TEKNISKA HÖGSKOLAN

HÖGSKOLAN I JÖNKÖPING

Att införa IPv6 i ett befintligt IPv4-nätverk

Olof Kasselstrand

EXAMENSARBETE 2007

Datateknik

TEKNISKA HÖGSKOLAN

HÖGSKOLAN I JÖNKÖPING

Deploying IPv6 in an IPv4 network

Olof Kasselstrand

Detta examensarbete är utfört vid Tekniska Högskolan i Jönköping inom ämnesområdet Datateknik. Arbetet är ett led i den treåriga högskoleingenjörsutbildningen. Författarna svarar själva för framförda åsikter, slutsatser och resultat.

Handledare: Christer Thörn

Omfattning: 10 poäng (C-nivå)

Datum: 2007-06-05

Arkiveringsnummer:

Postadress: Box 1026 551 11 Jönköping

Besöksadress: Gjuterigatan 5

Telefon: 036-10 10 00 (vx)

Abstract

Internet is growing every day and this is leading to an address depletion of the current IPv4 addresses. A new version of IPv4, called IPv6, is the protocol for addressing computers that will deal with this problem. IPv4 and IPv6 are unfortunately not compatible with each other. IPv4 and IPv6 have to co-exist for a long time until IPv6 will be the dominant protocol.

The purpose of this thesis is to examine how a transition could be done or more correctly, how to deploy IPv6 in an already existing IPv4 network. After that part of the report a case study at the local Internet service provider Junet AB will be conducted. This case study will investigate an IPv6 deployment scenario for Junet AB.

A theoretical background has been written that describes some steps an Internet service provider has to go through to deploy IPv6. The case study was conducted after the theoretical background was written. The result of this report shows that a deployment of IPv6 in an IPv4 network is technically achievable. All the main components to maintain and use IPv6 in a commercial network exist.

The case study indicates that it is possible to deploy IPv6 in Junet AB´s network. IPv4 and IPv6 could be used in their network without any major effort. IPv6 have been around for many years now but have not had that break through many early adopters have hoped for. A lack of documentation and experience is an obstacle for a deployment of IPv6.One thing that remains now is to prove that there is a need for IPv6, but that is out of scope for this thesis.

Sammanfattning

Internet växer så det knakar vilket leder till att det befintliga systemet för att adressera noder på Internet, IPv4, inte längre räcker till. Adresserna är helt enkelt för få. En ny version av IPv4, IPv6, är det protokoll som skall ta över efter IPv4. Tyvärr är inte IPv6 kompatibelt med IPv4 utan måste samexistera med IPv4 tills IPv4 har fasats ut.

Syftet med examensarbete är att undersöka hur en övergång eller rättare sagt, hur ett införande av IPv6 ska gå till i en Internetleverantörs redan befintligt IPv4-nätverk. Det är ett brett område med många olika aspekter. Efter denna del ska en fallstudie genomföras hos Internetleverantörer Junet AB för att se hur ett eventuellt införande av IPv6 ska gå till i deras IPv4-nätverk.

Syftet har uppnåtts genom en omfattande teoretisk bakgrund som behandlar olika delar som en Internetleverantör måste undersöka för att införa IPv6. Efter den teoretiska bakgrunden har en fallstudie utförts hos den lokala Internetleverantören Junet AB.

Rapportens resultat visar på att det är fullt tekniskt möjligt att införa IPv6. Resultatet av fallstudien visar på att det är klart möjligt med ett införande av IPv6 i Junet AB:s nätverk. IPv4 och IPv6 skulle utan större insatser kunna användas i deras nätverk. IPv6 har funnits i många år nu men inte fått det genombrott som förespråkare har hoppats på. Alla viktiga tekniska komponenter som behövs finns för att driva ett kommersiellt IPv6-nätverk. En brist på dokumentation och erfarenhet är det som talar emot IPv6. Denna rapport har visat att det är tekniskt möjligt att införa IPv6, nu är det bara att bevisa att det finns behov för det också. Det ligger dock utanför denna rapport avgränsningar.

Nyckelord

IPv6
IPv4
Dual Stack
Tunnlar
Routing

Innehållsförteckning

Figur- och tabellförteckning

1 Inledning

Denna rapport är ett resultat av ett examensarbete utfört hos Junet AB för att reda ut hur IPv6 skall kunna föras in i en Internetleverantörs IPv4-nätverk. Arbetet är uppdelat i två delar, dels en teoretisk bakgrund och en praktisk fallstudie. Examensarbetet är slutfasen på en kandidatexamen på Jönköpings Tekniska Högskola.

1.1 Bakgrund

Internet har en stor tillväxt vilket håller på att leda till att den begränsade tillgången på adresser i IPv4 blir allt mindre. Krav på högre säkerhet och flera nya användningsområden för IP-noder driver utvecklingen framåt. Idag ska mobiltelefonen, handdatorn, den bärbara datorn och kylskåpet ha sin egen IP-adress vilket det inte finns adresser för.

IPv6 har en adressrymd som möjliggör flera miljoner gånger större adressrymd än vad IPv4 kan erbjuda och anses bland annat därför vara den naturliga efterträdaren. Tyvärr är inte IPv6 inte bakåtkompatibel med IPv4 vilket resulterar i en ganska komplicerad övergång. Utbudet av dokumentation och erfarenhet om hur övergången skall gå till är väldigt begränsat och mycket sker genom att testa sig fram.

Det mesta som involverar att driva ett IPv4-nätverk idag så som routing, adressering, säkerhet är på ett eller annat sätt annorlunda i IPv6. En övergång måste även ta hänsyn till hur övergången ska ske (övergångsmetoder) och om mjukvaran (servrar, applikationer, brandväggar) är redo för att IPv6.

Det är inte troligt att övergången till IPv6 kommer gå över en natt utan att IPv4 och IPv6 kommer att leva i samma nätverk under en längre tid.

Denna uppsats ska försöka svara på vad man bör tänka på och hur man ska göra för att göra en övergång baserad på tidigare erfarenhet och befintlig dokumentation. Detta tydliggörs genom en studie hos Internetleverantören Junet AB i Jönköping.

1.2 Syfte och mål

Arbetet är uppdelat i två delar. Den första delen är en teorisk del som benar ut och organiserar upp arbetet med att införa IPv6 i ett redan befintligt IPv4-nätverk och visa på generella skillnader på att använda IPv6 och IPv4. Den andra delen är en fallstudie utförd hos Internetleverantören Junet AB.

Målet är att undersöka och beskriva följande delar när en Internetleverantör ska införa IPv6 i ett IPv4-nätverk:

- Jämförelse mellan IPv6 och IPv4
- Adressering
- Domain Name System (DNS)
- Routing
- Mjukvarustöd
- Säkerhet
- Övervakning och administrering
- Överblick över avancerade tjänster (multicast, Quality of Service)

Den teoretiska delen ligger sedan till grund för en fallstudie hos Internetleverantören Junet AB för att se om en övergång i deras fall är möjlig.

1.3 Avgränsningar

Rapporten beskriver inte vad IPv6 är utan bara ge en kort genomgång. Den kommer inte heller ge någon historisk bakgrund till IPv6. Det är inget försök till att motivera eller ge några argument för eller emot införandet av IPv6. Rapporten försöker inte beskriva eller ge exempel på syntax för konfigurering av routrar, noder eller andra nätverkselement. Det är en uppsats om hur och inte varför.

Fallstudien är enbart en teoretisk studie. Det är inte meningen att göra något praktiskt som att konfigurera nätverksutrustning eller liknande.

1.4 Disposition

Inledning (del 1)

Första delen går igenom och förklarar problemet och bakgrunden.

Teoretisk bakgrund (del 2)

Denna del beskriver och förklarar skillnader mellan att driva ett IPv4- och ett IPv6-nätverk. Nyheter, förändringar och likheter tas upp.

Genomförande (del 3)

Detta avsnitt beskriver fallstudien och vilket utgångsläge den har utgått utifrån. Det går igenom hur Junet AB:s IPv4-nätverk ser ut idag.

Resultat (del 4)

Resultatdelen redogör slutresultatet av fallstudien. Den belyser de delar som Junet AB måste ta i beräkning vid en eventuell övergång till IPv6.

Slutsats och diskussion (del 5)

I denna del följer en diskussion om införande av IPv6 i stort och införandet av IPv6 hos Junet AB.

2 Teoretisk bakgrund

2.1 Begrepp och definitioner

Tabell 2.1 nedan sammanställer begrepp och akronymer som används frekvent i rapporten.

Tabell 2.1:Begrepp och akronymer som används i rapporten

Akronym	Förklaring
ACL	Access List
ARP	Adress Resolution Protocol
AS	Autonoma System
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
EGP	External Gateway Protocol
IDS	Intrusion Detection System
IGP	Internal Gateway Protocol
ND	Neighbor Discovery
NTP	Network Time Protocol
PMTUD	Path Maximum Transfer Unit Discovery
QoS	Quality of Service
RFC	Request For Comments
RIB	Routing Information Base

Utöver dessa begrepp och akronymer finner jag det nödvändigt att förklara ett antal ord som förekommer i rapporten och är viktiga för förståelsen.

Adressrymd En finit mängd av distinkta adresser.

Dual Stack En nod i ett nätverk som både har en IPv4- och en IPv6-stack implementerad. Denna nod kan kommunicera med andra sammankopplade noder över både IPv4 och IPv6.

Host En nod som inte är en router.[39]

ISP En Internet Service Provider (ISP), eller Internetleverantör, är ett företag som erbjuder privatpersoner och företag anslutningar till Internet. Det kan ske med olika tekniker och hastigheter. ISP:n i sig har anslutning till Internet och andra ISP:er.

LIR En Local Internet Registry (LIR) är en organisation som har blivit tilldelad en IP-adressallokering från en RIR och delar ut delar av sin allokering till sina egna kunder. Internetleverantörer är ett exempel på en LIR. För att vara en LIR måste man vara medlem i en RIR.[3]

Nod En dator som har IPv6 implementerat.[39]

Prefix Ett decimalvärde som specificerar hur många bitar som identifierar nätverksdelen av en adress.[18]

RIR En Regional Internet Registry (RIR) är en organisation som ansvarar för adressallokeringar och registreringar av Internetnummerresurser i specifika regioner av världen. Internetnummerresurser inkluderar IP-adresser (både IPv4 och IPv6) och AS-nummer.[3]

Router En nod som vidarebefordrar paket som inte är adresserade till sig själv.[39]

Slutkund Slutkund (end site, end user, subscriber) definieras som en kund som har en affärsrelation med en Internetleverantör som innefattar att Internetleverantören allokerar adressrymd till Slutkunden och levererar trafik från Slutkund till andra nätverk. [3]

2.2 Jämförelse av IPv6 och IPv4

IPv4 och IPv6 har mycket gemensamt men IPv6 har tagit vara på erfarenheten från användandet av IPv4 över Internet. En förenklad struktur och fast storlek på IP-paketens huvud gör att hantering och vidarebefordring av IP-paket går snabbare i routrar. 14 fält har blivit 8 i pakethuvudet. En flow label har lagts till för att på ett snabbt och dynamiskt sätt kunna erbjuda Quality of Service (QoS). Utöver detta har IPv6 mer stöd för vanlig QoS. Stateless autoconfiguration och Neighborhood Discovery möjliggör självkonfiguration av noder utan hjälp av DHCP i IPv6. Broadcast har ersatts med multicast som dessutom ger ytterliggare möjligheter till strömmande medier till exempel video- och röstsamtal över ett IP-nätverk.

2.2.1 Adresser

IPv4 har sina begränsningar; främst den begränsade adressrymden. Den största nyheten i IPv6 är själva adressrymden, adresserna består av 128 bitar istället för 32 bitar som i IPv4. 128-bitars adresser möjliggör cirka 3.4×10^{38} adresser. Det är 1000 IPv6-adresser/gram av jorden. Vilket måste anses vara tillräckligt för en lång tid framöver[18]. En IPv6-adreess kan representeras av ettor och nollor men blir snabbt väldigt osmidigt att hantera. Istället skrivs IPv6-adresser som 4 hexadecimala siffror (16 bitar) i 8 grupper separerade med kolon (:). En giltig IPv6-adress kan se ut så här: 2001:0770:0010:0300:0000:0000:86e2:510b. Adressen är fortfarande väldigt lång och det finns därför två regler som kan användas för att förenkla en IPv6-adress:

- Inledande nollor kan tas bort i en grupp som börjar med en eller flera nollor.
- Förkorta en eller flera grupper som endast består av nollor till ”::”.

Den andra regeln får endast göras en gång per adress. IPv6-adressen 2001:0770:0010:0300:0000:0000:86e2:510b kan förkortas till 2001:770:10:300::86e2:510b enligt de ovanstående reglerna. Utöver det nya sättet att skriva de nya adresserna finns det tre olika typer av IPv6-adresser som är definierade i RFC 4291[18]:

- **Unicast -** Identifierar ett nätverksgränssnitt. Ett paket sänt till en unicast-adress skickas till det nätverksgränssnittet som är identifierat av unicast-adressen.
- **Anycast -** Identifierar en mängd nätverksgränssnitt. Ett paket som skickas till en anycast-adress levereras till ett nätverksgränssnitt som är identifierat med den adressen (det närmaste nätverksgränssnittet enligt routingprotokoll).
- **Multicast -** Identifierar en mängd nätverksgränssnitt. Paket som skickas till en multicast-adress levereras till samtliga nätverksgränssnitt som identifieras av adressen.

Broadcast som återfinns och används rikligt i IPv4 används inte i IPv6. Broadcastmekanismer har ersatts av anycast- och multicast-adresser. Detta påverkar alla program och funktioner som i IPv4 använder sig av broadcast och som ska fungera i IPv6 också.

IPv6 global unicast adresser är motsvarigheten till publika IPv4-adresser och är på samma sätt aggregerbara som CIDR. En adress består av ett prefix och en nätverksgränssnittidentifierare. Prefixets längd anges genom att skriva ett ”/” efter adressen följt av ett decimalvärde som anger längden, exempel: 2001:100::/64. Nätverksgränssnittidentifierare kan skapas på följande sätt:

- Från lager 2 adressen (MAC)
- Automatiskt genererade adresser[46]
- Erhåll ett från DHCPv6
- Manuellt konfigurerad
- Krytografiskt genererat baserat på RFC 3972[47]

Nytt från IPv4 är också begreppet scope. En IPv6-nod har flera adresser i flera olika scope. Exempel på scope är link-local och global scope. Link-local scope innebär alla noder på samma länk (Ethernet-segment, lager 2 domän) och dessa adresser genereras från lager 2 adressen (MAC-adressen). Denna adress går sedan att använda helt automatiskt för att kommunicera med övriga IPv6-noder på samma länk.
Global scope betyder en IPv6-adress som är nåbar över hela Internet och är motsvarigheten till en publik IPv4-adress.

En IPv6-nod måste lyssna på ett antal adresser enligt RFC 4291[18]:

- En link-local adress för varje nätverksport.
- Alla Unicast- och anycast-adresser som den har blivit tilldelad.
- En loopbackadress (::0).
- ”All Nodes Multicast”-adressen.
- Solicited-Node multicast-aderessen.
- Multicast-adressen som tillhör alla unicast- och anycast-adresser den har.

Om noden dessutom är en router måste den även lyssna på Alla ”Subnet-Router anycast”-adresser som den är konfigurerad att fungera router för. Har den konfigurerats för anycast måste den lyssna efter paket till denna anycast-adress. Den sista adressen den måste lyssna efter är ”All Routers”-multicast-adressen.

Det kan tyckas vara många adresser men en nod ställer in de flesta adresserna själva. Det enda som behöver konfigureras in manuellt är unicast-adressen.

2.2.2 IPv6-Paket

IPv6-paket ser inte riktigt ut som IPv4-paket. IPv6-paket har fått ett mer slimmat utseende och är mer optimerat för routing. IPv4-pakethuvud (se Figur 2-1) har 14 fält medan IPv6-pakethuvud (se Figur 2-2) endast har 10 fält. IPv6-pakethuvud har en fix längd på 40 bytes till skillnad från IPv4 där huvudet kan vara av variabel längd. Ett nytt fält är bland annat ”flow label” som tillsammans med Source Address (SA) och Destination Address (DA) kan identifiera ett IP-flöde som gör det möjligt för routrar att bygga upp tabeller över var paket ska skickas istället för att titta på DA hela tiden.

<table>
<tr><td>Ver (4)</td><td>Header Length</td><td>Type of Service</td><td>Total Length (16)</td></tr>
<tr><td colspan="2">Identification (16)</td><td>Flags (3)</td><td>Fragment Offset</td></tr>
<tr><td>Time to Live (8)</td><td>Protocol Number</td><td colspan="2">Header Checksum (16)</td></tr>
<tr><td colspan="4">Source IPv4 Address (32)</td></tr>
<tr><td colspan="4">Destination IPv4 Address (32)</td></tr>
<tr><td colspan="2">Options (Variable)</td><td colspan="2">Padding (Variable)</td></tr>
<tr><td colspan="4">Payload</td></tr>
</table>

Figur 2-1: IPv4-pakethuvud.

Ver (4)	Traffic Class (8)	Flow Label (20)	
Payload Length (16)		Next Header (8)	Hop Limit (8)
Source IPv6 Address (SA) (128)			
Destination IPv6 Address (DA) (128)			
Next Header (8)		Data or Options (Variable)	
Payload			

Figur 2-2: IPv6-pakethuvud.

2.2.3 Internet Control Message Protocol version 6 (ICMPv6)

Till skillnad från ICMPv4 måste ICMPv6 vara fullt implementerat i en IPv6-stack. ICMPv6 kombinerar funktionaliteten från ICMPv4, IGMP (Internet Group Management Protocol) och ARP (Address Resolution Protocol). ICMPv6 används över unicast- och multicast-adresser och definieras i RFC 2463[19].

ICMPv6 används på samma sätt som ICMPv4 även om en del funktioner har simplifierats och många nya funktioner har lagts till. ICMPv6 är ett multifunktionellt protokoll som används för att rapportera problem, utföra enkla diagnostester, utföra Neighbor Discovery och hantera medlemskap i olika IPv6-multicast-grupper. Meddelanden är uppbyggda på samma sätt som i ICMPv4. Den största skillnaden mellan de två protokollen är att ICMPv6 används i större grad då det bland annat är en del av Neighbor Discovery Protocol.

2.2.4 Neighbor Discovery Protocol (NDP)

Neighbor Discovery Protocol (NDP) är obligatoriskt för en IPv6-stack. NDP används för översättningar mellan lager 2 och lager 3 adresser, prefix detektering, autokonfigurering av adresser och router detektering för att nämna några funktioner. NDP tar över rollen av ARP och en del funktionalitet av ICMPv4. NDP gör det möjligt för IPv6-noder att hitta andra noder på samma länk och kommunicera med dem automatiskt. Det är också upp till NDP att genomföra Duplicate Address Detection (DAD) för att kontrollera att tilldelade adresser är unika.

NDP är ett opålitligt protokoll vilket innebär att det inte finns några garantier för att meddelanden kommer fram. Detta är oftast inte ett problem på trådbundna medier men kan innebära problem över trådlösa medier. Trådlös kommunikation tappar oftare paket vilket kan innebära problem under till exempel DAD.[1]

2.3 Leverera IPv6

Att hantera och dela ut IP-adresser (unicast) är en stor och viktig del i införandet av IP-tjänster. Manuell konfigurering är alltid en möjlighet men medför stora skalbarhetsproblem och är väldigt tidskrävande. Av denna anledning förlitar sig IPv4 på Dynamic Host Configuration Protocol (DHCP)[20]. Samma typ av mekanism finns också för IPv6 och kallas DHCPv6 eller ”stateful DHCP”. I IPv6 finns ytterliggare ett alternativ till adressering kallat ”stateless autoconfiguration”.

För att en nod ska kunna kommunicera över ett globalt IPv6-nätverk och ta del av dess fördelar behöver en nod veta tre grundläggande saker:

1. Nodens IPv6-adress (Unicast)
2. Primär och sekundär DNS-server
3. Adress till en NTP-server

Den första punkten gäller alla noder vare sig det är en PC, server eller router. De två sista punkterna krävs endast om noden vill slå upp domännamn eller säkerhetsfunktioner, se avsnitt om säkerhet.[1]

2.3.1 Adressallokering

Internetleverantörer ansöker om adressrymd direkt från lämplig Regional Internet Registry (RIR) eller sin uppströmsleverantör. Det finns fem RIRs i nuläget, en Internetleverantör måste vända sig till rätt beroende på var i världen (se Figur 2-3) man ansöker om adressrymd[51]. De fem är:[4]

- American Registry for Internet Numbers (ARIN)
- RIPE Network Coordination Centre (RIPE NCC)
- Asia-Pacific Network Information Centre (APNIC)
- Latin American and Caribbean Internet Address Registry (LACNIC)
- African Network Information Centre (AfriNIC)

Figur 2-3: Världskarta med samtliga Regional Internet Registry (RIR) markerade.

Internetleverantörer i Europa skall alltså vända sig till RIPE NCC för att ansöka om IPv4- och IPv6-adresser. Varje RIR har sina egna regler för adressallokeringar och regler om hur Internetleverantörerna skall allokera adresser i sin tur. För att kunna bli tilldelad en allokering av IPv6-adresser av RIPE NCC måste Internetleverantören:[3]

1. vara en Local Internet Registry (LIR):
2. inte vara en slutkund:
3. planerna att erbjuda kunder IPv6-konnektivitet och tilldela dessa /48-allokeringar och annonsera det genom sin aggregerade adressallokering: och
4. ha en plan för att dela ut 200 /48 till andra organisationer inom två år.

Om Internetleverantören uppfyller de fyra kraven är den kvalificerad att bli tilldelad minst en /32-allokering. Allokeringen kan bli större än ett /32 om Internetleverantören skickar in dokumentation som kan rättfärdiga det.

Med en adressallokering följer också ansvaret för att ta hand om den baklängesuppslagningszonen (reverse lookup zone) som måste finnas för adressrymden. Internetleverantören ansvarar för att zonen blir korrekt uppdaterad och fungerar som den ska.[3] Mer om hur DNS-servern skall konfigureras kommer i avsnittet om DNS.

2.3.2 Adressering av infrastruktur

De nätverk som var tidigt ute med att införa IPv6 använde ofta väldigt långa prefix (/127) på de IPv6-adresser som de gav till sina routrar. Ungefär som användandet av /30 i IPv4[22]. Detta är numer förbjudet enligt sektion 2.4 av RFC 4291[18]. Det rekommenderade tillvägagångssättet är idag istället att avsätta ett /48 för den egna infrastrukturen och använda /64 från det avsatta /48-prefixet[1] för att adressera routrarnas nätverksgränssnitt. Viktigt att notera är att routingprotokollen använder ofta link local-adressen för att kommunicera med direkt anslutna grannar.

2.3.3 Adressdelegering till slutkunder

Adressdelegering, utdelning av IPv6-adresser till slutkunder, skiljer sig från IPv4-utdelning. Internet Engineering Steering Group (IESG) och Internet Architecture Board (IAB) rekommenderar i RFC 3177 sektion 3 följande adressdelegeringar till slutkunder:[35]

- /48 i de flesta fallen, förutom väldigt stora kunder
- /64 när ett och endast ett subnät behövs (flesta privatkunder)
- /128 när det är väl konstaterat att bara en nod ansluter

Prefix längre än 64-bitar är effektivt förbjudet enligt RFC 4291 sektion 2.5.1 där man kan läsa: *"Interface IDs are required to be 64 bits long"*, vilket betyder att prefixets maxlängd begränsas till 64 bitar. Det resulterar i att den sista regeln i RFC 3177 sektion 3 inte gäller. Adressdelegering till slutkunder blir efter detta:

- /48 i de flesta fallen, förutom väldigt stora kunder
- /64 när ett och endast ett subnät behövs (flesta privatkunder)

Om en slutkund behöver en större tilldelning än ett /48 måste den kunna tillhandahålla dokumentation eller material som rättfärdigar detta.[3]

2.3.4 Stateless autoconfiguration

Detta är en enkel och automatisk metod som kan användas vid adressering av alla typer av noder. IPv6-aktiverade noder lyssnar efter Router Advertisment-meddelanden (RA) för att få tag på informationen som behövs för automatiskt adresskonfigurering. En nod kommer efter det följa tre steg:[21]

1. **Undersöka vilket prefix som används på länken -** Prefixet hämtar noden från RA-meddelandet som skickas ut från routrar på samma länk. Prefixet som finns RA-meddelandet har konfigurerats in av en administratör av routern.
2. **Generera ett interface-ID -** För att få en fullständig adress måste noden generera ett 64-bitar långt interface-ID och slå ihop det med prefix (<=64 bitar) för att uppnå en 128-bitars lång adress. Interface-ID:t genereras genom slumpning eller basera den på sin MAC-adress; så kallad EUI-64 ID[2].
3. **Verifiera att IPv6-adressen är unik -** Med hjälp av Duplicate Address Detection (DAD)[21] kontrolleras att den framtagna IPv6-adressen är unik före den används.

Denna metod för att adresser noder löser bara problemet med att ge noden en adress. Det finns ingen möjlighet att distribuera IP-adresser för DNS-servrar till noderna vilket måste konfigureras manuellt på varje nod.

2.3.5 Stateful DHCP

Dynamic Host Configuration Protocol (DHCP) är vanligt förekommande i IPv4, både hos Internetleverantörerna och ute hos kunderna. DHCP fungerar även i IPv6 men har uppdaterats och kallas därför DHCPv6[36]. Fördelarna med en DHCP-tjänst är att det är en central resurs som konfigureras och underhålls centralt, DHCP-servern kan även trycka ut annan information till noderna som till exempel IP-adresser till DNS-servrar vilket inte går med stateless autoconfiguration (se föregående avsnitt).

Den enda egentliga nackdelen med DHCP är att det behövs lite intelligens ute hos noderna i form av DHCP-klienter. I dagens Internet kör majoriteten av alla ansluta noder med ett modernt operativsystem (Windows 2000, Windows ME, Windows XP, Windows Vista, *BSD, *nix) som har en inbyggd DHCP-klient så det kan inte ses som en riktig nackdel.

En viktig skillnad mellan DHCPv4 och DHCPv6 är att DHCP-servern lyssnar på link-local multicast-adressen FF02::1:2 efter inkommande DHCP-förfrågningar från klienter. Routrar kan konfigureras för att vidarebefordra klienters DHCP-förfrågningar och skickar då förfrågningar direkt till en förkonfigurerad unicast adress till DHCP-servern eller till multicast-adrssen FF05::1:3. Att multicast-adresser används istället för broadcast (som i IPv4) beror på att broadcast inte längre finns i IPv6 och då heller inte i DHCPv6.

En annan viktig skillnad mellan DHCPv4 och DHCPv6 är att en klient kan begära fler än en adress på samma förfrågan. Klienten genomför Duplicate Address Detection[21] för varje IPv6-adress den får från DHCP-servern.

2.3.6 Övrig utrustning

Övergången från IPv4 till IPv6 fokuserar väldigt mycket på hur routrar, servrar och slutkunder kan hantera IPv6. Övrig utrustning glöms ofta bort. Det är viktigt att inte glömma bort äldre lager 3 switchar och skrivare till exempel.

Om ett kontor ska gå över till IPv6 är det nödvändigt att deras nätverksskrivare fortfarande fungerar och kan kommunicera i nätverket. Skrivare som har en nätverksport behöver uppdateras med en mjukvarauppdatering från tillverkaren för att klara av IPv6 om den inte redan gör det. IPv4 och IPv6 kommer sannolikt att samexistera i samma nätverk flera år framöver vilket ger tillverkarna tid för att göra mjukvarauppdateringar till sina skrivare om de inte redan kan erbjuda stöd för IPv6.

2.3.7 Domain Name System (DNS)

DNS är en mycket viktigt del av ett nätverk för att nätverk skall fungera. Det är dessutom ett krav att den som vill ha en IPv6-allokering måste tillhandahålla en baklängesuppslagningszon för sin allokering. Har man en modern DNS-server ska den klara av både IPv4 och IPv6 samtidigt.

För att slå upp domännamn mot IPv4-adresser används A-records. A-records får endast vara 32-bitar, det innebar att en ny typ av "record" var tvungen att utvecklas för att DNS-systemet skulle kunna hantera 128-bitars IPv6-adresser. Den slutgiltiga lösningen blev "AAAA Record" (uttalas "Quad-A" på engelska). AAAA-Records fungerar likadant som A Records men förväntar sig en 128-bitarsadress istället för en 32-bitarsadress.[37]

Precis som i IPv4 finns det en speciell domän för att översätta en IPv6-adress till ett nodnamn. Domänrooten för IPv6 är IP6.ARPA; tidigare IP6.INT. Precis som i IPv4 skrivs IP-adressen baklänges (punktseparerad, siffra för siffra) men avslutas med IP6.ARPA istället för IN-ADDR.ARPA som i IPv4. Den vanliga PTR recorden används precis som i IPv4.[28]

I en Dual Stack-miljö där alltså noder både har en IPv4- och en IPv6-adress måste alla noder ha dubbla DNS-inlägg. Både för uppslagning och baklänges uppslagning. Om en nod till exempel har IPv4-adressen 125.124.123.1 och IPv6-adressen 2001:ABC:ABC::1 måste den ansvariga DNS-servern ha följande inlägg för uppslagning:

cust-123.example.com	A	125.124.123.1
cust-123.example.com	AAAA	2001:ABC:ABC::1

och följande inlägg för baklänges uppslagning:

1.321.421.521.in.addr.arpa	PTR	cust-123.example.com
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.- 0.0.A.B.C.0.A.B.C.0.1.0.0.2	PTR	cust-123.example.com

När en nod frågar en DNS-server om ett nodnamn kommer DNS-servern svara med både IPv4- och IPv6-infornmation som den har tillgänglig[26]. Om den lokala DNS-servern endast använder IPv6 och root-servrarna endast pratar IPv4 kan namnuppslagning inte ske för att den lokala DNS-servern inte kan nå root-servrarna.[27]

Det kan också vara så att en extern DNS-servrar som har hand om en specifik domän bara pratar IPv4 eller IPv6 vilket innebär att den lokala DNS-servern måste använda den IP-version som stöds hos den externa DNS-servern för att kunna göra förfrågningar hos den. DNS-servern behöver vara Dual Stack för att undvika sådana här svårsökta problem.

2.3.8 Quality of Service (QoS)

Quality of Service (QoS) blir allt viktigare i moderna nätverk då man ofta vill prioritera realtidsapplikationer (IP-telefoni, IP-TV). Stödet för QoS i IPv4 är något begränsat och många har hoppats på att det ska bli bättre i efterträdaren. Sanningen är den att inga revolutionära eller evolutionära ändringar har skett i IPv6. Fältet Traffic Class i IPv6-pakethuvudet motsvarar Type of Service (ToS) fältet i IPv4-pakethuvudet och används på samma sätt. En ny Flow Label har introducerats i IPv6. RFC 3697 definierar hur den ska användas[44]. Flow Label-fältet har fördelen att den ligger före källadressen och destinationsadressen och behandlas därför snabbare. Den används för att sätta upp ”flöden” i nätet som gör att routrar inte behöver inspektera varje pakets käll- och destinationsadress.

Ett lite annorlunda problem uppstår när man implementerar QoS i ett nätverk som både kör IPv4 och IPv6, inte nog med att man kan välja att prioritera trafik på lager eller applikationsnivå, man kan även göra det på protokollnivå. IPv4-trafik kan prioriteras över IPv6-trafik och vice versa. IPv4-trafik är den typ av trafik som idag genererar intäkter och är därför initialt viktigast att eventuellt prioritera.

Att prioritera trafik beroende på applikation är bra lösning. När en användare använder en viss applikation, till exempel IP-telefoni, förväntar sig denne samma kvalitet och prioritet oavsett vilket IP-protokoll som används för att transportera samtalet. Att prioritera trafik på applikationsnivå förenklar dessutom konfigurationen av QoS genom att göra den IP-protokolloberoende. Samma policy för QoS kan användas på båda IP-protokollen.[1]

IPv6 gör det lättare för direkt nod-till-nod kommunikation (ingen Network Address Translation (NAT) behövs) vilket gör att QoS blir mer naturligt i ett nätverk. Användare som ligger bakom NAT på RFC 1918-adresser[43] får idag dela på prioriteten på den eller de skarpa IP-adresserna de använder åt mot Internet. I IPv6 kan alla dessa användare få en egen publik IPv6-adress och därmed egen prioritet oberoende av varandra.

2.3.9 Multicast

Multicast i IPv4 har utvecklats under flera år. Flera funktioner och protokoll har utvecklats, några lyckade och några mindre lyckade. Multicast i IPv6 bygger på funktioner, protokoll och erfarenhet tagna från IPv4. Funktioner och protokoll som visade sig impopulära eller oanvändbara har helt och hållet försvunnit. Multicast är enklare och renare i IPv6, mycket på grund av att multicast var i tankarna när IPv6 utvecklades från dag ett.

Multicast i IPv6 drar också nytta av den stora adressrymden som gör det möjligt för väldigt många multicast-grupper. IPv6 använder scope vilket också hjälper till och förenklar hanteringen av multicast trafik.

I IPv4 används protokollet Internet Group Management Protocol (IGMP) för att hantera multicast-grupper. Detta har ersatts av Multicast Listener Discovery (MLD) i IPv6. Det finns två versioner, MLDv1 och MLDv2. De motsvarar exakt de senaste två versionerna av IGMP. Både MLD och IGMP bygger på ICMP.

Multicast-adressen FF3X:0Y[64 bitar prefix]:[32-bitars grupp ID][1] används för att bygga upp publika multicast-adresser och grupper. Redundans är enkelt att uppnå genom att tilldela två olika servrar (med samma innehåll) samma multicast-adress.[48]

2.3.10 Övergångstekniker

Införandet av IPv6 kommer inte gå över en dag och det är inte heller troligt att nätverk kommer byta från IPv4 till IPv6 rakt av. IPv4 och IPv6 kommer att samexistera under en längre tid.[34]

Kunders anslutningar vid den så kallade ”Access Layer”-delen (AL) av nätverket kanske måste uppgraderas för att IPv6 skall kunna erbjudas. De flesta tekniker som används idag har stöd på ett eller annat sätt för IPv6. Tabell 2.2 sammanställer de medier som stödjer ren IPv6 idag:

[1] Där X representerar scope och Y representerar prefixlängden.

Tabell 2.2: Sammanfattning av anslutningstekniker som stödjer ren IPv6

Typ	Teknik
Uppringd förbindelse	PSTN, ISDN
Digital Subscriber Line (DSL)	SDSL, ADSL, VDSL
Ethernet	10/100/100 Mbps
Wifi	803.11a/b/g, WiMAX
Data Over Cable Service Interface Specification	DOCSIS 3.0
Dedikerad lina	E1, T1, SDH/SONET
ATM och Frame-relay	

Backbone-delen av nätverket kan definieras som den del som aggregerar och sammanbinder AL. Det finns tre huvudsakliga metoder för att köra IPv6 över backbone[1]:

- **Dual Stack** – Routrar har dubbla stackar och använder samma länkar för att skicka all trafik.
- **IPv6 och IPv4 använder olika lager 2 länkar** – Skickar data på samma infrasturktur men över olika ATM eller Frame-relay PVC:er, eller över olika lambda om SONET används.
- **IPv6 ute i kanterna på nätet och tunnlar för att skicka trafiken över backbone.**

En kortsiktig satsning kan vara att använda tunnlar. Det är en billig och relativt enkel lösning, men som inte skalar särskilt bra. När antalet tunnlar ökar blir administrationen snart en börda och snart blir det billigare att satsa på en mer långsiktig lösning. Dual Stack erbjuder en skalbar och effektiv lösning på problemet.

2.3.11 Dual Stack

En av de lättaste och kanske mest självklara övergångsmetoderna är Dual Stack. Dual stack finns beskrivet i RFC 2893[17] och innebär att en nod eller en router både har en IPv4- och en IPv6-stack. Varje sådan nod får sedan både en IPv4- och en IPv6-adress och delar sedan samma länk för transmission. Genom att göra alla routrar Dual Stack får man fullt stöd för IPv6 i sitt nätverk samtidigt som driften av IPv4 kan fortsätta som vanligt.

Nackdelar med Dual Stack är att det drar mer minne och processorkraft från routrarna. Dels måste routerna kommunicera över två protokoll och dessutom behöver man köra två olika routingprotokoll, ett för IPv4 och ett för IPv6. Det är inte säkert att alla routrar har stöd för Dual Stack och måste antingen uppdateras med ny mjukvara eller utrustas med mer minne eller helt enkelt bytas ut.

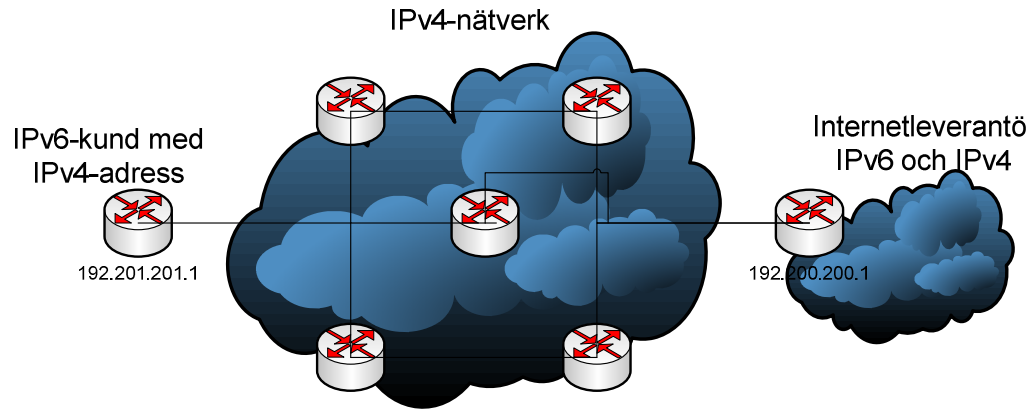
En Dual Stack-lösning kräver att alla routrar, som ska hantera IPv6, uppgraderas eller konfigureras om vilket gör det till en initialt dyr lösning. Alla routrar måste konfigureras med routingprotokoll, IPv6-adresser, Access kontroll-listor, QoS och så vidare. Att köra Dual Stack innebär att man måste underhålla och drifta två protokoll och medför extra kostnader. Extra utbildning för personal kan krävas då personalen måste kunna felsöka, säkra, underhålla två olika IP-protokoll.

Även om Dual Stack anses vara en långsiktig lösning ska man inte glömma bort tunnlar. Tunnlar är ett bra komplement till Dual Stack och kan användas med fördel i vissa delar av nätverket.[1]

2.3.12 Tunnlar

Ibland går det inte att göra hela nätverket Dual Stack eller så finns det inte anledning till det. För att kunna ansluta kunder och isolerade nätverk används olika typer av tunnlar[17]. En tunnel är ett sätt enkapsulera IPv6-paket i IPv4-paket och skicka dem över redan befintlig IPv4-struktur. Det är ett snabbt och kostnadseffektivt sätt för en Internetleverantör att kunna erbjuda IPv6-konnektivitet då det bara är tunnelslutpunkterna som behöver vara Dual Stack. Det finns idag två typer av tunnlar, automatiska tunnlar och konfigurerade tunnlar.

Konfigurerade tunnlar är en av de första mekanismerna som togs fram och stöds av de flesta IPv6-implentationerna. Det är en statisk punkt-till-punkt tunnel som terminerar i en Dual Stack router. Tunnelslutpunkterna måste ha en routebara IPv4-adress och en fast IPv6-adress. IPv6-paketen paketeras i IPv4-paket och skickas över ett IPv4-nätverk. Figur 2-4 visar ett exempel på hur ett sådant scenario kan se ut. Internetleverantören (till höger) och IPv6-kunden (till vänster) tunnlar all IPv6-trafik över det mellanliggande IPv4-nätverk ovanpå IPv4.



Figur 2-4: Exempel på IPv6- tunnel genom ett IPv4 nätverk.

6to4 är en automatisk tunnelmekanism definierad i RFC 3056[11] som använder speciella IPv6-adresser tagna ut IANA:s block 2002::/16. 6to4 fungerar så här: En nod har en publik IPv4-adress, 192.0.2.4. IPv4-adressen kan översättas till en IPv6-adress genom att ta 6to4-prefixet (2002::/16) och ersätta bitarna 17 till 49 med de 32 bitarna från IPv4-adressen. Gör man det får man 2002:c000:0204::/48. För att IPv6-Internet ska kunna kommunicera med denna adress (egentligen hela subnätet) behövs en så kallad relay-router (ansluten både till IPv6 och IPv4) som annonserar ut 2002::/16.[11]

När en relay-router tar emot ett paket till 2002:c000:0204::/48 extraherar den ut den inkapslade IPv4-adressen ur IPv6-paketet och skickar den över IPv4 till sin destination.

När man vill sända paket från sitt nät ut till IPv6-Internet används anycast-adressen 192.88.99.1. Default Route i noderna för IPv6 konfigureras till 2002:c058:6301::(ditt näts boarder-router med 192.88.99.1 inbakat i 6to4-blocket). IPv6-paket som skall routas ut på IPv6-Internet kapslas in i IPv4-paket adresserade 192.88.99.1 (närmaste relay-router) av din boarder-router. Relay routern packar upp och skickar paketet vidare över IPv6 till den destination paketet är ämnad för.

2.4 Routing i IPv6

De idag vanligaste routingprotokollen för IPv4 är RIP, EIGRP, OSPF, IS-IS och IGRP. Alla dessa har förutom IGRP en motsvarighet i IPv6. Ett viktigt beslut i en Dual Stack-miljö att ta är om man ska köra separata routingprotokollprocesser eller ej i routrarna. Att separera dem innebär att routrarna behöver mer minne och kraftigare CPU för att lagra routinginformationen och kalkylera bästa väg. I gengäld får man högre tillgänglighet då ett problem i IPv4-routingen inte påverkar IPv6-routingen och tvärt om[16]. Det externa routingprotokollet som används idag är BGPv4 och det används också i IPv6. Tabell 2.3 visar en översikt över de olika routingprotokollen och deras motsvarighet i IPv6.[1]

Tabell 2.3: Routingprotokoll som stödjer IPv6

Typ	IPv4-version	IPv6-version
IGP	RIP	RIPv2 (RIPng)
IGP	EIGRP	EIGRP for IPv6
IGP	OSPF	OSPFv3
IGP	IS-IS	IS-IS for IPv6
EGP	BGPv4	BGPv4

Även om routing i IPv4 och i IPv6 har mycket gemensamt så är det några viktiga saker som skiljer det åt. Först och främst är IPv6-Internet betydligt mycket mindre än IPv4-Internet. IPv6-Internet är dessutom uppbyggt mångt och mycket på olika överliggande nätverk på en IPv4-struktur[13]. Enligt data från CIDR Report[24] innehåller den globala routingtabellen över 200 000 IPv4-prefix och endast runt 800 IPv6 prefix[25]. De flesta routrar i den ”default fria”-zonen filtrerar ut prefix som inte är större än /32. Detta är nödvändigt för att hålla den globala routingtabellen i en hanterbar storlek.

2.4.1 OSPFv3

OSPFv2[33] för IPv4 är en väletablerad och ett mycket uppskattat routingprotokoll. För att kunna stödja IPv6 har en tredje version kommit ut; OSPFv3[31]. Mycket av den funktionalitet som finns i OSPFv2, flooding, val av DR, stöd för olika områden, uträkning av SPF återfinns i OSPFv3. Värt att notera är att OSPFv3 inte kan användas för IPv4 vilket gör att man måste köra OSPFv2 för IPv4 och OSPFv3 för IPv6. I pakethuvud i OSPFv3-meddelanden ingår ett 8-bitars fält för ett instans-ID vilket möjliggör flera OSPFv3 instanser per länk. OSPFv3 körs på en per länk basis istället för per IP-subnät som i IPv4. Routinginformation skickas med link local-unicast adressen som källa.

Autentisering har tagits bort från själva protokollet. Istället sker autentisering och kryptering med hjälp av de nya fälten ”IP Authentication Header” och ”IP Encapsulating Security Payload” i IPv6-headern.

Grannroutrar identifieras fortfarande av ett 32-bitars router-ID i OSPFv3.[33]

Multicast-adressen FF02::5 används av routrar för att kontakta och skicka uppdateringar till andra OSPFv3 routrar. Alla OSPF-routrar måste lyssna på denna multicast-adress. Multicast-adressen FF02::6 används för alla ”Designated”. och ”Backup”-routrar.[31]

2.4.2 IS-IS for IPv6 (IS-ISv6)

Det är inte mycket som skiljer IS-ISv4 och IS-ISv6 åt. Det fungerar för användaren ungefär likadant. IS-ISv6 är bara en förändring som gör att IS-IS kan hantera IPv6 utöver IPv4 och OSI.[13] IS-IS används ofta bara i en Internetleverantörs nätverk och sällan i ett företagsnätverk. Om IPv6-topologin är identisk med IPv4-topologin i en Dual Stack-miljö kan IS-ISv6 vara ett bra alternativ i fråga om administration och resursbesparingar.

2.4.3 EIGRP for IPv6

Enhanced Interior Gateway Protocol (EIGRP) är Ciscos egna proprietära protokoll och är uppbyggt på ett modulärt sätt. EIGRP stödjer flera olika routade protokoll genom så kallade Protocol-dependent Modules (PDM). Varje PDM har hand om sitt eget protokoll (IPv4, IPX, AppleTalk) vilket har gjort det väldigt lätt för det att stödja IPv6 genom att bara skapa en ny PDM för IPv6 [5]. Även om EIGRP för IPv4 och IPv6 är väldigt lika är det några saker man bör tänka på om man ska använda EIGRP för IPv6:[1]

- RouterID för EIGRP-processen är fortfarande 32-bitar
- EIGRP lyssnar på multicast-adressen FF02::A
- EIGRP för IPv4 använder MD5-hashning för autentisering vilket också stöds av EIGRP för IPv6. EIGRP för IPv6 använder alltså inte några speciella IPv6-säkerhetsfunktioner
- Det finns ingen Split Horizon för EGIRP för IPv6, flera prefix kan användas på samma port på samma router.

2.4.4 Routing Information Protocol version 2 (RIPv2)

RIP är ett enkelt protokoll tillhörande Distance Vector familjen av routingprotokoll. Det är lätt att förstå och implementera och finns därför i de flesta routrar idag. För att hantera IPv6 har RIP uppdaterats till RIPv2[23] eller RIPng som det också kallas. På grund av sin enkelhet har det också sina begränsningar med skalbarhet och konvergenstid.[1]

- RIP passar inte för större nätverk på grund av att längsta vägen i nätverket endast kan vara 15 hopp (routrar).
- Protokollet använder fasta värden för kostnader av olika vägar vilket inte passar i situationer när realtidsparametrar (belastning, pålitlighet, fördröjningar) spelar stor roll.
- RIP stödjer inte flera protokollinstanser. Det finns ingen sådan information i meddelanden som skickas mellan routrarna. Behöves sådan funktionalitet måste RIP konfigureras på olika UDP-portar eller använda olika multicast adresser (FF02::9 är standard).

De stora skillnaderna mellan RIPv2 (IPv4) och RIPv2 (IPv6) kan sammanfattas i tre punkter:[1]

- I IPv4 måste två routrar tillhöra samma subnät för att kunna utbyta routinginformation. I IPv6 befinner sig alla grannroutrar på samma link local-prefix (FF80/10) och därför har denna restriktion tagits bort. Detta medför att varje router måste annonsera sitt prefix på dessa länkar också.
- Eftersom broadcast inte används i IPv6 skickas alla RIP-meddelanden till link local multicast-adressen FF02::9.
- För att säkra upp kommunikationen mellan två RIPv2-routrar i IPv4 används MD5-hashning[32]. När RIPv2 används med IPv6 används istället ”IP Authentication Header” och ”IP Encapsulating Security Payload” för att säkerställa integriteten och autentiseringen.

När RIP används för både IPv4 och IPv6 sparas all routinginformation i två olika Routing Information Base (RIB), en för IPv4-information och en för IPv6-information[16].

2.4.5 Boarder Gateway Protocol (BGP)

RFC 2858[14] definierar Multiprotocol BGPv4 (MP-BGPv4) som är det External Gateway Protocol (EGP) som används i IPv6. RFC 2545[15] specificerar hur just IPv6 är implementerat och utformat för MP-BGPv4. MP-BGPv4 har stöd för samma funktioner som IPv4-versionen. Förändringar från IPv4 inkluderar stöd för IPv6-adresser, Network Layer Reachability Information (NLRI) och Next Hop-attribut som använder IPv6-adresser. För att BGP skall kunna hantera IPv6 måste en router förhandla med alla sina grannar om vad den kan och grannen kan. Båda routrarna måste kunna hantera IPv6 för att de ska kunna utbyta IPv6-information.

Stöd för att utbyta multicast-information mellan olika IPv6-nätverk har även lagts till i MP-BGPv4. Multicast-informationen måste utbytas mellan olika Internetleverantörer för att multicast ska fungera över gränserna mellan olika nätverk. Konfigurerar man bara MP-BGPv4 för unicast kommer multicast-information inte att utbytas utan det måste konfigureras. Subsequent Address Family Identifier (SAFI) används i MP-BGPv4 för att skilja på olika typer av NLRI, unicast använder SAFI 1-meddelande och multicast använder SAFI 2-meddelande. SAFI-1 innebär i praktiken att vägar endast går att använda för unicast och inte multicast.

För att hålla ner storleken på den globala routingtabellen måste BGP-routrar filtrera utannonserade vägar från grannroutrar. Adressrymden i IPv6 är så stor att hårda regler för filtrering måste finnas för att den globala routingtabellen ska hållas i en hanterbar storlek. BGP-routrar får enbart annonsera /32-prefix till andra BGP-routrar. Det innebär att Internetleverantörer måste aggregera alla sina kunders nätverksprefix till ett prefix och endast annonsera det med andra Internetleverantörer.

En BGP-router som har hand om både IPv6 och IPv4 bör utbyta information över respektive protokoll. Även om det är möjligt att utbyta information för både protokollen över en TCP-session är det vanligast att man separerar dem[16]. AS-nummer (Autonomous System) som används i IPv4 används också i IPv6. En administratör använder alltså samma AS-nummer för att identifiera sitt IPv4-nätverk som sitt IPv6-nätverk.[1]

2.4.6 Transport av routingprotokolldata

Routingprotokolldata för IPv4 skall transporteras över IPv4 precis som routingprotokolldata för IPv6 skall transporteras över IPv6[18]. Detta på grund av tre anledningar:

- IPv6 kan fortfarande fungera även om IPv4 inte fungerar (eller vice versa)
- Bästa vägen i ett IPv4 nätverk är inte alltid den bästa för IPv6
- Den logiska topologin för IPv4 och IPv6 kan se olika ut, olika "metrics" kan användas för olika länkar beroende på om IPv4 eller IPv6 används

2.5 Mjukvara

Mjukvaran är oerhört viktig när man ska inför IPv6. För att en router ska kunna hantera IPv6 måste den ha mjukvara som klarar av IPv6. Detta gäller mer än bara routrar, mjukvara i switchar, skrivare, persondatorer, mobiltelefoner, handdatorer, servrar, brandväggar och så vidare. måste alla klara av IPv6. Det är därför viktigt att kontrollera och kolla upp om all utrustning i nätverket som skall hantera IPv6 kan göra så. I värsta fall, om mjukvaran inte kan uppdateras, är ett utbyte av hårdvaran en sista utväg.

2.5.1 Operativsystem

En av de viktigaste komponenterna för att IPv6 skall fungera är ett operativsystem som har en IPv6-stack implementerad. Detta ligger till grund för att applikationer som kör på operativsystem skall kunna klara av IPv6. Det är inte bara operativsystem i persondatorer som måste klara IPv6 utan även operativsystem i routrar, switchar, brandväggar osv.

Stöd för IPv6 har funnits väldigt länge i vissa operativsystem men man ska komma ihåg att IPv6-stackarna som används idag fortfarande är väldigt unga i relation till de IPv4-stackar som finns. IPv4-stackarna har utvecklats och fått buggfixar i över 20 år. Risken för att det finns exploaterbara svagheter i IPv6-stackarna är stor. Detta är ett problem som löser sig själv med tiden då IPv6 används mer och mer och därför utsätts för testning. Tabell 2.4 sammanställer operativsystem som har en IPv6-stack implementerad[1].

Tabell 2.4: Opertaivsystem som har stöd för IPv6

Familj	**Operativsystem**
Apple	Mac OS X 10.2 eller senarare
BSD	FreeBSD 4.0 eller senare
	OpenBSD 2.7 eller senare
	NetBSD 1.5 eller senare
Cisco	IOS 12.2 eller senare
HP	HP-UX 11i eller senare
	Tru64 UNIX v5.1 eller senare
	OpenVMS v5.1 eller senare
IBM	AIX 4.3 eller senare
	OS/390 V2R6 eNCS
	z/OS Release 1.4 eller senare
Juniper	JunOS 5.1 eller senare
Linux	Red Hat 6.2 eller senare
	Mandrake 8.0 eller senare
	SuSE 7.1 eller senare
	Debian 2.2 eller senare
	Fedora Core 1 eller senare
Microsoft	Windows XP SP1 eller senare
	Windows Server 2003
	Windows CE (Pocket PC 4.1)
	Windows Vista
Novell	Netware 6.1 eller senare
Sun	Solaris 8 eller senare
Symbian	Symbian 7.0 eller senare

2.5.2 Applikationer

När man har kontrollerat om sitt operativsystem klarar av IPv6 gäller det att identifiera alla applikationer som används och kontrollera att de klarar av IPv6. Viktiga hörnstenar i sitt nätverk så som DNS-, Mail-, Web-servrar måste fungera och man bör därför kolla upp på respektive tillverkares hemsida om mjukvaran klarar av IPv6. Det gäller även att identifiera annan mjukvara som används till exempel Instant Message (IM), Office Paket, Webbläsare etc.

Brandväggar är en naturlig del av ett modernt nätverk. Tyvärr är stödet för att filtrera IPv6 i brandväggar väldigt begränsat. Många stora tillverkare har bara exprimentiellt stöd för det. En bra brandvägg skall klara av att filtrera både IPv4-trafik och IPv6-trafik på samma gång och på samma nätverksportar. Något som inte många tänker på idag är att även om man inte kör IPv6 bör brandväggen kunna hantera det för att filtrera bort IPv6-trafiken. Annars kan användare bakom brandväggen tunnla IPv6-trafik över brandväggen.

2.5.3 Övervakning och administration

Stora nät måste övervakas och därför är det säkert att anta att övervakning av IPv6 är smidigast om det kan integreras i samma system som idag används för att övervaka IPv4. Om övervakningsdata (Simple Network Management Protocol (SNMP), Netflow) inte kan skickas direkt över IPv6 kan den skickas över IPv4 istället. Används SNMP krävs det att övervakningsobjektet har stöd för Management Informations Base (MIB) som klarar av IPv6. För att få ut överskådlig information ur MIB:ar använder man så kallade Management program. Dessa program måste också ha stöd för IPv6. Programmet måste ha stöd för att skicka och ta emot övervakningsdata och kommando över IPv6 men även kunna bearbeta och presentera informationen ur IPv6-MIB:ar.[1]

Att underhålla och övervaka ett IPv6-nätverk skiljer sig inte så mycket från att göra det på ett IPv4-nätverk. Verktygen som finns tillgängliga idag har olika mycket stöd för IPv6. En kombination av dessa verktyg, egenutvecklade program och script kan vara nödvändigt för att övervaka och få ut all den information man vill åt. Allt beror på vilken information som skall övervakas.

2.6 Säkerhet

Säkerhet i IPv4 och IPv6 är inte två helt skilda världar även om förespråkare av IPv6 använder säkerhet som ett argument för att införa IPv6. Till exempel är det ett krav på IPSec hos alla IPv6-noder vid nod-till-nod kommunikation enligt RFC 2401[29]. I verkligheten är det inte så, inte i dagens IPv6-nätverk. När IPv6 är mer dominant och mer program utnyttjar IPv6 kommer det kanske bli så. När man inför mer kryptering är det viktigt att hålla rätt tid i alla system, Network Time Protocol (NTP) är en bra lösning. Brandväggar måste uppdateras för att kunna hantera och filtrera IPv6-trafik.

Nya typer av attacker, specifika för IPv6, kommer att upptäckas. Det kan till exempel tänkas att en attackerare gör attacken mot en Dual Stack nod över IPv4 för att sedan byta till IPv6 för att på så sätt göra det svårare att upptäcka.

2.6.1 Skanning av IP-adresser

I IPv4 är det ganska lätt att skanna av ett subnät med ett portskanningsverktyg som till exempel Nmap[7]. Problem uppstår för attackeraren i IPv6 då antalet möjliga IP-adresser är för många vilket gör det till en mycket tidskrävande uppgift. Att hindra denna typ av attack proaktivt är väldigt svårt då tekniken utnyttjar helt legala metoder som måste tillåtas i ett nätverk. Det som kan göras är att säkra noderna så bra som möjligt med brandväggar, antivirusprogram och uppdaterade program.[38] Samma sätt som i IPv4.

2.6.2 Otillåten tillgång

Otillåten tillgång är nästa steg för en attackerare efter att ha identifierat en lämplig nod. Attackeraren försöker logga in eller utnyttja en svaghet i något program som körs på noden.
Denna typ av attacker är svår att skydda sig mot och det spelar ingen roll om man använder IPv4 eller IPv6. Samma säkerhetspolicy som används i IPv4 bör appliceras i IPv6. Samma generella åtgärder som i föregående avsnitt bör vidtas ute hos noderna, brandväggar, antivirusprogram och uppdaterade program.

2.6.3 Paketmanipulation och fragmentering

IPv4-stackarna som används idag är väl beprövade med en 20 år lång bakgrund. Pakethuvuden i IPv6 har ändrats från IPv4 vilket kan medföra nya risker. Dåligt implementerade IPv6-stackar kan vara möjliga mål för en attack. Till exempel upptäcktes en bugg i operativsystem OpenBSD som via ICMPv6 kunde få systemet att krascha[8].

Fragmentering kan innebära risker till exempel genom att fragmentera paketen försöka gömma attacken från IDS:er. IDS måste hela tiden defragmentera paketen för att kunna inspektera vad som finns i dem. Om attackeraren fragmenterar och skapar otillåtna fragmenteringar kan det försvåra IDS:ens arbete.

Den minsta tillåtna storleken på Maximum Transfer Unit (MTU) i IPv6 är 1280 oktetter vilket gör att alla fragmenterade paket som är mindre än 1280 oktetter och inte är det sista paketet i ett fragmenterat flöde kan stoppas och droppas i brandväggar/filter[39]. Fragmentering bör undvikas/regleras i så stor grad som möjligt för att skydda sig.[6]

Nätverksadministratörer har få eller dåliga alternativ för att skydda nätverket och sina användare. Det är svårt att veta vilka IPv6-stackar som körs ute hos kunderna och i all nätverksutrustning.

2.6.4 Spoofing på lager 3 och på lager 4

För att försvåra arbetet med att spåra en attack tillbaka till attackeraren används spoofing. Spoofing innebär att den som sänder ett IP-paket (lager 3) sätter fel eller förfalskad avsändar IP-adress på paketen för att det inte ska gå att se vem som skickade det. Detta är väldigt vanlig i IPv4 och kan tillämpas på samma sätt i IPv6. Spoofing på lager 4 är fortfarande möjligt eftersom det inte är beroende på vilket lager 3 protokoll som används. Samma skydd som idag används för att skydda sig mot lager 4 spoofing går att använda även om IPv6 används.

RFC 2827[50] har rekommenderingar på om hur filtrering skall genomföras för att begränsa faran och riskerna med spoofing-attacker. Dessutom skall endast de adressblock som IANA har allokerat för publikt användande tillåtas routas[40]. Användadet av IPSec mellan IPv6-noder är ett effektivtsätt att hindra spoofing både när det gäller direkt kommunikation och vid tunnlade förbindelser.

2.6.5 ARP- och DHCP-attacker

I IPv4 används Adress Resolution Protocol (ARP) för att översätta lager 3-adresser till lager 2-adresser. ARP Spoofing är en teknik för att kunna avlyssna data trafik i ett Ethernet-nätverk[38]. ARP har i IPv6 ersatts av Neighbor Discovery (ND) men led från början av liknande svagheter som ARP[41]. RFC 3971 togs fram för att möta attacker och hot mot ND. RFC 3971 definierar SEcure Neighbor Discovery (SEND) som erbjuder en rad skydd:

- En mekanism för att certifiera routrar innan de används som ”default gateway”.
- Signaturbaserad kryptografi för att skydda att ND-meddelanden.
- Tidsstämplar och NONCE (random number used only once) för att förhindra ”replay attacks”[9].
- Kryptografiskt framtagna adresser för att verifiera ansändaradressen i ND-meddelanden.

DHCP-attacker går oftast ut på att ge klienten felaktig information om DNS-servrar eller ”default gateway”. DHCPv6 fungerar väldigt likt DHCPv4 och lider därför av samma svagheter. Attacken måste ske lokalt (sitta på samma länk) så den är inte så vanlig och inte så allvarlig. Det finns egentligen inget sätt att skydda noder idag om man inte använder statiskt utdelning av adresser till noder, speciellt de mest kritiska.[6]

2.6.6 Broadcast-förstärknings attacker

Broadcast-förstärknings attacker (Broadcast amplification attacks) eller smurf-attacker som den också kallas är en typ av Denial of Service (DoS) som utnyttjar möjligheten att skicka ett echo-request ICMP-meddelande till en broadcast-adress för ett subnät med offrets IP-adress som avsändare (spoofad). Alla noder på detta subnät kommer svara med ett echo-reply till offrets dator och på så sätt utsätta den för en DoS-attack.

I RFC 2463[24] står det att ett ICMPv6 meddelande inte skall genereras som ett svar på ett ICMPv6 meddelande som har källadressen som är en IPv6 multicast-adress, länklager multicast-adress eller en länklager broadcast adress. Om en nods IPv6-stack följer dessa specifikationer är inte smurf-attacker och andra förstärkningsattacker i IPv4 ett problem för IPv6.[6]

2.6.7 Routingattacker

Routing är en central och mycket viktigt del i ett större nätverk. Störningar mot routingen är allvarligt men dessvärre inte så svårt att skapa. Routingprocesser kan uppta alla resurser i en router genom flooding-attacker eller genom simulerade statusförändringar som route flapping[5]. Attacker kan också ha målet att föra in en attackerares länkar i nätet och korrumpera routinginformationen. Alla attacker är samma för IPv4 och IPv6.

För att skydda sig skall man åtminstone använda de inbyggda mekanismer i routingprotokollet som finns. BGP har stöd för att använda IPSec över sina TCP-anslutningar[42]. De flesta IGP-protokollen har nån typ av mekanism för att autentisiera sig mot andra routrar via MD5 eller liknande hash-funktioner.

2.6.8 Övergångs-, översättnings och tunnelmekanismer

Tunnlar och andra tekniker som underlättar övergången från IPv4 till IPv6 är väldigt bra hjälpmedel men tyvärr kan de innebära nya hot och risker. Övergångsmekanismer kan göra nätverket sårbart både över IPv6 och över IPv4. Tunnlar kräver att nya portar öppnas i brandväggar. Det är därför viktigt att vara konsekvent och köra samma säkerhet och policy för båda protokollen. Det är viktigt att nätverksadministratören tar hänsyn till tunnelmekanismer och den trafik som flödar i tunneln när säkerhetspolicyn skapas. Annars riskeras otillåten trafik trafikeras i tunneln. Kryptering av IPv4-trafiken där IPv6 tunnlas är ett bra skydd för tunneln och integriteten för trafiken i tunneln.

Generellt bör man använda Dual Stack som övergångsteknik istället för översättningstekniker (NAT) mellan IPv4 och IPv6 för att minska komplexiteten. Används tunnlar bör statiska tunnlar användas framför dynamiska tunnlar. Då har administratören en möjlighet att implementera IPSec mellan tunnelpunkterna för att skydda trafiken. Brandväggar kan även konfigureras så att endast kända tunnelpunkter får tunnla sin trafik ut ur nätverket.

2.6.9 Brandväggar och filtrering

ICMPv6 har fått en mer betydande roll i IPv6 än vad ICMPv4 har i IPv4. ICMPv4-trafik filtreras restriktivt i IPv4. ICMPv6 måste implementeras i en IPv6-stack och dess trafik måste få trafikera nätet för att IPv6 skall fungera[10]. ICMPv6 kan filtreras, tabell 2.5 visar vilka ICMPv6 meddelande som bör få trafikera IPv6-brandväggar[6].

Tabell 2.5: ICMPv6-meddelanden som ska trafikera brandväggen

ICMPv6-typ	Namn
Type 1	No route to destination (Code 0)
Type 2	Packet too big for PMTU Discovery
Type 3	Time Exceeded
Type 4	Parameter problem
Type 128	Echo request
Type 129	Echo request and echo reply
Type 133	Router solicitation
Type 134	Router Advertisement
Type 135	Neighbor solicitation
Type 136	Neighbor advertisement

Type 2 – Packet too big behövs för att Path Maximum Transfer Unit Discovery (PMTU) skall fungera. Att tillåta Type 2 är kritisk för att IPv6 skall fungera då noder inte får fragmentera IPv6-paket. Type 133 och Type 134 måste tillåtas för att autoconfiguration skall fungera korrekt. Type 135 och 136 behövs för att Duplicate Address Detection och MAC-to-IPv6 överstättning skall kunna genomföras. Utöver detta skall samma policy för filtrering av ICMPv4 tillämpas på ICMPv6. För att tunnlar skall kunna trafikera en brandvägg krävs att IP-protkoll typ 41 tillåts i brandväggen [11].

Filterfunktioner finns ofta inbyggt i routrar i form av Access-listror (ACL). ACL:er är ett enkelt sätt att filtrera trafik och kan filtrera trafiik på lager 3 och 4. De kan filtrera trafik på in- och utgående nätverksgränssnitt i en router. Existerande ACL:er skrivna för lager 3 (IPv4) måste skrivas om för att matcha IPv6-adresser. ACL:er skrivna för lager 4 (TCP, UDP) behöver inte skrivas om, om de inte innehåller IPv4-adresser.

2.6.10 Spårbarhet (Traceabillity)

De flesta Internetleverantörer har någon sorts mekanism för att spåra härkomsten av trafik. Detta är också att eftersträva i IPv6. Specifika IPv6-adresser och prefix måste kunna spåras tillbaka till tillhörande kund. Det gäller även tunnlade förbindelser.

Det kan göras genom att till exempel mappa DHCP-begäran till fysiska anslutningar och spara resultatet i en databas. Det kan också göras genom att tilldela kunder fasta adresser eller prefix. När det gäller tunnlar bör tunnel-servern kunna tillhandahålla spårbarhetsfunktioner.[16]

2.6.11 Network Time Protocol (NTP)

För att höja säkerheten och integriteten på trafik som trafikerar ett IPv6-nätverk kan kryptering användas på ett eller annat sätt. Kryptering är ofta väldigt beroende av tid och tidstämplar. Det är därför viktigt att tiden på noder går rätt och man bör därför använda NTP[30] för att synkronisera klockorna i datorer, switchar, routrar etc. Att nätverkselement (routrar, switchar) har rätt tid och framför allt samma tid är viktigt för att kunna analysera och korrelera loggar från olika källor.

3 Genomförande

För att besvara problemställningen och genomföra fallstudien har en stor del av arbetet ägnats åt den teoretiska bakgrunden. Arbetet inleddes därför med att skriva den teoretiska bakgrunden genom att leta upp fakta och Request For Comments (RFC) som handlar om IPv6-specifikationen och olika övergångstekniker. Litteraturen består till stor del av RFC:er. Antalet böcker som är skrivna om IPv6 och övergången är relativt få. Högskolebiblioteket ställde upp genom att köpa in litteratur från England då de saknade böcker inom området.

Fallstudien skulle göras på en Internetleverantör som erbjuder IP-baserade tjänster. Utöver detta kriterium skulle Internetleverantören enbart använda IPv4 idag. Valet av Internetleverantör föll på det lokala företaget Junet AB som levererar IP-konnektivitet till privatpersoner, företag och fastighetsägare i Jönköping.

Kontakt med Junet AB togs och de var villiga att hjälpa mig i studien. Fallstudien planerades att genomföras efter att en teoretisk bakgrund hade skrivits.

Utifrån den teoretiska bakgrunden och den litteratur jag använt mig av har jag tagit fram de delar och frågor som är viktiga när Junet AB undersöker införandet av IPv6. Eftersom Junet AB är en liten och enkelt uppbyggd Internetleverantör blir frågorna relativt få och enkla. Fallstudien genomfördes med samtal med Junet AB och ställda frågor återfinns i Bilaga A.

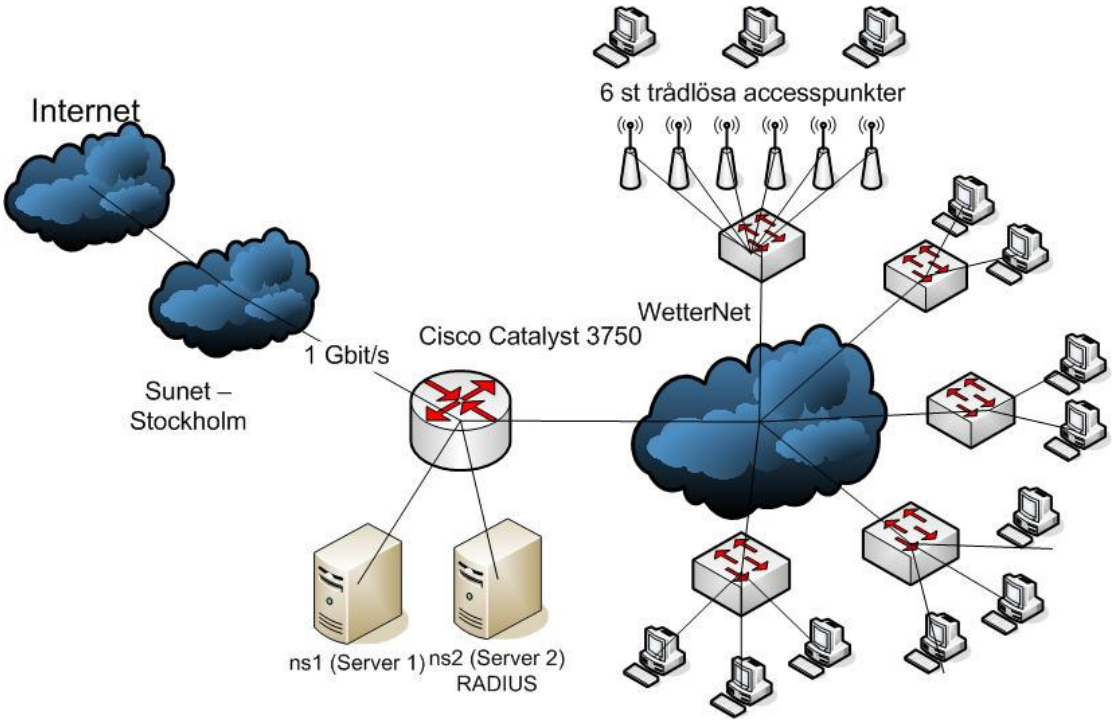
3.1 Junet AB:s nätverk i nuläget

Junet AB levererar Internet till studenter och har idag en IPv4-adressallokering från Sunet. Varje slutkund blir tilldelad en IPv4-adress var och är statiskt satt, ingen DHCP används. Nätets centrala del består av en Cisco Catalyst 3750 lager 3 switch som binder ihop hela nätverket och har en länk till Sunet. Den fungerar både som switch och router. Sunet är deras uppströms Internetleverantör och levererar en förbindelse till Sunets nätverk och Internet. En statisk route används istället för ett routingprotokoll. Kunderna ansluts över stadsnätet WetterNet över lager 2 som sedan kopplas samman i Cisco Catalyst 3750-switchen. I en del av nätet sitter sex stycken Cisco Aironet access-punkter för att ansluta ett mindre antal kunder trådlöst. Se Figur 3-1 för en överblick över nätverkets design.

Till Cisco Catalyst 3750-switchen är två servrar kopplade, en server som agerar primär DNS-server (ns1) och en som agerar sekundär DNS-server och RADIUS-server (ns2) som används för att autentisiera de trådlösa kunderna. Servrarna bygger på FreeBSD 5-serien och använder BIND 9.3.1 och FreeRADIUS. Dessa två servrar är de enda servrar som används för att leverera Internetanslutningar till kunderna. Företagets e-posttjänst och hemsida köps in som en utomstående tjänst och drivs av ett annat företag.

Brandväggsfunktionalitet erhålls genom access listor (ACL) i den centrala switchen. Filtreringen sker på lager 4 och på fasta IPv4-adrsser.

För att övervaka den dagliga driften används en dator som använder Fedora Core 6. Denna dator kör programmet Cacti för att visa grafer över utnyttjande av nätresurser. Intellipool Network Monitor används för övervakning av servrar och nätverkelement ute i nätverket på en Windows XP-maskin ståendes på kontoret.



Figur 3-1: Junet AB:s nuvarande IPv4-nätverk.

4 Resultat

Första steget för Junet AB att införa IPv6 är att ansöka om en adressallokering från Sunet. De skulle kunna ansöka direkt från RIPE NCC, men eftersom Sunet tillhandahåller deras IPv4-adresser och är deras uppströms Internetleverantör är det till Sunet de ska vända sig. Junet AB bör få en adressallokering i storleksordningen /32. Detta möjliggör en utdelning av /48 eller /64 till varje kund vilket följer de rekommendationer som RIPE har satt upp.

Kunderna består till största del av studenter som anses ha en eller ett fåtal datorer och därför är det lämpligt att ge varje kund ett /64. Är kunden i behov av att subnäta ute hos sig kan de erbjudas ett /48. Ett /48 kan avsättas för internt bruk för att adressera servrar, switchen och övervakningsstationen plus eventuellt annan utrustning som används för att driva nätet. För att adressera kundernas anslutningar kan man fortsätta med samma teknik som innan, fast tilldelning. Kunderna får du varsitt /64 och med hjälp av det kan de adressera alla sina tänkbara noder. Det finns inget behov för att införa DHCP när Junet AB inför IPv6. Kundstocken är administrativt hanterbar och införandet av DHCP skulle bara göra miljön onödigt komplicerad.

Ingen uppgradering av switchen behövs då den är modern och klarar av IPv6. Den ska konfigureras för att vara Dual Stack och hantera både IPv4 och IPv6 samtidigt. Innan detta kan göra måste man kontrollera att operativsystemet i den klarar av det. Det görs lämpligast via Ciscos hemsida. Skulle det visa sig att den kör en äldre version av operativsystemet kan den uppdateras från Cisco. Eftersom nätverket är enkelt uppbyggt och inga routingprotokoll används i IPv4 behövs det inte användas något routingprotokoll i IPv6 heller. En statisk route som används i IPv4 fungerar i IPv6 också. Samma länk till Sunet som används för IPv4-trafik kan användas för IPv6-trafik parallellt.

FreeRADIUS används för att autentisiera de trådlösa kunderna. Nuvarande version kan bara autentisiera kunder över IPv4. Nästa version av FreeRADIUS kommer ha stöd för att autentisiera klienter över IPv6. Eftersom nätverket kommer vara Dual Stack över överskådlig framtid gör det inget att kunderna autentisierar sig över IPv4 då det inte spelar någon roll om det sker över IPv4 eller IPv6.

ACL:erna som används i switchen för att filtrera IPv4-trafiken idag i nätverket behöver uppdateras och skrivas nya för att klara av IPv6. Det är ingen större åtgärd då mycket av filtreringen baseras på lager 4-protokoll och således inte påverkas mycket av ändringen av underliggande protokoll. ACL:erna måste uppdateras för att filtrera ICMPv6 korrekt.

Övervakningsstationens operativsystem, Fedora Core 6, ska klara av IPv6. Om de vill byta ut operativsystemet har de många möjligheter att välja, både på Unix- och Windowssidan. Programmet Cacti ska också klara av IPv6. Cacti kan rita grafer över nätverksanvändadet men inte skilja på IPv4-trafik och IPv6-trafik i dagsläget. Det kan alltså användas för att rita grafer över det totala utnyttjandet men inte per protokoll.

Programmet Intellipool Network Monitor som används för att övervaka nätverket stöder inte IPv6 i dagsläget enligt tillverkaren. De har heller ingen agenda för att göra så. Men eftersom nätverket kommer vara Dual Stack kan nätet övervakas över IPv4 tills tillverkaren börja utveckla stöd för IPv6. Switchen har stöd för IPv6-MIB:ar och kan samla in statistik från sina nätverksportar. I detta fall är det programvaran Intellipool Network Monitor som sätter gränserna för vilken information som kan bearbetas.

I och med införandet av IPv6 rekommenderas att de sätter upp och konfigurerar en NTP-server som kunder, switchen och servrar kan använda för att garantera att tiden går rätt. Detta är viktigt för eventuell kryptering och för att öka spårbarheten. NTP-servern bör kunna nås över både IPv4 och IPv6. Det behövs inte en enskild server för detta då det är en enkel uppgift. NTP-servern kan implementeras på DNS-server 2 till exempel.

Junet AB kan testa att sätta upp tunnlar för några kunder för att testa och utvärdera IPv6 mer praktiskt innan de rullar ut IPv6 i hela nätverket. Konfigurerade tunnlar är lämpliga för att testa på ett fåtal kunder då de ger full kontroll på hur de används. Tunnlar ger bra erfarenhet och kunskap om hur det är att drifa och konfigurera ett IPv6-nätverk.

De här åtgärderna som har beskrivits här är bara till för att ge Junet AB grundläggande IPv6-funktionalitet i deras nätverk. Avancerade tjänster som till exempel multicast och QoS kan senare införas då IPv6 har använts och har utvärderats.

5 Slutsats och diskussion

Det förefaller vara en stor och omfattande process för att införa IPv6 i en Internetleverantörs redan befintligt IPv4-nätverk. Det är många delar och bitar som ska falla på plats för ett lyckat införande. Mycket har ändrats i varje del, routingprotokoll har kvar samma funktioner men löser problem på olika sätt, införandet blottar nätverket för nya hot och risker, mjukvaran som används måste ha stöd för det. Vet man bara om skillnaderna och ändringarna har man en större chans att lyckas.

I fallet med Internetleverantören Junet AB vill jag påstå att det är fullt möjligt med ett införande utan större svårigheter. Deras IPv4-nätverk är enkelt uppbyggt innehåller endast en router/switch som behöver konfigureras om. De har modern utrustning som klarar av eller kan uppdateras för att klara av IPv6. Kundstocken är liten och består av studenter som måste anses som teknikfantaster och är antagligen mer intresserade av IPv6 än vad vanliga privatpersoner är. Ett införande av IPv6 hos Junet AB skulle medföra att studenterna, som är uppkopplade via Junet AB, i Jönköping får tillgång till det senaste inom Internetkommunikation.

En sak som talar emot en smidig allmän övergång är den dokumentation som finns. Få böcker finns skrivna inom området och det är få människor som har erfarenhet av att driva stora IPv6-nätverk. När fler och fler Internetleverantörer inför IPv6 kommer bristen på erfarna människor att fyllas. Det gäller bara att få de människor med erfarenhet att hjälpa andra och dela med sig av sina erfarenheter.

Idag är det nog viktigare att fråga varför man ska införa IPv6 istället för om det går att införa. Protokollet i sig är inte en nyhet, det har funnits länge och det har kommit till en nivå där det är fullt möjligt att använda det i stora nätverk som hos en Internetleverantör. Alla delar som behövs för att använda IPv6 i stora nätverk finns. IPv6 och IPv4 kommer att samexistera tillsammans under en lång tid framöver.

6 Referenser

[1] Popoviciu, Ciprian; Levy-Abegnoil, Eric; Grossetete, Patrick (2006) *Deploying IPv6 Networks*.
Cisco Press, Indianapolis, ISBN 15-87-05210-5.

[2] Guidelines for 64-bit global identifier (EUI-64)
http://standards.ieee.org/regauth/oui/tutorials/EUI64.html (2007-04-11)

[3] RIPE NCC (2007) http://www.ripe.net/ripe/docs/ipv6policy.html (2007-04-11)

[4] Address Supporting Organization http://www.aso.icann.org/rirs/ (2007-04-12)

[5] Cisco System (2004), *CCNA 3 and 4 Companion Guide Third Edition*
Cisco Press, Indianapolis, ISBN 15-87-13113-7

[6] Sean Convery; Darrin Miller (2004) *IPv6 and IPv4 Threat Comparison and Best Practice Evaluation*
White Paper, Cisco

[7] Nmap (2007) http://www.insecure.org/nmap/ (2007-04-17)

[8] Core Security (2007)
http://www.coresecurity.com/?action=item&id=1703 (2007-04-17)

[9] Microsoft MSDN (2007) http://msdn2.microsoft.com/en-us/library/aa738652.aspx (2007-05-03)

[10] A Conta; S Deering, (1998), *Internet Control Message Protocol (ICMPv6) for the Internet Protocol 6 (IPv6) Specification - RFC 2463*
IETF - http://www.ietf.org/rfc/rfc2463.txt

[11] Carpenter, Brian; Moore, Keith (2001) *Connection of IPv6 Domains via IPv4 Cloud -, RFC 3056*
IETF - http://www.ietf.org/rfc/rfc3056.txt

[12] Juniper Networks, Inc. (2005) *Juniper Networks Enables a Secure and Assured Transition to Internet Protocol Version 6 (IPv6) in the Federal Government.*
Juniper Networks, Inc.

[13] Dunmore, Martin (2005), *6net - An IPv6 Deployment Guide*
6net – http://www.6net.org

[14] Bates, Tony; Chandra, Ravi; Katz, Dave; Rekhter, Yakov (2000), *Multiprotocol Extensions for BGP-4 – RFC 2858*
IETF - http://www.ietf.org/rfc/rfc2858.txt

[15] Marques, Pedro R; Dupont, Francis (1999) *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing – RFC 2545*
IETF - http://www.ietf.org/rfc/rfc2545.txt

[16] M. Lind; V. Ksinant; S. Park; A. Baudot; P. Savola (2005) *Scenarios and Analysis for Introducing IPv6 into ISP Networks – RFC 4029*
IETF - http://www.rfc-archive.org/getrfc.php?rfc=4029

[17] Gilligan, Robert E; Nordmark, Erik (2000) *Transition Mechanisms for IPv6 Hosts and Routers – RFC 2893*
IETF - http://www.ietf.org/rfc/rfc2893.txt

[18] Hinden, Robert M; Deering, Stephen E (2006) *IP Version 6 Addressing Architecture – RFC 4291*
IETF - http://www.ietf.org/rfc/rfc4291.txt

[19] Conta, Alex; Deering, Stephen (1998) *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification – RFC 2463*
IETF - http://www.ietf.org/rfc/rfc2463.txt

[20] Droms, Ralph (1997) *Dynamic Host Configuration Protocol – RFC 2131*
IETF - http://www.ietf.org/rfc/rfc2131.txt

[21] Thomson, Susan; Narten, Thomas (1998) *IPv6 Stateless Address Autoconfiguration – RFC 2462*
IETF - http://www.ietf.org/rfc/rfc2462.txt

[22] Savola, Pekka (2003) *Use of /127 Prefix Length Between Routers Considered Harmful - RFC 3627*
IETF - http://www.ietf.org/rfc/rfc3627.txt

[23] Malkin, Gary Scott (1998) *RIP Version 2 – RFC 2453*
IETF - http://www.ietf.org/rfc/rfc2453.txt

[24] CIDR Report (2007) http://www.cidr-report.org/ (2007-04-18)

[25] BGP Analysis Reports (2007) http://bgp.potaroo.net/index-bgp.html (2007-04-18)

[26] Thomson, Susan; Huitema, Christian; Ksinant, Vladimir; Souissi, Mohsen (2003) *DNS Extensions to Support IP Version 6 – RFC 3596*
IETF - http://www.ietf.org/rfc/rfc3596.txt

[27] Root Server Technical Operations Assn. (2007) http://www.root-servers.org/ (2007-04-17)

[28] Bush, Randy (2001) *Delegation of IP6.ARPA – RFC 3152*
IETF - http://www.ietf.org/rfc/rfc3152.txt

[29] Kent, Stephen; Atkinson, Randall (1998) *Security Architecture for the Internet Protocol – RFC 2401*
IETF - http://www.ietf.org/rfc/rfc2401.txt

[30] Mills, David L. (1992) *Network Time Protocol (Version 3) Specification, Implementation and Analysis – RFC 1305*
IETF - http://www.ietf.org/rfc/rfc1305.txt

[31] Coltun, Rob; Ferguson, Dennis; Moy, John (1999) *OSPF for IPv6 – RFC 2740*
IETF - http://www.ietf.org/rfc/rfc2740.txt

[32] Baker, Fred; Atkinson, Randall (1997) *RIP-2 MD5 Authentication – RFC 2082*
IETF - http://www.ietf.org/rfc/rfc2082.txt

[33] Moy, John (1998) OSPF Version 2 – RFC 2328
IETF - http://www.ietf.org/rfc/rfc2328.txt

[34] Gallaher, Michael P; Rowe, Rowe R (2006) *The Costs and Benefits of Transferring Technology Infrastructure Underlying Complex Standards: The Case of IPv6*
Journal of Technology Transfer, 31, 519-544

[35] Internet Architecture Board (2001) *IAB/IESG Recommendations on IPv6 Address Allocations to Sites - RFC 3177*
IETF - http://www.ietf.org/rfc/rfc3177.txt

[36] Bound, Jim; Volz, Bernie; Lemon, Ted; Perkins, Charles E; Carney, Mike (2003) *Dynamic Host Configuration Protocol for IPv6 (DHCPv6) – RFC 3315*
IETF - http://www.ietf.org/rfc/rfc3315.txt

[37] Mockapetris, P (1987) *Domain Names – Implementation and Specification – RFC 1035*
IETF - http://www.ietf.org/rfc/rfc1035.txt

[38] McClure, Stuart; Scambray, Joel; Kurtz, George (2002) *Hacking i fokus*. ScandBook, Falun, ISBN 91-63-60707-7.

[39] Deering, Stephen E; Hinden, Robert M. (1998) *Internet Protocol, Version 6 (IPv6) Specification – RFC 2460*
IETF - http://www.ietf.org/rfc/rfc2460.txt

[40] Internet Assigned Numbers Authority
http://www.iana.org/assignments/ipv6-unicast-address-assignments (2007-04-17)

[41] Narten, Thomas; Nordmark, Erik; Simpson, William Allen (1998) *Neighbor Discovery for IP Version 6 (IPv6) – RFC 2461*
IETF - http://www.ietf.org/rfc/rfc2461.txt

[42] OpenBSD 4.0 Manual Page (2007) http://www.openbsd.org/cgi-bin/man.cgi?query=bgpd.conf (2007-04-18)

[43] Rekhter, Yakov; Moskowitz, Robert G.; Karrenberg, Daniel; de Groot, Geert Jan; Lear, Eliot (1996) *Address Allocation for Private Internets – RFC 1918*
IETF - http://www.ietf.org/rfc/rfc1918.txt

[44] Rajahalme, Jarno; Conta, Alex; Carpenter, Brian E.; Deering, Steve 2004) *IPv6 Flow Label Specification – RFC 3697*
IETF - http://www.ietf.org/rfc/rfc3697.txt

[46] Narten, Thomas; Draves, Richard (2001) *Privacy Extensions for Stateless Address Autoconfiguration in IPv6 – RFC 3041*
IETF - http://www.ietf.org/rfc/rfc3041.txt

[47] Aura, Tuomas (2005) *Cryptographically Generated Addresses (CGA) – RFC 3972*
IETF - http://www.ietf.org/rfc/rfc3972.txt

[48] Haberman, Brian; Thaler, Dave (2002) *Unicast-Prefix-based IPv6 Multicast Addresses – RFC 3306*
IETF - http://www.ietf.org/rfc/rfc3306.txt

[49] NITA.org: *Technical and Economic Assessment of Internet Protocol Version 6 (IPv6) (2007)*
http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/draft/draftglossary.htm (2007-04-18)

[50] Ferguson, Paul; Senie, Daniel (2000) *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing – RFC 2827*
IETF - http://www.ietf.org/rfc/rfc2827.txt

[51] American Registry for Internet Numbers (2007) http://www.arin.net (2007-05-18)

Bilaga A

Frågor till Junet AB.

Mjukvara

Vilka operativsystem i Network Operations Center (NOC)?
Vilka applikationer används i NOC?
Vilka måste fungera?
Kan de uppgraderas för att klara IPv6
Vilka servrar används? DNS, Mail, WWW, NTP

Använder ni utav utomstående servrar/tjänster?

Hårdvaruutrustning

Vilken Lager 3 utrustning finns (Lager 3 switchar, routrar)?
Behöver de uppgraderas?
Vad har ni för brandväggar?
Filtrerar ni trafiken?
Finns det några trådlösa förbindelser?

Routing

Vad använder ni er av för routingprotokoll?

Adressallokering

Var erhålls nuvarande IPv4-adresser ifrån?
Kan man köra IPv6 på samma länk till uppströms leverantör som IPv4?

Kundhantering

Autentiserias kunderna på något sätt?
Hur adresserar ni kunder, DHCP?
Hur många IPv4-adresser får varje kund?