Innføring av IPv6 i Norge

Status og teknisk relaterte aspekter

28 mars 2011

Post- og teletilsynet

Innhold

Figurer

Bakgrunn

Vi er i ferd med å gå tom for IPv4-adresser. Med dagens forbruk estimerer RIPE NCC[1] at de vil gå tom innen slutten av 2011.

Avhengig av buffer hos aktørene, er det rimelig å anta at de aller fleste norske aktørene vil være tomme for IPv4-adresser innen utgangen av 2012. Det er derfor nødvendig med et økt tempo på innføringen av IPv6.

Denne rapporten fra Post- og teletilsynet (PT) bygger på informasjon fra flere aktører i det norske ekommarkedet.

Målgruppen for rapporten er aktører i det norske ekommarkedet. Både beslutningstakere og teknikere vil kunne ha nytte av rapportens innhold. Personer med grunnleggende forståelse og interesse for IP vil også ha nytte av den. Vi har forsøkt å gjøre innholdet minst mulig teknisk.

Målet med rapporten er å kartlegge og utrede følgende:

- Ressurssituasjonen for IPv4 og utberedelsen av IPv6 (kap. 2).
- IPv6 – muligheter (kap. 3).
- IPv6 i Norge: Status for nett, sluttbrukerutstyr og innhold (kap. 4).
- Tekniske hinder for rask innføring av IPv6 (kap.5).

Innholdet i kapittel 2 baserer seg i hovedsak på informasjon fra RIPE NCC, mens kapittel 3, 4 og 5 i hovedsak baserer seg på informasjon PT har fått fra aktører i det norske markedet.

Det er også hentet informasjon fra artikler i nettbaserte medier som Inside Telecom, Telecom revy, digi.no, computerworld.no m.fl. (se referanser side 26).

Det er referert til Wikipedia flere steder. Wikipedia er brukt som kilde for å gi leserne mulighet til å lese mer om enkelttema, samt for å gi forklaringer til ord, uttrykk og begreper.

[1] RIPE NCC er et av de fem regionale internettregisterne (**Regional Internet Registry - RIR**). Norge ligger under RIPE NCC. Organisasjonene har ansvar for å tildele og registrere Internet-ressurser i gitte regioner i verden. Ressurser inkluderer IP-adresser (både IPv4 og IPv6) og ruting-prefikser (for bruk i BGP-ruting). (http://www.ripe.net/)

Sammendrag

Bruken av IPv6 øker. Økningen er likevel liten i forhold til behovet for nye adresser.

Per 28. oktober 2010 var det mindre enn 5 prosent igjen av ubrukte IPv4-adresser (ref. RIPE NCC). Tilgjengelige (nye) IPv4-adresser forventes å være brukt opp innen 1 til 2 år.

Den fremtidige veksten av Internett vil medføre behov for raskere innføring av IPv6 enn hva tilfellet har vært hittil. I Norge har om lag 45 prosent av LIR-ene (Local Internet Registries[2]) fått tildelt IPv6-adresser. Den faktiske bruken av IPv6 varierer imidlertid mye blant disse LIR-ene.

Antallet IPv6-adresser er tilnærmet uendelig, mens det totale antallet IPv4-adresser er ca 4,3 milliarder.

Grunnen til at innføringen av IPv6 har gått relativt sakte, skyldes i hovedsak god tilgjengelighet på IPv4-adresser, mangelen på en "killer-applikasjon" for IPv6 og manglende økonomiske insentiver.

Tilbydere har frem til nå forlenget levetiden til IPv4 ved å ta i bruk smarte metoder som dynamisk tildeling av IP-adresser og bruk av adresseoversetting (NAT). Den utstrakte bruken av disse metodene har likevel noen iboende svakheter og er blitt en begrensende faktor for flere typer tjenester og produkter.

Når IPv4-adressene er brukt opp, er IPv6 eneste alternativ for å koble nye brukere til Internett. Samtidig vil applikasjoner og tjenester som krever ende-til-ende forbindelse ha stor nytte av IPv6, ettersom enheter vil kunne tildeles en fast, unik IP-adresse.

Det er likevel innen mobilt bredbånd det i første omgang vil være behov for bruk av IPv6. Kundeveksten kan vanskelig fortsette med det antallet adresser som er tilgjengelige i IPv4.

Enkelte ISP-er informerer om at de allerede har IPv6 implementert i både kjerne- og aksessnett, og leverer IPv6 til brukere som eksplisitt etterspør dette. Andre tilbydere uttaler at de ikke har kommet lengre enn til planleggingsstadiet.

Administrative støttesystemer og systemer for drift og vedlikehold må tilrettelegges for IPv6 før IPv6 kan tilbys i stor skala. En slik tilrettelegging kan være teknisk krevende og kostbar.

Mangel på kompetanse, opplæring og erfaring hos teknikere og driftspersonell trekkes også frem som en viktig årsak til at innføring av IPv6 har gått relativt sakte frem til nå. Utfordringer relatert til sikkerhet og sameksistensen av IPv4 og IPv6 nevnes også som en faktor.

Rapporten indikerer at det er relativt få nettverksmessige utfordringer knyttet til implementering av IPv6. Faren for brekkasje gir negativ effekt på innholdsleverandørenes motivasjon for å formidle innhold via dual-stack IPv4/v6.

Utstyr som tilbyderne i dag har plassert ute hos sine kunder (CPE-utstyr) støtter IPv6 i varierende grad. I bedriftsmarkedet er tilgangen på utstyr bedre enn i privatmarkedet. De fleste enhetene som er levert av ISP-ene i privatmarkedet, eller er kjøpt over disk, støtter ikke IPv6.

[2] En lokal Internett-registrar (LIR) er en organisasjon som har blitt tildelt en blokk med IP-adresser fra en regional Internett-registrar (RIR), og som kan tildele deler av denne blokken til sine egne kunder. De fleste LIR-er er Internettleverandører, bedrifter og akademiske institusjoner.

Det er heller ikke sannsynlig at majoriteten av eksisterende CPE-er kan oppgraderes med ny programvare, og må i tilfelle byttes ut. Det må imidlertid understrekes at det blir stadig mer vanlig med støtte for IPv6 i nytt utstyr.

Innføring av IPv6 betyr ikke at IPv4 vil forsvinne. IPv4 vil leve i parallell med IPv6 i mange år fremover.

1 Innledning

(Rapporten inneholder mange forkortelser. Oversikt over forkortelsene finnes på side 25).

Internettadresser (IP-adresser) er en begrenset ressurs. Et stadig økende antall tjenester og brukere vil ha behov for adresser på Internett, og dette har ført til at de adressene som for det meste brukes i dag, IPv4-adresser, snart er brukt opp.

I oktober 2010 var det kun 5 prosent av de totale IPv4-ressursene igjen på verdensbasis, og 1. februar 2011 ble de siste blokkene med IPv4 adresser fordelt av ICANN til 5 registerenheter (RIR-ene) som videretildeler IP-adresser til internettleverandører.

RIR-en (RIPE NCC) som dekker Europa vil sannsynligvis være tom for IPv4-adresser mot slutten av 2011. Tildelingsreglene for IP-adresser (fastsatt av IANA[3] og RIPE NCC) tilsier at aktørene ikke skal sitte inne med større reserver av IPv4-adresser. Fra 2012 må derfor nye behov for internettadresser dekkes av IPv6-adresser.

Antallet IPv6-adresser er tilnærmet uendelig, mens det totale antallet IPv4-adresser er ca 4,3 milliarder.

Tilbydere har frem til nå forlenget levetiden til IPv4 ved å ta i bruk smarte metoder som dynamisk tildeling av IP-adresser og bruk av adresseoversetting (NAT). Den utstrakte bruken av disse metodene har likevel noen iboende svakheter og er blitt en begrensende faktor for flere typer tjenester og produkter.

Dette tilsier at innføringen av IPv6 ikke kan utsettes uten at det også vil ha negativ innvirkning på utviklingen av nye, og videreutvikling av en rekke eksisterende, tjenester og produkter.

Når tilgjengelige IPv4-adresser er brukt opp, vil alle som har behov for flere IP-adresser måtte ta i bruk IPv6-adresser. Omdisponeringer av eksisterende IPv4 adresser hos tilbydere og innføring av "smarte teknikker" kan forlenge levetiden noe.

Den fremtidige veksten av Internett vil kreve mye større behov for IP-adresser Det betyr at aktører må handle nå og klargjøre sine nett, sitt utstyr og sine systemer for IPv6.

Aktører med ønske om å innføre nye tjenester, nye produkter eller utvide kundemassen vil derfor i løpet av kort tid bli avhengige av IPv6. Dette gjelder spesielt for nye aktører som ønsker å etablere seg i markedet, men også for dem med små eller ingen lager av IPv4-adresser.

Innføringen og bruken av IPv6 akselererte merkbart i 2010, men trafikkvolumet er fortsatt veldig lite i forhold til IPv4s trafikkvolum. Bruken av IPv6-adresser er begrenset og utgjør i dag kun ca 0,15prosent av internettrafikken[4]. Organisasjoner og aktører over hele verden, som IETF, ICANN/GAC, NRO, RIPE NCC, EU-kommisjonen, OECD, ITU og IPv6 Forum, diskuterer utfordringer knyttet til å få til en raskere innføringen av IPv6.

> ***"The killer application of IPv6 is the survival of the open Internet as we know it."***
>
> Lorenzo Colitti, Google, 2010

(Sitatet over er hentet fra denne presentasjonen, slide 7)

[3] http://www.iana.org/
[4] Jfr. Comcast (www.comcast6.net)

2 Ressurssituasjonen for IPv4 og utbredelsen av IPv6

2.1 Global status for IPv4-adresser

Etterspørselen etter IPv4-adresser er økende i alle de fem[5] verdensregionene .

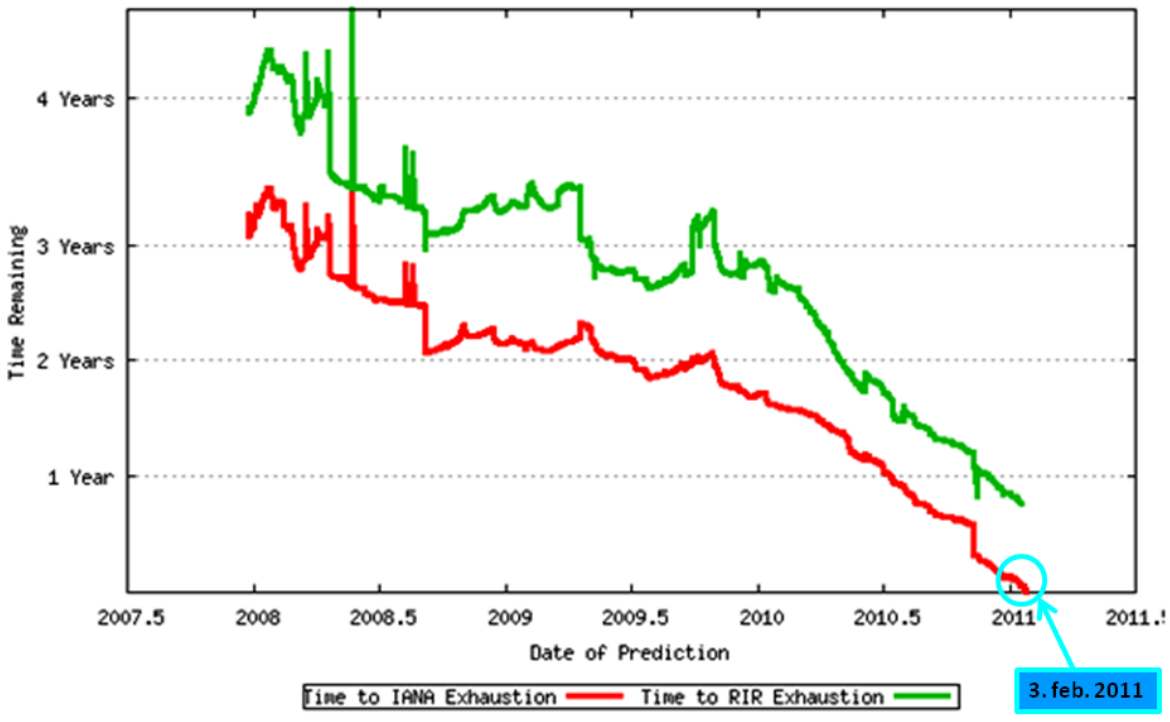
Rød kurve viser antall tilgjengelige adresser som Internet Assigned Numbers Authority (IANA[6]) per 22. desember 2010 ikke hadde delt ut til de fem "Regional Internet Registry"-ene (RIR-ene[7]).

Grønn kurve viser summen av antall tilgjenglige adresser som per. 22 desember 2010 er utdelt, men ikke tatt i bruk på RIR-nivå.

Fredag 3. februar 2011 sendte ICANN[8] (The Internet Corporation for Assigned Names and Numbers) ut en pressemelding med tittelen:

" Available Pool of Unallocated IPv4 Internet Addresses Now Completely Emptied - The Future Rests with IPv6"

Dette betyr at den røde kurven har nådd bunnen.



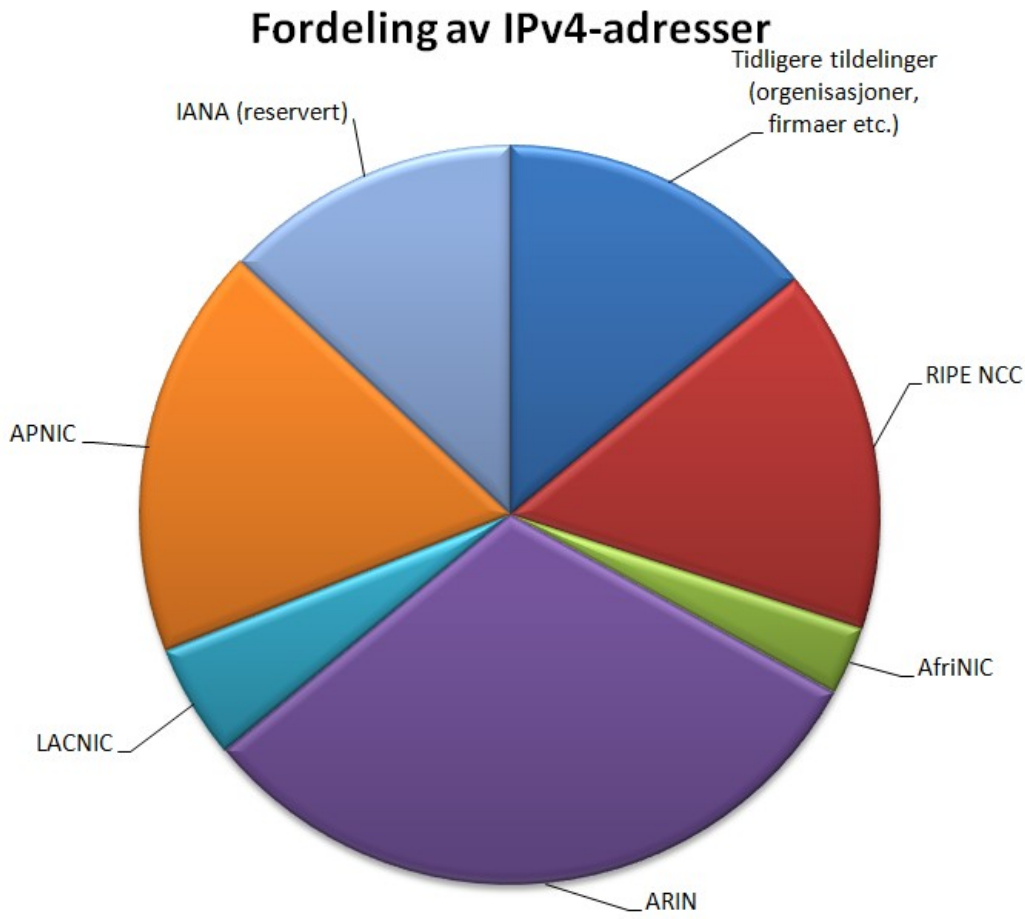
Figur 1 Tid til IANA og RIR-ene er tomme for IPv4-adresser[9]

[5] http://www.iana.org/numbers/
[6] http://www.iana.org/
[7] http://en.wikipedia.org/wiki/Regional_Internet_registry
[8] http://www.icann.org/
[9] http://www.potaroo.net/tools/ipv4/index.html

Fra 1. januar 2000 til 1. januar 2010 ble antall IPv4-adresser i bruk nær fordoblet. I samme periode ble ledige adresser redusert til om lag en tredjedel.

Norske internettleverandører (LIR-er[10]) får sine IPv4 adresseresurser fra RIPE NCC[11].
Tildelingspolicy hos RIPE NCC er at tildelingen av nye IPv4-adresser skal gjøres på bakgrunn av dokumentert behov.
Først når tildelte adresseresurser har oppnådd den utnyttelsesgrad som er bestemt i policy for forrige tildeling, vil en kunne søke om å få tildelt flere IPv4-adresser.

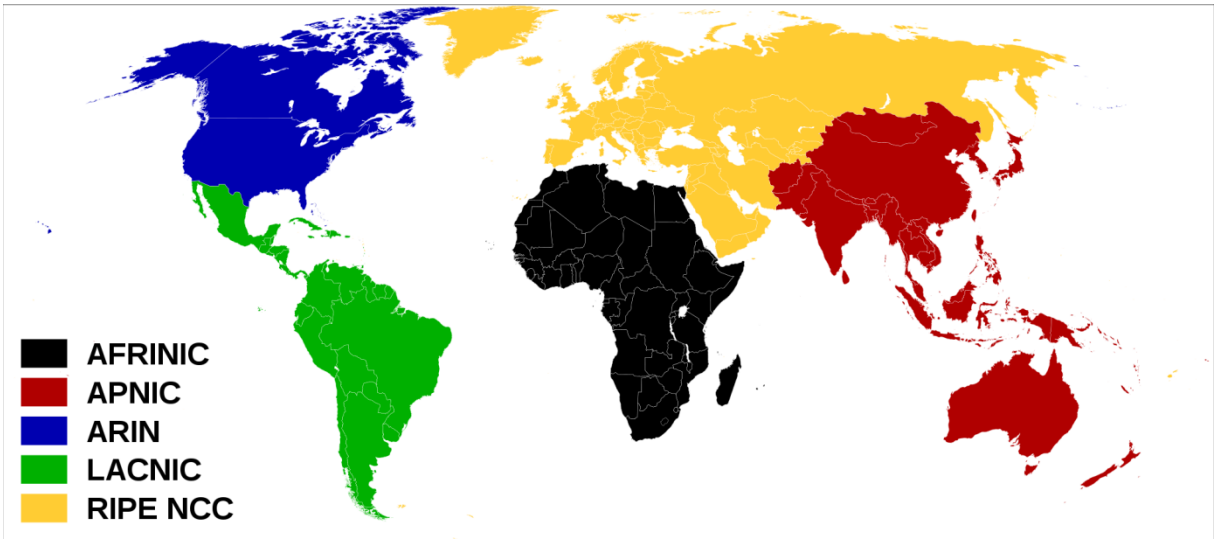
Så lenge det er IPv4-adresser tilgjengelig for tildeling fra RIPE NCC, vil norske Internettleverandører få IPv4-adresser når de har behov for det. Når det er tomt for IPv4-adresser hos RIPE NCC (antakelig på slutten av 2011), vil norske internettleverandører måtte bruke IPv6 adresser eller benytte annen teknologi for å spare på bruken av IPv4-adresser.



Figur 2 Fordeling av IPv4-adressene (IANA har nå fordelt hele IPv4-adresserommet)

Sektoren "IANA (reservert)" i Figur 2 viser at IANA har et signifikant antall adresser som er reservert for blant annet multicast (ref. RFC 1918[12]). Sektoren "Tidligere tildelinger" representerer adresser som ble tildelt før systemet med RIR-er ble etablert. Typisk har store organisasjoner og firma fått betydelige tildelinger, og eventuell bruk av disse er ikke synlig for det åpne Internett. De resterende fem sektorene representerer geografiske regioner. Disse er presentert i Figur 3 under.

[10] http://en.wikipedia.org/wiki/Local_Internet_Registry
[11] http://www.ripe.net/
[12] http://www.rfc-editor.org/rfc/rfc1918.txt

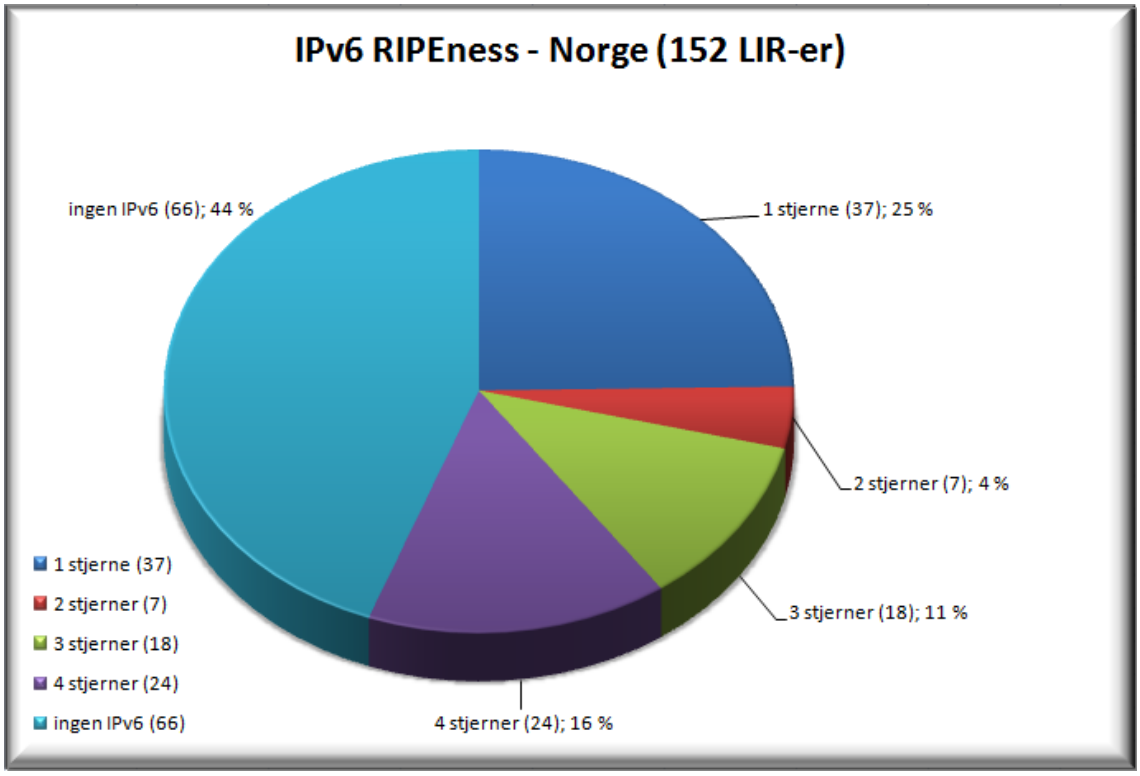


Figur 3 RIR-ene og deres regionale ansvarsområder[13]

- AfriNIC - African Network Information Centre → for Afrika
- ARIN - American Registry for Internet Numbers → for USA, Canada og flere deler av Karibien
- APNIC - Asia-Pacific Network Information Centre → for Asia, Australia, New Zealand og naboland
- LACNIC - Latin America and Caribbean Network Information Centre → for Latin-Amerika og deler av Karibien
- RIPE NCC → for Europa, Midtøsten og Sentral-Asia

[13] http://no.wikipedia.org/wiki/Regional_Internet_Registry

2.2 Status for utbredelsen av IPv6-adresser i Norge



Figur 4 Norsk IPv6-"RIPEness" (kilde: RIPE NCC 15. feb. 2011)

Som det fremgår av Figur 4, har 44 prosent av norske LIR (Local Internet Registries) fortsatt ikke skaffet seg IPv6-adresser.
Det vil si at 56 prosent av norske LIR-er har fått tildelt IPv6-adresser. Disse LIR-ene er plassert i fire ulike kategorier[14] (stjerner) avhengig av hvor flinke de har vært til å ta i bruk IPv6. Av de 56 prosentene som har fått tildelt IPv6-adresser er det:

1. *Èn stjerne* → 25 % av LIR-ene har fått tildelt adresser, men ikke gjort noe mer.
2. *To stjerner* → 4 % av LIR-ene har i tillegg annonsert sitt IPv6 prefiks på en ruter på Internett via Border Gateway Protocol (BGP).
3. *Tre stjerner* → 11 % av LIR-ene har også etablert et route6 objekt i RIPE NCC databasen, i tillegg til å annonsere sitt IPv6 prefiks.
4. *Fire stjerner* → 16 % av LIR-ene har i tillegg til alt det som er nevnt tidligere også konfigurert revers DNS for IPv6-adressene.

75 prosent av det norske privatmarkedet for internettilgang dekkes av følgende seks aktører: Telenor, NextGenTel, Get, Ventelo, Lyse og BKK. For bedriftsmarkedet er i tillegg TDC betydningsfull. Disse aktørene har alle fått tildelt IPv6 adresser.

På linken her finnes en oversikt over hvilke LIR-er i Norge som har oppnådd fire stjerner i forhold til inndelingen som RIPE NCC har gjort. Oversikten oppdateres fortløpende.

Det å oppnå fire stjerner sier lite om i hvilken grad det tilbys tjenester på IPv6. Likevel tyder registreringen på at det er gjort forberedelser for å kunne ta i bruk IPv6.

[14] http://ripeness.ripe.net/

3 IPv6 – muligheter

Innføringen av IPv6 vil, i tillegg til å avhjelpe problemet med mangel på IP-adresser, gi en rekke nye muligheter både for nettoperatører, innholdsleverandører, applikasjonsutviklere og sluttbrukere. Noen av disse mulighetene er kort beskrevet under.

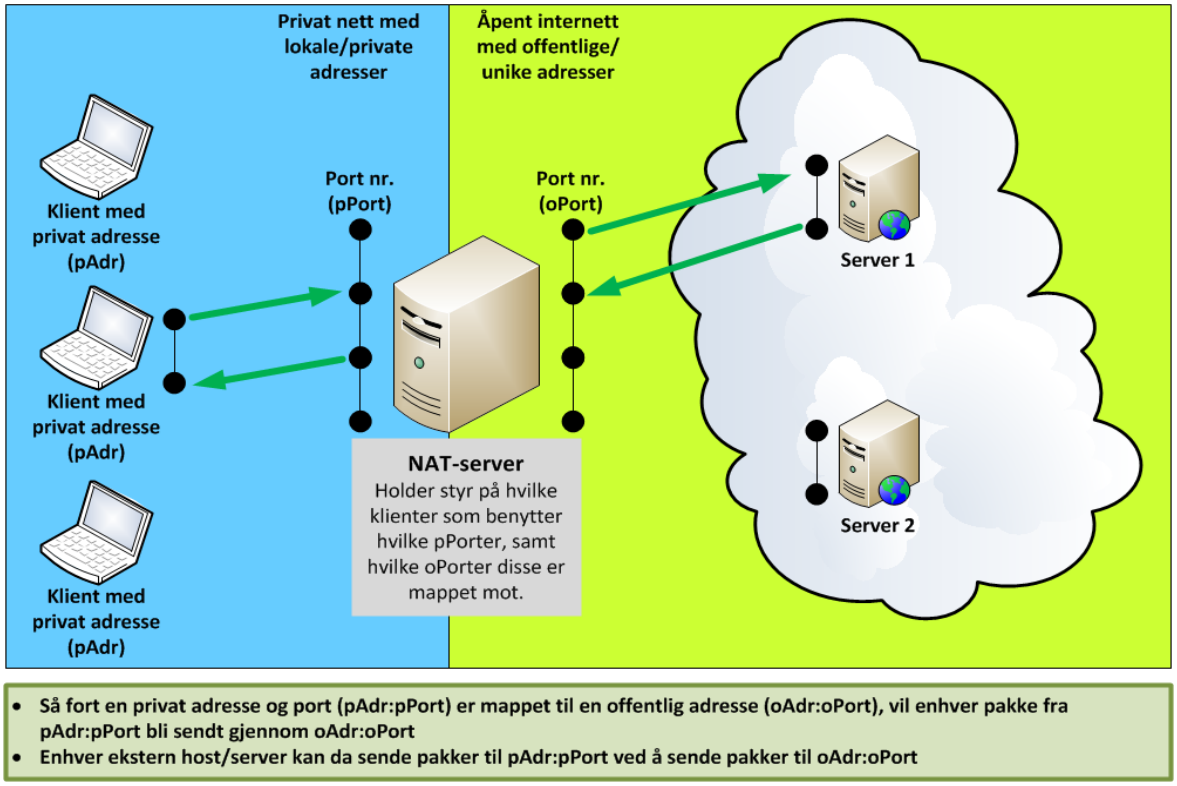
3.1 NAT - Network Address Translation

Frem til i dag har adresseoversetting (heretter; NAT[15] (Network Address Translation)) vært en effektiv metode for å redusere behovet for IP-adresser.

Metoden har fungert teknisk tilfredsstillende over mange år, og har også vært kostnadseffektiv. Teknologiutvikling og bruk av nye tjenester gjør at dette bildet er i ferd med å endres.

NAT fungerer ved at flere brukere deler på en eller flere IP-adresser. Dette har sine klare fordeler i sammenhenger der IP-adresser er en begrenset ressurs. I tillegg kan NAT ha positive sider når det kommer til sikkerhet.

Bruk av NAT medfører imidlertid dårligere presisjon for geografisk lokalisering, noe som skaper problemer knyttet til blant annet lisensiering av innhold som streames og geografisk lokalisering av nødanrop originert fra nomadiske enheter som benytter IP-telefoni.



Figur 5 Grunnleggende NAT

Bruk av NAT som løsning for å forlenge levetiden for IPv4, kan vise seg å bli kostbart etter hvert som bruken av kapasitetskrevende tjenester og applikasjoner øker. Nødvendig sanntidshåndtering av denne type tjenester krever svært mye av NAT-funksjonaliteten for at brukeropplevelsen ikke skal forringes.

[15] http://no.wikipedia.org/wiki/NAT

Nettverkselementer som befinner seg bak en NAT er vanskelige å fjernadministrere. Det er vanskelig å drive effektiv feilretting og konfigurering på nettverkselementene uten NAT-administratorens hjelp.

Eksempler på aktuelle tjenester som vanskelig kan fjernadministreres gjennom NAT er VPN, VoIP, streaming av video, spill og P2P. NAT er også kostbart med hensyn til administrasjon, drift og support.

Identifisering og eventuell blokkering av en kilde som genererer uønsket trafikk eller utfører ulovlige handlinger på nettet kan være vanskelig å utføre på utstyr som befinner seg bak en NAT. Dersom en IPv4-adresse sender spam, driver hacking etc., kan det være aktuelt å blokkere den aktuelle IP-adressen. Om adressen som blokkeres tilhører en NAT, vil samtidig en eller flere andre enheter/brukere bli blokkert.

Stadige utvidelser av NAT-arkitektur vil kunne skape problemer knyttet til mangel på porter (for "porter" se Figur 5 over). NAT har introdusert uønskede bivirkninger som vanskeligheter med retting av feil i nettverket, nettverksadministrasjon og implementering av sikkerhetsprotokoller som IPsec[16].

3.2 Sikkerhet, ruting og tjenestekvalitet

Tilgang på IPv6-adresser fjerner behovet for NAT som metode for gjenbruk av IP-adresser. Dette vil gi bedre muligheter for utvikling av programvare og tjenester hvor sikkerheten kan legges på IP-laget og dermed styrke ende-til-ende-sikkerheten.

Mekanismene for autentisering og kryptering er bedre tilpasset og sterkere integrert i IPv6. Med IPv6 er utvidelseshoder ("Extension headers[17]") for autentisering og kryptering blitt definert separat, slik at applikasjoner på høyere nivå kan bruke en eller begge funksjoner når det kreves. Sikkerhetselementer kan enkelt tas i bruk i IPv6, blant annet fordi IPv6 ikke trenger bruk av NAT.

I dag er IPv4-adressene tilfeldig tildelt geografisk sett. Dette har historiske årsaker. Den viktigste forutsetningen for en effektiv hierarkisk ruting er optimal tildeling av adresser. Med IPv6 er mulighetene for en slik optimalisering tilstede. Velregulert tildeling av IPv6-adresser, og bruk av hierarkisk adressering[18] gir nye muligheter for raskere og mer effektiv ruting.

IPv6 muliggjør automatisk tildeling og endring av IP-adresser og autokonfigurering av adresser. Dette forenkler i første rekke nettverksadministrasjon.

Mekanismer for kvalitetshåndtering (Quality of Service (QoS)) er innebygget i IPv6. Det er derfor enklere å få til prioritering av tidssensitive datastrømmer (altså streaming og "realtime") og effektiv pakkehåndtering. Overføring av tale- og videopakker i parallell med andre datapakker er også en av forbedringene med IPv6.

3.3 Kostnadseffektive nett, støttesystemer og tjenester

IPv6-støtte i nett, støttesystemer og sluttbrukerutstyr vil legge forholdene til rette for ny anvendelse av IP-adresser og gi grunnlag for kundevekst og økt innovasjon.

[16] http://en.wikipedia.org/wiki/Ipsec
[17] http://en.wikipedia.org/wiki/IPv6_packet#Extension_headers
[18] http://en.wikipedia.org/wiki/Hierarchical_routing

Etter hvert som støtte for IPv6 blir mer utbredt i nett, tjenester og brukerutstyr, vil behovet for å konvertere mellom de to IP-protokollene gradvis reduseres. Direkte kommunikasjon der alle enheter snakker samme "språk" vil sannsynligvis gi en bedre brukeropplevelse.

Vi ser i dag et økende antall produkter og tjenester med strenge krav til kort responstid, høy tilgjengelighet og direkte kommunikasjon. En av forutsetningene for at disse skal kommunisere på en mest mulig effektiv måte, er å benytte IPv6 ende-til-ende. Native (ren) IPv6 eller dual-stack er i dag to naturlige alternativer for å få til dette.

Enheter som skal kommunisere direkte med hverandre over Internet må ha hver sin unike og offentlige IP adresse. Det forventes en sterk økning av behovet for direkte ende-ende-kommunikasjon fremover, og dette vil være vanskelig å imøtekomme med et begrenset antall IPv4-adresser. IPv6 vil gi utvidede muligheter når flere enheter kan ha sin egen unike IP-adresse[19].

Brukere av trådløs internettaksess (WLAN, mobilt internett, WiMax, etc.) krever en IP-tjeneste med kort svartid, som alltid er på og alltid tilgjengelig. Peer-to-peer-nett gjør en gruppe enheter i stand til å kommunisere direkte med hverandre, i stedet for gjennom en sentral server. Dette gjør at en unngår kostnaden og forsinkelsen ved å håndtere all trafikken på denne måten.

3.4 Tjenester og produkter som vil ha nytte av IPv6-støtte i nettene

Det har gjentatte ganger vært etterlyst en såkalt "killer-applikasjon" for IPv6. Det vil si en applikasjon som "alle vil eller må ha" og som krever IPv6. En eller flere slik killer-applikasjoner finnes dessverre ikke.

Imidlertid vil et raskt økende antall brukere av Internett og utstyr (systemer) tilkoblet Internett, i tillegg til sammensmelting av tjenester til en felles infrastruktur (NGN[20]), presse frem etterspørselen etter IPv6.

Også innen mobilt bredbånd og hjemmenett (LAN) vil mangel på adresser bli en begrensende faktor for å kunne imøtekomme den store økningen i antall brukere og enheter[21]. Tilgang til nok adresser, og et nett som støtter IPv6, vil være helt avgjørende for en tilbyders mulighet til å overleve på sikt. Internettaksess er den mest åpenbare tjenesten å tilby på IPv6.

Som et eksempel krever nå den amerikanske operatøren Verizon at alle enheter som kobles til deres kommende LTE[22]-nett må støtte IPv6. Motivet for dette kravet er sannsynligvis å legge til rette for kundevekst, samt forenklet administrasjon av terminalene som knytter seg til nettet.

Det er i ferd med å komme internettbaserte tjenester som er skreddersydd for IPv6. Den siste tiden har også native IPv6-nettverk blitt implementert. Sistnevnte er tjenester som støtter at IPv6 kan sende IPv6 datapakker fra avsender til mottaker uten å bli konvertert til IPv4 underveis.

I de tilfellene der det ikke finnes native IPv6 på hele forbindelsen mellom avsender og mottaker må det utføres en oversettelse fra IPv6 til IPv4. Brukere som ikke har tilgang på IPv6-forbindelse ende-til-ende mot rene IPv6-tjenester, vil kunne oppleve dårligere kvalitet, og i verste fall å ikke få tilgang til tjenester. (se A.1).

[19] Tjenester som Skype, Bittorrent, osv. ville trolig ikke oppnådd samme utberedelse dersom brukerne ikke i stor grad hadde tilgang på unike IP-adresser.
[20] http://en.wikipedia.org/wiki/Next_Generation_Networking
[21] F.eks. M2M-enheter og "Smart hjem" -produkter: Mobiltelefoner, kjøleskap, lyspærer, varmtvannsberedere, sensorer, PC-er, Internett-aktiverte biler, sikkerhetssystemer og kjøkkenmaskiner.
[22] http://en.wikipedia.org/wiki/3GPP_Long_Term_Evolution

For de store ISP-ene vil mangel på IPv4-adresser være et operativt problem. Dette gjelder særlig behovet for nok adresser i eget aksessnett. Det vil derfor være helt nødvendig for disse å innføre IPv6 for å kunne adressere f.eks. kundens kabelmodem.

Innen ISP-enes egne administrative driftssystemer vil det fortsatt være behov for IPv4-adresser. Dette skyldes i hovedsak at slike systemer ofte er vanskelige og kostbare å erstatte eller oppgradere. Ved at ISP-ene tildeler sine kunder IPv6-adresser (på kundeaksessene), vil IPv4-adresser kunne frigjøres og gjenbrukes i de interne nettene/systemene.

For tilbydere vil det være viktig at brorparten av internettjenester, -produkter, -innhold og applikasjoner støtter IPv6 snarest mulig.

Etter hvert som flere websider og -tjenester blir tilgjengelige på IPv6, reduseres behovet for å benytte translasjonsteknologi[23]. Dette vil forenkle nettverkskompleksiteten og redusere kostnader.

Kostnader ved å implementere translasjonsteknologi vil kunne være omfattende: Dess større båndbredder som skal prosesseres, dess høyere kostnader og større grad av kompleksitet for å få på plass teknologien som kreves for at ikke kundene skal få en redusert brukeropplevelse

Mye tyder på at store globale aktører er i ferd med å ta grep for å sikre at deres innhold og tjenester fungerer over IPv6 (se eksempler).

Eksempler: Google over IPv6 og store IPv6-tester

- Google har lansert tjenesten "Google over IPv6[24]". Her har nettleverandører muligheten til å registrere sine DNS-navnetjenere, og gi sine kunder tilgang til Google-tjenester (søk, docs, gmail, maps, Picasa, YouTube) ved bruk av IPv6. Blant annet UNINETT har inngått en slik avtale med Google.
- A-pressens digitale medier (APDM) og VG nett har ved flere anledninger testet tjenester på IPv6. Testene har vært så vellykkede, at tjenestene nå er permanent tilgjengelig på IPv6[25].
- Den 8. juni 2011 arrangeres den såkalte "World IPv6 Day[26]". I ett døgn vil store aktører som Google, Facebook, Yahoo!, Akamai, Limelight Networks, samt norske APDM og VG nett tilby innhold over IPv6. Dersom denne testen blir vellykket, kan en forvente at flere av tjenestene vil gjøres permanent tilgjengelig på IPv6. Tatt i betraktning at ovennevnte aktører står for en svært stor andel av innholdsdistribusjonen på Internett, vil permanent overgang for disse aktørene være svært viktig for den videre innføringen av IPv6.

[23] NAT64 og 6to4 er eksempler på translasjonsteknologi i denne sammenheng (se http://en.wikipedia.org/wiki/IPv6_transition_mechanisms og http://en.wikipedia.org/wiki/6to4)
[24] http://www.google.com/intl/en/ipv6/
[25] VG-nett på IPv6: http://www.vg.no
[26] http://isoc.org/wp/worldipv6day/ og http://www.digi.no/860268/prover-ipv6-i-ett-dogn

4 IPv6 i Norge: Status for nett, sluttbrukerutstyr og innhold

Innholdet i dette kapitlet er basert på informasjon fra aktører i det norske ekommarkedet. Noe informasjon er innhentet ved direkte henvendelser, og noe er basert på aktørers informasjon gitt gjennom norske medier.

4.1 Status for kjerne- og aksessnett

Store ISP-er har som en hovedaktivitet å foreta testing med reelle brukere og testing i lab. For disse er det en målsetning å lansere IPv6-internettilgang mot slutten av 2011/starten av 2012.

Kontinuitet i tjenesteleveransene er en felles bekymring. Dette skyldes at enkelte tjenestefunksjoner som støttes i IPv4 fortsatt ikke er implementert av leverandører eller testet av ISP-ene i IPv6. Leverandørene trenger innspill fra ISP-ene om krav til tjenestene slik at implementeringen av slik funksjonalitet kan prioriteres. Standardisering blir sett på som viktig for å kunne enes om detaljene og dermed sikre interoperabilitet.

Enkelte større selskaper informerer om at de har IPv6 implementert både i kjerne- og aksessnett, mens andre melder at de foreløpig er på planleggingsstadiet.

Alle sentrale aktører vi har vært i dialog med sier de kommer til å ha stor aktivitet på dette området fremover: De har en forankret strategi som sier at alle deres tjenester (i eget nett) skal være tilgjengelige på IPv6, i første omgang som dual-stack.

Når det gjelder systemer for administrasjon, drift og vedlikehold må de fleste tilbyderne tilrettelegge disse før innføring av IPv6 kan gjøres i stor skala.

Generelt sett kan aktørenes hovedaktiviteter kort oppsummeres slik:

- Strategi - Alle sentrale aktører PT har vært i dialog med opplyser at de kommer til å ha stor aktivitet på å klargjøre nett, utstyr og tjenester for IPv6 i tiden fremover. De største aktørene har alle en forankret strategi som sier at samtlige av deres tjenester i eget nett skal være tilgjengelige på IPv6, i første omgang som dual-stack. Aktørene er opptatt av at nye produkter, så langt som det er mulig, skal støtte IPv6 fra lansering. Eksisterende kunder vil i tillegg bli tilbudt oppgraderingspakker som bl.a. inkluderer CPE-utstyr hvor IPv6-støtte inngår.

- Planlegging - De store aktørene er kommet langt i planstadiet. De har fått tildelt adresseblokker, de har tildels aktivert IPv6 i kjernenettet, de har adresseplaner klare, og de har gjort en gjennomgang av utstyret i egne nett for å kartlegge hvor klart det er for IPv6. Flere av de store innholdsleverandørene har også kommet langt. IPv6 er gjennomført, klargjort og tilgjengelig for A-pressen og VG nett. Det er gjennomført SWOT-analyser[27] (Strengths, Weaknesses, Opportunities, and Threats), og gjort kartlegginger både ved hjelp av egne og eksterne ressurser. Som oftest etableres det et løp for gradvis testing og integrasjon på de forskjellige nivåene i nettverkshierarkiet.

- Oppgradering - Nettverks- og brukerutstyr oppgraderes, eller byttes ut, for å etablere støtte for IPv6. For de fleste aktører er det primære målet å sørge for at nettene er klare for IPv6, slik at en kan gi god støtte for IPv6-tjenester og produkter når kundene begynner å etterspørre dette.

[27] http://en.wikipedia.org/wiki/SWOT_analysis

- Testing og klargjøring - Nett, systemer for administrasjon, drift og vedlikehold testes og klargjøres for IPv6. Dette er nødvendig før innføring av IPv6 kan gjøres i stor skala. For de aktørene som har kommet langt og har begynt å ta i bruk IPv6 i sine nett, gjenstår i hovedsak testing av mindre kritisk funksjonalitet, nye tjenester og oppgradering av støttesystemene.

- Innføring - Selve innføringen av IPv6 foregår på svært ulike måter og vil være avhengig av størrelse og kompleksitet på nettet, antall kunder i nettet, hvor IPv6-klare tjenestene og brukerutstyret til tilbyderne er, etc. Innføring av IPv6 for mindre aktører vil kunne skje raskere og i ett steg. For større og mer komplekse systemer er det derimot vanlig å gå gradvis frem, for eksempel ved å tilby IPv6 som løsning for pilotbrukere på frivillig basis før en fullskala innføring gjøres.

Eksempler på tilbydere som har kommet langt i innføringen av IPv6, er:

Broadnet[28] - Leverandører av bredbåndstjenester til bedrifter og offentlig forvaltning. Selskapet har tre hovedproduktkategorier: Ethernet, Internett og Telefoni.
Broadnet har innført IPv6, og innføringen rapporteres å ha vært uproblematisk. Så lenge kundene deres benytter brukerutstyr (CPE) som støtter IPv6, kan de benytte IPv6 i sameksistens med IPv4.

Redpill Linpro - Aktør som fasiliterer innhold for tjeneste- og innholdsleverandører. De arbeider målrettet for å få aktivert IPv6 på alt innhold og løse de utfordringer som oppstår (se A.1 brekkasje). Blant annet gjennomføres en rekke målinger, og resultatene deles fortløpende med ISP-miljøet (se http://www.fud.no/ipv6/).

Det kan her nevnes at IPv6 for VG Multimedia og A-pressen Digitale Medier ble testet i en prøveperiode på 24 timer (oktober 2010). Testen hadde hovedsakelig to formål; dels å få erfaring med hvordan brukere opplever ytelsene, dels å bidra til økt fokus på IPv6 hos de forskjellige ISP-ene ved å vise at innholdsleverandørene begynner å gjøre seg klare. Testen var så vellykket at tjenestene nå tilbys permanent på IPv6.

Nettet som IT-selskapet **UNINETT**[29] tilbyr for statlige universiteter, høyskoler og forskningsinstitusjoner, har vært IPv6–klart i nærmere 10 år. Nettene ved de fleste universitetene og høgskolene er tilknyttet dette nettet. Disse nettene er autonome, og status for innføring av IPv6 varierer. Mer om UNINETT i Vedlegg B.

Ventelo har hatt IPv6 implementert i kjernenett og aksessnett. I kjernenettet har IPv6 vært implementert siden 2004[30].

4.1.1 Kjernenett

Kjernenettene eller deler av kjernenett som fortsatt ikke støtter IPv6, er i stor grad klargjort for det og kan aktiveres for IPv6 trafikk når dette besluttes. I tillegg finnes det teknologier som gjør at en enkelt kan tunnelere gjennom de deler av kjernenettet som ikke støtter IPv6.

Flere ISP-er har IPv6 ferdig aktivert i kjernenettet, og kan allerede i dag levere IPv6 som et produkt til sine sluttkunder.
Andre må bytte ut hele eller deler av sin ruterplattform, ettersom den ikke støtter IPv6. Et alternativ for disse er bruk av translasjonsteknologi, men som det fremgår lenger ut i rapporten, vil dette

[28] Broadnet leverer Ethernet (lag 2 i OSI-modellen[28]) og linjene som tilbys kundene er upåvirket av overliggende protokoller (som IP-protokollen på lag 3).
[29] For detaljert oversikt vises det til UNINETTs GigaCampus side[29] med blant annet IPv6 informasjon. Denne siden inneholder også "Best Practises" når det kommer til innføring og bruk av IPv6 i en organisasjon (les mer i Vedlegg B).
[30] http://ventelo.no/filearchive/tg2010/internett-til-tg2010.pdf

kunne skape problemer for enkelte brukere (se A.1). Dessuten er det kostbart å etablere tilfredsstillende funksjonalitet av denne typen, spesielt for høye båndbredder.

Verktøy og applikasjoner for overvåkning av nett mangler fortsatt tilfredsstillende støtte for IPv6. Det samme er tilfelle for systemer for drift, vedlikehold og andre støttesystemer. Mer om dette i kap. 5.2.

4.1.2 Aksessnett

Aksessnettene, hvor de største investeringene er gjort og hvor en har de største antall nettverksenhetene, er mindre klargjort enn kjernenettene for IPv6.

Dagens aksessnett består av både gammelt utstyr (lag 2-utstyr; "agnostiske aksessnett") og nyere utstyr (lag 3; "aware nett"). Nettverk med utstyr som opererer på lag 2 vil i utgangspunktet støtte IPv6 direkte.
I dag gjør imidlertid det meste av dette utstyret en rekke tilleggsfunksjoner[31] som er avhengige av IP-versjon. Noe av dette utstyret kan oppgraderes med ny programvare og dermed bli IPv6-kompatibelt, men det meste må byttes ut.
Det finnes også en stor mengde nyere utstyr som til en viss grad støtter grunnleggende IPv6-funksjonalitet, men som likevel ikke er klar for en full utrulling av IPv6 (f.eks. begrenset IPv6-kapasitet).

Antallet ISP-er som har støtte for IPv6 i nettet frem til sluttkunder øker, men det er svært få bredbåndsleverandører som leverer IPv6 som fullskala kommersiell tjeneste med fullverdig kundestøtte til hele eller deler avkundemassen.
Den største samlingen med IPv6-aktiverte sluttbrukere er i dag tilknyttet UNINETT. Spesielt innenfor studentbyene leveres IPv6 til tusenvis av studenter.

Det er naturlig å se for seg en trinnvis innføring av IPv6 gjennom følgende:

1. Dual-stack gjøres gradvis tilgjengelig i nettverk og i brukerutstyret til nye kunder eller hos kunder som har bestilt oppgradering. Blant andre fører RIPE NCC liste[32] over det utstyr de mener støtter IPv6 på en tilfredsstillende måte.
2. Øvrig ikke-kompatibelt utstyr i nettet og brukerutstyr hos sluttbrukerne (CPE-utstyr) oppgraderes eller skiftes ut.

Ettersom aksessnettene verden over har manglende IPv6-støtte, er det utviklet teknologier som 6rd (IPv6 Rapid Deployment [33], RFC 5969) for å kunne tunnelere gjennom aksessnettutstyr som ikke støtter IPv6 enda.
6rd gjør at en ISP kan levere IPv6 til kunden, selv om ISP-ens aksessnett i seg selv ikke støtter IPv6 fullt ut.

De fleste store aktørene, men også mange mindre, informerer om at alle nye prosjekter for IP-produkter eller -plattformer skal inkludere innføring av IPv6 (hovedsakelig IPv6 dual-stack).

4.2 Status for IPv6-peering nasjonalt og internasjonalt

Det er ingen mangel på globale IP-transittleverandører med fullgod støtte for IPv6, og mange av disse er blant annet til stede på NIX[34]-en i Oslo (f.eks. Global Crossing og Tinet). NIX-knutepunktet støtter IPv6 like bra som IPv4.

---

[31] DSLAM[31]-er og aksessnoder som i utgangspunktet er lag 2 utstyr, gjør funksjoner som ARP proxy, DHCP snooping etc.
[32] http://labs.ripe.net/Members/mirjam/ipv6-cpe-survey-updated-january-2011
[33] http://en.wikipedia.org/wiki/IPv6_rapid_deployment

I dag er det omlag 25 prosent av nasjonale aktører tilknyttet NIX1(Oslo) som støtter utveksling av IPv6 trafikk.

4.3 Status for sluttkunders hjemmenett

Med hjemmenett menes utstyr og nettkomponenter som privatkunder har installert hjemme, og som de bruker til å sende og motta data på. Dette inkluderer typisk CPE-utstyr levert av tilbyderen som modem, trådløse rutere, Set-Top bokser og annet utstyr kjøpt i butikk av kunden selv som PC-er, spillkonsoller, periferutstyr, etc.

Når det gjelder dagens CPE-utstyr som allerede er levert av tilbyder, er det begrenset støtte for IPv6. Det er også lite sannsynlig at IPv4-utstyr kan oppgraderes i programvare til å støtte IPv6.

Dette betyr at det meste av gammelt utstyr vil måtte skiftes ut med nytt utstyr. Støtte for IPv6 på nytt utstyr er imidlertid sterkt økende.

Et stort volum kunder, både i privat- og bedriftsmarkedet, har sluttbrukerutstyr av type ”DSL modem”. Dette utstyret fungerer i all hovedsak kun som en ”bro”, og har ikke noe forhold hverken til IPv4 eller IPv6. Denne typen sluttbrukerutstyr er altså *klart* for IPv6 fordi det kan sies å være uavhengig av protokoll.

Tilsvarende situasjonen for utstyr levert av tilbyder finner vi også for utstyr og programvare kjøpt i butikk av kunden selv. Generelt er situasjonen slik at nye operativsystem, nettlesere og programvare støtter IPv6, mens eldre programvare og gammelt utstyr ikke støtter IPv6.

Den enkeltes nett og programvareinstallasjonen vil dermed være avgjørende for hvor omfattende oppgraderinger som må gjøres.

I bedriftsmarkedet får mange bedriftskunder sine tjenester levert på sluttbrukerutstyr av type ”managed CPE”; utstyr som tilbyderen selv drifter på vegne av kunden. Det er stor variasjon i denne typen CPE-utstyr og programvareversjoner som kjøres på dette utstyret.
I hovedsak kan CPE-utstyret sorteres i tre kategorier når vi snakker om støtte for IPv6:

1. Utstyr som må byttes ut siden det ikke har mulighet for å støtte IPv6.
2. Utstyr som krever programvareoppgradering for å støtte IPv6.
3. Utstyr som støtter IPv6.

Status for utstyr i sluttkunders hjemmenett og bedrifters private nett er uoversiktlig. Som nevnt er det rimelig å anta at mye av det utstyret som opererer på lag 3 (nettverkslaget/IP-laget) faller under kategori èn.

[34] Norwegian Internet eXchange

5 Tekniske hinder for rask innføring av IPv6

Innholdet i dette kapitlet er i hovedsak basert på informasjon fra aktører i det norske ekommarkedet. Noe informasjon er innhentet ved direkte henvendelser, og noe er basert på aktørers informasjon gitt gjennom norske medier.

Som det fremkommer av kapittel 4, har Norge kommet et godt stykke på vei med å forberede støtte for IPv6. Fortsatt er det imidlertid en del utfordringer som må løses før IPv6 kan brukes på samme måte som IPv4, uten at brukerne trenger å ha noe forhold til hvilken versjon av IP-protokollen som benyttes.

De viktigste utfordringene er:

1. Liten praktisk erfaring blant teknikerne.
2. Potensielt teknisk krevende og kostbare endringer i støttesystemer.
3. Manglende støtte for IPv6 i CPE-utstyr.
4. Tekniske utfordringer knyttet til sikkerhet, time-out og routing.

5.1 Liten praktisk erfaring blant teknikerne

Som det fremgår av kap. 2.2 ser vi at om lag 44 prosent av ISP-ene i Norge ikke har fått tildelt IPv6-adresser. Videre fremgår det at situasjonen er lysere enn som så, ettersom de resterende 56 prosent har markedsandeler på til sammen godt over 75 prosent.

Det er likevel signaler som tyder på at praktisk erfaring med IPv6 i relativt stor grad er mangelvare. Dette gjelder spesielt mindre ISP-er. Det må likevel nevnes at enkelte mindre ISP-er, som Lynet Internett og Broadnet, tilbyr IPv6 i fullskala til sine brukere i eget nett.

Nok tid til testing av alle potensielle scenarioer er en kritisk faktor for vellykket innføring av IPv6, spesielt i store og komplekse nett. Tilbyderne har fremdeles mye gjenstående arbeid innen testing og feilsøking før IPv6 kan innføres i stor skala.

Eksempelvis vil det være nødvendig med kompetanseheving knyttet til drift og overvåkning av IPv6-nett. I tillegg vil det være nødvendig å anskaffe og ta i bruk verktøy tilpasset IPv6, eventuelt en kombinasjon av IPv4 og IPv6.

5.2 Potensielt teknisk krevende og kostbare endringer i støttesystemer

Innføring av IPv6 krever omfattende oppgradering eller utskifting av eksisterende interne drifts-, vedlikeholds- og støttesystemer.
Dette inkluderer støttesystemer for fakturering, kundeadministrasjon, overvåkning og vedlikehold av nettverkselementer, tjenester for provisjonering[35], konfigurering av nettverkselementer og feilretting.

[35] Prosessen med å forberede og utstyre nettverket for å kunne tilby (nye) tjenester til brukerne.

Slike systemer er ofte proprietære, skreddersydd til den enkelte aktør eller produsert lokalt ("in-house"). Endringer og tilpasninger i slike systemer for IPv6-støtte, er i mange tilfeller svært ressurskrevende.

For enkelte systemer vil en tilpasning og/eller oppgradering ikke være mulig, og vil derfor medføre en fullstendig utskiftning av systemet. En omlegging til IPv6 i drifts- og vedlikeholdssystemer vil trolig skje gradvis og på et senere tidspunkt enn for kjerne- og aksessnettene.
En frigjøring av IPv4-adresser fra kunder vil kunne bedre muligheten for å fortsette med IPv4 i slike systemer i et noe lengre tidsperspektiv.

5.3 Manglende støtte for IPv6 i CPE-utstyr

Med CPE-utstyr menes her utstyr på grensesnittet mellom ISP-ens aksess og sluttbrukers private nett.
Som omtalt i kap. 4.3 støtter bare et fåtall av CPE-er som er levert av ISP-en, eller kjøpt over disk, IPv6 i dag. De fleste eksisterende CPE-er kan heller ikke oppgraderes i programvare.

En full oppgradering og utskiftning av CPE-utstyret vil derfor være en omfattende, tidkrevende og kostbar prosess som vil involvere svært mange av dagens kunder. Det er viktig at tilbyderne i sin IPv6-strategi har høy oppmerksomhet på denne delen av verdikjeden, og at oppgradering/utskifting gjøres i høyt tempo.

Utskiftning som gjøres i forbindelse med den ordinære syklusen vil utgjøre det største bidraget, mens faren er at dette kommer for sent i forhold til behovet for innføring av IPv6.

5.4 Tekniske utfordringer knyttet til sikkerhet, time-out og ruting

Sikkerhet – muligheter og utfordringer

Med økende innføring av IPv6 fokuseres det stadig mer på sikkerhetsaspektene. IPv6 åpner for ny og forbedret sikkerhetsfunksjonalitet. Derimot åpnes det også for nye risikoer og sårbarheter.

Det at IPv4 og IPv6 opererer i parallell og deler den samme fysiske infrastrukturen, vil i tillegg vanskeliggjøre implementasjonen av sikkerhetsfunksjonalitetene i IPv6.

Muligheter: Innføring av IPv6 vil kunne gi nye muligheter for økt sikkerhet til nettoperatører og sluttbrukere. Dette inkluderer mulighet for:

- *å etablere en mer oversiktlig og kontrollerbar ende-til-ende sikkerhet.* Som nevnt flere andre steder i rapporten, fjerner IPv6 behovet for å bruke NAT for å spare offentlige adresser. Dette gir grunnlag for fullstendig gjennomsiktig ende-til-ende-sikkerhet.

- *å enklere ta i bruk autentisering og kryptering ved bruk av IPsec.* Autentisering og kryptering er obligatorisk i IPv6 og tilbys gjennom IPsec. I IPv6 er "utvidelseshoder" (extension headers) for autentisering og kryptering blitt definert separat, slik at applikasjoner på høyere nivå kan bruke en av eller begge disse funksjonene når det kreves. Ettersom et IPv6-miljø ikke trenger å bruke NAT, kan disse sikkerhetselementene enkelt tas i bruk.

- *å få utnyttet IPsec fullt ut.* IPsec ble opprinnelig laget for IPv6 men er "tvangstilpasset" IPv4. Dette har ført til at IPv4-implementasjoner av IPsec er mer kompliserte og ressurskrevende enn for IPv6. Det er også komplisert å få utnyttet IPsec fullt ut med IPv4.

- *økt driftssikkerhet.* IPv6 tilbyr utvidede muligheter for ruting og trafikkstyring (prioritering) og har potensial for å gi større driftssikkerhet gjennom en oppgradert og utvidet utgave av DNS (navnetjener).

- *å i større grad legge sikkerheten "der den bør være".* En node som er konfigurert med en rutbar IPv6-adresse blir eksponert mot resten av IPv6-Internett. Altså blir det naturlig at sikkerheten legges på enheten selv.

Utfordringer: Selv om IPv6 gir en rekke sikkerhetsmessige muligheter og legger til rette for forenklinger, er det enkelte ikke-trivielle utfordringer knyttet til praktisk implementering. Dette inkluderer:

- *Manglende erfaring med bekjempelse og forebygging av ondsinnede internettangrep over en IPv6-arkitektur.* IPv6 i nettverks- og sluttbrukerutstyr har som følge av begrenset utbredelse ikke vært like eksponert for forsøk på angrep og integritetsbrudd som tilfellet er på dagens IPv4-implementeringer. En må regne med at det vil avdekkes visse svakheter i nett og utstyr som vil utnyttes ettersom bruken av IPv6 tiltar.

- *Mangel på driftspersonell og administratorer med tilstrekkelig kunnskap og kompetanse til å håndtere kritiske hendelser for IPv6.*

- *Utstyr som feilaktig tror det opererer i et nett med støtte for IPv6.* For mange av dagens operativsystemer er IPv6 førsteprioritet. Operativsystemet vil med andre ord først forsøke å få en IPv6-adresse. Det er viktig å sørge for at IPv6-adresser ikke blir delt ut av enheter i nettet før den nye protokollen faktisk skal innføres. Det er dermed nødvendig å påse at støtte for IPv6 er deaktivert inntil IPv6 faktisk er innført i nettverket. Dette betyr blant annet at DHCP-tjenere i nettet ikke må dele ut IPv6-adresser. I dag støtter alle de vanligste operativsystemene IPv6 sammen med IPv4. Dette gjelder for eksempel Windows Vista, Windows 7, Mac OSX og de fleste Linux-distribusjoner (se også A.3). Som oftest er det IPv6 som blir prioritert av disse operativsystemene.

- *Å sikre servere og nettnoder som ikke skal være synlige på Internett for offentlig eksponering.* Ulike transisjonsmekanismer for å koble sammen IPv4- og IPv6-nett kan øke risikoen for at en ved uhell eksponerer nettsegmenter som skal være beskyttet og skjult. Teknikker for å tiltrekke seg trafikk, overvåke data og opptre med falsk identitet vil trolig videreføres fra IPv4 og tilpasses bruk i IPv6.

Time-out og Ruting

Innholdsleverandører sliter i dag med å få overført innholdet sitt til enkelte "sluttbrukere" som er tilknyttet et IPv4-nett og som benytter applikasjoner og/eller hjemmenett som feilaktig tror de er tilknyttet et IPv6-nett.

Når disse brukerne forsøker å nå en IPv6-applikasjon eller -tjeneste, f.eks. en webside, vil de forsøke med sin ikke-eksisterende IPv6-konnektivitet. Resultatet kan da bli at brukerne opplever at ingenting skjer før et tidsavbrudd oppstår. Avhengig av implementasjon vil applikasjonen enten gi opp å nå tjenesten, eller alternativt forsøke på nytt ved bruk av IPv4.

Uansett utfall er en slik situasjon svært lite ønskelig for leverandør av tjenester på Internett. Problemet kalles ofte for "brekkasje" og antas å være hovedgrunnen til at leverandører av tjenester og innhold nøler med å tilby IPv6-grensesnitt i parallell med IPv4. Problemstillingen er dypere beskrevet i A.1.

Under ”The Gathering 2009” var Ventelo Wholesale gigabitleverandør også med IPv6-støtte. De så blant annet en god del IPv6-transitt basert på IPv6 tunnelert over IPv4. Dette resulterte i mange ”rare” veier fram til mottaker, og ofte merkbart økt forsinkelse.

Konklusjonen ble at for IPv6 isolert sett, er det er kun ”native” IPv6 transitt/peering som bør benyttes. Dette gir raskere transport uten overraskelser.

Forkortelser

6rd	IPv6 rapid deployment
AN	Access Node
ARP	Address Resolution Protocol
CPE	Customer-Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IPFIX	Internet Protocol Flow Information eXport
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet service provider
ITU	International Telecommunication Union
LIR	Local Internet Registries
LTE	3GPP Long Term Evolution
M2M	Machine-to-Machine
NAT	Network Address Translation
NIX	Norwegian Internet eXchange
NTT IPTV	Nippon Telegraph and Telephone Corporation IPTV
OECD	Organisation for Economic Co-operation and Development
OSI	Open Systems Interconnection
OSS	Operations Support Systems
P2P	Peer-to-peer
QoS	Quality of service
RFC	Request for Comments
RIPE NCC	Réseaux IP Européens Network Coordination Centre
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SWOT	Strengths, Weakness, Opportunities, Threats
TCP	Transmission Control Protocol
TOS	Type Of Service
UDP	User Datagram Protocol
UH	Universitet & Høgskole
VoIP	Voice over IP
VPN	Virtual Private Network

Referanser

http://www.idg.no/computerworld/article177915.ece
http://www.broadnet.no/filestore/PDF__xps/Presse__Media/BroadnetlansererIPv6tjeneste_Final.pdf
http://www.lynet.no/lynet/presse/2010-11-03
http://www.mymayday.com/MR/arkiv/MR2002/mr100-ipv6hvor.pdf
http://www.telecomrevy.no
http://www.insidetelecom.no
http://www.digi.no
http://www.idg.no/computerworld/
http://en.wikipedia.org og http://no.wikipedia.org/wiki/Portal:Forside

Øvrige referanser fremkommer som fotnoter gjennom rapporten.

Vedlegg A. Tekniske utfordringer som krever ekstra oppmerksomhet

A.1. Brukkenhet / Brekkasje

A.1.1. Introduksjon til problemet

Rapporten indikerer at det er relativt få nettverksmessige utfordringer knyttet til implementering av IPv6. Både teknologien og relevante standarder betraktes som modne.

Likevel er det en spesifikk feilsituasjon som ser ut til å ha negativ effekt på innholdsleverandørenes motivasjon for å formidle innhold via dual-stack IPv4/v6. Feilen kalles for *brekkasje* eller *brukkenhet*.

A.1.2. Teknisk beskrivelse

Fenomenet brekkasje relateres til hvordan en ISP konfigurerer nettverket sitt, men det er sluttbruker/kunde som i første omgang får redusert sin kvalitetsopplevelse.

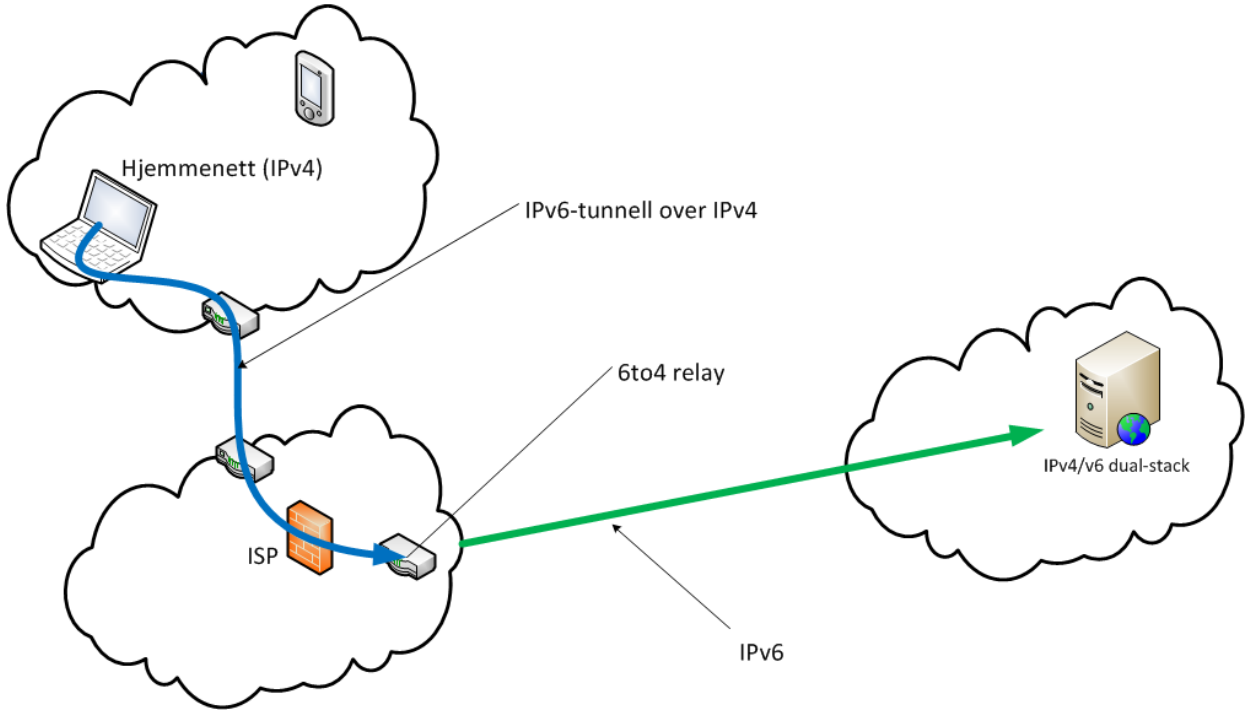
Paradokset er at innholdsleverandøren vil unngå at besøkende opplever problemer med dennes tjenester, og derfor vegrer seg for å tilby innhold via IPv6. Uten tilgjengelig innhold vil det heller ikke eksistere et naturlig behov for å implementere IPv6 hos brukerne, og dermed oppstår raskt en negativ spiral.

Brekkasje oppstår i lokalnett/hjemmenett der følgende kriterier er til stede:

1. Maskiner inneholder applikasjoner som kommuniserer med ressurser på Internett
2. Applikasjonen(e) kan velge mellom å benytte IPv4 eller IPv6, og har IPv6 som sitt førstevalg
3. IPv6-trafikk tunneleres ved hjelp av en transisjonsmekanisme på sin vei fra lokalnett/hjemmenett til IPv6-innhold på Internett

Applikasjonen vil først forsøke å nå den aktuelle ressursen (som er dual-stack) ved hjelp av sin egen IPv6-adresse. Den legger IPv6-pakken inn i en IPv4-pakke, og merker innholdet med protokollnummer 41. Avsenderen har nå etablert sin ende av tunnelen som skal frakte innholdet (IPv6-pakken) gjennom ett eller flere IPv4-nettverk.

Den andre enden av tunnelen termineres i en node som betegnes *6to4 relay*. Dette er en ruter som er satt opp med dual-stack, og som derfor kan videreformidle trafikk fra brukerens applikasjon til IPv6 ressurser på Internett.



Figur 6 Brekkasje – Utgående trafikk

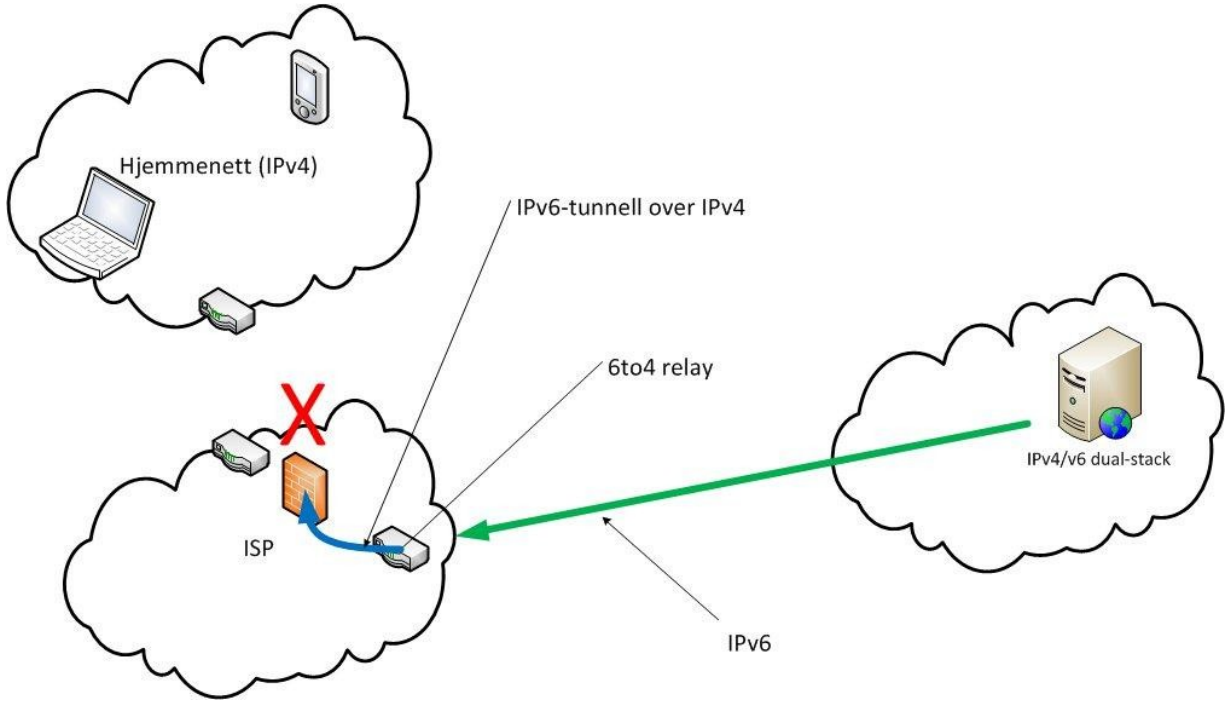
Brekkasje oppstår når trafikken returnerer fra Internett og tilbake til applikasjonen i hjemmenettet. Ressursen/serveren sender IPv6 til et 6to4 relay (gjerne den geografisk nærmeste), herfra blir dataene tunnelert i retning applikasjonen og igjen merket med protokollnummer 41.

Når denne trafikken kommer tilbake til opprinnelig avsenders ISP, vil nettverksutstyr hos ISP-en validere all trafikk som er på vei mot kunden opp mot en godkjenningsliste. I denne listen er det ofte ikke tatt høyde for at IP-pakker merket med protokoll nummer 41 skal få slippe gjennom. Dataene termineres, og applikasjonens forsøk på å etablere en forbindelse med IPv6-ressursen mislykkes ved at det oppstår en time-out.

Hva som så skjer er opp til den enkelte applikasjon, men det viser seg at mange ikke automatisk forsøker forfra igjen, men denne gangen med IPv4 i stedet for IPv6. For mer detaljer, se fotnote[36].

Brukeren vil vanligvis ikke ane noe som helst om detaljene i dette, men opplever likevel at ressursen (for eksempel en web-server) er enten veldig treg eller ikke gir svar i det hele tatt. Veien er dermed kort for brukeren til å prøve en annen leverandør/tjeneste i stedet.

36 http://getipv6.info/index.php/Customer_problems_that_could_occur#.C2.ABBroken.C2.BB_users_unable_to_access_dual-stacked_content



Figur 7 Brekkasje – Returtrafikk

Hvilke systemer er omfattet

1. Windows Vista/7 med Opera nettleser versjon eldre enn 10.50, samt Macintosh eller Linux med Opera nettleser versjon 10.63 eller eldre
2. Windows Vista/7 som benytter BitTorrent applikasjon med IPv6-støtte påskrudd
3. Maskiner fra Apple (Macintosh) som benytter eldre versjoner enn OS X versjon 10.6.5
4. Enkelte implementasjoner av *glibc* (GNU C Library) for bruk på Linux-plattformen
5. Android eldre enn versjon 2.2 Froyo

A.1.3. Mulig løsning

Den enkle løsningen på problemet er å tillate 6to4-trafikk fra Internett og inn til kunden. I praksis betyr dette at ISP-en legger til en regel i sine godkjenningslister som sier at IPv4 merket med protokoll nummer 41 skal slippe gjennom.

Imidlertid vil dette gjøre kunden mer utsatt for skadelig programvare, fordi den innkapslede IPv6-pakken samt dens innhold ikke lett lar seg inspisere. Kunden er dermed i større grad eksponert for trusler i IPv6-delen av Internett.

Dette stiller høyere krav til lokal beskyttelse i form av brannmurer og antivirusprogramvare på kundens egen maskin, i tillegg til at maskinen bør være satt opp med de seneste sikkerhetsoppdateringene.

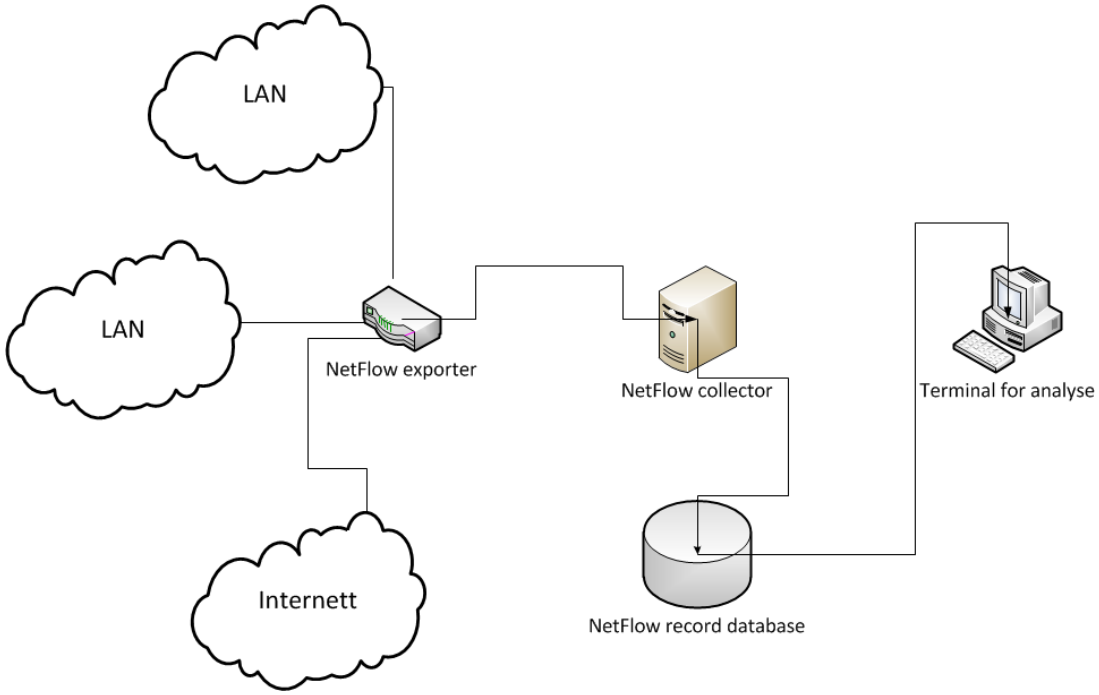
En annen løsning er å implementere IPv6 i nettet hos både ISP og kunde. Dersom dette implementeres fornuftig vil en unngå problematikk rundt tunnelering og blokkering av data. Da legger en også til rette for at brukere av IPv6-tjenester ikke får redusert sin opplevelse som følge av ikke-optimal konfigurering hos sin ISP.

Moderne nettverksutstyr som brukes av ISP-ene kan overvåke hvilken type trafikk som fraktes over IPv6. Dermed ivaretas i stor grad sikkerhetselementet i henhold til brukerens behov og ISP-ens eventuelle forpliktelser.

A.2. NetFlow

NetFlow er en protokoll som samler informasjon om trafikk i et IP-nett. Protokollen kommer opprinnelig fra Cisco, og er etter hvert blitt de facto standard for denne type verktøy. Utstyr fra andre produsenter er nå også kompatible med NetFlow.

Protokollens oppslutning kommer også til uttrykk ved at den nå formelt sett er erstattet av Internet Protocol Flow Information eXport (IPFIX), beskrevet av IETF i en rekke RFC-er. Mange utstyrsprodusenter legger nå til støtte for IPFIX i sine produkter.



Figur 8 NetFlow

Begrepet Flow (Flyt) er ikke entydig, men tradisjonelt har det vært brukt om en sekvens av IP-pakker som, i tillegg til å bevege seg i samme retning, alle har følgende parametre felles:

1. IP-avsenderadresse
2. IP-mottakeradresse
3. Avsender TCP- og UDP-portnummer, eventuelt 0 for andre protokoller
4. Mottaker TCP- og UDP-portnummer, eventuelt ICMP-type og -kode, eller 0 for andre protokoller
5. IP-protokollnummer
6. Ingress grensesnitt (SNMP)
7. IP Type of Service (TOS)

En ruter vil sende ut en Netflow Record når den anser at en trafikkstrøm som møter ovenfor nevnte kriterier, er avsluttet.

Et eksempel kan være når en av tilbyderens kunder er ferdig med å laste ned en film fra Internett. Detaljert informasjon om denne hendelsen (varighet, rutinginformasjon og antall bytes, i tillegg til de syv nevnte parametre) sendes fra ruteren og til en node som samler sammen slike rapporter (NetFlow collector). Disse rapportene er viktige fordi:

1. Analyse av dataene gir informasjon om trafikkmønstre og trafikkmengder i nettverket for netteier/ISP
2. Informasjonen kan benyttes til å verifisere trafikkopplysninger ved forespørsel fra påtalemyndighet og politi

A.2.1. NetFlow og IPv6

Det er kun den siste utgaven (NetFlow v9) og IPFIX som har støtte for IPv6-data. Netteiere/ISP-er som benytter NetFlow i sine rutere, må derfor sørge for å benytte riktig versjon før implementering av IPv6. Dette vil igjen medføre at maskinvare og operativsystem i ruteren må støtte NetFlow v9, noe som ikke nødvendigvis er tilfelle for eldre utstyr.

Potensielt sett kan dette være et hinder på veien mot full implementering av IPv6 hos netteier/ISP. Tilbakemelding fra UNINETT indikerer at nettopp problematikken med manglende IPv6-støtte for NetFlow er direkte årsak til at enkelte universiteter og høgskoler ikke ønsker å innføre IPv6 enda.

A.3. Operativsystemer som Windows 7

I dag støtter alle de vanligste operativsystemene IPv6 sammen med IPv4. Dette gjelder for eksempel Windows Vista, Windows 7, Mac OS X og de fleste Linux-distribusjoner. Som oftest er det IPv6 som blir prioritert.

Moderne applikasjoner, som ser at operativsystemet støtter begge versjoner av IP-protokollen, vil med andre ord først forsøke IPv6 (se A.1). Dersom dette ikke lykkes, vil systemet forsøke å bruke IPv4.

Operativsystemene er satt opp på denne måten for å gjøre overgangen til den nye Internett-protokollen så sømløs som mulig den dagen nettverket maskinen står på begynner å støtte IPv6. Ettersom IPv6 er førsteprioritet er det viktig å sørge for at IPv6-adresser ikke deles ut før den nye protokollen faktisk skal implementeres. Det anbefales derfor å skru av støtte for IPv6 før det skal brukes (f.eks. kan det være lurt å sørge for at DHCP-tjenere i nettet ikke deler ut IPv6-adresser).

Vedlegg B. UNINETT og IPv6

Innføring av IPv6 i UNINETTs kjernenett startet for om lag 10 år siden. Etter hvert som nettverksutstyr ble byttet ut, sørget en for at innfaset utstyr kom med full støtte for IPv6.

Dette har medført at UNINETT sitt kjernenett i dag benytter IPv6 i parallell med IPv4 (dual-stack). Utenfor kjernenettet benyttes native IPv6 internt i deler av UNINETTs egen organisasjon.

Teknikere ved UNINETT betegner det som trivielt å rulle ut IPv6 i kjernenett. Dette forutsetter da at nettverksutstyret er tilrettelagt for IPv6 fra leverandørens side. Det er rimelig å anta at utstyr som er mindre enn tre år gammelt bør kunne kjøre IPv6, dette gjelder spesielt utstyr i kjernenettene.

UNINETT holder informasjonsmøter der de deler sin erfaring knyttet til hva som kreves for å innføre IPv6. På deres nettsider presenteres også en innføringsplan på overordnet nivå.

Aktører som trenger råd og veiledning er velkomne til å kontakte den erfarne IPv6-gruppa ved UNINETT. For detaljert oversikt over innføringen av IPv6 på universiteter og høgskoler, vises det til UNINETTs GigaCampus side[37]. Her finnes også annen nyttig IPv6 informasjon. Siden inneholder også "Best Practises" for innføring og bruk av IPv6 i en organisasjon.

UNINETT har en type live-tjeneste som viser hvor mange IPv6-klienter som er aktive innenfor UH-sektoren. Tallene viser at det er store forskjeller mellom de enkelte institusjonene når det gjelder utberedelsen av IPv6.

Kilder tilknyttet UNINETT mener det foreløpig er mest interessant å vite noe om antall aktive klienter, fremfor den aktuelle trafikkmengden disse genererer.

UNINETT har IPv6-peering på NIX med 10 – 15 ISP-er.

GigaCampus arbeider aktivt med å øke utbredelsen av IPv6 i UH-sektoren. Status finnes på nettsidene deres[38], og her er noen kjernepunkter (høsten 2010):

- **Alle** universiteter og høgskoler har fått **tildelt** IPv6-adresseblokker fra UNINETT (se oversikt[39]).
- **14** GigaCampus-institusjoner får sin IPv6-adresseblokk **rutet** ut til sitt campusnett.
- Av disse igjen viser statistikken hvem som har **reell bruk**, for tiden **8**, hvorav noen av disse igjen har få aktive maskiner.
- UNINETT fører også oversikt over hvilke sentrale tjenester (e-post, web, etc.) IPv6 er innført for ved den enkelte organisasjon tilknyttet UNINETT.

[37] https://ow.feide.no/gigacampus:ipv6
[38] https://ow.feide.no/gigacampus:ipv6status
[39] http://drift.uninett.no/nett/ip-nett/ipv6-address-delegation