



An Overview of Mobile IPv6 Home Agent Redundancy

-

Katsaus Mobile IPv6 -protokollan kotiagenttien varmennukseen

Diplomityöesitelmä 14.3.2006

Heikki Keränen

Valvoja: Prof. Jörg Ott

Suorituspaikka: Tietoverkkolaboratorio

Sisällys

1. Etusivu
2. Sisällys
3. Tutkimusaihe
4. Onglemat
5. Arviointimalli
6. MIPv6
7. HARP 97 ja Sub 01
8. HSRP
9. VRRPv6 + MIPv6
10. HAHA
11. VHAR
12. Pohjustus simulaatioihin
13. Simulaatiot
14. Muutokset VHAR:iin
15. Topologia
16. VHAR:n perustoiminta
17. VHAR ja reitinoptimointi
18. VHAR ja useita päätelaitteita
19. RA -mainosten välin vaikutus
20. HA:n vaihdon aiheuttaman viiveen minimointi
21. HA:n vaihdon aiheuttaman viiveen minimointi – tulos
22. Simulaatioiden tulokset
23. Diplomityön tulokset
24. Jatkotutkimus

Tutkimusaihe

- Yksi kotiagentti voi palvella lukuisia liikkuvia päätelaitteita
- Mobiili IPv6:n “heikko lenkki”: Kotiagentti
- IPv6 sallii useita kotiagentteja kotilinkillä, mutta:
 - Kuinka jakaa ja päivittää päätelaitteen sidostietoa redundanttien kotiagenttien kesken?
 - Kuinka pitää kotiagentin vaihtumiseen menevä aika pienenä?

Ongelmat

- Implementaation vaatimat muutokset
- Ylimääräiset viestit kotiverkossa
- Näkymättömyys liikkuvalla päätelaitteelle:
 - Yhteydet katkeavat, viive kasvaa
 - Uuden kotiagentin rasittuminen kun useat MN:t muodostavat yhteydet yhtäaikaa
- Kotiagentin vaihto (ainakin) tapahduttava HA:n toimesta, eikä MN:n.
- Tietoturva-assosiaatio

Arviointimalli

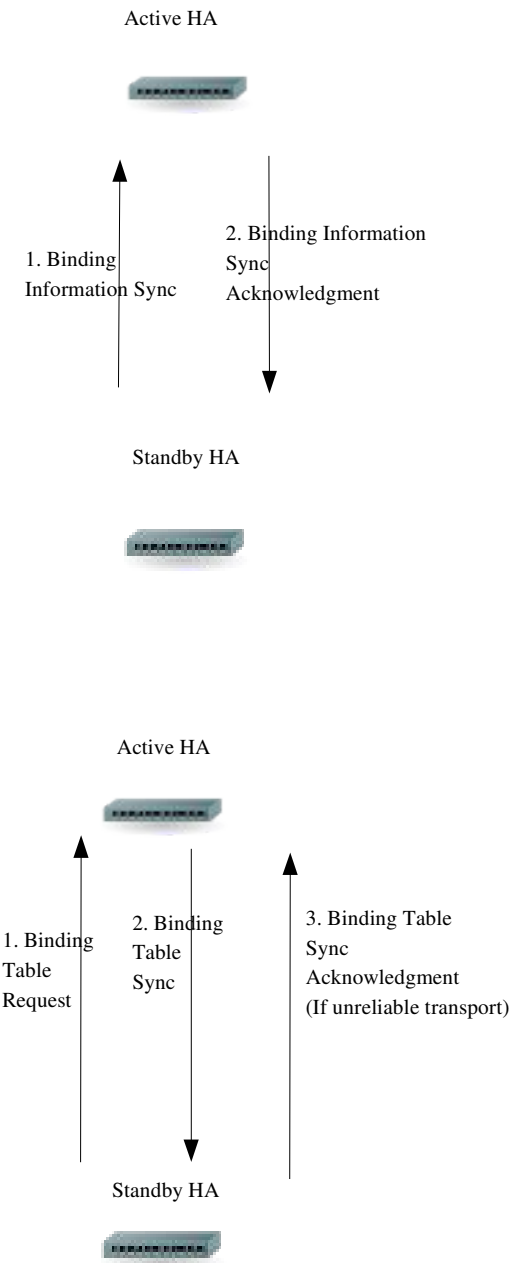
Number of new messages introduced	Every new message adds extra overhead and makes implementation more complex
How to detect failed HA	Detection should not cause long delay, and to provide invisibility to MN, it should not involve MN.
What to do when a failed HA is detected	Amount of delay is evaluated, no extra messaging should occur.
Invisible to MN	Does any part of redundancy mechanism involve MN?
Security Issues	Is SA between MN and HA maintained by mechanism? Is messagin between HAs secure? How about BU sequence number? No new issues should be introduced.
Load Balancing	Is dynamic load balancing supported or does even any load sharing apply?

MIPv6

- Vikatila havaitaan BU Ack:n viipymisestä (hidas)
- HA:t ylläpitävät listaa, jossa preferenssiarvot.
- MN saa DHAAD käytännöllä HA listan, josta MN valitsee uuden HA:n (hidas, 32 s.)
- Ei näkymätön MN:lle: kuormaa ja viivettä.
- Kuormaa myös uudelle HA:lle.
- SA uudelleen neuvoteltava. BU sekvenssi häviää.
- DHAAD tarjoaa kuormanjakoa (uusille yhteyksille)

HARP 97 ja Subbarao 01

- Yksi ensimmäisistä ehdotuksista, ja redundanssiongelman esittelijöistä: HARP. (IPv4)
- HARP Esitti nyt yleistyneen mallin virtuaalisesta IP osoitteesta ja Sub01 sidostiedon synkronoinnin.
- Sub01, ei ota kantaa virhetilan havaitsemiseen eikä siitä toipumiseen.
- Molemmat näkymättömiä MN:lle.
- Sub01mainitsee SA synkronoinnin
- Kuorma jakautuu molemmille / kaikille HA:ille, mutta ei dynaamista kuorman jakoa. (Sub01 Peer HA-moodi).



HSRP

- Perustuu vahvasti Sub01:seen.
- Cisco IOS softaan implementoitu MIP tuki, uusimissa versioissa myös sovellettu MIPv6
- HSRP viesteistä havaitaan vikatila, n. 3 sek.
- Yhteydenvaihto toiselle HA:lle
- Ei tue MN ja HA:n välistä dynaamista SA:ta
- Näkymättömyys MN:lle häviää, jos SA halutaan muodostaa. Eikä HA:t osaa aloittaa MN:n yhteydenvaihtoa.

VRRPv6 & MIPv6

- Laajentaa (VRRP RFC 3768) VRRPv6 Internet-Draftia HA redundanssia varten.
- BC_REQUEST ja BC_UPDATE + VRRPv6
- VRRP-mainoksista havaitaan virhetila
- VRRPv6 äänestys tai HA:n käynnistämä yhteydenmuodostus (hidas)
- Näkymätön MN:lle niin kauan kuin vanha BU voimassa, ja olettaen että SA:ta ei tarvitse MN:n ja HA:n välillä.
- RFC 3775 (MIPv6): “The mobile node and the home agent MUST use an IPsec security association to protect the integrity and authenticity of the Binding Updates and Acknowledgments”
- Dynaaminen kuorman jako voidaan saavuttaa laajennuksella.

HAHA

- “Peer HA” synkronointi, eli kaikki HA:t palvelevat yhtäaikaisesti, ja päivittävät BUI keskenään.
 - myös kuormanjako
- Vikatila havaitaan HELLO-viesteistä, myös VRRPv6:sta voidaan käyttää.
- Havaitsemisen aika riippuu asetettavasta HELLO-viestien taajuudesta, “muutama sekunti ei vielä kasvata viestien määrää merkittävästi”.
- Vikatilasta toivutaan HA Switch Request viestin toimeenpanemalla, sidoksen uudelleen muodostamisella.
- Tietoturva-assosiaatiokin muodostuu näin uudestaan
- Ei ole näkymätön MN:lle.
- Sidosten uudelleenmuodostus hidasta, ja voi aiheuttaa verkkoon ruuhkautumista
- Globaali distribuutio Global HAHA spesifikaatiolla

VHAR

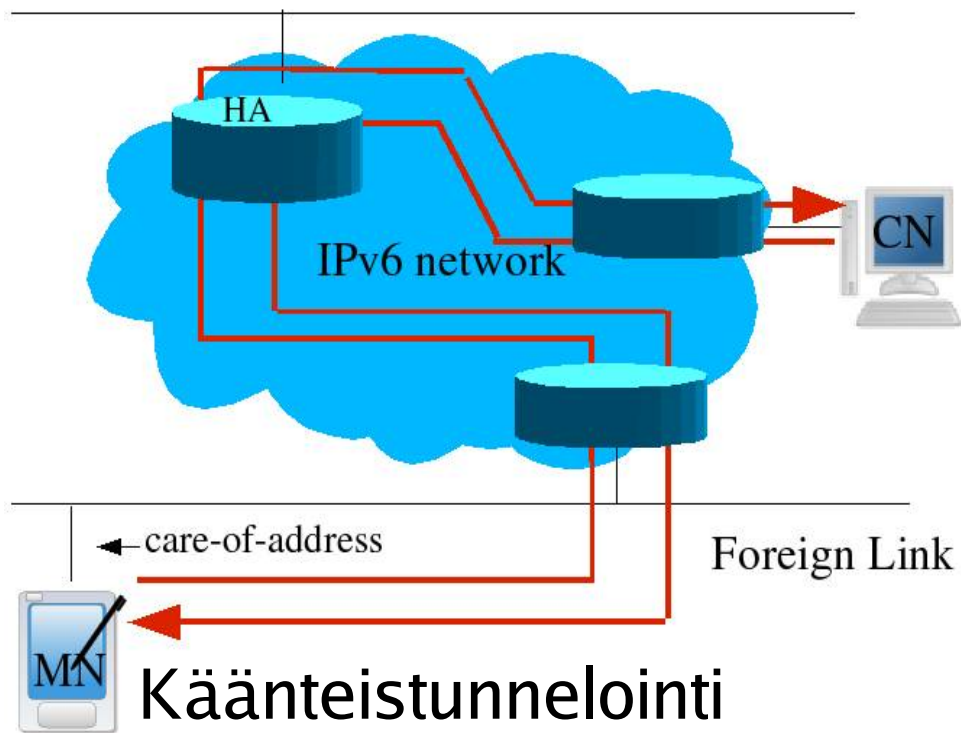
- Aktiivinen HA ja kaksi Backup agenttia, joiden välillä BIU synkronoidaan
- Vikatila havaitaan spontaaneista monilähetysmainoksista (puuttuminen), mainoksen pyyntö vahvistuksena.
- Mainosten väli asetettavissa, “muutama sekunti ei vielä kasvata viestien määrää merkittävästi”.
- Aktiivisen HA:n tilalle uusi toisesta Backup HA:sta, joka puolestaan pyytää itselleen uuden Backup HA:n vapaana olevista HA -reitittimistä (Inactive HA).
- Tietoturva-assosiaatio välitetään SA synkronisaatioviesteillä Active HA:n ja Backup HA:den välillä, myös BU sekvenssinumerot synkronisoidaan.
- Näkymätön MN:lle.
- Ei kuormanjakoa

Kirjallisuustutkimus - tulos

- VHAR tämän tarkastelun perusteella kiinnostavin
 - Tietoturva
 - Tietoturva-assosiaatio ja
 - Sidosviestien sekvenssinumero päivitetään
 - Nopeus
 - Näkymättömyys MN:lle
 - Kuormanjakokin laajennuksella

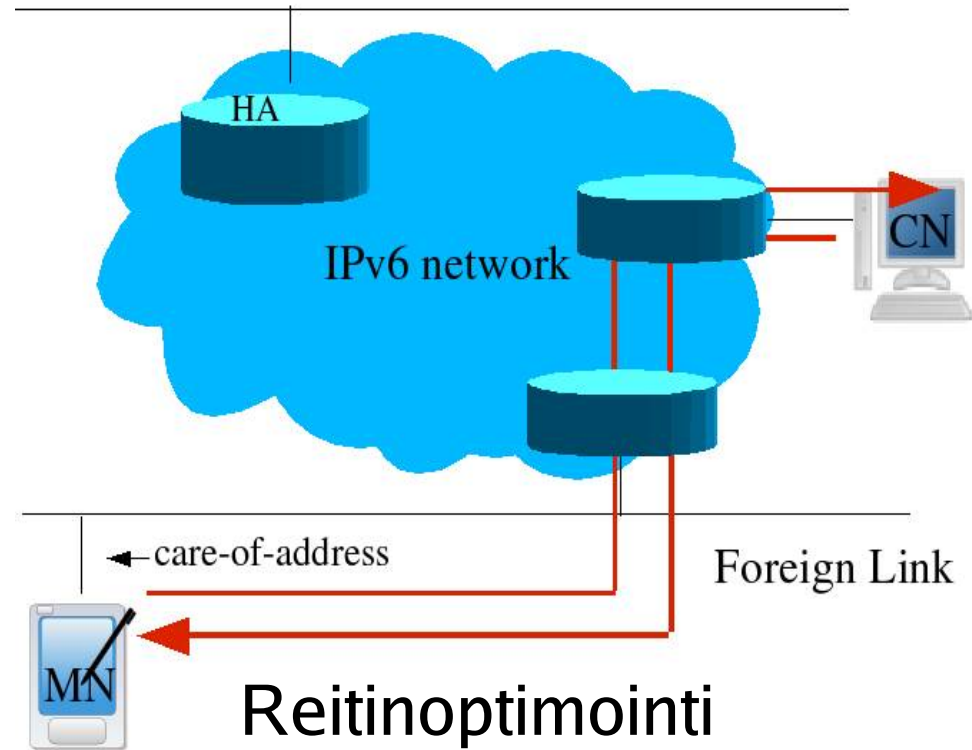
Pohjustus simulaatioihin – kertaus liikkuvuudenhallinnasta

Home Link



Liikenne päätelaitteen ja vertaislaitteen välillä kulkee aina kotiagentin kautta.

Home Link



Liikenne päätelaitteen ja vertaislaitteen välillä kulkee singaloinnin jälkeen suoraan, kulkematta kotiagentin kautta.

RFC 3775: Kotiagentin ja päätelaitteen välinen liikenne suojattava! Tähän tarvitaan IPSec -protokollakokoelmaa.

Simulaatiot

- VHAR tämän tarkastelun perusteella kiinnostavin
 - Tietoturva, nopeus, näkymättömyys MN:lle, kuormanjakokin laajennuksella
- Onko VHAR toteutettavissa?
- Toimiiko reitinoptimoinnin kanssa?
- Miten liikenteen määrä vaikuttaa?
- Mitkä ovat oikeat parametrit?
 - ”dead interval” ja ”heart beat” interval

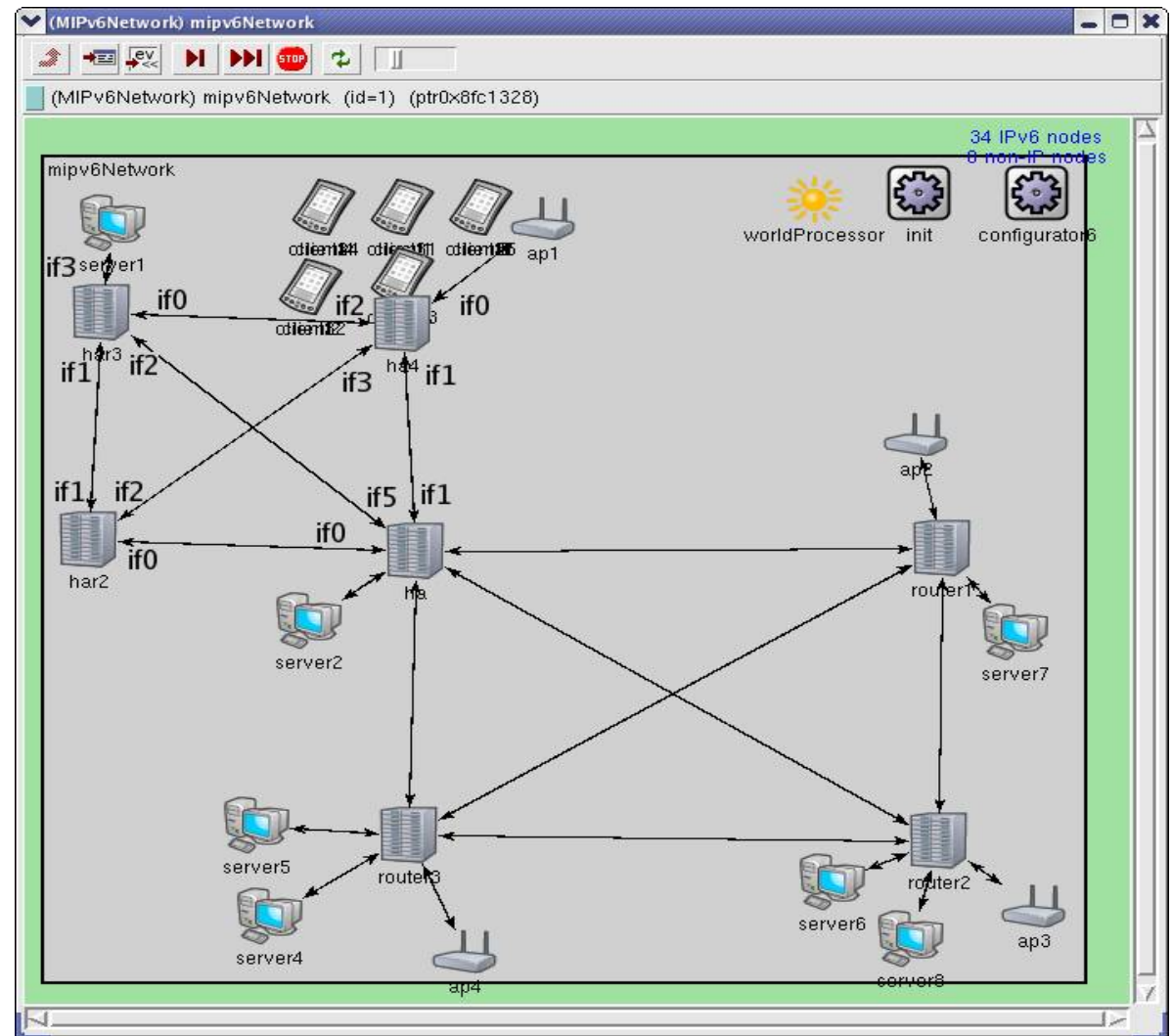
Muutokset VHAR:iin

- Backup havaitsee Active HA:n kuoleman ”dead intervallin” välein päivitettävästä statustiedosta, joka kerätään reitittimien mainosviesteistä.
- Koska kaksi Backup HA:ta, on todennäköistä, että molemmat havaitsevat yhtäaikaan, ja siirtyvät yhtä aikaa Active tilaan.
- Tästä johtuen VHAR:n ei toimi oikein.
- RATKAISU: Erotetaan Backup HA:t prioriteetilla Backup1 ja Backup2.
- Backup2 odottaa pitempään kuin Backup1, ennen kuin ryhtyy toimenpiteisiin.
- Mikäli Backup1:stä tulee uusi Active HA, niin Backup2 vastaanottaa taas mainostuksen Activelta, joten se tietää olla vaihtamatta tilaansa.

Topologia

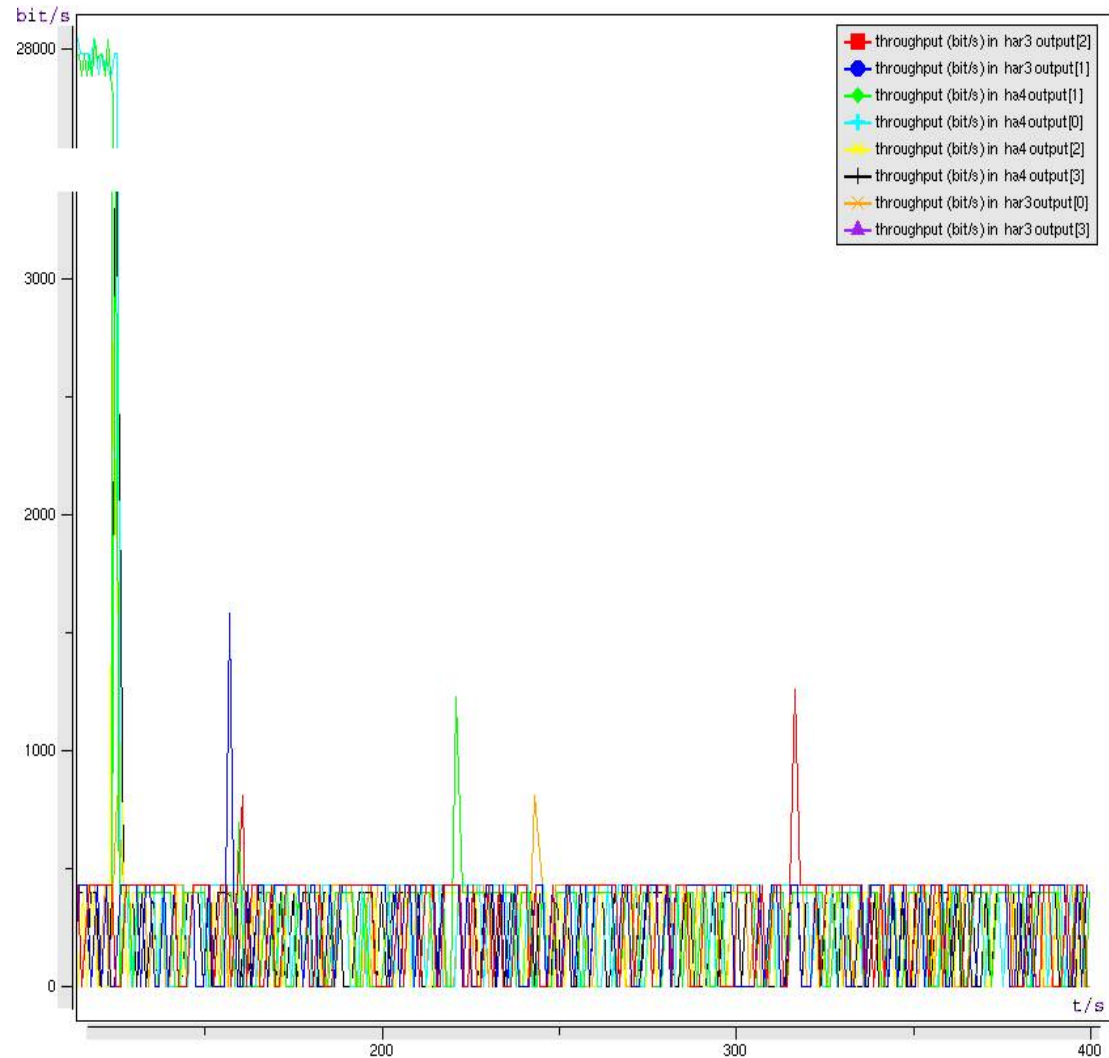
Päätelaitteiden
määrää vaihtelee

VoIP -liikenne



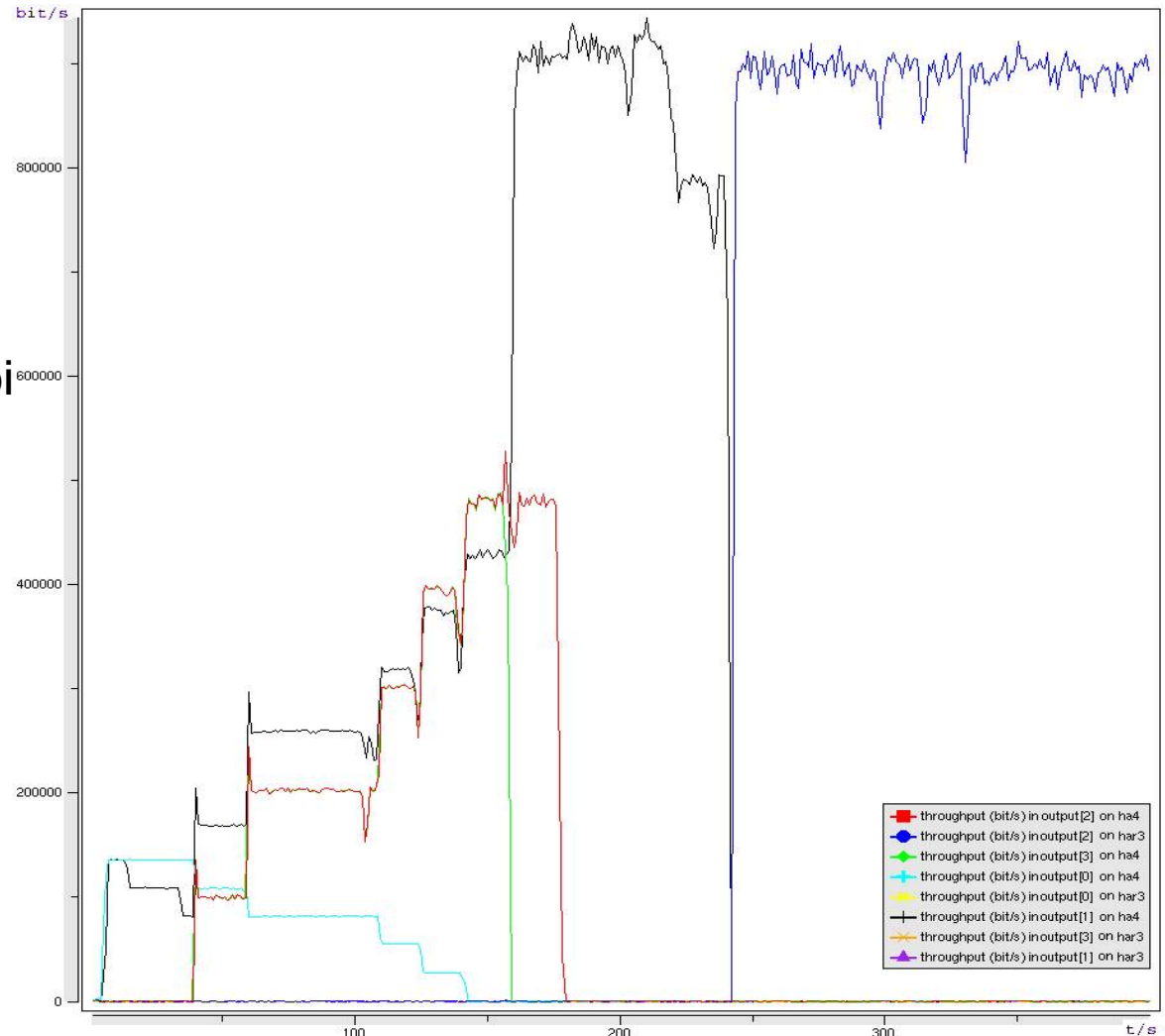
VHAR ja reitinoptimointi

- 1 MN
- Reitinoptimointi
- Valittujen kotiagenttien rajapintojen läpäisystä nähdään, että VHAR toimii oikein myös reitinoptimoinnissa
- 0-120s MN kotiverkossa
- 155s BACKUP2 kaatuu
- 220s AP vaihtuu
- 240s ACTIVE HA kaatuu
- 310s AP vaihtuu
- Ei kuormita juuri lainkaan kotiverkkoa



Useita päätelaitteita

- 5 MN, käänneistunnelointi
- 155s BACKUP2 kaatuu.
- 240s ACTIVE HA kaatuu.
- Valittujen kotiagenttien rajapintojen läpäisystä nähdään, että VHAR ei toimi oikein
- Liikenne ACTIVE:lta BACKUP1:lle loppuu 175s (punainen)
- ACTIVE luulee, että BACKUP1 vikaantunut
- BU:t ja SeqNo jne. eivät päivitty BACKUP1:lle



RA -mainosten välin vaikutus

5 MN, käänneistunnelointi

155s BACKUP2 kaatuu

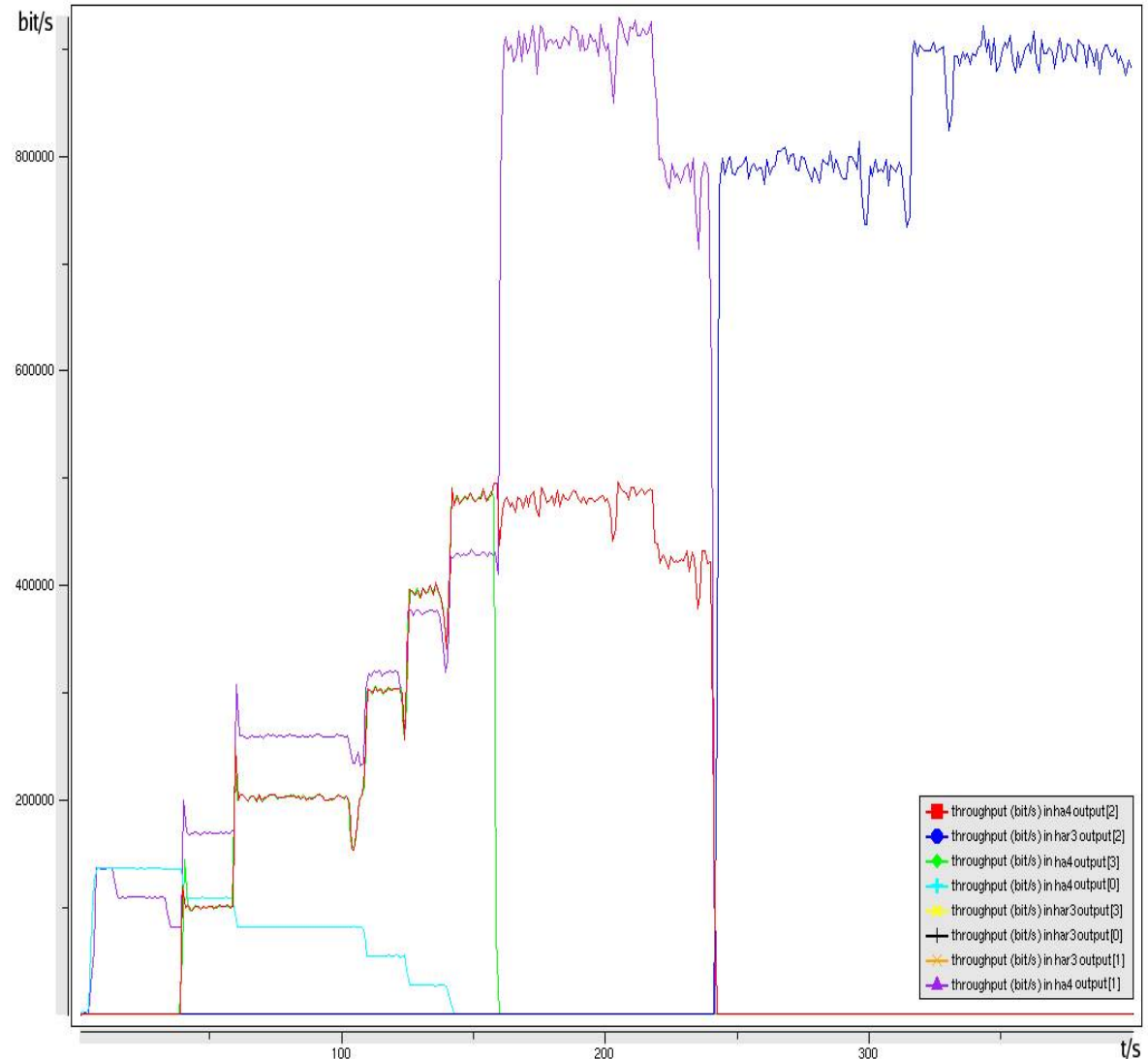
240s ACTIVE HA kaatuu

Nyt "heart beat" -viestien väliajaksi
vaihdettu 0,4s – 0,6s

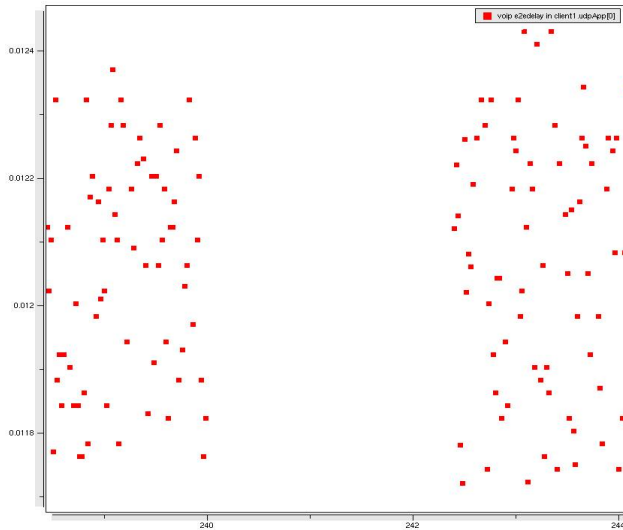
VHAR toimii oikein.

JOHTOPÄÄTÖS:

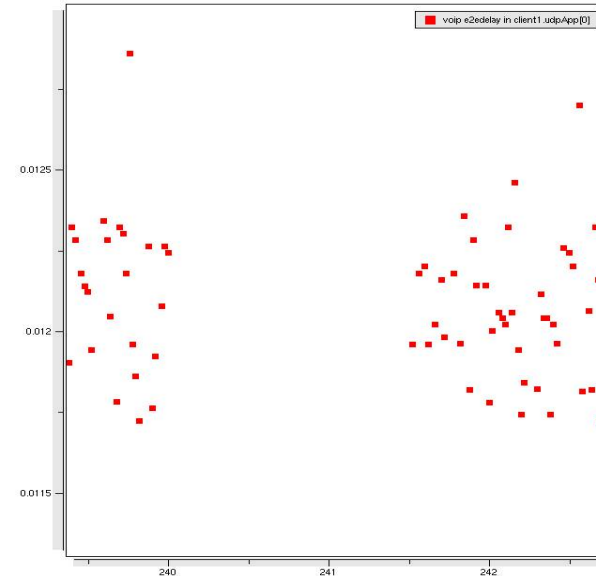
Kuorman kasvaessa RA intervallia I.
"heart beat" viestien väliä
pienennettävä.



HA:n vaihdon aiheuttaman viiveen minimointi



- 1 MN
- "dead interval" 1,2 s
- Katkos kestää n. 2,1 s



- 20 MN
- "dead interval" 0,8 s
- Katkos kestää 1,3 s

20 MN ja 20 simulaatiota:

"dead interval"	Average	Standard Deviation	Variance
0.8	1.24416	0.04566	0.21369
1.2	1.79697	0.17125	0.41383

HA:n vaihdon aiheuttaman viiveen minimointi - tulos

- Toiminnan kannalta oleellista on "heart beat" intervallin ja "dead intervallin" suhde
- MN:n kokemaan viiveeseen vaikuttaa suoraan vain "dead interval"
- Kun "dead intervallia" p ienennetään, täytyy myös RA mainosten välistä aikaa pienentää

Simulaatiot - tulos

- VHAR -protokolla on käytännössä toteutettavissa.
- Toimii parhaiten reitinoiminnilla
- Liikenteen määrä vaatii oikeat parametrit
- Oikeat parametrit määräytyvät seuraavasti:
 - ”dead interval” vaikuttaa katkosten pituuteen
 - ”heart beat interval” vaikuttaa VHAR:n toimivuuteen
 - ”dead intervallin” oltava ”heart beat”n monikerta

Diplomityön tulokset

- Varmennusprotokollalla tarkat vaatimukset
 - Toteutuksen helppous, näkymättömyys, nopeus, tietoturva-asiat
- VHAR täyttää vaatimukset parhaiten
- VHAR implementoitavissa tietyin muutoksin
- VHAR:n parametrit asetettava oikein
 - ”dead interval” moninkertainen verrattuna ”heart beat” -intervalliin

Jatkotutkimus

- VHAR -protokollan toteutus käytännössä MIPv6 verkkoon.
- VHAR -protokollan käytännön vertailu toiseen toteutettuun varmuusprotokollaan, esim. Cisco HSRP
- Useiden tässä työssä tutkittujen protokollien tai laajennuksien parhaiden puolien yhdistäminen yhdeksi toimivaksi protokollaksi