

IPv6-juleverkstad

Tore Anderson
CG Security and Networking
Redpill Linpro
Norsk Tipping, Hamar, Desember 2011

Del 1:
Kva er IPv6, egentleg,
kvifor treng me det?

Fyrst litt historie

- TCP/IP vart utvikla av Bob Kahn og Vint Cerf på 70-tallet, og spesifikasjonen på versjon 4 vart publisert i 1978
- Den 1. januar 1983 vart TCP/IPv4 den einaste offisielle protokollen på ARPANET, då Vint Cerf og John Postel enkelt og greit skrudde av støtte for forgjengaren NCP i samtlege ruterar i nettverket
- I IPv4 er ei adresse eit 32-bits nummer:

192 . 0 . 2 . 254

11000000 00000000 00000010 11111110

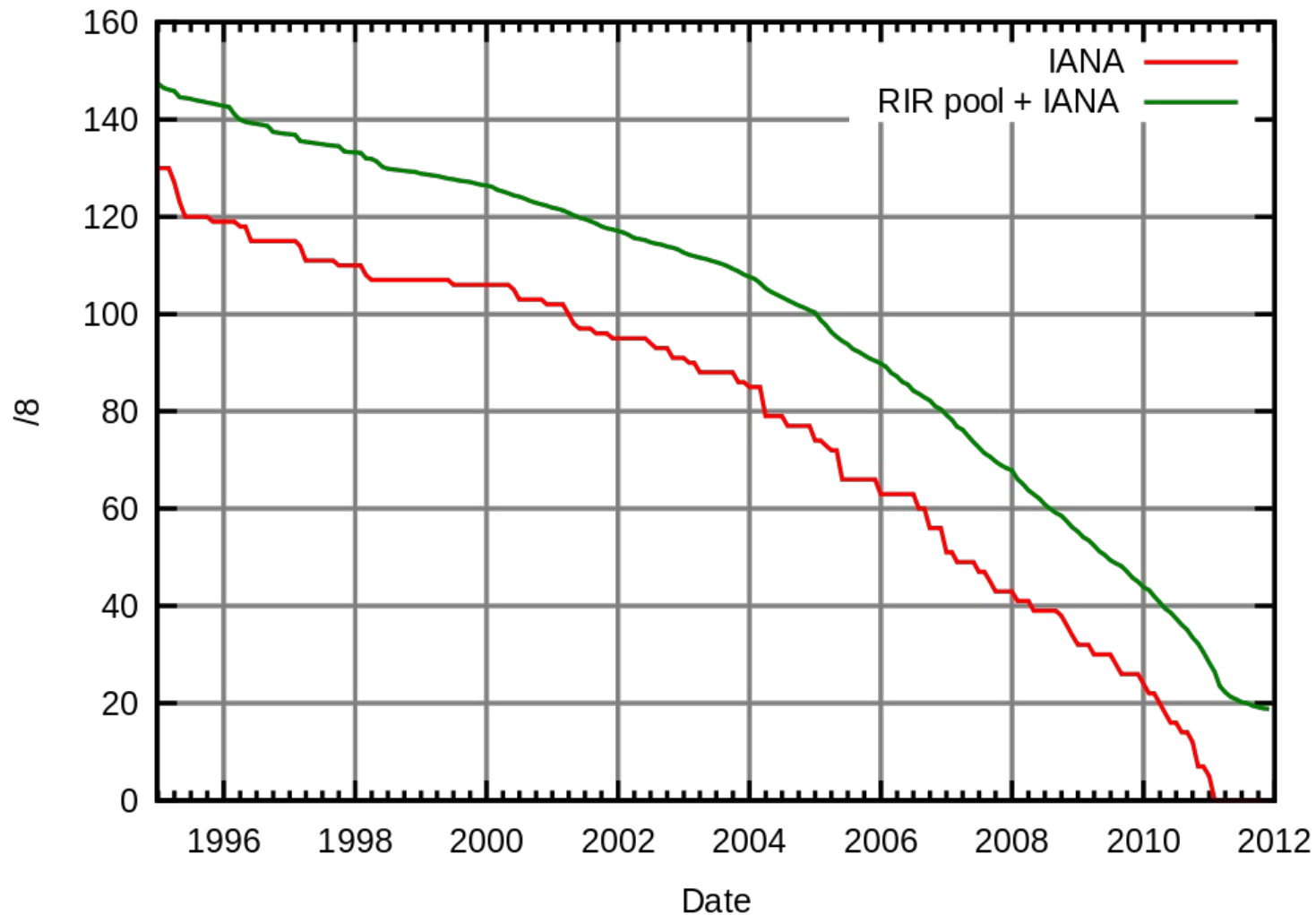
- 32 bits gjev 4,3 milliardar unike kombinasjonar
 - 100% utnyttingsgrad er dog fullstendig urealistisk
- Kvar einaste node på internett treng si eiga unike IP-adresse
- Det vart rundt 1990 klart at verda snart ville gå tom for IP-adresse

Kunsten å få IPv4 til å vare

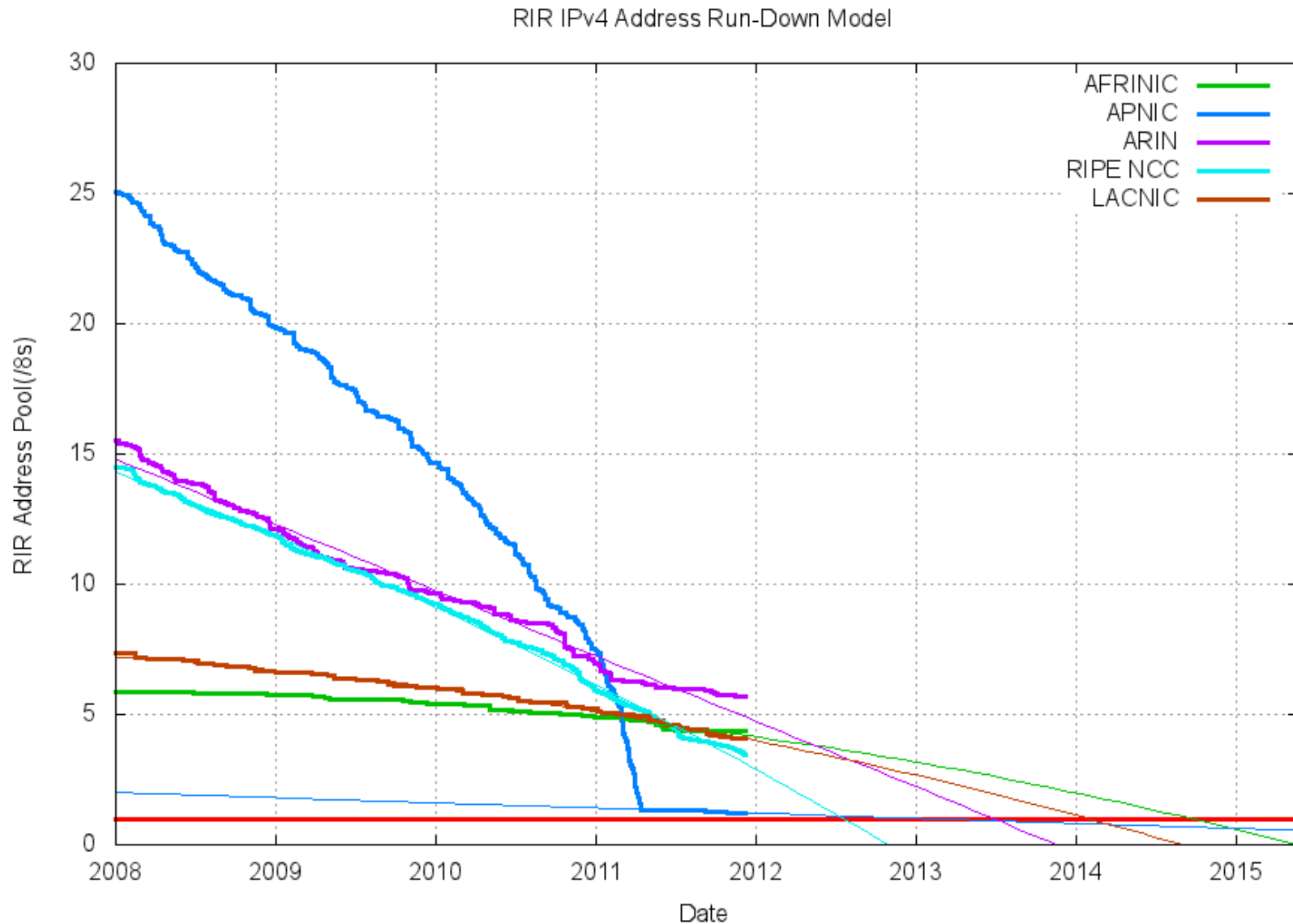
- I utgangspunktet var det kun tre moglege mengder adresser ein organisasjon kunne få tildelt: **16.777.216**, **65.536**, eller **256** IP-ar.
 - For å få ei blokk med adresse, måtte du berre sende ein e-post til Jon Postel, som så ville gje deg det du trengte å meine
- Dette systemet vart erstatta med eit formelt distribusjons-hierarki med ein global reserve (IANA) på toppen, som deler ut store blokker adresser til fem regionale distributørar (RIR), som igjen fordelar adresser ut til internettleverandørar og større organisasjonar (LIR)
 - RIR-ane kan no tildele blokker i alle storleikar som kan utrykkast som ein toar-potens – 1, 2, 4,, 1024, 2048, 4096, ..., osv. osv.
- **NAT** vart vanleg – privatbrukarar får kun éi IP-adresse, og deira heimeruter «skjuler» alle maskinene i heimen bak denne eine IP-adressa
 - Same prinsippet som ei bedrift som kun har éit telefonnummer; alle utgåande samtalar kjem tilsynelatande frå det same nummeret

Utviklinga sidan 1995

Free /8



Tilgjengeleg per RIR sidan 2008



IPv4-status i dag

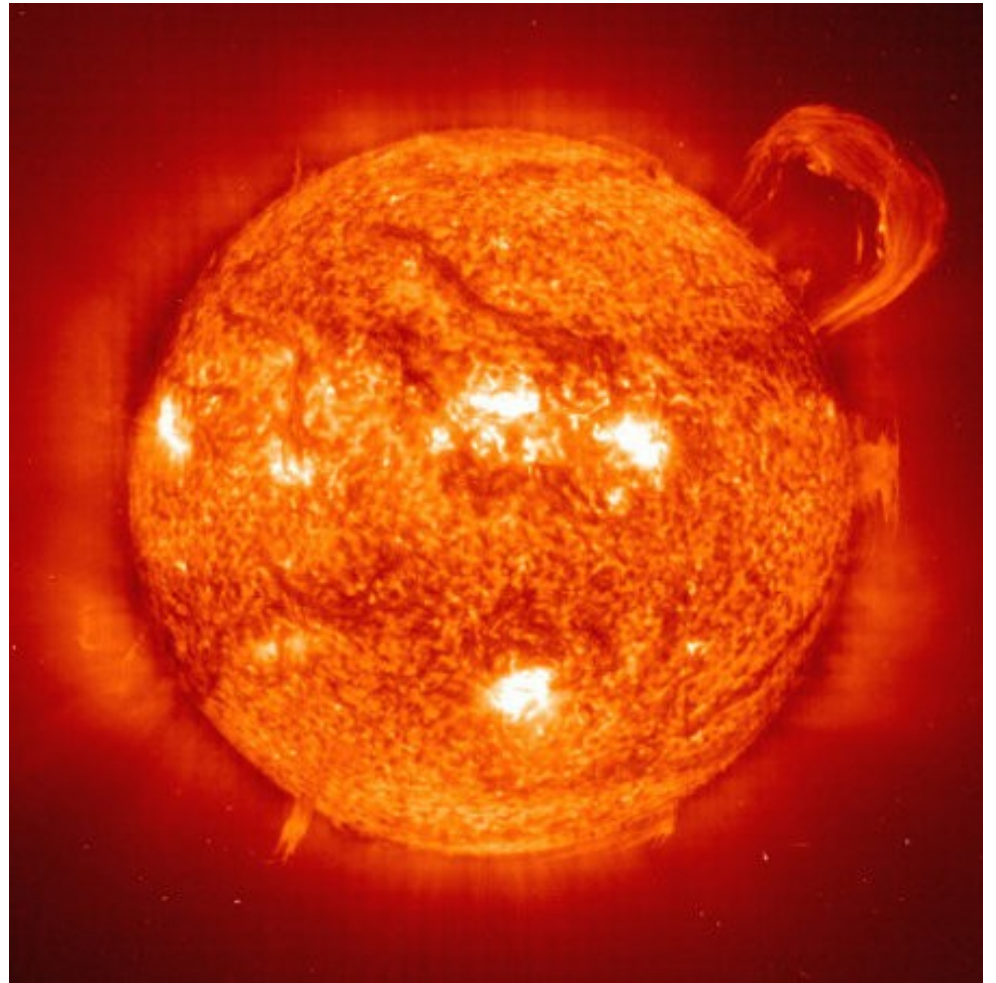
- Den globale reserven (IANA) gjekk tom for IPv4-adresser i februar
- Asia og stillehavsregionen (APNIC) gjekk tom i april
- Her i Europa (RIPE NCC) har me fortsatt nokre adresser igjen
 - Estimert til å i beste fall vare fram til sommaren
- 16,7 millionar adresser er satt av til ein siste rasjoneringsrunde
 - Kvar internettleverandør/organisasjon vil kunne få tildelt éi einskild blokk med 1024 adresser
 - Nye aktørar vil dermed kunne få ein IPv4-smule i framtida
- Skal internett kunne fortsette å vekse trengs det ei radikal endring..

IPv6 to the rescue?

- IPv6-standarden vart publisert i 1998
- Den viktigaste endringa sidan IPv4 er eit markant større adresserom
- Det er andre justeringar og nye funksjonar, men ingen som i seg sjølv er interessante nok til å rettferdiggjere eit bytte
 - Somme påstår at IPv6 har større tryggleik, meir optimal ruting, eller andre fordelar over IPv4 – det stemmer ikkje (lengre)
- IPv6 er essensielt det samme som før, berre mykje meire enn før

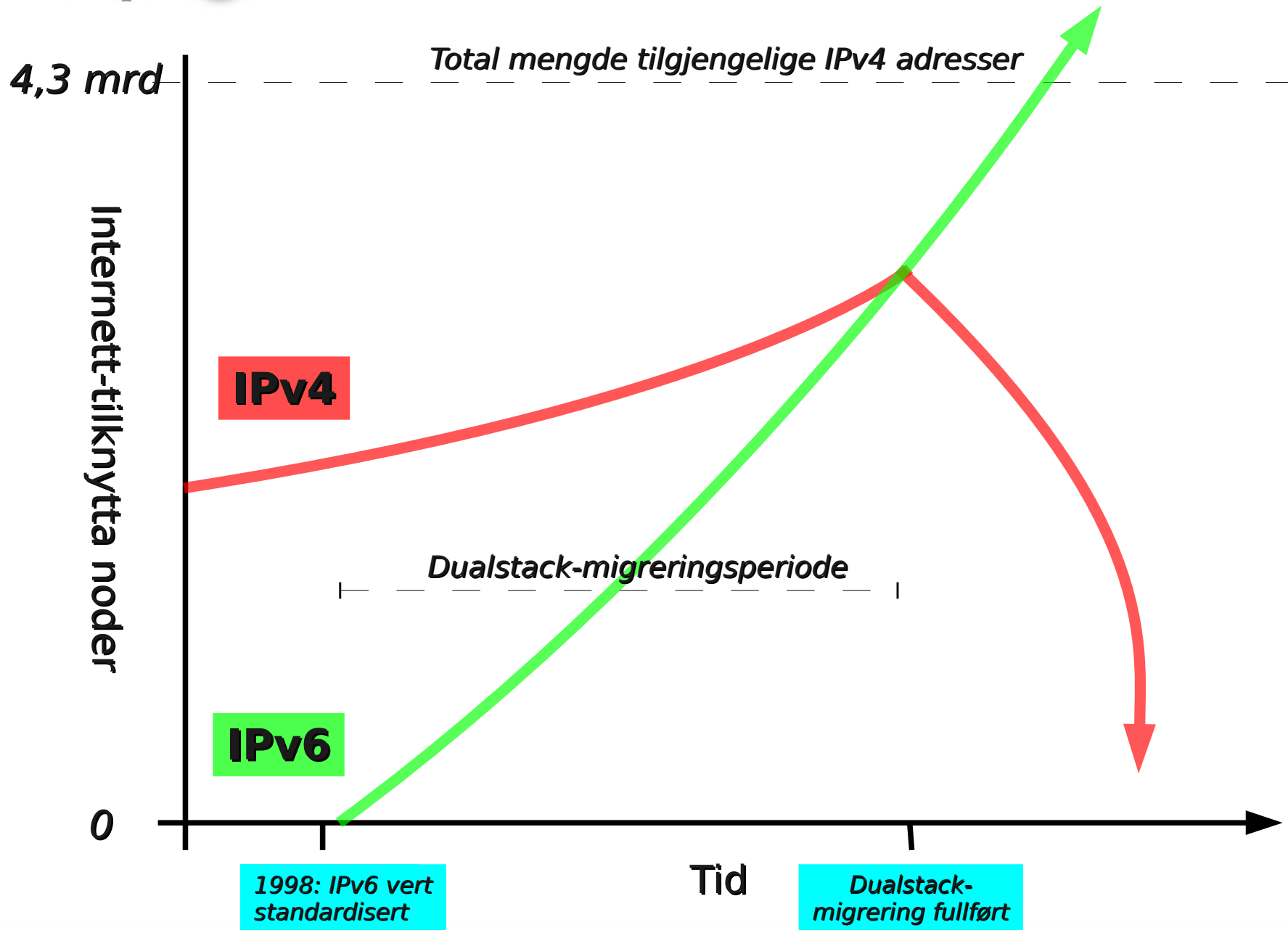
«96 more bits, no magic»

IPv4 vs IPv6 - visualisert

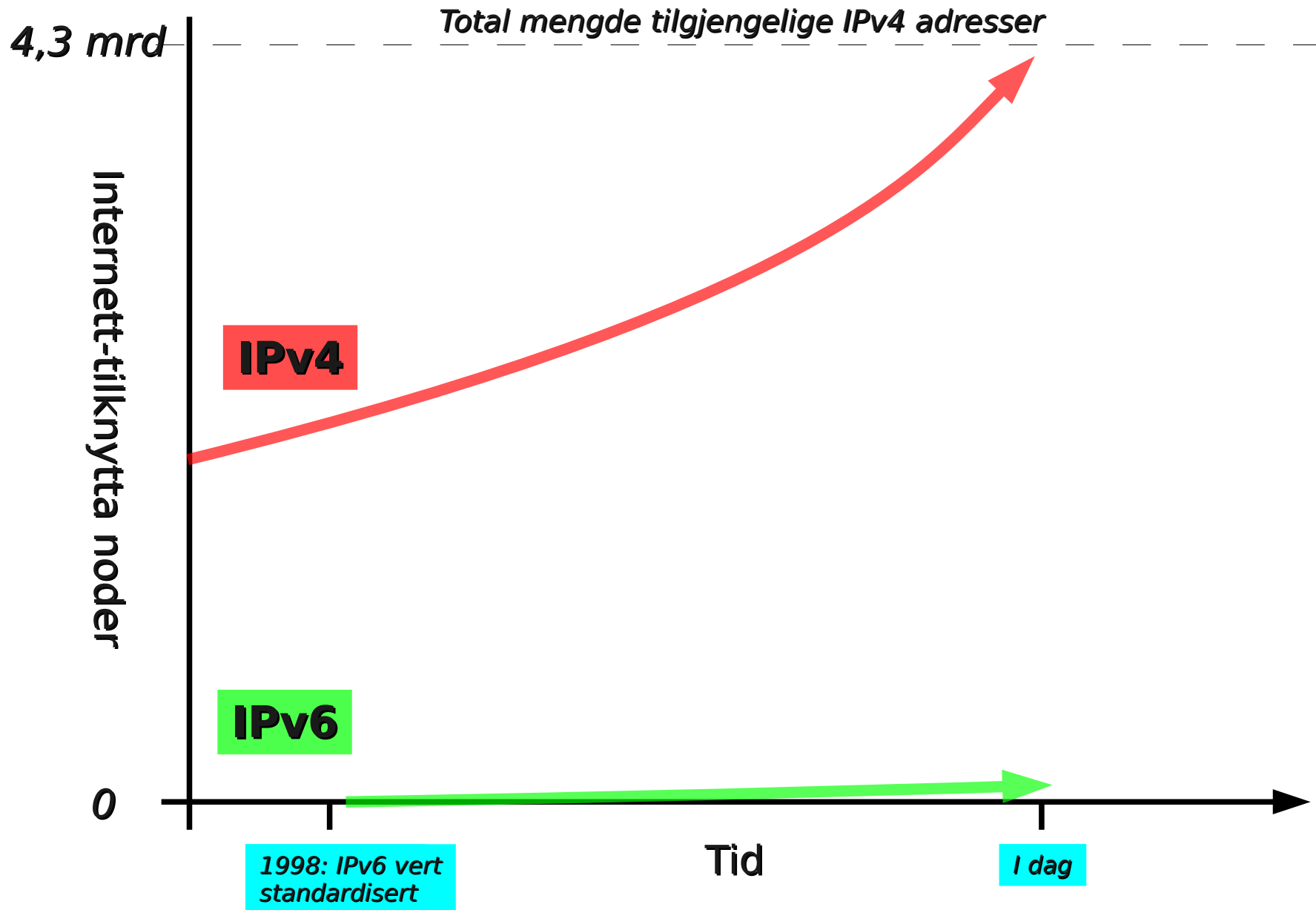


- IPv4 og IPv6 er ikkje direkte kompatible med kvarandre
 - Tenk AM- og FM-radio
 - Eller telefaks og e-post
 - Eller TCP/IP og IPX/SPX
- Protokollane kan sameksistere på det samme fysiske nettverket, men er ikkje klar over kvarandre
- På kort sikt vil IPv6 difor ikkje kunne erstatte IPv4, kun supplere
 - Same prinsippet som når NRK Radio sender både på FM og DAB
 - «*Dualstack*»
- På lengre sikt, når «alle» har IPv6, kan ein skru av IPv4 om ein vil
 - Få radiostasjonar igjen på AM-bandet i dag...

Plan A: Dualstack

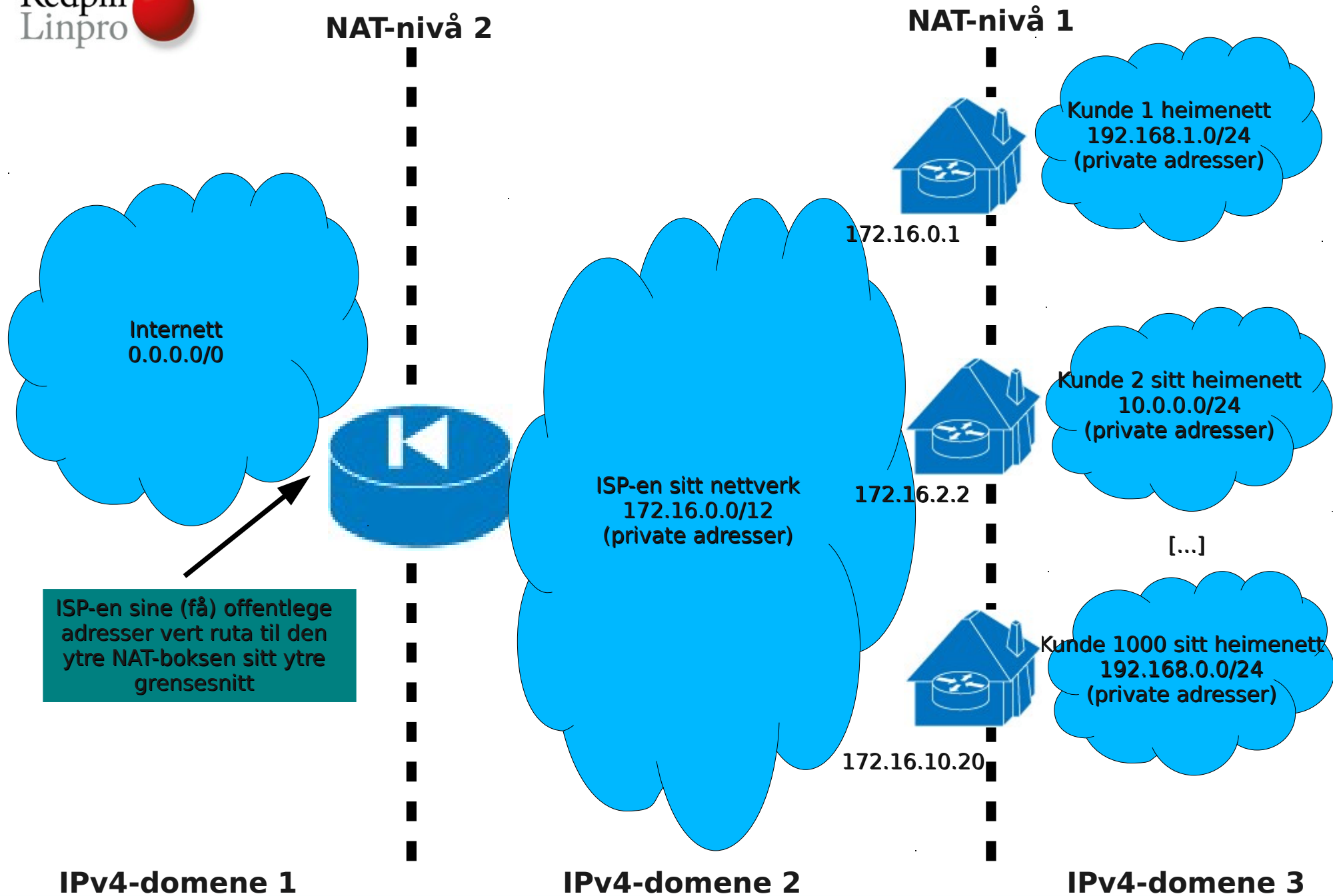


Dualstack-status i dag



Ooops

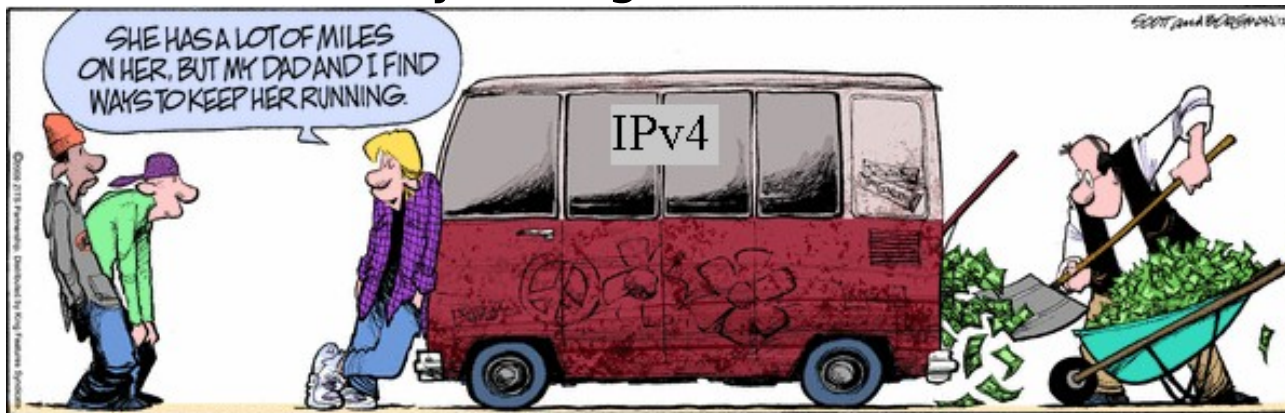
- Det er **for seint** til at IPv6 vil kunne redde internett frå å gå tomt for IPv4-adresser
- IPv4 er fortsatt den dominante protokollen på internett, ca. 99,7% av sluttbrukarane har i dag ikkje IPv6-konnektivitet
- ISP-ane vert difor plent nøydd til å halde liv i IPv4....
 - ...sjølv om dei ikkje har nok adresser til alle kundane sine lengre
- Løysinga: Meire NAT – la kundane dele på IPv4-adressene!
 - Kjend som:
 - CGN – Carrier Grade NAT
 - LSN – Large Scale NAT
 - NAT444 – NAT mellom tre separate IPv4-domener



- Kan samanliknast å ha eit felles «sentralbordnummer» for ei gate, bydel, kommune, leverandør, eller liknande.
 - Ein vil ikkje lengre kunne identifisere einiskilde brukarar ved bruk av IP-adressa deira – korleis handtere abuse?
 - Geo-location vil miste treffsikkerheit
- Dei store sentrale NAT-boksane er kompliserte og **dyre**
 - Dei må halde kontroll på alle aktive sesjonar, i motsetning til vanlege ruterar (som heller ikkje akkurat er billige)
 - Potensiell flaskehals – har de opplevd korleis f.eks. BitTorrent får NAT-funksjonen i ein heimeruter til å sveitte? Skaler opp det problemet til tusenvis av brukarar...
- Ein IPv4-marknad er i ferd med å dukke opp, markedspris for éi IPv4-adresse ligg allereie på ca. US\$12

Nye incentiv for IPv6

- Internett-leverandørane....
 - ...må no **uansett** gjere endringar i nettverka sine
 - ...vil kunne redusere trafikken gjennom dei sentrale NAT-boksane og få den til å minske ytterlegare over tid – dermed unngå dette:

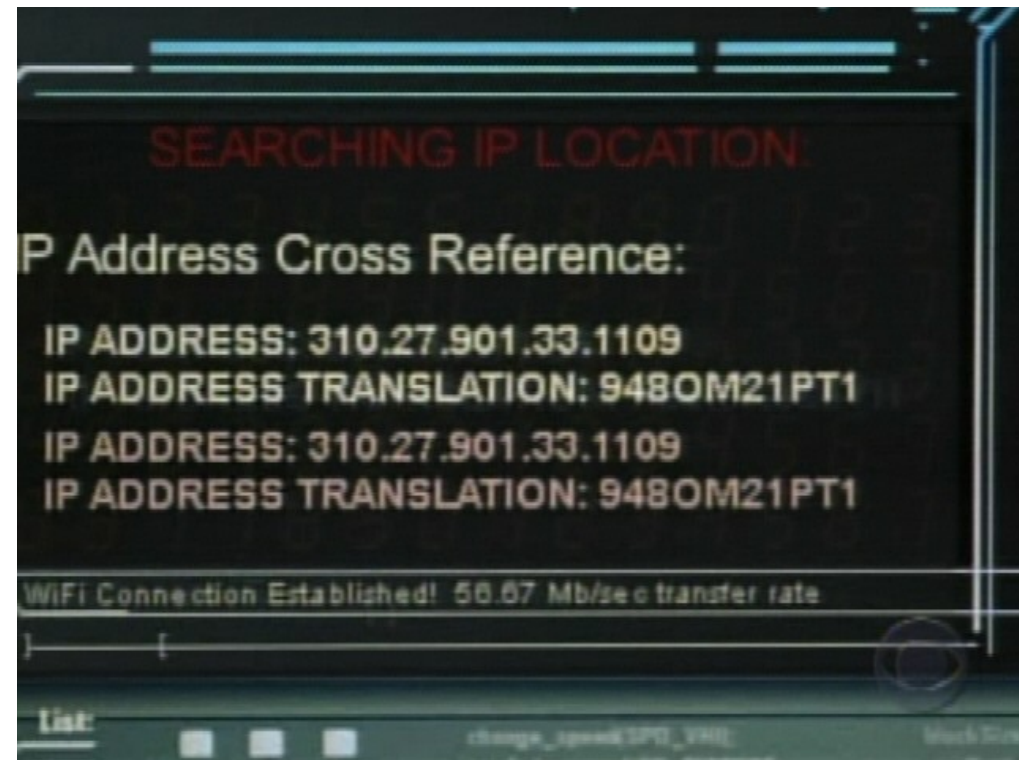
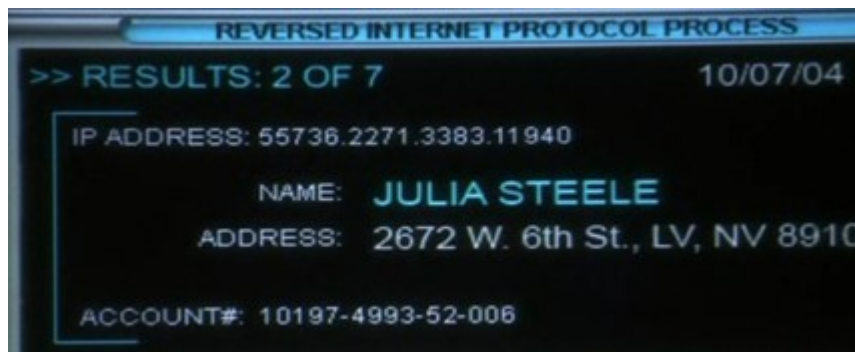
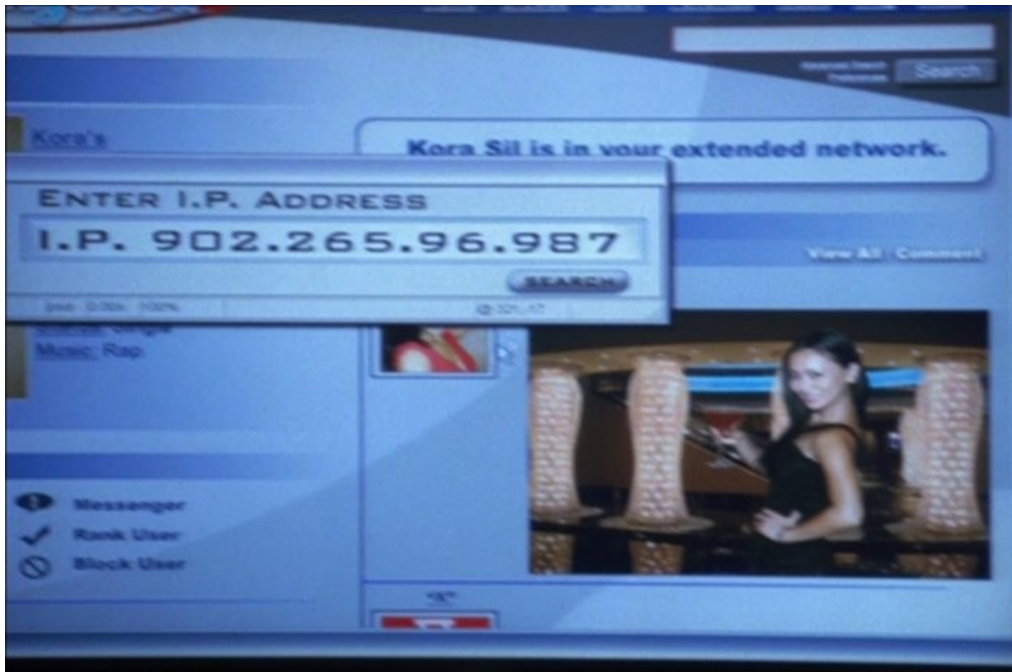


- Innhaldsleverandørane....
 - ...vil kunne sikre seg ei optimal brukaroppleving ved å omgå heile NAT-problematikken knytta til bruk av IPv4
 - ...vil kunne fortsetje å kunne skille sluttbrukarane frå kvarandre

Så kva er IPv5?

...fins kun i *CSI*-seriane. ;-)

Neida.. «IPv5» heiter i grunn *Internet Stream Protocol v2* (sjå RFC 1819), men den vart aldri teke i bruk i nokon grad.



Del 2:
Ei bedrift sine sine
fyrste steg på veien
til IPv6

Myte: «Me har massevis av IPv4-adresser, så me treng ikkje IPv6»

- **FEIL.** Om dei de ynskjer å kommunisere med over internett har problem med sin IPv4-konnektivitet, hjelp det fint lite at de sjølve ikkje har det.

(Faks-maskina dykkar fungerer kanskje perfekt den, men den hjelp dykk fint lite når de skal sende eit dokument til ei bedrift som ikkje har noko faksmaskin.)

Myte: «IPv6 vert fyrst aktuelt mange år fram i tid»

- **FEIL.** Asia/Stillehavsregionen er allereie tomme for IPv4, og Europa vil fylgje etter i løpet av få månader.

Effektane av at me gjeng tomme for IPv4 vil byrje å gjere seg gjeldande i vår del av verda allereie i neste budsjettperiode - Telenor Mobil har varsla at dei er allereie i ferd med å implementere sentralisert NAT for sine kundar.

Samstundes har fleire store norske ISP-ar gjort det klart at dei vil levere IPv6 til privatkundane i løpet av 2012.

Førebuing og kompetansebygging

- Krev IPv6-støtte i alle nyinnkjøp av maskinvare, programvare, og tenester
 - Unngå å ende opp med å måtte skifte ut maskinvare eller programvare før vanleg tidsskjema kun for å få IPv6-støtte
 - Unngå å være låst i ei kontrakt med ein leverandør som ikkje leverar tenestene sine over IPv6
- Sett opp ein liten lab
 - Få konnektivitet frå dykkar ISP, evt. til nøds via tunnelar
 - La nettverksteknikarane få litt hands-on erfaring!

IPv6-adressesyntaks

- 32 heksadesimale siffer, delt opp i åtte grupper à fire siffer

2a02:00c0:1002:0011:0000:0000:0000:0002

- Som i IPv4 kan du forkorte ved å stryke ledande 0-ar i kvar gruppe:

2a02:00c0:1002:0011:0000:0000:0000:0002



2a02:c0:1002:11:0:0:0:2

- Kan bli ytterlegare forkorta ved å trekje saman eit eller fleire samanhengande felt med verdien 0 til eit dobbelt kolon (maks éin gong):

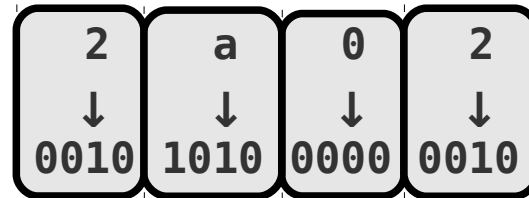
2a02:c0:1002:11:0:0:0:2



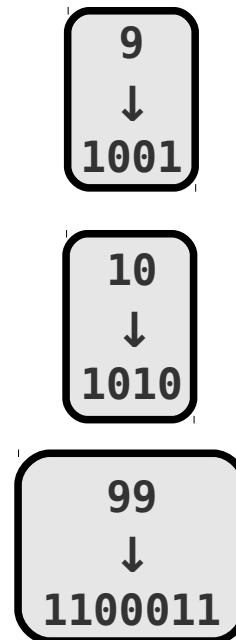
2a02:c0:1002:11::2

Usj, kvifor heksadesimalt?

- **2a02:c0:1002:11::2** vert **42.2.0.192.16.2.0.17.0.0.0.0.0.0.0.2** på «IPv4sk»..
- **Eit hex-siffer gjeng alltid nøyaktig opp i fire bits:**



- **Dette er ikkje tilfelle for desimalt:**



Adresse-planlegging

- Kvar sluttbrukar/organisasjon vil få ein /48 utan dokumentasjon
 - Standard subnett-storleik er /64 (tilnærma likt uendeleg)
 - Gjev 65536 tilgjengelege subnett, eller 16 bits med ruting:

End Site-prefiks (48 bits) 2001:db8:1234:	Ruting (16 bits) :0123:	Host Interface ID (64 bits) :0123:4567:89ab:cdef
---	---------------------------------------	--

- Kvart heksadesimale siffer er fire bits, det er praktisk å tilpasse adresseplana deretter (maks fire nivå)
- Det kan være lurt å reservere mesteparten av plassen til framtidige og reviderte versjonar av adresse-plana

Eksempel 1: organisasjonshierarki

End Site-prefiks (48 bits) 2001:db8:1234:	Ruting (16 bits) :1234:	Host Interface ID (64 bits) :0123:4567:89ab:cdef
---	-------------------------------	--

- Siffer 1 (4 bits): Adresseplan-versjon (1 – fyrste versjon)
- Siffer 2 (4 bits): Bygning/lokasjon (2 – hovudkontoret)
- Siffer 3 (4 bits): Avdeling/funksjon (3 – datasenteret)
- Siffer 4 (4 bits): Nettverk (4 – ytre e-posttenarar)

Ankepunkt: Kanskje 4 bits (16 kombinasjonar) gjev for få tilgjengelege nettverk i datasenteret?

Eksempel 1: organisasjonshierarki

End Site-prefiks (48 bits) 2001:db8:1234:	Ruting (16 bits) :1234:	Host Interface ID (64 bits) :0123:4567:89ab:cdef
--	--	---

- Siffer 1 (4 bits): Adresseplan-versjon (1 – fyrste versjon)
- Siffer 2 (4 bits): Bygning/lokasjon (2 – hovudkontoret)
- Siffer 3 (4 bits): Avdeling/funksjon (3 – datasenteret)
- Siffer 4 (4 bits): Nettverk (4 – ytre e-posttenarar)

Ankepunkt: Kanskje 4 bits (16 kombinasjonar) gjev for få tilgjengelege nettverk i datasenteret?

Eksempel 2: VLAN-mapping

End Site-prefiks (48 bits) 2001:db8:1234:	Ruting (16 bits) :2345:	Host Interface ID (64 bits) :0123:4567:89ab:cdef
---	-------------------------------	--

- Siffer 1 (4 bits): Adresseplan-versjon (2 – andre versjon)
- Siffer 2-4 (12 bits): VLAN-tag 0x345, dvs. VLAN 837

Ankepunkt: Kva om ein har overlappende VLAN i to forskjellige lokasjonar, eller nettverk som ikkje har ein eigen VLAN-tag?

PA eller PI?

- I IPv4 er fylgjande modell vanleg:
 - Interne nettverk har private adresser, skjult med NAT
 - Ei lita mengde offentlege adresser PA-adresser (eigd av ISP-en) vert brukt for NAT-boksen sitt internett-grensesnitt, pluss offentlege tenester (web, mail, etc.)
 - Dette gjer ein relativt ISP-uavhengig, då mengda utstyr som er direkte avhengig av ISP-en sine adresser er begrensa
- I IPv6 derimot vil som hovudregel alle maskiner få offentlege adresser, og det er dermed ikkje behov for NAT
 - Dette gjev dog ei langt sterkare ISP-tilknytning enn i IPv4
- Det er difor verd å vurdere å skaffe seg sin eigen PI /48 frå dag 1
 - Krevjer dog p.t. multihoming (mogleg dette endrast snart)

- Start ytterst, beveg deg innover i nettverket, og aktiver IPv6 parallelt med IPv4 på kvar link og teneste ein kjem forbi
 - 1) Internett-oppkoplinga(ne) og ruter(ane) dei er kopla i
 - 2) Essensielle nettverkstenester (DNS-resolverar, NTP, osv.)
- Teknikarane sine arbeidsstasjonar – viktig for å kunne teste
- Offentleg tilgjengelege tenester er ofte lavthengande frukter, som er bra å få tilgjengeleg over IPv6 tidleg (før sluttbrukarar med problematisk/NAT-a IPv4-konnektivitet byrjar å dukke opp)
 - Organisasjonen sine heimesider og e-postmottak, for eksempel
- Øvrige kontor-nettverk og interne tenester kan kome til slutt...

Applikasjonsutvikling

- Dei aller fleste moderne programmeringsspråk har socket-bibliotek/APIs som oppfører seg identisk uavhengig av kva IP-versjon dei jobbar med
 - F.eks. `getaddrinfo()` vs. `gethostbyname()`
 - Eigenutvikla applikasjonar vil difor ofte fungere fint med IPv6
- Ein må imidlertid passe på å ta høgde for IPv6 når ein manipulerar IP-adresser
 - Database-kolonner definert som `VARCHAR(15)` vil fungere dårleg
 - Unngå hardkoding av IP-adresser i applikasjonar
- Eksplisitt inkludere IPv6 i standard test- og QA-rutiner

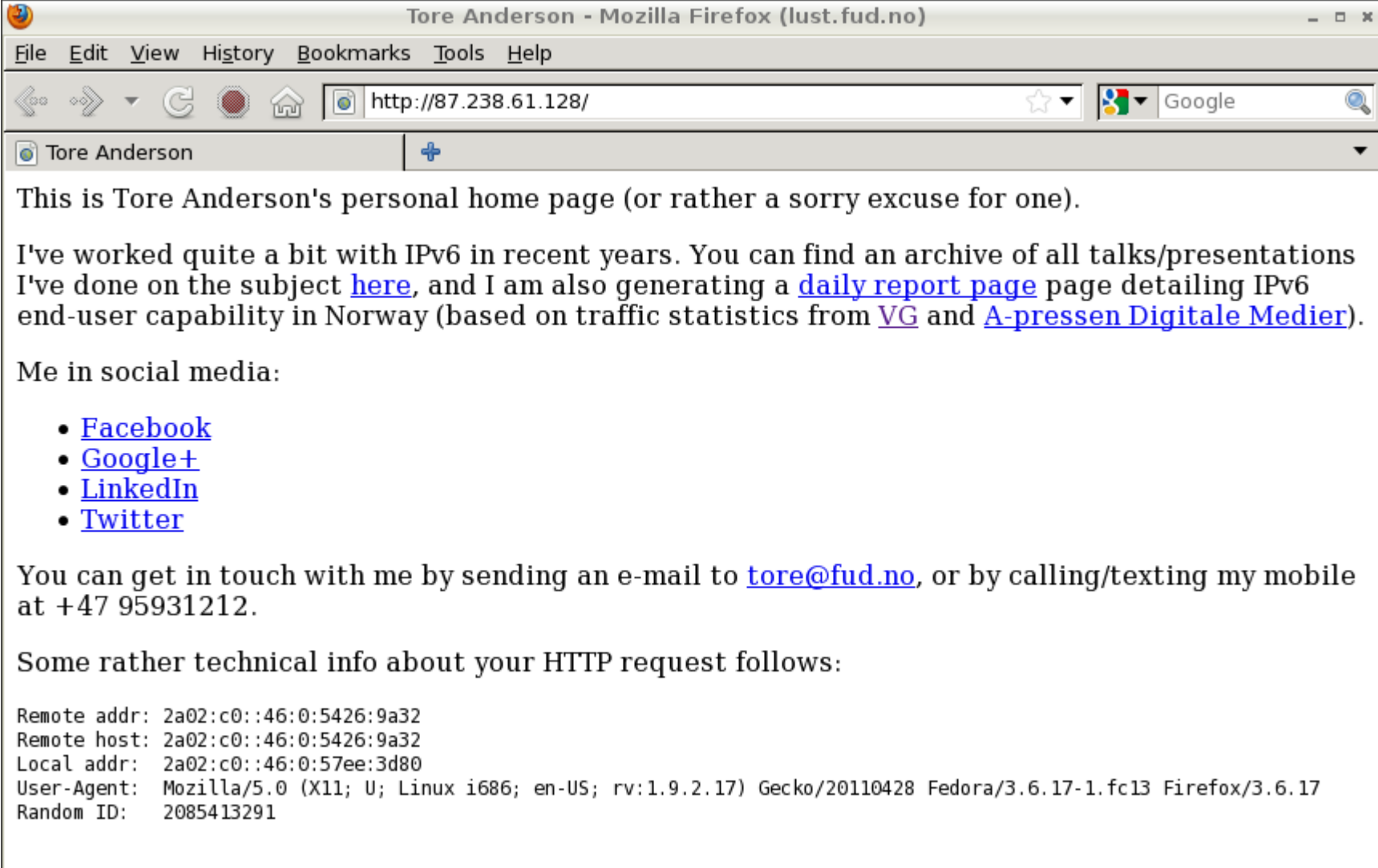
SLAAC

- Stateless Address AutoConfiguration
- Den mest synlege nyvinninga i IPv6 (sett vekk ifrå adresserom)
- Ein ruter kan periodisk sende ut **Router Advertisements** til eit LAN, som seier f.eks. «eg er ein ruter, og på dette nettverket fins prefikset 2001:db8:1:2::/64, og DNS-tenaren er 2001:db8::53»
- Ein host vil då automatisk finne seg ei ledig adresse i nettet og konfigurere opp alt den treng for å kome seg på nett
- Dette gjer at ein ikkje treng DHCP i IPv6 for enkle plug'n'play nett
- Ulempa er at ein ikkje har sentralisert kontroll på kva maskiner har kva for nokre adresser
 - DHCPv6 fins dog, og fungerer stort sett likt som i IPv4

Skru av IPv4 etter kvart?

- Å drifte IPv4 og IPv6 i parallel er meire jobb enn å drifte ein av dei
 - Fleire ting å overvake, fleire brannveggreglar å skrive, fleire ting å feilsøke, fleire ting å teste for når ein utviklar, fleire ting å...
- Det fins teknologiar som gjer ein i stand til å køyre IPv6-only nettverk men likvel ha konnektivitet mot IPv4-internettet
 - NAT64+DNS64 for IPv6-only klientar, f.eks. eit kontor-LAN
 - SIIT for IPv6-only tenarar som skal nåast frå IPv4-only klientar
- Det er enklare å køyre IPv6-only med oversetting, enn omvendt
 - Heile IPv4-adresserommet kan lett mappast inn i IPv6!

Stateless IP/ICMP Translation i praksis



Tore Anderson - Mozilla Firefox (lust.fud.no)

File Edit View History Bookmarks Tools Help

http://87.238.61.128/ Google

Tore Anderson

This is Tore Anderson's personal home page (or rather a sorry excuse for one).

I've worked quite a bit with IPv6 in recent years. You can find an archive of all talks/presentations I've done on the subject [here](#), and I am also generating a [daily report page](#) detailing IPv6 end-user capability in Norway (based on traffic statistics from [VG](#) and [A-pressen Digitale Medier](#)).

Me in social media:

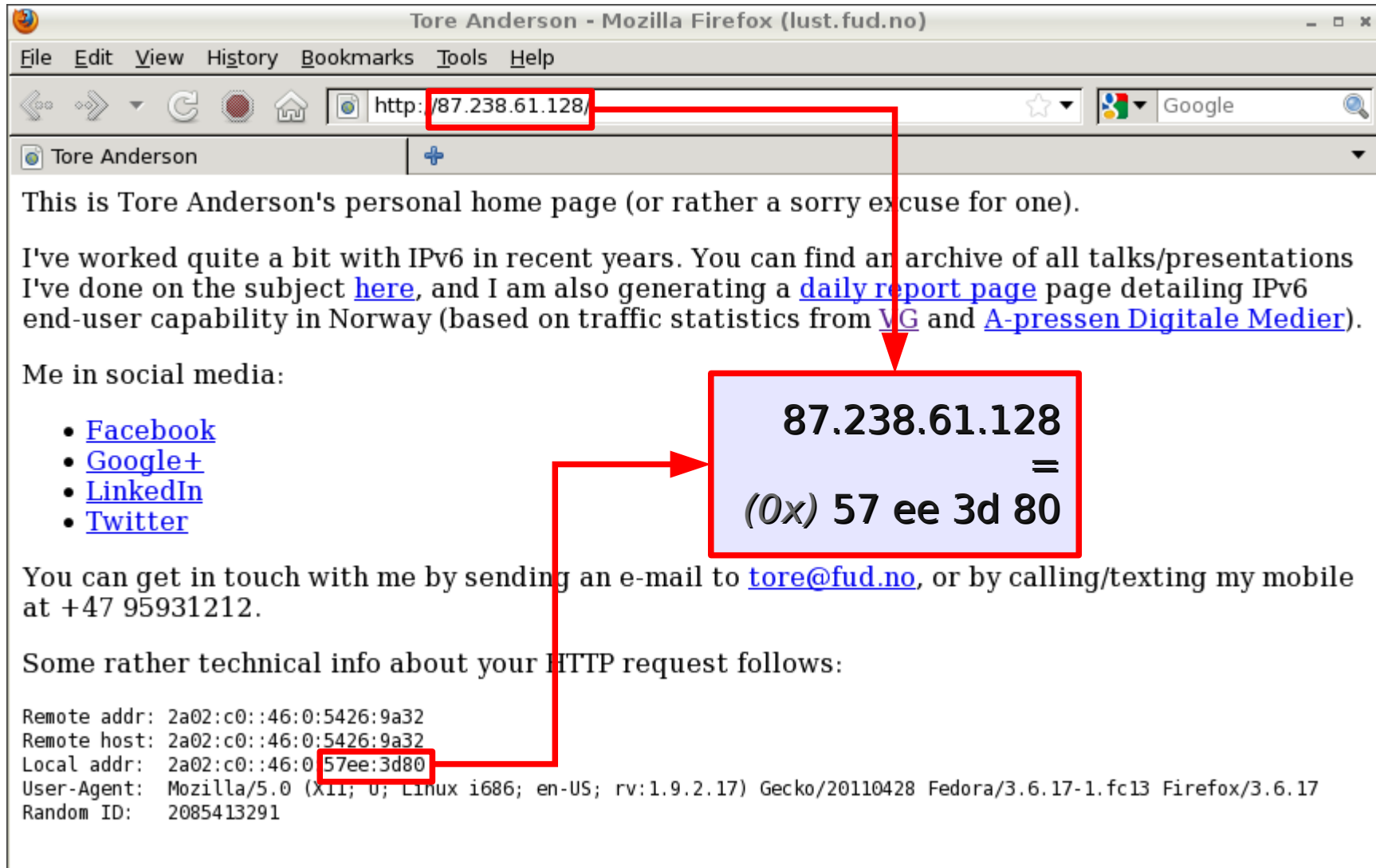
- [Facebook](#)
- [Google+](#)
- [LinkedIn](#)
- [Twitter](#)

You can get in touch with me by sending an e-mail to tore@fud.no, or by calling/texting my mobile at +47 95931212.

Some rather technical info about your HTTP request follows:

```
Remote addr: 2a02:c0::46:0:5426:9a32
Remote host: 2a02:c0::46:0:5426:9a32
Local addr: 2a02:c0::46:0:57ee:3d80
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110428 Fedora/3.6.17-1.fc13 Firefox/3.6.17
Random ID: 2085413291
```

Stateless IP/ICMP Translation i praksis



Tore Anderson - Mozilla Firefox (lust.fud.no)

File Edit View History Bookmarks Tools Help

http://87.238.61.128/

Tore Anderson

This is Tore Anderson's personal home page (or rather a sorry excuse for one).

I've worked quite a bit with IPv6 in recent years. You can find an archive of all talks/presentations I've done on the subject [here](#), and I am also generating a [daily report page](#) detailing IPv6 end-user capability in Norway (based on traffic statistics from VG and [A-pressen Digitale Medier](#)).

Me in social media:

- [Facebook](#)
- [Google+](#)
- [LinkedIn](#)
- [Twitter](#)

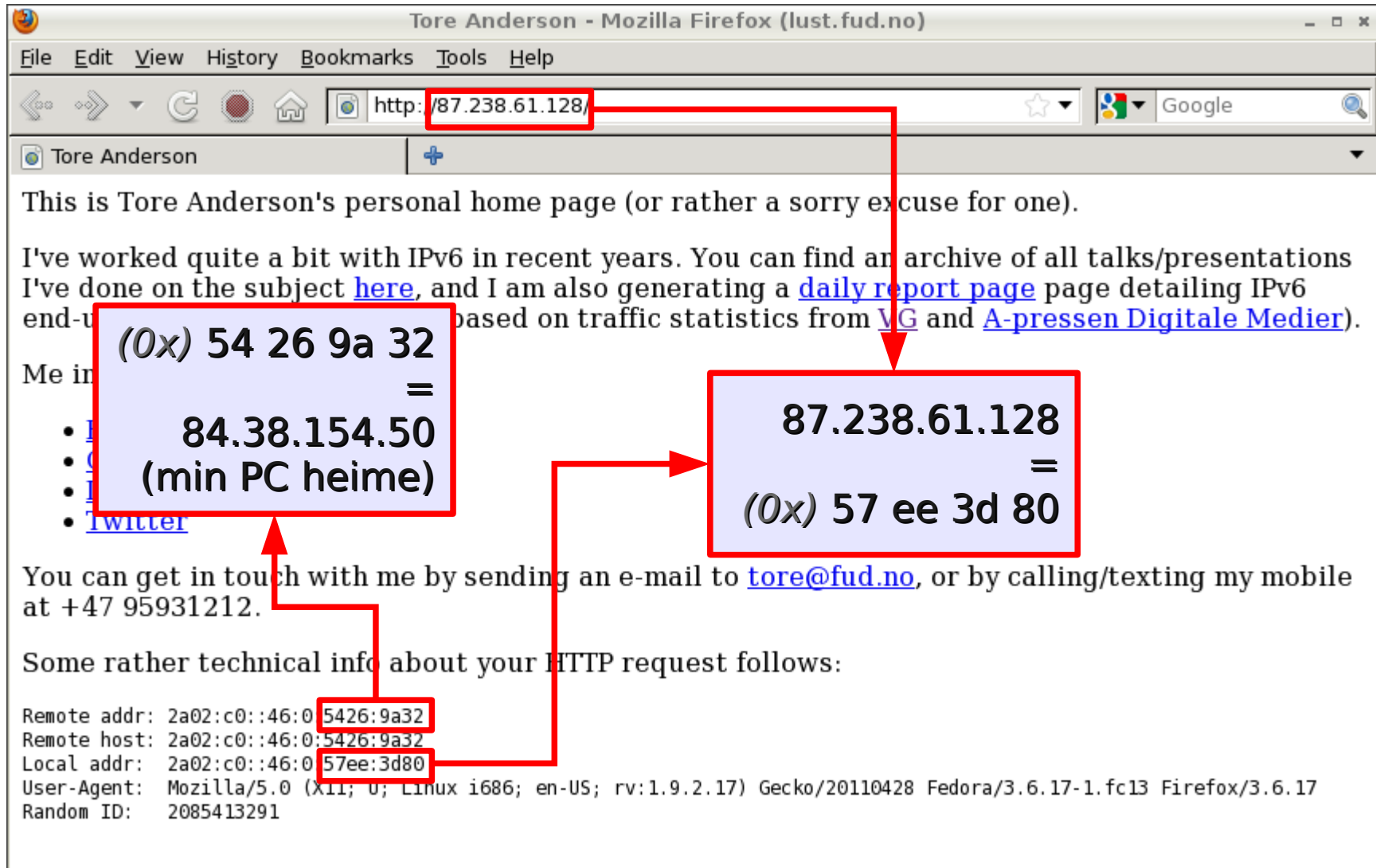
You can get in touch with me by sending an e-mail to tore@fud.no, or by calling/texting my mobile at +47 95931212.

Some rather technical info about your HTTP request follows:

```
Remote addr: 2a02:c0::46:0:5426:9a32
Remote host: 2a02:c0::46:0:5426:9a32
Local addr: 2a02:c0::46:0:57ee:3d80
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110428 Fedora/3.6.17-1.fc13 Firefox/3.6.17
Random ID: 2085413291
```

87.238.61.128
=
(0x) 57 ee 3d 80

Stateless IP/ICMP Translation i praksis



Tore Anderson - Mozilla Firefox (lust.fud.no)

File Edit View History Bookmarks Tools Help

http://87.238.61.128/

Tore Anderson

This is Tore Anderson's personal home page (or rather a sorry excuse for one).

I've worked quite a bit with IPv6 in recent years. You can find an archive of all talks/presentations I've done on the subject [here](#), and I am also generating a [daily report page](#) detailing IPv6 end-user activity (based on traffic statistics from VG and [A-pressen Digitale Medier](#)).

Me in

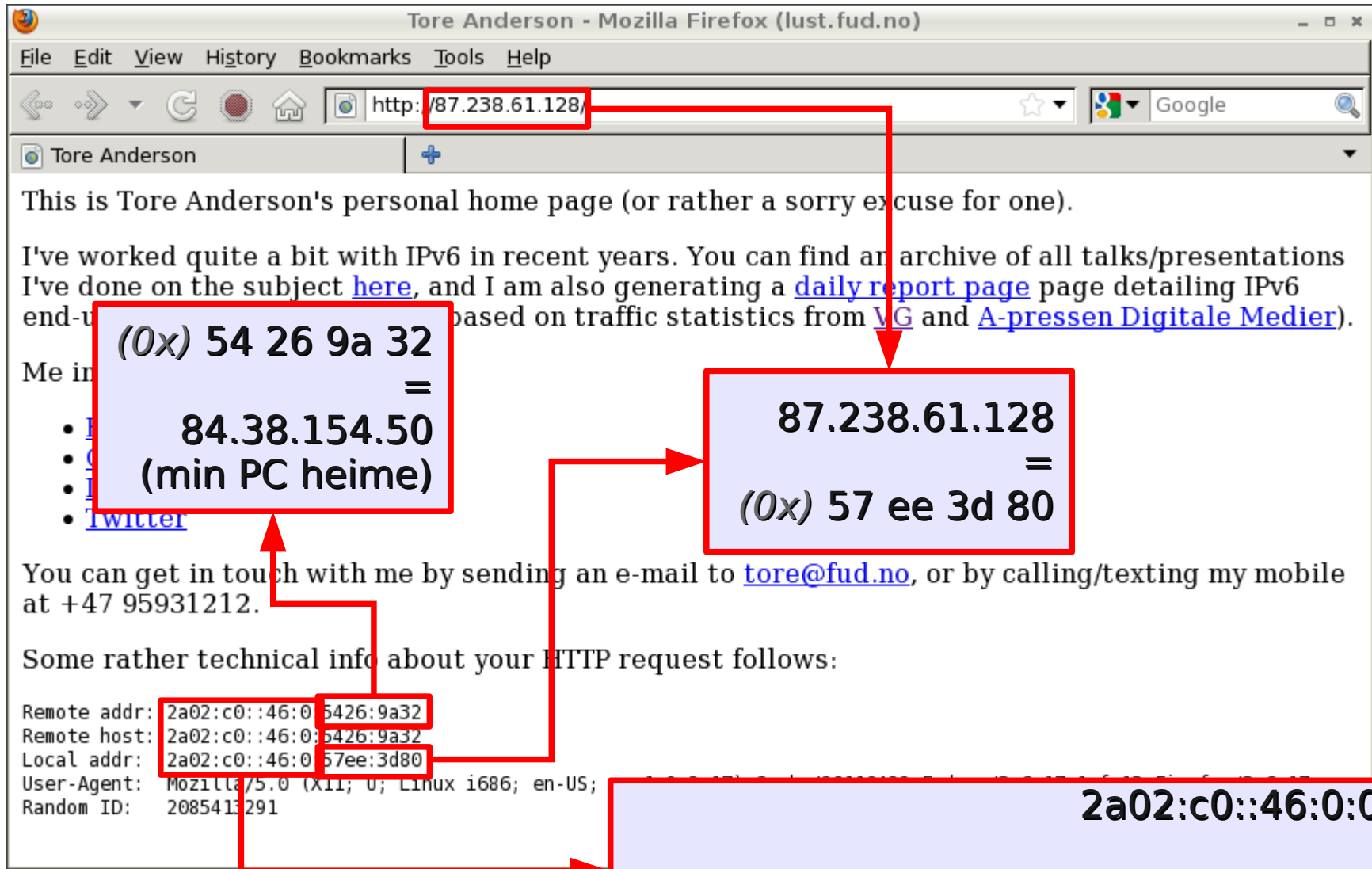
- [...](#)
- [...](#)
- [Twitter](#)

You can get in touch with me by sending an e-mail to tore@fud.no, or by calling/texting my mobile at +47 95931212.

Some rather technical info about your HTTP request follows:

```
Remote addr: 2a02:c0::46:0:5426:9a32
Remote host: 2a02:c0::46:0:5426:9a32
Local addr: 2a02:c0::46:0:57ee:3d80
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110428 Fedora/3.6.17-1.fc13 Firefox/3.6.17
Random ID: 2085413291
```

Stateless IP/ICMP Translation i praksis



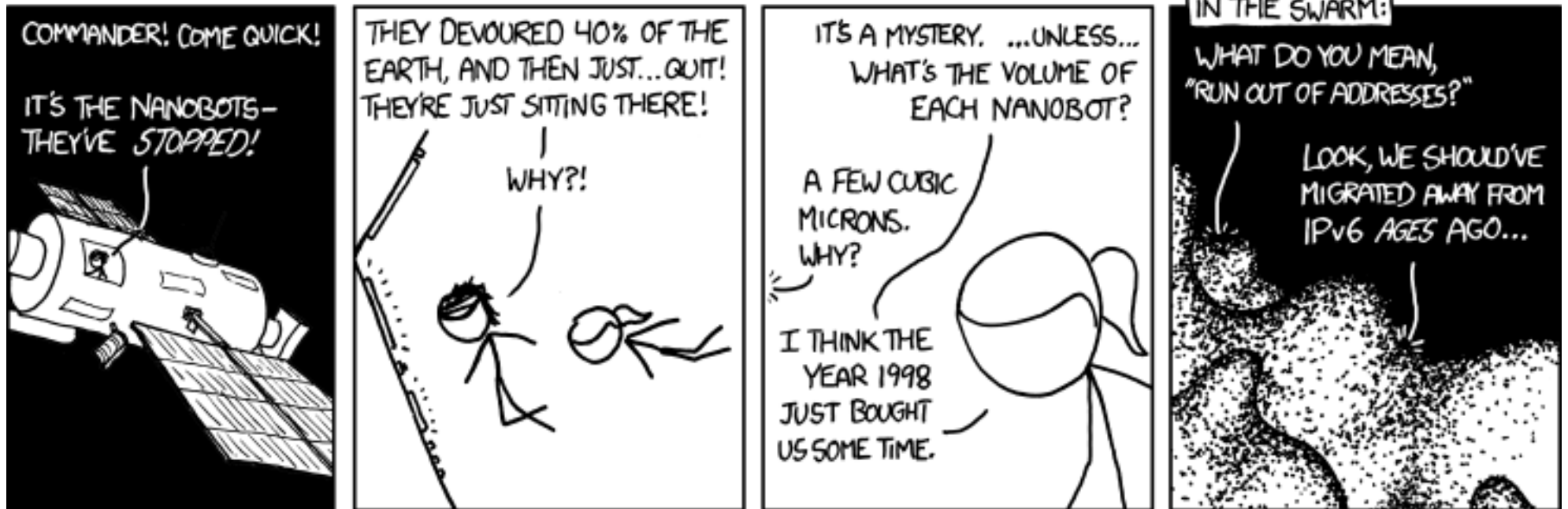
The screenshot shows a Mozilla Firefox browser window titled "Tore Anderson - Mozilla Firefox (lust.fud.no)". The address bar contains "http://87.238.61.128/". The page content includes a personal home page introduction and technical details about an HTTP request. Red boxes and arrows highlight the mapping between IPv4 and IPv6 addresses:

- Address bar: `http://87.238.61.128/`
- Technical details: Remote addr: `2a02:c0::46:0:5426:9a32`, Remote host: `2a02:c0::46:0:5426:9a32`, Local addr: `2a02:c0::46:0:57ee:3d80`
- Mapping boxes:
 - Box 1: `(0x) 54 26 9a 32 = 84.38.154.50 (min PC heime)`
 - Box 2: `87.238.61.128 = (0x) 57 ee 3d 80`
 - Box 3: `2a02:c0::46:0:0:0/96 = 0.0.0.0/0 (heile IPv4-adresserommet mappa inn i IPv6)`

NAT64+DNS64

- DNS64 genererer IPv6-adresser for IPv4-only hostnamn ved å leggje til eit prekonfigurert prefiks:
 - 1) Klient spør DNS: Kva er IPv6-adressa for “v4-only.no”?
 - 2) v4-only.no har kun ei IPv4-adresse, f.eks. 1.2.3.4
 - 3) DNS svarar klient: IPv6-adressa til “v4-only.no” er:
2a02:c0::46:0:**0102:0304**
- Dette prefikset vert så oversatt til IPv4 av ein NAT64-boks
 - Brukar same algoritme som SIIT
 - Stateful operasjon (tilsvarande NAT44)
 - I motsetning til NAT44, treng ikkje NAT64-boksen å stå midt mellom klient og internett (ein rutar berre 2a02:c0::46:0:0:0/96 til den på heilt vanleg vis)

Vil me gå tom for IPv6-adresser?



Del 3: Teknisk gjennomgong

96 nye bits, kva anna er nytt?

- Nytt adresse-syntaks og DNS-ressursar
- Link-lokale adresser
- Innebygd multicast (IPv4 broadcast har blitt fjerna)
- ICMP har blitt utvida (ersttar m.a. IPv4 ARP)
- Slanka og meir fleksibel protokoll-header
- Fragmentering vert kun gjort av ende-noder, aldri ruterar
- Nye metodar for auto-konfigurasjon (ICMPv6/DHCPv6)
- Levetid på adresser, ruterar, og liknande
- Standard subnett-storleik på 64 bits (tilnærma likt uendeleg)
- Ikkje behov for NAT – kvar sluttbrukar får minst eit /64-subnett, antageleg langt fleire (/56 eller /48 – hhv. 256 eller 65536 /64-ar)

IPv6-syntaks, del 2

- Ny **AAAA** DNS-ressurs for vanlege oppslag:

*www.redpill-linpro.com. IN **AAAA** 2a02:c0:1002:11::2*

- Nytt **ip6.arpa.**--domene for revers-oppslag:

*2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.0.0.2.0.0.1.0.c.0.0.2.0.a.2.**ip6.arpa.**
IN PTR *www.redpill-linpro.com.**

- Må ha klammeparantes rundt seg i URI-ar:

*https://[**2a02:c0:1002:11::2**]:443/*

- Eit subnett eller eit prefiks visast med prefikslengde i bits:

2a02:c0:1002::/48

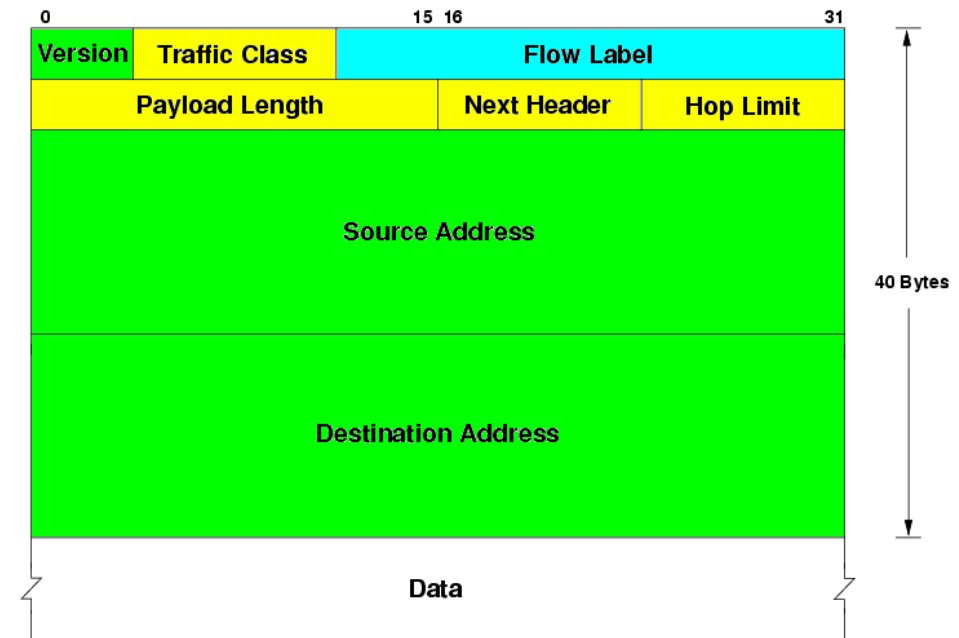
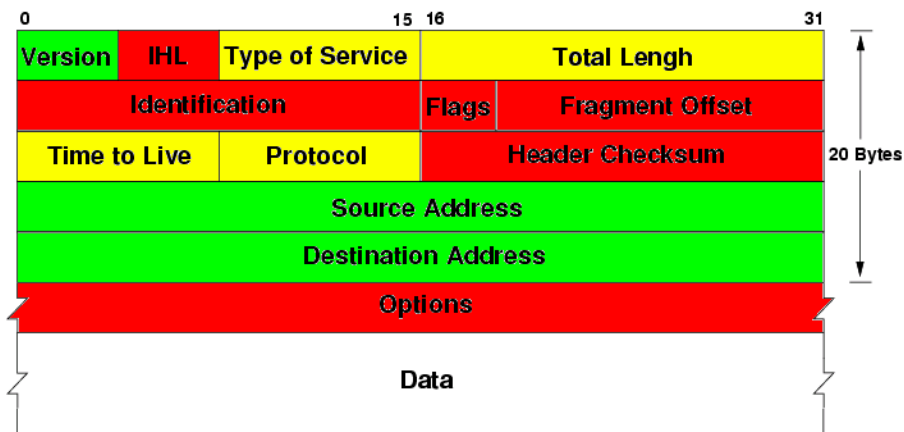
- Nettverksgrensesnittet kan bli eksplisitt oppgjeve etter prosent:

fe80::1234:abcd%eth0

Andre nemneverdige ting

- IPv6-ruterar kan **ikkje** fragmentere
 - Pass på å ikkje brekke Path MTU Discovery
 - Unngå bruk av IPv6-i-IPv4-tunnelar til produksjonsformål
- Du (og dine evt. kundar) får massevis av adresser
 - Sluttbrukarar får opp t.o.m. ein /48 (16K /64-subnett) utan å måtte dokumentere noko behov - «one size fits all»
 - /32 er den minste tildelinga ein ISP/LIR kan få frå RIPE NCC
 - Inneheld 16,7M /56-ar, eller 64K /48-ar
 - RIPE NCC sett av plass slik at tildelinga kan vekse til ein /29
 - Mindre BGP-rutingtabell pga. færre ruter per ISP?

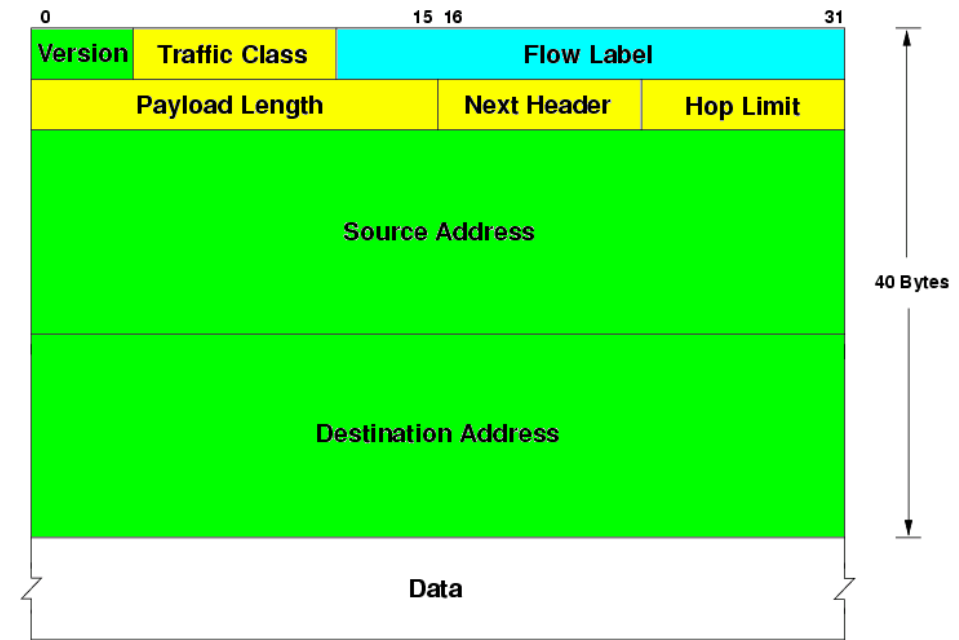
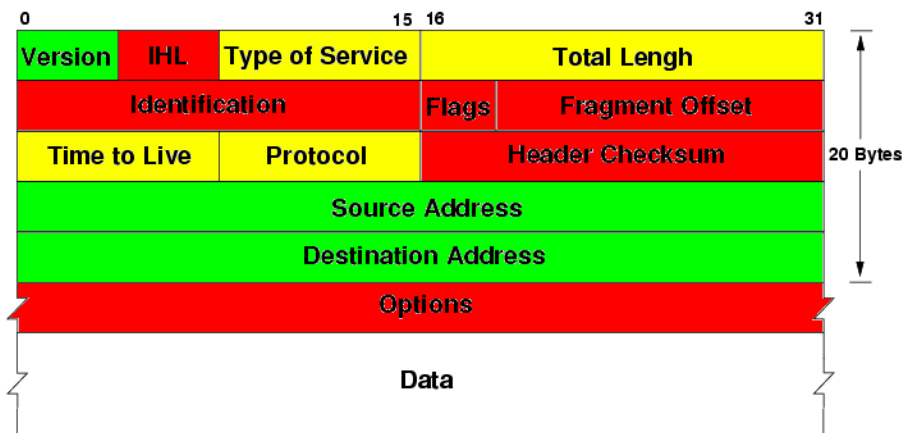
IPv4/IPv6-samanlikning



Grøn: Uendra felt
 Gul: Omdøpt eller endra felt
 Raud: Fjerna frå IPv6
 Turkis: Nytt i IPv6

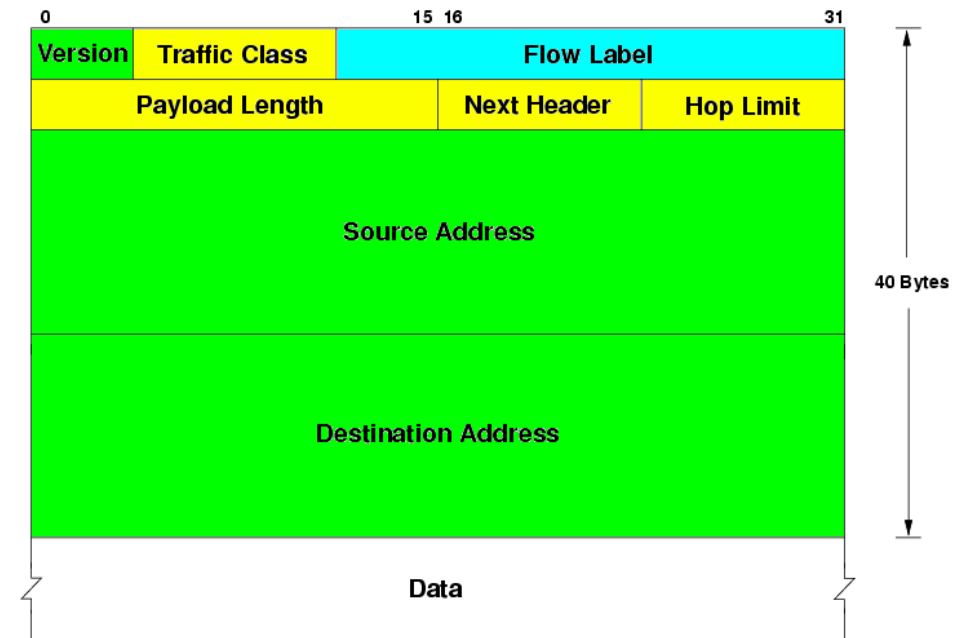
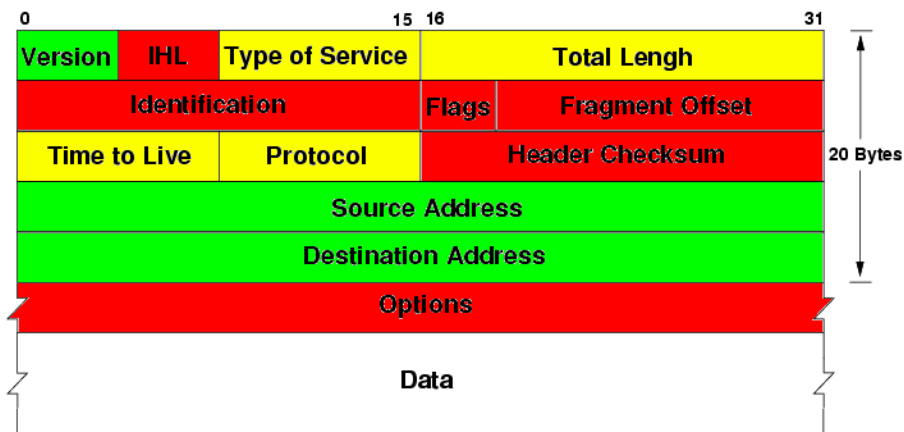
- Felta **Version** og **Source/Destination Address** er uendra
- Det (valgfrie) **Options**-feltet har blitt fjerna frå IPv6
- **Internet Header Length** har blitt fjerna, då ein IPv6-header er alltid 40 bytes
- **Header Checksum** har blitt fjerna frå IPv6

IPv4/IPv6-samanlikning



Grøn: Uendra felt
 Gul: Omdøpt eller endra felt
 Raud: Fjerna frå IPv6
 Turkis: Nytt i IPv6

- Dei tre felta som har med fragmentering å gjere (**Identification**, **Flags**, and **Fragment Offset**) har blitt fjerna frå IPv6
- **Type of Service** har blitt omdøpt til **Traffic Class**; bruken er dog uendra (dei seks første bitsa er DiffServ/DSCP, dei to siste ECN)
- **Time to Live** har blitt omdøpt til **Hop Limit**; inga endring i bruk



Grøn: Uendra felt
 Gul: Omdøpt eller endra felt
 Raud: Fjerna frå IPv6
 Turkis: Nytt i IPv6

- **Total Length** har blitt omdøpt til **Payload Length**; og verdien inkluderar ikkje lengre storleiken på sjølve IP-headeren
- **Protocol** har blitt omdøpt til **Next Header**; og kan no indikere at det fins ein **IPv6 Extension Header**
- **Flow Label** er eit nytt felt som er meint å brukast til å identifisere individuelle forbindelsar/strømmer, f.eks. for lastbalanseringsformål

Velkjende IPv6-prefiks

- `::/0` - defaultruta (tilsvarande 0.0.0.0/0)
- `::/128` - den uspesifiserte adressa (tilsvarande 0.0.0.0/32)
- `::1/128` - loopback-adressa (tilsvarande 127.0.0.1/32)
- `::/96` - IPv4-kompatible adresser (f.eks. `::192.0.2.1/128`). **DEPRECATED.**
- `::ffff:0:0/96` - IPv4-mapped adresser (f.eks. `::ffff:192.0.2.1/128`). Kun brukt internt av applikasjonar som brukar IPv6-systemkall for å kommunisere med IPv4-hostar.
- `2000::/3` - Globale unicast-adresser (IANA til RIR-tildelingar er gjort frå dette prefikset)
 - `2001:0::/32` - Teredo (automatisk IPv6-i-IPv4-tunnelering)
 - `2001:10::/28` - ORCHID – Overlay Routable Cryptographic Hash IDentifiers
 - `2001:db8::/32` - Til bruk i dokumentasjon (tilsvarande to 192.0.2.0/24)
 - `2002::/16` - 6to4 (automatisk IPv6-i-IPv4-tunnelering)
- `3ffe::/16` - 6BONE v2 (eksperimentelt tunnelert IPv6-i-IPv4-nettverk). **DEPRECATED.**
- `5f00::/8` - 6BONE v1 (eksperimentelt tunnelert IPv6-i-IPv4-nettverk). **DEPRECATED.**
- `fc00::/7` - Unique Local Addresses (tilsvarande 10.0.0.0/8, 172.16.0.0/12, og 192.168.0.0/16). Skal ikkje opptre på internett
- `fe80::/10` - Link-lkal unicast (tilsvarande 169.254.0.0/16). Skal ikkje opptre på internett.
- `ff00::/8` - Multicast (tilsvarande 224.0.0/4). Bits 9-12 inneheld flagg, 13-16 definerar skop.
 - Fleire under-inndelingar, mellom andre:
 - `ff02::/16` - Link-lokal multicast (tilsvarande 224.0.0.0/24)
 - `ff05::/16` - Site-local multicast
 - `ff0e::/16` - Global multicast

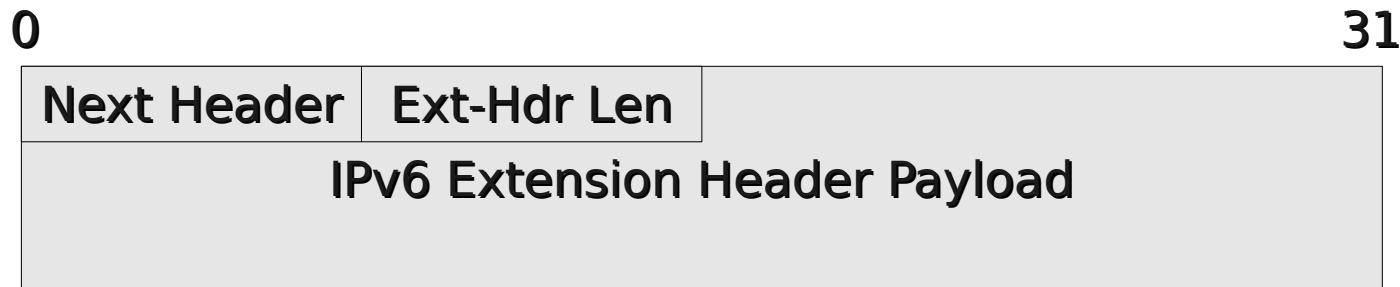
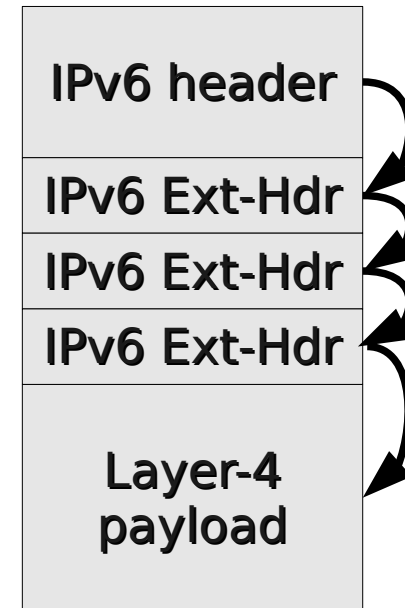
- Tilsvarande RFC 1918 private adresser, berre langt større
 - fc00::/8 er reservert for framtidig bruk
 - fd00::/8 er definert til lokal bruk:

fd	Tilfeldig generert ID (40 bits)	Sluttbrukaren sitt adresserom (80 bits; ein /48, eller 64k subnett)
----	------------------------------------	--

- Bitsa 9-48 er definert til å være tilfeldige, for å unngå kollisjonar
- Kan gje stabile interne adresser på eit LAN sjølv om det ISP-tildelte prefikset endrar seg eller om internett-linja gjeng ned
- Operativsystem skil generelt sett ikkje mellom ULAs og GUAs
 - Om ein host har kun ULA-adresser, og ei default-rute, vil denne generelt verte foretrukke framfor bruk av IPv4
 - Resulterar i timeouts og ein trist brukaropplevelse

IPv6 Extension Headers

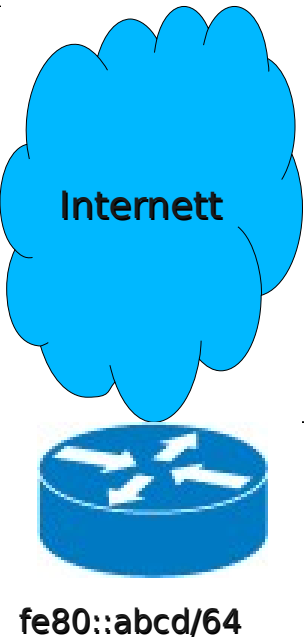
- **Next Header-feltet** kan innehalde eit protokoll-nummer som er tildelt ein **IPv6 Extension Header** i staden for ein lag-4 protokoll som f.eks. TCP eller UDP
- En Extension Header byrjar alltid meit eit nytt **Next Header-felt**, fulgt av eit **Length-felt**, og deretter innhaldet i Extension Headeren.
- Fleire Extension Headers kan opptre i ei IPv6-pakke, i så fall lagar dannar dei ei kjede



IPv6 extension headers

- Vert kun proessert av endenodene, unntekte **Hop-by-Hop** extension headeren (Next Header = 0), denne **MÅ** være fyrst i ei evt. kjede
 - Hop-by-Hop header vert proessert i control plane – slow path
- Nokre eksempel på definerte IPv6 Extension Headers:
 - IPSEC (AH og ESP som i IPv4)
 - Fragmentering
 - Mobile IPv6
- Dei vanskeleggjer filtrering/brannvegging av IPv6-pakkar:
 - Vanskeleg å vite kor lag-4-data (TCP/UDP) byrjar, då ein må fylgje heile kjeda av extension headers til slutten
 - Aksesslister som inspiserar lag-4 protokollar fungererar ikkje alltid når extension headers fins (maskinvare-avhengig)

IPv6-initialiseringsprosess





Konfigurere link-lokale adresser

Verten må generere ein unik 64-bits Interface ID for seg sjølv.

EUI-64-algoritma er den mest vanlige:

- 1) Start med MAC-adressa:

00:11:22:33:44:55

- 2) Blås den opp til 64 bits ved å putte inn **ff:fe** i midten

0011:22ff:fe33:4455

- 3) Inverter bit nr. 7 (universal/local bit):

0211:22ff:fe33:4455

- 4) Sett inn det fast definerte prefikset **fe80::/64** foran:

fe80::211:22ff:fe33:4455



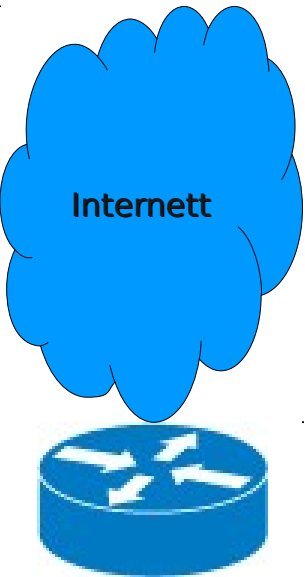
fe80::abcd/64



fe80::211:22ff:fe33:4455/64
::1/128
(state tentative)

Bli med i multicast-grupper

Verten må bli med i minst to link-lokale multicast-grupper, ved å bruke **Multicast Listener Discovery (MLD)** – erstatninga for IGMP i IPv6:



fe80::abcd/64

- 1) **ff02::1** a.k.a. All Nodes on link, essensielt IPv6 broadcast
- 2) **ff02::1:ff33:4455** a.k.a. Solicited Node, brukt til ICMPv6 Neighbor Discovery (tilsvarar IPv4 ARP). Sett saman **ff02::1:ff00:0/104** med dei siste 24 bitsa av grensesnittet si IPv6-adresse



fe80::211:22ff:fe33:4455/64
::1/128
(state tentative)

Src: :: (Unspecified)
Dst: ff02::16 (All-MLDv2-Routers)
MLDv2 Report
Interface joins groups **ff02::1** and
ff02::1:ff33:4455

Duplicate Address Detection

Verten prøvar så å finne ut om nokon andre brukar adressa eller ei ved å sende ein ICMPv6 **Neighbor Solicitation** (tilsvarande ARP who-has) for den valde adressa til Solicited Node-multicastadressa, med **Unspecified** som source:



fe80::abcd/64

Src: :: (*Unspecified*)
Dst: ff02::1:ff33:44:55 (*Solicited Node*)
ICMPv6 Neighbor Solicitation
Who has fe80::211:22ff:fe33:4455?



fe80::211:22ff:fe33:4455/64
::1/128
(state tentative)

Duplicate Address Detection

Verten prøvar så å finne ut om nokon andre brukar adressa eller ei ved å sende ein ICMPv6 **Neighbor Solicitation** (tilsvarande ARP who-has) for den valde adressa til Solicited Node-multicastadressa, med **Unspecified** som source:



fe80::abcd/64

Src: :: (*Unspecified*)
Dst: ff02::1:ff33:44:55 (*Solicited Node*)
ICMPv6 Neighbor Solicitation
Who has fe80::211:22ff:fe33:4455?



::1/128
fe80::211:22ff:fe33:4455/64

Om ikkje noko **Neighbor Advertisement** vart motteke (til nokre av dei to multicast-gruppene), flagget *tentative* vert fjerna, og adressa er klar til bruk.

Ruting og global adressering

Verten forespør konfigurasjon frå evt. ruterar ved å sende ein **Router Solicitation**, som vert besvarar med ein **Router Advertisement** som inneheld mykje informasjon

Src: fe80:211:22ff:fe33:4455
Dst: ff02::2 (All Routers)
ICMPv6 Router Solicitation



fe80::abcd/64

Src: fe80::abcd
Dst: ff02::1 (All Nodes)
ICMPv6 Router Advertisement
Router Lifetime: 30m
Managed flag: 0
Other Configuration flag: 0
Prefix Information Option:
Prefix: 2001:db8::/64
Valid Lifetime: 24h
Preferred Lifetime: 6h
Autonomous flag: 1
On-Link flag: 1
Recursive DNS Server Option:
DNS server 1: 2001:db8::53:1
DNS server 2: 2001:db8::53:2



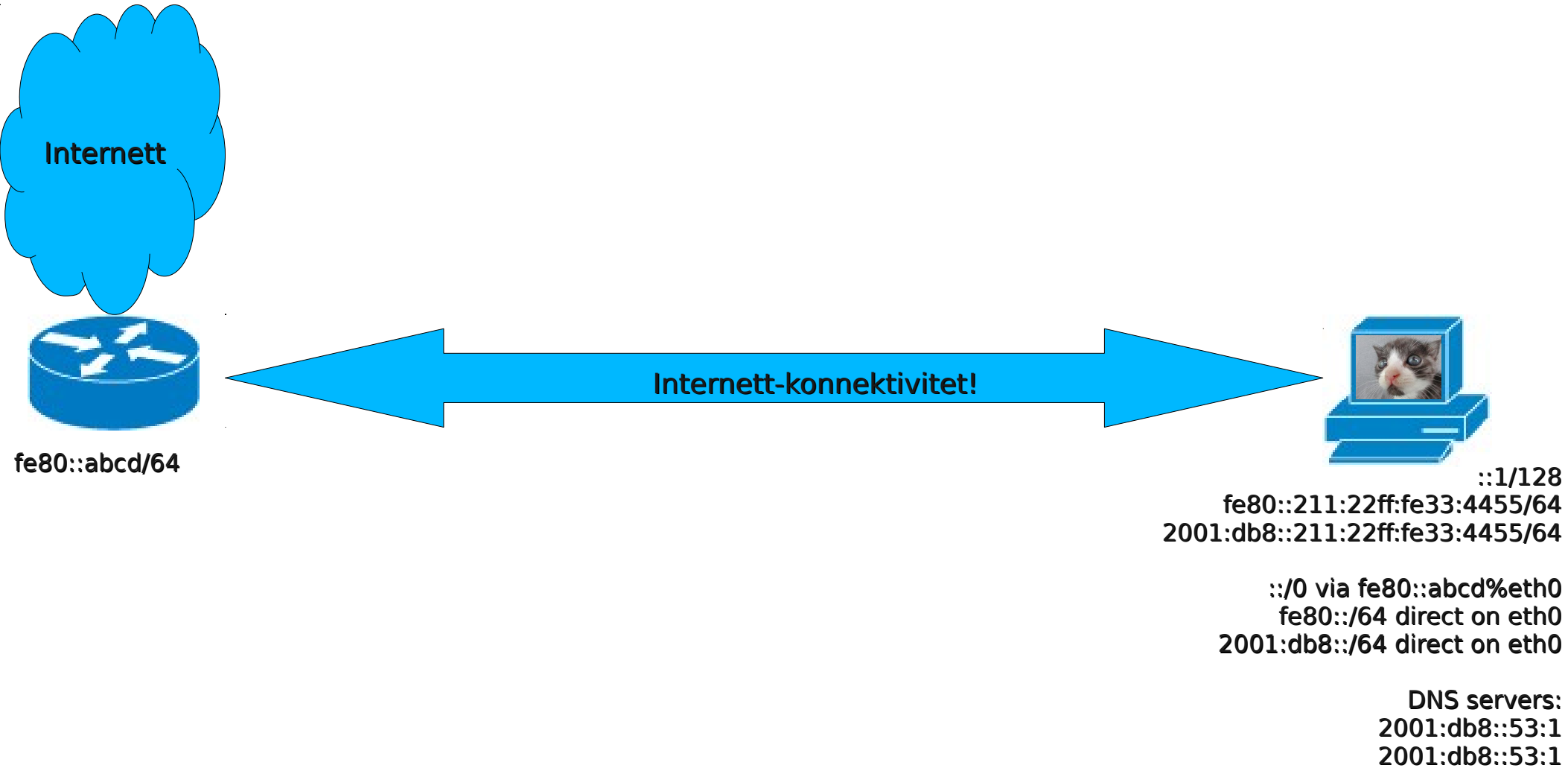
::1/128
fe80::211:22ff:fe33:4455/64

Mottak av Router Advertisements

- Om **Router Lifetime** er >0 , vert ruterer lagt til som ei defaultrute. Dette er den **einaste måten** ein IPv6-vert kan lære defaultruta si!
- Om flagget **Managed** er satt, så skal verten freiste å få tildelt adresser og anna konfigurasjon (DNS, NTP, ...) frå ein **DHCPv6**-server
 - Om ikkje, men om flagget **OtherConfig** er satt, spør **DHCPv6** om konfig (DNS osv) men ikkje om adresser (*Information-Only DHCPv6*).
- For alle **Prefix Information Options** med flagget **Autonomous** satt:
 - Generer ein 64-bits interface ID (f.eks. med *EUI-64*), sett saman med det oppgjevne prefikset, konfigurerer opp adressa, og gjer **DAD**
 - Om **On-Link** er satt, legg til ei direkterute til prefikset på interfacet. (Om det ikkje er satt, må all trafikk på LAN-et sendast via ruterer.)
- Legg til **Recursive DNS Servers** til operativsystemet sitt DNS-oppsett

- Diverse nedtelling startar etter at ein RA er motteke:
 - Når **Router Lifetime** når 0, vert default-ruta fjerna
 - Når ei adresse si **Preferred Lifetime** når 0, vert den ikkje lengre brukt til å etablere nye forbindelsar med
 - Når ei adresse si **Valid Lifetime** når 0, vert den fjerna fullstendig
 - DNS-tenarar har òg lifetimes
- Det fins mange andre tilgjengelege opsjonar som kan finnast i ein RA:
 - More-Specific Routes (med nedteljing)
 - DNS Domain Search List (med nedteljing)
 - Ruter-preferanse
 - MAC-adressa til rutereren (slik at ein kan hoppe over ND)

Ferdig! (inntil vidare iallfall...)



Verten vil fortsetje å lytte etter RA

- Ein ruter vil med jamne mellomrom sende ut RAs (utan å ha blitt spurd)
 - Startar all nedteljing på nytt att
 - Kan brukast for å endre adressene/konfig som er i bruk
 - Send det gamle prefikset/konfigen med levetid 0
 - Send det nye prefikset/konfigen med normal levetid
 - Fjerne seg sjølv som ein default-ruter, f.eks.:
 - Før shutdown eller planlagt vedlikehald
 - Umiddelbart etter at dens eigen internett-konnektivitet forsvinn

- Alle moderne OS støttar å lære adresser og default-ruter frå RA:
 - Kallast **SLAAC** for Stateless Address AutoConfiguration
 - DHCPv6 støttast mindre grad (Windows samt nyare OS X/iOS/Linux)
- DNS-tenarar er vanskelegare å lære...
 - Windows støttar kun DHCPv6, ikkje RDNSS-opsjonen i RA
 - OS X 10.6 støttar kun RDNSS, ikkje DHCPv6
 - OS X 10.7 og nyare Linux/iOS støttar begge
 - For maks kompabilitet, annonser DNS-tenarar begge stadar: RDNSS i RA, samt i DHCPv6 (sett OtherConfig-flagget i RA til 1)
- Mange operativsystem/implementasjonar støttar ikkje IPv6 ordentleg:
 - Android, Windows før Vista, OS X før 10.6, PS3, Xbox,
 - Vanlege privatbrukarar vil fortsetje å krevje IPv4-tilgong

Det var alt eg hadde...

Spørsmål?

Takk for meg – god jul og godt
nytt år!