**Rapportnummer**
PTS-ER-2011:18

**Datum**
2011-XX-YY

# Att införa internetprotokollet IPv6

## En praktisk beskrivning för offentlig sektor

*Remissversion 2011-09-08*

**Att införa internetprotokollet IPv6**

**Rapportnummer**
PTS-ER-2011:18

**Diarienummer**
11-157

**ISSN**
1650-9862

**Författare**
Erika Hersaeus, NS1
Joakim Aspengren, NS2
Anders Rafting, NS2
Roland Svahn, NS1

**Post- och telestyrelsen**
Box 5398
102 49 Stockholm
08-678 55 00
pts@pts.se
www.pts.se

# Förord

De flesta verksamheter i vårt samhälle är allt mer beroende av att kunna kommunicera elektroniskt. Utrustning som ansluts till internet kräver en unik adress och måste använda gemensamma regler s.k. protokoll för att kunna kommunicera med varandra. Adresserna som används i den hittills dominerande standarden för detta, IPv4, internetprotokoll version 4, håller på att ta slut.

För att internet ska kunna fortsätta växa med fler tillämpningar och användare, krävs tillgång till fler adresser – ett behov som den nya standarden IPv6 kan tillgodose. Genom införande av IPv6 vid sidan om IPv4, kan en organisation behålla och förbättra sin förmåga att vara nåbar för alla även i framtiden.

Genom att tjänster som tillhandahålls av offentlig sektor görs tillgängliga även via IPv6, väntas effekten bli att IPv6 tar fart. Ett flertal rapporter har tidigare tagits fram som beskriver varför IPv6 behövs och som har fyllt sin uppgift som underlag för ledningsgrupper att ta ett strategiskt beslut om införande av IPv6. Denna rapport är tänkt som nästa steg med sin mer praktiska inriktning. Syftet är att vara till stöd för it-personal i arbetet med att installera och driftsätta IPv6 i sin organisation.

Stockholm den XX oktober 2011

Göran Marby

Generaldirektör

# Innehåll

# Sammanfattning

....

# Abstract

……

# 1 Bakgrund

## 1.1 Regeringsuppdrag om att ta fram en beskrivning över införande av IPv6

Post- och telestyrelsen, PTS, har fått i regeringsuppdrag[1] att ta fram en beskrivning över hur införande av den nyare adresseringsstandarden IPv6, Internet Protocol version 6, kan ske på myndighetsnivå. Beskrivningen ska fungera som stöd vid införande av IPv6.

Beskrivningen ska redogöra för konsekvenser av införandet av IPv6 med avseende på tillgänglighet, säkerhet och ekonomi. PTS egna erfarenheter av införande samt beaktande av andra relevanta aktörers arbete avseende IPv6 ska även redogöras för.

Den ska också beskriva eventuella komplikationer vid införande av IPv6 i en organisations publika e-tjänster samt ge förslag på åtgärder hur dessa kan hanteras. Dessutom ska beskrivningen redogöra för vilka konsekvenser införandet av IPv6 har på ekonomi, säkerhet och tillgänglighet.

I uppdraget anges att PTS ska göra en konsekvensanalys av IPv6 som enda protokoll.

Till sist ska PTS även beskriva hur E-delegationens vägledning för införande av IPv6 från december 2010 ska förvaltas och utvecklas.

## 1.2 Syfte med beskrivningen

Syftet med beskrivningen är att den ska fungera som stöd för aktörer inom offentlig sektor i införande av IPv6 vid sidan av IPv4. Det innebär en konkret beskrivning innebärande en teknisk vägledning för det praktiska genomförandet.

## 1.3 Målgrupp för beskrivningen

Den primära målgruppen för beskrivningen är personal som arbetar med IT-frågor i organisationen, främst till dem som har ansvar för publika e-tjänster. Därmed är beskrivningen på en praktisk och teknisk nivå. Vad som avses med publika e-tjänster i denna beskrivning beskrivs i avsnitt 1.4.

## 1.4 Beskrivningens omfattning och avgränsningar

Beskrivningen redogör för införande av IPv6 i publika e-tjänster samt i nödvändiga säkerhetsrelaterade funktioner i syfte att behålla en hög

[1] , Dnr: 11-157

tillgänglighet och säkerhet. Med andra ord definieras och avgränsas publika e-tjänster till de e-tjänster som en organisation kommunicerar externt med sina användare/kunder. Med publik e-tjänst avses i denna beskrivning organisationens:

- Internetanslutning
- Brandvägg
- DNS (server som hanterar adress- och domännamnsuppslagningar, s.k. intern resolver och s.k. extern auktoritär)
- Webbplats
- E-postkommunikation (skicka samt ta emot e-post av e-postservrar som stödjer IPv6)
- Intern åtkomst av resurser på internet som endast stödjer IPv6/ Internetsurfing från det interna nätverket ut på internet

I uppdraget anges att PTS ska göra en konsekvensanalys av IPv6 som enda protokoll. Samexistens kommer att råda i överskådlig framtid, därför ges en begränsad redogörelse över IPv6 som enda protokoll i bilaga.

## 1.5 Metod

Beskrivningen baserar sig på underlag från en konsultrapport genomförd av Interlan Gefle AB. Därutöver baserar sig rapporten på kompetens vid PTS och de erfarenheter som finns vid myndigheten vid införandet av IPv6.

PTS har vidare samrått beskrivningen med ett antal aktörer. Dessa är E-delegationen, Skatteverket, Kammarkollegiet, .SE, CERT-SE, Myndigeten för samhällsskydd och beredskap (MSB). Synpunkter från områden har inarbetats löpande i beskrivningen.

Ett utkast av beskrivningen har varit föremål för en bred remiss hos ett stort antal aktörer.

## 1.6 Läsanvisningar

Huvudtexten redogör för ett övergripande tillvägagångssätt för införande av IPv6. Ett antal bilagor kompletterar huvudtexten. I bilagorna ges bl.a. konkreta exempel på lösningar för produkter och tjänster som förekommer inom

offentlig förvaltning. PTS lägger ingen värdering gällande olika produkter och tjänster. I bilagorna finns även regeringsuppdraget och ordlista m.m.

Rapportens huvuddisposition i texten är:

**Kapitel 2:** Om tillvägagångssätt för införande av IPv6 och övergripande om de fyra grundläggande faserna.

**Kapitel 3:** Om inventering. Hur säkerheten och tillgängligheten bibehålls, kravställning, val av addresstyp, krav på all berörd utrustning för extern kommunikation, övervakning, ramavtal och utbildning mm.

**Kapitel 4:** Om planering. Ansökan av IPv6-adresser via ett LIR, nätverksstruktur ,beställning av IPv6-internetanslutning från en internetleverantör, att upphandla eventuellt ny utrustning, om att se över processer, rutiner och säkerhetspolicier för att även inkludera IPv6-trafik och IPv6-nät.

**Kapitel 5:** Om genomförande.Aktivering av IPv6 i internetanslutning och berörd utrustning etc.

**Kapitel 6:** Om förvaltning. Vikten av att ha en kontinuitetsplan. Övervakning, uppföljning och anpassning för bibehållen tillgänglighet. Kontroll av DNS-funktionalitet.

**Kapitel** 7: Sammanfattning av konsekvenser vid införande av IPv6.

**Kapitel 8:** PTS förslag gällande förvaltning av beskrivningen och av E-delegationens vägledning samt förslag till fortsatt arbete**.**

# 2 Införande av IPv6

I detta kapitel redogörs först för motiv för införande av den nyare adresseringsstandarden, IPv6, vid sidan av IPv4 (s.k. dual stack). Därefter redogörs övergripande för införande av IPv6 i publika e-tjänster.

Det övergripande sättet vid hantering av IPv6 och införande av protokollet skiljer sig inte mycket från IPv4. De grundläggande funktionerna (t.ex. DMZ, TCP, UDP, http, smtp och DNS) är i huvudsak desamma. Det finns dock vissa skillnader, vilka kommer att belysas.

## 2.1 Motiv för införande

Det finns flera olika skäl för att införa IPv6. Avsnittet kommer att utvecklas.

### 2.1.1 Dagens adresser på internet håller på att ta slut

För att datorer, smarta mobiltelefoner, surfplattor och andra enheter på internet ska kunna kommunicera med varandra krävs att varje enhet tilldelas en unik IP-adress. Standarden för adressering på internet är IPv4, Internet Protocol version 4. IPv4-adressen består 32 bitar och möjliggör 4 294 967 296 unika adresser (eller ca 4,3 miljarder adresser).

IPv4-adresserna håller på att ta slut. Någon gång under 2011 och 2012 beräknas det inte finnas några fler att tilldela till organisationer som önskar fler adresser.

### 2.1.2 En standardiserad lösning på adressbristen – IPv6

Det finns en nyare adresseringsstandard, Internet Protocol version 6 kallat IPv6, för att lösa adressbristen. IPv6-adressen består av 128 bitar, vilket medför 2^128 adresser eller 3,4 • 1038 adresser (340 282 366 920 938 463 463 374 607 431 768 211 456 ). Detta innebär en ofantligt stor adressrymd som sannolikt kommer att räcka för all överskådlig framtid.

### 2.1.3 IPv6 möjliggör kommunikation med alla på internet

I dagsläget är knappt en tredjedel av jordens invånare anslutna till internet. En stor del av innevånarna i de regioner där åtkomst till internet byggs ut de närmaste åren, kommer sannolikt att använda IPv6-kommunkation. Det kommer under mycket lång tid finnas användare som fortsatt kommunicerar med den gamla standarden IPv4.

De båda standarderna IPv6 och IPv4 är två olika kommunikationsprotokoll med skilda adressformat som inte är kompatibla med varandra. De kan gå i samma kabel, men de kan inte kommunicera med varandra. Det kommer att

dröja innan all kommunikation sker över IPv6. Därför är det av yttersta vikt att alla organisationer kan stödja båda protokollen samtidigt genom s.k. dual stack. Detta gör det möjligt att kommunicera med alla på internet.

## 2.2 Börja i liten skala och utifrån och in

Vid införande av IPv6 i en organisations publika e-tjänster är det grundläggande rådet att börja i liten skala. Vidare behöver IPv6-införandet utföras ”utifrån och in”. Dessa övergripande råd är viktiga för att behålla en fortsatt hög tillgänglighet och säkerhet.

I första hand bör följande funktioner och tjänster, som en organisation kommunicerar med användare externt, vara tillgängliga över både IPv6 och IPv4, s.k. dual stack:

- Internetanslutning/-ar
- Brandvägg
- DNS:er: s.k. intern resolver och extern auktoritär DNS
- Webbplatser
- E-postkommunikation (skicka och/eller ta e-post mot e-postservrar som stödjer IPv6).
- Internetsurfing från det interna nätverket ut på internet.
- Intern åtkomst mot resurser på internet som stödjer IPv6

Avgränsa och prioritera arbetet gällande införandet av IPv6 utifrån organisationens behov och resurser. Att införa IPv6 för alla dessa funktioner och tjänster på en gång är nästintill omöjlig uppgift och riskerar att göra övergången för stor för att hantera. Dra istället nytta av att IPv4 och IPv6 kan samexistera och inför IPv6 stegvis.

## 2.3 Starta införandet i tid

Det finns flera fördelar med att påbörja införandet av IPv6 i tid. Då kan kostnader för införandet planeras. Vidare slipper man ett införande under tidspress, vilket kan påverka tillgänglighet och säkerhet. Om man väntar för länge med att påbörja införandet av IPv6 kan det uppstå situationer där man kan tvingas ta till skyndsamma åtgärder med risk för mindre lämpliga lösningar.

Samtliga arbetsmoment för införandet tar tid. Det förberedande arbetet inför införandet tar tid och bör får ta sin tid; inventering av intern it-miljö och av nya hård-/mjukvara med stöd för IPv6 och som uppfyller organisationens säkerhetskrav. Vidare tar upphandling, med framtagning av säkerhets- och funktionella krav på utrustning/programvara, samt ställtider från beställning till leverans av IPv6-stöd tid och riskerar att fördröja införandet, m.m.

Utöver detta krävs att personal vidareutbildas och lär sig att hantera det nya protokollet. Det tar tid.

## 2.4 Ta beslut om införande och tillsätt ett införandeprojekt

Det har visat sig att den svåraste frågan gällande IPv6 har varit att fatta beslut om att införa det i organisationen. Organisationer som har infört eller kommit långt med införande av IPv6 tycks ha berott på att det funnits en eller några eldsjälar som har drivit frågan i organisationen. Ofta har 5-10 procent av en årsarbetskrafts tid har räckt för att organisationen ska komma igång med arbetet med införande av IPv6.

Tillsätt ett projekt för att underlätta och effektivisera införandet av IPv6 i organisationen. Målbild och tidplan kan variera utifrån organisationens beslut, behov, krav.

## 2.5 Arbeta i fyra faser – inventera, planera, genomföra och förvalta

Att införa IPv6 kräver ett systematiskt och planerat tillvägagångssättför att behålla en fortsatt hög säkerhet och tillgänglighet. Ett införande bör ske strukturerat i fyra faser. Det är

- att inventera
- att planera
- att genomföra
- att förvalta.

Vissa aktiviteter i inventerings- och planeringsfaserna kan göras parallellt.

Aktiviteter och råd inom respektive fas kommer att beskrivas i följande kapitel. Tillvägagångssätt presenteras i en kronologisk ordning för att underlätta införandet.

# 3 Inventera

I detta kapitel beskrivs ett antal aktiviteter som behöver genomföras i det förberedande arbetet för att kunna införa IPv6 i organisationen.

## 3.1 Inventera IT-miljön

Innan IPv6 kan införas i nät och tjänster är det viktigt att inventera organisationens IT-miljö. Syftet med inventeringen är att identifiera behov av åtgärder för att tjänster ska ha stöd för både IPv4 och IPv6. Dokumentera befintlig utrustning med avseende på förändringsbehov av att kunna stödja dual stack, dvs. både IPv4 och IPv6. Inventeringen är, beroende av storlek på miljö och kvalitet på befintlig dokumentation.

Inventera och dokumentera

- berörda serverplattformar med avseende på mjuk- och hårdvara med stöd för IPv6
- nätverksutrustning, nätverksstruktur och adressering på en mer övergripande nivå med stöd för IPv6
- klientplattformar (operativsystem samt programvaror) med stöd för IPv6
- identifiera tjänster och funktioner som ansvaras för internt respektive funktioner som tredje part ansvarar för.

Utifrån tillgänglighet, säkerhet och ekonomi inventera följande funktioner:

- Internetanslutning
- Brandväggslösningar
- DNS-lösningar
- Webblösningar
- E-postlösning
- E-postfiltreringslösning

- Accesswitch
- L3-switch
- Accesspunkter för uppsättning av trådlösa nät
- DHCPv6-server
- VPN-lösning
- Proxylösning för aktivering av IPv6 på klientdatorer
- Administrationsverktyg
- Övervakningsverktyg

## 3.2 Utred förslag på åtgärder för att införa IPv6 med bibehållen säkerhet och tillgänglighet

Efter inventeringen av IT-miljön krävs ett utredningsarbete i syfte att identifiera lämpliga åtgärder. Det avser åtgärder så att utrustningen kan stödja såväl IPv6 som IPv4 och ha bibehållen säkerhet och tillgänglighet.

### 3.2.1 Upprätthåll säkerheten i nivå med IPv4

Det är viktigt att säkerheten inte försämras vid införande av IPv6. De säkerhetsfunktioner som är implementerade med IPv4 måste ge samma skydd efter införande av IPv6. Något som inte är helt självklart. Ett vanligt exempel är att enheter kan adresseras med IPv6, men att säkerhetsfunktionerna inte kan analysera samt blockera skadlig trafik.

### 3.2.2 Inventera lämpliga produkter

Utredningsarbetet kan bestå i att inventera produkter på marknaden med stöd för IPv6 och t.ex. beaktande säkerhet, tillgänglighet och ekonomi (kommersiell mjukvara/hårdvara, öppen källkod).

Läs produktleverantörers information avseende IPv6- och säkerhetsstöd i aktuell hårdvara/mjukvara för att få kännedom om dess IPv6-mognad. I eventuell kontakt med tillverkaren, begär en lista över funktioner som stödjer respektive inte stödjer IPv6.

Man bör kontrollera att produkter med IPv6-stöd även ger ett likvärdigt

administrativt gränssnitt som vid administration av IPv4. Produkters befintliga gränssnitt kan i vissa fall inte vara uppdaterat/uppdateras med avseende på IPv6. Användaren hänvisas till att administrera IPv6-funktionalitet via konfigurationsfiler eller kommandotolk. Något som kan försvåra det dagliga arbetet.

### 3.2.3 Gör en risk- och sårbarhetsanalys för införandet

Beaktande resultatet av inventeringen av mjukvara/hårdvara med stöd för IPv6 samt säkerhetsaspekter, gör en risk- och sårbarhetsanalys avseende införandet av IPv6 göras för att bedöma risker och hotbilden mot nätverket.

Utifrån risk- och sårbarhetsanalysen kan åtgärder vidtas för att minimera risker och ta fram reservplaner.

### 3.2.4 Utred om tjänster ska ansvaras för i egen regi eller läggas ut externt

I inventerings- eller planeringsarbetet bör en översyn göras över hur publika e-tjänster som t.ex. webb, DNS (domännamnssystemet), e-postkommunikation ska ansvaras för. Ett alternativ är i egen regi, ett annat är att läggas ut externt. Resultatet har påverkan på vad som behöver beaktas i det fortsatta arbetet, t.ex. kravställning och upphandling av tjänster.

Oavsett om DNS ansvaras för i egen regi eller externt, är en korrekt uppsatt DNS-infrastruktur en förutsättning för fungerande IPv6-kommunikation.

För mer konkreta råd se bilagor X, Y.

### 3.2.5 Gör en årtgärdsförandeplan för övergången

Gör en åtgärdsplan över vad som behöver åtgärdas för att funktioner och tjänster ska ha stöd för dual stack med fortsatt hög tillgänglighet och säkerhet.

## 3.3 Anpassa ramavtal och upphandlingsunderlag med krav på IPv6

I regelbundna översyner av upphandlingsunderlag gällande elektroniska kommunikationstjänster är det lämpligt att kravställa stöd för IPv6. Beakta därutöver krav på säkerhet och tillgänglighet. På detta sätt innebär införandet av IPv6 inga direkta merkostnader i denna del.

Om så inte har skett, måste nu en anpassning av underlagen göras inför införandet av IPv6.

Mer konkreta råd att beakta i kravställning ges i bilaga X.

### 3.3.1 Använd Kammarkollegiets ramavtal för IT och telekom

Kammarkollegiet har ett flertal ramavtal på IT-området som statliga myndigheter, kommuner och landsting kan använda sig av. Ramavtalen finns på http://www.avropa.se. De är grupperade i flera områden, t.ex.:

- Datakommunikation, nätverk och telefoni
- IT-Driftstjänster
- IT-konsulttjänster (t.ex. uppdragskonsulter)
- PC och tjänster
- Programvaror och tjänster
- Servrar, lagring och produktnära tjänster
- IT-utbildning
- E-förvaltningsstödjande tjänster

Avtalen är utformade på olika sätt och har olika detaljeringsgrad, vilket gör att varje organisation måste se till sina behov och rikta krav utifrån dessa.

Avtalen ger möjlighet att erhålla både tjänster och produkter. Exempel på tjänster är:

- IT-utbildning avseende IPv6

- Uppdragskonsulter att ta fram en genomförandeplan för IPv6.

### 3.3.2 Kravställ enligt rekommendationer från RIPE

Inom RIPE (det tekniska internetsamfund i Europa- och Mellanösternregionen), har ett kravdokument om IPv6 i ICT-utrustning framarbetats. Dokumentet är tänkt att fungera som stöd vid upphandling av ny ICT-utrustning med stöd för IPv6. Den tar upp krav att tänka på för olika typer av utrusning kopplade till internet (lager 2-switch, lager tre, brandvägg osv.). Dokumentet har dokumentationsnummer/-id ripe-501 och finns på http://www.ripe.net/ripe/docs/ripe-501#2text (på engelska). Kravdokumentet kommer med sannolikhet att utvecklas ytterligare av RIPE.

## 3.4 Inventera utbildningsbehov

Under inventerings- och planeringsarbetet, dvs. innan IPv6 införs, är det lämpligt att se över IT-personalens behov av utbildning avseende IPv6. Kurser som belyser särskilda skillnader mellan IPv4 och IPv6 är värdefulla.

Några dagars utbildning brukar räcka om kompetens finns på IPv4.

# 4 Planera

I detta kapitel ges både tillvägagångssätt och mer konkreta råd för hur planering för införande av IPv6 kan ske. Planera införandet av IPv6 utifrån framtagen checklista under inventeringen. Det underlättar genomförandet och kan även medföra upptäckt av eventuella felbedömningar.

Aktiviteter inom inventering och planering kan utföras parallellt. Planeringsfasen innehåller flera viktiga moment för ett väl införande.

## 4.1 Planera adresser

RIPE NCC[2] har bl.a. i ansvar IP-adresshantering i Europa- och Mellanösternregionen. RIPE har tagit fram en policy för hur tilldelning av IPv6-adresser får ske. För mer information om den, se IPv6 Address Allocation and Assignment Policy[3].

### 4.1.1 Välj typ av IPv6-adress

En stor skillnad mellan IPv4- och IPv6-adresser är att IPv6-adresser är globalt adresserbara[4] även på insidan av brandväggen. Det finns två olika typer av IP-adresser s.k. Provider Independent (s.k. PI eller operatörsberoende adresser) och s.k. Provider Aggregatable (PA). Utred i god tid vilken IP-adresstyp som ska användas.

Med PI-adresser kan organisationen behålla sina IPv6-adresser (dvs. sin nätverksstruktur) i händelse av byte av internetleverantör. Organisation som har tilldelats PI-adresser får inte dela ut dessa till tredje part.

Med PA-adresser behöver organisationen numrera om sitt nät i händelse av byte av internetleverantör.

För att bli beviljad PI-IPv6-adresser krävs att organisationen som ansöker är s.k. multi-homed (dvs. har internetanslutningar till minst två olika leverantörer). Viktigt att tänka på är att om PI-adresser ska användas, krävs det att gränsroutern mot internetleverantören har stöd för BGP[5] och IPv6. Det kan vara ett stort steg att börja med multi-homing och BGP för en mindre organisation.

---

[2] Reseaux IP Européens Network Coordination Center ,det regionala internetregistryt för Europa och Mellanöstern, http://www.ripe.net
3 IPv6 Address Allocation and Assignment Policy, ripe-523
[4] GUA, Global Unicast Address, se bilaga Y.
5 Border Gateway Protocol, se bilaga Y.

IP-adresser kostar i sig inget. Men det finns en årlig avgift för att täcka administrationskostnader hos RIPE NCC. Kostnaden uppgår till några tiotusentals kronor per år.

### 4.1.2 Ansök om adresser

För att ansöka och bli beviljad adresser krävs att organisationen:

- fyller i aktuellt ansökningsformulär (IPv6 PI Assignment Request Form)[6]. Det finns att ladda ner på RIPE NCC:s webbsida, http://www.ripe.net/ripe/docs/ripe-467 . Instruktioner för hur ansökan bör fyllas i finns http://www.ripe.net/ripe/docs/ripe-483

- ingår avtal med LIR bl.a. om att förse med aktuella kontaktuppgifter till organisationen vid var tid och hur IPv6-adresser får användas (Contractual Requirement for Provider Independent Resources Holders in the RIPE NCC Service Region). Original med underskrift ska skickas till RIPE NCC.

Mer information om avtalet finns på följande länk: http://www.ripe.net/lir-services/resource-management/direct-assignments/independent-assignment-request-and-maintenance-agreement

Då en korrekt ansökan och undertecknat avtal har skickats in till RIPE NCC, direkt till RIPE NCC eller via sitt LIR, kommer adressblocket att tilldelas organisationen.

## 4.2 Ta fram en adressplan

En internetleverantör, eller ett LIR, delar normalt ut ett prefix på 48 bitar till varje organisation. Det innebär fler IPv6-adresser än vad det finns IPv4-adresser totalt sett. Mer specifikt innebär det 65 536 stycken 64-bitars subnät (eller s.k. LAN-segment). Ett 64-bitars subnät är den minsta rekommenderade subnätsmasken[7] i ett IPv6-nät och ger 1,8 *10^19 adresser.

En väl genomtänkt nätverksstruktur och adressplan är en förutsättning för fungerande IPv6-kommunikation.

[6] Ansökan, dokument-id: ripe-467
[7] Subnätsmask definierar i antal bitar vilken del av IP-adressen som är lokal och vilken som tillhör prefix.

Det finns flera sätt hur adressplan och nätverksstruktur kan göras. Ett sätt är att utgå ifrån er adressplan för IPv4-adresser och vlan[8].

Planera och dokumentera en nätverksstruktur och adressplan för IPv6. Bestäm även hur dynamiska adresser ska delas ut; SLAAC eller DHCPv6. En rekommendation är att alltid använda DHCPv6.

Tidsåtgången för att ta fram en adressplan beror på storlek och komplexitet i infrastrukturen. Gäller det en liten organisation (t.ex. en liten kommun) med få segment går det relativt fort. Gäller det ett landsting med flera hundra anslutningar är det mer komplext och tar längre tid.

Det är vidare viktigt att adressplanen finns väldokumenterad och hålls uppdaterad.

För mer information om hur en adressplan kan tas fram, se bilaga X alternativt Surfnets manual[9] (på engelska).

## 4.3 Beställ IPv6-internetanslutning från en internetleverantör

Det första är att utreda om internetleverantören kan tillhandahålla en IPv6-internetanslutning. Om det är så, bör en följdfråga vara hur lång tid det tar för leverans. Fråga efter IPv6-referenser från internetleverantören; finns erfarenhet av tekniken, finns andra IPv6-kunder osv.

En viktig fråga i kravställning gentemot internetleverantör är om den kan leverera s.k. transit[10] för multihoming[11] med BGP och inte endast kapacitet.

Beroende på om organisationen avser vara s.k. multihomed krävs olika typer av IPv6-adresser. Se avsnitt 4.2.3 Välj typ av adresser för vilken typ av IPv6-adresser organisationen ska ansöka om.

Det är viktigt att ställa och erhålla samma SLA-krav på IPv6-anslutningen som på IPv4.

Överväg att tillfråga en annan leverantör för tillhandahållande av en IPv6-internetanslutning om de inte kan leverera tjänsten med samma SLA-krav eller om leveransen tar allt för lång tid.

[8] Virtual LAN – teknik för att bygga logiskt skilda nätverk som transporteras över samma fysiska infrastruktur.
[9] Preparing an IPv6 Addressing Plan -Manual
[10] Se ordlista, bilaga x.
[11]

En rekommendation är att inte använda en tunnelleverantör för skarp drift av en IPv6-internetanslutning. Det kan däremot fungera i labbsammanhang.

Ett stöd för beställning av internetanslutning över IPv6 är Kammarkollegiets ramavtal, se avsnitt 3.3.1.

Krav att ställa på internetleverantören är:

- Native IPv6-anslutning med PA- eller PI-adresser. Om PI-adresser används, krävs att såväl internetleverantören som organisationen hanterar BGP för IPv6 PI-adresser.

- DNS-resolvrar: Operatörens resolvrar ska ha stöd för frågor och uppslag över IPv6.

Använder man internetleverantörens e-postreläer (s.k. Mail Transfer Agents) för utgående e-post ska den vara konfigurerad med IPv6.

Mer konkreta råd att beakta i kravställning ges i bilaga X.

## 4.4 Upphandla ny utrustning och tjänster

Om kravställning av IPv6-stöd och säkerhetsaspekter inte har gjorts för ny utrustning (hårdvara/mjukvara) och för tjänster (internetanslutning, DNS, webben, e-postservrar m.m.), är det dags att anpassa upphandlingsunderlag med krav på dessa. Beakta att detta normalt tar tid.

Se avsnitt 3.2.4 och 3.3 för inventeringsarbete i dessa frågor. Mer konkreta råd att beakta i kravställning ges i bilaga X.

## 4.5 Se över processer, rutiner och säkerhetskrav för att inkludera IPv6

Innan IPv6 införs i organisationen är det viktigt att se över befintliga processer och rutiner så att de omfattar IPv6-trafik och -nät. Trafik över IPv6 ska driftas och förvaltas på samma sätt, på samma allvar, som för IPv4.

T.ex. kan risk- och sårbarhetsanalyser ses över så att de beaktar IPv6-trafik/hot samt rutiner för penetrationstester.

### 4.5.1 Ta fram en kontinuitetsplan

I händelse av att en störning eller avbrott uppstår är det är viktigt att organisationen har tagit fram en kontinuitetsplan. Syftet med en kontinuitetsplan är att ha en beredskap och förmåga att hantera oönskade

händelser som exempelvis avbrott och störningar i publika e-tjänster, IT- och administrativa system etc. på ett snabbt och systematiskt sätt. Planen ska även säkerställa att verksamheten vid ett eventuellt avbrott i IT-stödet kan bedrivas i begränsad omfattning, men under kontrollerade förhållanden. Kontinuitetsplanering innefattar även att vidta åtgärder för att förebygga eller minimera effekten av en oönskad händelse.

En kontinuitetsplan för IPv6 kan i stort påminna om den för IPv4.

# 5 Genomföra

Efter inventerings- och planeringsarbetet kan genomförandet påbörjas. Genomförandet består av att införa IPv6 genom successiv och kontrollerad aktivering och driftsättning. Efter varje driftsättning krävs att övervakning sker för en bibehållen god funktion och säkerhet m.m., se avsnitt 6.2.

## 5.1 Aktivera IPv6-internetanslutning

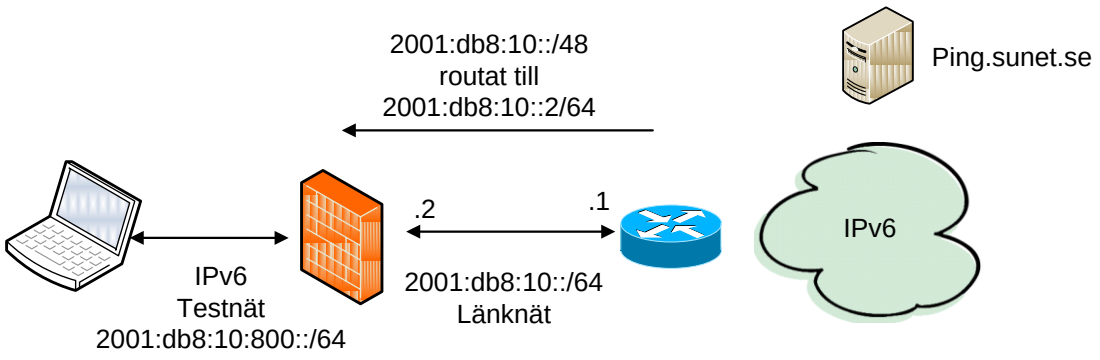
Första steget i genomförandet är leverans av IPv6-internetanslutning från internetleverantören.

### 5.1.1 Verifiera att trafiken fungerar

När en internetleverantör har aktiverat IPv6 fram till brandväggen är det viktigt att kontrollera att den tilldelade adressrymden fungerar. Konfigurera eventuella egna routrar som är anslutna direkt mot internetleverantören (gränsrouter eller default gateway router). Kontrollera att ni vet att IPv6 är korrekt routat från operatören genom att ansluta en dator på insidan och testa genom brandväggen. Gör det från ett isolerat nät så att ni inte annonserar IPv6 på en plats där ni inte vill det eller om ni är osäker på vad ni gör.

Ett testkommando är `ping -6 ping.sunet.se`. Fungerar inte det, testa med `tracert -6 ping.sunet.se` för att se hur långt ni kommer (traceroute i Linux och Unix).

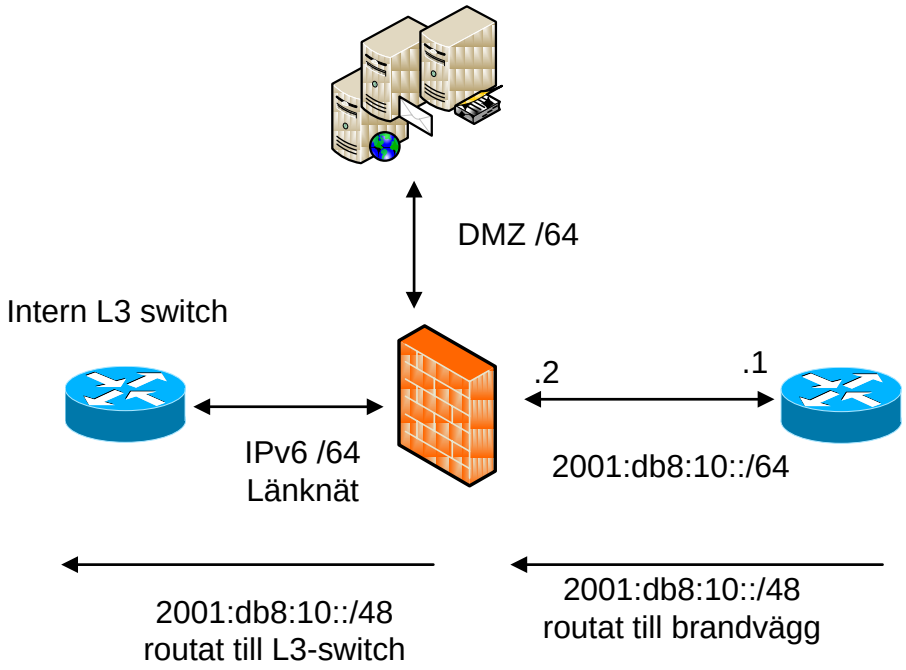
Bilden visar hur aktivering av IPv6 mot internetleverantör kan se ut:




Har ingen funktionskontroll av detta gjorts är det vanligt med problem och störningar med fördröjningar och anslutningar som inte fungerar. Så börja utifrån och arbeta in genom brandväggen.

## 5.2 Fördela tilldelade adresser utifrån adressplanen

När internetanslutningen är aktiverad och kontrollerad kan IPv6-införandet fortsätta. Den /48 som ni tilldelats ska nu fördelas på alla segment där IPv6 ska aktiveras. Nedanstående bild visar hur /48:an routas ett steg längre in till den interna centralswitchen (s.k. L3-switch).




### 5.2.1 Att tänka på vid användning av PI-adresser

Vid införandet av PI-adresser ska man tänka på att ett s.k. route6-objekt är skapat i RIPE NCC:s databas. Gör ni en sökning på adressrymden ska ett route6-objekt finnas i den, se exempel på PTS nedan.

```
route6:     2001:67c:dc::/48
descr:      PTS
origin:     AS50273
mnt-by:     RESILANS-MNT
source:     RIPE
```

Om route6-objektet inte finns, kommer adresserna med största sannolikhet inte att routas överallt på internet.

## 5.3 Konfigurera brandväggen för IPv6

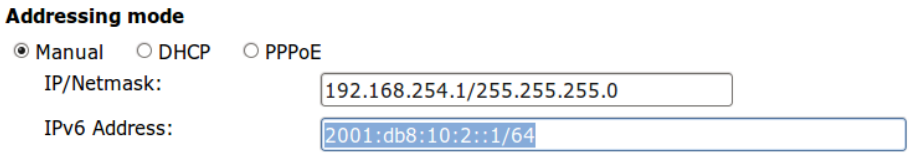
Efter att internetleverantören har aktiverat IPv6 för er internetanslutning och kontrollen har gjorts, kan aktivering av IPv6 i brandväggen ske.

### 5.3.1 Numrera interface i brandväggen

Nu är det dags att numrera interface i brandväggen enligt framtagen adressplan. Ett exempel på hur detta kan utföras, se nedan.

| Interface | Adress | Eventuell statisk route |
|---|---|---|
| Internal | 2001:db8:10:2::1/64 | 2001:db8:10::/48 via 2001:db8:10:2::10 |
| Wan1 | 2001:db8:10:ffff::2 | ::/0 via 2001:db8:10:ffff::1 |
| Etc. | | |

Bilderna nedan visar i ett typiskt administrationsgränssnitt hur lika det är att administrera regler för IPv6 och IPv4.



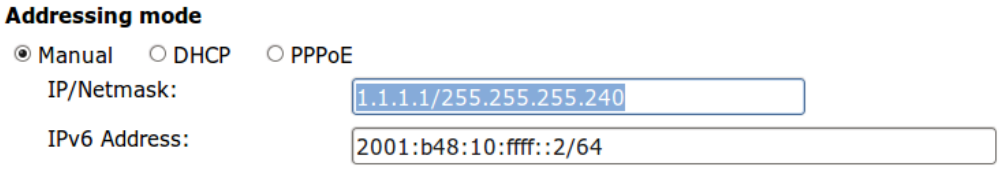
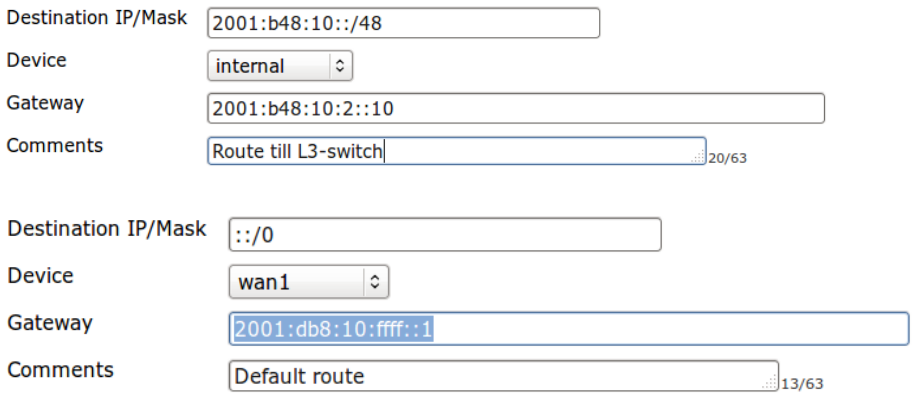



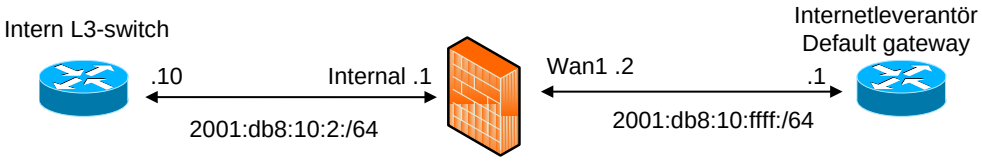

Bild på uppsättning av route till intern L3-switch och default route mot resten av världen.




### 5.3.2 Sätt upp regler för IPv6 i brandväggen

Sätt upp de mest nödvändiga brandväggsregler först. Vänta med enstaka tjänster tills de är aktuella att IPv6-aktiveras.

Att aktivera IPv6 och sätta upp interface, routes, hostar, nät och regler påminner om tillvägagångssättet för IPv4. I en del brandväggar hanterar man IPv4 och IPv6 i samma regelverk. I de flesta använder man dock separata adresslistor och regelverk. I bilden nedan visas ett exempel på uppsättning:



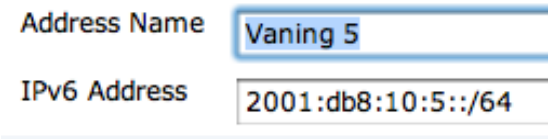

Gå igenom och dokumentera vilka hostar, nät, protokoll och portar som ska vara source samt destination i brandväggen. Det är en fördel att göra detta innan man börjar med uppsättningen av reglerna. Då sparar man tid och behöver skapa färre regler. För hur dokumentation kan göras, se tabellen nedan:

| Source | Protokoll/Port | Destination |
|---|---|---|
| All | http | www.myndighet.se |
| All | Smtp | Mail.myndighet.se |
| Våning 5 | IP-telefoni | IPteleservice |
| DNS-servrar | DNS | All |

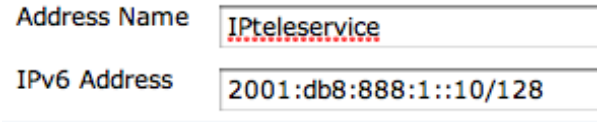
| | | |
|---|---|---|
| m.m. | - | - |

**Ett exempel på regel att lägga upp i brandväggen**
Bilderna nedan visar hur regler för nät, hostar och tjänster för ett visst segment, t.ex. våning 5 i en organisation, kan läggas upp i brandväggen.

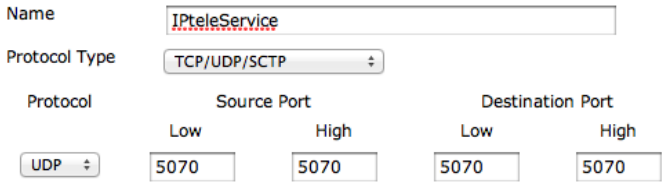
1. **Lägg upp nätet Våning 5**




2. **Lägg upp hosten IPteleservice**




3. **Skapa tjänsten för att köra över UDP-porten 5070**




4. **Lägg till sist upp regeln**

| | |
|---|---|
| Source Interface/Zone | internal |
| Source Address | Vaning 5 |
| Destination Interface/Zone | wan1 |
| Destination Address | IPteleservice |
| Schedule | always |
| Service | IPteleService |
| Action | ACCEPT |

### 5.3.3 Att tänka på om ICMPv6 i brandväggen

I IPv4-världen anses Ping och ICMP generellt vara olämpliga protokoll så de filtreras ofta bort i brandväggen. För IPv6-trafik är däremot ICMPv6 viktigt. Filtrera inte bort okända ICMPv6-typer. Om det är nödvändigt att filtrera bort dessa, filtrera som mest bort ICMPv6 echo request och ICMPv6 echo reply.

Neighbor Discovery Protocol (NBP, RFC 4861[12]) är grundläggande i IPv6 och använder ICMPv6.NDP motsvarar bl.a. Address Resolution Protocol (ARP) i IPv4. Var därför försiktig med filtrering, för blir det fel slutar IPv6 att fungera. Mer rekommendationer för filtrering av ICMPv6, se RFC 4890[13].

## 5.4 Konfigurera och driftsätt routrar, switchar och annan nätverksutrustning

Aktivera IPv6 på de switchar och routrar, steg för steg, som behövs för att uppnå de första införandemålen.

Slå av automatisk adresstilldelning hos routern (SLACC, StateLess Auto Configuration) och se till att servrar kan ansluta med statiska adresser. Detta ger större kontroll över vilka servrar som blir IPv6-aktiverade och underlättar felsökning.

## 5.5 Aktivera IPv6 för serverplattformar

Inför IPv6 i en server åt gången. Innan IPv6-aktiveringen aktiveras i ytterligare funktioner och tjänster är det viktigt att testa att tjänsten fungerar som den ska, att den har hög tillgänglighet och säkerhet och inte påverkar andra tjänster på ett negativt sätt.

[12] http://tools.ietf.org/html/rfc4861
[13] http://www.ietf.org/rfc/rfc4890.txt

### 5.5.1 Aktivera IPv6 i DNS

De flesta DNS-servrar har stöd för IPv6. För mer information om hur aktivering av IPv6 görs i DNS, se bilaga X. Det finns flera råd vid kravställning av IPv6-stöd för DNS (dvs. auktoritär DNS samt intern resolver).

### 5.5.2 Aktivera IPv6 för publik webbplats

De flesta webbservrar inklusive dess operativsystem, CMS-system (Content Management System) samt webbmotorer (t.ex. Apache) har IPv6-stöd idag.

Om den interna organisationen ansvarar för den publika webbplatsen, aktivera IPv6 i operativsystemet. Konfigurera servermjukvara att lyssna på IPv6-adresser och se över eventuella konfigurationer av hostar och CMS-system. Om CMS-system används kommer de oftast med automatik att fungera med IPv6 eftersom de byggs som tillägg till webbservrar.

För att kunna aktivera IPv6 i webbservern, krävs det att hela kedjan från internetleverantör, brandvägg, webbserver fungerar över IPv6 med god funktion. Lägg inte upp något AAAA RR, utan sätt upp ett temporärt namn för webbtjänsten i DNS eller hostfil för att verifiera funktionen.

Om extern leverantör ansvarar för webbtjänsten är det viktigt att kravställa IPv6-stöd vid upphandling av tjänsten. Dessutom är det viktigt att kringfunktioner för webbtjänsten har stöd för IPv6-trafik, som t.ex. statistikföring så att organisationens trafik och trafikmönster kan mätas (antal besök osv. över IPv4 respektive IPv6).

Det är vanligt att lastdelare/proxys används för att säkerställa webbserverns kapacitet. I detta fall måste lastdelaren ha stöd för IPv6, medan IPv6-stöd på webbservern inte blir nödvändig.

### 5.5.3 Aktivera IPv6 för e-post

Det finns flera lösningar för hur e-postkommunikation kan ske över IPv6 (MTA, e-postreläer, e-postservrar). För mer information om detta, se bilaga 4.

Det finns flera olika hårdvaror och programvaror för att filtrera bort spam och virus i e-postkommunikation. Kontrollera status för IPv6 och hur IPv6 aktiveras i dem med tillverkare.

## 5.6 Möjliggör åtkomst till externa IPv6-tjänster för klientdatorer på det interna nätverket

Åtkomst till externa IPv6-tjänster för klientdatorer på det interna nätverket kan uppnås på ett antal olika sätt. Det kan göras antingen genom att aktivera native

IPv6 eller aktivering av IPv6 i en proxyserver. Vilken metod man väljer, beror på hur den befintliga miljön ser ut, vilken proxy som används (stöd finns inte i alla) och hur den interna infrastrukturen ser ut.

Aktiverandet via native eller proxy (dvs. lösning 1 i 5.5.2) är att föredra då de är enklare att aktivera och underhålla än övriga förslag.

### 5.6.1 Aktivera native IPv6

Alla moderna operativsystem stödjer IPv6. Genom att aktivera IPv6 på det interna nätverket kan aktuella datorer nå externa datorer/resurser som har stöd för IPv6 eller IPv4. Med native-lösning kan IPv6-stöd för alla möjliga tänkbara tjänster och funktioner fås som normalt inte använder en proxyserver, t.ex. IP-telefoni.

### 5.6.2 Alternativ aktivering genom proxy

Exempel på lösningar för att aktivera IPv6 i klientplattformar genom proxy är:

1. Om proxyservern stödjer IPv6, kan IPv6 enkelt aktiveras för alla datorer som använder den.

2. Om proxyn inte stödjer IPv6, kan s.k. policybaserad routing tillämpas. I detta fall styr routern om t.ex. http-trafik för IPv4 till proxyn, medan http för IPv6 passerar. Denna lösning ska ses som tillfällig. Om proxytjänsten ansvaras för av en extern leverantör, bör ni kravställa IPv6-stöd från denna. Kan leverantören inte erbjuda stödet, överväg att låta en annan leverantör tillhandahålla tjänsten.

3. Som sista förslag på lösning, visas hur man kan sätta upp en proxy med IPv6-stöd framför proxyn som inte har stödet.

De två senare lösnigarna kan tillämpas om t.ex. den befintliga proxyn har identitetshantering, filtrerar innehåll och/eller virusskannar.

Det finns idag även proxy- och säkerhetstjänster som tillhandahålls i molnet. Om en sådan lösning används bör organisationen ställa krav på IPv6-stöd för den. Är öppen källkod en lösning, är Squid och Tinyproxy två alternativ. För fler öppna källkodslösningar, se bilaga X – Öppen källkod.

## 5.7 Kontrollera och övervaka

När IPv6 är aktiverat är det viktigt att övervaka och följa upp att trafik och trafikmönster sker på samma nivå och med samma säkerhetskrav som för

övervakning och statistikföring för IPv4. För mer information om övervakning, se avsnitt 6.1.

Precis som för IPv4 bör t.ex. penetrationstester genomföras efter att IPv6 införts.

# 6 Förvalta

När IPv6 har införts krävs en löpande förvaltning. Förvaltning innebär att övervaka, justera och anpassa tekniken.

## 6.1 Övervaka, följ upp och anpassa för bibehållen tillgänglighet

Övervakningsverktyg för IPv6 finns både som kommersiella verktyg och programvaror med öppen källkod. Webbportalen Freshmeat samlar programvaror med öppen källkod (http://www.freshmeat.net).

Exempel på övervakningsverktyg är What's up, Nagios (http://www.nagios.org) och Cacti (http://www.cacti.net).

### 6.1.1 Övervaka IPv6-trafiken och särskilj larm från IPv4 och IPv6

En del övervakningsprogram kan inte ge larm om det är störning från IPv4 eller IPv6. Därför är viktigt att skilja på larm från övervakning om det avser IPv4 eller IPv6. Detta i syfte att kunna vidta åtgärder för att hantera avbrott och störningar. Samma kvalitet bör råda på övervakning över IPv6 som på IPv4.

För att få särskilja larm från IPv4 och IPv6 kan man sätta upp olika namn för diverse servrar, t.ex. för en webbserver. På nedanstående sätt kan övervakning ge larm om alla möjliga kombinationer för IPv4- och IPv6-trafik i händelse av att något protokoll inte fungerar.
http://ipv4-only.myndighet.se (endast IPv4, A RR)
http://ipv6-only.myndighet.se (endast IPv6, AAAA RR)
http://dualstack.myndighet.se (både IPv4 och IPv6, A och AAAA RR)

### 6.1.2 För driftstatistik över trafikmängd och tillgänglighet

Det är viktigt att föra statistik över trafikmängd och tillgänglighet till olika tjänster, t.ex. DNS, e-post och publika e-tjänster. På detta sätt får man kännedom om IPv6 fungerar som det ska. Information om trafikmängd kan även vara bra för att anpassa så att utrustning klarar av trafikmängden. Ett exempel är om en eventuellt mindre IPv6-brandvägg behöver uppgraderas.

Med t.ex. Cacti[14] kan statistik föras och trender urskiljas på ett enkelt och överskådligt sätt.

[14] http://www.cacti.net

Om din brandvägg inte stödjer funktionen MIB[15] för IPv6-trafik kan separat statistik för IPv4 respektive IPv6 erhålla genom att använda ett interface för IPv4 och ett för IPv6 mot internetleverantören.

## 6.2 Hantera störningar

Olika former av störningar kan inträffa. I detta avsnitt ges några råd för att kunna hantera dessa på ett systematiskt och tillfredställande sätt.

### 6.2.1 Dokumentera inträffade incidenter och följ upp orsaker

Dokumentera systematiskt inträffade incidenter. Detta i syfte att kunna följa upp orsaker till avbrott och störningar. Det ger också möjlighet att felanmäla buggar till leverantörer.

IPv6 har ännu inte samma mognad som IPv4 då det inte har tillämpats lika länge och i samma utsträckning. Det är därför extra viktigt att eventuella problem och hinder följs upp. Därmed uppnås successivt en bättre funktionalitet.

### 6.2.2 Kontakta CERT-SE vid IT-incidenter

CERT-SE är Sveriges nationella CSIRT (Computer Security Incident Response Team) med uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter. Verksamheten bedrivs vid Myndigheten för samhällsskydd och beredskap (MSB). Till CERT-SE:s uppgifter hör bland annat att:

- Agera skyndsamt vid inträffade IT-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i arbete som krävs för att avhjälpa eller lindra effekter av det inträffade.

- Samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet.

- Vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt utveckla samarbetet och informationsutbytet med dessa.

I händelse av avbrott och/eller störningar, kontakta CERT-SE. Deras kontaktuppgifter är:

E-postadress: cert@cert.se
Telefonnummer: 08-678 57 99.

[15] Management Informaiton Base

# 7 Förslag på fortsatt arbete

I detta kapitel redovisas ett antal förslag på fortsatt arbete kring IPv6-frågan.

## 7.1 Förslag X gällande fortsatt arbete

…..

# Bilaga 1 –Uppdraget från regeringen

**Utdrag ur uppdrag till PTS avseende IPv6**

**Regeringens beslut (N2010/7521/ITP)**

Regeringen uppdrar åt Post- och telestyrelsen (PTS) att beskriva hur IPv6 kan införas på myndighetsnivå med avseende på tillgänglighet, säkerhet och ekonomi. Syftet med beskrivningen är att den ska kunna fungera som stöd till myndigheter, kommuner och andra organisationer i offentlig sektor i deras införande av IPv6. PTS ska i detta arbete ta tillvara de erfarenheter som myndigheten fick när den under våren 2010 implementerade IPv6 i delar av sin IT-miljö. Inom uppdraget ska PTS även göra en konsekvensanalys av införandet av IPv6 som enda protokoll men även i samexistens med IPv4.

PTS ska beakta det arbete som utförts av dels E-delegationen, dels Stiftelsen för Internetinfrastruktur (IIS) men även andra liknande arbeten inom och utanför Sverige. PTS ska samråda med E-delegationen, andra berörda myndigheter och berörda aktörer inom privat sektor. PTS bör även, inom arbetet med uppdraget, inhämta erfarenheter från andra myndigheter och organisationer som har implementerat eller står i begrepp att implementera IPv6. Beskrivningen ska gälla såväl intern som extern kommunikation. PTS ska också beskriva aspekter kring säkerhet, robusthet och funktionalitet i kommunikation och tjänster vid införandet av IPv6 samt vilka komplikationer som kan uppstå och hur man kan åtgärda dessa. E-delegationen har under hösten 2010 tagit fram en vägledning för myndigheternas införande av IPv6. PTS ska i samråd med E-delegationen föreslå hur denna vägledning ska förvaltas och utvecklas.

Uppdraget ska delredovisas till Regeringskansliet (Näringsdepartementet) senast den 31 december 2010 och slutredovisas tillsammans med en ekonomisk redovisning senast den 31 oktober 2011.

Anna-Karin Hatt

# Bilaga 2 – Råd vid kravställning

## Att tänka på vid kravställning av DNS-tjänst i extern regi

DNS-tjänsten består av två funktioner: extern auktoritär och resolver. Ofta erhålls en resolver från din internetleverantör i samband med anskaffning av internetanslutning.

När en extern aktör ansvarar för din DNS-tjänst är det viktigt att ställa krav på IPv6 för såväl resolver som auktoritär DNS. Alla moderna DNS-mjukvaror har stöd för IPv6. DNS bör inte vara både auktoritär och resolver samtdigt.

Ett best practice är att ha minst två geografiskt åtskilda auktoritära DNS:er, helst med olika AS-nummer, som stödjer IPv6.

## Att tänka på vid kravställning för dina domännamn och domännamnstjänster

Kravställ så att er domännamnsleverantör (DNS-operatör, registrar) som ansvarar för er DNS-tjänst och hos vilken era domäner är registrerade, behöver hantera s.k. IPv6 glue records[16]. En del registrarer hanterar detta, men inte genom deras normala webbgränssnitt (GUI) utan det sköts via t.ex. en e-post till deras supportavdelning.

Val av DNS-operatör bör väljas utifrån de behov och krav som finns i organisationen utifrån IPv6 samt säkerhet för domännamnsuppslagning t.ex. DNSSEC.

**Kravställ IPv6 mot din webbserverleverantör** När webbservern ansvaras för externt, kravställ att webbserverleverantören har IPv6-stöd för er webbtjänst. De flesta operativsystem och webbservrar har stöd för IPv6 i dagsläget.

Använder organisationen en proxy/lastdelare för att skydda webbservern, krävs det att den har stöd för IPv6. Då blir inte IPv6 påslaget i webbserver nödvändig längre.

[16] Se bilaga x, ordlista.

# Bilaga 3 - Råd för fortsatt hög tillgänglighet och säkerhet

I denna bilaga ges mer konkreta råd för att behålla en fortsatt hög tillgänglighet och säkerhet vid införande av IPv6. En del råd är produktspecifika. Råden ges i en kronologisk ordning efter hur införandet bör genomföras, på samma sätt som i huvudtexten.

Flera brandväggar har stöd för IPv6 i dagsläget, dvs. det går att skapa regelverk för trafikflöden för IPv6. Dock kan vissa viktiga säkerhetsfunktioner som den tillhandahåller sakna stöd för IPv6. En sådan funktion är UTM[17]-funktionen, vilken används för att t.ex. sätta upp regler för användning/begränsad användning av diverse applikationer.

I inventeringsarbetet bör man undersöka vad som skiljer IPv6-brandväggens funktioner från IPv4-brandväggen (t.ex. stöd för statistikföring och användargränssnitt) så att stödet är fullgott med IPv4 som möjligt.

Det är viktigt för en brandvägg med stöd för IPv6, att dess kringfunktioner även har stöd för IPv6.

Används en brandvägg med en flerårig, dyr licens och vilken inte stödjer IPv6, kan en ny med stöd för IPv6 anskaffas och placeras parallellt med den tidigare för att hantera IPv6-trafik till det interna nätverket. Den senare behöver initialt inte ha samma kapacitet som den för IPv4.

## Korrekt uppsatt DNS är en förutsättning för fungerande kommunikation över IPv6

För att DNS med adressering och domännamnsuppslagning (dvs. vanlig namnuppslagning och bakåtuppslagning) ska fungera på ett korrekt och enkelt sätt över IPv6 är det viktigt att DNS är uppsatt korrekt. En välordnad DNS-struktur för klienter, servrar och annan utrustning är en förutsättning för framgångsrik användning av IPv6.

IPv6-adressernas längd gör att DNS blir en än viktigare funktion i infrastrukturen.

Senare versioner av DNS-mjukvara har stöd för att svara på frågor som innehåller IPv6-information.

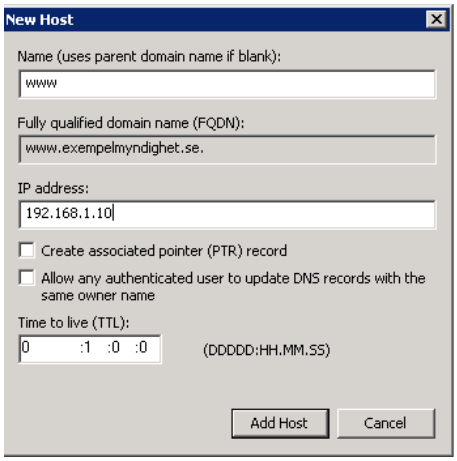
[17] Se bilaga 1 – Ordlista.

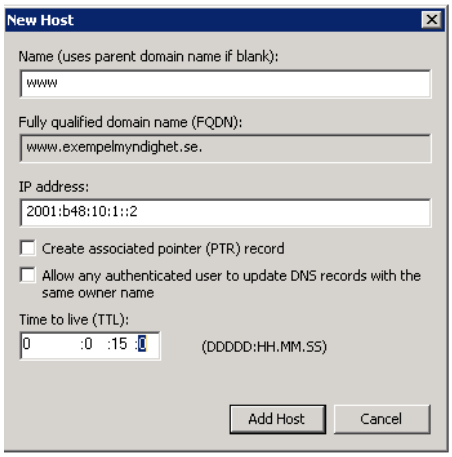
Att DNS kan utföra förfrågningar om IPv6 respektive att DNS-servern har anslutning över IPv6 är två skilda saker.

## Att tänka på om IPv6 och DNS TTL

I händelse av att problem uppstår med IPv6 är det är viktigt att inte sätta för långa TTL:er på sina RR så att man snabbt kan ta bort dem i DNS:en och på så sätt stabilisera tjänsten och få bort IPv6-trafiken dit. Detta är mer en inkörningsprocedur än en långsiktig lösning men är det är viktigt att känna till hur man enkelt och snabbt kan backa ur ett problem om man inte har gjort rätt från början.

I en Windows DNS visas inte alternativet med separat TTL per RR normalt utan man måste gå via meny Visa->Avancerat för att det alternativet ska synas och kunna ändras. Det går på så sätt att ha olika TTL:er för IPv4 och IPv6 och på så sätt snabbt kunna inaktivera IPv6 på t.ex. en publik e-tjänst.



I BIND skriver man:

```
www         3600              IN              A
            192.168.1.10
www         1800                    IN        AAAA
            2001:db8:10:1::10
```

## Råd vid användning av CNAME

En ytterligare viktig sak att tänka på är att om CNAME[18] används, kan många tjänster aktiveras för IPv6 utan att man tänkt på det. Aktiverar ni ett AAAA RR på en server kommer alla CNAME mot det namnet att aktiveras med IPv6 utan att man kanske vill det. Tänk även på att CNAME kan knytas mot andra domäner så det behöver inte bara vara huvuddomänen.

[18] Canonical Name record eller ett alias

## Relationen mellan DNS, IPv4 och IPv6

Med endast IPv4 är det enkelt att förstå hur DNS:en fungerar. DNS ställer och svarar då på frågor över IPv4 och all information om A, MX, PTR osv. den lämnar eller hämtar handlar om IPv4.

Med IPv6 blir det mer komplext. En DNS som endast har IPv4 aktiverat kan hantera IPv6 RR som AAAA eller ip6.arpa. En DNS med endast IPv6 aktiverat kan hantera A och in-addr.arpa. Detta är viktigt att förstå så man inte sätter upp IPv6-only-DNS:er för att hantera IPv6 RR osv.

Se en dig över IPv4 och IPv6 som exempel

```
dig +short aaaa www.pts.se @192.121.211.226
2001:67c:dc:1810::2
```

Den här frågar över IPv4 men begär och får ett AAAA RR som svar.

```
dig +short a www.pts.se @2001:67c:dc:43::227
192.121.211.215
```

Den här frågar över IPv6 men begär och får ett A RR som svar.

## Att tänka på avseende intern användning av IPv4 PA-/PI-adresser

En del organisationer använder PA/PI IPv4-adresser på det interna nätverket. Då uppstår problem om 6to4 inte har inaktiverats redan, se avsnitt Viktigt om Tunnlar i Windows nedan.

Om PA/PI används på det interna nätverket bakom brandväggen kommer datorn/servern automatiskt att generera en 6to4 adress enligt 2002:IPv4-address::IPv4-adress och registrera den i DNS:en om den är medlem i ett Active Directory. Andra datorer med native IPv6 påslaget kommer då först försöka nå datorer med 6to4 på deras onåbara IPv6-adress vilket kan medföra stora störningar.

## Viktigt om tunnlar i Windows

Windows Vista/7 och Windows server 2008 har tunnlarna Teredo och 6to4 installerade. För att minska felkällor för IPv6 är en rekommendation att ni inaktiverar dessa. 6to4 har i dagsläget stora problem med stabiliteten. Det finns en RFC-draft som rekommenderar att 6to4 ska inaktiveras globalt på alla hostar. Båda ställer också till problem med native IPv6 i det interna nätverket om ni vill aktivera och använda Microsofts VPN-feature Direct Access. Se exempel på denna länk:

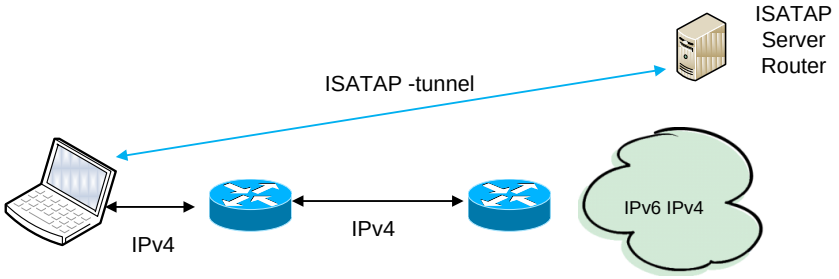
http://www.circleid.com/posts/microsoft_direct_access_is_it_heaven_or_hell_for_ipv6/.

Med nedanstående kommandon inaktiverar ni 6to4 och Teredo:

```
netsh interface teredo set state disabled
netsh interface 6to4 set state disabled
```

## Tunnelprotokollet ISATAP

ISATAP[19] är en tunnel som också är aktiverad i Windows, men som bara används i det interna nätverket. Den ger datorer och servar möjlighet att få IPv6 på platser där det inte går eller är för dyrt att aktivera i närmaste router. Se bilden nedan




Om inte ISTAP ska användas så inaktivera det med:

```
netsh interface isatap set state disabled
```

## Inaktivera Router Advertisment

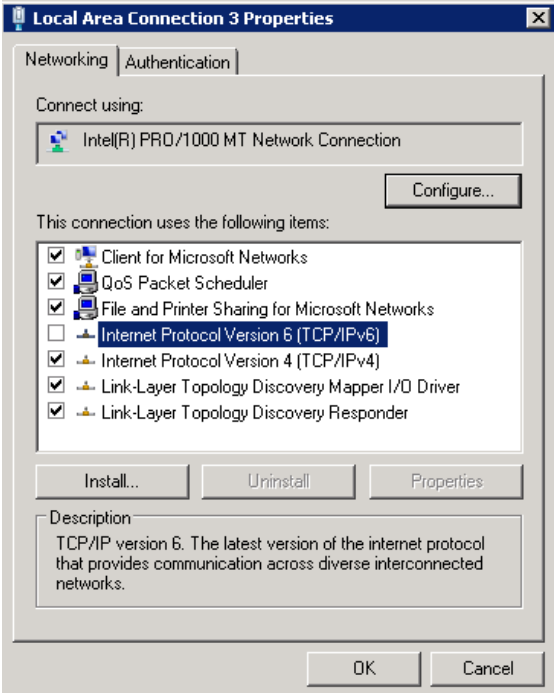
I VLAN, där man inte vill att SLAAC och/eller DHCPv6 ska användas, är det en god idé att inaktivera RA fullständigt. Exemplet nedan är från Cisco och nedanstående kommando inaktiverar Router Advertisment då bara statiska adresser kan användas på aktuellt VLAN

```
interface vlan 100
    ipv6 nd suppress-ra
```

## Inaktivera IPv6 på nätverkskortet

Inaktivera alltid IPv6 på nätverkskortet istället för globalt i Windowsdatorn så slipper ni bl.a. problem när ni ska aktivera IPv6 på datorn igen.

19



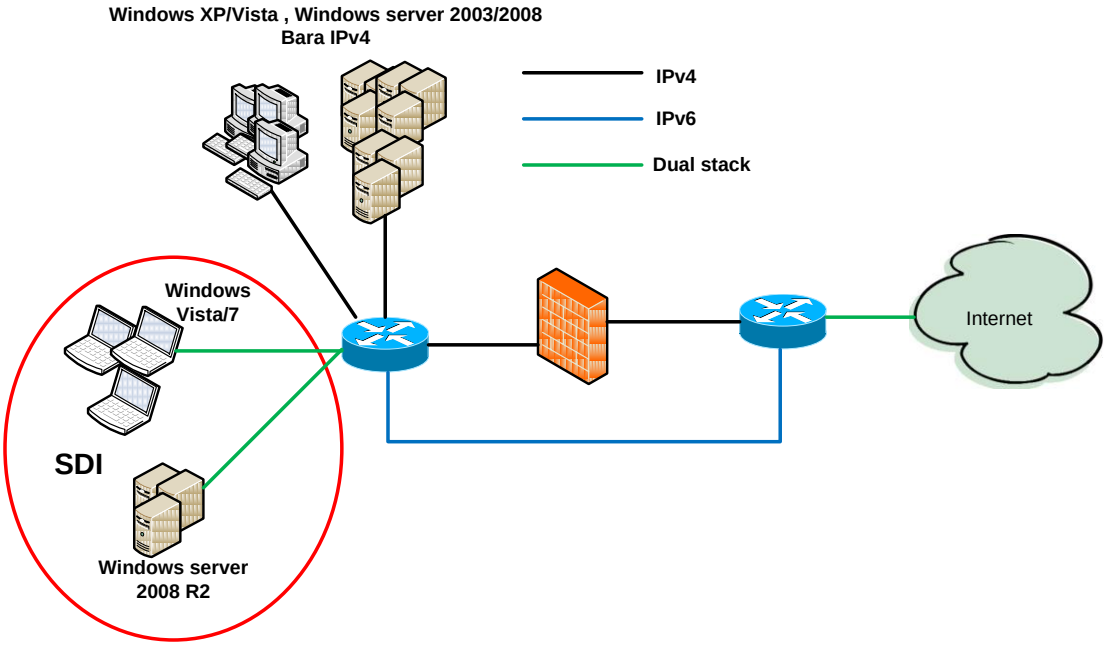

## Att tänka på om säkerhetskopiering

När ni aktiverar IPv6, tänk på att kontrollera så att säkerhetskopiering (backup) fungerar över IPv6 och att prestandan är likvärdig med den för IPv4. Vid problem kan det enkelt kontrolleras genom att aktivera/inaktivera IPv6 på backup-servern. Problem kan uppstå med en mindre brandvägg då dessa inte alltid har funktion för säkerhetskopiering.

## Produktspecifikt råd om brandväggslösning

En möjlig brandväggs- och säkerhetslösning för Windows 7 och server 2008 R2 är Microsofts Server and Domain Isolation (SDI). Dessa operativsystem har bl.a. integrerad brandvägg för IPv4 och IPv6. Med SDI-lösningen kan datorer skydda sin IPv6-kommunikation både internt och mot internet. Med SDI hanteras brandväggsreglerna centralt genom Group Policy, GPO. SDI kan även påverka den interna IPv4-trafiken.

I bilden nedan routas IPv6-trafiken in till den interna L3-switchen. Alla datorer som har SDI implementerat skyddas genom den inbyggda brandväggen. Det går att göra med denna lösning eftersom endast Windows7 och Windows server 2008 R2 har IPv6 aktiverat.




Mer information om Microsofts Server Domain Isolation finns på http://technet.microsoft.com/en-us/network/bb545651

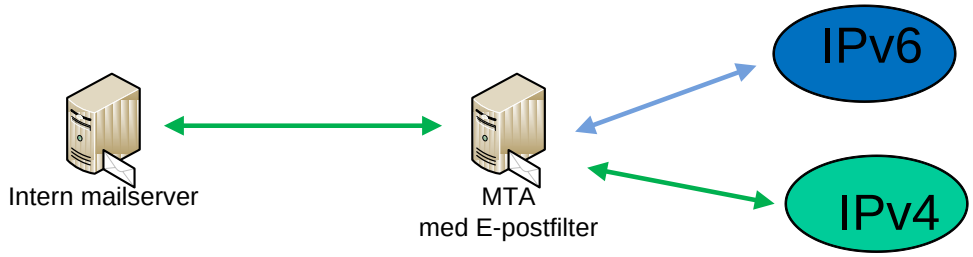
Microsofts kommundesign[20], MSKD, bygger på SDI. Mer information om den senaste versionen av MSKD finns på http://download.microsoft.com/download/4/C/B/4CB67316-B327-4043-A6EE-398C5E63AF78/MSKDv4%200.pdf

## Säkerhetsaspekter för e-post

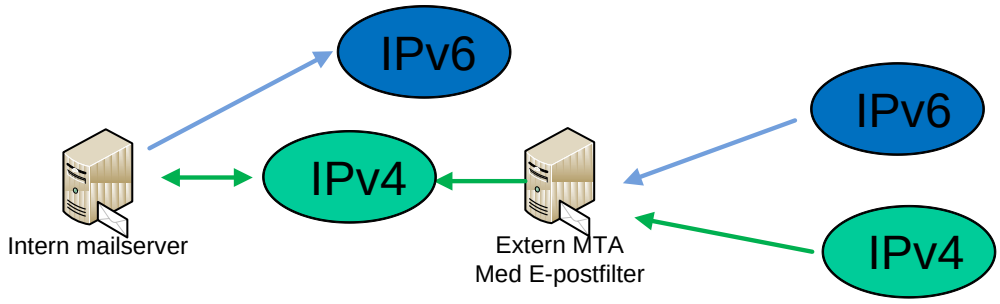
E-postfiltrering, dvs. filtrering av oönskad e-post (spam) och virus i e-postkommunikation, är en viktig säkerhetsfunktion. Flera organisationer i offentlig sektor har lagt ut ansvaret för denna tjänst i molnet. Där finns det idag väldigt få leverantörer som har stöd för IPv6.

Bilden nedan visar en vanlig uppsättning med en MTA (Mail Transfer Agent), dit myndighetens/kommunens MX RR pekar. Den har stöd för dual stack i OS och på MTA och kan då skicka och ta emot e-post med både IPv4 och IPv6. MTA:s placering beror ofta på tillverkare. En del står på ett DMZ, medan andra placeras parallellt med den befintliga brandväggen.

[20] En referensdesign som beskriver en Microsoft-infrastruktur optimerad för en svensk kommun



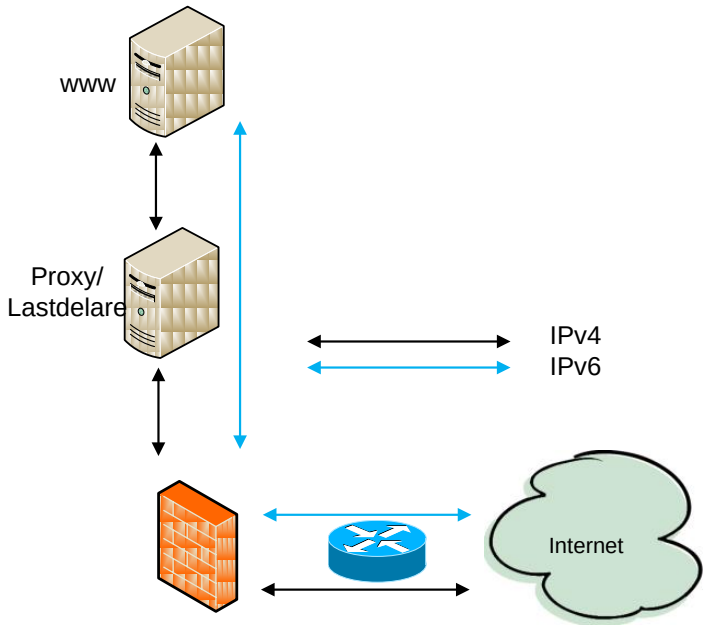

Om man däremot, som i bilden nedan, filtrerar e-post hos en extern part måste den stödja både IPv4 och IPv6 för inkommande trafik, medan transporten till det interna e-postsystemet kan ske över IPv4. Eftersom väldigt få externa e-postfiltrerare erbjuder MTA för utgående e-post, måste organisationen i det här fallet aktivera IPv6 för utgående e-post i det interna e-postsystemet. Det är oftast inget problem då alla moderna e-postsystem har stöd för IPv6.




## Produktspecifikt råd om IPv6-mognad i proxy för aktiviering av IPv6 för webben

Några av de vanligast förekommande proxy/lastdelare som används idag är Microsoft ISA, Microsoft Forefront TMG och Websense. ISA kommer aldrig att få stöd för IPv6, medan TMG kommer att få det. Microsoft kan dock inte i skrivande stund, augusti 2011, säga när det kommer att ske. Websense ska också komma med stöd, men de kan inte heller ange någon tidpunkt. Det går att komma runt detta genom att låta IPv6-trafiken passera till webbservern utan att gå genom proxyn. Detta gäller såklart alla proxy/lastdelare som inte

har stöd för IPv6. Se bild nedan.




Denna lösning är betrakta som temporär tills proxy/lastdelare har bytts ut eller att stöd för IPv6 har kommit. Tänk också på att vid eventuell SSL/HTTPS-trafik, behövs certifikatet i både proxyservern och webbservern.

## Säkerhetsråd för accesswitchar

En accesswitch ger klienter tillgång till ett visst nätverk, t.ex. till interna tjänster. De flesta nya L3-switchar har stöd för IPv6 eller med hjälp av ett licenstillägg. Äldre accesswitchar hindrar ibland IPv6 att fungera som det ska. Denna behöver hantera Ethertyp (ethertypen 0x86DD) och multicast-grupperna för att IPv6 ska fungera.

Filtrering av multicast (sk. IGMP-snooping) har i en del fall stört hanteringen av IPv6-multicast. Därför har den varit tvungen att inaktiveras.

Ur ett säkerhetsperspektiv bör man blockera s.k. falska IPv6-routrar och DHCPv6-servrar. Detta har oftast inte gjorts hos de flesta organisationer för IPv4-trafiken (t.ex. DHCP-snooping och Dynamic Arp Inspection). När IPv6 ska införas kan det vara en god idé att se över detta för både IPv6 och IPv4.

För mer information om säkerhetskrav på i accesswitchar, se RIPE:s rekommendationer (ripe-501)[21] .

### Säkerhetskrav för trådlösa nät

Kraven på trådlösa nät är i princip desamma som för accesswitchar. De måste hantera ethertypen 0x86DD och multicast-grupper för att IPv6 ska fungera.

### Råd för fortsatt hög tillgänglighet i VPN

I inventeringsarbetet bör man kontrollera vad som händer med VPN-tjänster för roaming clients[22], som de flesta organisationer har för distansarbete, om IPv6 aktiveras.

Om en dator har IPv6 aktiverat och ska nå interna resurser, kan problem uppstå om den interna resursen har stöd för både IPv6 och IPv4, och VPN-anslutningen inte har stöd för IPv6. Det kan t.ex. vara en intern resurs med både A och AAAA RR, och datorn som ansluter, försöker först nå AAAA RR och sedan ”timar det ut” och den väljer A istället.

### Råd om DHCPv6-server

Adresstilldelning för IPv6 kan ske på flera sätt. En rekommendation är att använda DHCPv6 utan temporära DHCPv6-adresser för dynamisk tilldelning. SLAAC[23] och temporära DHCPv6-adresser gör att det blir svårare att strukturera adresserna på samma sätt som med IPv4.

Microsofts inbyggda DHCPv6 finns från och med server 2008, ISC DHCPD (http://www.isc.org) från version 4 och många IPAM-system stödjer detta.

### Övergripande råd för fortsatt hög tillgänglighet

Ställ aldrig ett lägre SLA-krav på en tjänst eller funktion som har dual stack aktiverat jämfört med IPv4. När dual stack är aktiverat på en tjänst kommer datorer och servrar som har IPv6 aktiverat att välja IPv6 först. Är tjänsten då nere över IPv6 så kan det uppstå långa fördröjningar.

### Råd för fortsatt hög tillgänglighet och säkerhet vid aktivering av IPv6 på arbetsdatorer

När native IPv6 ska aktiveras i arbetsdatorer krävs att befintliga mjukvarubaserade brandväggar och andra viktiga funktioner för att administrera arbetsdatorer också har stöd för IPv6. Med andra viktiga

[21] http://www.ripe.net/ripe/docs/ripe-501#layer2ent
[22]
[23]

funktioner avses t.ex. fjärrstyrning av och uppdateringsfunktioner för arbetsdatorer, m.m. I de flesta fall går detta bra.

Men hårt styrda brandväggar och fjärrstyrningsprodukter som inte har stöd för IPv6 har orsakat problem. Problemet beror ofta på att datorerna registrerar sitt datornamn med ett AAAA RR. Stödjer t.ex. inte fjärrstyrningsprodukten IPv6, fungerar det inte att ansluta sig till dem.

Ett annat vanligt fel är för hårt styrda mjukvarubaserade brandväggar som hindrar IPv6 multicast att skicka och ta emot på ett korrekt sätt. Se bilden nedan som visar resultatet av kommandot **netstat –an** på en Windows server. Bilden visar att http, SMB[24], RPC[25] och RDP[26] lyssnar alla fyra på både IPv4 och IPv6.

```
Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0        LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0        LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0        LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0        LISTENING
  TCP    [::]:80                [::]:0           LISTENING
  TCP    [::]:135               [::]:0           LISTENING
  TCP    [::]:445               [::]:0           LISTENING
  TCP    [::]:3389
```

[24] Server Message Block
[25] Remote Procedure Call
[26] Remote Desktop Protocol

# Bilaga 4 – Råd för att sätta upp en adressplan

Att adressera sitt nät med IPv6 är egentligen inte svårare än med IPv4. Skillnaden ligger i att IPv6-adresserna är 128 bitar mot IPv4-adressernas 32 bitar. I större nät kan det därför vara en god idé att se över sin adresshantering och inte minst de verktyg man har för detta. Windows interna DNS, DHCP-server tillsammans med Excelkalkyler kanske inte räcker till när IPv6 aktiveras. Om man har hundratals nät med många servrar och skrivare så bör man titta på en komplett IPAM-lösning för att underlätta adresshanteringen.

## Organisera tilldelade IPv6-adresser

En rekommendation från IETF är att kunder som tilldelasIPv6-adresser ska få en sådan mängd att det räcker för en "rimlig framtid". Det innebär att många ISP tilldelar varje kund (företag som privat) en /48. Det finns dock de som tilldelar ner till ett enstaka /64 – och allt där emellan.

När en organisation tilldelats en /48 (/52, /56 eller /60) kan det vara svårt att veta hur man ska hantera alla prefix man får och hur de ska fördelas.

Om man får en /48 eller /52 får man 2^16 (65 536) eller 2^12 (4 096) nät/prefix att fördela. En sådan fördelning kan man göra på lite olika sätt. Nedan ges en beskrivning över några användbara metoder när du har en /48 att fördela.

**Exempel**

Låt säga att du har fått 2001:db8:55::/48 . Du får då 2001:db8:55:0000::/64 till 2001:db8:55:ffff::/64 att fördela i ditt nät.

När vi som i detta fall har tilldelats en /48, ser strukturen ut så här:

| Tilldelad /48 från Internetleverantör | Tillgängliga prefix/nät | Hostdel |
|---|---|---|
| 2001:db8:55::/48 | 2001:db8:55:0::/64 – 2001:db8:55:ffff::/64 | 0000:0000:0000:0000 – ffff:ffff:ffff:ffff |

Med en sådan stor mängd nät gör det att vi kan adressera nätet på en mängd olika sätt, men undvik att krångla till det. Försök att hålla en så enkel adressplan som möjligt. Nedan visas två strategier på hur detta kan se ut.

## Metod 1: Matcha IPv4 med IPv6

Låt säga att idag har ni näten 10.123.0.0/16 fördelat på 10.123.0.0/24 till 10.123.255.0/24. Vi kan då för att göra en liknande fördelning med IPv6 göra så här:

10.123.0.0/24 => 2001:db8:55:0::/64
10.123.1.0/24 => 2001:db8:55:1::/64
.
10.123.254.0/24 => 2001:db8:55:254::/64 alternativt 2001:db8:55:fe::/64
10.123.255.0/24 => 2001:db8:55:255::/64 alternativt 2001:db8:55:ff::/64

Om vi använder 55:255:: eller 55:ff:: är en smaksak, 255 hexadecimalt är visuellt lika som decimala 255 medan hexadecimalt ff är 255 decimalt.

## Metod 2: Matcha VLAN ID med v6

En del tycker det är bra att veta vilka VLAN IPv6-prefixen sitter i. Det kan vi göra på ungefär samma sätt som v4-matchningen ovan.

VLAN ID 154 => 2001:db8:55:154::/64 eller 2001:db8:55:9a::/64

Fördelen med den hexadecimala numreringen ovan är att du får ett till fält att nyttja och kan då matcha mer än bara VLAN ID. Ett fält som kan matcha och markera ytterligare någon funktion.

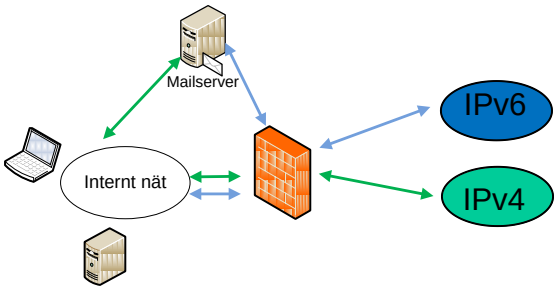
**Exempel**
VLAN ID 154 på Administrativa nätet för en kommun =>
2001:db8:55:**A**9a::/64
VLAN ID 2675 på elevnätet för en kommun => 2001:db8:55:**E**a73::/64
(En v6-adress kan skrivas med VERSALER och jag använder **A** och **E** för att förtydliga exemplet ovan)

## Nätarkitektur

Om man har en befintlig bra struktur på nätet är det bara att göra en kopia på det och aktivera IPv6 enligt samma struktur på vlan och segment. Krångla inte till det, utan gör IPv6 så lika IPv4 som möjligt så blir lösningen enklare för er. Är man däremot inte riktigt nöjd med sin nuvarande struktur och vill bygga om, finns det inget som hindrar att man aktiverar bara IPv4 på ett interface

och bara IPv6 på ett annat. Idag, när de flesta virtualiserar sin miljö, så är det enkelt att göra detta utan någon tillkommande hög kostnad.

Se bild för exempel på två interface.




## Numrering av länknät mellan routrar

En fördel med IPv6 är att det är samma storlek på nät/prefix överallt. Det är inget krångel som med IPv4 där vi snålat i många år och många olika subnätsmaskar används. Men såklart finns det ett undantag och det är IPv6 och länknät mellan routrar. Där finns det en del fördelar med att inte använda standard /64. En av anledningarna är att man slipper SLAAC, RA och andra NDP-baserade protokoll som du inte vill ha på länknät mellan routrar. Men ni kan fortfarande ta en /64, men bara använda /127 för enkelhetens och tydlighetens skull.

## Exempel på adressplan

Som exempel tar vi ett nät som kan vara ett landsting, en större kommun eller en myndighet. I nätet finns stationära datorer på alla platser, bärbara datorer som kör trådlöst på en del platser, servrar på en plats och IP-telefoni på alla platser. Stationära och bärbara datorer med trådlös anslutning, IP-telefoni och servrar är alla uppdelade i olika VLAN. Beroende på antalet anslutna enheter är även ibland stationära och IP-telefoni uppdelade i flera VLAN/plats. VLAN-id är unika inom organisationen och inget VLAN-id finns på fler platser. För att förenkla har vi tagit bort skrivare och annan liknande utrustning.

Se nedanstående bild för exempel. På A och B är antalet stationära och IP-telefoner så många så de är uppdelade i olika VLAN. Det finns en L3-switch centralt på platserna och nätet distribueras ut via L2 accessswitchar. Plats C består av ett fåtal enheter och allting är anslutet till en L3-switch. Internet tas in via en central brandvägg på plats C där publika e-tjänster står placerade på ett DMZ.

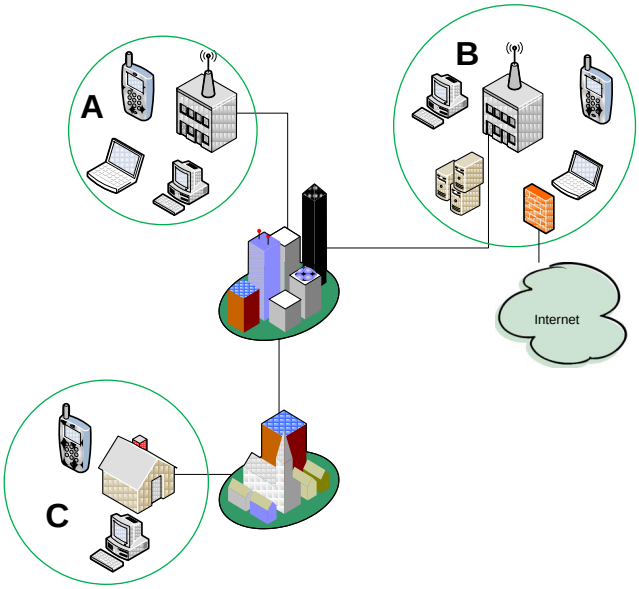



Bild på hur A och B är logiskt uppbyggda med skillnaden att DMZ och Internet bara finns på plats B.

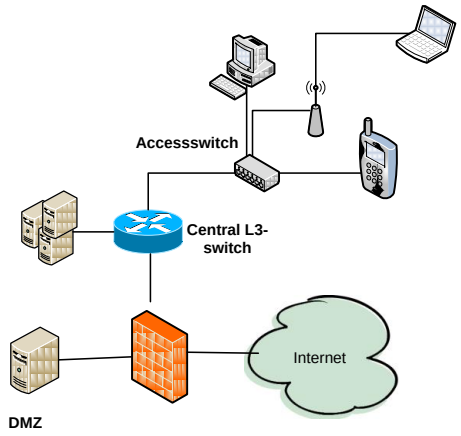
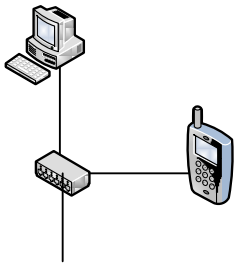



Bild på plats C, bestående av bara stationära och IP-telefoner.



Vi väljer nu att numrera IPv6-nätet efter funktion och VLAN-id. Även om IP-telefoner och de flesta interna servrar inte kommer att ha IPv6-aktiverat från start så tar vi med dem i planen redan nu.

## Att numrera näten per VLAN

Från vår internetleverantör har vi blivit tilldelade 2001:db8:55::/48 och vi väljer att göra så här:

| Prefix | Funktion |
|---|---|
| 2001:db8:55:**1001**-2001:db8:55:**1fff**::/64 | Servrar |
| 2001:db8:55:**2001**-2001:db8:55:**2fff**::/64 | Stationära |
| 2001:db8:55:**3001**-2001:db8:55:**3fff**::/64 | Trådlösa bärbara |

| | |
|---|---|
| 2001:db8:55:**4001**-3001:db8:55:**4fff**::/64 | IP-telefoni |
| Etc | |

För att detta ska fungera måste VLAN-id skriver hexadecimalt så VLAN-id 100 på ett servernät ger IPv6-prefixet 2001:db8:55:1064::/64 för 100 hexadecimalt är 64. Med tre hexadecimala, eller 12 bitar, täcker vi precis in antalet möjliga VLAN-id:n 4096.

OBS! Vill ni göra det mer läsbart och inte behöver möjligheten att använda alla 4096 möjliga VLAN, kan ni istället göra så här.

| **Prefix** | **Funktion** |
|---|---|
| 2001:db8:55:**1001**-<br>2001:db8:55:**1999**::/64 | Servrar |
| Etc | |

Vi använder då något som ser ut som decimal numrering och VLAN-id 1-999 kan utnyttjas. Om vi inte använder någon inledande funktions siffra så får vi även möjligheten att använda alla 4096 VLAN i numreringen.

| **Prefix** | **VLAN** |
|---|---|
| 2001:db8:55:**0001**-<br>2001:db8:55:**4096**::/64 | ---- |

## Att numrera upp varje VLAN och funktion

Nu kan vi numrera upp nätet enkelt och då även bestämma hur adresserna ska tilldelas.

| Plats | Funktion | VLAN id | IPv6 Prefix | Adresstilldelning |
|---|---|---|---|---|
| C | DMZ | 100 | 2001:db8:55:1064::/64 | Statisk |
| C | Servervlan 1 | 237 | 2001:db8:55:10ed::/64 | Statisk |
| C | Servervlan 2 | 238 | 2001:db8:55:10ee:/64 | Statisk |
| C | stationära hus 2 | 567 | 2001:db8:55:2237::/64 | DHCPv6 |
| C | Stationära hus 3 | 568 | 2001:db8:55:2238::/64 | DHCPv6 |
| C | Trådlösa hus 2 och 3 | 569 | 2001:db8:55:3239::/64 | DHCPv6 |
| C | IP-telefoni hus 2 | 570 | 2001:db8:55:523a::/64 | DHCPv6 |
| Etc | | | | |
| D | Stationära | 2000 | 2001:db8:55:27d0::/64 | DHCPv6 |
| D | IP-telefoni | 2001 | 2001:db8:55:47d1::/64 | DHCPv6 |
| etc | | | | |

## Att fördela adresser inom VLAN:en

När den grova adressplanen är genomförd liksom i det förra avsnittet ska vi sedan numrera upp varje /64. I varje VLAN finns det t.ex. en default gateway, var ska de statiska adresserna på servrarna placeras och hur ska DHCPv6 tilldelningen se ut? Default gateway väljer vi att alltid lägga på första adressen .1, så den är inte med i tabellen nedan och vi väljer att ha maximalt 255 hostar i ett VLAN.

| Funktion | Adresstilldelning | Scope |
|---|---|---|
| Servrar | Statiska | 2001:db8:55:**1**???::**1001**-<br>2001:db8:55:**1**???::**10ff** |
| Stationära | DHCPv6 | 2001:db8:55:**2**???::**1001**-<br>2001:db8:55:**2**???::**10ff** |
| Trådlösa bärbara | DHCPv6 | 2001:db8:55:**3**???::**1001**-<br>2001:db8:55:**3**???::**10ff** |
| IP-telefoner | DHCPv6 | 2001:db8:55:**4**???::**1001**-<br>2001:db8:55:**4**???::**10ff** |

Den säkerhetstänkande ser här nackdelar med DHCPv6 och ganska statisk tilldelning eftersom det blir mycket enklare att scanna av näten och söka efter sårbarheter etc. Vi anser dock att fördelarna överväger nackdelarna i detta fall.

På de platser där fasta adresser används, kan man med fördel sätta samma slutadress på båda IPv4 och IPv6. Ex. en server som har 192.168.234.**77** får IPv6-adresen 2001:db8:55:1034::**77**.

## Viktigt att tänka på vid skapande av adressplan

Exemplet är gjort för en större organisation med förmodligen några hundra VLAN och anslutningar. Är ni en mindre organisation så fungerar det lika bra att faktiskt numrera de få VLAN:en precis hur som helst. Hur ni ska tänka beror mycket på hur er infrastruktur ser ut. Är ni ett företag/organisation med centraliserad routing i ett fåtal L3-switchar fungerar idén med att numrera näten med funktion och VLAN's ID bra medan har ni mycket decentraliserad routing är funktion och plats bättre

# Bilaga 5 – Råd för att aktivera IPv6

I denna bilaga beskrivs hur IPv6 kan införas i webbserver, e-postserver, DNS, i brandvägg osv.

## Aktivera IPv6 i webbserver

De mest använda webbservrar tillsammans med de mest använda CMS-systemen har idag stöd för IPv6. Det är oftast bara att aktivera IPv6 i serverns operativsystem så får ni automatiskt stöd för IPv6 på webben.

I Microsofts Internet Information Server aktiveras IPv6 automatiskt när ni gör det i operativsystemet. Ni kan kontrollera status med kommandot netstat –an och ni ska då se att webbservern lyssnar på IPv6 och port 80.

```
TCP    [::]:80          [::]:0          LISTENING      0
```

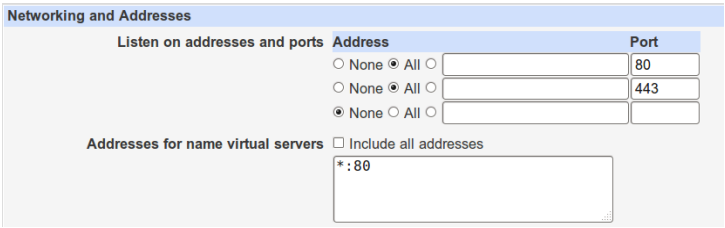
CMS-systemet Sitevision körs ibland via webbservern tomcat och den fungerar bra med IPv6 och i server.xml ska det se ut så här:

```
<connector port="80">
```

Om det är en apache webbserver ska ni ange nedanstående (om det inte redan står så ) i httpd.conf

```
Listen 80
NameVirtualHost *:80
```

Om man har Webmin (http://www.webmin.net) installerat på servern ska det se ut så här.




Webmin är en Open Sourceprogramvara för att enklare administrera Linux, Solaris och t.om Windows.

Och med netstat –an ska ni också här se att det är korrekt uppsatt.

```
tcp6       0      0 :::80                   :::*                    LISTEN
```

## Aktivera IPv6 på e-postservern

Microsoft Exhange och Windows server 2003/2008 har stöd för IPv6. För mer information, läs.SE:s guide för införande av IPv6 i ett medelstortföretag (http://www.iis.se/docs/IPv6-guide_MedBilaga1.pdf ). I den beskrivs erfarenheter med Windows 2003 och Exhange då en del kombinationer inte fungerar med IPv6.

Om ni har en postfixxerver är oftast inte IPv6 aktiverat i den utan i main.conf lägger ni till/ändrar nedanstående rad till:
inet_protocols = all

I sendmail är det nästan aldrig aktiverat utan i sendmail.mc aktiveras det med
DAEMON_OPTIONS(`Name=MTA-v6, Family=inet6')
Observera att i en del versioner av sendmail måste man ange exakt vilka IP-adresser som sendmail ska lyssna då, det kan då krävas att man sätter upp det så här:

DAEMON_OPTIONS(`Port=smtp,Addr=192.168.1.25, Name=MTA')
DAEMON_OPTIONS(`Port=smtp,Addr=::1, Name=MTA-v6, Family=inet6')
DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA2')
DAEMON_OPTIONS(`port=smtp,Addr=2001:db8:10::25, Name=MTA2-v6, Family=inet6')

Och precis som i exemplet ovan med webbservrarna kan ni kontrollera så att mailservern tar emot mail med IPv6 med netstat –an

```
tcp6       0      0 :::25                   :::*                    LISTEN
```

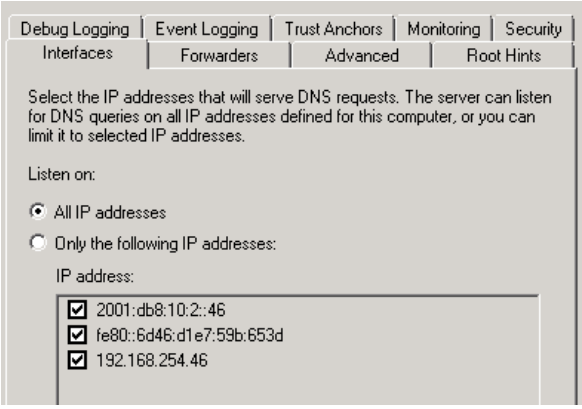
Det finns en mängd olika hårdvaror/programvaror för att filtrera bort spam och skanna virus och ni får kontrollera med tillverkarna vad status på IPv6 och hur man aktiverar det i dem.

## Aktivera IPv6 i DNS-server

Alla vanliga DNS-servrar har stöd för IPv6 idag och det är enkelt att aktivera det. Nedan ges några exempel på hur man gör det i Windows, BIND och Unbound.

## Aktivera IPv6 i Windows 2008 DNS

I Windows Server 2008 och senare versioner är stödet för IPv6 aktiverat så aktiverar ni IPv6 på servern kommer den att svara på och ställa frågor över IPv6.




## Aktivera IPv6 i BIND

BIND har inte IPv6 aktiverat, utan aktiverar det i named.conf med nedanstående option.

```
options {
        listen-on-v6 { any; };
};
```

Det finns en mängd inställningar i named.conf som behandlar hur IPv6 och dual stack ska hanteras men det räcker med ovanstående.

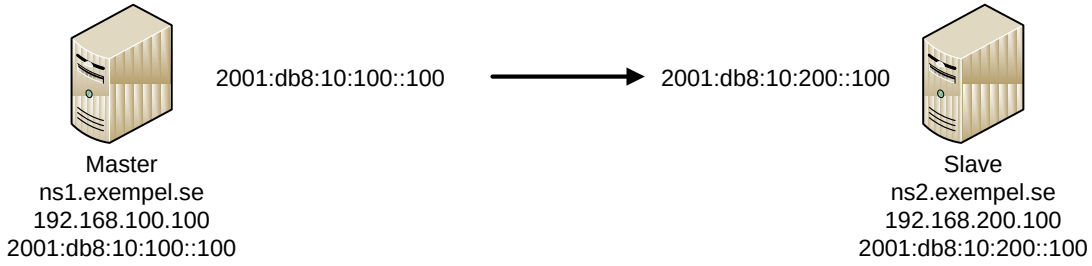
## Aktivera IPv6 i Unbound

I Unbound är det lika enkelt som i BIND och ni ställer in det med unbound.confdo-ip6: yes

## Viktigt att tänka på när man aktiverar IPv6 i DNS

När ni aktiverar IPv6 på auktoritära DNS:er kommer mastern att föredra IPv6 före IPv4. När en domän är förändrad skickar master-DNS:en en notify till slaven/slavarna om att en förändring har skett. Slaven kommer då inte att godta notify:en eftersom den har masterns IPv4 som master.

I bilden nedan kommer mastern att skicka notify till ns2.exempel.se från sin IPv6 adress. ns2.exempel.se kommer inte att godta det. Den kommer att vänta på SOA refresh RR innan den frågar ns1 om någon förändring har skett. Det kan innebära långa fördröjningar innan en förändring är propagerad.




I exemplet nedan för pts.se kan en förändring ta upp till fyra timmar innan den är genomförd på alla slav-DNS:er.

```
dig +multiline soa pts.se
pts.se.                     3600 IN  SOA
majestix.pts.se. hostmaster.pts.se. (
                                     2011061302 ;
serial
                                     14400      ;
refresh (4 hours)
                                     3600       ;
retry (1 hour)
                                     604800     ;
expire (1 week)
                                     3600       ;
minimum (1 hour)
                                     )
```

En lösning på problemet är att tillåta notify från båda IPv6 och IPv4-adressen. Här ett exempel från BIND och inställningen är global för alla domäner i ns2.

```
named.conf i ns2.exempel.se:
options {
        allow-notify { 192.168.100.100;
2001:db8:10:100::100 };
}
```

## Aktivera IP6.arpa

Precis som med IPv4 behövs bakåtuppslagning. Med IPv6 delegerar de flesta operatörer det default till era DNS:er. Ni bör ha denna funktion igång och framför allt på er MTA:er för in- och utgående e-post då en hel del inte tar emot e-post om inte AAAA och PTR RR överensstämmer.

## Se till att er ip6.arpa är delegerad till era DNS:er

Ett exempel med PTS DNS

PTS blev tilldelade 2001:67c:dc::/48 och deras ip6.arpa blir då c.d.0.0.c.7.6.0.1.0.0.2.ip6.arpa.Vi gör en whois-sökning på http://www.ripe.net på det objektet och då ser vi att c.d.0.0.c.7.6.0.1.0.0.2.ip6.arpa är delegarad till majestix.pts.se. och senilix.pts.se.
En ip6.arpa skapas precis som IPv4:as motsvarande in-addr.arpa.
Man börjar med ip6.arpa och tar sedan hela adressen baklänges, här finns det tyvärr inga genvägar med :: .

Se www.pts.se som har 2001:67c:dc:43::215 som exempel.
Dess ip6.arpa blir då
5.1.2.0.0.0.0.0.0.0.0.0.0.0.0.0.3.4.0.0.c.d.0.0.c.7.6.0.1.0.0.2.ip6.arp
Alla 32 hexadeximala siffror måste vara med i ip6.arpa.

**Query the RIPE Database**

Search for c.d.0.0.c.7.6.0.1.0.0.2.ip6.arpa. Search Reset Form

By pressing the "Search" button you explicitly express your agreement with the RIPE Database Terms and Conditions.

Advanced Search Form

Switch to the RIPE TEST Database

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf


% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.


% Information related to 'c.d.0.0.c.7.6.0.1.0.0.2.ip6.arpa'


domain:         c.d.0.0.c.7.6.0.1.0.0.2.ip6.arpa
descr:          Reverse delegation for Post och Telestyrelsen v6-space
admin-c:        RESI1-RIPE
tech-c:         RESI1-RIPE
zone-c:         RESI1-RIPE
nserver:        majestix.pts.se
nserver:        senilix.pts.se
mnt-by:         RESILANS-MNT
source:         RIPE # Filtered
```

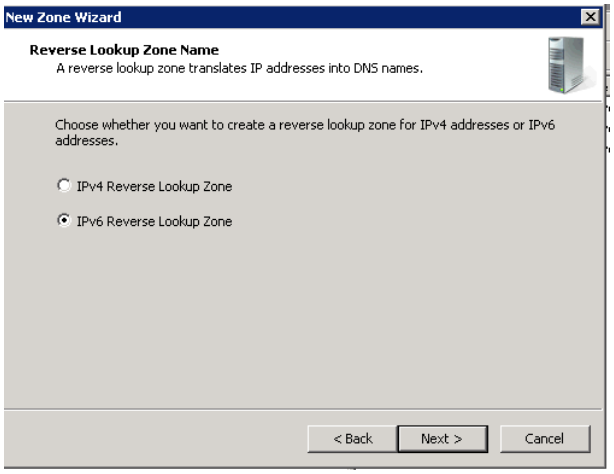
## Sätt upp ip6.arpa i DNS

Det är viktigt att sätta upp ip6.arpa för åtminstone eventuellt auktoritära DNS:er och e-postservrar. Då datorer och andra hostar på insidan av brandväggen har officiella adresser som syns på Internet bör man ta ställning till hur man hanterar ip6-arpa för arbetsstationer. Om en eller flera proxyn används för åtkomst mot Internet räcker det med att lägga upp de servrarna, men finns inte det bör man ta ställning till om man vill exponera sitt interna nät på Internet.
En ip6.arpa kan signeras med DNSSEC precis som vilken annan DNZ-zon som helst.

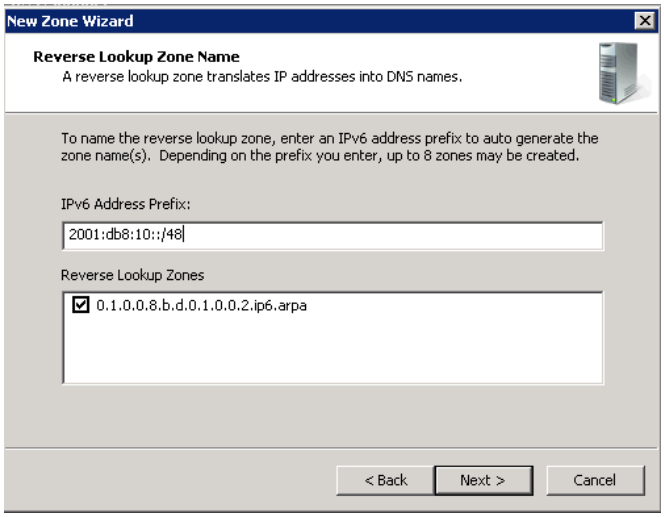
## Aktivera ip6.arpa i Windows

Bilderna är inte kompletta och det är några steg till men det är enkelt att skapa en ip6.arpa i Windows.

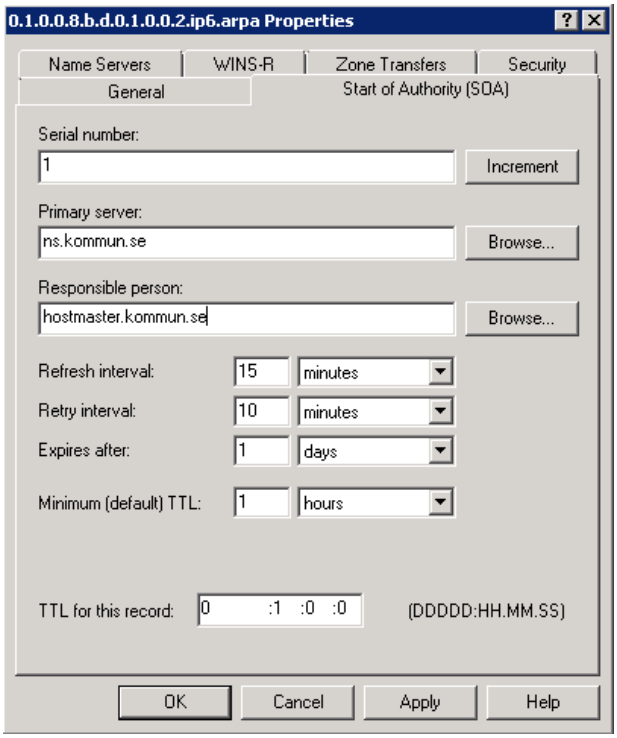
Välj att skapa en IPv6 reverse Lookup Zone.



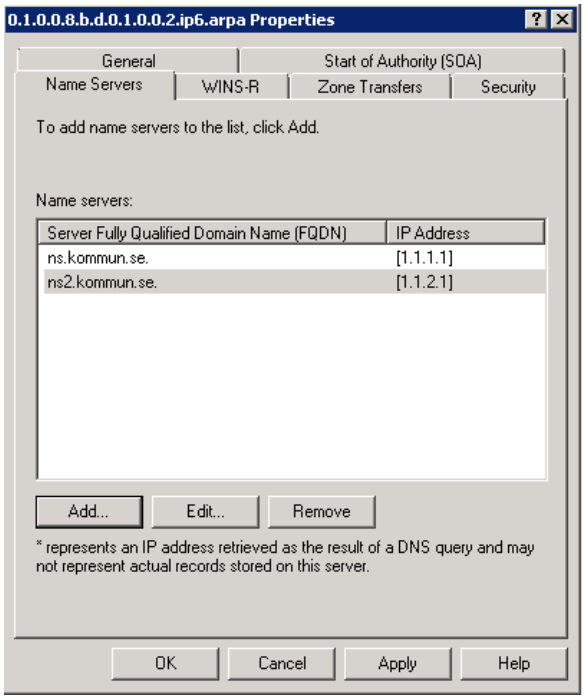

Välj prefix som den ska hantera, en finess är att Windows hjälper dig med att skapa den så du slipper räkna ut den själv vilket kan vara knepigt ibland.



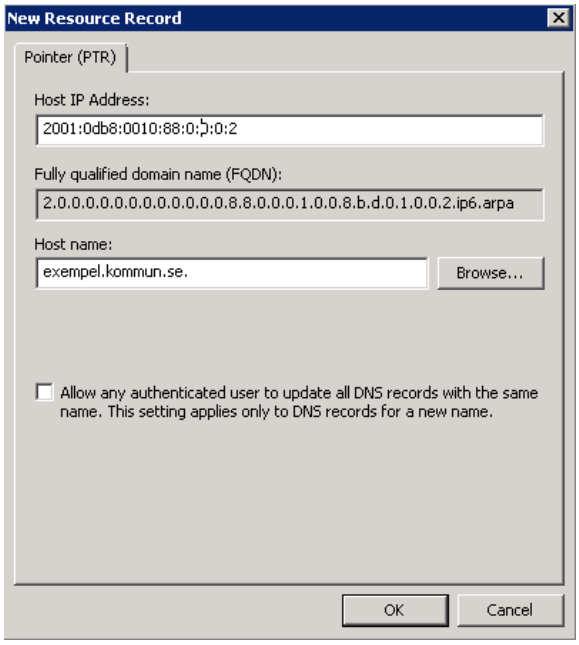

När zonen är klar är det viktigt att din SOA är korrekt, primary name server och responslible email adress ska vara rätt. Om zonen är publik mot Internet är oftast namnet på servern inte det samma som namnet den har som DNS.



Samma sak med NS RR, namnen måste överensstämma. I Windows kan du inte ange en NS utan att ange dess IP-adress vilket kan ställa till det vid omnumreringar av nätet.




Sedan lägger vi upp vårat första PTR RR




Det går tyvärr inte att ange adressen som 2001:db8:10::2 utan :: måste skrivas som 0:0:0

## Aktivera ip6.arpa i BIND

1. Skapa ip6.arpa för 2001:db8:10::/48 med att skapa en ny zone i named.conf som i exemplet nedan

```
zone "0.1.0.0.8.b.d.0.1.0.0.2.ip6.arpa." {
        type master;
        file
"0.1.0.0.8.b.d.0.1.0.0.2.ip6.arpa”;

};
```

2. Skapa sedan filen 0.1.0.0.8.b.d.0.1.0.0.2.ip6.arpa

```
@ IN SOA ns.myndighet.se.
hostmaster.myndighet.se. (
                        2011060202
                        1800
                        7200
                        2678400
```

```
                                3600 )
                                NS
ns1.myndighet.se.
                                NS
ns2.myndighet.se.
```

Och för att skapa ett ett PTR RR för 2001:db8:10:10::2 lägger vi till

```
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0 IN PTR
smtp.myndighet.se.
```

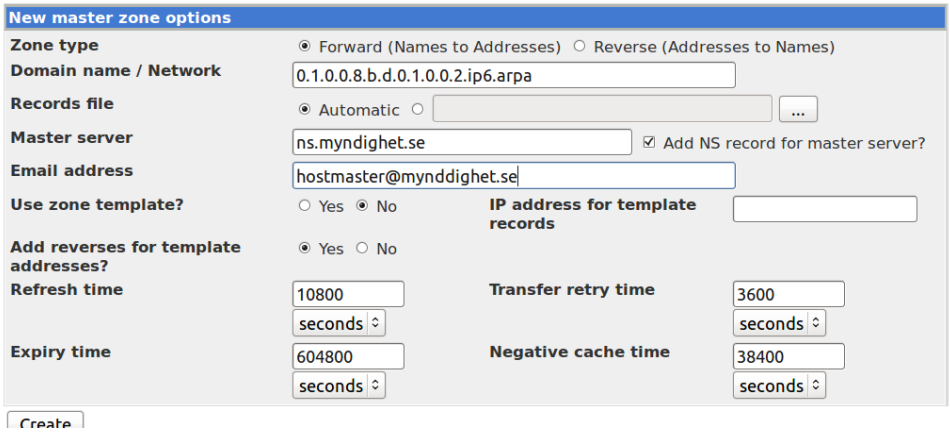
`i filen` 0.1.0.0.8.b.d.0.1.0.0.2.ip6.arpa.

Man kan med $ORIGIN flytta sig i in6.arpan för att underlätta namnsättningen.

```
$ORIGIN
0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.1.0.0.8.b.d.0.1.0.0.2.ip6.a
rpa.
2.0.0.0 IN PTR smtp.myndighet.se.
```

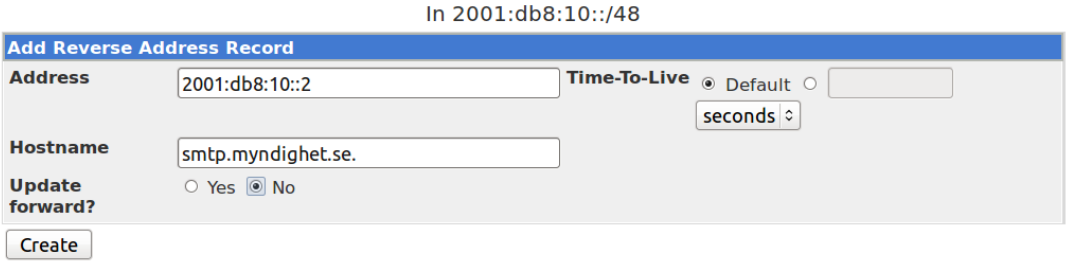
Om ni som i exemplen tidigare vill använda Webmin istället för att editera textfiler gör ni så här

Skapa en ip6.arpa för er /48, observera att Webmin vill att man anger zonen som en Forward ”Name to Addresses” och inte som en Reverse.




Här ser vi att Webmin skapat en 2001:db8:10::/48 av 0.1.0.0.8.b.d.0.1.0.0.2.ip6.arpa


```
För att lägga till ett ip6.arpa PTR anger vi sedan IPv6-
adressen och hostnamnet, komihåg avslutande punkt i
hostnamnet.
```




## Viktigt att tänka på om ip6.arpa

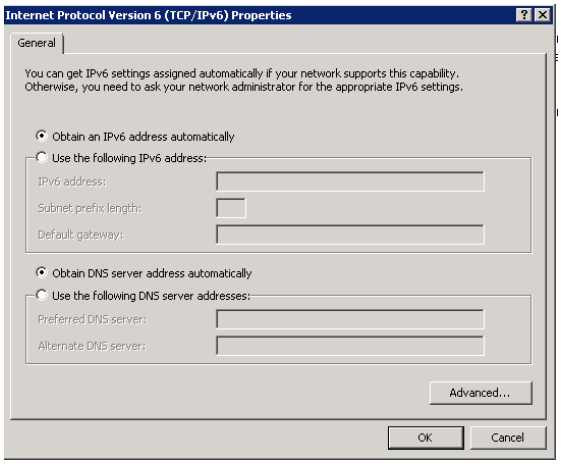
Använd **aldrig** wildcard, *, då det kommer att ställa till problem med loggfiler och det är bättre med NXDOMAIN än ett icke motsvarande AAAA och PTR RR.

Vi rekommenderar inte att ni publikt använder den dynamiska ip6.arpa som Active Directory skapar.

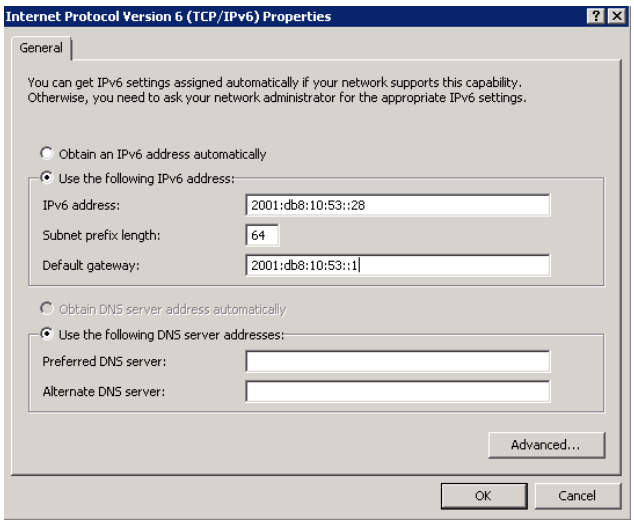
## Adresstilldelning till datorer/servrar

I IPv6 var det från början tänkt att SLAAC skulle sköta adresstilldelningen, men det finns brister i den och idag kan SLAAC ordna så att datorer kan generera egna adresser och få en DNS tilldelad. Tyvärr räcker inte det, utan många gånger vill man tilldela andra DHCPv6-options som t.ex sip-server eller ntp-server och då måste DHCPv6 användas. Nackdelen med DHCPv6 är att Mac OS X (Innan MAC OS X Lion, 10.7) inte stödjer det och i Linux har någon gjort en tankevurpa och därför måste man ofta aktivera DHCPv6 manuellt.

Se exempel nedan på inställningar i Windows. Observera att du inte behöver ange någon DNS när du anger en statisk IPv6-adress, frågor om AAAA RR kan då lika gärna gå över IPv4.
Automatisk – Routern talar om för datorn om den ska köra eller inte köra SLAAC och/eller DHCPv6




Statisk – Läs nedan om datorn sitter i ett nät där andra har dynamisk tilldelning




Det finns ett ganska stort problem med Windows. Det är att även om man aktiverar statiska IPv6-adresser kommer datorn fortfarande att generera SLAAC och köra DHVPv6 om routers RA säger det.

Om en Windowsdator ska ha en fast adress i ett nät där andra ska använda SLAAC och/eller DHCPv6 så måste man disabla så att den inte lyssnar på RA med
netsh interface ipv6 set interface "Local Area Connection" routerdiscovery=disable

Hur den inställningen aktiveras beror på operativsystem och kanske även på service pack nivå. Ibland räcker det med att man skriver kommandot och avaktiverar och aktiverar IPv6 på nätverkskortet och ibland kräver det en omstart. Vi har tyvärr inte kunna hitta någon röd tråd för hur det egentligen är.

Om vi har Linux på servern kan vi ställa in en fast adress antingen via en textfil eller via Webmin (http://www.webmin.net). Webmin har stöd för att konfigurera IPv6 på nätverksinterface sedan version 1.540

Vill ni konfigurera det via textfil och ni har en distribution baserad på Debian är det i /etc/network/interfaces ni gör det.så här

```
iface eth0 inet6 static
        address 2001:db8:10:3::18
        netmask 64
        gateway 2001:db8:10:3::1
```

En annan vanlig distribution som många andra använder som grund är RedHat och där ställer vi in det så här
/etc/sysconfig/network

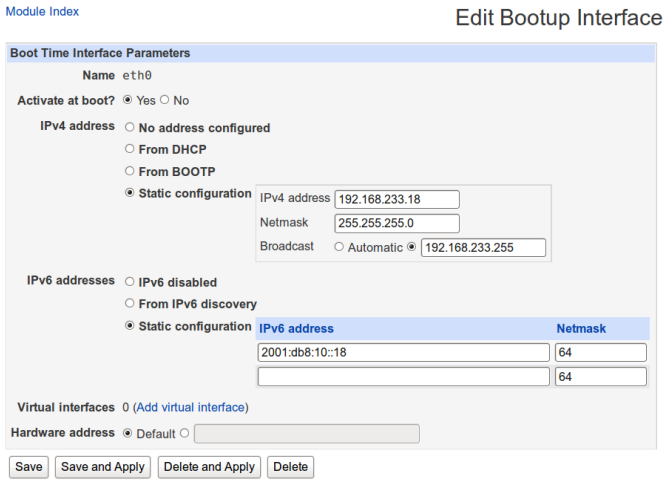
```
NETWORKING_IPV6=yes
IPV6_DEFAULTGW=2001:db8:10:3::1
```

/etc/sysconfig/network-scripts/ifcfg-eth0

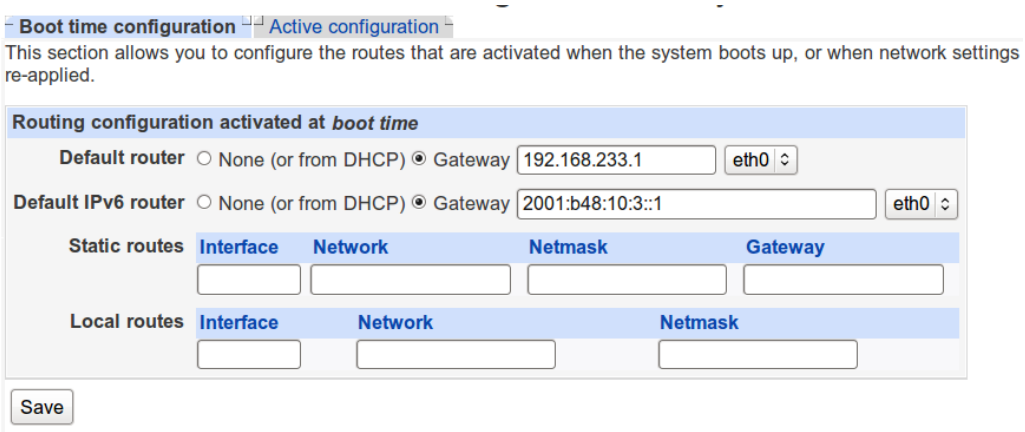
```
IPV6INIT=yes
IPV6ADDR="2001:db8:10:3::18/64"
```

Hur man gör det i andra distributioner som inte är baserade på Debian och RedHat kan variera men med Webmin ser det ut så här för att aktivera IPv6 på eth0.

Sätta upp IPv4 och IPv6 adress på eth0




Sätta upp default gateway för IPv4 och IPv6



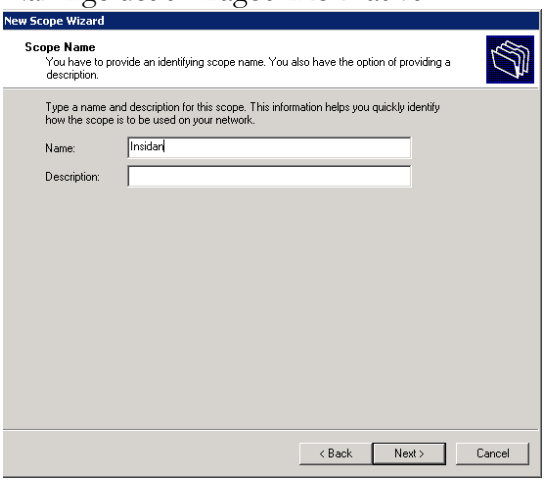

## Aktivera DHCPv6

Två exempel beskrivs nedan över hur vi aktiverar DHCPv6 i Windows 2008 och med ISC:s DHCPv6 server. http://www.isc.org

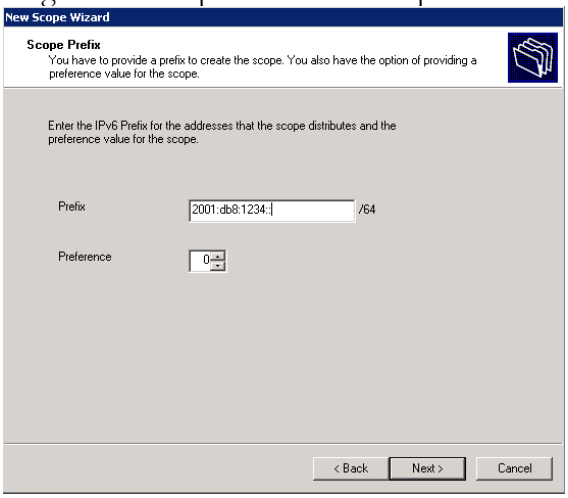
## Aktivera windows 2008 DHCPv6 server

Windows Server 2008 och nyare versioner har DHCPv6-server inbyggt i operativsystemet. Den installeras som en ”roll” och oftast är den redan installerad och aktiverad för IPv4.

1. Skapa nytt DHCPv6 scope.
   Namnge det till något informativt

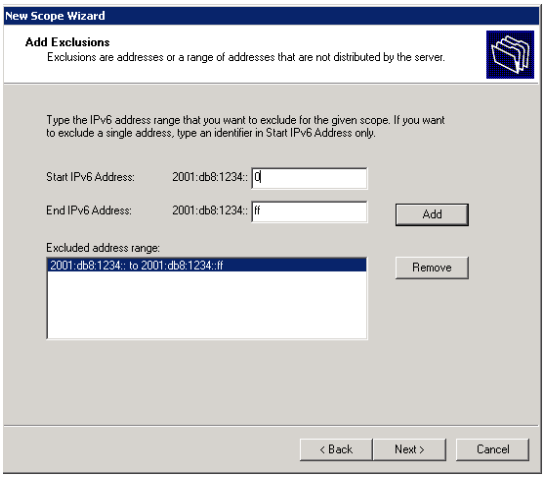



2. Ange vilket prefix
   Ange för vilket prefix DHCP-scopet ska vara

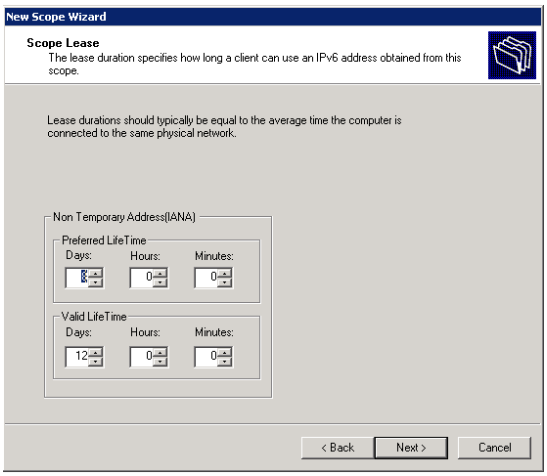



3. Ange address range
   Intervall som det ska delas ut adresser från, här 256 stycken, från 0 till

ff.

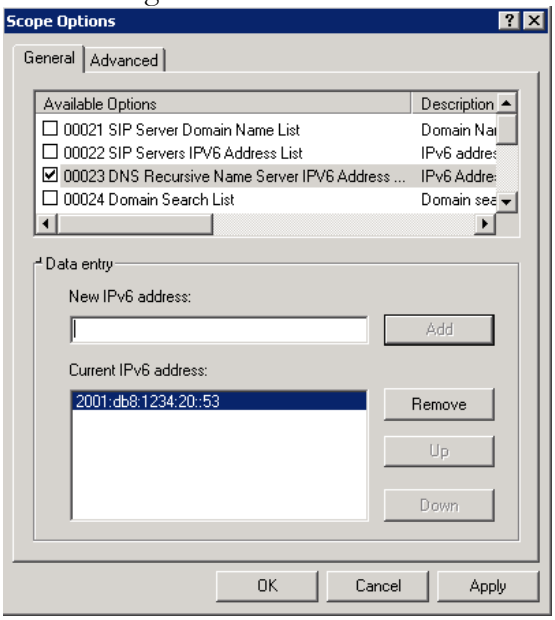



4. Ange lifetime
   Lifetime, ange kortare Preferred och Valid Lifetime så länge tester pågår.

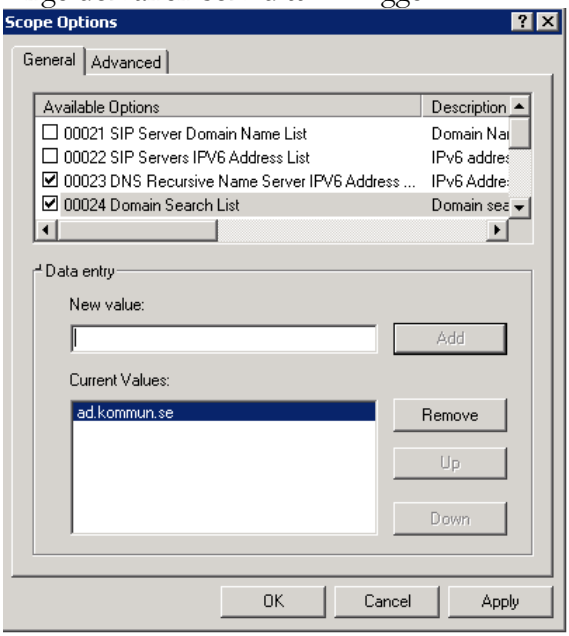



5. Ange DNS
   Aktivera DNS-uppslag över IPv6, det görs en kontroll om DNS-

servern fungerar från DHCP-servern när den läggs upp.




6. Ange search domain
   Ange domänen som ditt AD ligger i.




## Aktivera DHCPv6 i ISC:s DHCP-server

ISC:s DHCP-server måste vara från version 4 och uppåt för att stödja DHCPv6. Den ingår som färdigt paket i en del nyare Linuxdistributioner men måste kompileras in manuellt i en del äldre distributioner.
Vid användning av ISC's DHCP-server för både IPv4 och IPv6 i samma server måste man starta två processer, en för IPv4 och en för IPv6. Uppstartsscriptet och Webminmodulen för ISC DHCPv6 är anpassade för IPv4 så det måste göras manuellt med egna uppstartscript och separat konfigureringsfil.
Se t.ex. www.iis.se/docs/Jörgen-Eriksson-Torbjörn-Eklöv.pdf för mer information om ISC och DHCPv6.

1. Konfigureringsfil, t.ex /etc/dhcpv6.conf
```
max-lease-time 7200;
default-lease-time 3600;
authoritative;
option dhcp6.name-servers 2001:db8:10:2::46;
option dhcp6.domain-search "ad.myndigheten.se";

subnet6 2001:db8:10:22::/64 {
        range6          2001:db8:10:22::                2001:b48:10:2::ffff;
}
```

2. Uppstartskommando
```
/usr/sbin/dhcpd -6 -cf /etc/dhcpv6c.conf
```

3. Det går här också att ange temporära DHCPv6-adresser med ISC:s DHCPv6-server. Det är inget vi rekommenderar men direktivet i dhcpv6.conf ser ni nedan.
```
range6 2001:db8:10:22::/64 temporary;
```

## Aktivera IPv6 i det interna nätverket

Nu har vi fått IPv6 levererat och brandvägg och routing fungerar som det ska så nu börjar vi aktivera IPv6 på punkt för punkt som behövs. Som vi sagt tidigare så är det viktigt att internetanslutningen och brandvägg fungerar innan ni börjar med det interna nätverket. Har ni externa funktioner som DNS, MTA och webbsidor bör de prioriteras före det interna nätet.

Vad vi sedan fortsätter med beror mycket på hur nätet ser ut innanför brandväggen. Men vi antar här att det finns en L3-switch, datorer som ska köra DHCPv6 och någon server som ska ha en fast IPv6-adress.

## Anslutningsswitch - L2-switch

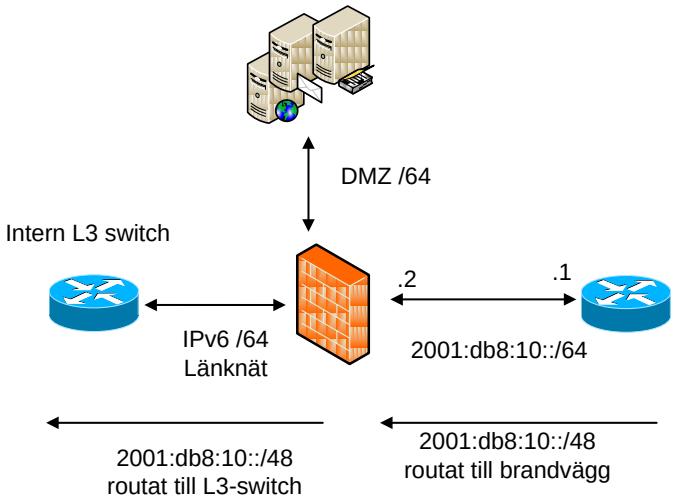
Ni ska sträva efter att ha L2-switchar som stödjer RIPE 501 men gör de inte det så räcker det med att enabla MLDv2 snooping. I en Cisco-switch aktiverar vi det med:

```
ipv6 mld snooping
```

När ni upphandlar nya switchar ska RIPE 501 vara med som krav för att säkra upp nätet.
(Det är bra att samtidigt aktivera DHCP snooping och Dynamic Arp Inspection för IPv4 då.)

## Central switch - L3-switch

När IPv6 är uppsatt som på bilden nedan är det dags att numrera vlan/segmenten i L3-switchen.



Att aktivera IPv6 i en L3-switch är oftast ganska lika som med IPv4.
Se kommandona
`ip address 192.168.10.1 255.255.255.0`
eller
`ipv6 address 2001:db8:10::1/64`
som exempel.

Här ett kortfattat exempel från en Cisco-switch. Vi adresserar hostarna och tilldelar de DNS och search suffix med DHCPv6 genom Managed och Other-flaggan och med
`ipv6 nd prefix default no-advertise` slår vi av all annonsering för SLAAC.

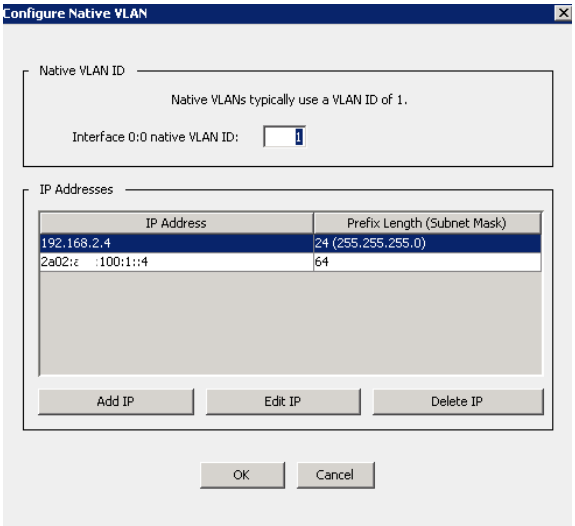
```
!Aktivera IPv6-routing
ipv6 unicast-routing

interface vlan 6
  !sätt en fast adress på vlan 6 – Insida – Ekonomi i
brandväggsexemplet ovan
  ipv6 address 2001:db8:10:6::10/64
  ! O och M flaggan satt => DHCPv6 skall användas för
adressen och   andra optioner
  ipv6 nd managed-config-flag
  ipv6 nd other-config-flag
  ! Ange vilken DHCPv6-server som skall användas
  ipv6 dhcp relay destination 2001:db8:10:50::20
  !Disabla SLAAC på alla prefix på detta interface
  ipv6 nd prefix default no-advertise
```

Exemplet visar ett interface/VLAN som vi aktiverar DHCPv6 på, slår av SLAAC och aktiverar routingen globalt i switchen. Andra tillverkare sätts upp på liknande sätt men med annorlunda syntax.

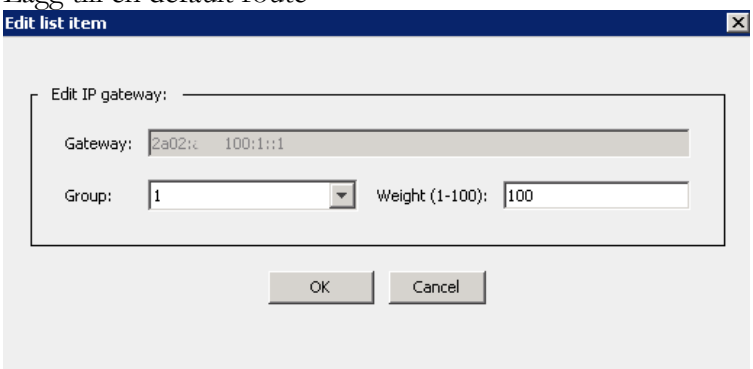
## Aktivera IPv6 i Proxy

Bilderna nedan visar hur enkelt det är att aktivera IPv6 i en Bluecoat proxy.

1. Ställ in en adress

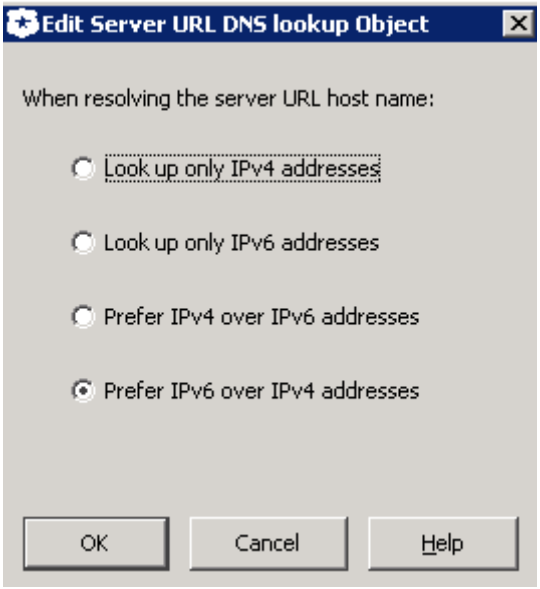



2. Lägg till en default route




3. I Bluecoat kan du enkelt ställa in om du vill föredra IPv6 AAAA eller om IPv4 A ska väljas först. Det är en fördel om ni vill testa för att

snabbt kunna backa vid problem.



# Bilaga 6 – Konsekvenser på ekonomi

I denna bilaga förs ett resonemang kring kostnads- och tidsuppskattningar för införande av IPv6 i publika e-tjänster.

Kostnaden för införande av IPv6 beror dels på organisationens befintliga interna IT-miljö och dess behov av att anskaffa en stor mängd ny hårdvara och kommersiell mjukvara. Används relativt ny hårdvara kan mjukvara med stöd för IPv6 laddas ner och konfigureras på befintlig utrustning. När organisationen i sin löpande verksamhet ser över/anskaffar och uppgraderar hård- och mjukvara, se till att i upphandling/anskaffning ställa krav om att utrustning och tjänster har stöd för IPv6. Dels beror den på i vilken utsträckning konsultstöd används för genomförandet.

Vidare beror kostanden för införandet av det interna nätverkets komplexitet, antal e-tjänster (verksamheter som finns ”ute på webben”/antalet domännamn), samt krav på säkerhet och tillgänglighet. Om höga krav på tillgänglighet råder, på t.ex. upp- och nertid, dvs. SLA-krav och t.ex. krav på tillgänglighet och jour efter kl. 08.00-17.00 ökar kostnaden. Om uppdateringar och skarpa driftsättningar (brandväggsuppgradering) ska kunna utförs efter kontorstid, innebär det högre kostnader (kr/tim) oavsett om intern personal eller extern konsulter. Brandväggskluster och stöd för IP-adresshantering (IPAM) kostar flera tiotusentals kronor. Dessutom beror kostnaden på hur pass välorganiserat och dokumenterat nät organisationen redan har när införandet av IPv6 ska göras.

Uppskattad tidsåtgång för inventering av den interna IT-miljön respektive de tjänster som ansvaras för av extern part (i molnet) uppgår till två till 24 timmar för egen personal eller externa konsulter.

En ytterligare kostnads gäller utbildning av personal. En kurs inom IPv6 behöver inte ta många dagar om man kan sin IPv4. En till två dagar räcker för att komma igång med IPv6. En kurs som beskriver skillnader mellan IPv4 och IPv6 kan vara särskilt värdefull. När man sedan blivit varm i kläderna kan man komplettera med mer avancerade kurser**.** Uppskattad tid och kostnad för utbildning av intern personal: initialt en till två dagar. Kostnad: från 5 000 kr per dag.

Uppskattad kostnad för anskaffning av ny hård- och mjukvara med stöd för IPv6 samt tid för genomförande X.

# Bilaga 7 – Erfarenheter från PTS

I denna bilaga redovisas erfarenheter samt en övergripande kostnads- och tidsåtgång för införande av IPv6 i PTS externa e-tjänster.

## PTS erfarenheter av införande av IPv6

PTS påbörjade 2009 arbetet med införande av IPv6 vid sidan om IPv4 på sina publika e-tjänster. IPv6-stöd finns idag för PTS externa webbplats och alla e-tjänster under etjanster.pts.se, för e-post och DNS.

Ny hård- och mjukvara med krav på IPv6-stöd upphandlades samlat i samband med flytt till nya lokaler. Myndigheten använde för detta Kammarkollegiets ramavtal.

PTS ville inte göra avkall på tillgänglighet avseende brandväggens klusterfunktion, vilken då endast hade stöd för IPv4 i den befintliga hårdvaran. En separat brandvägg köptes in, genom vilken all IPv6 trafik routades. Att anskaffa brandvägg och e-postfilter, båda med IPv6- stöd och tillräcklig säkerhetsnivå, var svårt. Efter att PTS genom avtal säkerställt samma SLA för IPv4 och IPv6, infördes IPv6-stöd för DNS, e-post och sin externa webbplats. Dessa tjänster driftar myndigheten i egen regi.

PTS befintliga system för att ta emot och filtrera inkommande e-post mot spam och virus hade inte stöd för IPv6. PTS fick ta till en temporär lösning inledningsvis. Den innebar att istället för att byta ut hela systemet infördes ett kompletterande system som hade möjlighet att utföra samma funktion över IPv6. Endast inkommande e-post över IPv6 skickas till det nya systemet. Det nya systemet baserades på linux och öppen källkod.

PTS erfarenheter är att konfiguration av routrar och brandväggar var särskilt tidskrävande. Detsamma gällde konfigurering av BGP-routern (gränsroutern mot internetleverantör) för externa anslutningar då myndigheten är multi-homed. Erfarenhet är att aktivering av IPv6 på webbserver är minst tidsödande.

Cirka 120 konsulttimmar har PTS använt för införandet. Ett råd är att säkerställa att inhyrda expertkonsulter använder konsulttid till det komplicerade arbete med att konfigurera hård- och mjukvara. Vidare har PTS egen IT-personal arbetat med införandet sammantaget ca 250 mantimmar.

| Komponent | Uppskattad kostnad | Uppskattad tidsåtgång* |
|---|---|---|
| **Utbildning för personal på IT-enhet.** | 5000 kr/dag/person | 2 personer x 3 dagar |
| **IPv6-internetanslutning inkl. BGP** | Ingen extra kostnad för IPv6 i befintlig internet-anslutning.<br><br>+ 1000 kr/månad/för BGP över IPv6.<br><br>Konsultkostnad ca 28 000 kr | Konsulttid för konfigurering och aktivering, 2-3 dagar |
| **Brandvägg** | 1. Tillfällig kompletterande IPv6-brandvägg, 10000 kr<br>2. Flytt av IPv6-trafik från tillfällig IPv6-brandvägg till befintlig klustrad miljö | 1. Tid för att lägga upp regelverket, 8 tim<br>2. Konsulttid ca 60 tim |
| **L2- och L3-switchar** | Befintlig miljö, 0 kr<br><br>Konsultkostnad ca 72 000 kr | Konsulttid ca 60 tim |
| **Operativsystem (webbserver, e-post server, etc.)** | Uppgradering Windows OS ca 5000 kr, överflyttning av CMS | Konfigurering och aktivering, 2-3 dagar |
| **DNS:** | Befintlig miljö, 0 kr | Konfigurering 1 dag |
| **E-post med SPAM- och antivirus-skydd** | Öppen källkod, 0 kr. | Installation och konfiguration 4-5 dagar |
| **Konsulttimmar** | | |

*Notera att tidsåtgången även inkluderar lärotid då införande av IPv6 gjorde för första gången av PTS personal.

## Saker vi kunde ha gjort bättre

PTS implementerade IPv6 utan att i förväg ha ett komplett, systematiskt tillvägagångssätt. Det orsakade till viss del onödigt arbete. En erfarenhet är att den nu framtagna beskrivningen hade utgjort ett gott underlag för

myndigheten vid införandet.

### Utbildning

Om personalen är i behov av ökad kompetens inom IPv6 och skillnader mot IPv4 men redan har tillräcklig/grundläggande kunskap om nätverk och IP protokoll, behövs inte en renodlad IPv6 kurs. Ofta tas områden upp väldigt detaljerat t.ex. olika headers och information om dessa på protokollnivå. Detta är onödigt för de flesta som bara vill komma igång med IPv6. En utbildning som täcker in nyheter med IPv6 och dess specifika funktioner och skillnaden mot IPv4, är lämpligare för de flesta tekniker i en offentlig förvaltning.

### Internetleverantör

Om multihoming och BGP skall driftsättas, glöm inte i samband med beställningen av anslutningen att säkerhetsställa att det finns stöd för IPv6 BGP och inte bara en IPv6 transittjänst. I annat fall är man fortfarande beroende av sin IPv4 routing. Dessutom måste ditt routeobjekt för IPv6 vara registrerat hos RIPE via din internet-leverantör.

### Administrationsverktyg

Undersök om dina befintliga administrationsverktyg verkligen stödjer samma funktioner som den gör för IPv4. I vissa fall måste man ge avkall på viktiga funktioner som t.ex. clustring och redundans, vilket kanske endast fungerar för IPv4. Alternativet är att byta till nya verktyg med bättre stöd.

### Val av operativsystem

Även om det finns stöd för IPv6 i Windows Server 2008 och det ser ut att fungera, fungerar det inte lika bra som i Windows Server 2008R2. Använder du Microsoft som serveroperativsystem, lönar det sig att uppgradera till 2008R2. Detta gör att oförklarliga fel och icke planerade störningar undviks, vilket annars kan leda till långa felsökningstider.

### Stäng av IPv6 för de servrar som inte berörs

Beroende på operativsystem, räcker det ofta inte att bara avmarkera IPv6 i nätverks inställningar för att avaktivera det. Exempelvis så kan olika tunneltekniker fortfarande generera ofrivilliga IPv6-adresser. Kontrollera noga att nätverksinterfacet inte lyssnar på och presenterar en IPv6-adress. Windows 7 tilldelar automatiskt en IPv6-adress till en 6to4–tunnel standardmässigt så fort en host har en publik IPv4 adress. För att undvika detta, kan man avaktivera 6to4 på en Windows-maskin genom att på kommandoraden skriva:
**”netsh interface 6to4 set state disable”**
Ofrivilliga IPv6 adresser på servrar som registrerar sig själv i DNS:en leder ofta till problem för den tjänst som den levererar.

# Bilaga 8 – Redovisning av IPv6-arbete nationellt och internationellt

Denna bilaga lyfter fram ett axplock av aktiviteter och initiativ som genomförs/genomförts både inom och utanför Sverige.

## Nationellt arbete

I Sverige finns ett antal organisationer och företag som engagerar sig i IPv6. Nedan beskrivs några exempel på organisationer och webbplatser där man kan hitta mer information på området.

### .SE

.SE (Stiftelsen för Internetinfrastruktur) som primärt har ansvar för driften av den nationella svenska toppdomänen ,.se, har även till uppdrag att främja och utveckla Internet i Sverige. Stiftelsen har tagit fram flera guider om IPv6, t.ex. om IPv6-mognaden inom privat respektive offentlig sektor i Sverige, CPE-utrustning med stöd för IPv6, en guide för införande av IPv6 i ett medelstort företag. I den ges exempel på hur IPv6 aktiveras på olika ställen i nätet.

.SE har även anordnat seminarier och utbildningar gällande IPv6. På .SE:s webbplats gällande IPv6 (http://www.iis.se/internet-for-alla/ipv6 ) finns mer information. Några av seminarierna finns att se på http://www.youtube.com/user/internetfoundation.

.SE har ett styrelsebeslut om att införa IPv6 för sina publika e-tjänster sedan ett par år.

### E-delegationen

E-delegationen har tillsammans med Sveriges Kommuner och Landsting samt Kommunförbundet Stockholms Län tagit fram en vägledning för införandet av IPv6. Den publicerades under hösten 2010. Vägledningen finns på följande länk
http://www.edelegationen.se/sida/vagledning-for-inforande-av-ipv6.

E-delegationen har infört IPv6 för sin externa webbplats.

### Skatteverket

Skatteverket har tagit fram en handlingsplan för införande av IPv6 för sina publika e-tjänster. Införandet planeras till början av 2012.

### CERT.SE

CERT.SE har haft stöd för IPv6 sedan flera år. Internetförbindelser, system

m.m. har stöd för IPv6.

**Kammarkollegiet**
Kammarkollegiet har inte infört IPv6 för sina publika e-tjänster.

**Kommuner och myndigheter som har stöd för IPv6**
På de svenska webbplatserna http://www.kommunermedipv6.se och http://www.myndighetermedipv6.se finns bl.a. sammanställningar om aktörer inom offentlig sektor som har aktiverat IPv6 för sin publika webbplats.

## Internationellt

**ARIN**
Den nordamerikanska RIR:en, ARIN, har flera webbsidor om IPv6. Två bra utgångssiter är http://teamarin.net/spread-the-word/ och http://www.getipv6.info. Dessutom har ARIN satt upp en IPv6-wiki.

**ISOC**
Internet Society, ISOC, http://www.isoc.org, anordnade den 8:e juni 2011 World IPv6 Day. Under World IPv6 Day aktiverade flera större organisationer och företag IPv6 under ett dygn. Syftet med detta dygn vara att testa IPv6 i en större skala samt att se om det uppstod några problem när IPv6 var aktiverat. Mer info om och lärdomar från World IPv6 Day finns på http://www.worldipv6day.org/ och under punkt 1.3.2 nedan om RIPE NCC:s erfarenheter av dagen.

**IPv6-forum**
IPv6 forum, http://www.ipv6forum.com/, är en organisation som samlar information om IPv6 och om alla de landsspecifika IPv6-forum som finns, t.ex. http://www.ipv6forum.se. IPv6-forum har även en certifieringsdel där man kan bli t.ex. certifierad utbildare, tekniker inom IPv6 eller varför inte internetleverantör. De står även bakom certifieringen av hårdvara som ni hittar på http://www.ipv6ready.org

**Irish IPv6 Task Force**
Irish IPv6 Task Force är en grupp bestående av representanter från offentliga och privata sektorn på Irland. Deras mål är att främja spridningen och medvetenhet om IPv6 under ledning av myndigheterna för kommunikation, energi och naturresurser.
Läs mer på http://www.ipv6.ie/

**RIPE NCC**
RIPE NCC (Réseaux IP Européens Network Coordination Center, http:/www.ripe.net) är ett s.k. RIR (Regional Internet Registry) som bl.a. har ansvara för tilldelning av IPv4- och IPv6-adresser i Europa och Mellanöstern. RIPE NCC har under lång tid tydligt propagerat för IPv6 och har ett antal statistiksidor om hur IPv6 sprider sig runtom i världen.

RIPE ligger även bakom sidan IPv6ActNow, http://www.ipv6actnow.org/, en informationsportal för flera olika typer av organisationer.

Trender på hur många AS-nummer som aktiverat IPv6:
http://v6asns.ripe.net/

På följande webbsida kan man hämta information om hur många procent av de svenska internetoperatörer som aktiverat IPv6:
http://v6asns.ripe.net/v/6?s=_ALL;s=SE;s=_RIR_RIPE_NCC

RIPE:s verykty RIPEness ger statistik på hur långt internetoperatörer kommit med att aktivera IPv6. Det går att jämföra mellan länder men även se enskilda operatörers status.
http://ripeness.ripe.net/
http://ipv6ripeness.ripe.net/pies.html

RIPE NCC:s sammanställning över resultat utifrån World IPv6 Day.
https://labs.ripe.net/search?review_state:list=published&b_start:int=0&Subject:list=ipv6day

På RIPE:s webbsida över sina möten http://www.ripe.net/ripe/meetings finns presentationer om IPv6 som hållits på deras regelbundet arrangerade medlemsmöten.

**Go6**
Go6, http://go6.si ,är ett institut med ursprung i Slovenien. Dess medlemmar återfinns dock nu runt om i hela världen. Tanken är att samla experter som kan sin IPv6 och som har erfarenheter av IPv6. Dessa skall genom Go6 sprida sin kompetens, utbilda och komma med råd och tips om hur man aktiverar IPv6. Medlemmarna i Go6 håller många föredrag om IPv6 och nedan ser ni en del aktiviteter som genomförts under 2011.

- Den 10:e februari 2011 presentation atv6 World Congress http://www.upperside.fr/v6world2011/v6world2011program_day2.html

- Den 2-6:e maj 2011 RIPE62 Amsterdam:
  Fyra föredrag om IPv6

- Den 24:e maj 2011 Norwegian IPv6 summit
  http://ipv6forum.no/ipv6-konferansen/

- Den 2:a juni 2011 Slovenian IPv6 Summit
  http://go6.si/5-slo-ipv6-summit/

- Den 8:e juni 2011 World IPv6 Day
  http://go6.si/2011/06/world-ipv6-day-monitoring/

- Den 15:e juni 2011 World IPv6 summit
  http://www.ipv6event.com/conference/speakers/

- Den 29:e juni 2011 Macedonian IPv6 summit
  http://www.ipv6.mk/?p=44

**Slovenien**
Regeringen i Slovenien arbetar tillsammans med Go6 på att ta fram en plan för att aktivera IPv6. Planen baseras på en studie som gjorts om IPv6, denna studie finns i skrivande stund endast tillgänglig på slovenska men en engelsk översättning är under framtagande. http://go6.si/docs/Studija-IPv6-MVZT.pdf
Den slovenska regeringen har också planer på att finansiera utbildning, för de som behöver det, för att snabbare komma igång med IPv6.

En av de största Internetoperatörerna i Slovenien, Telekom, har meddelat att de kommer att aktivera native IPv6 för privatpersoner i september 2011.

**USA**
I USA har OMB (Office of Management and Budget) startat en federal IPv6 task force. Denna task force har i flera år arbetat för att alla myndigheter skall aktivera native IPv6 på sina webb, mail, DNS och Internetoperatörer. Målsättningen är att detta skall vara utfört senast vid utgången av år 2012. I slutet av 2014 skall alla datorer i de interna nätverken ha stöd för IPv6. OMB påpekar också vikten av dual stack så att man alltid har både IPv4 och IPv6 aktiverat.
OMB samarbetar med NIST, se nedan, och de skall under hösten 2011 träffa alla myndigheter för att få dem på spåret.

En del av detta går att läsa på
http://www.cio.gov/documents/IPv6MemoFINAL.pdf.

**NIST**
National Institute of Standards and Technology, NIST, som är en del av det amerikanska handelsdepartementet (U.S. Department of Commerce) har publicerat en mängd dokument om vikten av IPv6 och hur man går till väga för aktivera IPv6. Nedan ges två exempel, men det finns fler att hitta under http://www.nist.gov.

- En upphandlingsguide för utrustning som stödjer IPv6 för offentlig sektor:
  http://www.antd.nist.gov/usgv6/.

- SP 800-119, Råd för hur man aktiverar IPv6 säkert:
  http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf.

**Nordamerika**
I Nordamerika har ett flertal lokala IPv6 "Task Forces" uppstått. Dessa är löst sammanbundna med North American Ipv6 task force och det globala IPv6 forumet http://www.ipv6forum.com/. De lokala organisationerna är självständiga och har egna stadgar. Merparten av de lokal organisationerna organiserar träffar och möten för att diskutera IPv6. De lokala organisationerna som har kommit längst är TXv6TF i Texas och RMv6TF i Colorado. Båda dessa är organiserade som non-profit organisations (välgörenhets organisationer) och behöver således ej betala skatt. En intressant detalj är att en Svensk boende i Dallas, Stephan Lagerholm, sitter i styrelsen för TXv6TF. Andra lokala task forces inkluderar CAv6TF (California), Hawaiiv6TF, Midatlanticv6TF (NYC Metro, Pennsylvania, New Jersey, Delaware, Maryland, or DC Metro.), Canada v6TF och Mexico v6TF.

**Surfnet**
Den holländska organisationen Surfnet har tagit fram en kort manual (på engelska) över hur en IPv6-adressplan kan tas fram.

## E-utbildningar
Det finns flera elektroniska utbildningar och certifieringar om IPv6. Här redovisas kortfattat ett axplock av dem. Om ni vill veta mer så Googla på *electronic ipv6 education* så får ni fram en mängd fler alternativ.

**6Deploy.eu**
6deploy har en webbsida med tips, information och utbildningar. Se mer på http://www.6deploy.eu/index.php?page=tutorials och http://www.6deploy.eu/e-learning/english/

**.SE**
.SE har en elektronisk utbildning här http://www.iis.se/internet-for-alla/ipv6/e-utbildning

**RIPE NCC**
RIPE NCC anordnar utbildningar inom bl.a. IPv6 för sina medlemmar (s.k. LIR).

**Utbildningar i Sverige**
.SE har sammanställt en webbsida med information om företag som håller utbildningar i IPv6.
http://www.iis.se/internet-for-alla/ipv6/utbildningar-v6

**Hurricane Electric**
Den amerikanska internetleverantören Hurricane Electric är en av de största pionjärerna inom IPv6 och de har ett populärt certifieringsprogram.
http://ipv6.he.net/certification/

# Bilaga 9 – Exempel på lösningar med öppen källkod

Den här bilagan ger ett axplock av lösningar med öppen källkod som har stöd för IPv6.

Open Source och licensiering är ett avancerat område. Nedan listade program kanske inte räknas som Open Source, men de är kostnadsfria att ladda ner och använda.

Förteckningen över olika programvaror och system är inte fullständig. Den består av vanliga system som är kända att fungera bra. Den innehåller Open Source-produkter så att IPv6 kan aktiveras på/i L3-switch/router, www, DNS, mail, proxy och brandvägg utan att behöva bekosta nya avgifter för licenser och hårdvara. Den senaste versionen av programvaran ska användas.

| Funktion | Program | Kommentar |
|---|---|---|
| Brandvägg | M0n0wall - http://m0n0.ch | Baserad på FreeBSD |
| Brandvägg | Pfenese - http://pfsense.com/ | Do. |
| Brandvägg | Vyatta - http://www.vyatta.org/ | Finns även som licensierad betalversion |
| Brandvägg | LEAF Project - http://leaf.sourceforge.net/ | |
| CMS | Wordpress – http://www.wordpress.org | Stödet för IPv6 beror på stöd/aktivering av IPv6 på underliggande webbserver. |
| CMS | Joomla – http://www.joomla.org | Do. |
| CMS | Drupal – http://drupal.org | Do. |
| CMS | Frog CMS - http://www.madebyfrog.com/ | Do. |

| | | |
|---|---|---|
| DNS | Unbound – http://www.unbound.net | Enbart en cachande resolver |
| DNS | BIND – http://www.isc.org | Både auktoritär och resolverfunktionalitet |
| DNS | PowerDNS | |
| DNSSEC | ZKT - http://www.hznet.de/dns/zkt/ | Wrapper runt BIND för att förenkla hanteringen av signering av zoner med DNSSEC |
| DNSSEC | OpenDNSSEC – http://www.opendnssec.org/ | Avancerat hjälpmedel för hanteringen av signering av zoner med DNSSEC |
| Mailserver | Dovecot - http://www.dovecot.org/ | Stöd för POP3 och IMAP |
| Mailserver | Roundcube - http://roundcube.net/ | Webbmail som kopplas mot t.ex Dovecot's IMAP |
| Mailserver Antispam/Antivirus | MailScanner - http://www.mailscanner.info | Läs mer på hemsidan, behöver kompletteras med fler program |
| Mailserver/MTA | Sendmail - http://www.sendmail.org | Enbart en MTA |
| Mailserver/MTA | Postfix - http://www.postfix.org | Enbart en MTA |
| Proxy | Squid - http://www.squid-cache.org/ | |
| Proxy | Apache - http://projects.apache.org/projects/http_server.html | |

| | | |
|---|---|---|
| Proxy | Nginx - http://nginx.org/ | |
| Proxy | Tinyproxy - https://banu.com/tinyproxy/ | |
| Router | Quagga - http://www.quagga.net/ | |
| Router | Vyatta - http://www.vyatta.org/ | |
| Router | Xorp - http://www.xorp.org/ | |
| Webbserver | Apache - http://projects.apache.org/projects/http_server.html | |
| Webbserver | Nginx - http://nginx.org/ | |

.

# Bilaga 10 – Förklaringar till använda begrepp och förkortningar

| Begrepp | Förklaring |
|---|---|
| 6RD | 6 Rapid Deployment, en kontrollerad IPv6 över IPv4 tunnel som oftast används inom en operatörs nät |
| 6to4 | En automatisk IPv6-över-IPv4 tunnel. Den är aktiverad från start i Windows Vista och Windows 7. |
| A RR | A RR |
| AAAA RR | Quadruple A, AAAA RR |
| Anycast | Anycast är en teknologi som används för att publicera en tjänst, ofta DNS, på flera olika platser men med samma IPv4/IPv6-adresser. Se t.ex http://www.netnod.se/ som anycastar sina DNS-tjänster på 38 platser i världen. |
| Appliance | En godtycklig hårdvaru- eller virtuell maskin, vilken kan finnas i många olika skepnader/för många olika funktioner/tjänster. |
| AS-nummer | Ett AS-nummer är ett nummer som identifierar vilken du är på internet. Alla större internetleverantörer, men även mindre organisationer, som är multihomade via BGP har egna AS-nummer. |
| Auktoritär namnserver | En DNS-server som har ansvaret för en domäns information – en zon. |
| BGP | Border Gateway Protocol |
| CMS | Content Management System är ett hjälpmedel för att enkelt skapa webbsidor utan att behöva någon kunskap om HTML. Vanliga system är t.ex. Wordpress, Drupal, Episerver och Sitevision. |
| DHCP Snooping | DHCP snooping är en funktion för att förhindra att falska DHCP-servrar kan sättas upp. |

| | |
|---|---|
| DHCPv6 | DHCPv6 tilldelar IPv6-adresser på ett kontrollerat sätt på ett segment. Precis som DHCP för IPv4. |
| DNS | Domännamnssystemet (Domain Name System) är en hierarkiskt, distribuerad databas för att sköta namnuppslagning och adressering på internet. DNS består av auktoritativa DNS-servrar och resolvrar. DNS innehåller olika typer av poster/information s.k. Resource Records eller RR.<br><br>A RR (DNS med stöd för IPv4)<br>AAAA RR (DNS med stöd för IPv6)<br>MX PTR |
| DNS64 | Översätter t.ex. IPv4 A RR till IPv6 AAAA RR för att NAT64 ska fungera. |
| DNSSEC | DNS Security Extensions är en utvidgning av DNS-systemet som syftar till att öka säkerheten i DNS. |
| Dual stack | Dual stack kallas det när en nod har stöd för IPv4 och IPv6 samtidigt. |
| Dynamic Arp Inspection | Funktion för att förhindra så kallad ARP-poisoning där attackeraren typiskt blir default gateway och på så sätt kan avlyssna och styra trafiken. |
| Gluerecord | Ett gluerecord är typiskt ett A eller AAAA RR som pekar på en adress på en DNS-server. Det krävs då en namnserver är ansvarig för sin egen zon. |
| GUA | Global Unicast Address<br>IPv6 Unicast address som routas och kan nås över internet. Alla som surfar och alla tjänster som nås över internet måste använda GUA |
| IETF | Internet Engineering Task Force, tar fram s.k. Request For Comments (RFC:er) över nya protokoll/protokollförslag |
| IP6.arpa | IP6.arpa är IPv6 motsvarighet till IPv4'as in-addr.arpa. Alltså vad har den här IPv6-adressen för namn<br>Ex. |

| | |
|---|---|
| | host 2001:67c:dc:43::231<br>1.3.2.0.0.0.0.0.0.0.0.0.0.0.0.0.3.4.0.0.c.d.0.0.c.7.6.0.1.0.0.2.ip6.arpa domain name pointer mailscanix.pts.se. |
| IPv6 Only | En nod som bara har IPv6 aktiverat. Måste används NAT64 för att nå IPv4 only noder. |
| Local Internet Registry (LIR) | Ett lokalt internetregistry, ofta på nationell nivå, som tillhandahåller IP-adresser/nät till slutkunder, ofta en Internetoperatör som t.ex. Telia eller Telenor. |
| MIB | Management Information Base |
| MIM | MIM- Man in the middle attack<br>En attack där men med IPv4 använder arp-protokollet och låtsas vara default gateway och på så sätt kan avlyssna trafik. Med IPv6 låtsas man vara router och/eller DHCPv6-server |
| MTA | Mail Transfer Agent – En server som transporterar e-post, typiskt via smtp-protokollet. Ofta tillhandahåller en internetleverantör en sådan service till sina kunder. |
| Multicast för IPv6 | Multicast – en källa som skickar en dataström till en eller flera registrerade mottagare. IPv6 NDP bygger på Multicast. |
| Multihoming för IPv6 | Multihoming – om man har fler än en operatör, används oftast för att skapa redundans på Internetanslutningen |
| NAT , NAT64 | NAT – Network Address Translation. Lösning för att låta flera IPv4 adresser dela på en publik IPv4 address.<br>NAT64 – Adressöversättning mellan IPv6 och IPv4, måste användas tillsammans med DNS64 för att fungera bra. |
| Native IPv6 | ”Riktig” IPv6 som inte tunnlas inuti IPv4 |
| PA-IPv6-adress | Provider Aggregated- IPv6-adress. Operatörsberoende adresser. Byter man operatör måste man numrera om nätet. |
| PI-IPv6-adress | Provider Indepentent Ipv6-adress. Operatörsoberoende adresser, byter man operatör behöver man inte numrera om nätet. Används också för att multihoma nätet. |

| | |
|---|---|
| Regional Internet Registry | Det finns fem RIR runtom i världen som täcker olika geografiska zoner: RIPE - Europa och Mellanösternregionen, ARIN- Nordamerika, APNIC- Asien och Pacific, LACNIC – Latinamerika, och AFRNIC – Afrika<br>RIR:ens främsta uppgift är att förse LIR med IPv4 och IPv6-adresser och AS-nummer. |
| Registrar | En registrar är ett företag eller organisation som ansvarar för hantering av tjänster runt ett domännamn. Exempel kan vara ny- och avregistrering förändring av domännamn som byte av DNS-servrar aktivering av DNSSEC mm. |
| Resolver | En DNS som används för uppslag av DNS-data, t.ex. vilken IP-adress har www.pts.se? |
| Roaming Clients | Är t.ex. distansarbetare eller externa konsulter som ansluter sig via VPN till kontoret/arbetsplatsen |
| Route-6 objekt | Ett objekt som talar om hur ett IPv6-prefix routas på internet. Visar vilket AS-nummer som det routas via och AS-numret visar sedan hur det routas. |
| Router Advertise-ment (RA) | En IPv6-router talar om för noderna i segmentet hur de ska adressera IPv6-interfacen genom RA. Det kan vara om de ska använda SLAAC, DHCPv6 m.m. |
| SLAAC | StateLess Automatic Address Configuration – Noden använder information från RA för att automatiska sätta upp en eller flera IPv6-adresser på ett nätverksgränssnitt. |
| Teredo | En automatisk IPv6 över IPv4 tunnel. Är aktiverad från start i Windows Vista och Windows 7. |
| Transit | |
| UTM | Unified Threat Management är ofta en funktion i brandväggar eller andra säkerhetsprodukter som analyserar trafiken djupare och sätter stopp för virus, ser till att det är http som körs på port 80 osv. |