden yhtäaikaisten käytön ja perustietoturvan
- Helpottaa monien asioiden tekemistä, mm.
 - IPv4 ja IPv6 yhtäaikainen käyttö
 - Signaointi- ja dataliikenteen erotus
- Standardointi menossa IETF:ssä
 - Perusprotokolla lähes valmis