TEKNILLISEN KORKEAKOULUN YLIOPPILASKUNTA
TEKNISKA HÖGSKOLANS STUDENTKÅR
THE STUDENT UNION OF HELSINKI UNIVERSITY OF TECHNOLOGY

Verkkopalvelujen IPv6-tuen toteuttaminen

Funetin tekniset päivät 2008

3.12.2008

TKY/Trinet, Jani Myyry <jani.myyry@tkk.fi>

Huom!

- Esityksen pienellä präntätyn voi lukea nyt tai myöhemmin koneelta (jos kiinnostaa):

  http://verkko.tky.fi/funet2008/trinet-ipv6.pdf

Taustaa: mikä on Trinet?

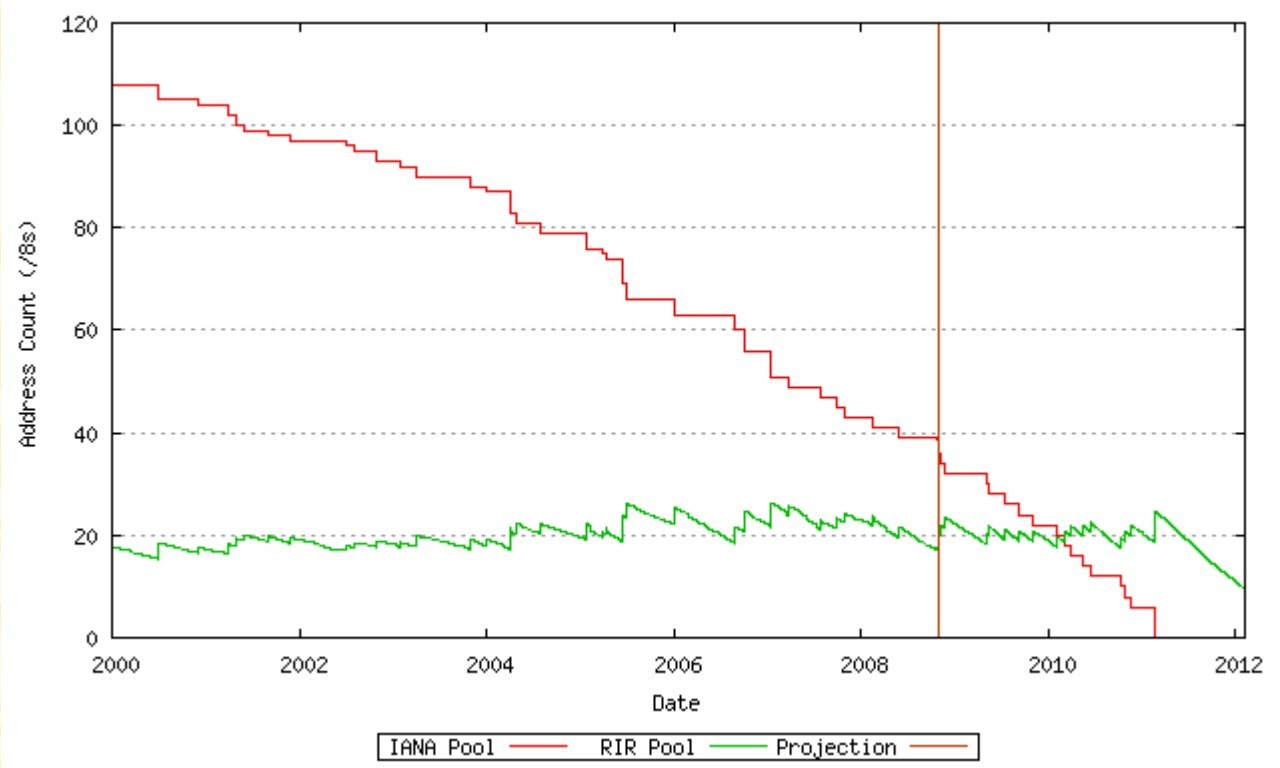
- Otaniemen Teekkarikylän tietoliikenneverkko
- TKY:n kaikissa ja HOAS:n Otaniemen asunnoissa
- 2500 asiakasta, noin 3500 liitäntää
- Toiminut vuodesta 1986 ensin sarjayhteyksin. 90-luvun loppupuolella verkosta tuli “pakollinen” kaluste, vuosituhannen vaihteesta asuntoihin 100 Mbps Ethernet
- Vuodesta 2007 suoraan Funetissa omassa osoiteavaruudessa, sitä ennen TKK:n verkossa
- 2 reititintä (Cisco 6500) ja 86 kytkintä (97% HP, 3% Cisco)
- Oma kuituverkko Teekkarikylässä, loput vuokrattu
- 5 ylläpitäjää

Miksi IPv6 käyttöön?

- Asiakkaat toivoivat!
- Sopiva ajankohta, migraatio uuteen verkkoon asukkaiden osalta ohi
- Suoran Funet-yhteyden myötä natiivi IPv6 mahdollista
- Laitteisto tuki IPv6:sta, uusi ohjelmistoversio julkaistiin sopivasti
- Kilpailukyvyn säilyttäminen verrattuna muihin (kaupallisiin) verkkoihin
- “Historian painolasti” :)

Miksi IPv6 käyttöön?

Projected RIR and IANA Consumption (/8s)



http://www.potaroo.net/tools/ipv4/index.html

Tavoitteet IPv6:een liittyen

- Natiivi IPv6, ei tunnelointeja
- Dual-stack -verkko, palvelut saatavilla sekä IPv4:lla että IPv6:lla
- Nimipalvelussa palvelimien A ja AAAA -tietueet samalla nimellä, ei ipv6.domain.fi -kikkailuja
- Tarjotaan myös multicast (tulevaisuudessa)
- Palvelunlaatu on vastaava kuin IPv4 -puolella

Aikataulu IPv6:n käyttöönotolle

- 2007 heinä/elokuu: osoitehakemus RIPE NCC:lle CSC:n kautta, käänteisnimipalvelu prefixille ja staattinen reititys
- 2007 syyskuu: ensimmäiset palvelut (dns, aika, ssh, ylläpidon www, palomuurit)
- 2007 lokakuu: tarjolle asukkaille
- 2008 talvi: yhdistysten (otax) ja TKY:n www, muut palvelimet, nyyssit
- 2008 toukokuu: multicast, beaconit, sisäiset iptv-testit (oubs)
- 2008 kesä: IPv6 tarjolle kattavasti aliverkkoihin
- 2008 marraskuu: Funet-varayhteys, siirtyminen BGP:hen

IPv6-osoitteiden hakeminen

- Aloitetaan ottamalla yhteyttä <hostmaster@csc.fi>
- Hakemus tehdään RIPE:n lomakkeelle http://www.ripe.net/ripe/docs/ipv6-assignment-request.html
- Palautus CSC:lle, paluupostissa tulee /48 prefix, meille 2001:708:30::/48
- Hakemuksen haastavin osuus on osoitteiden käytön suunnittelu (joka kannattaa miettiä/tehdä)

Esimerkki osoitehakemuksesta

confirmation: **yes**
reason: **n/a**
organisation-name: **The Student Union of Helsinki University of Technology**
organisation-location: **Espoo, Finland**
org-description: **The Student Union of Helsinki University of Technology**
is the official student organization of the Helsinki
University of Technology.
The Student Union owns approx. 1400 flats on campus in
Otaniemi and nearby in Leppavaara providing them with
Internet connection.
website-if-available: **http://www.tky.fi/en/**
for-whole-or-part-of-the-organisation: **whole**
name: **Tommi Saranpaa**
phone: **+35894681**
fax-no: **+35894683218**
e-mail: **verkko@tky.fi**
nic-hdl: **TS3134-RIPE**
#[IPv6 ASSIGNMENT USAGE PLAN]#
subnet: **/48 x - - Campus network**
netname: **FI-TKY-20070801**
#[INSERT SUPPLEMENTAL COMMENTS]#
We intend to run dual-stack IPv4/IPv6 with the equipment we already have.

Prefix will be 48 bits and individual networks 64. That leaves 16 bits for local network prefixes. We intend to leave last 4 bits reserved for future expansions.

Network usage planning...

Networks in block A will be deployed first, as soon as we get ipv6 network up and running (Aug 2007). Once critical services are up, blocks C-E will be deployed in Sep/Oct 2007. Windows domain in block B and others in block F will be handled later.

Osoitesuunnittelu

- Käyttötarpeen mukaan, TKY:n tapauksessa tarpeet rajatut
- Ei kytköstä IPv4-osoitteistukseen (puhtaalta pöydältä)
- Aliverkon reititin 2001:708:30:xyz::1 (HSRP ::e ja ::f), staattiset osoitteet 2001:708:30:xyz::2 ->

```
2001:708:y:

A 0000.0xxx.xxxx.0000  Various server networks

B 0000.10xx.xxxx.0000  Windows domain networks

C 0001.xxxx.xxxx.0000  Campus networks (we already have 96 ipv4 subnets
                       for apartments and more are expected)

D 0010.0xxx.xxxx.0000  Student clubs, guilds etc

E 0010.11xx.xxxx.0000  Visitor networks (WLAN etc)

F 0011.xxxx.xxxx.0000  Other tenants
```

Käänteisnimipalvelu prefixille

- Määritellään uusi käänteiszone IPv6-prefixin pohjalta, esimerkissä 2001:708:30::/48
- Ilmoitetaan nimipalvelimet (ns3.tky.fi ja ns4.tky.fi) CSC:lle delegointia varten

```
$ORIGIN .
$TTL 3600       ; 1 hour
0.3.0.0.8.0.7.0.1.0.0.2.ip6.arpa IN SOA ns3.tky.fi. hostmaster.tky.fi. (
                                2008112200 ; serial
                                3600       ; refresh (1 hour)
                                600        ; retry (10 minutes)
                                1209600    ; expire (2 weeks)
                                3600       ; minimum (1 hour)
                                )
                        NS      ns3.tky.fi.
                        NS      ns4.tky.fi.
                        NS      ns-secondary.funet.fi.
```

Käänteisnimipalvelu prefixille

- Määritetään juuri luodulle zonelle konfiguraatio nimipalvelimiin (esimerkissä BIND9)
- Konfiguraatioesimerkki on julkisille palvelimille (slave)
- Nimipalvelimien ei tarvitse tukea IPv6-kyselyitä!

```
zone "0.3.0.0.8.0.7.0.1.0.0.2.ip6.arpa" {
        type slave;
        notify explicit;
        also-notify {
                128.214.248.132;
        };
        file "slaves/rev-2001:708:30.zone";
        masters {
                82.130.0.x;
        };
};
```

Staattinen IPv6-reititys

- Staattinen reititys sovitaan Funetin kanssa <noc@funet.fi>
- Uudesta osoiteavaruudesta varataan esim. /64 Funet-yhteyttä varten ja sovitaan yhteyteen käytettävät osoitteet (sekä oma organisaatio että Funet)
- Reitittimestä kytketään IPv6 unicast käyttöön, jos ei ole jo

```
ipv6 unicast-routing
no ipv6 source-route
interface Vlan94
  ipv6 address 2001:708:30:7F0::1/64
  ipv6 traffic-filter funet_6in in
  ipv6 traffic-filter funet_6out out
  ipv6 nd suppress-ra
  no ipv6 redirects
!
ipv6 route 2001:708:30::/48 Null0
ipv6 route ::/0 2001:708:30:7F0::11
```

Suodatukset ulkorajalla

- Oma verkko ja muiden verkot kannattaa suojata osoitespooffausten osalta (esim. BCP 38:n pohjalta)
- Lisäksi voi palomuurata, jos avoin verkko ahdistaa

```
ipv6 access-list funet_6in
 permit ipv6 2001:708:30:7F0::/64 any
 deny ipv6 2001:708:30::/48 any
 permit ipv6 any 2001:708:30::/48
 permit ipv6 any FE80::/10
 permit ipv6 any FF00::/8
 deny ipv6 any any
!
ipv6 access-list funet_6out
 permit ipv6 2001:708:30:7F0::/64 any
 permit ipv6 any FE80::/10
 permit ipv6 any FF02::/16
 permit ipv6 2001:708:30::/48 any
 deny ipv6 any any
!
```

IPv6-yhteyden testaus

- Siirtyminen IPv6-aikaan voidaan juhlistaa testaamalla uutta yhteyttä (reitittimestä)
- Funetin IPv6-status näyttää jo kahta vihreää valoa! http://www.csc.fi/funet/status/tools/funet_ipv6_status

```
gw-1#ping 2001:948:0:f005::42

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:948:0:F005::42, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms
```

IPv6 palvelinverkkoihin

- Palvelimet käyttävät pääosin manuaalikonfiguraatiota
- Autokonfiguraatiota ei edes ole tarjolla suurimmassa osassa palvelinverkkoja

```
interface Vlan101
 description server-101
 ! IPv4 ...
 ipv6 address 2001:708:30:xyz::1/64
 ipv6 nd ra suppress
 no ipv6 redirects
!
```

IPv6 asiakasverkkoihin

- Opiskelija-aliverkkoihin IPv6 tarjotaan autokonfiguraatiolla (stateless address autoconfiguration)
- DHCPv6 on tarjolla nimipalvelintietojen välittämiseen, mutta ei osoitteiden jakamiseen
- Verkoissa tehdään tarkistus lähdeosoitteelle (ACL:llä, koska muuten liikenne tipahtaa RP:lle)
- Reitittimellä on määritetty korkeampi prioriteetti, jotta se pärjäisi kilpahuutotilanteessa
- Lisäksi verkoissa suodatetaan muutamaa protokollaa

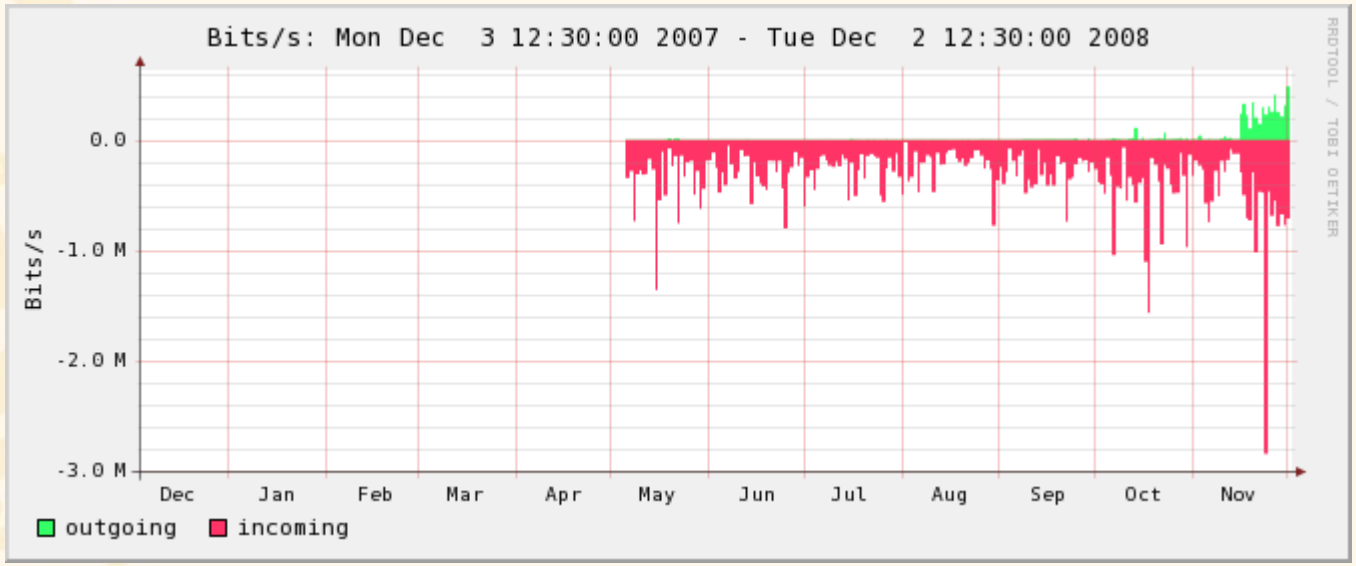
IPv6 asiakasverkkoihin

```
ipv6 dhcp pool nd-kyla-pool
 dns-server 2001:708:30:10::2
 dns-server 2001:708:30:20::2
 domain-name kyla.fi
!
interface Vlan301
 description taloxyz
 ! IPv4 ...
 ipv6 address 2001:708:30:xyz::1/64
 ipv6 traffic-filter trinet_6in_v301 in
 ipv6 traffic-filter trinet_6out out
 ipv6 nd other-config-flag
 ipv6 nd router-preference High
 no ipv6 redirects
 ipv6 dhcp server nd-kyla-pool
!
ipv6 access-list trinet_6in_v301
 ! ...
 permit ipv6 FE80::/10 any
 permit ipv6 2001:708:30:xyz::/64 any
 deny ipv6 any any
!
```

IPv6-tuki asiakaskoneissa

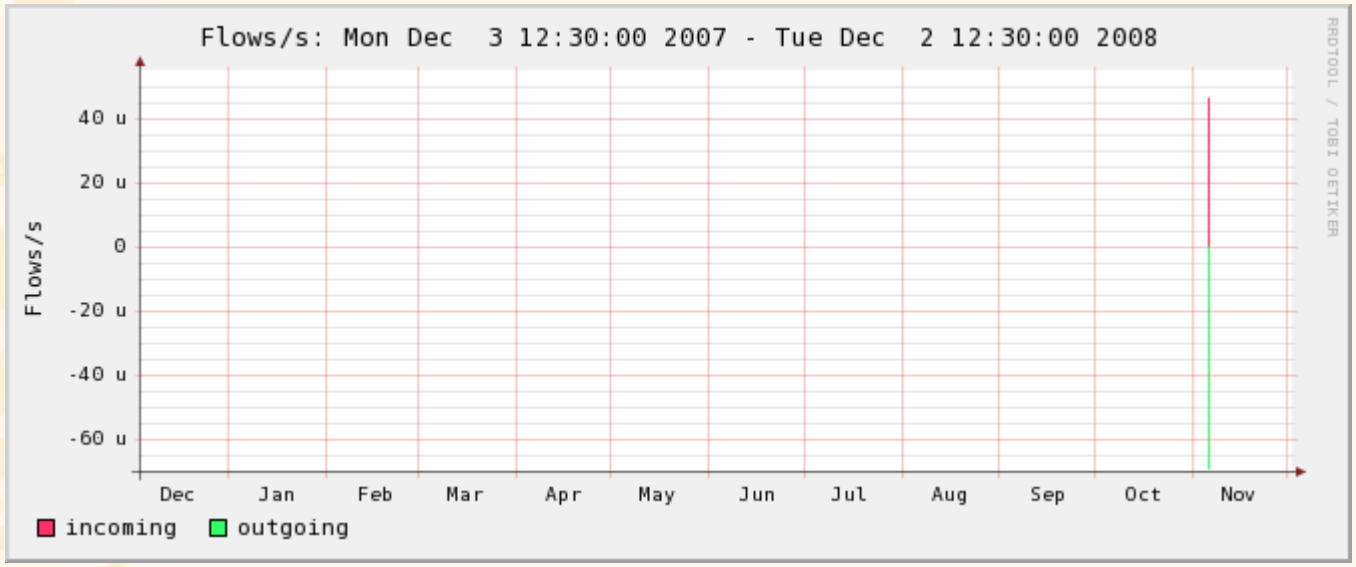
- Windows Vista ok
- Linux (Ubuntu, Fedora, ...) ok
- MacOSX ~ ok
- Windows XP ~ vähän purkkaa

IPv6 löytyy, käytetäänkö sitä?



Trinetin IPv6-liikenne Internettiin toukokuusta 2008 lähtien

TKK osaa myös IPv6:sta



Trinetin IPv6-liikenne TKK:lle toukokuusta 2008 lähtien

Palveluiden IPv6-tuki

- Palveluohjelmistojen IPv6-tuki on usein varsin triviaali ottaa käyttöön
- Palvelun IPv6-tuen julkaiseminen tapahtuu lisäämällä palvelimelle AAAA -tietue nimipalveluun
- Seuraavaksi esimerkkejä (RHEL5)
  - DNS (BIND9)
  - NTP
  - SSH (OpenSSH+ tcp_wrappers)
  - Apache

BIND9

- Vaatii IPv6-käyttöön option listen-on-v6
- ACL:iin tulee lisätä tarvittavat IPv6-osoiteavaruudet

```
## /var/named/chroot/etc/named.conf
acl RECURSION {
#       ...
        ::1;
        2001:708:30::/48;
};

options {
#       ...
        listen-on-v6 {any;};

        allow-recursion {
                RECURSION;
        };
};

## restart
service named restart

## testaus
dig @2001:708:30:10::2 www.nordu.net AAAA +short
2001:948:0:f005::42
```

Autoratiivinen nimipalvelu

- IPv6 -tuki autoratiivisella puolella hoituu AAAA-tietueiden lisäyksellä nimipalvelimille
- Kannattaa kuitenkin varmistaa, että nimipalvelu tukee oikeasti IPv6:sta ennen tietueiden lisäystä
- Esimerkissä tky.fi -zoneen määritetyt nimipalvelimet (palvelevat samalla n. muuta domainia)

```
## tky.fi zone
tky.fi.                 3600  IN NS ns3.tky.fi.
tky.fi.                 3600  IN NS ns4.tky.fi.
ns3.tky.fi.             3600 IN A 82.130.0.5
ns3.tky.fi.             3600 IN AAAA 2001:708:30:10::2
ns4.tky.fi.             3600 IN A 82.130.63.5
ns4.tky.fi.             3600 IN AAAA 2001:708:30:20::2
```

NTP-palvelu

- Tukee sekä IPv6 unicastia että multicastia
- Konfiguraatioon lisätään sallituiksi IPv6-osoiteavaruudet
- Määritetään multicast-ryhmä (ff05::101), johon aikaa lähetetään
- Multicast vaatii kohtuullisen tuoreen NTP-ohjelmiston (testattu 4.2.4p4, RHEL5:n oma versio ei toimi)

```
## /etc/ntp.conf
restrict        -6 default ignore
restrict        -6 ::1

# unicast
restrict        -6 2001:708:30:: mask ffff:ffff:ffff:: nomodify notrap nopeer

# multicast
broadcast       -6 ff05::101 ttl 3

## restart
service ntpd restart
```

NTP-asiakas

- IPv6 unicast ja multicast toimivat (testattu Ubuntu 8.04)

```
## /etc/ntp.conf
restrict        -6 default ignore
restrict        -6 ::1
restrict        -6 2001:708:30:10::2 nomodify notrap noquery
restrict        -6 2001:708:30:20::2 nomodify notrap noquery

# unicast
server          -6 2001:708:30:10::2
server          -6 2001:708:30:20::2

# multicast
multicastclient -6 ff05::101

## multicast-esimerkki
service ntpd restart
ntpq -pn
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 LOCAL(0)        .LOCL.          10 l   49   64  377    0.000    0.000   0.001
*2001:708:30:10: 130.233.224.52   3 m   59   64  376    0.143    0.092   0.014
+2001:708:30:20: 130.233.224.52   3 m   39   64  376    0.200    0.001   0.013
```

SSH

- Vaatii IPv6-käyttöön lisäoption ListenAddress
- Lisäksi kannattaa varmistaa, että hosts.allow sallii Ipv6-osoitteet

```
## /etc/ssh/sshd_config
ListenAddress ::

## /etc/hosts.allow
sshd : [2001:708:30::]/48 : allow
ALL : UNKNOWN : deny
ALL : localhost localhost.localdomain localhost6 localhost6.localdomain6 : allow
ALL : ALL : deny

## restart
service sshd restart
```

Apache

- Apache täytyy konfiguroida kuuntelemaan IPv6:sta
- Mahdollisiin rajoituksiin (httpd.conf ja .htacess) tulee lisätä tarvittavat IPv6-osoiteavaruudet

```
## /etc/httpd/conf/httpd.conf
Listen 80

## /etc/httpd/conf.d/ssl.conf
Listen 443

## /etc/httpd/conf/httpd.conf tai .htaccess
Allow from ::1
Allow from 2001:708:30::/48

## restart
service httpd restart
```

IPv6 ja verkonvalvonta

- Nfdump ja nfsen (liikenteen lokitus): tukevat, kunhan käytössä on NetFlow v9 (SXH ->)
- Netdisco (kytkinporttien hallinta/lokitus): ei tukea
- IPv6<->MAC neighbor cache SNMP:llä: ei tukea, vai onko???
- Smokeping (latenssit tms.): tukee, ping6...
- Nagios: tukee, ping6...

IPv6 unicast -reititys BGP:llä

- Sovitaan Funetin kanssa <noc@funet.fi>
- Tarvitaan AS-numero (esim. privaatti)
- Oletettavasti käytetään varayhteyteen, joten tarvitaan toinen /64 osoiteavaruus varayhteydelle ja sopimus Funetin kanssa käytettävistä osoitteista
- Verkosta riippuen kannattaa harkita, onko tarpeen ajaa jotain sisäistä reititysprotokollaa vai riittääkö iBGP?
- Lisäksi vaatimuksena on “kyky” konfiguroida BGP:tä :)

BGP: pääyhteyden reititin 1

```
router bgp 39857
 bgp router-id 82.130.63.202
 bgp log-neighbor-changes
 neighbor 2001:708:30:7F0::11 remote-as 1741
 neighbor 2001:708:30:7F0::11 description IPv6 peering with AS1741 - Funet
 neighbor 2001:708:30:7FE::2 remote-as 39857
 neighbor 2001:708:30:7FE::2 description IPv6 iBGP peering with AS39857 - gw-2
 neighbor 2001:708:30:7FE::2 update-source Loopback0
 !
 address-family ipv6
  neighbor 2001:708:30:7F0::11 activate
  neighbor 2001:708:30:7F0::11 route-map funet-ipv6-main-in in
  neighbor 2001:708:30:7F0::11 route-map funet-ipv6-out out
  neighbor 2001:708:30:7FE::2 activate
  neighbor 2001:708:30:7FE::2 next-hop-self
  network 2001:708:30::/48
  no synchronization
 exit-address-family

! Staattinen reitti -> gw-2 loopback0
ipv6 route 2001:708:30:7FE::2/128 2001:708:30:7FD::2
ipv6 route 2001:708:30::/48 Null0

ipv6 prefix-list own-ipv6-prefixes seq 10 permit 2001:708:30::/48
route-map funet-ipv6-main-in permit 10
 set local-preference 100
route-map funet-ipv6-out permit 10
 match ipv6 address prefix-list own-ipv6-prefixes
```

BGP: pääyhteyden reititin 2

```
interface Loopback0
 ipv6 address 2001:708:30:7FE::1/128
 no ipv6 redirects

! Reitittimien välinen yhteys
interface Vlan97
 ! IPv4 ...
 ipv6 address 2001:708:30:7FD::1/64
 ipv6 nd ra suppress
 no ipv6 redirects
```

BGP: varayhteyden reititin 1

```
router bgp 39857
 bgp router-id 82.130.63.203
 bgp log-neighbor-changes
 neighbor 2001:708:30:7F1::11 remote-as 1741
 neighbor 2001:708:30:7F1::11 description IPv6 peering with AS1741 - Funet
 neighbor 2001:708:30:7FE::1 remote-as 39857
 neighbor 2001:708:30:7FE::1 description IPv6 iBGP peering with AS39857 - gw-1
 neighbor 2001:708:30:7FE::1 update-source Loopback0
 !
 address-family ipv6
  neighbor 2001:708:30:7F1::11 activate
  neighbor 2001:708:30:7F1::11 route-map funet-ipv6-backup-in in
  neighbor 2001:708:30:7F1::11 route-map funet-ipv6-out out
  neighbor 2001:708:30:7FE::1 activate
  neighbor 2001:708:30:7FE::1 next-hop-self
  network 2001:708:30::/48
  no synchronization
 exit-address-family

! Staattinen reitti -> gw-1 loopback0
ipv6 route 2001:708:30:7FE::1/128 2001:708:30:7FD::1

ipv6 prefix-list own-ipv6-prefixes seq 10 permit 2001:708:30::/48
route-map funet-ipv6-backup-in permit 10
 set local-preference 90
route-map funet-ipv6-out permit 10
 match ipv6 address prefix-list own-ipv6-prefixes
 set metric 50
```

BGP: varayhteyden reititin 2

```
interface Loopback0
 ipv6 address 2001:708:30:7FE::2/128
 no ipv6 redirects

! Reitittimien välinen yhteys
interface Vlan97
 ! IPv4 ...
 ipv6 address 2001:708:30:7FD::2/64
 ipv6 nd ra suppress
 no ipv6 redirects
```

IPv6 HSRP

- Testissä muutamassa aliverkossa, uusin reitittimen ohjelmisto tukee (SXI)
- Default-reitti aliverkosta on link-local -osoite

```
key chain hsrp2
 key 1
   key-string foobar2

## gw-1
interface Vlan105
 ipv6 address 2001:708:30:xyz::E/64
 standby version 2
 standby 2105 ipv6 FE80::1
 standby 2105 priority 105
 standby 2105 preempt delay minimum 30
 standby 2105 authentication md5 key-chain hsrp2
 standby 2105 track GigabitEthernet4/47

## gw-2
interface Vlan105
 ipv6 address 2001:708:30:xyz::F/64
 standby version 2
 standby 2105 ipv6 FE80::1
 standby 2105 preempt
 standby 2105 authentication md5 key-chain hsrp2
```

IPv6 multicast

- Periaatteessa “toimii”, mutta käytännössä ei kovin hyvin
- Interdomain multicastia on testattu sekä Embedded RP:hen että Renaterin RP:hen pohjautuen, lähinnä multicast beaconeita ajaen
- HP:n kytkimet eivät tue (puuttuu MLDv2 snooping) -> liikenne kaikuu kaikkiin aliverkon portteihin
- IPv6 multicastin tukeminen tarkoittaa laitteiston 100% vaihtoa (HP:n tapauksessa ProVision-sarjan laitteisiin)

IPv6 multicast staattisella reitillä

- Käyttö oli vähäistä, mutta toimi ok

```
ipv6 multicast-routing

interface Vlan94
 ! IPv4 ja IPv6 unicast...
 ipv6 pim bsr border
 ipv6 multicast boundary scope 8

! Renater RP
ipv6 pim rp-address 2001:660:3007:300:1:: m6bonerp_6in
! Embedded RP
ipv6 pim rp-address 2001:708:30:7FF::1 embrp_6in

ipv6 access-list m6bonerp_6in
 permit ipv6 any FF0E::/16
 permit ipv6 any FF1E::/16
 permit ipv6 any FF3E::/16
 deny ipv6 any any

ipv6 access-list embrp_6in
 permit ipv6 any FF7E:140:2001:708:30:7FF::/96
 deny ipv6 any any

interface Loopback1
 ipv6 address 2001:708:30:7FF::1/128
```

IPv6 multicast BGP:llä

- Tällä hetkellä varsin isoja ongelmia (reititin ei kestä streamausta), rajoitettu hieman käyttöä...
- Multicast-stream kaatanut pääyhteyden reitittimen 2 kertaan viimeisen viikon aikana
- Multicast-beaconit näkevät vähemmän kohteita kuin aiemmin
- Ei tukea PIM Anycast RP:lle, yritelmänä sen sijaan stateless Embedded RP
- Selvitellään...

Ei ole pakko kattoo

- IPv6 multicastin läpilyömisen piinallista odotusta voi lieventää osoitteissa:
  udp://@oubs.iptv.kyla.fi
  udp://@oubshd.iptv.kyla.fi
- Pääsylippuna käy vlc (jos verkko ei oo rikki)
- Toimintatakuuta ei ole ja katsomisen aiheuttamaa mielipahaa ei korvata

Kiitos!

?