Blekinge Tekniska Högskola
Institutionen för Programvaruteknik och Datavetenskap

IP version 6

Inte längre frågan OM och inte så mycket NÄR utan snarare HUR!

Kandidatarbete inom datavetenskap
Juni 2001

Författare: Birkan Atilmis
Linda Hoff

Kontaktinformation

Författare:

Birkan Atilmis

Folkparksvägen 18:19
372 38 Ronneby

E-mail: adb98bat@student.bth.se
Hemsida: http://www.student.bth.se/~adb98bat
Telefon: 0457-128 58

Linda Hoff

Folkparksvägen 18:20
372 38 Ronneby

E-mail: is98lho@student.bth.se
Hemsida: http://www.student.bth.se/~is98lho
Telefon: 0457-267 77

Handledare och examinator:

Universitetslektor Håkan Grahn

E-mail: hakan.grahn@bth.se
Telefon: 0457-38 58 04

Institutionen för
Programvaruteknik och Datavetenskap
Blekinge Tekniska Högskola
Box 520
372 25 Ronneby

Hemsida: http://www.ipd.bth.se
Telefon: 0457-38 58 00
Fax: 0457-271 25

Sammanfattning

Titel: IP version 6 – Inte längre fråga OM och inte så mycket NÄR utan snarare HUR!

Författare: Birkan Atilmis och Linda Hoff

Problemområde: Idag har Internet blivit var mans egendom. Detta innebär tyvärr en hel del problem. Det tydligaste vi står inför idag är att IP-adresserna håller på att ta slut. För att bli av med problemet används olika temporära lösningar (”lappningsteknik”) men även en permanent lösning utvecklas, nämligen Ipv6 (*Internet Protocol version 6*).

Det nya protokollet löser adressbristen men har även många andra funktioner så som säkerhet och bättre routinglösningar. Vi ställde oss då frågan varför har ingen övergång skett trots dessa fördelar.

Frågeställning: Var i övergången mellan IPv4 och IPv6 står vi idag?

Varför har inte övergången mellan IPv4 och IPv6 redan skett? Vilka är de största anledningarna och vilka fler möjliga finns det?

Slutsats: Arbetet visar att tiden för en övergång ännu inte är inne. Huvudanledningarna är att det saknas produkter och en allmän anledning för en migration.

Nyckelord: IP, IPv6, IPv4, 6bone, IETF, adressbrist, standard, teknik, produkter, kunskap.

Förord

Vi vill börja detta kandidatarbete med att tacka alla som deltagit och hjälpt oss i vårt arbete. Först och främst vill vi tacka Håkan Grahn, vår handledare och examinator, för all stöd och hjälp vi fått genom arbetes gång. Sedan vill vi även tacka alla de företag som vänligen ställde upp i vår undersökning samt alla IPv6-utvecklare som svarat på diverse frågor.

Denna rapport vänder sig främst till människor inom IT-branschen och studenter som studerar inom ämnet datavetenskap. Förkunskaper i ämnet nätverk och datakommunikation erfordras av läsaren för att få en större förståelse av innehållet.

Innehållsförteckning

1 Introduktion

1.1 Problemområde

IP betyder *Internet protocol* och idag använder vi version 4. Denna version har använts i 20 år och bara det är ett tydligt tecken på att tekniken varit lyckad. Det har dock dykt upp olika problem som kan innebära stora problem om de inte löses inom en snar framtid.

I dag finns det fyra miljarder IP-adresser och ca 200 miljoner av dessa används idag. Det kan tyckas att det finns gott om adresser kvar. Problemet är dock att användandet av IP-adresser ökar kraftigt och många företag använder redan nu tekniker för att komma undan problemet. Dessutom kan inte alla 4 miljoner användas. Många adresser är allokerade men används inte och kan inte överlåtas till någon annan.

Ett annat problem med dagens IP är att routingtabellerna håller på att formligen explodera. De innehåller massor av information som försvårar och drar ner prestanda av paketroutingen.

Idag ser IP-tekniken lite ut som ett lapptäcke. För att få de funktioner en organisation vill ha så lägger de till olika lösningar för att lösa de problem som finns i IPv4. En stor del företag använder t ex tekniker för att öka säkerheten.

En möjlig lösning på alla dessa problem är den nya versionen av IP, IPv6 (*Internet Protocol version 6*). Den största skillnaden är att de nya adresserna består av 128 bitar istället för 32 som IPv4. Detta innebär att antalet adresser ökar kraftigt. Den nya versionen har försökt ta tillvara på alla de fördelar föregående version hade plus att lägga till de funktioner som företag och organisationer idag får genom tilläggstekniker. I den nya versionen finns t ex kryptering, identifiering och automatisk konfiguration.

Utvecklandet av IPv6 började i mitten av 90-talet och det har varit heta debatter om hur standarden ska se ut. I många artiklar kan man nu börja läsa saker så som ”varför dröjer IPv6?”. Detta är något vi tänkt utreda lite mer. Var i utvecklingen och övergången mellan IPv4 till IPv6 är vi idag? Om det nu är så bra varför börjar inte företag och organisationer migrera till den nya versionen? Detta var frågor som dök i den inledande delen av vår arbetsprocess.

En fråga som många ställer sig är vad som hände med IPv5. Den femte versionen av protokollet utvecklades för överföring av multimedia via multicast. Den fick dock inget genomslag.

1.2 Syfte

IPv6 tenderar till att liknas vid Y2k (2000-problemet), då alla visste att problemet skulle komma men ingen gjorde något åt det förrän i sista sekunden. Det finns nog inte många som motsäger att en dag kommer IPv4-adresserna att ta slut. Allt detta lappande som pågår idag, hur länge håller det? Det gäller att vara förberedd och att undersöka

eventuella problem tidigt för att förhindra en liknande situation som vi hade vid årsskiftet 1999-2000.

Utvecklingen av IPv6 har lett till många förbättringar för IP-tekniken. Säkerheten är ett stort område som har bearbetats väl och andra problem som upplevs med IPv4 har förbättrats. Trots alla fördelar har IPv6 inte fått något större erkännande av IT-branschen ännu.

Syftet med arbetet är att ge en lägesrapport med kommentarer om vad som bör utvecklas mer, främst för organisationer och företag, så att en övergång till IPv6 kan påbörjas.

2 Frågeställning

Ur problemområdet har vi kunnat plocka ut följande frågeställning:

- Var i övergången mellan IPv4 och IPv6 står vi idag?
- Varför har inte övergången mellan IPv4 och IPv6 redan skett? Vilka är de största anledningarna och vilka fler möjliga finns det?

2.1 Hypotes

Utredningen är till viss del hypotesprövande. Vad vi menar med ”till viss del” är att vi inte bara utreder om de faktorer vi satt upp stämmer utan att vi även letar efter andra möjliga.

Ur frågeställningen har vi då kommit fram till följande hypotes:

Övergången från IPv4 till IPv6 har inte kommit igång på grund av:

- Utvecklingsarbetet är inte helt färdigt då det gäller standard, teknik och produkter som stödjer IPv6.
- Tiden är inte inne ännu då det ej är brist på IP-adresser idag.
- Kunskapen hos företag/organisationer är bristfällig.

2.2 Begränsningar

Vi kommer att vara tvungna att begränsa oss då det gäller möjliga faktorer till att övergången dröjer. Troligen kommer organisatoriska anledningar att vara en stor faktor men då detta hamnar utanför vårt område (datavetenskap) kommer vi inte att undersöka det närmare. Vi kommer heller inte att gå in så djupt tekniskt sett ur någon synvinkel.

3 Metod

3.1 Litteratur och experter inom området

Vi har haft kontakt med några av de personer som varit med och utvecklat IPv6 från början och som arbetar med övergångsteknikerna. Vi har haft kontakt via e-mail där de svarat på olika frågor och gett rekommendationer om dokument och artiklar. Dessa personer är:

- Bob Fink (ngtrans och 6bone)
- Alain Duran (ngtrans och 6bone)
- Tony Hain (ngtrans och 6bone)

Vi ser dem alla tre som starka källor då de varit med och utvecklat standarden. Även viss information om testnätet 6bone har samlats in och analyserats.

Örigt material vi använt är böcker, rapporter och diverse dokument med vetenskaplig anknytning. En del av materialet har vi hittat genom bl a ovannämnda personer.

3.2 Undersökning

Vi har valt att göra en kvalitativ undersökning då detta vetenskapliga arbetssätt lämpar sig för vår utredning och vi inte söker ett statistiskt resultat. Denna utredning bör inte låsa sig, utan i slutändan kunna erbjuda ett resultat som presenterar nya synsätt på problemet.

3.2.1 Population

Populationen är företag och organisationer som har någon form av kunskap om IPv6. Vi har bedömt att företag sosm inte har denna kunskap inte kan tillföra vår utredning något. Hur ska man kunna svara på frågan varför man inte använder IPv6 om man inte vet vad det innebär? Vidare har vi valt att göra ett urval ur denna population då denna undersökning är av kvalitativ karaktär. Vi har valt företag och universitet som är kopplade till 6bone och på så sätt har praktisk erfarenhet av IPv6. Här hade vi ett ganska stort bortfall av företag som inte svarade men vi valde även att ta bort mindre företag och privatpersoner som var kopplade till testnätverket. Detta då vi i denna utredning valt att inte inrikta oss på företag eller privatpersoner vars intentioner med IPv6 är mer av hobbykaraktär.

Vidare består vårt urval i undersökningen av företag som är insatta i IPv6 tekniken, men som inte är kopplade till testnätverket 6bone, för att få en bredare undersökning. Dessa företag har vi valt mest på grund av tillgängligheten och då de uppfyller våra krav, det vill säga att de är företag med god kunskap om IPv6.

För att vårt resultat ska bli så rättvisande som möjligt har vi valt att vinkla undersökningen ur många olika vinklar. Därför var det även naturligt att ett antal Internetleverantörer, eller som de även kallas ISP, samt nätverksföretag deltog. Detta då de kan betraktas som grunden i en global övergång till IPv6. ISP är företag som bl a tillhanda-

håller IP-adresser till olika användare så som privatpersoner och företag. Kan inte ISP-förtagen erbjuda några IPv6-adresser och nätverksföretagen inte levererar produkter som stödjer det nya protokollet är det väldigt svårt att påbörja en övergång. Val av dessa har även här baserats på tillgänglighet.

Frågeformuläret vi använde oss av finns som bilaga 1. De företag/organisationer som deltog i undersökningen var:

ISP	**Universitet**
Spray	Chalmers
Sunet	KTH (Kungliga Tekniska Högskolan)
Telenordia	Lunds Universitet
Nätverksföretag	**Övriga företag**
Axis	SPP (Säker Pensions Partner)
Cisco	Tietoenator

Vi har även valt att kategorisera de olika företagen, som här ovan, för att lättare organisera och kategorisera materialet från undersökningen. Valet av olika kategorierna har fastställts utifrån de olika verksamheter organisationerna bedriver

3.2.2 Tillvägagångssätt vid analys av undersökning

Syftet vid kvalitativa studier är att få ut något av stora mängder data. Svårigheten förstärks av att det inte finns några självklara regler för hur man tolkar och drar slutsatser från kvalitativ data. Detta innebär att vi blir tvungna till att använda vår egen analysförmåga. Vi har dock valt att rätta oss efter de riktlinjer Judith Bell nämner i ”Introduktion till forskningsmetodik” [1]. Dessa riktlinjer är i korta drag följande:

- Först görs en noggrann beskrivning och sammanställning av data från fallen. Detta arbete är nödvändigt för att de som läser det ska kunna veta vad våra tolkningar, resultat och slutsatser baseras på samt att läsaren ska kunna dra sina egna slutsatser utifrån materialet.

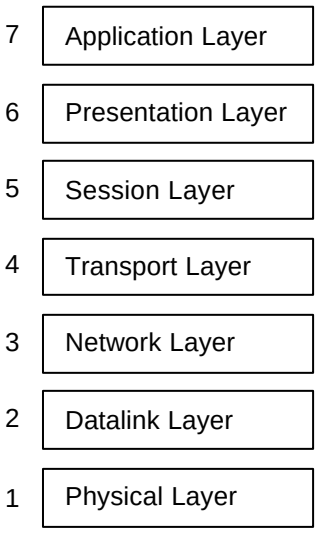
- Analysen görs för att organisera och bearbeta data från fallen, så att data blir mer hanterlig och tolkningsbar.

- Vår tolkning görs för att tydliggöra vad saker och ting betyder, skapa förståelse för händelseförlopp och resultat, samt för att dra slutsatser.

4 Vad är IP?

För att kommunikationen på Internet ska fungera gäller det att alla datorer förstår varandra. Det gäller att alla pratar samma språk som Jesper Ek uttrycker det i sin bok "Lättpoket om Internet" [4]. Detta språk eller protokoll som det heter, som används på Internet heter TCP/IP. Egentligen är TCP/IP flera protokoll, en så kallad protokollstack, där IP eller *Internet Protokoll* som det heter är ett av dessa.

För att förstå hur själva kommunikationen fungerar kan referensmodellen OSI-modellen (se figur 4.1) användas. Förkortningen står för *Open Systems Interconnetion.* I boken "Lokala nät" av Lars Ewald [5] förklaras modellens olika lager ingående. Här nedan finns en kort genomgång av dessa.



Figur 4.1 : OSI-modellen med dess sju olika nivåer.

Det översta skiktet, applikationsskiktet, ger olika tjänster för slutanvändaren. Med hjälp av fönsterpresentationer styrs processer och systemresurser. Det är i detta skikt användaren talar om vad som ska hända genom att använda sig av någon programvara, t ex e-mailprogram eller en webbrowser.

I nästa skikt, presentationsskiktet, formuleras användarens instruktioner om så att transporten blir möjlig. Här ingår kod- och formatkonvertering, data- och textkomprimering samt kryptering.

Sessionskiktet kan, som Lars Ewald antyder i sin bok "Lokala nät" [5], även kallas användarens gränssnitt mot nätverket. Det ska upprätthålla kommunikationen mellan de aktuella processerna (programmen) i respektive ändpunkt.

I transportlagret skapas ett klart och tydligt gränssnitt gentemot överliggande skikt. Det fungerar lite som en samordnare av alla de olika skikten i modellen. På denna nivå arbetar t ex TCP och UDP, vilka också är protokoll.

I nästa nivå, nätverksskiktet är det dags för att behandla själva transporten av data. Det är här IP kommer in i bilden. På denna nivå väljs vilken väg paketet ska ta, dv s mellan vilka noder i nätet data ska transporteras.

Ytterligare ett skikt krävs för att själva dataöverföringen ska vara tillförlitlig, nämligen datalänkskiktet. Dess tre huvuduppgifter enligt Lars Ewald [5] är:

- Synkronisering av datameddelandet vid start och identifiering av dess slut.
- Fördela trafikflödet till skilda mottagare.
- Feldetektering och felkorrigering.

Längst ner i modellen hittar vi det fysiska skiktet som ett tillhandahåller mekaniskt och elektriskt gränssnitt. Det används sedan för uppkoppling av den fysiska anslutningen men även bibehållande och nedkoppling.

IP är alltså protokollet som bestämmer hur data ska skickas från en dator till en annan. Hur adresserna på Internet ser ut styrs även av detta protokoll. IP fungerar ungefär som ett postsystem - det låter sändaren ange en adress på ett paket och posta det, men det finns ingen länk mellan sändaren och mottagaren. IP har alltså ingenting med själva anslutningen att göra, den delen tar, som vi gått igenom här ovan, t ex TCP eller UDP hand om. IP ser bara till att adresser finns på de olika paketen och bestämmer sedan hur de ska skickas.

5 Hur skiljer sig IPv6 från IPv4?

5.1 Routing och adressering

5.1.1 IPv6 adressrepresentation

I boken ”IPv6 – Clearly Explained” av Pete Loshin [11] kan man läsa att en fundamental anledning till att IPv6 finns idag är den kommande adressbrist som kan inträffa då Internet växer allt fortare för varje år. Visserligen kunde utvecklarna av IPv6 valt att lösa problemet med att endast förbättra IPv4-adressering, men de ville inte missa möjligheten att skapa ett nytt protokoll vilket även gav dem chansen att göra förbättringar för adressering och routing.

Den största skillnaden mellan själva IPv4- och IPv6-adresserna är adresslängden. IPv4 adresser är 32 bitar lång medan IPv6 är hela 128 bitar. Denna skillnad innebär först och främst fler adresser med IPv6, men även möjligheter till adressering som IPv4 inte kunnat erbjuda, vilket kommer behandlas senare.

IPv4 adresser är representerade som ett fyrdelat värde som separeras med punkter. Varje värde är ett decimalt tal mellan 0-256 och hela IPv4 adresser kan se ut som följande:

10.5.3.1
127.0.0.1
194.139.67.53

IPv6 adresser är som tidigare nämnt 128 bitar, och är därmed fyra gånger längre än IPv4. En IPv6-adress har därmed en adressformat som ser ut som följande:

X:X:X:X:X:X:X:X

Varje X motsvarar en hexadecimal siffra på fyra tecken. Varje tecken motsvarar 4 bitar och totalt har en adress 8 värden, separerade med kolon. Därmed motsvaras adressen av totalt 128 bitar (4 x 4 x 8 = 128). Exempel på IPv6-adresser är följande:

CDCD : 910A : 2222 : 5498 : 8475 : 1111 : 3900 : 2020
1030 : 0 : 0 : 0 : C9B4 : FF12 : 48AA : 1A2B
2000 : 0 : 0 : 0 : 0 : 0 : 0 : 1

Pete Loshin [11] skriver att detta format är det rekommenderade adressformatet för IPv6, men även att det finns två ytterligare metoder för hur adresserna ska se ut. Det kan bl.a. förekomma adresser som består av långa serier av nollor (som tredje adressen i ovanstående exempel). Då är det tänkt att nollorna ska ersättas med ett tomrum. Så adressen *2000 : 0 : 0 : 0 : 0 : 0 : 0 : 1* kan ersättas med *2000 : : 1*, för att effektivisera behandlingen av dessa typer av adresser. De dubbla kolonen innebär att adressen kan breddas ut till en komplett 128 bitars adress. Denna metod kan dock endast ersätta nollor som ligger i ett helt 16 bitars värde, d v s mellan två kolon, och kan endast användas en

gång i en adress. Om det finns flera 16-bitars nollor på flera olika ställen i adressen, men som inte sekventiellt följs åt, kan inte dubbelkolon användas.

*1030 : **0000 : 0000 : 0000** : C9B4 : **0000** : **0000** : 1A2B*

kan alltså inte bli

*1030 : : C9B4 **: :** 1A2B.*

Det tredje adressformatet är en lösning i mixad miljö, d v s en adress som ska fungera i IPv4- och IPv6-miljö. I en sådan adress används de sista 32 bitarna till IPv4-adressering. Denna metod bygger på en adressuppbyggnad med formen X:X:X:X:X:X:D.D.D.D, där X motsvarar ett 16 bitar långt hexadecimalt värde och D ett 8 bitar långt decimalt värde. En integrering av IPv4-adresser sker och därmed är det fullt möjligt för paketen att arbeta i både IPv4- och IPv6-miljöer. Adresser kan se ut som följande:

0 : 0 : 0 : 0 : 0 : 0 :***194.47.139.54***

CDCD : 910A : 2222 : 5498 : 8475 : 1111 : ***194.47.139.54***

Den första adressen är en komplett IPv4-adress och den andra en IPv4-kompatibel adress i IPv6 miljö.

5.1.2 IPv6 adressmodell

IPv6 adressmodell är lik IPv4 på många olika sätt. Som IPv4 använder IPv6 unicast-adressering för att identifiera nätverksgränssnitt. Ett nätverksgränssnitt förknippas ofta med ett nätverkskort, men är även andra typer av kopplingar mot Internet. Varje unicast-adress kan anslutas till endast ett nätverksgränssnitt, dock kan varje gränssnitt ha flera unicast-adresser.

En begränsning i IPv4 adressering är att varje nätverksgränssnitt har en globalt unik unicast-adress. En populär server kan lätt sänka sin prestanda beroende på den höga trafiken till en unicast-adress. Med detta i åtanke har en lösning för detta implementerats i IPv6. Lösningen bygger på en princip som tillåter flera nätverksgränssnitt att dela på en unicast-adress. På så sätt kan arbetsbördan delas jämnare mellan flera gränssnitt under en och samma adress. Mer om unicast beskrivs i avsnittet 5.1.3.

5.1.3 IPV6 adresstyper

IPv6 adresstyper är idag unicast, multicast och anycast. Notera att broadcast-adresser som används i IPv4 inte används i IPv6. De tre adresstyperna är definierade i RFC 2373 [11] som följande:

Unicast: Identifierare av ett nätverksgränssnitt. Ett paket sänt till en unicast-adress identifieras av gränssnittet och accepteras om adressen stämmer överens med det egna.

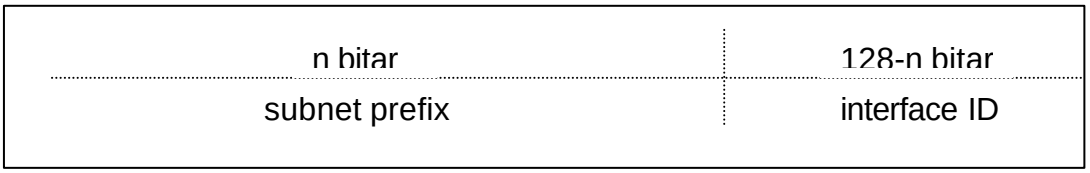
Anycast: Identifierare för en uppsättning nätverksgränssnitt. Ett paket som skickats till en anycast-adress tas emot och vidarebefordras till ett av alla

nätverksgränssnitt. Principen är att den kan skickas till vilket av gränssnitten som helst under en adress, men vanligtvis till den som närmast finns till.

Multicast: Också en identifierare för en uppsättning nätverksgränssnitt. Skillnaden mellan anycast och multicast är att ett paket sänt till en multicast-adress levereras till alla nätverksgränssnitt under den adressen.

Unicast

Unicast-adresser identifierar, som tidigare nämnt, ett IPv6 nätverksgränssnitt. Detta innebär att varje gränssnitt har en adress som är unik och består av 128 bitar. Adressen kan delas upp och kategoriseras beroende på vem som tittar på den. En nod på Internet ser adressen som en helhet och vet att den identifierar en unik nod i ett annat nätverk, medan en router kan utläsa mer information än så. Routern skulle förmodligen kunna avgöra utifrån adressen att delar av den identifierar en unik nod i ett specifikt nätverk eller subnät. Därför kan unicast-adresser ses som en tvåfälts adress (se figur 5.1), med ett fält som identifierar nätverket, även kallad Interface ID, och ett annat för att fastställa vilket nätverksgränssnitt det är på det nätverket, ett s k subnäts prefix.



Figur 5.1 : Enkel beskrivning av unicast-adressens uppbyggnad (Loshin, 1999, sid 98)

Multicast

Multicastadresser identifierar, som tidigare nämnt, alla nätverksgränssnitt som identifierar sig med multicast-adressen. Man kan med andra ord säga att en nod kan prenumerera från en multicast-adress och gör det genom att annonsera att den vill bli medlem. Detta innebär att all trafik som skickas till aktuell multicast-adress vidarebefordras till alla dess medlemmar. Multicastadresser måste i IPv6 alltid användas som destinationsadress och kan aldrig vara sändare av data.

Formatet för denna adresstyp skiljer sig ifrån övriga två adresstyper då den första oktetten endast består av ettor för att identifiera den som en multicast-adress. Med detta menas att de första åtta bitarna i adressen alltid måste bestå av ettor.

Anycast

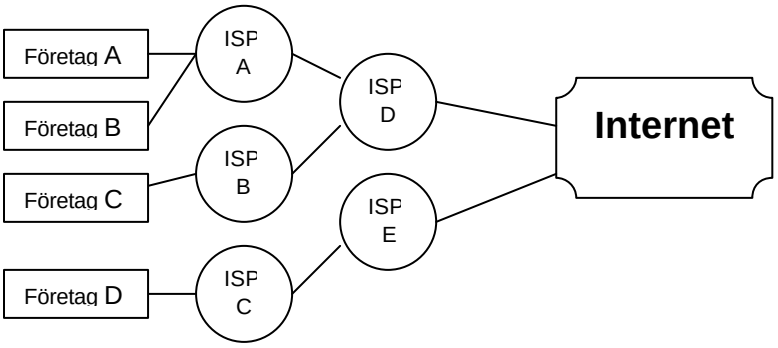
Pete Loshin [11] liknar anycast-adresser vid multicast-adresser då flera noder kan dela på en anycast-adress. Dock kan endast en av dessa noder förvänta sig att få data levererat till anycast-adressen och det gör denna adresstyp lämpad för ett visst antal tjänster. Ett bra exempel på en sådan tjänst är *time servers.* En begäran skickad till en *time server* skickas till en anycast-adress som väljer den närmaste time servern medlem för att på så sätt få de mest korrekta data för denna tjänst. Anycast-adressen vidarebefordrar alltså begäran till

den närmaste servern och det innebär att svaret på begäran kommer på så kort tid som möjligt.

5.1.4 Routing

Enligt Pete Loshin i sin bok ”IPv6 – Clearly Explaned” [11] är adressbristen ett välkänt problem med IPv4. Vad många inte känner till är problemet med de routers som idag arbetar på Internet. En router fungerar som så att den lagrar information om Internets olika delar i en routingtabell för att den enkelt ska kunna kolla upp mottagaradressen och leverera paket till nästa lämpliga nod. Allteftersom Internet växer har dessa routing-tabeller växt och detta inverkar på en routers prestanda då den måste söka igenom väldigt stora tabeller efter rätt nätverksadress. Det är ett problem som har belysts i utvecklingen av IPv6 och förslag på hur detta kan hindras har diskuterats.

I ett tidigt skede i utvecklingen av IPv6 fanns ett förslag på att införa ett system som baserades på ISP (*Internet Service Providers*). Adresserna skulle fördelas bland ISP-företag för att kunna uppnå en IP-hierarki där varje adress kopplas till en ISP i form av ett prefix i adressfältet. Detta innebär i viss mån att routingtabell problemet löses då det ger en adressering som underlättar identifiering av olika nätverk. Bilden nedan illustrerar hur topologin för detta enkelt skulle kunna se ut:



Figur 5.2 : Topologi vid ISP-baserad adressfördelning (Loshin, 1999, sid 133)

ISP-baserad adressfördelning ger alltså en lättare routing. Detta då ett paket till Företag A adresseras till ISP D av sändaren och denne vet att mottagaren ligger bakom routern hos ISP D. ISP D har endast två länkar och vet att paketet ska till ISP A som i sin tur levererar till Företag A. Detta förslag har dock brister då det idag finns stora företags-nätverk som väljer ett flertal ISP som samarbetspartner. Idén skulle fungera, men det administrativa arbete som detta skulle innebära för företagen är en orsak till varför detta förslag inte är optimal. Istället arbetades ett förslag fram där en geografisk tilldelning av IP-adresser kan ske. Detta innebär att adresserna kan fördelas så att de kan spåras till ett geografiskt område, och tilldelning sker på en permanent basis som IPv4-adresser.

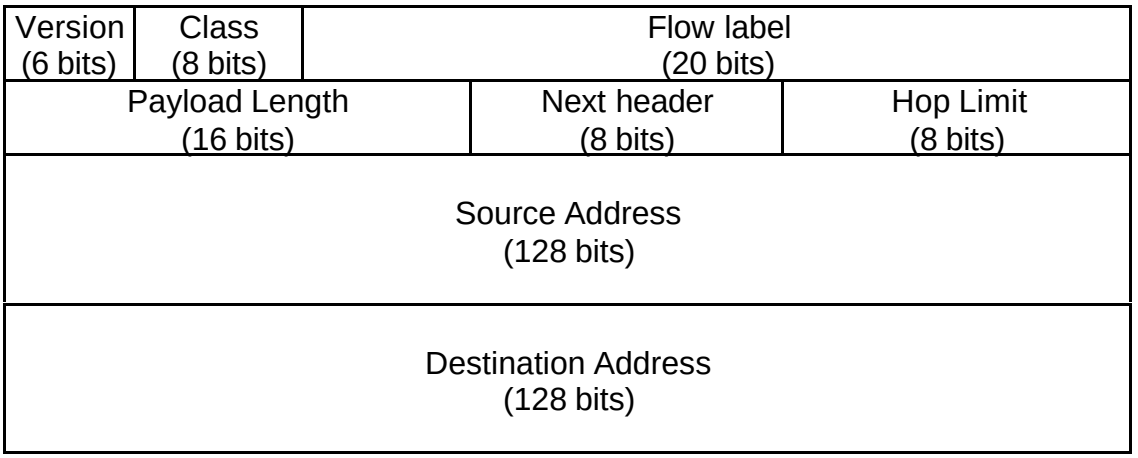
5.2 Paketformat

I mitten av 90-talet började utvecklandet av IPv6-specifikationen av arbetsgruppen IP Next Generation Working Group (ipngwg). Denna arbetsgrupp ingår i The Internet Engineering Task Force’s (IETF) som jobbar med Internetarkitekturen och för ett

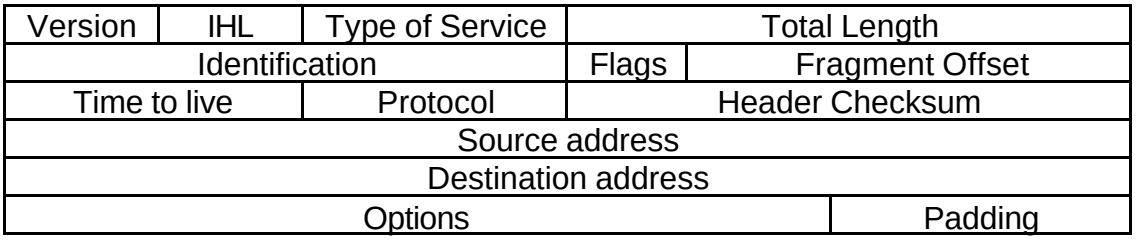
Internet som drivs smidigt [13]. De flesta funktioner som finns i IPv6 finns även i IPv4, i grunden eller som tillägg, men utvecklarna har löst det på ett bättre sätt som gör det lättare och snabbare att använda. Det går alltså idag att använda sig av finesser som finns i IPv6 med den gamla versionen, men det blir extra arbete och kompletterande lösningar.

5.2.1 IPv6 huvudet i jämförelse med IPv4 huvudet

IPv4 har funnits länge och fungerat bra. Det gäller att ta tillvara på det som fungerat bra och inte ta bort viktiga funktioner. Det har dock skett stora förenklingar och några nyheter. För att förstå detta kapitel krävs grundkunskaper om IPv4 och dess huvud. Vi kommer dock inte att gå så djupt in tekniskt.



Figur 5.3 : IPv6 header (King m fl, 2000, sid 21)



Figur 5.4 : IPv4 header (King m fl, 2000, sid 21)

I figurerna 5.3 och 5.4 visas huvudena till IPv4- respektive IPv6. Fältet *version* har samma namn och samma innebörd i både IPv4 och IPv6, dv s det talar om vad det är för format på huvudet.

Utvecklarna av det nya protokollet har i version 6 tagit bort fältet IHL (*IP Header Length*) då en fast längd satts på huvudet. I version 4 finns fältet options där användaren kan lägga till säkerhetsfunktioner m.m. Detta gör då att huvudet kan variera mycket i storlek. IPv6 har en fast längd på huvudet och lägger istället på s k *extension headers*, eller påbyggnadshuvud som vi valt att kalla det, för att få önskade funktioner (se figur 5.5).

IPv6 Header Next Header = Routing	Routing Header Nest Header = TCP	TCP Header + Data

Figur 5.5 : Exempel på hur de olika huvudena kan kopplas ihop (Huitema, 1998, sid 15)

Vi kommer att ta upp dessa olika huvuden lite mer i 5.2.2. För att detta ska fungera finns ett fält som heter *next header* som visar ifall det kommer ytterligare ett huvud och i sådana fall vilken sort.

Type of Service används i IPv4 för att indikera om paketet ska gå den säkraste, kortaste eller billigaste vägen. Christian Huitema beskriver dock i sin bok ”IPv6 – The New Internet Protocol” [9] att det inte fungerat så bra då det är långt ifrån alla applikationer som sätter något värde i detta fält. Det visar sig därför vara ganska givet att bort detta fält helt och hållet.

Class och *flow label* används till realtidstrafiken. I fältet *class* sätts en prioritet på paketen så att realtidspaketen går före vid eventuell kö. *Flow label* används för att hitta paket, som tillhör samma flöde (*flow*), som ska behandlas på lika sätt. Ett flöde är en sekvens av paket, sända från en specifik sändare till en specifik mottagare, unicast eller multicast. De flesta paket kommer dock inte att tillhöra något flöde. Mer om flöden tas upp i kapitlet 5.6 ”Stöd för realtidstrafik”.

En annan förändring utvecklarna gjort är att byta ut *total length* till *payload length.* Även detta är ganska självklart då huvudet alltid är av en fast längd. Det är bara lasten som kan variera i storlek, därför är det den enda längdvariabeln som behövs.

Fragmenteringenfältet är helt borttaget i den nya versionen av IP. Istället ska sändande dator lära sig den högsta tillåtna paketstorlek för en förbindelse. Denna procedur kallas *path MTU discovery.* Enkelt förklarat skickas ett ICMP meddelande tillbaka till sändaren då ett paket är för stort och talar om den maximala storleken förbindelsen klarar. Paketet skickas då igen med rätt storlek. Detta gör att fälten *flag* och *fragment offset* inte behövs.

Time to live har endast döpts om, till *hop limit* då det namnet bättre talar om vad fältet innebär, den har dock kvar samma innebörd.

Checksumman är borttagen och det kan verkas radikalt men faktum är att variabeln erbjöd endast en begränsad nivå av säkerhet. Det finns redan idag flera IPv4 routrar som hoppar över checksumman helt och hållet just för att den inte fungerat tillfredsställande.

5.2.2 Påbyggnadshuvud

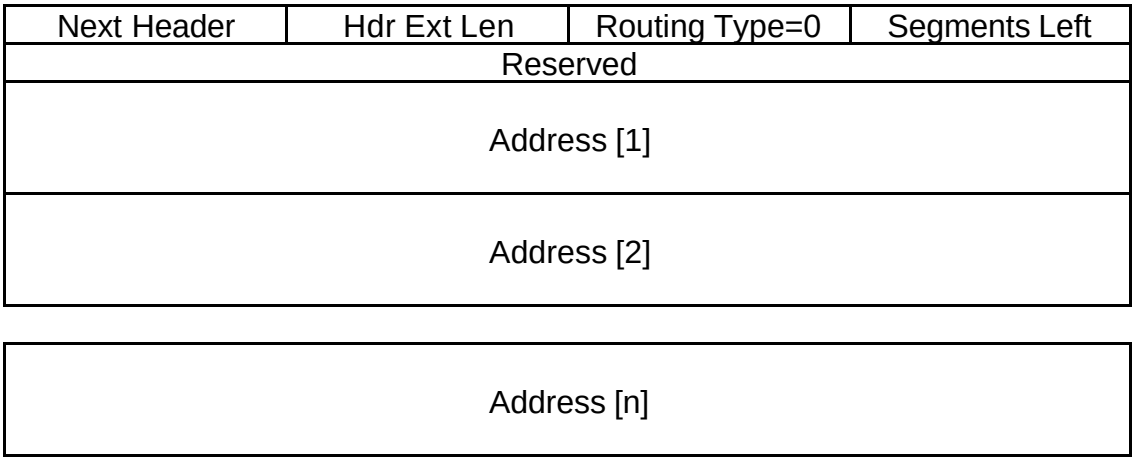
Det finns sju olika påbyggnadshuvud. Med hjälp av dessa kan användaren lätt lägga på den funktion som ska användas och samtidigt ha en snabb och smidig trafik. Utvecklingsarbetet har grundats på filosofin att undvika onödiga processer i mellanliggande noder i nätverket, då det drar ner hastigheten. Alltså har utvecklarna valt att ha få fält i IPv6 huvudet och i stället lägga till extra huvuden om funktionen önskas.

Hop-by-hop options header

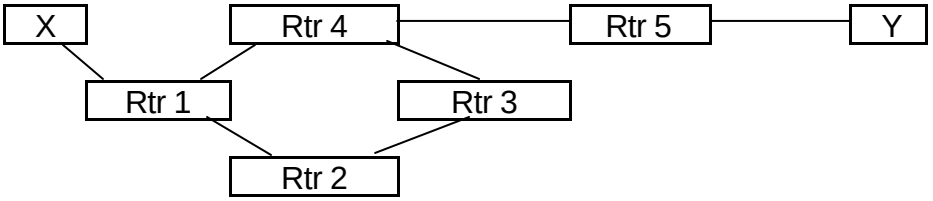
Detta huvud läggs alltid först efter det inledande IPv6 huvudet. Varje router som paketet passerar måste nämligen läsa och utföra instruktionerna som anges i detta huvud. Det innehåller information i form av olika alternativ. Routern kan t ex inte skicka vidare ett paket p g a en funktion som inte stöds av routern eller förbindelsen. Då kan routern kolla i huvudet vad den ska göra med paketet. Ska det slängas och inget mer eller kräver sändaren ett ICMP meddelande o s v.

Routing header

Huvudet innehåller en lista med adresser vilka paketet ska skickas via (se figur 5.6). Den utpekade vägen kan vara antingen strikt kopplad eller löst. Med en lös koppling har paketet flera vägväl, medan den strikta endast har ett alternativ. Se exempel figur 5.7.



Figur 5.6 : Routing header (Huitema, 1998, sid 16)



Figur 5.7 : Exempel på löst kopplad. Den utpekade vägen är 1,2,3,5 (King m fl, 2000, sid 25)

För varje utpekat steg som besöks minskas värdet i fältet *segments left.* Detta huvud är bra för att styra viss trafik. En organisation kanske vill hålla så mycket som möjligt av sin trafik borta från en viss förbindelse eller tvärt om.

Fragment header

Som nämnts innan så använder inte IPv6 sig av fragmentering. Det hela fungerar på samma sätt som om *don't fragment* flaggan i version 4 vore satt. Däremot så måste paketet

fragmenteras, delas upp i ett antal mindre paket, innan det skickas ut på nätet. Det är då *fragment header* används (se figur 5.8).

Next Header	RESERVED	Fragment Offset	RES	M
Identification				

Figur 5.8 : Fragment header (Huitema, 1998, sid 20)

Authentication header

Authentication header är ett av de två som ökar säkerheten med IPv6, *encrypted* är det andra. Genom att kräva identifiering av mottagaren skyddas paketlasten, själva datan som skickas, från att modifieras av obehöriga. Tekniken skyddar även mot att någon annan än mottagaren svarar paketet. Säkerheten med IPv6 är en av de största fördelarna med den nya tekniken.

Encrypted security header

Authentication header skyddar dock inte mot att data läses av någon utomstående men det gör *encrypted security header.* Datan krypteras då så att den inte kan läsas av någon som inte har krypteringsnyckeln. Det betyder att kryptering sker i ett sk *end to end* förhållande mellan sändare och mottagare.

Destination option header

I ”The Case for IPv6” [10] beskriver King m fl att detta huvud används för att kunna lägga till ny funktionalitet i det nya protokollet. Det finns två olika sorter; Om det ligger före ett *routing header* så går varje nod paketet passerar in och läser informationen i huvudet. Ligger det efter ett *routing header* eller om sådant saknas så körs huvudet endast av mottagaren.

5.3 IPv6 i OSI

I och med det nya protokollet krävs det även ändringar längre upp i OSI-modellens nätverkslager, i allt ifrån ICMP till DNS och applikationer. Det är många saker som måste fungera tillsammans och detta kräver mycket arbete. För att få en global övergång måste alla tillverkare, t ex Microsoft, Sun m m, ta sitt ansvar och se till att deras produkter stödjer det nya protokollet. Teknikerna i de lägre skikten jobbar IETF hårt med för att ta fram en standard.

5.4 Plug and play

En annan stor fördel Pete Loshin [11] nämner med IPv6 i jämförelse med IPv4, förutom antalet adresser och bättre säkerhet, är dess *plug and play* funktioner. En IPv6 nod kan konfigureras automatiskt. Noden använder sig i normalfall av sin MAC-adress kombinerat med nätverksprefixet som noden tar reda på hos närmaste router.

För att uppnå liknande automatiska konfigurering med IPv4 används olika protokoll beroende på ifall användaren vill ha statiska eller dynamiska adresser. Ska en dator alltid

få samma adress? Detta kan vara en nackdel i dagens läge då det råder adressbrist. En del av dessa protokoll, t ex DHCP, har utvecklats vidare för att kunna användas även med den nya versionen av IP.

Plug and play som verkligen fungerar är en oerhörd tillgång. Det tar ofta väldigt mycket tid för administratören att installera och konfigurera mjuk- och hårdvara manuellt. IPv6 kan alltså bli lite av en ekonomisk guldgruva då administrationen av nätverk kan komma att förenklas betydligt.

5.5 Säkerhet

Aldrig tidigare har det varit så mycket trafik på Internet, aldrig tidigare har det varit så mycket känsligt eller hemlig trafik som färdats över nätet, aldrig tidigare har det heller funnits så många *hackers*, *crackers* och liknande. Detta bidrar till att nätsäkerhet diskuteras mycket. I IPv4 kan man uppnå en viss grad av säkerhet genom att använda sig av vissa tilläggsfunktioner t ex IPsec. Förkortningen står för IP *security* tillhandahåller funktioner för kryptering och verifiering. Detta har i många fall fungerat bra. Det fanns stora förväntningar om att designerna av IPv6 skulle utveckla bra och stabila säkerhetsfunktioner i den nya versionen.

Som vi nämnt tidigare finns det två huvuden i IPv6 som arbetar med säkerhetsfrågor, identifiering- och krypteringshuvudena (*Authentication header* och *encrypted security header*). Dessa gicks igenom i stycke 5.2.2 och kommer därför inte att gås igenom mer.

Ämnet säkerhet kan dock diskuteras länge. Det är svårt att hitta en algoritm som kommer att fungera för all framtid. Det finns många andra saker som ”stör” utvecklingen, t ex olika bestämmelser i olika länder. Det är väldigt svårt att kombinera alla länders olika lagar och regler och få fram bra och hållbara säkerhetsfunktioner.

Säkerheten i IPv6 beskrivs dock av Christian Huitema [9], vara en av de stora och efterlängtad fördelarna med den nya versionen i jämförelse med den gamla.

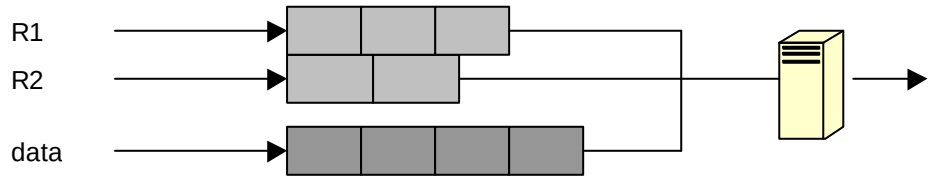
5.6 Stöd för realtidstrafik

De flesta experter som rekommenderade *flow label* som en del av IPv6 huvudet (se avsnitt 5.2.1) hade en vision om något de kom att kalla *resource reservation*, eller med andra ord resurs allokering. De ansåg att traditionella paketförmedlade nätverk inte stöder realtidsapplikationer som tal och video speciellt bra. De tyckte därmed att en resursallokering vore ett lyft för enkel paketförmedling.

Vi kan tänka oss traditionell telefonförbindelse. Det analoga ljudet, eller rättare sagt rösten, samplas och kvantiseras vilket resulterar i en överföringshastighet på 64 Kbit/s. Denna signal kan sedan skickas över Internet i ett flöde av paket, vars storlek varierar beroende på applikation och tjänst. Om vi antar att det skickas 50 paket i sekunden och transmissionsmediet är god, dv s inte övertrafikerad, så kan mottagaren ta emot och packa upp paketen för att sedan lyssna av ljudet i godtycklig kvalité. Kvalitén sjunker dock ju mer trafik det förekommer på transmissionsmediet. Några av paketen i flödet kommer att ställas i köer. Kanske försvinner en och en annan helt och hållet på vägen från sändare till mottagare. Fördröjningen är ett problem i paketförmedlade nätverk för

realtidsprogram och detta har sin förklaring i den flödesalgoritm som konstruerats för paketförmedlade nät. Den som först kommer till en nod behandlas först, eller som policyn kallas *first come, first served.* Därmed fastnar de realtidsberoende paketen i köer bland andra paket med lägre prioritet, dv s paket som inte är beroende av tiden för transmission i förhållande till realtidspaketens.

Att använda applikationer som ska fungera i realtid är alltså svårt med dagens paketförmedlade nätverk. Därför har något som kallas för *special services* arbetats fram. Problemet med köer kan enligt denna metod lösas enkelt genom att göra flera köer beroende på vilken sort av paket som ska behandlas. En till flera köer endast för realtidskommunikation skapas och utöver dessa finns alltid en kö för all traditionell datakommunikation (se figur 5.9). Varje kö för realtid motsvarar ett flöde av paket och har normalt högra prioritet än kön för datakommunikation, som behandlas när tid för detta ges.



Figur 5.9 : Två realtidsflöden och en datakö (Huitema, 1998, sid 177)

6 Övergången mellan IPv4 och IPv6

Alain Durand, en av utvecklarna av IPv6, sammanfattar sin artikel “Deploying IPv6” [2] med meningen ”With all of the recent activity surrounding IPv6, it’s no longer a question of ‘if,’ and less a question of ‘when,’ but rather ‘how’ IPv6 will be deployed.” Detta är precis vad vi har stött på under arbetets gång. Det är ingen som tvivlar på att IPv6 kommer att slå igenom, men många funderar på hur övergången kommer att gå till. Arbetet kommer senare att presentera en dagslägesrapport över hur det ser ut idag och hur utvecklare och företag ställer sig till olika metoder och problem med övergången mellan IPv4 och IPv6.

Den arbetsgrupp som arbetar mest inom detta område är IETFs arbetsgrupp Next Generation Transistion (ngtrans) [14]. Deras uppgifter består av att:

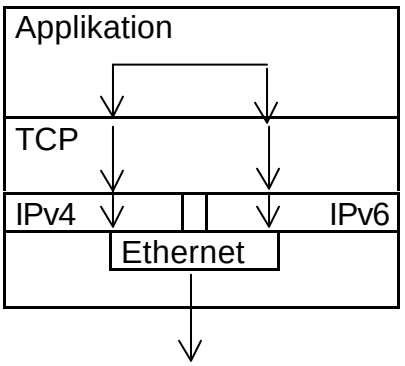
- Specificera verktyg och metoder som kan vara användbara i övergången till IPv6.
- Skriva dokument om hur dessa verktyg och metoder kan användas i olika situationer.
- Samarbeta med testnätet 6bone, som drivs under ”IPv6 Testing Address Allocation” (RFC 2471), för att främja utveckling och testning av IPv6.
- Samarbeta med andra lämpliga IPv6-relaterade aktiviteter i IETF och i andra organisationer.

Tidigt i utvecklingsarbetet togs det fram tekniker för hur övergången ska gå till. I RFC 1933 ”Transition Mechanisms for IPv6 Hosts and Routers” [6] skriver författarna, Gilligan och Nordmark, att kompatibilitet med den gamla versionen är nyckeln till en lyckad migration. Här nedan beskrivs två tekniker som utvecklats och som beskrivs i ovannämnd RFC.

Som vi nämnt tidigare så består en IPv6 adress av 128 bitar och en IPv4 adress av 32 bitar. Dessa två nedanstående tekniker använder sig av IPv4-kompatibla IPv6 adresser. Som det nämndes i stycke 5.1.1 är det en full 128 bitars adress där de första 96 bitarna är nollor och de resterande 32 en IPv4 adress.

6.1 Dubbla IP lager (Dual-stack)

Denna metod innebär att alla noder i nätet kan hantera både IPv4- och IPv6-paket (se figur 6.1). Ett IPv6 baserat Internet kommer alltså då att utvecklas parallellt med IPv4 nätet. Skillnaderna mellan de två versionerna är ganska stora detaljmässigt men inte i princip.

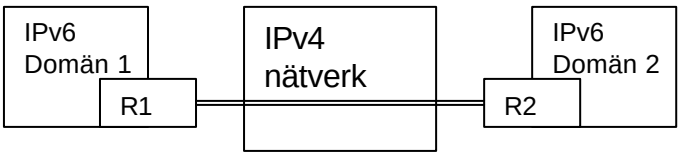


Figur 6.1 : Hur en dual-stack nod fungerar (Huitema, 1998, sid 198)

Noderna kommer att använda sig av IPv6-trafik så långt som möjligt. Detta innebär att en övergång kommer att ske i egen takt flytande och så småningom kommer all trafik bestå av endast IPv6-paket.

6.2 Tunnlar

För att kunna använda sig av IPv6 över ett IPv4-nätverk kan tunnlar användas. Då läggs ett IPv4-huvud före IPv6-paketet för att transporten ska fungera, dv s IPv6-paktet blir *payload* i IPv4-paketet. Man skulle kunna uttrycka det som Christian Huitema gör i sin bok ”IPv6 – The New Internet Protocol” [9], att man kopplar ihop två IPv6-öar i IPv4-havet (se figur 6.2).



Figur 6.2 : IPv6-trafik över IPv4-nätverk med hjälp av en tunnel (Huitema, 1998, sid 201)

Tunnling kan användas på olika sätt:

- Router till router
- Användare till router
- Användare till användare
- Router till användare

I de två första fallen måste ändnoden av tunneln, routern, häva inkapslingen och skicka vidare paketet till sitt slutmål. Detta innebär då att IPv6-adressen inte är den samma som destinationsadressen som då är en IPv4-adress. Detta kräver att adressen i förväg konfigureras till ändpunkten i tunneln hos den nod som kapslar in paketet. Detta kallas konfigurerad tunnling.

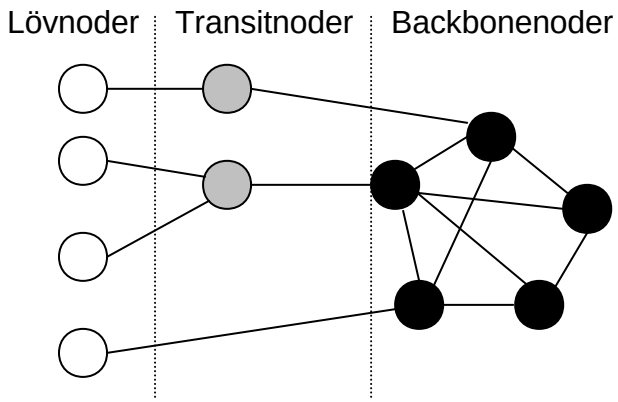
I de två sista fallen, användare till användare och router till användare, fungerar det omvänt. IPv6-adressen som används i tunneln är också den slutliga destinationsadressen.

Om då IPv6 adressen är en IPv4-kompatibel adress behöver inte ändpunkten av tunneln konfigureras i förväg. Denna typ av tunnling kallas automatisk tunnling.

6.3 6bone

6bone är ett testnätverk för IPv6 som startades sommaren –96 med inspiration från Mbone som är ett testnät för multicasting som använder sig av tunnling. En erfarenhet från det nätet är att tunnlar ska konfigureras med viss försiktighet, annars blir det lätt ett enda trassel av tunnlar hit och dit i all oändlighet.

6bone består av ett antal routrar som stödjer den nya versionen som på så sätt erbjuder ett IPv6-nät ovanpå IPv4 Internet. Som nämnts tidigare så agerar testnätet under skrivelsen ”IPv6 Testing Adress Allocation” (RFC 2471) [8] som beskriver själva adresserna och hur de ska användas. I rapporten förklaras tydligt att 6bone endast är ett testnät och de adresser som använd där kan inte användas då IPv6 börjar dra igång. Nätverket är utformat med tre hierarkilager; backbonenoder, transitnoder och lövnoder (se figur 6.3).



Figur 6.3 : Hierarkin i 6bone. (Guardini m fl, 2000)

På 6bones hemsida, www.6bone.net [12], beskrivs det att nätverket växte fram från IETF IPng gruppen som utvecklade IPv6-protokollet. I början användes 6bone för att testa standarder och implementationer. Idag är det inriktat mer på testning av procedurer för själva övergången. Testnätet fungerar nu även relativt fritt där vem som helst kan ansluta sig. Gruppen ngtrans, som tidigare nämnts övervakar dock nätverket.

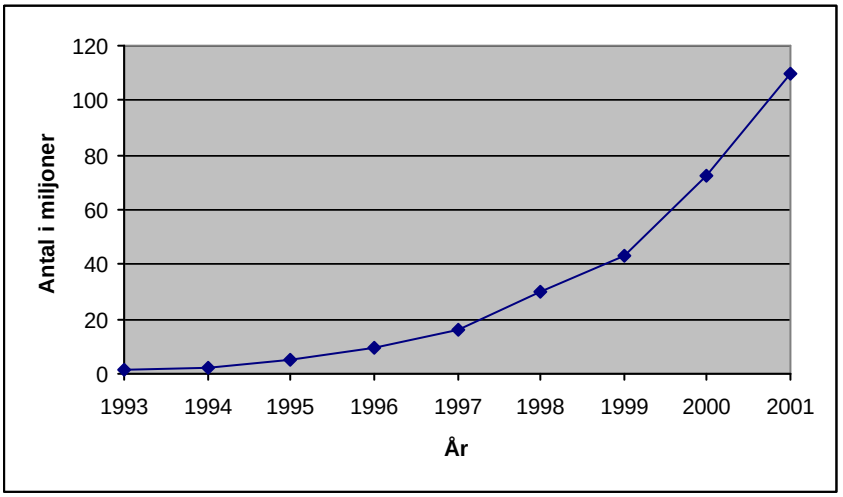
7 Resultat och analys

7.1 Bristen på IPv4-adresser

I vår undersökning och på andra håll visas tecken på hur bristen av IP-adresser drabbar företag och organisationer. Med tecken menas t ex den ökade användningen av NAT. Åsikten om hur allvarligt problemet är skiljer sig dock kraftigt. Det finns många utredningar som gjorts om när adresserna ska ta slut men resultaten skiljer sig väldigt mycket. Vad forskare trodde för några år sedan stämmer heller inte alls i dagsläget. I mitten av 90-talet kom det en ny policy vid tilldelning av adresser (bl a RFC 1366, RFC 1466, RFC 2050) som bidrog till att tillväxten mattades av något.

Av de 4 miljarder IPv4-adresser som finns idag är ca 1.5 miljarder reserverade av IANA (se bilaga 2) för framtida bruk. IANA står för *Internet Assigned Numbers Authority* och arbetar med att centralt koordinera Internet. Resterande 2.5 miljarder är idag allokerade. Detta betyder dock inte att de används. ISP-företag t ex kan ha ett visst antal adresser på lager. Alain Durand nämner i sin artikel ”Deploying IPv6” [2] att det är ca 200 miljoner adresser som använd idag.

Internet Domain Survey [16] undersöker regelbundet antalet noder kopplade till Internet genom att undersöka domän namn systemet (DNS). Utvecklingen mellan januari 1993 till januari 2001 kan skådas här nedan (figur 7.1). Viktigt är dock att siffrorna är underskattade då alla noder inte har ett motsvarande namn i domän namn systemet.



Figur 7.1 : Internets utveckling mellan 1993-2001 [16]

Om då antalet adresser som är kvar läggs ihop med hur expansionsutvecklingen av Internet ser ut så kan varje individ själv försöka uppskatta när krisen infinner sig. Tekniker som t ex NAT (*Network Address Translation*) skjuter upp krisen eller förhindrar en övergång till IPv6, hur man nu vill se på det.

NAT definieras I RFC 1631 ”The IP Network Address Translator (NAT)” av Kjeld Borch Egevang och Paul Francis [3]. Tekniken fungerar så att man har en s k NAT-box

som utåt Internet har en unik IP-adress. Bakom boxen finns det lokala nätverket. Alla stationer som finns i detta nät har lokala IP-adresser, som inte är globalt unika. Utifrån ser man alltså endast ett IP-nummer och all trafik som går till datorerna i det lokala nätverket skickas till en och samma IP-adress, nämligen den som finns angiven för NAT-boxen. De lokala IP-adresserna kan sedan återanvändas i ett annat nätverk som använder sig av NAT. På detta sätt löser man ofta problemet med bristen på IP-adresser idag.

I vår undersökning har vi stött på heta diskussioner om NAT. Ett av företagen som ingick i vår undersökning (se 7.4 ”Undersökning”) tyckte NAT var en väldigt dålig teknik som fick användarna att få i en falsk känsla av säkerhet. Alain Durand [2] har även han starka åsikter mot tekniken. Han anser att det är för komplext, tidskrävande och förstör *end-to-end* principen på Internet. Ytterligare ett argument han har mot NAT är att IPsec inte fungerar då denna teknik används.

7.2 IETFs workgroups

7.2.1 IP Next Generation Work Group (ipngwg)

Arbetsgruppen ipngwg har som uppgift att ta fram en standard för de grundläggande funktionaliteten hos IPv6. På deras webbsida [15] går det att läsa att alla deras mål och milstolpar är avklarade. Vi kan alltså konstatera att den grundläggande standarden är helt klar. Detta hävdar även de utvecklare vi varit i kontakt med. Tony Hain, som är verksam i ngtrans, hävdar dock att det hela tiden dyker upp allmänna ofullständigheter och förvirringar i standarden. Dessa arbetar dock IETF med för att försöka rätta till.

7.2.2 Next Generation Transition Work Group (ngtrans)

Vad denna arbetsgrupp sysslar med har vi redan gått igenom tidigare och deras arbete är ännu inte färdigt. De planerar dock, enligt deras webbsida [14], att vara klara med den största delen av arbetet detta år.

Alla de utvecklare vi varit i kontakt med är eniga om att utvecklandet av IPv6 och migrationsarbetet tar väldigt lång tid att genomföra. Tony Hain uttrycker det så som att utveckla IPv4 till IPv6 var alltid planerat att ta minst tio år och vi är bara halvvägs igenom. Han tror dock att innan årets slut borde det finnas produkter så att det går att påbörja en migrationsplanering. Alain Durand anser samma sak, att byta från IPv4 som fungerat så bra till IPv6 kan inte ske över en natt.

Alla utvecklarna är även eniga om att är det något som kommer att fördröja övergången så är det p g a brist på produkter som stödjer det nya protokollet. Många system och applikationer kommer kanske aldrig att uppgraderas då företaget bakom kanske inte existerar längre eller känner någon motivation. Kunnig teknisk personal nämns även som en faktor.

Utvecklaren Alain Durand tror att övergången kommer att ske i vågor, beroende på olika branscher och geografiska områden. Troligen så kommer Asien att vara längst fram i övergången. Japan t ex har redan visat stort intresse och engagemang för det nya protokollet.

För att få fart på övergången från IPv4 till IPv6 även i Europa har EU bildat IPv6 Task Force [17]. Första uppgiften är att ta fram en plan för hur övergången ska genomföras. Slutmålet är att hela Europa ska vara kompatibelt med det nya protokollet år 2005, då de anser att IP-adresserna kommer att ta slut.

7.3 6bone

Från början hade vi tänkt att analysera 6bone för att få fram ungefär var tekniken står idag och vilka för- och nackdelar som uppstått. Efter vår kontakt med bl a Bob Fink, som arbetar med ngtrans och 6bone, ändrade vi dock synvinkel på det hela. 6bone är ett testnät där det är menat att det ska uppstå problem. Vi ställde frågan huruvida 6bone var realistiskt i den bemärkelsen att ett framtida IPv6-nätverk kommer att ha samma uppbyggnad. Svaret på frågan blev att i 6bone är de flesta tunnlar konfigurerade manuellt och så kommer troligen inte fallet vara i ett framtida verkligt nät. Med detta som grund är det lätt att konstatera att 6bone inte är något bra underlag för att utvärdera utvecklings- och migrationsarbetet. Resultat som dock kan utläsas är att så länge det uppstår problem i 6bone finns det något som behövs bearbetas.

Ytterligare en sak som kan utläsas från 6bone är antalet anslutna. I dag är det 51 olika länder som är anslutna och totalt 767 anslutningar [18]. Det finns tyvärr inga uppgifter om hur utvecklingen sett ut under de åren som 6bone varit verksamt. Bob Fink uppskattar dock att efter de tolv första månaderna har ökningen varit linjär. Det är alltså fler och fler som visar intresse för den nya tekniken och vill testa.

7.4 Undersökning

Inom detta område presenteras och diskuteras de data vi samlat in, bearbetat och analyserat från vår undersökning. Kapitlet är uppdelat efter de områden som behandlats i intervjuerna. Frågorna till undersökningen finnes som bilaga 1.

7.4.1 Bakgrund

I detta avsnitt diskuteras kunskapsnivån, erfarenhet och satsningar på IPv6 hos företagen och organisationerna, samt om de idag använder substitut till IPv6 funktioner.

Företagen och organisationerna varierar i engagemang och intresse för IPv6. Hos de flesta ISP-företagen finns ett intresse av IPv6s utvecklingsarbete och ett av företagen deltar i IETFs arbete i att utveckla nya standarder för det nya protokollet. Nätverksföretagen har ett intresse som kan liknas vid det ISP-företagen har, men det största intresset ligger i att utveckla framtida IPv6-produkter. Ett av nätverksföretagen påpekar att intresset för IPv6-produkter inte medför att intresset för det egna företagsnätet ökar, utan det kan betraktas som två helt olika intresseområden. De menar att inget arbete gjorts med det egna företagsnätet, utan det som görs ligger på produktnivå.

På universiteten och högskolorna är intresset högt för IPv6 och två av tre bedriver någon slags testverksamhet. Det finns ett intresse, men det påpekas av majoriteten av de som deltog att det saknas påtaglig anledning till vidare arbete. Detta är en åsikt som även delas av de övriga företagen, som säger att de följer utvecklingen av IPv6, men som inte bedriver något testnät.

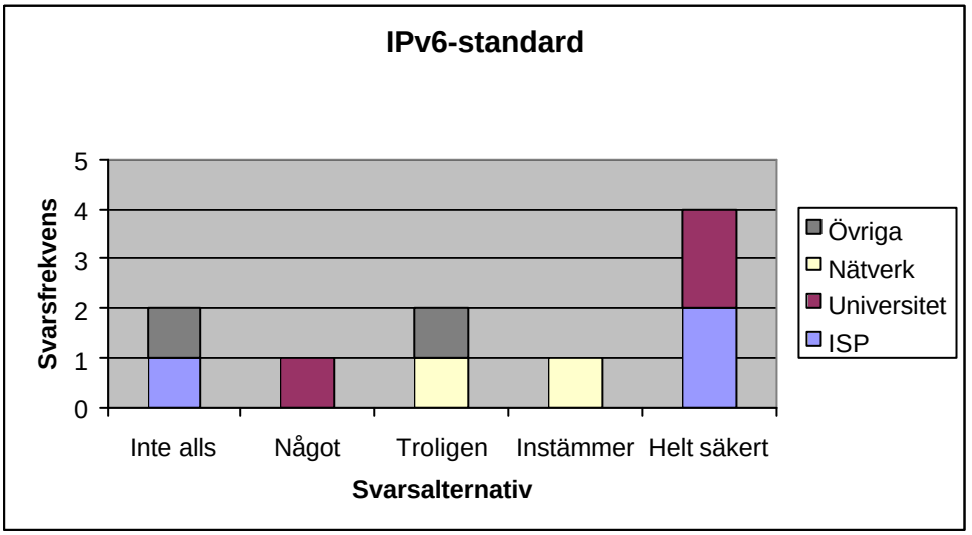
Kunskapsnivån om IPv6 är hos företagen och organisationerna i de flesta fallen grundläggande. Ett nätverksföretag och ett av de övriga företagen säger sig ha goda kunskaper. Vad som återigen bör nämnas är att det aktuella nätverksföretaget gärna ser sig ha två sorters kunskap; en för sin produktutveckling och en för det egna företagsnätet. På produktnivå anser det att de har mycket goda kunskaper, medan de på det egna företagsnätet endast har goda kunskaper. Den mycket goda kunskapen delas även av det andra nätverksföretaget, som bl a har produkter som idag stöder IPv6, men även ett av ISP-företagen ser sig ha mycket goda kunskaper.

Tekniker som fungerar som substitut till funktioner som finns implementerade i IPv6 kan användas i IPv4 och på frågan om företagen och organisationerna använde sådan teknik konstaterades att ca 90 % av de som deltog i undersökningen använde antingen IPsec eller NAT. Ett av universiteten påpekade att de inte använder dessa tekniker i förbättringssyfte, utan snarare för att de vill testa ny teknik.

7.4.2 Övergången från IPv4 till IPv6

I undersökningen var ett av målen att försöka kartlägga företagens och organisationernas syn på övergången till IPv6. Frågor vi sökte svar på var att se vilka faktorer som enligt dem är avgörande för en övergång och vad är det som idag hindrar en övergång. De som ingick i undersökningen skulle först och främst ta ställning till huruvida IPv6 standarden, tekniken eller tillhörande produkter var otillräckliga för en övergång.

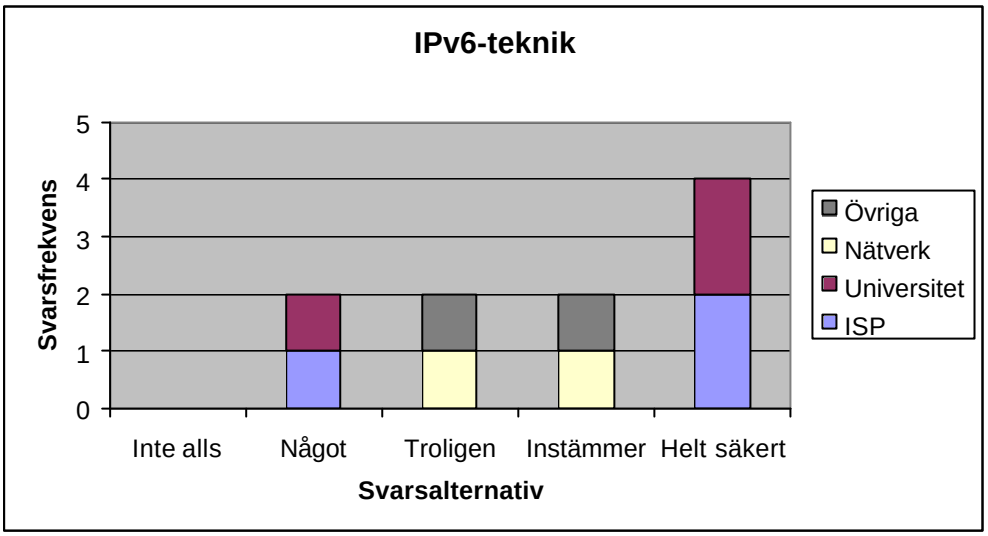
Först och främst fick de svarande ta ställning till huruvida utvecklingen av IPv6 standarder är färdig för övergång eller ej. På denna fråga hade de svarande olika synpunkter beroende på vilken företagskategori de tillhörde och detta kan utläsas i nedanstående diagram 7.1.



Figur 7.1 : Svarsfördelning på ställningstagande till huruvida en eventuellt bristande IPv6-standard förhindrar en övergång från IPv4.

I diagrammet 7.1 kan det utläsas att det är huvudsakligen två kategorier som är helt säkra på att IPv6 standarder är en orsak till att en övergång inte skett från IPv4. Dessa två grupper är ISP och universiteten. Nämnvärt i sammanhanget är att en av de som svarade inte alls är ISP-företaget som har representant i IETFs arbetsgrupp.

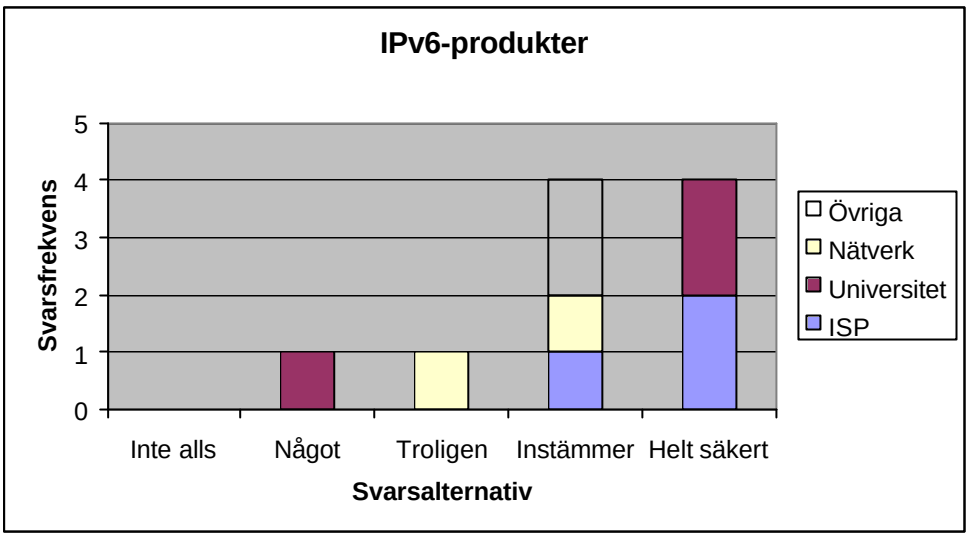
Vidare skulle de svarande ta ställning till huruvida IPv6 tekniken är otillräcklig för en övergång idag. Svaren från denna fråga fördelades som visas i diagram 7.2.



Figur 7.2 : Svarsfördelning på ställningstagande till huruvida en eventuellt bristande IPv6-teknik förhindrar en övergång från IPv4.

Denna fråga gav ett liknande svar som vid föregående fråga om IPv6 standarder. Dock är det ingen som motsätter sig argumentet att IPv6-tekniken skulle vara bristfällig för en övergång. Vi kan även här se två ISP och två universitet som svarat att de är helt säkra på att tekniken kan ses som en brist och är en orsak till varför de inte valt att övergå till IPv6. Förövrigt är det en jämn fördelning på de övriga svarsalternativen förutom inte alls.

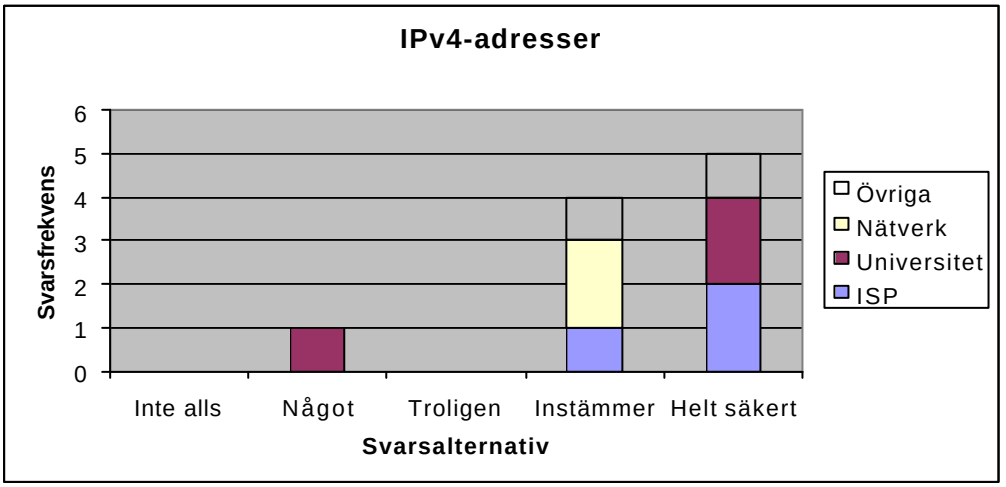
Nästa delfråga var att kolla hur företagen och organisationerna såg på utbudet av IPv6 produkter. Med produkter menas mjukvara till routers såväl som operativsystem, men även hårdvara m m.



Figur 7.3 : Svarsfördelning på ställningstagande till huruvida en eventuellt brist av IPv6-produkter förhindrar en övergång från IPv4.

Diagram 7.3 visar att det inte finns någon större optimism i fråga om produkter bland de svarande. Hela 40 % svarar att de instämmer vid påståendet att bristen på IPv6 produkter är en orsak till övergången inte genomförts, och ytterligare 40 % har svarat att de är helt säkra på samma påstående. Ett av universiteten ser ingen anledning till att gå över till IPv6 då det inte finns några tjänster som kräver detta. Ett annat universitet påpekar även bristen på slutanvändarprogram. Vidare påpekar tre av de svarande i sina svar att routerproblem är något som de upplever som ett hinder och en av dem påpekar att de saknar stöd från routingföretagen.

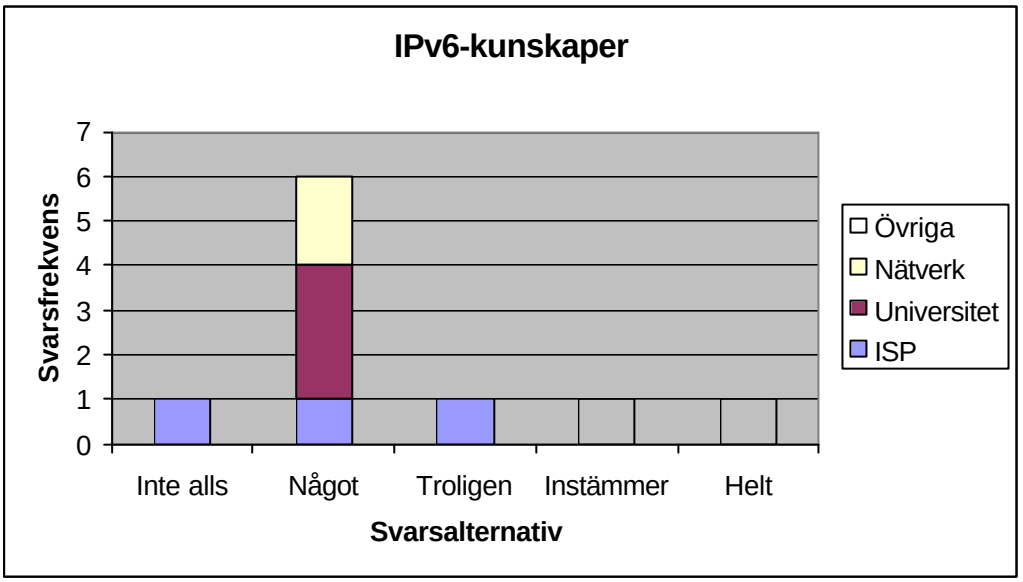
Ett område som har behandlats tidigare är frågan om det råder brist på IPv4-adresser (se 7.1 ”Bristen på IPv4-adresser”). I vår undersökning ville vi också se hur deltagarna i undersökningen såg på fenomenet genom att ta ställning till påståendet att övergången till IPv6 inte skett då det inte råder någon adressbrist på IPv4. Resultatet kan utläsas i nedanstående diagram.



Figur 7.4 : Svarsfördelning på frågan om övergången inte skett då det inte råder brist på IPv4-adresser.

Diagrammet 7.4 visar tydligt att den allmänna uppfattningen är att det inte råder någon brist på IPv4-adresser. Det är dock enligt två av deltagarna mycket p g a NAT (*Network Address Translation*), som enligt dem får många att tro att det finns fler adresser än vad det egentligen gör. En av dessa påpekar även att NAT bara drar ut på problemet med adressbrist.

Slutligen ställdes en fråga om bristande IPv6-kunskaper inom företaget eller organisationen kunde vara en orsak till varför en övergång inte skett (se diagram 7.5).



Figur 7.5 : Svarsfördelning på frågan om IPv6-kunskaper inom företaget eller organisationen kunde vara en orsak till varför en övergång inte skett

Denna fråga domineras av svarsalternativet något, som motsvarar 60 % av alla svaren. En av ISP-företagen säger i samband med denna fråga att de inte ser okunskap som ett problem och därmed inte som en orsak till varför en övergång till det nya protokollet skett.

7.4.3 Framtiden

Vad har företagen och organisationerna i undersökningen för syn på framtiden gällande en övergång till IPv6? Har de tänkt/planerat att gå över till IPv6 och i sådant fall när? Det är några av frågorna vi sökte svar på i detta avsnitt där vi försöker se hur deltagarna av undersökningen ser på framtiden.

Vi ville först och främst se om deltagarna hade tänkt eller planerat att gå över till IPv6 och i sådant fall när. Det genomgående svaret, ca 60 %, på denna fråga var att de inte hade några planer i dag. Två ISP-företag svarade att de skulle övergå så fort nyckelprodukter såsom routrar och brandväggar släppts. Ett av universiteten svarade att de börjat övergå i mindre portioner och uppskattade att de skulle bli i större omfattning om ett till två år. De trodde vidare att de skulle sluta köra IPv4 i större mängd om fem till tio år och sluta köra IPv4 helt om ca femtio till hundra år.

Vidare ville vi även se hur en övergång skulle kunna se ut för företaget/organisationen, d v s om de skulle använda IPv6 till vissa delar av nätverket, byta ut hela nätverket eller delar av det. Ett av de övriga företagen svarade att de skulle övergå i form av autonoma IPv6 system (IPv6 öar). Det andra företaget i kategorin övriga företag, två ISP samt ett universitet säger i sina svar att de tror på en parallell körning av de två protokollen som etappvis kommer att bytas ut med tiden till IPv6. Med andra ord kan det sägas att de flesta är överens om att deras övergång kommer att ske i etapper där delar byts ut med tiden.

7.4.4 Analys av undersökning

Vi konstaterade tidigare att det fanns ett högt intresse från ISP-företagens sida när det gällde utvecklingen av det nya protokollet. En av deltagarna i undersökningen tycker att ISP-företagen har en stor roll i den globala övergången, men även lokalt, då de utgör ryggraden på Internet. Så tycker även vi. Även faktumet att den nya adresshierarkin (se även 5.1.4 Routing) kan baseras på ISP är för dem en anledning att följa utvecklingen. Andra som har en avgörande roll i arbetet med IPv6 är nätverksföretagen. Även där är intresset påfallande då deras utrustning ska bygga framtidens nätverk. Universitetens och högskolornas höga intresse ligger mer på en akademisk nivå då de vill lära sig nya tekniker och samtidigt följa utvecklingen för att kunna erbjuda det senaste i sin utbildning. Det stora intresset utgörs även av dataföreningar på skolorna som bedriver testverksamhet av eget intresse, men med skolans utrustning. Övriga företag har intresse, men känner att det behöver en påtaglig anledning till att gå vidare i sitt arbete med IPv6. Vad de menar är att utvecklingen och intresset inte är stort nog för att t ex skapa ett testnät. De är pålästa i ämnet, men har hamnat i ett vakuum där inget sker i dagsläget, utan man inväntar på någon form av omvälvning innan något görs från den egna sidan.

Kunskapsnivån om IPv6 är som tidigare nämnt i regel grundläggande hos de som deltog i undersökningen. De som säger sig ha goda eller t o m mycket goda kunskaper är de företag och organisationer som har en stor roll i övergången, d v s nätverksföretag. Dock har två av tre ISP-företag sagt sig ha grundläggande kunskaper, även om intresset är högt. Detta beror enligt oss på att de inte avsatt större resurser i frågan, även om intresset för IPv6 är påfallande. De övriga som svarat att de har grundläggande kunskaper är företag som inte känner något större ansvar i övergången, vilket troligtvis är en anledningen till att det inte har mer kunskaper än vad de behöver.

I undersökningens andra del där övergången bearbetades är tyngdpunkten lagd på faktorerna standard, teknik, produkter, IP-adresser och kunskap. Vi ser tydligt att det inte råder någon gemensam åsikt i fråga om IPv6-standarden. Svarsalternativen är olika beroende på vem som svarar, men man kan klart se att det finns ett stort antal som ser standarden som en flaskhals. De som tycker detta är i första hand ISP och universitet. Det bör dock poängteras att de som svarat detta var bl a de två ISP som endast hade grundläggande kunskaper. Vidare är det liknande på teknik, där även ett flertal ISP och universitet är eniga om att IPv6-tekniken inte är fullt utvecklat för en övergång. Det är en tendens som återkommer i de flesta frågor, d v s att universiteten och ISP-företagens svar skiljer sig från mängden.

IPv6-produkter är ett område som de flesta tycks ha nåt att säga om. ISP-företagen påpekar att de inte finns någon anledning till att erbjuda sina kunder IPv6 då det idag inte

finns några tjänster som kräver detta. Även i universitetsvärlden delar man detta synsätt. Det finns helt enkelt inget utbud av slutanvändarprogram som är IPv6 baserade, menar de.

Vidare ställs krav på produkter från nätverksföretagen som tillverkar routers av flertalet av de svarande. Många av företagen och organisationerna, bortsett från nätverks-företagen i undersökningen, tycker att de inte har tagit sitt ansvar och upplever det som ett hinder. Ett av nätverksföretag har dock i skrivande stund släppt en skarp version av sin mjukvara för IPv6-routers.

Framtidsarbetet är för många av de svarande något som man väljer att avvakta med då de inväntar på produkter och riktlinjer från de större IPv6-organisationerna. Någon handlingsplan finns inte hos de flesta och det råder i dagsläget en väntan på att något stort ska ske innan man agerar. De flesta är dock ense om ungefär hur övergången kommer att ske för sin egen del, d v s i etapper eller parallellt, men inte exakt hur eller när.

8 Diskussion och slutsats

Utredningen har varit både förutsägbar i vissa fall och i andra överraskande. Vi har upptäckt synsätt som vi tidigare inte tänkt på. Det är dessa som är så viktiga att föra fram i diskussionen om övergången till IPv6.

Dilemmat om det går att påbörja en migration idag är svårlöst. Vissa anser att det går andra inte. Utvecklingen har dock kommit ganska långt. Standarden är färdig men vi befinner oss i ett stadium där företag och organisationer endast bedriver testverksamhet inom området. Kanske behövs det ännu mer testning innan en skarp övergång kan påbörjas. Dock kan man se att skarpa versioner kommer så smått. Var i övergången befinner vi oss då? Det är svårt att säga med exakthet, men ett stort steg är taget men minst ett lika stort steg återstår att ta. Vad som är gjort och vad som återstår att göras behandlas senare i detta kapitel. Nu är det inte heller endast upp till utvecklarna att det ska gå framåt utan nu hänger det på alla.

En trend vi sett är att de företag som drar de tyngsta lassen i övergången (ISP och nätverksföretag) har visat stort intresse för tekniken och det är ytterst viktigt. Utan de förutsättningarna kommer vi ingenstans. Dock fick vi uppfattningen när vi letade företag till vår undersökning att det är ganska få bland lite mindre företag som har någon kunskap eller intresse alls. Detta kan bli ett problem senare om det inte ändras.

Vad som är den största bromsklossen idag är att det knappt finns några produkter som stödjer det nya protokollet. Kommer bara tillverkningen igång ordentligt så tror vi att resten följer med automatiskt. Dock bedrivs en hel del forskning runt produkter och IPv6. Det gäller också att företag och organisationer ser någon vinst i att migrera. Standarden, tekniken och produkter var som tidigare nämnt tänkt att ta ganska lång tid att utveckla, trots detta så stressar många, t ex journalister och andra intressenter, på utvecklingen. Det är något som man ofta ser då det gäller IT. Allt ska gå snabbt som vinden. Att slå ihop två fabriker kan ta tio år men att slå ihop två system vill man ska gå över en natt.

I dagens läge är standarden mogen för en övergång men det krävs mer än så. Tekniken och produkterna är en klar och tydlig anledning till att övergången inte är påbörjad.

Problematiken runt bristen på IPv4-adresser är något som varit väldigt svårt att utreda. Frågan är om det finns något svar överhuvudtaget. Vi har dock fått den uppfattningen under vår undersökning att det är ett stort problem med all lappningteknik som inger en falsk känsla trygghet. Den allmänna uppfattningen tycks vara att det inte råder någon adressbrist medan många ”experter” anser att teknikerna som används för att komma runt problemet endast förlänger lidandet. Denna allmänna uppfattning beror bl a på den policy som tillämpas vid distribution av adresser och lappningtekniker så som NAT. Det är även svårt att säga med säkerhet om dessa tekniker håller för alltid. Hela detta dilemma är något man skulle kunna utreda i sig.

I vår undersökning visade det sig att det finns grundläggande kunskap inom området. Vad som dock överraskade oss lite var att bristfällig kunskap inte sågs som ett problem.

Det anses vara lätt att skaffa sig den kunskap man behöver för att genomföra en migration när tiden är inne. Vi ser dock en fara med de företag som inte visar något intresse alls för den nya tekniken. Vad vi menar är att det är viktigt att upplysa istället för att utbilda. En känsla vi fått är att det är långt ifrån alla som vet om att IPv6 finns.

Sammanfattningsvis är vårt huvudresultat att det måste finnas en påtaglig anledning för företag och organisationer att övergå till det nya protokollet. Detta finns inte idag. Det måste alltså skapas produkter som kräver IPv6. Om alla produkter stödjer både IPv4 och IPv6 kan risken vara stor att användarna hänger kvar i den gamla tekniken. Kanske behövs det även en rejäl marknadsföring för att få upp ögonen och intresset hos användarna.

Vår hypotes stämde alltså till viss del. Det som var rätt i vårt antagande var alltså att tekniken inte var helt färdig och det saknas produkter. Det upplevs heller inte vara någon brist på IP-adresser idag. Däremot så är standarden fastställd med mindre modifikationer och kunskapsbristen upplevs inte som ett hinder.

Övriga förslag på framtida arbete är att göra en djupare utredning om vart och ett av våra delområden t ex produkter och bristen på IP-adresser. En idé är också att granska olika organisatoriska faktorer till varför många företag väljer att avvakta. Är det organisatoriskt genomförbart med en sådan radikal förändring? Som vi tidigare nämnt är det väldigt viktigt att få igång tillverkningen av IPv6-produkter. Så någon form av framtida aktivitet som främjar detta är att rekommendera.

9 Källförteckning

[1] Bell, Judith (1993) *Introduktion till forskningsmetodik*, 2nd ed. Studentlitteratur.

[2] Durand, Alain (2001) Deploying IPv6. *IEEE Internet Computingi*, januari-februari 2001, sid 79-81.

[3] Egevang, Kjeld Borch & Francis, Paul (1994) The IP Network Address Translator (NAT). *Request for Comments*, nr 1631.

[4] Ek, Jesper (1998) *Lättpoket om Internet*, 3d ed. Graphi Systems AB.

[5] Ewald, Lars (1986) *Lokala nät*, Studentlitteratur

[6] Gilligan, R & Nordmark, E (april 1996) Transition Mechanisms for IPv6 Hosts and Routers. *Request For Comments*, nr 1933.

[7] Guardini, I & Fasano, P & Girardi, G (2000) IPv6 operational experience whithin the 6bone.

[8] Hinden, R & Fink, R & Postel, J (1998) IPv6 Testing Adress Allocation. *Request For Comments*, nr 2471

[9] Huitema, Christian (1998) IPv6 – *The New Internet Protocol*, 2nd ed. Prentice-Hall, Inc.

[10] King, S & Fax, R & Haskin, D & Ling, W & Meehan, T & Fink, R & Perkins, C E. (2000) The Case for IPv6. *Internet draft.*

[11] Loshin, Pete (1999) *IPv6 – Clearly Explaned.* Academic Press.

Webbsidor:

[12] 6bone, 6bone Home Page (april 2001) *http://www.6bone.net*

[13] IETF Secretariat, IETF Overview (april 2001) *http://www.ietf.org/overview.html*

[14] IETF Secretariat, Next Generation Transision (ngtrans) Charter (april 2001) *http://www.ietf.org/html.charters/ngtrans-charter.html*

[15] IETF Secretariat, IPNG (ipngwg) Charter (april 2001) *http://www.ietf.org/html.charters/ipngwg-charter.html*

[16] Internet Domain Survey, Internet Software Consortium (maj 2001) *http://www.isc.org/ds/host-count-history.html*

[17] IPv6 Task Force (maj 2000) *http://www.ipv6tf.org/*

[18] Lancaster University Computing Department, UK IPv6 Resource Centre (maj 2001)
http://www.cs-ipv6.lancs.ac.uk/ipv6/6Bone/Whois/bycountry.html

Bilagor

Undersökningsfrågor

Internet Protocol v4 Address Space

Bilaga 1 – Undersökningsfrågor

Vi tackar för Er medverkan och hoppas att både Ni och vi får ut så mycket som möjligt utav undersökningen.

Undersökningen är en kvalitativ undersökning vilket innebär att vi vill ha så uttömmande svar som möjligt. Ni behöver alltså inte hålla svaren kort, utan kan känna Er fria att svara med detaljer, fakta osv.

Vissa frågor kan kännas svåra att svara på utan att avslöja allt för mycket om företaget/organisationen. Vi är dock ute efter generella svar och kommer då att behandla Era uppgifter som konfidentiellt material.

Vi vill också be Er att försök svara ur organisationens synvinkel och inte ur Er personliga.

Tack på förhand!

Linda Hoff och Birkan Atilmis

Bakgrundsfrågor

För att skaffa oss ett bedömningsunderlag för nästkommande frågor behöver vi lite bakgrundsfakta om Ert företag/organisation.

- Hur stort är Ert nätverk och hur ser det ut i stora drag? (ex. enbart eget mindre LAN eller kopplat med koncernen i Sverige, över hela världen etc.)

- Vad har Ni för erfarenheter utav IPv6 sedan tidigare? Hur har Er organisation visat intresse för IPv6? Om inget intresse visats, varför?

- Hur god kunskap anser ni att Ert företag har om IPv6?

Inga alls ( ) Dåliga ( ) Grundläggande ( ) Bra ( ) Mycket bra ( )

- Använder Ni NAT, tillägg i IPv4 för kryptering eller annan liknande teknik som IPv6 har bättre lösningar på?

Övergången mellan IPv4 till IPv6

- Bedöm de tre möjliga faktorerna, här nedan, huruvida de hindrar Ert företag/organisation idag till en övergång av IPv6?

  - Utvecklingen av IPv6-standarden, tekniken och tillhörande produkter är inte färdig.

  Inte alls ( ) Något ( ) Troligen ( ) Instämmer ( ) Helt säkert ( )

  - Då det inte är någon brist på IP-adresser idag är tiden helt enkelt inte inne ännu.

  Inte alls ( ) Något ( ) Troligen ( ) Instämmer ( ) Helt säkert ( )

  - Företaget/organisationen saknar kunskap om IPv6 både teoretiskt och praktiskt.

  Inte alls ( ) Något ( ) Troligen ( ) Instämmer ( ) Helt säkert ( )

- Vad finns det för andra specifika faktorer som hindrar Ert företag till en övergång? Bedöm faktorernas inverkan på samma sätt som ovanstående fråga!

Framtidsfrågor

- Har Ni tänkt/planerat att gå över till IPv6 och i sådant fall när?
- Anser Ni att Ert företag har kapacitet till att påbörja en övergång redan idag?
- Hur ser framtidsplanerna ut med aktiviteter och satsningar för IPv6? Har Ni en tidsplan?
- Hur skulle en eventuell övergång se ut för Er del? *(ex. endast byta delar av nätverk, använda IPv6 till vissa funktioner, byta allt rakt av etc.)*

Verksamhetsfrågor

Notera att det är möjligt att svara på flera av nedanstående frågorna beroende på Er verksamhet. Kanske är Ni kopplade med 6BONE och är ett universitet, vilket skulle innebära att det finns två uppsättningar av frågor att besvara.

6BONE

- Hur ser Ert testnät som är kopplat till 6BONE ut i stora drag?
- Hur har testningen gått? Mycket problem? Största problemen? Största fördelarna Ni upplevt?

ISP (Internet Service Provider)

- Känner Ni något ansvar gentemot Era kunder i fråga om en snar övergång till IPv6?
- Kan Ni idag erbjuda IPv6-adresser till era kunder? Om inte, varför?
- Vad gör Ni för att Era kunder ska börja använda IPv6?

Nätverksföretag

- Hur stor del av Era produkter som ni utvecklar/producerar idag stödjer IPv6? Om inte 100 %, varför?

Universitet

- På vilken nivå, utöver Ert samarbete med 6BONE, har Ni arbetat med IPv6? Bedriver Ni någon forskning inom området?

Bilaga 2 - Internet Protocol v4 Address Space

INTERNET PROTOCOL V4 ADDRESS SPACE

The allocation of Internet Protocol version 4 (IPv4) address space to various registries is listed here. Originally, all the IPv4 address spaces was managed directly by the IANA. Later parts of the address space were allocated to various other registries to manage for particular purposes or regional areas of the world. RFC 1466 documents most of these allocations.

Address Block	Registry - Purpose	Date
000/8	IANA - Reserved	Sep 81
001/8	IANA - Reserved	Sep 81
002/8	IANA - Reserved	Sep 81
003/8	General Electric Company	May 94
004/8	Bolt Beranek and Newman Inc.	Dec 92
005/8	IANA - Reserved	Jul 95
006/8	Army Information Systems Center	Feb 94
007/8	IANA - Reserved	Apr 95
008/8	Bolt Beranek and Newman Inc.	Dec 92
009/8	IBM	Aug 92
010/8	IANA - Private Use	Jun 95
011/8	DoD Intel Information Systems	May 93
012/8	AT&T Bell Laboratories	Jun 95
013/8	Xerox Corporation	Sep 91
014/8	IANA - Public Data Network	Jun 91
015/8	Hewlett-Packard Company	Jul 94
016/8	Digital Equipment Corporation	Nov 94
017/8	Apple Computer Inc.	Jul 92
018/8	MIT	Jan 94
019/8	Ford Motor Company	May 95
020/8	Computer Sciences Corporation	Oct 94
021/8	DDN-RVN	Jul 91
022/8	Defense Information Systems Agency	May 93
023/8	IANA - Reserved	Jul 95
024/8	ARIN - Cable Block (Formerly IANA - Jul 95)	May 01
025/8	Royal Signals and Radar Establishment	Jan 95
026/8	Defense Information Systems Agency	May 95
027/8	IANA - Reserved	Apr 95
028/8	DSI-North	Jul 92
029/8	Defense Information Systems Agency	Jul 91
030/8	Defense Information Systems Agency	Jul 91
031/8	IANA - Reserved	Apr 99
032/8	Norsk Informasjonsteknologi	Jun 94
033/8	DLA Systems Automation Center	Jan 91
034/8	Halliburton Company	Mar 93
035/8	MERIT Computer Network	Apr 94
036/8	IANA - Reserved (Formerly Stanford University - Apr 93)	Jul 00
037/8	IANA - Reserved	Apr 95
038/8	Performance Systems International	Sep 94
039/8	IANA - Reserved	Apr 95
040/8	Eli Lily and Company	Jun 94

041/8	IANA - Reserved	May 95
042/8	IANA - Reserved	Jul 95
043/8	Japan Inet	Jan 91
044/8	Amateur Radio Digital Communications	Jul 92
045/8	Interop Show Network	Jan 95
046/8	Bolt Beranek and Newman Inc.	Dec 92
047/8	Bell-Northern Research	Jan 91
048/8	Prudential Securities Inc.	May 95
049/8	Joint Technical Command	May 94
	Returned to IANA	Mar 98
050/8	Joint Technical Command	May 94
	Returned to IANA	Mar 98
051/8	Deparment of Social Security of UK	Aug 94
052/8	E.I. duPont de Nemours and Co., Inc.	Dec 91
053/8	Cap Debis CCS	Oct 93
054/8	Merck and Co., Inc.	Mar 92
055/8	Boeing Computer Services	Apr 95
056/8	U.S. Postal Service	Jun 94
057/8	SITA	May 95
058/8	IANA - Reserved	Sep 81
059/8	IANA - Reserved	Sep 81
060/8	IANA - Reserved	Sep 81
061/8	APNIC - Pacific Rim	Apr 97
062/8	RIPE NCC - Europe	Apr 97
063/8	ARIN	Apr 97
064/8	ARIN	Jul 99
065/8	ARIN	Jul 00
066/8	ARIN	Jul 00
067-079/8	IANA - Reserved	Sep 81
080/8	RIPE NCC	Apr 01
081/8	RIPE NCC	Apr 01
082-095/8	IANA - Reserved	Sep 81
096-126/8	IANA - Reserved	Sep 81
127/8	IANA - Reserved	Sep 81
128-191/8	Various Registries	May 93
192/8	Various Registries - MultiRegional	May 93
193/8	RIPE NCC - Europe	May 93
194/8	RIPE NCC - Europe	May 93
195/8	RIPE NCC - Europe	May 93
196/8	Various Registries	May 93
197/8	IANA - Reserved	May 93
198/8	Various Registries	May 93
199/8	ARIN - North America	May 93
200/8	ARIN - Central and South America	May 93
201/8	Reserved - Central and South America	May 93
202/8	APNIC - Pacific Rim	May 93
203/8	APNIC - Pacific Rim	May 93
204/8	ARIN - North America	Mar 94
205/8	ARIN - North America	Mar 94
206/8	ARIN - North America	Apr 95
207/8	ARIN - North America	Nov 95
208/8	ARIN - North America	Apr 96
209/8	ARIN - North America	Jun 96
210/8	APNIC - Pacific Rim	Jun 96
211/8	APNIC - Pacific Rim	Jun 96
212/8	RIPE NCC - Europe	Oct 97
213/8	RIPE NCC - Europe	Mar 99

214/8	US-DOD	Mar 98
215/8	US-DOD	Mar 98
216/8	ARIN - North America	Apr 98
217/8	RIPE NCC - Europe	Jun 00
218/8	APNIC - Pacific Rim	Dec 00
219-223/8	IANA - Reserved	Sep 81
224-239/8	IANA - Multicast	Sep 81
240-255/8	IANA - Reserved	Sep 81

(last updated May 11 2001)