Att gå över till IPv6

En guide om att införa IPv6 i ett medelstort företag

Av Jani Juvan, IP Solutions
Bilaga av Torbjörn Eklöv, Interlan

.se

Syfte

Idag ser vi att medvetenheten kring IPv6 ökar, men att det saknas praktiska erfarenheter kring IPv6. Som ett steg i att minska tröskeln till IPv6 ämnar vi med denna guide förenkla en organisations planeringsarbete kring en (oundvikligen) annalkande IPv6-övergång.

Syftet med guiden är att praktiskt beskriva för en IT-chef/nätverkschef och/eller tekniker vad det innebär att gå över till IPv6. Hinder och praktiska erfarenheter tas med. Utifrån denna guide skall mottagaren kunna estimera kostnader och nytta för ett eventuellt IPv6-projekt samt kunna producera en grov projektplan.

Denna guide begränsar sig till att behandla en grunduppsättning av tjänster. Säkerhetsaspekter tas inte upp.

Sammanfattning

En övergång till IPv6 kan delas upp i två faser. Fas 1 är att låta inkommande uppkopplingar nå externt tillgängliga tjänster via IPv6. Detta steg innebär att man inte stänger ute eventuella kunder (eller andra inkommande kopplingar) som endast har IPv6-tillgång till Internet, eller som valt det som preferens.

Fas 2 innebär att ge det interna nätverket IPv6-tillgång både till företagets tjänster och Internet. Dessa två faser behöver inte nödvändigtvis utföras i samband med varandra så länge man har kvar IPv4 parallellt med IPv6.

Stöd för IPv6 i operativsystem är väl utbrett i dagsläget. Aktivering och konfigurering av IPv6 på servrar och klienter är därför en relativt enkel process. Däremot är stöd för IPv6 i brandväggar något nyare och kan kräva uppdatering av mjukvara eller i värsta fall hårdvara för att vara möjligt. Det största hindret ligger dock i dagsläget i tillgång till IPv6 från Internetleverantörer. Det finns ännu få förpaketerade IPv6-lösningar att tillgå, men det går att få IPv6 från många leverantörer via andra kanaler.

Uppskattad arbetstid för att konfigurera ett typiskt företagsnät att tillåta access från omvärlden via IPv6 är 20-24 timmar, varav en stor del är design/planeringstid. Detta innefattar dock endast grundläggande tjänster som brandvägg, dns, webb, e-post och klientaccess. Det finns också många andra tjänster som kan behöva migreras, till exempel databaser, vpn, ekonomisystem och diverse egenutvecklade lösningar. En grundtanke är att denna guide skall i framtiden kunna kompletteras med migrering av andra tjänster.

IT-miljö

IT-miljön i detta dokument skall reflektera miljön i ett medelstort företag, där det finns en IT-avdelning med ansvarig chef. Vidare behandlar vi till en början endast grundläggande tjänster i miljön, för att senare kunna bygga på med fler tjänster. Följande skiss illustrerar hur miljön ser ut:

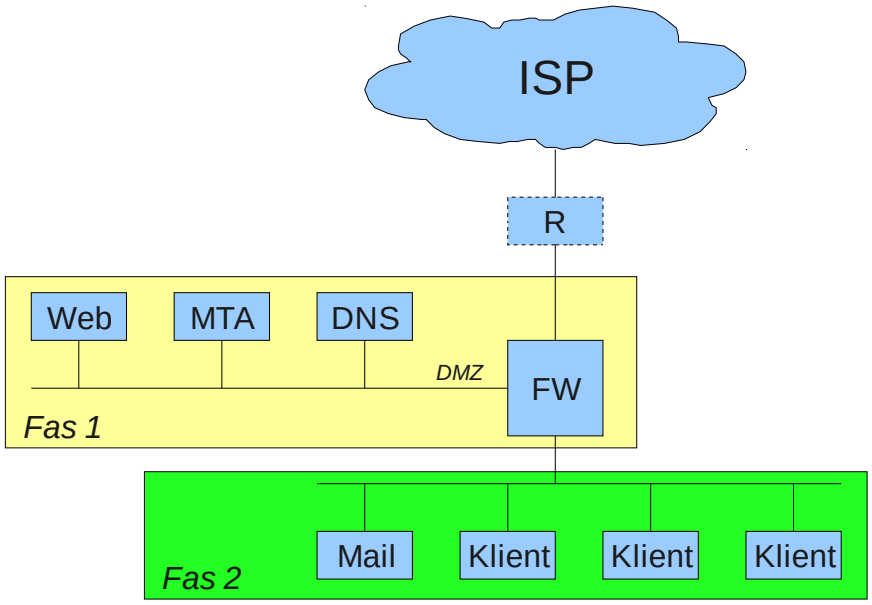


Illustration 1: Miljö som behandlas i denna guide

Projektet delas upp i två faser, där fas 1 täcker brandvägg och DMZ, medan fas 2 täcker interna tjänster och klienter.

Följande mjukvara och hårdvara har valts att representera IT-miljön i ett medelstort företag:

- (ISP = IPOnly – *Finns redan på plats*)
- (R = pf / OpenBSD – *Tillhör ej labbet)*
- FW = Cisco ASA 5505
- DNS = Bind 9.3.4-P1.2 / Debian Etch (Linux 2.6.26) 64bit
- MTA = Postfix 2.7.20090528 / OpenBSD 4.6 64bit
- Webb = Apache 1.3.29 / OpenBSD 4.6 64bit
- E-post = Microsoft Exchange 2007 (sp2) / Microsoft Windows 2003/2008 64bit Server
- Klienter = Windows XP, Windows Vista, Ubuntu Linux, Debian Linux, Mac OS X, OpenBSD

Projektplan

Detta kapitel ger ett exempel på hur ett IPv6-migreringsprojekt kan planeras, med delmoment, personal, kostnader och tidsuppskattning. Detta baseras på det exempelscenario som används i denna guide, och skall motsvara de grundläggande tjänsterna hos ett medelstort företag.

Delmoment

Som nämnts tidigare kan en övergång till IPv6 delas upp i två faser, där fas 1 omfattar externa tjänster och fas 2 omfattar interna tjänster och klienter. Vidare kan fas 1 delas in i ISP-konnektivitet, brandvägg, operativsystem och tjänster. Nedan är förslag till en punktlista med lämpliga delmoment, tillsammans med exempel på mjukvara relevant för denna guide (mjukvaran gås igenom mera detaljerat i senare kapitel):

Delmoment, fas 1:

- Beställ, konfigurera och verifiera IPv6-konnektivitet till ISP
- Brandväggsregler i IPv6 – Cisco ASA
- IPv6 stöd i OS – OpenBSD, Debian, Windows Server 2003/2008
- Konfigurering av IPv6 i tjänster – bind, postfix, apache

Delmoment, fas 2:

- Konfigurering av IPv6 i Exchange
- IPv6 i klientdatorer

Nedanstående figur illustrerar ett möjligt tidsflöde för detta migreringsprojekt.

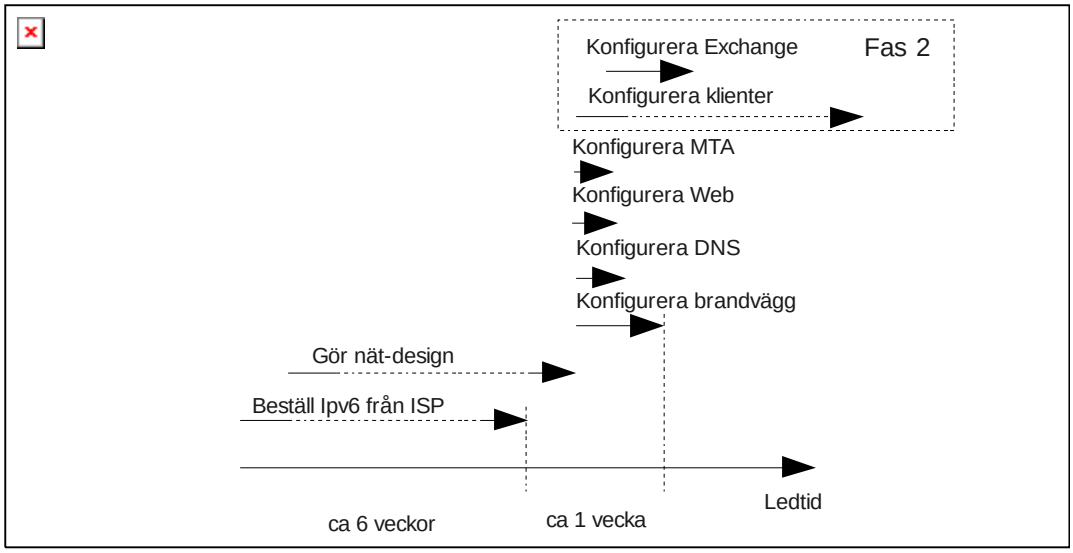


Illustration 2: Exempel på tidsplan

Det finns inget beroende som tvingar en att vänta med fas 2 till fas 1 är avslutad, men rekommendationen är att fokusera på fas 1 i första hand om man inte har ett överflöd av tillgänglig driftpersonal som kan arbeta parallellt.

Projektmedlemmar

Det första som behöver göras är att få en IPv6-förbindelse från sin operatör. Detta utförs lämpligen av ansvarig beställare eller IT-ansvarig.

Liksom i ett IPv4-nät behövs det för IPv6-nät göras en adressplan. Skillnaden är att man har ett betydligt större spann av adresser att använda sig av. Dessutom behöver man bestämma sig för vilken typ av adressering man vill använda; manuell konfigurering eller stateful- eller stateless autokonfigurering (eller en lämplig kombination). Denna uppgift utförs lämpligen av IT-ansvarig eller nätdesigner.

Bland de mera praktiska stegen finns konfigurering av brandväggar, servrar och klienter. Detta utförs lämpligen av brandväggstekniker respektive drifttekniker.

Sammanfattningsvis kan projektmedlemmarna summeras enligt nedan, där flera roller kan innehas av en och samma person.

Lämpliga projektmedlemmar:

- projektägare/beställare
- IT-ansvarig
- nätdesigner
- brandväggstekniker
- drifttekniker – DNS-ansvarig
- drifttekniker – E-postansvarig
- drifttekniker – Webbansvarig
- drifttekniker – klientansvarig

Kunskapskrav

Den personal som skall genomföra projektet bör utöver kunskap inom sitt respektive område ha god kännedom om IPv6. Framförallt gäller detta de praktiska delarna. En brandväggstekniker bör till exempel känna till hur ICMPv6 används och vilka olika adresstyper det finns för att kunna skriva lämpliga brandväggsregler. En drifttekniker bör känna till hur nätverkskonfigurering utförs på respektive operativsystem som skall migreras till IPv6, och känna till manuell och automatisk adresskonfigurering.

Tid

Uppskattad tidåtgång för inblandade personer vid ett IPv6-migreringsprojekt ser ut som följer:

Aktivitet	**Utföres lämpligen av**	**Uppskattad tidsåtgång**
Beställning av IPv6-konnektivitet	IT-ansvarig / firmatecknare	3 h *(+ väntetid)*
Nätdesign	IT-ansvarig / nätdesigner	8 h *(designtid)*
Brandväggsregler	Brandväggstekniker	6 h *(konfigurationstid)*
Konfigurering av servrar	Drifttekniker	7 h *(konfigurationstid)*
Övrig tid *(väntetid, mötestid, uppgraderingar osv)*		15-50 h *(beroende på utgångsläge mm, se nedan)*
Totalt fas 1		**39-74 h**
Konfigurering av klienter	Drifttekniker	1 h per klient

Tabell 1: Tidsuppskattning per delmoment

Notera att tidsuppskattning för de rent praktiska bitarna ligger på cirka 24 timmar, resterande tid är i hög grad beroende på rådande arbetsrutiner, utgångsläge för IT-miljön och väntetider mot Internetleverantör.

Till detta projekt fanns redan IPv6-tillgång via Internetleverantör (tillgång till testnät via kontakter hos leverantören). Tidsuppskattningar för att få IPv6 från leverantörer i allmänhet baseras på information

inhämtad från marknaden.

Efter fas 1 skall man vara fullt åtkomlig utifrån via IPv6 till de vanligaste tjänsterna (webb, e-post och dns).

Många klienter är redan förberedda för IPv6 och kan automatiskt börja använda det om man använder stateless autokonfigurering. Andra klienter behöver enklare ingrepp för att slå på IPv6. Detta kan göras fortlöpande då man med allra största sannolikhet kommer att behöva använda dual-stack under överskådlig framtid.

Notera att eftersom delmomenten är så pass korta tjänar man inte så mycket på att utföra dem parallellt. Den största delen tid går ändå åt till att få IPv6-konnektivitet från ISP. Dock kan man använda väntetiden till att tänka ut en lämplig adresseringsplan som man sedan kompletterar med de adresser man får tillgång till.

Risker

Här följer en sammanställning av de risker man bör ha i åtanke för ett IPv6-migreringsprojekt:

- IPv6-access kan vara tidskrävande att få från Internetleverantör, räkna med långa ledtider.
- Mjukvara kan behöva uppgraderas, vilket kan innebära extra kostnader i tid och pengar.
- Hårdvara kan behöva uppgraderas, vilket kan innebära extra kostnader i tid och pengar.
- Viss hårdvara eller mjukvara kanske inte ens går att uppgradera och behöver bytas ut.
- Personal kan behöva utbildas, vilket skulle innebära extra kostnader i tid och pengar.
- Säkerhetserfarenheter kring IPv6 saknas i stor utsträckning, då det fortfarande är nytt.

Övriga kostnader

Vid en kostnadsberäkning bör man även beakta eventuellt utbildningsbehov för personalen. Dessutom kan man behöva uppgradera mjukvara och i värsta fall hårdvara för att få stöd för IPv6. Denna guide utgår från en viss uppsättning hårdvara/mjukvara som skall representera ett medelstort företag. I det projekt som ligger till grund för den här guiden krävdes endast en uppgradering, från Windows 2003 Server till Windows 2008 Server. All mjukvara har genomgående varit uppdaterad till nya versioner.

Kostnadspost	**Kostnad**	**Tid**
Utbildning	-	-
Uppdatering av hårdvara	-	-
Uppdatering av mjukvara	9500 kr	8 h *(+ leveranstid)*
Summa	9500 kr	8 h

Tabell 2: Exempel på kostnadsberäkning

Övergång till IPv6

Externa tjänster (Fas 1)

Access

Det absolut mest grundläggande kravet för att kunna gå över till IPv6 för publika tjänster är att det finns IPv6-konnektivitet utifrån till företaget. Det första steget i denna migreringsprocess bör därför vara att kontrollera att den aktuella internetleverantören kan erbjuda IPv6. I dagsläget är det långt ifrån alla leverantörer som kan erbjuda detta. I takt med att efterfrågan ökar kommer även tillgången från leverantörerna att bli bättre.

Uppgiften bör utföras av: IT-ansvarig eller ansvarig firmatecknare.

Räkna med långa responstider då många leverantörer i dagsläget ligger långt efter med information om IPv6 till sina handläggare. Med rätt kontakter hos leverantören kan man dock få ett snabbt svar.

Estimerad tid: I hög grad beroende av väntetid och kontakter, ren arbetstid bör dock ligga under 1 timme.

Adressplan

Innan man påbörjar konfigureringsarbetet bör man ha adressplan och tänkta brandväggsregler klara för sig. Vill man använda DHCPv6, Stateless autoconfiguration eller manuell konfigurering?

En föreslagen lösning är att dela ut prefix från brandväggen men sätta manuella interface-addresser på servrar (dels för att underlätta felsökning/konfiguration, dels för att undvika nya adresser vid hårdvarubyten) och låta klienter göra automatisk konfiguration.

Typiskt kommer ett företag att tilldelas ett IPv6-nät med 48 bitars prefix från sin leverantör. Detta ger möjlighet att konfigurera 65536 underliggande subnät med 64 bitars prefix. Detta gör att subnätsindelning blir en relativt enkel process.

Uppgiften bör utföras av: Nätplanerare i samråd med IT-ansvarig.

Estimerad tid: 8 timmar.

Brandvägg

Verifiera att brandväggen har stöd för IPv6. Dagens brandväggar uppdateras fortgående med IPv6-stöd, så det kan behövas en mjukvaruuppdatering eller i värsta fall en uppgradering av hårdvaran.

Konfigurering av brandväggen innefattar:

- Konfigurering av IPv6-adresser på interfacen.
- Prefix (och alternativt andra parametrar) för Router Advertisement.
- Default route för IPv6-trafik.
- Brandväggsregler för IPv6-trafik.

Uppgiften bör utföras av: Brandväggstekniker.

Komplexiteten i uppgiften beror i hög grad på komplexiteten i det befintliga nätverket. Regler motsvarande de för IPv4 behöver dupliceras för IPv6, dessutom behöver man ägna en särskild tanke åt eventuella ICMPv6-meddelanden som kan behövas för IPv6 i nätverket. Dessutom bör man beakta möjligheten till multipla IPv6-addresser och deras respektive scope. Med en gedigen adressplan blir detta steg en enkel implementering av reglerna.

Estimerad tid: 4-8 timmar.

Operativsystem

Kontrollera stöd för IPv6 i de operativsystem som körs på servrar och klienter. De flesta nyare OS har redan stöd för IPv6 och har det aktiverat som standard. Om manuella IPv6-adresser används behöver dessa konfigureras, samt även andra manuella parametrar som till exempel default gateway och adress till namnserver.

Att ta emot Router Advertisements är också en konfigurerbar inställning som behöver kontrolleras (om man vill ta emot prefix och default routes, till exempel). Till exempel har OpenBSD som standard stängt av mottagandet av Router Advertisement.

Microsoft Windows 2003 Server samt Windows XP kräver att man installerar IPv6-protokollet i nätverksinställningarna. I Windows är Router Advertisements påslaget som standard, och eventuella manuella justeringar får man göra via kommandoprompt.

Uppgiften bör utföras av: Drifttekniker.

Estimerad tid: ca 30 min per dator. Ca 2-4 timmar för denna exempelmiljö.

DNS (namnserver)

Förutsatt att operativsystemet är förberett för IPv6 återstår inte mycket för att göra DNS redo för IPv6:

- Eventuella IP-baserade regler i named.conf behöver uppdateras till att även ta hänsyn till IPv6-adresser/nät. (Till exempel views, dynamic updates, loggning.)
- AAAA (quad-A) Records behöver läggas till i master-zonen för att peka ut IPv6-adresserna för respektive maskin.
- Verifiera att delegering av IPv6-adresser görs.

Uppgiften bör utföras av: Drifttekniker/DNS-ansvarig.

Estimerad tid: 2 timmar.

MTA (e-postrelä)

Postfix har inbyggt stöd för IPv6 sedan version 2.2. I nyare versioner är IPv6 påslaget som standard. Följande konfigurationsparametrar i postfix/main.cf har en inverkan på IPv6-kompatibilitet:

- inet_interfaces – anger vilka interface postfix lyssnar på, standard är alla
- inet_protocols – anger vilka protokoll som stöds, standard är ipv4 & ipv6
- smtp_bind_address6 – anger vilken adress e-post skickas från, standard är första bästa

Dessa behöver man kontrollera ifall de har ändrats från standardvärden.

Uppgiften bör utföras av: Drifttekniker.

Estimerad tid: 30 min.

Webb

Förutom att förbereda operativsystemet, behöver man även konfigurera webbservern (i detta fall Apache) att ta emot anslutningar över IPv6. I enklaste fall är detta så enkelt som att lägga till ”Listen [::]” i httpd.conf, i miljöer med flera Virtual Hosts kan man dock behöva lägga till en IPv6-mottagningsaddress per host-adress.

- Konfigurera webbservern till att ta emot anslutningar över IPv6.

Uppgiften bör utföras av: Webbansvarig eller Drifttekniker.

Estimerad tid: 1-2 timmar.

Interna tjänster (Fas 2)

Exchange

Ursprungliga uppsättningen mjukvara för detta test var Exchange 2007 installerad på Windows Server 2003. Men det visade sig att denna kombination inte stödde IPv6. (Se mer information under kapitlet Nyttiga erfarenheter.)

Istället fick Windows Server 2003 bytas ut mot Windows Server 2008, som har stöd för IPv6 aktiverat från start. Enda konfigurering som krävs är att sätta manuell IPv6-adress (om sådan önskas) och adress till namnserver. Inga särskilda inställningar för Exchange krävs för att stödja IPv6.

Klientaccess

Klienter konfigureras i denna guide till att använda stateless autokonfigurering, det vill säga att de får nätdelen av IPv6-addressen från brandväggen i en Router Advertisement och skapar host-delen själva från mac-addressen (modifierad EUI-64). Typiskt behöver alla klienter en IPv6-adress, prefixlängd, default route och adress till namnserver. Via Router Advertisement kan de tre första parametrarna alltid automatkonfigureras men adressen till namnservern kan inte delas ut eller tas emot av all utrustning (i dagsläget). Till exempel skickar brandväggen i denna guide inte ut denna parameter. Alternativen då är att konfigurera den manuellt eller låta namnserveranropen gå över IPv4 tills vidare (om parametern konfigureras via DHCP).

I de fall det finns en konfigurerad IPv6-adress tillgänglig kommer den att användas i första hand vid utskick förutsatt att destinationen är en IPv6-adress. Om det saknas IPv6-transport någonstans längs vägen kommer detta resultera i timeout och utskicket sker via IPv4 istället (förutsatt att mottagaren även har en IPv4-adress).

Vid användandet av IPv6 finns det i många fall motsvarande nätverkskommandon som för IPv4, som till exempel *ping6* och *tracert6*/*traceroute6*, medan andra kommandon har stöd för IPv6 inbyggt (tex *ssh*).

Windows XP

Detta test utfördes på Windows XP med Service Pack 2.

För att få tillgång till IPv6 i Windows XP krävs minst Service Pack 1. Den inkluderar nödvändiga filer för att aktivera IPv6. Protokollet aktiveras sedan genom att lägga till det under nätverksinställningar (se detaljerad guide längre ner), alternativt genom att skriva kommandot *ipv6 install* (eller *netsh interface ipv6*

install) i en kommandoterminal. Detta aktiverar IPv6 med stateless autokonfigurering som standard. Vid behov av manuell konfigurering används kommandot *ipv6* eller *netsh interface ipv6* i en kommandoterminal (mer dokumentation om kommandona finns på Microsofts dokumentationsportal).

En viktig sak att notera är att Windows XP inte har stöd för DNS-anrop över IPv6, då dess resolver inte stöder IPv6. Dual stack krävs för att göra DNS-uppslag. (Quad-A uppslag går bra att göra även över IPv4.)

Ubuntu Linux

Detta test utfördes på Ubuntu 9.10 (*Karmic Koala*).

Ubuntu har stöd för IPv6 aktiverat från start. Den kommer automatiskt att acceptera Router Advertisements och konfigurera IPv6-adress och default route enligt mottagen information. IPv6-adress till DNS kan läggas till manuellt i resolv.conf.

Debian Linux

Detta test utfördes på Debian 5.0 (*Lenny*).

Då Ubuntu bygger på Debian har de exakt samma funktionalitet vad gäller IPv6, det vill säga påslaget som standard med möjlighet att konfigurera DNS manuellt.

OpenBSD

Detta test utfördes på OpenBSD 4.6.

Stöd för IPv6 finns som standard, dock är accepterandet av Router Advertisements avslaget som standard. Med en enkel konfigurationsändring kan Router Advertisements tas emot och IPv6-adresser autokonfigureras. IPv6-adress till DNS kan konfigureras manuellt i resolv.conf.

Mac OS X

Detta test utfördes på Mac OS X 10.6 (*Snow Leopard*) och 10.4 (*Tiger*).

Mac OS X har stöd för IPv6 aktiverat från start. Den kommer automatiskt att acceptera Router Advertisements och konfigurera IPv6-adress och default route enligt mottagen information. IPv6-adress till DNS kan läggas till manuellt i det grafiska gränssnittet.

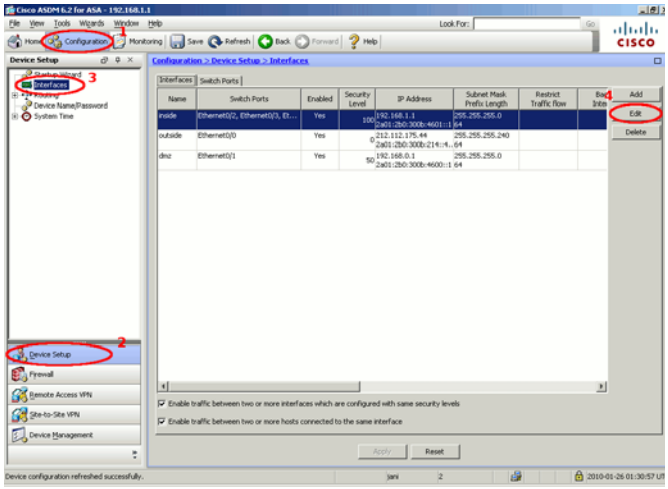
Konfigurationsguider

Denna sektion innehåller steg-för-steg instruktioner för konfigurering av IPv6 enligt punkterna ovan. De IPv6-adresser som är skrivna i dessa konfigureringsguider använder det så kallade dokumentationsprefixet, *2001:db8::/32*. Detta prefix är avsett endast för dokumentationsändamål och skall inte förekomma i riktiga nätverk.

Brandvägg - Cisco ASA 5505

Denna konfiguration är gjord under ASA Version 8.2(1) och ASDM Version 6.2(3).

Följande illustrationer visar hur man aktiverar IPv6 på ASA 5505, sätter IPv6-adresser på interface samt anger inställningar för RA.

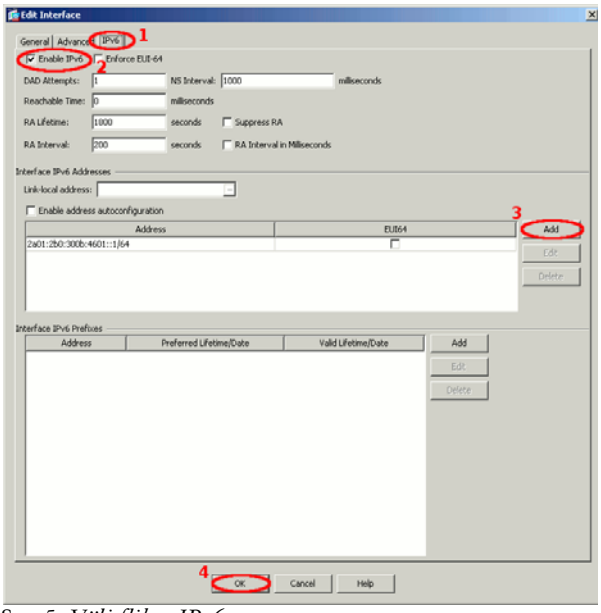


Steg 1: Välj konfigureringsläget

Steg 2: Välj enhetsinställningar

Steg 3: Välj interfaceinställningar

Steg 4: Konfigurera valt interface



Steg 5: Välj fliken IPv6

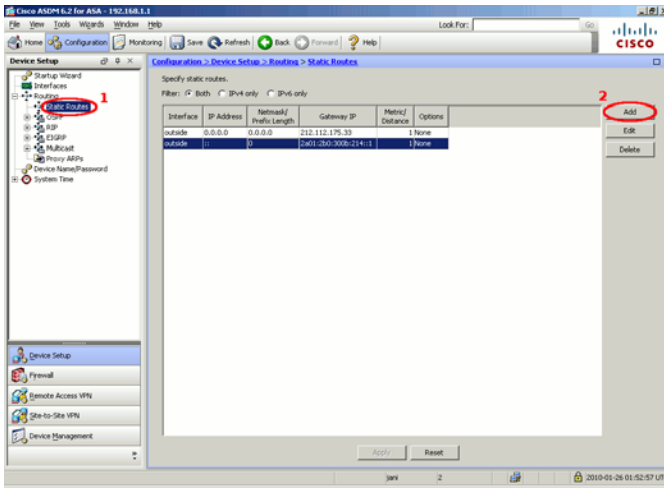
Steg 6: Bocka i användandet av IPv6

Steg 7: Lägg till en IPv6 adress

Steg 8: Slutför med OK

Här ställer vi in en manuell IPv6-adress på insidan av brandväggen. När brandväggen har aktiverat IPv6 kommer den automatiskt att skicka Router Advertisement med aktuellt prefix för interfacet samt sin egen IPv6-adress som default gateway. Detta kan man stänga av genom att bocka i *Suppress RA*, vilket kan vara lämpligt för utsidan av brandväggen till exempel.

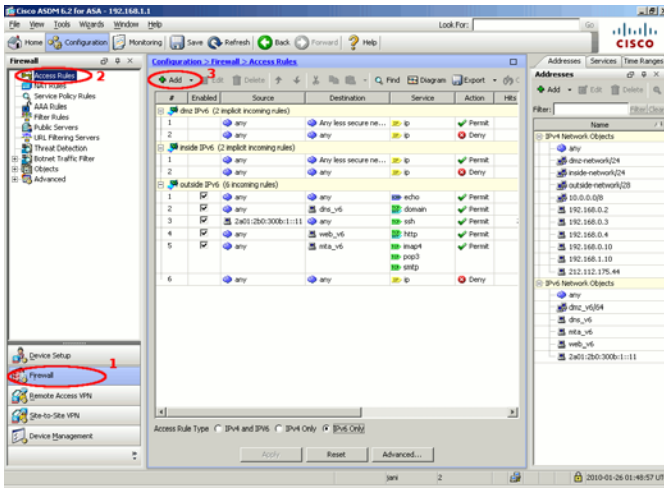
Vi behöver åtminstone en default route för att få ut trafik via IPv6 genom brandväggen. Detta lägger man till på samma sätt som IPv4 routes.



Steg 1: Välj statisk routing

Steg 2: Lägg till default route (::/0) och dess gateway

Återstår att konfigurera brandväggsregler. Detta görs likadant som för IPv4.



Steg 1: Välj brandväggsfunktion

Steg 2: Välj brandväggsregler

Steg 3: Lägg till IPv6 regler

Debian/Ubuntu Linux

För att konfigurera fasta IPv6-adresser behöver man lägga till följande i */etc/network/interfaces*:

```
#IPV6 static configuration
iface eth0 inet6 static
pre-up modprobe ipv6
address 2001:db8:10:4600::2
gateway 2001:db8:10:4600::1
netmask 64
# END IPV6 configuration
```

Där *address*, *gateway* och *netmask* byts ut mot egna värden (observera att dessa är påhittade dokumentationsadresser).

För att förhindra autokonfigurering av adresser lägger man till följande i*/etc/sysctl.conf*:

```
# Disable RA since we use static addresses
net.ipv6.conf.default.accept_ra=0
```

För att göra DNS-uppslag över IPv6 kan man lägga till IPv6-adress till DNS-server i */etc/resolv.conf*:

```
domain v6lab.ip-solutions.se
nameserver 2001:db8:10:4600::2
nameserver 192.168.0.2
```

OpenBSD

Skillnaden mellan linux och BSD är minimal. I OpenBSD lägger man manuella IPv6-adresser i */etc/hostname.if (*där *if* beror på interfacenamn) enligt följande konvention:

```
inet6 alias 2001:db8:10:4600::3 64
```

Default gateway läggs i */etc/mygate*:

```
192.168.0.1
2001:db8:10:4600::1
```

Autokonfigurering är avslaget som standard. För att aktivera det kan man avkommentera följande rad i */etc/sysctl.conf*:

```
#net.inet6.ip6.accept_rtadv=1    # 1=Permit IPv6 autoconf (forwarding must be 0)
```

För att göra DNS-uppslag över IPv6 kan man lägga till IPv6-adress till DNS-server i */etc/resolv.conf*:

```
domain v6lab.ip-solutions.se
nameserver 2001:db8:10:4600::2
nameserver 192.168.0.2
```

DNS – Bind 9

Sektioner i /var/named/etc/named.conf som kan påverkas av IPv6-konfigurering:

```
controls {
        inet 127.0.0.1 port 953
        allow { localhost; 127.0.0.1; ::1; } keys { "rndc-key"; };
};

acl local_clients {
        localnets;
        ::1;
        192.168.0.0/16;
        2001:bd8:10:4600::/64;
};

acl updaters {
        localhost;
        ::1;
        192.168.1.10;
        2001:db8:10:4601::4711/128;
```

```
};

options {
        version "Yes I have a version";

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

Baklängesuppslag för loopback är inkluderat som standard i named.conf, men om man vill lägga till sin egen baklängesuppslagning i */var/named/etc/named.conf* gör man det på följande format:

```
zone "0.0.6.4.0.1.0.0.8.b.d.0.1.0.0.2.ip6.arpa" in {
        type master;
        file "/var/named/master/0.0.6.4.0.1.0.0.8.b.d.0.1.0.0.2.ip6.arpa";
        allow-update { updaters; };
};
```

IPv6-uppslag läggs till i zone-filen med följande syntax:

```
www             AAAA    2001:db8:10:4600::4
```

Baklängesuppslag läggs till i zone-filen med följande syntax:

```
4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0    IN    PTR    www.v6lab.ip-solutions.se.
```

Webb – Apache 1.3

För att webbservern skall ta emot anrop via IPv6 behöver man lägga till följande i filen */var/www/conf/httpd.conf*:

```
Listen [::]:80
```

Detta innebär att apache tar emot anrop på port 80 på alla interface som har en IPv6-adress konfigurerad.

MTA – postfix

Det man behöver kontrollera i */etc/postfix/main.cf* är följande variabel:

```
# OpenBSD is IPv6-capable - use all available address families.

inet_protocols = all
```

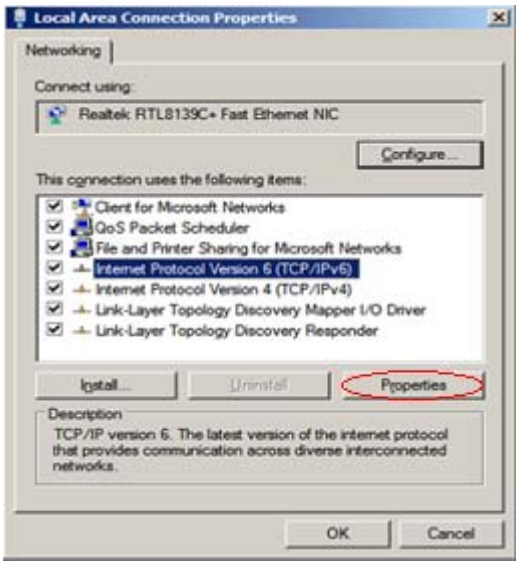
Vill man specifiera vilken adress e-posten ska skickas från kan man ange detta med variabeln *smtp_bind_address6*. Vidare bör man kontrollera att nästa destination i */etc/postfix/transport* för en vidarebefordran är satt till ett dns-namn eller en IPv6-adress såvida inte IPv4-transport önskas.

Exchange 2007

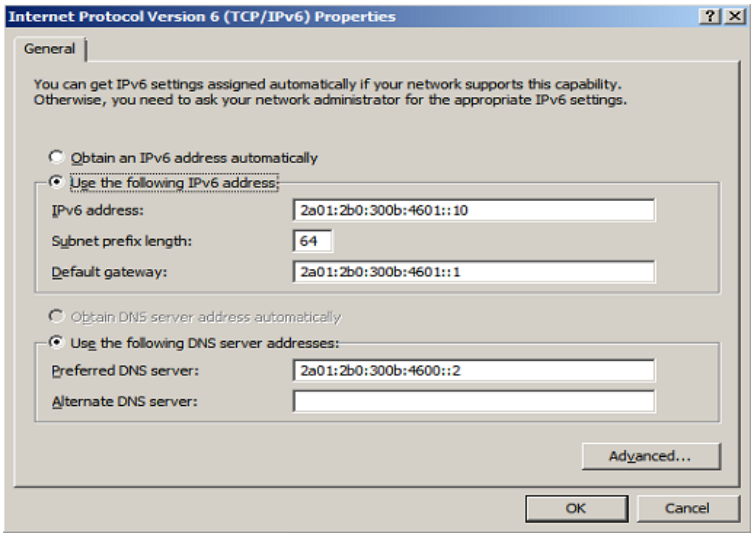
Ingen särskild konfigurering krävs i Exchange så länge operativsystemet är Windows Server 2008 och namnservern gör uppslag till IPv6-adresser.

Windows Server 2008

Windows Server 2008 har IPv6 påslaget och använder autokonfigurering som standard. Manuella adresser kan man ställa in under nätverksegenskaper enligt bilderna nedan.



Steg 1: Välj IPv6

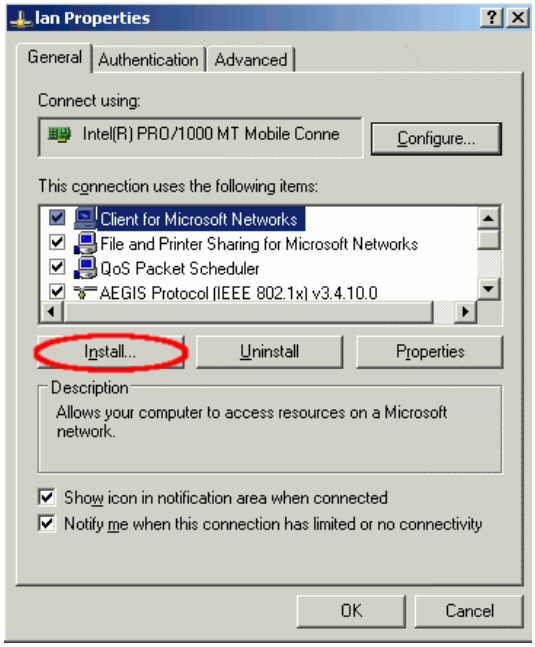


Steg 3: Ställ in aktuella IPv6-adresser

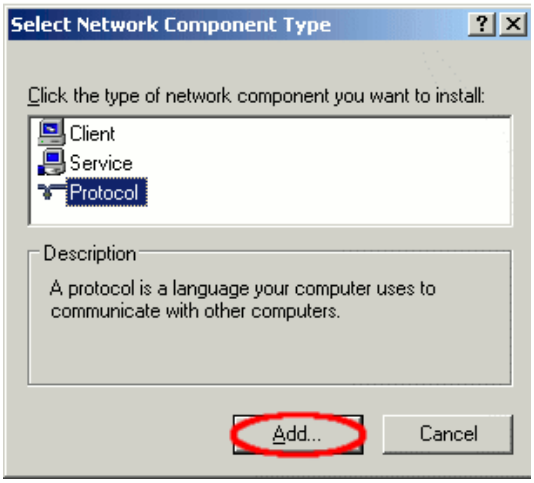
Steg 2: Välj egenskaper

Windows XP/2003 Server

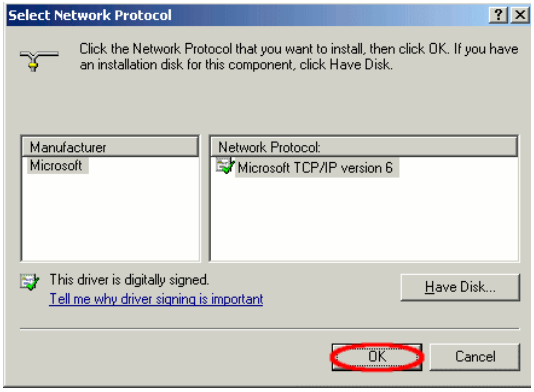
För att lägga till IPv6 i Windows XP eller 2003 Server, välj egenskaper för valfri nätverksenhet. Följ därefter instruktionerna i bilderna nedan.



Steg 1: Välj installera...



Steg 2: Välj Protokoll

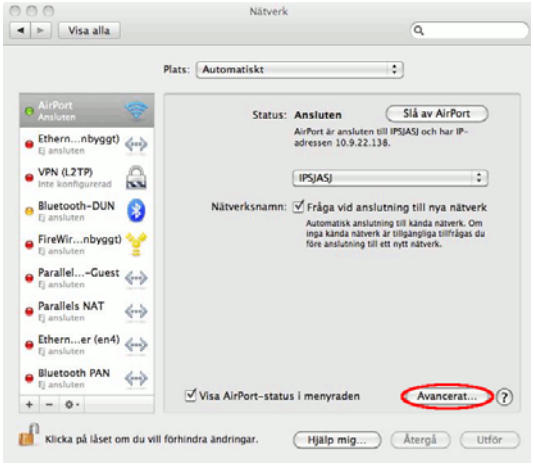


Steg 3: Markera IPv6

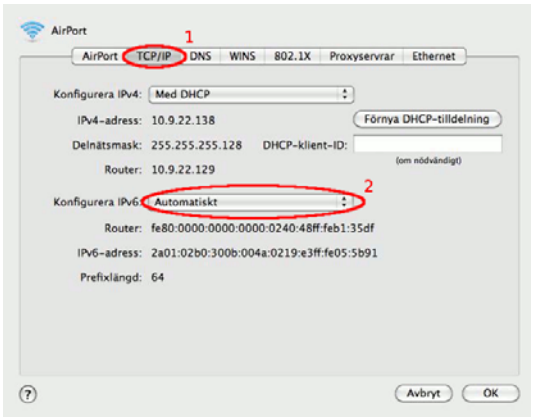
Mac OS X

Mac OS X har IPv6 påslaget som standard. För att ändra inställningar går man till väga enligt ovan.

Steg 1: Välj nätverk under systeminställningar



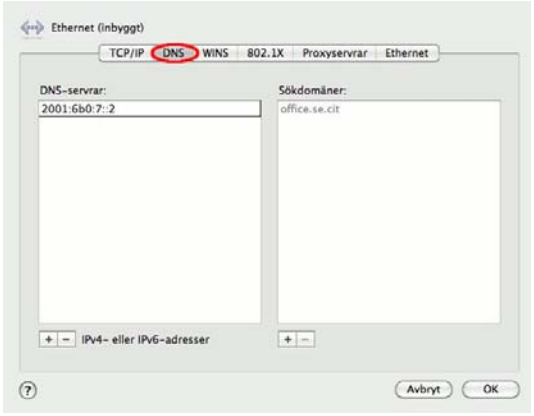
Steg 2: Välj nätverksenhet och klicka Avancerat...



Steg 3: Välj fliken TCP/IP

Du kan nu ändra IPv6 inställningar om du vill

Du kan sätta en manuell namnserver adress under fliken DNS



Nyttiga erfarenheter

Detta är en sammanställning av de erfarenheter och kunskaper som redovisas i denna guide.

Access

Tillgång till IPv6 är än så länge ganska begränsad. Oftast får man gå via inofficiella kanaler för att få tillgång till IPv6. När efterfrågan stiger kommer även leverantörerna att kunna erbjuda färdigpaketerade lösningar.

Brandväggar

Börjar få bra stöd för IPv6, men uppdateringar kan krävas.

Operativsystem

De flesta moderna operativsystem har bra stöd för IPv6.

Exchange 2007 på Windows Server 2003

Även om både Exchange 2007 och Windows Server 2003 stödjer IPv6, så stödjer de inte IPv6 i denna kombination. Exchange 2007 kräver minst SP1 och Windows Server 2008 för att kunna köra IPv6. För att köra Exchange 2007 på Windows Server 2008 R2 krävs Exchange 2007 med SP3 (som ännu ej släppts när detta dokuments skrivs).

Autokonfigurering

Brandväggar kan skicka Router Advertisements för att autokonfigurera IPv6-förberedda datorer. Det går dock inte att konfigurera namnserver-adresser den vägen. Alternativen är att köra dual-stack och använda DNS över IPv4 (via DHCP) eller att manuellt konfigurera namnservrar på varje maskin.

Utveckling i denna fråga pågår och möjligen kan detta lösas antingen via en option till Router Advertisement eller via en fast multicast-IPv6-adress för namnservrar.

Timeouter

En IPv6-konfigurerad dator kommer alltid att premiera IPv6-trafik vid utskick till en IPv6-destination. Om det saknas IPv6-förbindelse någonstans längs vägen till destinationen, kommer man att stöta på en timeout innan den sändande datorn övergår till IPv4.

Diverse

Ping av link-local adresser kräver specificering av interface.

IPv6 URL:er måste anges med [] om port skall anges (till exempel [2001:db8:10:4600::4]:80).

Påbyggnad

Denna guide tar endast upp de grundläggande tjänster som man kan förvänta sig ett medelstort företag använder sig av. Det finns en uppsjö av andra tjänster som också är aktuella för en övergång till IPv6, som till exempel databaser, vpn, ekonomisystem samt egenutvecklad mjukvara. Det kommer med största sannolikhet också att finnas kvar tjänster i näten som är gamla och inte kommer att uppdateras till IPv6,

men som alltjämnt används. Därför kommer nog IPv6 och IPv4 få leva parallellt ett tag framöver.

Denna guide kan senare komma att kompletteras med andra populära tjänster för att underlätta övergången till IPv6.

Bilaga 1
Ett praktiskt exempel på installation av IPv6

Parallellt med att IP-Solutions byggt sitt labbnät för IPv6 har vi på konsultföretaget Interlan infört IPv6 på bioenergiföretaget Bruks AB i Arbrå, Hälsingland (http://www.bruks.com). Flera problem och frågeställningar som dykt upp under detta arbete känns igen ifrån IP-Solutions guide, men Interlan lägger till några viktiga saker.

Införandet av IPv6 på Bruks inleddes med en inventering av de centrala punkterna i nät och operativsystem där vi, kanske något förutfattat, försökte kontrollera vilket stöd för IPv6 som redan borde finnas. Till exempel pekade vår undersökning kring Cisco, utifrån deras hemsida, på att erfarenheter fanns kring lösningar med Cisco Catalyst 3750, IPv6 och Fortigate brandvägg. Erfarenheter fanns förvisso men informationen var inte på långa vägar tillräckligt noggrann för att vara omedelbart användbar.

En viktig slutsats av vårt arbete är att när man inför IPv6 bör man arbeta i en miljö där man kan experimentera relativt ostört eller, om detta inte är möjligt, ha beredskap för att snabbt backa tillbaka till en fungerande konfiguration.

Nätskiss Bruks - Arbrå, Cisco Catalyst 3750 som L3-switch och Cisco Catalyst Express 500 som distributionsswitchar. Brandväggen är en Fortigate 100.

IPv6 i Cisco Calalyst 3750

Enligt ”Ciscos Feature Navigator” (http://www.cisco.com/go/fn) ska programmodulen IP Services 12.2(25) stödja IPv6. Vi slog på IPv6 i Cisco 3750:an med configurationsraden:

```
sdm prefer dual-ipv4-and-ipv6 routing
```

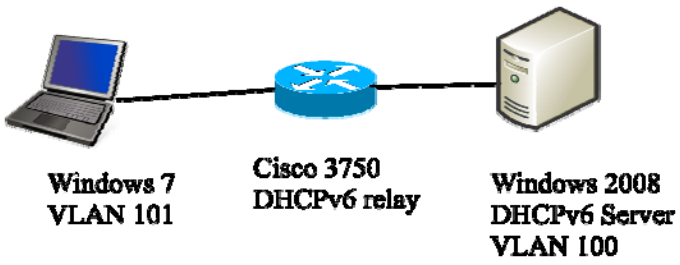
Efter detta startade vi om switchen. Det visade sig dock att den releasen inte stödjer *"IPv6 Routing: Unicast Routing"* som vi behövde för installationen. Därför blev det nödvändigt att uppgradera till den senaste versionen, 12.2(53).

Tyvärr medförde dock version 12.2 (53) andra problem som resulterade i att vi delvis fick avbryta införandet. Den versionen gjorde att Bruks Cisco Catalyst Express 500-switchar, som var anslutna mot trunkportar i Cisco 3750:an och hade äldre versioner av IOS, inte kunde ansluta då Cisco 3750:ans mjukvara nu ansåg att det krävdes 802.1X-inloggning för de portarna. Vi kommer att lösa detta problem genom att uppgradera Express 500-switcharna, men i skrivande stund är vi inte i mål med detta.

Resterande installation av IPv6 genomfördes därför i labbmiljö då vi inte ville störa Bruks produktion ytterligare.

IPv6 i Cisco Calalyst 3750 del 2

Hemma på bänken sattes följande scenario upp för att testa DHCPv6-relay



Konfigurering i 3750

```
ipv6 unicast-routing

interface GigabitEthernet1/0/23
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/24
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast

interface Vlan2
 ipv6 address 2001:db8:10:2::101/64
 ipv6 nd ra suppress
 ipv6 nd ra lifetime 3600

interface Vlan100
```

```
ipv6 address 2001:db48:10:101::1/64
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp relay destination 2001:db8:10:2:C27F:7648:CCC3:22F8
```

Här uppstod ett problem. När datorn anslöts i port 23, dvs. VLAN 2, började 3750:n skicka ut RA för `2001:db8:10:2::101/64 på` port 24 som tillhör VLAN 100. Detta fenomen tog en hel del tid att felsöka och förstå att detta var en bugg. Efter ett byte av portar och VLAN-ID fungerade det dock som det skulle.

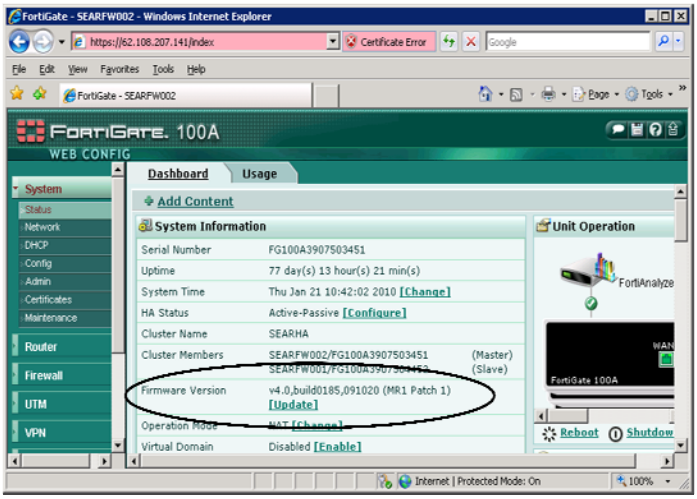
Fortigate

Då vi hade stora problem med att få IPv6 levererat till kunden, oavsett vilken ISP vi tillfrågade, beslöt vi att ta in IPv6 enbart till Bruks enhet i Arbrå och sedan tunnla IPv6 till de andra orterna. Vad vi då upptäckte var att det i Fortigate-brandväggen finns en begränsning på fyra IPv6 över IPv4-tunnlar per virtuell domän. Information om detta gick inte att återfinna i någon dokumentation över huvud taget. Efter att ha öppnat ett supportärende har vi fått denna brist bekräftad av leverantören. Den enklaste lösningen verkade då istället vara att skapa Ipv6-över-IPv4-tunnlar via varje 3750 på varje ort. Återigen fick vi konstatera att vi skulle ha läst på mer noggrant i Ciscos Feature Navigator - Catalyst 3750 stödjer nämligen inte IPv6-över-IPv4 tunnlar.

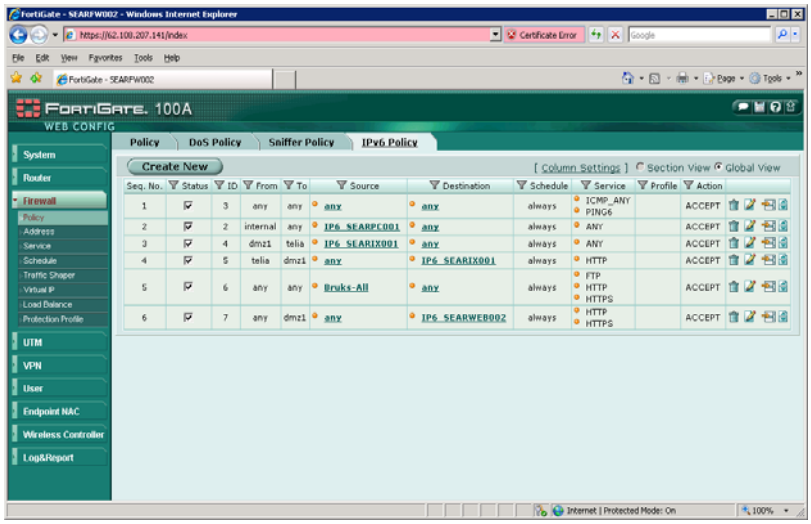
Fortigate konfigurering

Fortigate hanterar all regeluppsättning och adresser/nätverk/routing i det grafiska användargränssnittet. Fortfarande måste dock mer avancerade inställningar göras från kommandoraden. Exempel på det är IPv6 över IPv4 (SIT-tunnel) och mer avancerade ICMPv6 funktioner. Se nedan för exempel på hur det kan se ut.

Fortigate version



Fortigate regelverk



SIT-Tunnel

Exempel på en SIT-Tunnel mellan 194.17.167.85 och 212.181.12.14

```
config system sit-tunnconfig system sit-tunnel
     edit "telia"
         set destination 194.17.167.85
         set interface "wan2"
         set ip6 2001:db8:4070:b::2/64
         set source 212.181.12.14
     next
```

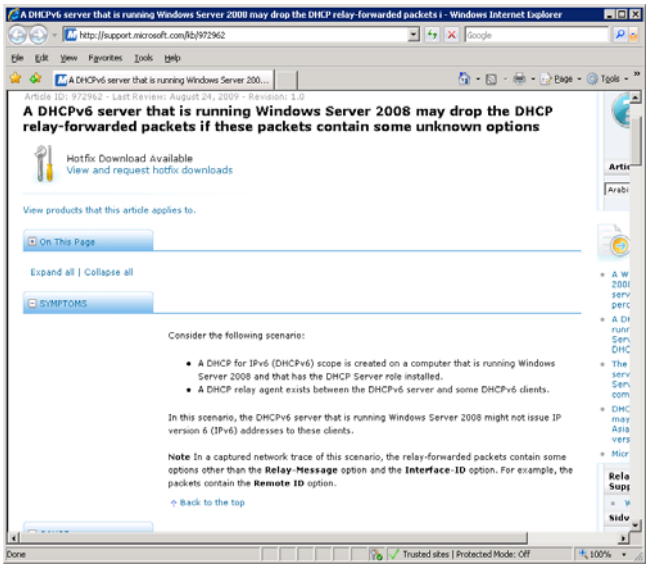
Interface med M (Manage flag) och O (Other flag) flagga och lite annat konfigurerat för att klienter skall hämta både en managerad IPv6-adress och övrig information från DHCPv6-server.

Det som är markerat med fetstil nedan går inte att ställa in i det grafiska gränssnittet i den version som vi använde. Detta är inget större problem då man gör det endast en gång och sedan till större delen använder det grafiska gränssnittet efter detta.

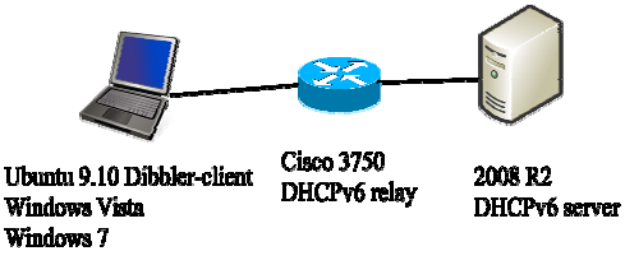
```
config system interface
    edit "vlan-7"
        set vdom "root"
            config ipv6
                set ip6-address 2001:db8:10:8::1/64
                set ip6-allowaccess ping
                set ip6-manage-flag enable
                set ip6-other-flag enable
                    config ip6-prefix-list
                        edit 2001:db8:10:8::/64
                            set autonomous-flag enable
                        next
                    end
                set ip6-send-adv enable
            end
        set interface "internal"
        set vlanid 7
```

Windows 2008 Server

Vi ville använda Windows 2008 Servers inbyggda DHCPv6-server för tilldelning av IPv6-adresser till Windows 7-klienter. En sådan server även upp i labbet men vi fick det inte att fungera direkt. Vi kunde se att förfrågningar kom in till DHCPv6-servern men de såg inte ut att tas om hand och det skickades inga svar. Efter lite googlande och sökande hittade vi till slut en hotfix för detta till Windows Server 2008. (Denna hotfix behövs inte om du redan kör Windows 2008 Server R2.)



Här kan man ju fråga sig varför detta ska distribueras som en hotfix och inte ingår i en vanlig ”tisdagsuppdatering”?



När vi lagt DHCPv6-servern i en Windows Server 2008 R2 testade vi enligt bilden ovan och fick allting att fungera bra.

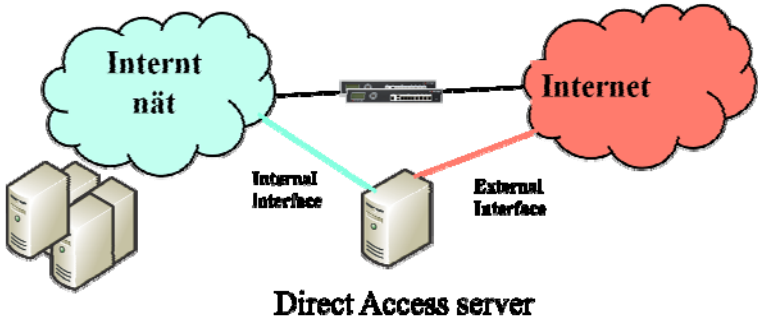
Microsofts Direct Access, Windows 7 Phone Home

Den stora kioskvältaren för IPv6, Microsoft Direct Access (ett annat bra namn skulle vara *"Windows 7 Phone Home"*) är en mycket bra lösning som ger en känsla av att du alltid sitter på kontorsnätet. Direct Access är i stort sett en automatisk VPN som gör att din dator vid Internetaccess alltid loggar in på kontorsnätet oberoende av var du befinner dig. Funktionen finns i Windows 7 tillsammans med Windows Server 2008 R2 och bygger på IPv6 och en Direct Access Server som placeras rakt ut på Internet. Lösningen skall dock absolut kompletteras med någon form av perimeterskydd som en brandvägg.

Direct Acess bygger på native IPv6, Teredo, 6to4 och Microsofts egna IPv6-tunnel IP https (IPv6 över https).

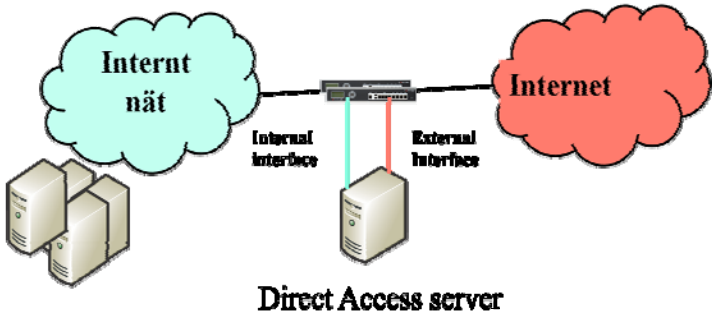
Direct Access , metod 1

Här placerar man DA-servern parallellt med sin befintliga brandvägg och förlitar sig på Microsofts brandvägg i 2008 R2.



Direct Access, metod 2

Här placerar man DA-servern på ett DMZ där vi måste öppna IPv4 protokoll 41, TCP port 443 och UDP port 3544 för att få de olika tunnlarna att fungera. IPv4-adresserna på det externa interfacet kan inte vara privata (hämtade ur RFC 1918) för då fungerar inte 6to4-tunnlingen. För native IPv6 måste IKE och ESP öppnas till DA-servern. Vi testade detta med native IPv6 på DA-servern vilket då borde innebära att det går att stänga av 6to4 på det externa interfacet men det lyckades vi inte med.



Slutsats

Den tydligaste erfarenheten från införandet på Bruks AB är att om man har en större miljö bör man börja i

en mindre skala, slå inte på IPv6 överallt och på en gång. Dessutom skall man göra en inventering som är betydligt noggrannare än den vi genomförde i det här fallet. Men även om vi lagt mer tid på inventering skulle vi ha stött på patrull då vi råkade ut för flera odokumenterade brister gällande, i detta fall, leverantörerna av aktuell hårdvara. Hade vi inte lagt om detta till en installation i labbmiljö hade störningarna för produktionen blivit fler. Man bör alltså planera testerna med möjligheten att det blir störningar i åtanke.

Bakom detta införande

Nu kan man ju tro att allt detta är ännu ett inlägg i debatten från den där Torbjörn Eklöv, sanningen är dock att allt det praktiska arbetet i Arbrå är utfört av Interlans Per Olsson och Esko Laitila.