



IPV6:
Övergångsmekanismer och relaterade
säkerhetsproblem

Examensarbete inom huvudområdet Datalogi
Grundnivå 15 högskolepoäng
Vårtermin 2014

Dorian Mandic

Handledare: Joe Steinhauer
Examinator: Göran Falkman

Sammanfattning

I januari 2011 delades de två sista fria IPv4-adressblocken ut av Internet Assigned Numbers Authority (IANA) till den asiatiska Internetregistratorn Apnic (Asia Pacific Network Information Centre). Detta innebär att adresserna som fanns i den centrala adresspoolen nu är slut. Registratorn hade ansökt om dessa adressblock eftersom det råder akut brist på Internet Protocol version 4- (IPv4-adresser) i Asien samtidigt som Internetanvändarna i denna del av världen ökar explosionsartat (Magnusson, 2011a). Apnic delar ut adresser i Asien och Stilla havsregionen.

Det begränsade adressutrymmet har lett till en ökad användning av Network Address Translation (NAT) för att lösa problemet med adressbristen i IPv4-protokollet (Das, 2008a). För att istället bemöta detta problem med en mer långsiktig lösning, utvecklades Internetprotokollet Internet Protocol version 6 (IPv6) med ändamålet att helt ersätta IPv4-protokollet (Das, 2008b).

I Sverige hade regeringen som mål att samtliga svenska myndigheter skulle ha infört IPv6 senast år 2013. Trots detta föredrar idag fortfarande många myndigheter IPv4-protokollet framför IPv6 i de grundläggande tjänsterna. Med de grundläggande tjänsterna menas extern webbplats, Domain Name System (DNS) och e-post kommunikation (PTS, 2013).

Anledningen till denna måluppsättning är att regeringen vill att myndigheternas e-tjänster ska vara framtidssäkrade och nåbara med IPv6. Post och telestyrelsen (PTS) har fått i uppdrag att följa hur det går med införandet av IPv6 (PTS, 2013). Utvecklingen tycks inte ha skett i den takt som regeringen önskat och idag står 22 % av alla myndigheter fortfarande helt utan IPv6 (PTS E-tjänster, 2013).

IPv6 för med sig inbyggd säkerhet som t.ex. Internet Protocol Security (IPSec) men också nya säkerhetsproblem (Magnusson, 2011b). Rapporten behandlar de säkerhetsproblem som kan uppstå vid olika övergångsmekanismer och kommer även att beröra de problem som kan uppstå vid en samexistens av IPv6 och IPv4.

Rapporten visar på nya resultat som att ämnet övergångsmekanismer med relaterade säkerhetsproblem är ett oerhört känsligt ämne för många administratörer i branschen. Kännedomen om kategoriseringen för övergångsmekanismerna var överraskande bra. Rapporten avslöjar även att majoriteten av undersökta organisationer har blivit negativt påverkade vid en övergång till IPv6.

Nyckelord: IPv4, IPv6, Övergång, Problem

Ordlista

Application Level Gateway (ALG) – En ALG är en avancerad teknik för paketfiltrering och förstärker en brandvägg eller NAT i ett nätverk.

Application Programming Interface (API) – En samling av regler för hur en applikation kan kommunicera med en annan applikation.

Denial of Service (Dos/DDos) – En DoS-attack är en riktad attack mot ett nätverk med syftet att hindra normal användning av tjänster i nätverket. Distribuerad DoS-attack är när flera datorer tas över och används för att attackera ett nätverk med samma syfte som en DoS-attack.

Hop – Ett paket gör ett hopp när den vidarebefordras från en router till nästa router.

Ingress Filtering – Är en teknik som används för att säkerställa att inkommande paket är faktiskt från den källan de påstår sig vara ifrån.

Mask (worm) – En mask är en skadlig datorprogramvara som kan replikera sig själv för att sprida sig till andra datorer.

Neighbor Discovery Protocol (NDP) – Ett protokoll som används tillsammans med IPv6-protokollet för autokonfiguration av adresser för klienter och för att upptäcka andra datorer.

Next hop – En term som används för routing och syftar på den nästa router som paketen ska vidarebefordras till på vägen till slutdestinationen.

Socket Application Programming Interface (API) – En socket API är ett programmeringsgränssnitt som förses av operativsystem och tillåter ett program att kontrollera nätverkssocket. En nätverkssocket är en slutpunkt för kommunikationsflödet mellan processer i ett nätverk. En socket adress är en kombination av en IP-adress och ett portnummer.

Spoofing – I detta fall en IP-adress förfalskning där man använder en annan avsändar-IP-adress för att dölja källan. Används ofta i DoS-attacker.

User Datagram Protocol (UDP) – UDP är ett förbindelseöst protokoll som opererar i transportlagret i TCP/IP-modellen. Förbindelseöst innebär att ingen anslutning etableras mellan sändare och mottagare innan paket skickas.

Internet Protocol Security (IPSec) – Används för att säkra IP-kommunikation genom att erbjuda autentisering och kryptering. Protokollet opererar på Internetlagret i TCP/IP-modellen.

Innehållsförteckning

1	Introduktion	1
1.1	Avgränsningar	1
2	Bakgrund	2
2.1	Nätverk	2
2.2	TCP/IP	3
2.3	IPv4	4
2.3.1	IPv4-adressering	5
2.3.2	Subnätverk (Subnät)	5
2.3.3	NAT	6
2.3.4	IPv4 Paketstruktur	6
2.3.5	Routing	7
2.4	Tunneling	7
2.5	IPv6	8
2.5.1	IPv6-adressering	8
2.5.2	IPv6-header	10
2.5.3	ICMPv6	11
2.5.4	Auto-configuration	11
2.5.5	IPv6-adresser med inbyggda IPv4-adresser	11
2.6	Informationssäkerhet	12
3	Övergångsmekanismer	13
3.1	Dual Stack (Dubbla lager)	13
3.2	Tunneling som övergångsmekanism (Inkapsling)	13
3.2.1	6over4	14
3.2.2	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)	14
3.2.3	6to4	14
3.2.4	Teredo (Tunneling IPv6 over UDP through NAT)	15
3.3	Translation (Översättningsteknik)	15
3.3.1	Stateless IP/ICMP Translation	15
3.3.2	NAT-PT	15
3.3.3	Bump-in-the-Host (BIH)	16
3.4	Jämförelse av övergångsmekanismer	16
3.4.1	Dual Stack	16
3.4.2	Tunneling	17
3.4.3	Translation	17
3.5	Relaterande arbeten	17
4	Problem	19
4.1	Formulering av problem	19
5	Metod och Genomförande	21
5.1	Metod	21
5.1.1	Delmål 1	21
5.1.2	Delmål 2	21
5.1.3	Delmål 3	22
5.1.4	Delmål 4	22
5.1.5	Delmål 5	22

5.2 Genomförande	22
5.2.1 Delmål 1	22
5.2.2 Delmål 2, 3 och 4.....	22
5.2.3 Delmål 5.....	23
6 Resultat och Analys	24
6.1 Identifierade säkerhetsproblem för delmål 1	24
6.1.1 Dual Stack och säkerhetsproblem	24
6.1.2 Tunneling och säkerhetsproblem.....	24
6.1.3 Translation och säkerhetsproblem.....	26
6.1.4 Samexistensen mellan IPv4 och IPv6 och relaterade problem.....	26
6.2 Enkät för delmål 2, 3 och 4	27
6.2.1 Enkät Del 1	28
6.2.2 Enkät Del 2.....	30
6.2.3 Enkät del 3	34
6.3 Sammanfattning Enkät	39
6.4 Intervju för delmål 3	41
6.5 Analys	42
6.5.1 Bakgrund och erfarenhetsanalys del 1 onlineenkät.....	43
6.5.2 Sammanfattande analys	43
7 Slutsats	45
7.1 Slutsats och delmål	45
7.1.1 Delmål 1	45
7.1.2 Delmål 2.....	45
7.1.3 Delmål 3.....	45
7.1.4 Delmål 4.....	46
7.1.5 Delmål 5.....	46
7.1.6 Sammanfattning	46
8 Diskussion	47
8.1 Framtida arbeten	48

Appendix A Onlineenkät

Appendix B Enkätinbjudan

Appendix C Enkätdata

1 Introduktion

Internet Protocol (IP) är ett protokoll som är designat för att användas i sammankopplade system av paketbaserade kommunikationsnätverk, som t.ex. Internet. Datorer och andra kommunicerande enheter som ansluts till Internet, behöver en egen unik adress för att kunna kommunicera med varandra. (IETF, 1981a).

Den dominerande versionen idag är IPv4-adressen, vilket är den unika adress som tilldelas en enhet innan för att den ska kunna kommunicera. En enhet idag kan vara t.ex. en dator eller router. Allt fler datorer idag kopplar upp sig mot Internet men även mobiltelefoner och surfplattor är ett exempel på enheter, som bidrar till den rådande adressbristen. IPv6-protokollet utvecklades för att helt ersätta IPv4 och för att stödja den expanderande Internetanvändningen och funktionaliteten, men även för att förbättra säkerheten för information, som skickas över Internet (Das, 2008b). Trots sin överlägsenhet med adressutrymmet har inte IPv6 fått det genombrott som var förväntat. En anledning till detta kan vara att det fortfarande idag används enheter (routrar, switchar, datorer), som inte har stöd för IPv6-protokollet. En annan anledning kan vara att IPv6 inte är bakåtkompatibelt med IPv4, vilket innebär att delar av nätverk kan behöva struktureras om vid en eventuell övergång (Lewis & Che, 2010).

Vidare är tjänsten NAT en bidragande orsak till den förlängda livslängden för IPv4. Samtidigt har NAT tillsammans med IPv4 dålig inverkan på applikationer som t.ex. (Voice over Internet Protocol) VoIP. NAT som en extra tillagd komponent i ett IPv4-nätverk, kan orsaka latens för t.ex. videosamtal (Lewis & Che, 2010). En övergång från IPv4 till IPv6 är inget som oftast sker på kort sikt utan är ofta en långvarig process med olika övergångsmekanismer som t.ex. Dual Stack, vilket gör att frågor om säkerhet som rör övergångsmekanismer, kommer ständigt att vara en aktuell fråga (Davies, Krishnan & Savola 2007). Övergångsmekanismer som Dual Stack möjliggör att IPv6-enheter kan samexistera med IPv4-enheter och mekanismen är tänkt att underlätta en övergång men har dock visat sig vara utmanande gällande säkerhet (Gont, 2011). Syftet med detta arbete är att identifiera alla övergångsmekanismer med relaterade problem som de kan medföra och hur detta kan påverka en organisations informationssäkerhet. I sektion 2 presenteras de begrepp som ligger till grund och är viktigast för övergångsmekaniserna. Sektion 3 introducerar och beskriver övergångsmekanismer som denna rapport kommer att diskutera. Sektion 4 presenterar problemfrågeställning och problemformulering. Sektion 5 går igenom de metoder som används för att nå målen med rapportens problemundersökning. I sektion 6 beskrivs resultat och analys. I sektion 7 dras slutsatserna för resultaten och analysen.

1.1 Avgränsningar

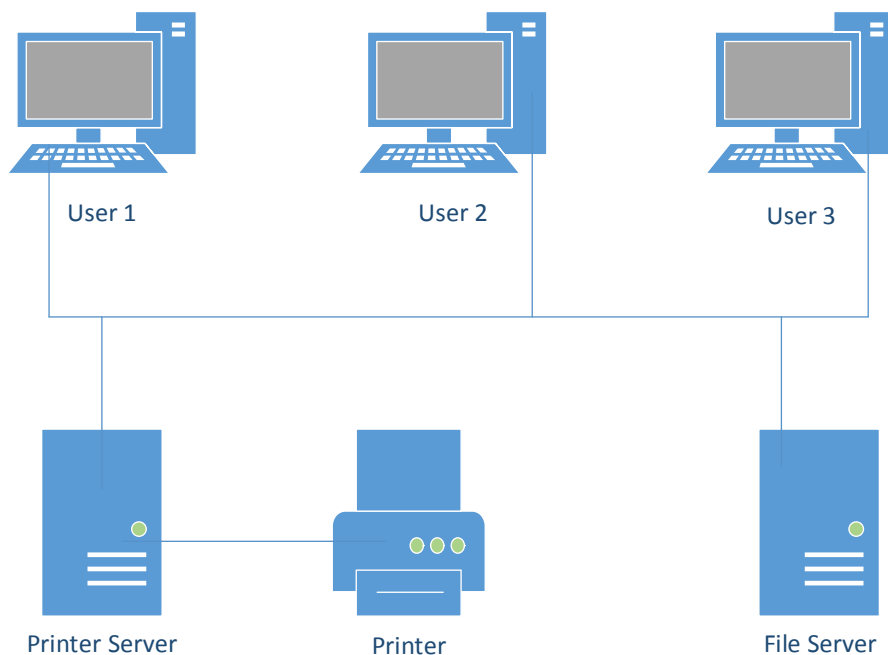
Detta arbete berör inte tekniska problem eller säkerhetsrisker gällande funktionerna som IPv6 medför. Arbetet berör heller inte någon aspekt gällande IPv6-protokollet som har med prestanda att göra. Arbetet berör endast övergångsmekanismer som de är kategoriserade i detta arbete. Fokus ligger istället på säkerhetsproblem vid övergångsmekanismer som kan resultera i t.ex. brandväggsstöd för IPv6, paketförfalskning och DoS-attacker, där ett fåtal tekniker har valts ut för respektive övergångsmekanism. Anledningen till att endast ett fåtal tekniker har valts är att det finns väldigt många tekniker och en begränsning var tvungen att göras på grund av tidsbrist.

2 Bakgrund

Denna sektion beskriver funktionaliteten och uppbyggnaden av IPv4 och IPv6 med relaterade protokoll. Sektionen sammanfattar relevant information för dessa protokoll och ger insikt i vad dessa protokoll är för något och har för funktion. Andra protokoll som har ett samband med ämnet, kommer också att beskrivas för att underlätta förståelsen för ämnet som berörs. Det förekommer begrepp i detta arbete som inte beskrivs i bakgrundssektionen. Förklaring för dessa begrepp finns i ordlistan innan innehållsförteckningen. Begreppen är framöver kursiverade. De som redan har goda kunskaper gällande datakommunikation och IPv6-protokollet, kan istället starta från sektion 2.6, informationssäkerhet om så önskas.

2.1 Nätverk

Ett nätverk består av två eller fler kommunicerande datorer och andra enheter som t.ex. routrar. Antalet värdar och hur de kommunicerar definierar vad för typ av nätverk det är. Local Area Network (LAN) är ett nätverk som täcker ett litet avstånd och ryms vanligtvis inom en byggnad. Ett LAN kan bestå av ca 100 användare som delar data, program, printar samt åtkomst till servertjänster som t.ex. dedikerad filserver (Pfleeger & Pfleeger, 2006). Figur 1 illustrerar ett typiskt LAN.



Figur 1 LAN enligt (Pfleeger & Pfleeger, 2006).

Ett Wide Area Network (WAN) skiljer sig i både storlek och avstånd från ett LAN. Den täcker ett område geografiskt och kan sträcka sig över flera byggnader, städer och länder.

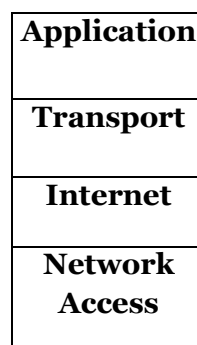
Internet är en sammankoppling av två eller flera publika separata nätverk där varje nätverk kontrolleras och hanteras separat (Pfleeger & Pfleeger, 2006).

För att datorer ska kunna kommunicera och förstå varandra, används protokoll för att kommunikationen ska lyckas. Ett protokoll ger en bild av en samling av regler för kodning och avkodning gällande data, så att kommunicerande datorer kan förstå varandra

(SecurityFocus, 2010). Protokoll möjliggör för data att kunna färdas över olika typer av medium som t.ex. kopparkabel, optisk fiber eller mikrovågor och kan separeras från mediet (kabeln) vilket innebär att datakommunikationen inte är beroende av mediet. Protokoll gör det även möjligt för användare att modellera kommunikationen enligt en protokollstack Ett protokollstack är en lagerbaserad modell för kommunikation där varje lager i stacken är som ett språk för entydig kommunikation, som är relevant för varje lager (Pfleeger & Pfleeger, 2006). Protokollstacken beskrivs mer utförligt i nästa sektion.

2.2 TCP/IP

En protokollstack är en schematisk arkitektur avsedd för datakommunikation över datanätverk. Stacken är en lagerbaserad arkitektur där olika typer av protokoll delas in i olika lager och öppnar för kommunikation mellan applikationer. Transmission Control Protocol/Internet Protocol (TCP/IP) är den protokollstack, som idag är vanligast och används mest för WAN-kommunikation. Protokollstacken är enbart avbildning av hur nätverksproceduren fungerar. Modellen beskriver inte ett fysiskt verkligt nätverk. (Pfleeger & Pfleeger, 2006). TCP/IP-protokollstacken består av fyra lager: applikationslagret, transportlagret, internetlagret och det fysiska åtkomstlagret. Figur 2 nedan illustrerar TCP/IP modellen.



Figur 2 TCP/IP Protokollstack

Även om TCP/IP används som ett ord eller en beteckning så betecknar den egentligen två olika protokoll: TCP och IP. (Pfleeger & Pfleeger, 2006). TCP opererar på transportlagret och är ett förbindelse-orienterat protokoll för dataöverföring mellan två värdar över Internet (Cisco, 2005). Förbindelse-orienterat innebär en mer tillförlitlig kommunikation där en anslutning mellan två värdar först skapas, innan data i form av olika paket skickas. Denna typ av förbindelse garanterar även att paketen anländer i rätt ordning efter varandra. Om några av paketen går förlorade på vägen, skickar TCP de förlorade paketen igen tills de har nått sitt mål eller en time-out uppstår (IETF, 1981b).

I applikationslagret opererar protokoll som t.ex. Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP) och Domain Name System (DNS). SMTP är ett kommunikationsprotokoll och används för leverans av e-post. FTP används vid överföring av filer. DNS används för att översätta en IP-adress till domännamn eller tvärtom. Ett exempel är om man besöker sidan www.exempel.com som har IP-adressen (192.0.4.35). Istället för att behöva memorera och skriva IP-adressen till sidan man besöker, kan användaren skriva domännamnet istället, som sedan översätts till IP-adress av DNS-servern. HTTP är ett kommunikationsprotokoll som används till att överföra webbsidor på Internet (Cisco, 2009).

Nätverksåtkomstlagret specificerar hur data överförs fysiskt till ett medium som t.ex. kopparkabel eller trådlöst. Om man tittar på själva sändningsprocessen för protokollstacken så startar den i applikationslagret, där HTTP-protokollet skickar en webbsida till transportlagret. I transportlagret bryts applikationsdata ner i olika TCP-segment.

Transportlagret kapslar in webbsidans data i segmentet och skickar dessa vidare till Internetlagret. Här implementeras IP-protokollet och hela TCP-segmentet kapslas in i ett IP-paket där en IP-header skapas. Header beskrivs mer utförligt i sektion 2.3.2. IP-header innehåller avsändarens och destinationens IP-adresser, samt information som behövs för leverans av paket till sin motsvarande destinationsprocess (Cisco, 2009).

När IP-paketet slutligen når nätverksåtkomstlagret kapslas den in igen fast med en frame-header och en trailer. Frame-headern innehåller den fysiska avsändar- och destinationsadressen, som t.ex. MAC-adressen (Media Access Control). MAC-adressen är en unik adress för nätverkskort hos t.ex. datorer. Denna adress identifierar enheter på det lokala nätverket. Trailern innehåller kontrollinformation för eventuella fel (Cisco, 2009).

Efter inkapslingen kodas bitarna av ett paket på media dvs. på kabeln från nätverkskortet. Processen går omvänt när bitarna når slutdestinationen i nätverksåtkomstlagret, där avkapsling sker från lager till lager i protokollstacken tills data når applikationslagret (Cisco, 2009).

IP-protokollet opererar endast i Internetlagret. I IP-protokollet specificeras två viktiga funktioner, adressering och fragmentering. Adressering innebär att paketen skickas med information om uppgifter rörande t.ex. avsändar- och mottagaradress i form av IP-adresser (Cisco, 2009).

Fragmentering innebär att avsändaren kan dela upp paket i mindre bitar (fragment) om paketet har större storlek än destinationens MTU (Maximum Transmission Unit). Med hjälp av information sätts fragmenten samman igen av måldatorn. Detta protokoll ser till att meddelandet kommer till rätt måldator men garanterar inte att paketen når måldatorn (IETF, 1981b). Ansvar för detta återfinns istället hos TCP-protokollet på transportlagret. De versioner som används idag är IPv4 och IPv6 där IPv4 fortfarande är den version som dominerar (Halsall, 2005).

2.3 IPv4

Varje enhet som kommunicerar över Internet behöver en unik IP-adress. IPv4 är den protokollstandard som idag dominerar Internet och används i större utsträckning. (Comer, 2014). Det är ett ca 30 år gammalt protokoll som specificerades och publicerades 1981 i RFC-791 (Request For Comments). Protokollet har inte förändrats mycket och har till en början visat sig vara stabilt och skalbart för Internet (Parkhurst, 2004). Men tyvärr har den explosionsartade tillväxten av Internet bidragit till behovet av fler adresser, speciellt i befolkningstäta länder som Indien och Kina, vilket har lett till att det behövs fler IP-adresser än vad IPv4 kan leverera (Das, 2008b). Adressbristen beror även på andra enheter än datorer som det senaste årtiondet också har börjat kräva IP-adresser. Exempel på sådana enheter är mobiltelefoner och fordon av olika slag, som kan kopplas till Internet och därmed behöver en unik IP-adress (Parkhurst, 2004).

2.3.1 IPv4-adressering

En IPv4-adress är 32 bitar stor vilket är detsamma som fyra bytes (en byte per oktett) och ger maximalt ett antal av 4 294 967 296 IP-adresser (Parkhurst, 2004). IPv4-adressen skrivs vanligtvis i decimalform med punkter emellan. Varje siffergrupp motsvarar en byte vilket är samma som åtta bits. Åtta bits multiplicerat med alla fyra siffergrupper blir 32 bits, vilket gör en IPv4-adress 32 bitar stor. IP-adresser är för människor lättare att förstå i decimalform än binära tal. Datorer förstår bara binära tal dvs. ettor och nollor (Halsall, 2005). Figur 3 illustrerar strukturen av en IPv4-adress i decimal form och binärt.

Decimal form	172.16.254.1
Binär form	10101100.00010000.11111110.00000000

Figur 3 Struktur för IPv4-adress

En viktig aspekt att nämna i denna rapport är de lokala IP-adresserna som används i ett LAN. Många adresser, däribland de lokala, är reserverade för lokala nätverk av IANA och går inte att använda på Internet. För att nå Internet från ett LAN, används NAT för att översätta den privata adressen till en publik adress. Det är viktigt eftersom NAT är en av de bidragande och möjligen största orsaken genom ökad användning, till varför övergången till IPv6 dröjer och kommer att diskuteras mycket i rapporten (Das, 2008a).

De IPv4 adresser som är reserverade för lokala nätverk är följande:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

2.3.2 Subnätverk (Subnät)

Ett subnät är ett sätt att logiskt dela upp ett nätverk i mindre delar. Att dela upp ett nätverk i två eller fler nätverk kallas subnetting. Ett nätverk som är baserat på IP delas in i olika klasser där A-klassen är störst. Ett klass A-nätverk rymmer 16 777 216 adresser, dvs. 2^{24} adresser där adressen börjar med 0.0.0.0 och slutar på 127.255.255.255 (Halsall, 2005). Det finns få organisationer som är i behov av så många adresser, vilket resulterar i ett slöseri med användbara adresser.

Ett klass B-nätverk har ett IP-intervall från 128.0.0.0 - 191.255.255.255 och rymmer 65,536 adresser per nätverk. Klass C som är den sista som används, använder 192.0.0.0 - 223.255.255.255. Denna klass öppnar för 256 tillgängliga adresser för ett nätverk.

Det klassfulla systemet används inte längre idag utan det klasslösa systemet Classless Inter-Domain Routing (CIDR) används istället för att tolka IP-adresser. Systemet är effektivt vid uppdelning av stora nätverk till mindre nätverk. Därmed uppnås en mer effektiv användning av adresserna för IPv4 och ett nätverk kan göras mer skalbart genom att dela upp nätverket i olika hierarkier vid adresstilldelning (Halsall, 2005).

En subnet-mask, även kallat nätmask, används för att tala om vilket nätverk en IPv4-adress tillhör genom att visa var nätverksadressen i en IP-adress slutar och var värdadresserna

börjar (Halsall, 2005). Subnätverk för IPv4 diskuteras inte mer i detalj eftersom rapporten fokuserar på IPv6-protokollet och övergångsmekanismer.

2.3.3 NAT

NAT är en teknik som går ut på att ändra adressinformationen för IP-adressen i ett IP-pakets header. Tekniken anses vara en temporär lösning till problemet med adressbristen hos IPv4-protokollet. Den minimerar problemet med adressbristen genom att mappa en privat IPv4-adress med en publik IPv4-adress eller tvärtom. IPv4-adresserna lagras i en översättningstabell i routern. Detta innebär att en användare som sitter i ett lokalt nätverk och har en privat IP-adress tilldelad, kan ansluta till Internet genom att få en publik IPv4-adress istället (Comer, 2014).

NAT fick en stor genomslagskraft eftersom tekniken visade sig vara effektiv i att sakta ner tömningen av de publika IPv4-adresserna. Genom NAT sparas fler adresser eftersom en eller fler publika adresser kan användas till en privat adress. De privata adresserna som har diskuterats i sektion 2.3.1, används av datorer och andra enheter som kommunicerar lokalt i ett LAN. Där får varje enhet en unik privat adress medan samma enhet på andra sidan routern mot Internet, istället har en publik adress vid kommunikation med andra enheter (Hagen, 2006).

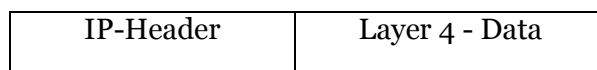
Nackdelen med denna teknik är att den har en negativ inverkan på trafik som baseras på från värd till värd (dator till dator). Datorn i det lokala nätverket ser bara routern med NAT-tjänsten och inte bortom den, medan måldatorn på andra sidan routern, enbart ser den publika adressen och inte den privata. Detta kan innebära problem för tjänster som IP-telefoni och videokonferenser där dessa är beroende av en komplett anslutning mellan två värdar.

Ett exempel på detta inom IP-telefoni är där två parter upprättar en anslutning genom en server för att sedan utbyta datapaket med varandra. Problemet är att servern måste tala om för båda parter hur och var paketen skall skickas emellan dem. Detta måste då vara den publika adress och inte den privata som parterna från början innehar (Cho & Bae, 2010).

NAT löser inte problemet med adressbristen helt utan är enbart en tillfällig lösning. Övergången till IPv6 kommer att resultera i att alla enheter som ansluts till Internet, kan få en egen unik IP-adress vilket troligtvis kommer att minimera eller helt eliminera behovet av NAT (Cho & Bae, 2010).

2.3.4 IPv4 Paketstruktur

Ett IPv4-paket (IP-datagram) består av två sektioner: en header och en datasektion. Datasektionen som normalt kommer från transportlagret, kapslas in av IP-paketet där IP-paketet lägger till sin egen header-information. Denna inkapslade data kallas för IP-payload (Comer, 2014). Figur 4 nedan illustrerar ett IP-paket.



Figur 4 IP-paket enligt (Comer, 2014)

EN IP-header består av fjorton fält där tretton används. Fjortonde fältet är valfritt och val för olika alternativ. De övriga tretton fälten granskas av främst routrar och datorer för trafik. Figur 5 nedan illustrerar en IPv4-header (Comer, 2014).

+	Bits 0 - 3	4 - 7	8 - 15	16 - 18	19 - 31
0	Version	Header Length	Type of Service	Total Length	
32	Identification			Flags	Fragment Offset
64	Time to Live		Protocol	Header Checksum	
96	Source Adress				
128	Destination Adress				
160	Options				

Figur 5 IPv4-header enligt (IETF, 1981a)

Exempel på hur fält granskas är time to live-fältet (TTL). TTL-fältet hjälper till att förhindra så att inte IP-paketet hamnar i en evig loop ute på Internet. Ett paket kan behöva göra flera hopp mellan olika routrar innan det når sin slutdestination. För varje hopp som görs minskar routern TTL-fältets värde med 1. Om fältet får värdet 0 innan det når sin slutdestination, kastas paketet bort av routern och ett felmeddelande skickas tillbaka till källan (Comer, 2014).

2.3.5 Routing

Routing är en process som innebär att välja de bästa vägarna i ett nätverk. En router är en enhet som befinner sig mellan nätverk eller kopplar samman två eller fler nätverk. Routern dirigerar/vidarebefordrar datapaketerna tills de når sin slutdestination. Olika paket med samma meddelande kan färdas olika rutter beroende på mängden trafik. Routern används även i större anläggningar där en mängd lokala nätverk kräver routingfunktion. Routern läser av en IP-header för att avgöra källadress samt destination och för att fastställa den bästa vägen för vidarebefordring av paket. Den är även den enhet som oftast sköter NAT-funktionen (Halsall, 2005).

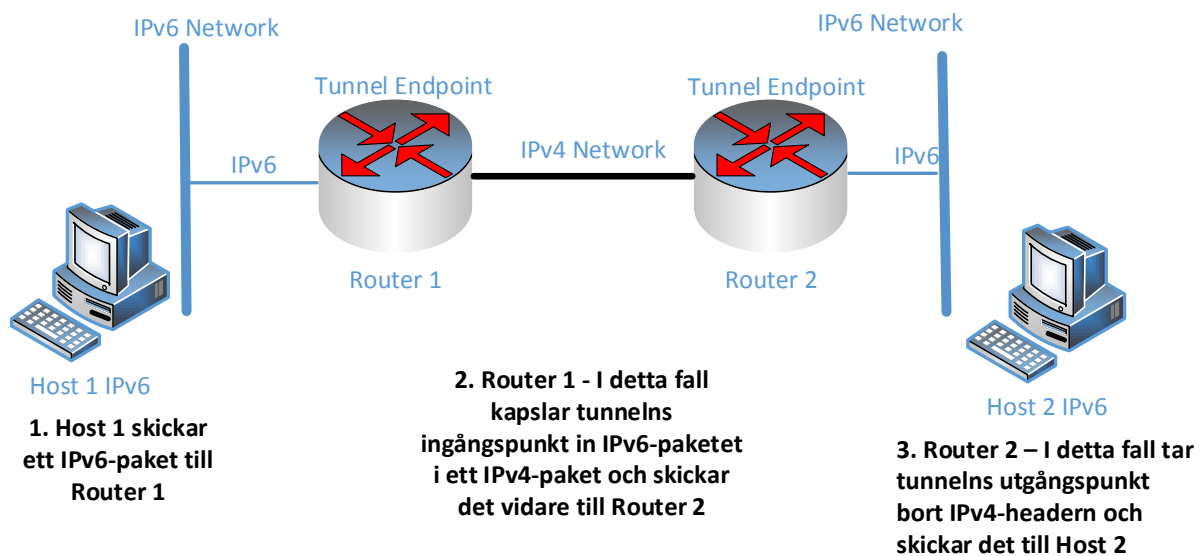
2.4 Tunneling

En tunnel är ett kommunikationssätt som genom en kommunikationskanal kan koppla samman två eller fler olika nätverk. Det är i princip en extra IP-inkapsling. Med hjälp av tunnling kan data föras över ett nätverk som är inkompatibelt för leverans eller över nätverk som inte är tillförlitliga (Amoss & Minoli, 2008).

Tunneln har slutpunkter där en punkt ses som en ingångspunkt eller utgångspunkt. Routrar är de enheter i ett nätverk som oftast används som slutpunkter (Hagen, 2006). Tunnlarna kan antingen vara manuellt konfigurerade eller automatiska. En manuellt konfigurerad tunnel är en punkt till punkt tunnel som även har möjligheter att säkras med protokoll som t.ex. *IPSec*. Här kapslas hela IPv6-paket in i IPv4-paket som sedan färdas över ett IPv4-baserat nätverk (Hagen, 2006).

Automatiska tunnlarna är de som denna rapport kommer fokusera på eftersom de öppnar för användning av olika typer av adresstekniker som t.ex. Teredo och möjliggör transport över en

dynamisk tunnel, för att skicka IPv6-paket över IPv4-baserade nätverk. Figur 6 nedan illustrerar hur tunnling fungerar enligt Hagen, (2006).



Figur 6 Tunnling, texten i bilden är direkt översatt från (Hagen, 2006 s. 257)

2.5 IPv6

Användningsområdet för Internet har till mitten av 1990-talet varit begränsat till t.ex. universitet och statliga myndigheter. Halsall (2005) hävdar att ökad uppmärksamhet för webben (WWW) sedan dess har orsakat en enastående ökning av Internetanvändningen. Ett resultat av detta är att de flesta hem, skolor och olika organisationer idag är anslutna till Internet (Halsall, 2005). Utöver detta har tillväxten tilltagit ytterligare genom nya framtagna applikationer, som i sin tur stödjer Internetanslutningen även för mobiltelefoner, fordon av olika slag och t.ex. TV-apparater (Halsall, 2005). Detta är en bidragande orsak till adressbristen för IPv4 och som ett svar till Internets kraftfulla expansion, utvecklades IPv6-protokollet och publicerades i RFC 2460 (Das, 2008b).

2.5.1 IPv6-adressering

IPv6 är en standardiserad lösning som är framtagen främst för att lösa begränsningarna med adressutrymmet hos IPv4. Eftersom IPv6 stödjer en adresslängd på 128 bitar (16 bytes), kan den definiera upp till 2^{128} adresser som motsvarar 340 282 366 920 938 463 374 607 431 768 211 456 adresser eller 6.65×10^{23} , vilket innebär ca 340,3 sextiljoner adresser (Comer, 2014). Detta innebär b.l.a. att tjänster som NAT inte längre skulle behöva användas. Adresslängden separeras normalt med kolon i åtta grupper (16 bitar per grupp) och noteras med hexadecimala tecken (Hagen, 2006). Nedan visas ett exempel på en IPv6-adress:

2001:DB8:0000:0000:0202:B3FF:FE1E:8329

Adressen kan förkortas genom att ta bort grupperna med enbart nollor för att istället skriva ihop adressen med två kolon utan nollor och göra adressen mer läsbar för användare (Hagen, 2006):

2001:DB8::202:B3FF:FE1E:8329

De hexadecimala tecken som används, räknas från 0 till F. Siffran 10 övergår i A, 11 blir B och så här fortsätter det tills F nås. Precis som med IPv4-adresser läser man av adressen från vänster. (Amoss & Minoli, 2008).

Precis som med IPv4-adresser kan man med IPv6-adresser dela upp ett nätverk i mindre subnätverk (subnät). En IPv6-adress avslutas ofta med ett snedstreck följt av ett prefix, som specificerar hur många bitar från vänster i adressen identifierar subnätet (Hagen, 2006).

2001:DB8::56/32

Snedstreckets i exemplet ovan är ett prefix följt av siffran 32 vilket innebär att de 32 första bitarna subnätet identifieras, alltså 2001:DB8. De bitar som återstår tillhör en enhet i nätverket (Amoss & Minoli, 2008). Routrar använder sig av denna information vid vidarebefordring av paket (Hagen, 2006).

IPv6-adresser klassificeras i 3 olika kategorier efter t.ex. routingmetoder som är vanliga i nätverk (Hagen, 2006).

Unicast – En unicast-adress identifierar ett enskilt nätverksgränssnitt (interface) på en IPv6-enhet. Ett paket som skickats till en unicast-adress, levereras till ett specifikt gränssnitt för den adressen (Hagen, 2006).

Multicast – En multicast-adress identifierar en grupp av IPv6-enheter. Ett paket som skickas till en multicast-adress, levereras till alla gränssnitt som anslutit sig till multicast-gruppen (Hagen, 2006).

Anycast – En anycast-adress tilldelas till en grupp av gränssnitt som tillhör flera olika enheter. Ett paket som skickats till en unicast-adress levereras oftast till den värden i gruppen som routern bedömer som närmast (Halsall, 2005).

En IPv6-adress består av 128 bitar. Beroende på vilket adressformat det handlar om (unicast, multicast), delas dessa 128 bitar upp logiskt i grupper av bitar, där regler skapas för att sammankoppla värden för varje grupp med adresseringsfunktioner.

Ett exempel på detta är unicast eller anycast-adresser som delas upp logiskt i två delar, en 64-bitars nätverksprefix för routing och en 64-bitars del som används för att identifiera ett nätverksgränssnitt för en värd. Figur 7 nedan illustrerar ett unicast adressformat (Comer, 2014).

bitar	48 (eller fler)	16 (eller lägre)	64
fält	Routing prefix	Subnät ID	Identifierare för gränssnitt

Figur 7 Adressformat för unicast enligt (Comer, 2014)

I detta format delas IPv6-adressen in i tre delar. Routing-prefixet identifierar nätverket. Subnät ID används för att skilja mellan flera olika nätverk. Storleken för routing prefix kan variera beroende längden för prefixet. En större prefixstorlek innebär en mindre subnet ID

storlek. Identifierare för gränssnitt innebär identifikation av en särskild enhet t.ex. dator som är ansluten till den aktuella delen av nätverket (Comer, 2014).

2.5.2 IPv6-header

Precis som med IPv4 är en IPv6-headern den delen som börjar i ett paket där paketet består av en header och en datasektion. Paketstrukturen är dock förändrad sen IPv4 där headern b.l.a. är mindre än den i IPv4. Detta medför att routern kan lättare processa varje paket. Routern har dessutom ett mindre antal fält att analysera i en IPv6-header än en IPv4-header. Fem fält som fanns i IPv4-headern har tagits bort i IPv6-headern. De fält som tagits bort är: *Header Length*, *Identification*, *Flags*, *Fragment Offset* och *Header Checksum* (Hagen, 2006).

Header Length har tagits bort eftersom en IPv6-header är fixerad till skillnad från IPv4-headern och är inte nödvändig. IPv4 har ett extra fält för alternativ, vilket är omnämnt tidigare i denna rapport. Om alternativ information läggs till, utökas headerns storlek i ett IPv4-paket. *Identification*, *Flags*, och *Fragment Offset* används vid fragmentering av paket i IPv4-headern. Fragmentering har diskuterats i sektion 2.2. Hagen (2006) hävdar att fragmentering är en ineffektiv process och routrar som har IPv6, hanterar inte fragmentering för paket i en kommunikationslina som med IPv4. Istället används andra funktioner som t.ex. *Extension Header* för detta, vilket inte diskuteras och är inte relevant för denna rapport. *Header Checksum* togs bort för att förbättra routerns hastighet med att analysera IP-paket. Hagen (2006) hävdar att om routern slipper kontrollera eller uppdatera en checksum dvs. kontrollera fel i data, ökar routerns prestanda. Figur 8 nedan illustrerar en IPv6-header.

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

Figur 8 IPv6-header enligt (Comer, 2014)

Versionsfältet indikerar vilken version IP-protokollet har, som i detta fall är 6. Dock har detta fält routern ingen användning för utan den skiljer på versionerna i lager 2-inkapslingen. Fältet för källadressen talar om vilken avsändarenhet IP-paketet kommer från. Fältet för destinationsadressen innehåller IPv6-adressen för den avsedda mottagaren (Das, 2008c).

Det kan finnas paketflöden mellan en källa och destination. Flow Label används av källan för att märka en del paket som talar om att de tillhör samma flöde. Traffic Class-fältet används för att skilja på paket för leverans genom att prioritera leveranserna olika för olika paket. Routrarna kan då identifiera paket med samma trafikklass och skilja på paket med olika prioriteringar. Payload-fältet innehåller data i form av information. Om datan överskrider gränsen för längden i detta fält, förses paketet istället med en payload extension header som utökar längden för fältet (Das, 2008c).

Next Header identifierar nästkommande header som specificerar protokoll för transportlagret, vanligtvis TCP och User Datagram Protocol (UDP). Hop Limit är fältet där värdet för detta fält minskas med 1 varje gång en enhet, som t.ex. en router vidarebefordrar ett paket. Om detta fälts värde slår om till 0 innan paketet når sin destination, kastas paketet bort. Syftet med detta fält är att paketen inte ska hamna i en evig loop (Das, 2008c). Om paketet kastas, skickas ett felmeddelande med protokollet Internet Control Message Protocol (ICMP), vilket i detta fall är ICMPv6.

2.5.3 ICMPv6

I IPv4-nätverk används ICMP-protokollet av enheter som routrar eller datorer för att b.l.a. skicka felmeddelanden och diagnostisering av trafik och anslutning. Protokollet används av nätverksverktyg som Ping för att undersöka om enhet är nåbar eller inte (Comer, 2014). ICMPv6 är en version av ICMP-protokollet och utgör en väsentlig del av IPv6-arkitekturen där ICMPv6-meddelanden färdas inom ett IPv6-paket (Das, 2008d).

Version 6 skiljer sig lite från föregångaren i att det är mångsidigt protokoll som används för olika tjänster som t.ex. felrapportering för paket, diagnostisk verksamhet, processer för upptäckt av andra noder och rapportering för IPv6 multicast-medlemskap (Das, 2008d).

2.5.4 Auto-configuration

Enheter eller klienter i ett IPv4-nätverk har möjligheten att få sina IPv4-adresser automatiskt tilldelade när de kopplar upp sig mot nätverket. Tilldelningen sker från en Dynamic Host Configuration Protocol (DHCP) server varje gång enheten kopplar upp sig. Denna tilldelningsprocess kallas stateful auto-configuration. IPv6-protokollet har stöd för DHCPv6 och stödjer även stateful auto-configuration men även stateless auto-configuration för enheter. Stateless använder inte DHCP utan använder routern för att skapa egna unika adresser. På detta sätt underlättar stateless hantering av adresser för nätverksadministratörer (Govil et al. 2008).

2.5.5 IPv6-adresser med inbyggda IPv4-adresser

En övergång från IPv4 till IPv6 sker oftast gradvis och för att det ska vara möjligt med en övergång, har en liten del adresser i IPv6-adressutrymmet allokerats för att koda IPv4-adresser. Denna teknik används under en övergång med övergångsmekanismer av två anledningar. Först, en dator med en IPv4-adress tilldelad, ska ha möjlighet att uppgradera till IPv6-anpassad mjukvara innan den tilldelats en IPv6-adress istället (Comer, 2014).

Vidare ska en dator som kör applikationer med IPv6 kunna kommunicera med en enhet som endast använder applikationer med IPv4. Dock löser möjligheten med inbyggda IPv4-adresser fortfarande inte problemet med att försöka få de båda protokollen att fungera gemensamt med varandra, utan en översättning av adressformatet är nödvändig (Comer, 2014).

Det finns två typer av IPv6-adresser med inbyggda IPv4-adresser. Den första är en IPv4-kompatibel IPv6 där routern kan användas för att tunnla IPv6-paket över en infrastruktur för IPv4. Det andra alternativet är att mappa en IPv4-adress till en IPv6-adress. Detta alternativ gör att enheter med endast IPv4-adresser presenteras som IPv6-adresser. En IPv6-enhet kan använda sig av sådana adresser för att skicka paket till en enhet som endast stödjer IPv4-adressering (Hagen, 2006). Nedan visas ett exempel på en IPv4-kompatibel IPv6-adress:

0:0:0:0:0:0:172.130.10.10

Dessa varianter av adresser underlättar för de övergångsmekanismer som möjliggör IPv6-trafik över IPv4-strukturerade nätverk (Comer, 2014). Figur 9 nedan illustrerar formaten för IPv6-adresser med en inbyggd IPv4-adress.

IPv4-kompatibel IPv6-adress

0000 0000	0000	IPv4-adress
80 bitar	16 bitar	32 bitar

IPv4-mappad IPv6-adress

0000 0000	FFFF	IPv4-adress
80 bitar	16 bitar	32 bitar

Figur 9 Två varianter av IPv6 adressformat med en inbyggd IPv4-adress enligt (Comer, 2014)

2.6 Informationssäkerhet

Informationssäkerhet går ut på att skydda en organisations informationstillgångar som t.ex. hårdvaran och mjukvaran i nätverket. När man utövar informationssäkerhet inför man åtgärder med målet att göra informationen tillgänglig vid behov, förhindra förstörelse av information och skydd mot hot samt läckage. Det finns tre viktiga aspekter att beakta för att uppnå dessa mål (Pfleeger & Pfleeger, 2006).

Tillgänglighet – Innebär att information ska vara tillgänglig för alla som är behöriga för åtkomst och denna åtkomst skall inte förhindras (Pfleeger & Pfleeger, 2006).

Sekretess – Innebär att informationstillgångar är åtkomliga endast för de personer som är behöriga för att komma åt informationen (Pfleeger & Pfleeger, 2006).

Integritet – Innebär att informationstillgångar modifieras endast av de som har behörighet för detta. Modifiering innebär att skriva, ändra, radera eller skapa t.ex. information (Pfleeger & Pfleeger, 2006).

Enligt PTS (2011) ökar komplexiteten för ett nätverk vid ett införande av IPv6, där kostnaden ökar i takt med att nätverket kan växa. I ett sådant fall kan hårdvara och mjukvara behöva bytas ut. Även kraven för utbildning, säkerhet och tillgänglighet ökar, där säkerhetsarbetet vid en övergång blir en ständig process (PTS, 2011).

I samband med statliga myndigheter som förväntats redan ha gjort en fullskalig övergång, har en vägledning för införande av IPv6 utarbetats som stöd för en övergång till IPv6. Denna vägledning fokuserar på tillgänglighet, säkerhet och ekonomi (PTS, 2011). Vägledningen följer även grundpelarna för informationssäkerhet som är tillgänglighet, sekretess och integritet (Informationssäkerhet.se).

I detta arbete kommer säkerhetsproblem att identifieras som kan uppstå vid en övergång till IPv6, samt om dessa problem bryter mot något av målen för informationssäkerhet och hur detta påverkar organisationen i fråga.

3 Övergångsmekanismer

Denna sektion ger insikt i de övergångsmekanismer som idag är aktuella och som används mest. Det finns många övergångsmekanismer, dock diskuteras endast de som idag är mest vanliga i denna rapport.

IPv6 är inte bakåtkompatibelt med IPv4 och därför krävs övergångsmekanismer. En övergång till IPv6 kan pågå i flera år där IPv4 och IPv6-protokollet samexisterar, eftersom kommunikation till det idag spridna IPv4-protokollet fortfarande ska vara möjlig. Övergångsmekanismer kan medföra säkerhetsproblem då två protokoll samverkar och sårbarheter och hot från båda protokollen behöver beaktas. Övergångsteknikerna delas normalt in i tre olika huvudtyper: *Dual Stack*, *Tunneling* och *Translation* (Taib & Budiarto, 2007). Viktigt att känna till vid denna kategorisering av ovan nämnda övergångsmekanismer är att flera tekniker för varje kategori, kan användas tillsammans av t.ex. routern.

3.1 Dual Stack (Dubbla lager)

Dual Stack som innebär dubbla lager, är en teknik som tillåter att IPv4 och IPv6-protokollet kan samköras parallellt mellan olika enheter och nätverk (Amoss & Minoli, 2008). Detta innebär t.ex. att routrar kan hantera IPv4-paket och IPv6-paket samtidigt. Dock är förutsättningen att enhetens operativsystem måste ha stöd för båda protokollen. Moderna operativsystem som t.ex. *Windows 8* har inbyggt stöd för Dual Stack-arkitekturen (Palmer, 2012).

Dual Stack-mekanismen är den mekanism som idag är vanligast. Men denna mekanism gör det bara möjligt för applikationer att köra IPv6-IPv6 och IPv4-IPv4-kommunikation och tekniken utgör en grund för att även andra mekanismer ska kunna fungera. Ett exempel är tekniker som tunneling, vilken är beroende av dual stack i grunden för att kunna kommunicera (Amoss & Minoli, 2008).

3.2 Tunneling som övergångsmekanism (Inkapsling)

Användning av tunneling-tekniken som en övergångsmekanism från IPv4 till IPv6 innebär att kunna förse en IPv6-anslutning över ett IPv4-nätverk. Tekniken innebär att kapsla in ett IPv6-paket i ett IPv4-paket som möjliggör att IPv6-paket kan färdas över IPv4-nätverk tills det når slutet av tunneln. Vid slutet av tunneln avkapslas paketet och IPv6-paketet kan då vidarebefordras till rätt mottagare över ett IPv6-nätverk istället (Amoss & Minoli, 2008). Enligt Amos & Minoli (2008) finns det mängd definierade metoder som fastställer olika tunnlingstekniker. Dessa tekniker beskrivs i undersektionerna nedan. Figur 10 nedan illustrerar arkitekturen för hur IPv6 kapslas in i ett IPv4-paket.

IPv4-header	IPv6-header	Transport-header	Applikationsdata/Payload
-------------	-------------	------------------	--------------------------

Figur 10 Ett IPv6-paket inkapslat i ett IPv4-paket

3.2.1 6over4

6over4 är en övergångsmekanism som kapslar in IPv6-paket i IPv4-paket och är avsedd för att transportera IPv6-paket mellan dual stack-enheter över ett IPv4-nätverk med multicast (Govil et al. 2008). Övergångsmekanismen kallas även för IPv4 multicast tunneling. Den används som en virtuell datalänk-lager där IPv6 kan användas dvs. att IPv4-nätverket tillåts att agera som ett subnätverk för IPv6-enheter och routrar (Amoss & Minoli, 2008).

Med denna mekanism används IPv4-nätverket som lager två-transport för IPv6, där automatisk tunnling är möjlig först efter att klienterna i det lokala nätverket har konfigurerats manuellt. Mekanismen använder sig av *neighbor discovery* där IPv4-nätverket är det virtuella nätverket. Eftersom 6over4 använder en enda länk i sin infrastruktur med tunnling från enhet till enhet, kan neighbor discovery, som t.ex. router discovery fungera normalt över fysiska länkar med möjligheter till multicast (Amoss & Minoli, 2008).

3.2.2 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

ISATAP är en övergångsmekanism som stödjer transport av IPv6-paket mellan dual stack enheter i ett IPv4-nätverk. ISATAP tillåter enheter som är flera IPv4-hopp (*next-hop*) bort från en IPv6-router att automatiskt tunnla IPv6-paket över IPv4 till ISATAP-routern som next-hop-adress. Enheter med dual stack som i detta fall är klienter behöver endast konfigureras för att sedan automatiskt skapa tunnlar emellan dem själva. (Amoss & Minoli, 2008). Automatisk tunnling kan utföras oavsett om adresserna privata eller publika. Denna lösning möjliggör för organisationer att implementera IPv6 på ett enkelt och hanterbart sätt (Hagen, 2006).

Hagen (2006) skriver att ISATAP-mekanismen är designad att transportera IPv6-paket i ett nätverk där IPv6-arkitektur saknas, trots att den är lik andra automatiska tunnlingsmekanismer som 6over4. ISATAP är lik 6over4 genom att den använder IPv4 som ett länklager för att koppla samman IPv6-enheter och transporterar IPv6-paketerna genom tunnlar över IPv4, vilket skapar en virtuell länk över IPv4-nätverket. Men skillnaden mellan dessa är att ISATAP inte använder sig av en multicast-kapabel IPv4-infrastruktur, utan utgår istället från att IPv4-strukturen är Non-Broadcast Multiple Access (NBMA) nätverk. I ett NBMA-nätverk är enheter länkade men datapaket skickas enbart från en enhet till en annan genom en virtuell kanal.

3.2.3 6to4

Övergångstekniken 6to4 ansvarar för routing av trafik mellan nätverk genom att kapsla in IPv6-paket i IPv4-paket. På detta sätt kan båda protokollen samexistera. Endast en router i nätverket behöver konfigureras med 6to4 och resterande enheter för detta nätverk behöver inte konfigureras (Amoss & Minoli, 2008). Hagen (2006) menar att 6to4 som lösning inte bör vara permanent utan bör enbart användas under en övergång till IPv6.

Med 6to4 behövs inga IPv4-adresser som ska vara kompatibla med IPv6-adresser, vilket gör att 6to4-tekniken inte är beroende av det underliggande IPv4-nätverket. Oftast används en border router (gränrouter mellan 2 eller fler nätverk) som 6to4-router (Hagen, 2006).

För enheter i ett 6to4-nätverk som behöver kommunicera med enheter i andra nätverk med 6to4, behöver inte tunnlar konfigureras. Routers ingångspunkt tar istället själva IPv4-adressen av tunnelns utgångspunkt (router), som den använder för destinationens IPv6-adress (Hagen, 2006).

3.2.4 Teredo (Tunneling IPv6 over UDP through NAT)

Denna teknik används av enheter som befinner sig bakom NAT och tjänsten kräver för nätverket Teredo-konfigurerade servrar, klienter och Teredo-relays (IPv6-routrar). Denna övergångsmekanism förser med funktioner som adresstilldelning och automatisk tunnling från värd till värd genom unicast IPv6-trafik för IPv6/IPv4-enheter som använder NAT (Amoss & Minoli, 2008).

6to4 är den teknik som mest används idag men denna teknik fungerar inte med NAT om båda tjänsterna inte används på samma router. NAT skapar problem för tunnling av IPv6 över IPv4 därför att användare bakom NAT använder privata adresser. Vidare använder NAT en typ av paketfiltrering som undersöker paketets data (payload). IPv6-paketet är vid tunnling payload i IPv4. Eftersom tunnlingstekniker som 6to4 kräver publika IP-adresser, filtreras paketet mest sannolikt bort (Huitema, 2006).

Teredo tillåter istället IPv6-trafik att färdas genom IPv4-nätverk med NAT eftersom IPv6-paket kan kapslas in i IPv4 *UDP*-paket. *UDP-datagram* kan routas genom IPv4-baserad Internet och NAT-enheter. Figur 11 nedan illustrerar ett Teredo-paket (Huitema, 2006).

IPv4-header	UDP-header	IPv6-header	IPv6-payload
-------------	------------	-------------	--------------

Figur 11 Teredo-paket enligt (Hagen, 2006)

3.3 Translation (Översättningsteknik)

Enligt Hagen (2006) är målet med denna teknik att ge enheter i IPv6-nätverk en klar och transparent routing så att de kan kommunicera med IPv4-enheter. Det finns en del olika varianter av mekanismer för översättning. De mest förekommande och vanligaste från litteraturen diskuteras i denna rapport.

3.3.1 Stateless IP/ICMP Translation

Denna teknik använder IP/ICMP Translation Algorithm (SIIT) för att översätta mellan IPv4 och IPv6 paket. Detta innebär att IPv6-enheter kan kommunicera med IPv4-enheter. Med denna teknik mappas IPv4-adresser med IPv6-adresser algoritmiskt. Stateless innebär att en tabell med adresser används inte som med stateful, eftersom IPv4 och IPv6 har en algoritmisk relation till varandra (Amoss & Minoli, 2008). En stateless översättare kan därmed hantera varje översättning utan att behöva undersöka redan översatta paket. En stateful måste istället bibehålla en mappning mellan IPv4 och IPv6-adresser.

Översättning från IPv4 till IPv6 fungerar genom att en IPv4 till IPv6-översättare tar emot ett IPv4-paket. Eftersom den är förkonfigurerad till att veta vilka IPv4-adresser som är bundna till de interna IPv6-adresserna i nätverket, kan den veta vilket paket som behöver översättning (Hagen, 2006).

3.3.2 NAT-PT

Network Address Translation-Protocol Translation (NAT-PT) möjliggör för IPv4-enheter att direkt kommunicera med IPv6-enheter eller tvärtom genom att översätta mellan de båda protokollen. En router med NAT-PT implementerat använder en pool av globala IPv4-adresser och binder dem till IPv6-adresser. Processen liknar den som används av NAT (Hagen, 2006). NAT-PT översätter ett IPv6-paket till ett IPv4-paket eller tvärtom. Inga förändringar behöver göras hos värdarna eftersom all konfiguration görs på t.ex. en router

(Amoss & Minoli, 2008). Relaterade tjänster till NAT-PT enligt Hagen (2006) beskrivs nedan:

Network Address Port Translation and Protocol Translation (NAPT-PT) – Tillåter IPv6-vårdar att kommunicera med IPv4-vårdar genom att använda en enda en IPv4-adress

NAPT – Utöver de fält som översätts av NAT transporten så översätts även TCP-portnummer och ICMP-meddelanden.

Denna tjänst har dock på grund av problem blivit förklarad som föråldrad av Internet Engineering Task Force (IETF) och bör inte användas längre (IETF, 2007). Problemen som berör detta protokoll finns att läsa i RFC 4966 och beskrivs även i undersektion 6.1.3.

3.3.3 Bump-in-the-Host (BIH)

Denna övergångsteknik är ett värdbaserat IPv4 till IPv6-protokoll och är en översättningsteknik, som gör IPv4-applikationer kan kommunicera med IPv6-baserade enheter genom att använda NAT. BIH får IPv4-applikationer att tro att de kommunicerar med IPv4-enheter istället för IPv6-enheter (IETF, 2012). Tekniken nämns i denna rapport eftersom den är ny och är en nyspecificerad RFC (Request for Comments), vilket kan vara bra för administratörer att känna till som alternativ.

BIH är efterföljare till och är en blandning av de båda översättningsteknikerna Bump-in-the-Stack (BIS) och Bump-in-the-API (BIA). Båda teknikerna finns att läsa om i RFC3338 och RFC2767. Som efterträdare ärver den även deras egenskaper och kan därmed också implementeras på två olika sätt. Den ena är protokoll-översättare som översätter mellan IPv4-stacken och IPv6-stacken hos en värd. Den andra varianten är en Application Programming Interface (API)-översättare som översätter mellan modulen för IPv4 *socket API* och TCP/IP-modulen (IETF, 2012). Rapporten går inte in på tekniska detaljer för BIH utan hänvisar till RFC6535 för vidare tekniska detaljer.

3.4 Jämförelse av övergångsmekanismer

Nu när en del övergångsmekanismer som idag är aktuella och tillgängliga har beskrivits, görs en jämförelse mellan dessa enligt litteraturen från Hagen (2006).

3.4.1 Dual Stack

Om man jämför dual stack-mekanismen med andra tekniker så anses dual-stack vara flexibel och enkel för både implementation och användning. Enheter med IPv4 kommunicerar med andra enheter med IPv4 och detsamma gäller för IPv6-enheter.

Dual stack-nätverk erbjuder stor flexibilitet när man har att göra med IPv4-baserade exempel som applikationer, utrustning. Tidigare i rapporten har det även diskuterats att den kan användas som grund för andra övergångsmekanismer. Tunnlar behöver slutpunkter som är dual stack och översättningstekniker behöver t.ex. routrar som stödjer dual stack.

Nackdelen med denna teknik är att eftersom två separata protokollstackar används, behövs det mer kraft från routerns processor och mer minne hos värden.

3.4.2 Tunneling

Tunnlar är enligt Hagen (2006) enkla att skapa och ger möjligheter att gå över till IPv6 på egna villkor. Några större konfigurationer är inte nödvändiga för värdar, enheter och nätverk vid skapandet av tunnlar och det behövs inget IPv6-stöd från Internetleverantören heller.

Även med denna teknik belastas routern mer genom att ingångs- och slutpunkterna behöver mer tid och processorkraft för att kapsla in och avkapsla paket. I detta fall kan man även stöta på storlek- och fragmenteringsproblem för paket. Detta diskuteras även i sektion 6.1.3 som ett problem.

3.4.3 Translation

Enligt Hagen (2006) ska översättningstekniker användas endast om ingen annan mekanism är möjlig att implementera och bör ses endast som en temporär lösning.

Översättningstekniker som använder NAT (t.ex. NAT-PT) är begränsade eftersom svar måste komma tillbaka genom samma NAT-router, som tidigare använts för kommunikationen. NAT-routern är enskild felpunkt i nätverket (single point of failure) och flexibla mekanismer kan inte användas här.

Fördelen med översättningstekniker är att de tillåter en direkt kommunikation och förbindelse mellan IPv4- och IPv6-enheter och tvärtom.

3.5 Relaterande arbeten

Det finns en stor mängd av arbeten som relaterar till detta arbete där övergången från IPv4 till IPv6 berörs ur flera olika synvinklar. Ett arbete som relaterar till detta arbete är Frank Torvmos rapport (Torvmo, 2011). Torvmo (2011) fokuserar på att identifiera hinder för övergång till IPv6 och hans arbete riktar sig främst mot företag som t.ex. webbhotell och IT-konsultföretag.

Ett annat projekt är Linus Dahlströms arbete som handlar om status för införandet av IPv6 för kommunerna i Skaraborg. Detta arbete behandlar status för implementation av IPv6 och riktar sig mycket mot beslutsfattarna och de IT-ansvariga för respektive kommun (Dahlström, 2011).

Oscarsson, (2010) skriver om övergångsmekanismer där målet är att belysa hur övergångsmekanismerna är uppbyggda med för och nackdelar samt vilken teknik som är bäst för vilket användningsområde. Dock granskas de kategoriserade övergångsmekanismerna på en generell nivå och går inte in i detalj för vilka tekniker som faktiskt används för varje kategori.

Karlsson, (2012) skriver om säkerhetsrisker gällande tillgänglighet som relateras till IPv6-protokollets olika funktioner och en övergång från IPv4 till IPv6 och vilken medvetenhet systemadministratörer har om dessa. Undersökningen består av detaljerade frågor som testar systemadministratörernas kunskap om säkerhetsrisker. Enligt Karlsson, (2012) är medvetenheten om säkerhetsriskerna låg. Dock baseras resultatet av enkätundersökningen endast på 10 erhållna svar.

Arbetet har besvarat frågor angående övergångsmekanismernas funktionalitet och användningsområde, dock inte vilken övergångsteknik som är den bästa (Oscarsson, 2010).

Denna fråga går inte att besvara då olika nätverk använder olika nätverksarkitektur, vilket överensstämmer med detta arbete.

I Kroatien gjordes en landsomfattande enkätundersökning om övergången till IPv6, som var riktad till flertalet statliga myndigheter och de internetleverantörer som har störst andel på marknaden (Dobrijevic, Svedek & Matilasevic 2012). Undersökningen behandlade b.l.a. den generella kunskapen om IPv6 och planering för övergång till IPv6 hos de statliga myndigheterna, som t.ex. tekniska kunskaper, motivation och övergångsstrategi.

En majoritet av de statliga myndigheterna hade varken planerat eller påbörjat någon övergång till IPv6 och bristen på IPv4 adresser var för den delen ingen motiverande faktor heller (Dobrijevic, Svedek & Matilasevic 2012), vilket kan relateras en del till situationen i Sverige. Dobrijevic, Svedek och Matilasevic (2012) hävdar att orsakerna till detta kan vara generellt dåliga ekonomiska resurser och hög kostnad av övergång. Majoriteten av de tillfrågade internetleverantörerna planerar däremot en övergång till IPv6 och ser bristen på IPv4 adresser som en stor motiverande faktor.

Det mest intressanta som undersökningen avslöjade var att majoriteten av de statliga myndigheter klassade sina kunskaper om övergång till IPv6 som bra. Men hälften av myndigheterna uttrycker samtidigt att de inte har "tillräckliga" kunskaper och erfarenhet för att förbättra nätverksstrukturen. Dobrijevic, Svedek och Matilasevic (2012) tror att detta kan bero på otillräcklig utbildning, information, praktisk erfarenhet och otillräckliga praktiska kunskaper gällande övergången till IPv6.

4 Problem

IPv6-protokollet för med sig i förhållande till IPv4 förbättringar gällande enkelhet, routinghastigheter och säkerhet där säkerheten och konfidentialiteten tas till en högre nivå för information som skickas över nätverk (Zagar & Grgic, 2006).

Övergången till IPv6 beräknas bli långvarig och är inget som sker över en natt. Det finns en mängd övergångsmekanismer som var tänkta att underlätta övergången. Dessa övergångsmekanismer har istället medfört ökade risker för säkerhetsproblem, vilket har visat sig vara mer komplicerat och utmanande än underlättande för systemadministratörer (Bi et al., (2007). En övergång till IPv6 är ändå oundviklig eftersom de sista IPv4-adresserna delades ut i januari 2011.

Denna rapport fokuserar på de kategoriserade övergångsmekanismerna Dual Stack, Tunneling och Translation och vilka säkerhetsproblem olika tekniker för respektive kategori kan medföra. Organisationer som statliga myndigheter och företag, som redan infört IPv6 dvs. de grundläggande tjänsterna DNS, e-post och webbtjänst, befinner sig i en fas där IPv6 samexisterar med IPv4. Syftet är att få en bättre uppfattning om hur relaterade problem till denna samexistens eventuellt kan påverka dem. Rapporten fokuserar även på de organisationer som är mitt uppe i en övergång idag. Rapporten kommer också att utreda och jämföra ovan nämnda övergångsmekanismer och deras olika tekniker, som olika organisationer använder samt de problem de kan medföra och hur organisationen påverkas av dessa.

Rapporten kommer främst att fokusera på statliga myndigheter eftersom de har press på sig från regeringen, som har sagt att alla myndigheter bör ha infört IPv6 senast år 2013 (Regeringen, 2012). Detta har blivit ett problem då en del myndigheter tycks avsiktligt har valt att dröja med en övergång, vilket har resulterat i att dessa myndigheter fortfarande inte har implementerat IPv6 (PTS E-tjänster, 2013). Genom att undersöka hur övergångsmekanismer och eventuella säkerhetsproblem kan påverka en organisation, kan undersökningen eventuellt ge en del svar på varför migreringen till IPv6 går långsamt. Rapporten ämnar också skapa en djupare förståelse för IPv6 och dess problem för systemadministratörer samt vara till hjälp för utveckling av skydd mot eventuella säkerhetsproblem, som kan medföra potentiella attacker.

4.1 Formulering av problem

Problemfrågan som adresseras och behandlas i denna rapport är:

Vilka säkerhetsproblem gällande informationssäkerhet kan uppstå vid olika övergångsmekanismer från IPv4 till IPV6 och hur påverkar de organisationen?

Problemfrågan syftar till att identifiera problem rörande tekniker som tidigare nämnda övergångsmekanismer använder och hur de kan påverka en organisations verksamhet för IT gällande informationssäkerhet. För att kunna förstå och besvara frågan krävs en del följdfrågor och en omfattande undersökning som berör relaterande områden till denna fråga.

Ett tillvägagångssätt är att bryta ned problemet i mindre delar och behandla dem som olika delmål. I delmål 2 kommer administratörernas kunskap och erfarenhet om IPv6 och relaterade övergångsmekanismer att undersökas. Undersökningen ämnar underlätta för en

bedömning om hur trovärdig och giltig administratörernas svar är i den kommande enkätundersökningen. Delmål 2 är därför ett hjälpmedel i bedömningen av respondenternas svar. Relaterande arbeten som presenterats i sektion 3.5 berör status för implementation av IPv6 i en begränsad del av landet, vad som hindrar svenska företag att migrera till IPv6 samt jämförelser av olika övergångsmekanismer.

Även medvetenheten hos systemadministratörer angående IPv6 och säkerhetsrisker har också presenterats samt situationen gällande en övergång i andra länder, som t.ex. Kroatien. Anledningen till varför just arbetet med Kroatien presenteras här är på grund av att en landsomfattande enkätundersökning har genomförts där angående IPv6 och övergångsstrategier och undersökningen är riktad mot statliga myndigheter.

Detta arbete berör istället övergångsmekanismerna och de problem de kan medföra samt om och hur de kan påverka en organisation gällande informationssäkerhetens alla aspekter och inte enbart tillgänglighet som tidigare adresserats.

Delmål 1: Identifiera de säkerhetsproblem gällande informationssäkerhet som kan uppstå vid olika övergångsmekanismer.

Delmål 2: Undersökning om hur stor kunskap och erfarenhet organisationens systemadministratörer har gällande övergångsmekanismer och IPv6.

Delmål 3: Undersöka hur övergångsmekanismer och relaterade säkerhetsproblem kan påverka organisationen gällande informationssäkerhet.

Delmål 4: Undersöka om systemadministratörer idag i en fas av samexistens mellan IPv4 och IPv6 upplever problem/säkerhetsproblem.

Delmål 5: Jämföra och sammanställa resultat från organisationerna och de föregående delmålen för att sedan analysera och dra slutsatser utifrån dessa delmål.

5 Metod och Genomförande

Denna sektion kommer att ta upp vilka metoder som kommer att användas för respektive delmål. För och nackdelar för varje metod kommer att jämföras och diskuteras. Även genomförandet för metoderna beskrivs i denna sektion.

5.1 Metod

I denna delsektion presenteras de metoder som kommer att användas för respektive delmål.

5.1.1 Delmål 1

För att kunna identifiera säkerhetsproblem gällande informationssäkerhet kommer information att samlas in genom en omfattande litteraturstudie. En litteraturstudie är ett sätt att systematiskt undersöka ett specifikt problem med hjälp av analys från publicerade källor (Berndtsson, et al., 2008). Eftersom tiden för arbetet är begränsat är en litteraturstudie ett effektivt sätt tidsmässigt att få en generell bild över de olika säkerhetsproblemen.

Med litteraturstudier kan det vara svårt att avgöra när man ska upphöra med insamling av information (Berndtsson, et al., 2008). Det är viktigt att vara försiktig med hur man tyder och systematiskt analyserar varje källa samtidigt som det är viktigt att även välja rätt källa (Berndtsson, et al., 2008).

Det finns ett antal tekniker för att försäkra sig om att relevanta källor har valts. En strategi är att söka igenom biblioteksdata-baser genom att använda relevanta nyckelord från t.ex. bakgrundsstudierna. En annan strategi är att söka efter relevant information i journaler i bl.a. innehållsförteckningar (Berndtsson, et al., 2008).

Utifrån denna information kommer information att samlas in från vetenskapliga artiklar och journaler genom att söka i biblioteksdata-baser och Internet. Informationen från artiklarna ska vara relevant och giltigt för ämnet och skapa trovärdighet hos läsaren men även besvara avsikten med litteraturstudien.

5.1.2 Delmål 2

För att undersöka hur stor kunskap organisationens systemadministratörer har gällande övergångsmekanismer och eventuella problem med IPv6, kommer en enkät att genomföras. Här anses det viktigt att veta hur stor kunskap och erfarenhet systemadministratören har av IPv6 när frågorna besvaras i nästkommande delmål. Administratörens kunskapsnivå underlättar en analys och tolkning av svar för läsaren.

Här kommer en enkätundersökning att genomföras eftersom det finns ett stort antal respondenter i form av systemadministratörer, som har kunskap om problemet i fråga. Dessutom kan det stora antalet respondenter nås med relativt små resurser, vilket är en fördel (Berndtsson, et al., 2008). En nackdel är bristen på tvåvägskommunikation där det blir svårt att klargöra och diskutera frågorna på en mer fördjupad nivå. Vidare är det omöjligt att veta om det ens är den respondent som enkäten är avsedd för som faktiskt svarar (Berndtsson, et al., 2008). En annan nackdel är att den här typen av undersökningar brukar resultera i en låg svarsfrekvens då motivationen hos respondenten ofta är låg (Berndtsson, et al., 2008). För att få en bättre klarhet och en bättre helhetsbild kommer en stor mängd enkäter att skickas till olika företag och myndigheter över hela landet.

5.1.3 Delmål 3

För att uppnå detta delmål kommer en kombination av enkätundersökning och muntlig intervju att utföras. Tanken här är att den muntliga intervjun ska komplettera enkätundersökningen för att ge mer tydliga och utvecklade svar. Denna del av enkätundersökningen kommer att slås ihop med enkätundersökningen för delmål 2. Den form av intervju som troligtvis kommer att användas för detta ändamål är en stängd intervju. En stängd intervju innebär att den som intervjuar ställer en del fasta fixerade frågor där frågorna är förstrukturerade och beroende på svar inte ändras under pågående intervju (Berndtsson, et al., 2008).

En stängd intervju är mer fördelaktig jämfört med en öppen intervju där risken för upprepning av frågor och svar minskar. Dock kan den som intervjuas uppleva en del frågor som mindre väsentliga, vilket i sin tur kan leda till ett inkomplett svar (Berndtsson, et al., 2008). En öppen intervju används oftast till kvalitativ forskning där forskaren har ingen eller mycket begränsad kontroll problem som kan uppstå under pågående intervju. Adresserade problem som tas upp under intervjun planeras inte i förväg för frågeställning. Istället försöker frågeställaren rikta frågeställningen till problem som denne tror kommer att intressera den som intervjuas (Berndtsson, et al., 2008).

5.1.4 Delmål 4

Även detta delmål kommer att inkluderas i samma enkätundersökning som avses för delmål 3. Delmål 4 kommer att få en egen del i enkätundersökningen där vissa frågor riktas specifikt till de problem som kan uppstå i en fas av samexistens mellan IPv4 och IPv6.

5.1.5 Delmål 5

Slutligen kommer resultaten från enkäterna, litteraturstudien och intervjuerna att jämföras och analyseras för att kunna fastslå säkerhetsproblemen gällande informationssäkerhet och deras inverkan på organisationen.

5.2 Genomförande

I denna delsektion presenteras genomförandet för varje delmål.

5.2.1 Delmål 1

En litteraturstudie har utförts med fokus på vetenskapliga publicerade artiklar och även en del utgivna böcker som är relevanta för ämnet i fråga. Omfattande sökningar efter information har även utförts i Request for Comments (RFC), som är dokument och beskriver standarder för b.l.a. de övergångsmekanismer som existerar idag. Dessa dokument publiceras av IETF. Ett antal säkerhetsproblem har sammanställts och kommer att presenteras och delas in i kategorier efter hur övergångsmekanismerna är kategoriserade.

5.2.2 Delmål 2, 3 och 4

Litteraturstudien som utförts har tillfört en bredare förståelse för identifierade övergångsmekanismer och relaterade problem. Vidare har detta underlättat för utformningen och strukturen för enkäten. Enkäten är en onlineenkät som har skapats med hjälp av Google Docs. Google erbjuder ett flertal webbtjänster som t.ex. email och att skapa dokument online. Onlineenkäten är ytterligare en av många tjänster som erbjuds av Google, där en enkät kan struktureras och utformas efter eget behov och resultaten till onlineenkäten kan lagras online.

Strukturen för enkäten utformas till tre delar. Onlineenkäten startar med en inledning som presenterar de tre delarna och bakgrunden till arbetet. I inledningen framgår det även att enkäten är anonym eftersom ämnet berör säkerhetsfrågor som kan vara känsliga för organisationen i fråga att diskutera. Inledningen förklarar även för svarsdeltagaren genom att betona vikten av ett ärligt svar.

Den första delen som knyts till delmål 2, består av frågor som berör respondentens bakgrund till IT och deras kompetens och erfarenhet av IPv6-protokollet och relaterade övergångsmekanismer.

Den andra delen knyts till delmål 3 och denna del delas upp i två delar. En del slås ihop med enkäten och bildar del 2 i enkäten. Den andra delen berör muntliga frågor vid en fysisk intervju.

Del 2 i enkäten startar med att övergångsmekanismerna presenteras i form av att frågor ställs för att ta reda på vilken eller vilka övergångsmekanismer företaget använder. Därefter utformas frågorna som berör eventuella problem under införandefasen. Beroende på vilket svaret är, ges respondenten möjlighet att utveckla svaret själv. Därefter berör frågorna på vilket sätt organisationen har påverkats av införandet.

Del 3 i enkäten undersöker vilken/vilka övergångsmekanismer som idag orsakar problem vid samexistensen för båda protokollen och vilka problem det i så fall är, samt hur organisationen upplever dessa. Här ges administratören även möjlighet att uttrycka egna tankar och vidareutveckla varje svar beroende på vad svaret är.

I inledningen följer även instruktioner gällande vilken del som är anpassad för vilken organisation. Med detta menas att instruktionerna talar om för läsaren att om organisationen befinner sig mitt i en fas av införande, ska de svara på del 1 och 2. För de som är klara med införandet och befinner sig i en fas av samexistens mellan protokollen, ska del 1 och 3 besvaras. Enkäten finns tillgänglig i Appendix A. Inbjudan till enkäten finns att läsa i Appendix B.

Det är mycket information som ska efterfrågas men frågeställningen kommer ändå att begränsas till ett mindre antal frågor, som bör ta max 10 minuter att svara. Anledningen till detta är att enligt Berndtsson, et al., (2008) brukar denna typ av undersökningar resultera i en låg svarsfrekvens. Även samtal med flera erfarna nätverksadministratörer har avslöjat att de inte lägger mer än 10 till 15 minuter på denna typ av undersökningar, oftast på grund av tidsbrist och ointresse.

5.2.3 Delmål 5

Säkerhetsproblem som identifierats presenteras i nästa sektion. De säkerhetsproblem som identifierats, kommer att analyseras genom att jämföras med resultaten från onlineenkäten och de fysiska intervjuerna med målet att kunna fastställa säkerhetsproblemen för övergångsmekanismerna, och hur de kan påverka en organisation.

6 Resultat och Analys

I denna sektion presenteras identifierade säkerhetsproblem från litteraturstudien, som kan uppstå vid användning av olika övergångsmekanismer. Även resultatet från onlineenkäten och de fysiska intervjuerna presenteras i denna sektion. Vidare kommer svaren från onlineenkäten och intervjuerna att analyseras genom att jämföras med varandra och med de säkerhetsproblem som identifierats i litteraturstudien. All information och data har samlats in från tjänsten Google Docs. Huvuddelen av litteraturstudien genomfördes i form av sökningar i databaserna IEEE Xplore®, ACM Portal, Google Scholar och CiteSeer. Studien omfattade även en mängd vetenskapliga artiklar som refererats till i Wikipedia.

6.1 Identifierade säkerhetsproblem för delmål 1

I denna delsektion presenteras de säkerhetsproblem som kan uppstå vid olika övergångsmekanismer. Säkerhetsproblemen presenteras efter övergångsmekanismernas kategoriuppdelning.

6.1.1 Dual Stack och säkerhetsproblem

Det har varit svårt att hitta säkerhetsproblem för dual stack som just en egen mekanism, eftersom det är en mekanism som gör det möjligt och öppnar för enheter att kommunicera t.ex. IPv6-IPv6 eller IPv4-IPv4. Det krävs mer som t.ex. tunneling för att öppna för en lösning som IPv6-IPv4 eller IPv4-IPv6-kommunikation. I ett sådant läge kanske det är bättre att titta på problem och risker med själva IPv6-implementationen och de säkerhetsrisker IPv6 som eget protokoll kan medföra. Att titta på problem som enbart IPv6 medför som egen stack och protokoll hamnar utanför omfånget för detta arbete.

Liu et al. (2009) skriver om *nätverksmaskar* som kan drabba dual stack-system. Masken ska kunna nå och attackera potentiella mål genom en slumpmässig skanning av adressutrymmet för IPv4-protokollet Liu et al. (2009) skriver även att en övergång från IPv4 till IPv6 är ett effektivt sätt att skydda sig mot spridning av maskar och att det samtidigt är svårare för en mask att skanna IPv6-adressutrymmet pga. dess stora adressutrymme. Vidare hävdar Liu et al. (2009) att det finns en ny mask som kallas för *IPv4-IPv6 dual-stack worm*, som kan skanna och upptäcka mål i IPv6-subnät genom multicast-skanning. Denna mask kan skanna både IPv6-subnät och IPv4-nätverk genom slumpmässig skanning. Vanliga försvarsstrategier för att upptäcka och förhindra maskar kan inte direkt appliceras för IPv6 i dual stack-nätverk (Liu et al. 2009).

Taib & Budiarto (2007) hävdar att gällande dual stack-system, måste varje värd i ett dual stack system ha säkerhetsmekanismer som även stödjer IPv6. T.ex. ska värdens brandvägg, intrångsdetekteringssystem och eventuella VPN-klienter kunna kontrollera trafik för båda IP-versionerna och även blockera och logga misstänkt skadlig trafik.

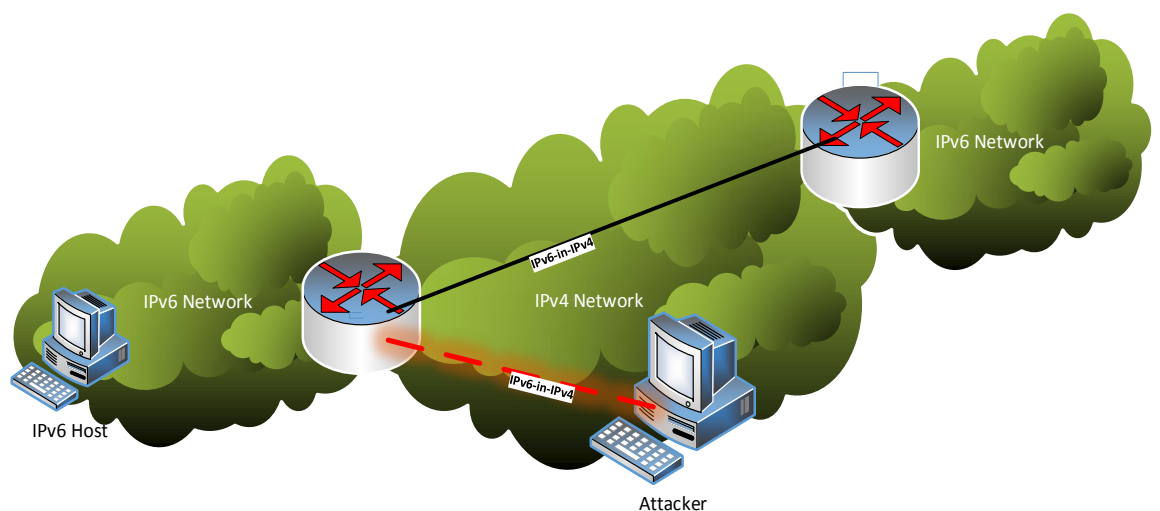
Vidare skriver Taib & Budiarto (2007) att nätverksadministratörer i detta fall bör överväga att antingen implementera en brandvägg med regeluppsättningar för IPv6-trafik som IPv4 har, eller se till att brandväggen stödjer och kan kontrollera båda versioner av protokollen.

6.1.2 Tunneling och säkerhetsproblem

Detta arbete har beskrivit 6over, 6to4, ISATAP och Teredo som tunnlingstekniker. Dessa tekniker har även beskrivits som automatiska tunnlingstekniker. Anledningen till att fokus ligger på automatisk tunnling är för att denna teknik är mer vanlig för nätverksmiljön och

mindre komplex än konfigurerad tunnling. Taib & Budiarto (2007) skriver att automatisk tunnling är mindre säker än konfigurerad därför att den är mer känslig och öppen för paketförfalskning och *DoS*-attacker. Automatiska tunnlar är mer känsliga eftersom det inte finns någon förkonfigurerat samband mellan tunnelns slutpunkter. Konsekvenserna av *DoS*-attacker är vanligtvis att tjänster för användare blir otillgängliga, vilket bryter mot tillgänglighetsprincipen.

Enligt Bi et al. (2007) är hot mot säkerheten i tunnlingsmekanismer som *6over4*, orsakat av *spoofade* inkapslade paket som skickas av angripare i IPv4-nätverk. Bi et al. (2007) menar att målet som attackerar kan antingen vara en IPv6-enhet eller slutpunkt för en tunnel. Ett problem här är att *spoofade* paket kan vara svåra att spåra tillbaka till angriparen. Detta kan relateras till ett brott mot integritetsprincipen och spårbarheten. Figur 12 nedan illustrerar detta säkerhetsproblem för tunnling.



Figur 12 Säkerhetsproblem vid tunnling. Direkt översatt från (Bi et al. 2007)

Bi et al. (2007) nämner också automatiska tunnlingsmekanismer, som Teredo och *6to4* och att de utöver de nämnda problemen kan skapa fler säkerhetsproblem, som att angripare kan attackera med IPv4-broadcast adresser eller genom att stjäla tjänster. Med stöd av tjänster menas att nätverksadministratörer ibland kan vilja begränsa användningen av *6to4*-routers relay-funktion genom att fastställa policys, till att begränsa specifika *6to4* eller IPv6-sajter för interna användare.

Men erfarna användare kan ändå kringgå policyn genom att använda routers IPv4-adress istället (Bi et al. 2007).

Enligt Bi et al. (2007) finns det inget effektivt sätt att skydda sig mot *DoS/DDoS*-attacker från angripare i IPv4-nätverk när det gäller automatisk tunnling. Konfigurerade tunnlar kan skyddas mer effektivt från t.ex. *spoofing* genom att implementera *IPSec*, vilket inte stöds av automatiska tunnlingstekniker.

Enligt Zagar & Grgic (2006) är det viktigt att nätverksadministratörer förstår de säkerhetskonsekvenser som finns för övergångsmekanismer. Då kan de mer effektivt använda lämpliga säkerhetsmekanismer som t.ex. brandväggar och intrångsdetekteringssystem medför.

Tunnling kan underlätta för angripare att undvika vissa filtreringsmetoder som routrar använder, t.ex. *ingress filterin*, där angripare genom tunnling kan kringgå dessa (Zagar & Grgic, 2006). Zagar & Grgic nämner också två vanliga tunnlingsmekanismer. 6to4-mekanismen och Teredo kan enligt Zagar & Grgic (2006) orsaka stora problem för säkerheten genom att alla mottagande enheter måste tillåta avkapsling av paket som kan spåras av vilken erfaren angripare som helst på Internet.

En 6to4-arkitektur består av 6to4-routrar och 6to4-relay routrar. 6to4-routern avkapslar paket från andra 6to4-routrar och 6to4-relay routern tar emot paket från interna IPv6-enheter. Denna mekanism tillåter adressförfalskning i IPv4 och IPv6-headern, vilket innebär att det öppnar för DoS/DDoS-attacker (Zagar & Grgic, 2006).

6.1.3 Translation och säkerhetsproblem

Denna rapport fokuserar endast på säkerhetsproblem som kan uppstå med övergångsmekanismer i nätverkslagret. Dessa har beskrivits i sektion 3.3. Enligt IETF (2011) medför inte Stateless IP/ICMP Translation några nya problem förutom de som redan existerar för IPv4-protokollet och IPv6-protokollet. Detta gäller även för routingprotokollen, som ser till att paketen når översättarna.

Enligt IETF (2007) är de problem som NAT-PT medför inte enbart relaterade till problem som kommer med NAT, utan problemen med NAT-PT förvärras avsevärt genom att de använder *application level gateway (ALG)*. ALG har svårigheter att översätta IPv4-adresser och IPv6-adresser eftersom de har olika storlek. IPv6-enheter måste i detta fall skicka DNS-förfrågningar genom ALG, som översätter IPv4-adresser till IPv6-adresser där dessa adresser sedan vidarebefordras till en NAT-PT-enhet som utför översättning (IETF, 2007).

En konsekvens av detta kan innebära att de omskrivna DNS-svaren skulle kunna läcka ut och snappas upp av IPv6-värdar, som inte använder NAT-PT och där dual stack inte finns, vilket kan skapa stor förvirring med adresshantering (IETF, 2007).

En naturlig del för översättningsmekanismer som jobbar i nätverkslagret är att de är oförenliga med de protokoll som är tänkta att skydda IP-headern. En BIH-implementation kan då innebära problem för säkerheten. BIH har enligt IETF (2007) ett antal begränsade resurser som kan utnyttjas av angripare för att skapa DoS-attacker.

BIH har ett begränsat antal adresser som den använder för översättning men dessa gör det ändå möjligt för angripare att utnyttja IPv4-adresspoolen genom att få en värd att utföra DNS-förfrågningar (IETF, 2007). Om fragmenten är många i antal, kan klientens minne bli tömt och oåtkomligt.

DOS-attackerna kan i sin tur också påverka andra begränsade resurser som t.ex. minnet hos en värd. En angripare kan utföra en DoS-attack psom är riktat mot minnet för värden som använder BIH genom att skicka egna fragmenterade paket till den värden.

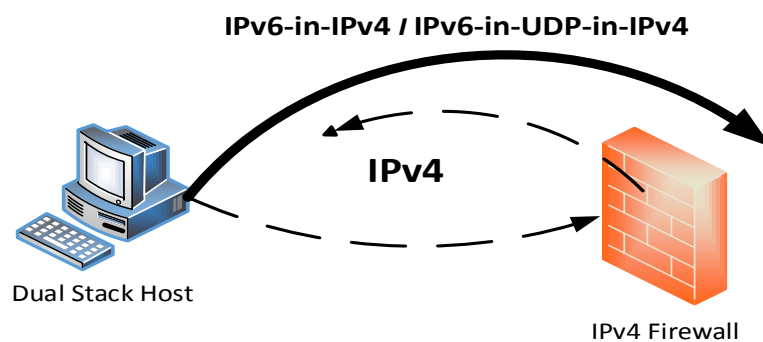
6.1.4 Samexistensen mellan IPv4 och IPv6 och relaterade problem

När en eller flera övergångsmekanismer har implementerats uppstår en samexistens mellan de två separata IP-protokollen. Wu et al. (2013) skriver att redan implementerade mekanismer hos värdar eller organisationer skapar generella problem ur olika synvinklar. Brandväggar, utrustning som t.ex. routrar och servrar behöver eventuellt uppgraderas på mjukvara och hårdvara-nivå.

För en blandad nätverksmiljö behöver extra resurstilldelning övervägas för att fördela resurser mellan nätverken, som t.ex. bandbredd för att garantera likvärdig tjänst åt både IPv4- och IPv6-nätverket. IPv6 för med sig nya protokoll som *Neighbor Discovery Protocol (NDP)* och *DHCPv6* där dessa i sin tur kan medföra nya säkerhetsrisker som behöver undersökas. När det gäller klienter behöver applikationer som används kunna vara tillräckligt intelligenta för att avgöra vilket protokollstack som skall användas, om destinationen kan nås med båda alternativen (Wu et al. 2013).

Men enligt Wu et al. (2013) är nätverksanslutningen i en blandad IPv6-IPv4-miljö av en mer problematisk karaktär. Wu et al. (2013) menar att utan extra övergångsmekanismer kan inte protokollen kommunicera med varandra, utan protokollen kör t.ex. routing individuellt. Å andra sidan är Internet en blandad IPv4-IPv6 miljö där Internetleverantörer och användare själva väljer att börja använda IPv6. Medan en nätverksanvändare har IPv4- eller IPv6-åtkomst, vill ändå olika användare kunna kommunicera fritt med varandra (Wu et al. 2013).

Bi et al. (2007) skriver däremot att säkerhetsproblem mest kan relateras till IPv4 under period av samexistens, där en angripare enkelt kan ta sig förbi IPv4-paketfiltreringen med IPv6-IPv4-tunnel. Normalt används brandväggar för att skydda nätverket och begränsa interna användare. Men under en samexistensperiod kan interna användare korsa kringgå IPv4-brandväggen för att komma åt externa nätverk genom att använda IPv4-IPv6-tunnel. Enligt Bi et al. (2007) finns det en lösning mot detta med en paketfiltreringsmetod. Bi et al. (2007) relaterar även detta problem till övergångsmekanismen Teredo som kan användas för att kringgå en IPv4-filtrering. Figur 13 nedan illustrerar hur IPv4-brandväggen kringgås.



Figur 13 Korsad IPv4-brandvägg. Direkt översatt från (Bi et al. 2007)

Bi et al. (2007) skriver också om att det är viktigt att införa IPv6-brandväggar i god tid vid ett införande av IPv6-protokollet.

6.2 Enkät för delmål 2, 3 och 4

Av de 150 enkäter som skickats ut har totalt 30 respondenter valt att delta i enkätundersökningen. Påminnelser har skickats ut två gånger och ändå har enkätundersökningen resulterat i en svarsfrekvens på 20 procent. Information om data i form av respondenternas svar finns tillgänglig i Appendix C. Det verkar förekomma en låg stämning bland myndigheters IT-administration och deras relation till PTS mål med införandet av IPv6. Med detta menas att systemadministratörer inte delar PTS uppfattning om situationen med IPv6. En respondent svarade b.l.a. på följande sätt:

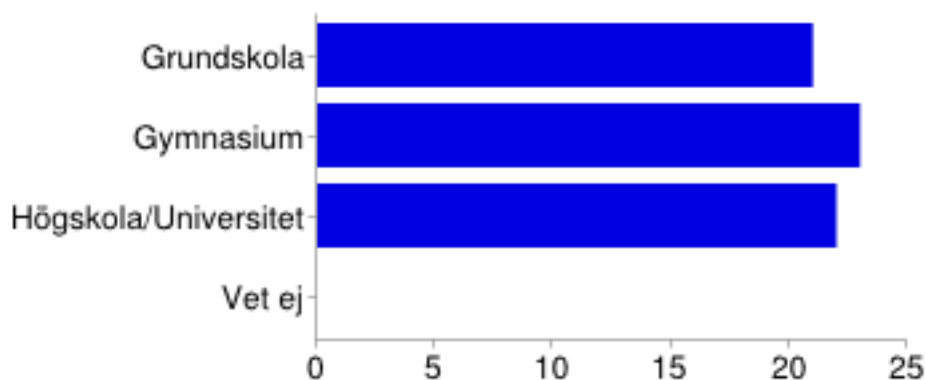
”IPv6-propagandan som sprids från pts på deras ”ipv6-möten” är direkt felaktig då de hela tiden säger ipv6 -adresser kan inte kommunicera med ipv4-adresser. De operatörer som kör ipv6-only (i asien) erbjuder också nat64 -gateways för att tillgängliggöra ipv4-internet den vägen.”

Detta kan tolkas som en negativt motsägande kommentar mot PTS, vilket i så fall innebär att PTS med deras metod att uppfylla regeringens mål, haft en negativ inverkan på denna myndighet och dess IT-verksamhet. Denna delsektion presenterar svaren från onlineenkäten. Respondenters vidareutvecklade svar till frågorna kommer att diskuteras i en sammanfattande analys längre fram i arbetet.

6.2.1 Enkät Del 1

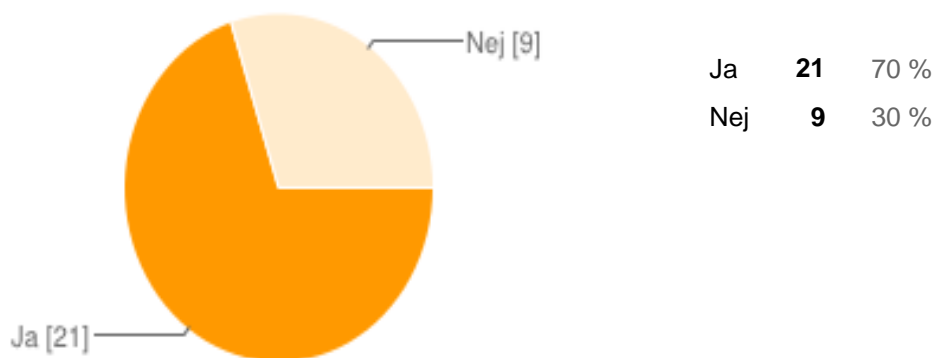
På den första frågan som undersöker systemadministratörernas utbildningsnivå, har sammanlagt 23 respondenter svarat att de har gymnasieutbildning och 22 personer av dessa har svarat att de dessutom har en högskola/universitetsutbildning. Bland svarsalternativen fanns även en möjlighet att välja om man har en grundskoleutbildning. Grundskolealternativet kommer dock inte att diskuteras i detta arbete då det egentligen inte är relevant för undersökningen. Resultatet (figur 14) visar att cirka 73 procent av respondenterna är utbildade på en högre nivå.

Vilken utbildningsnivå har du?



Figur 14 Utbildningsnivå

Har du gått någon IT-utbildning som berör IPv6?

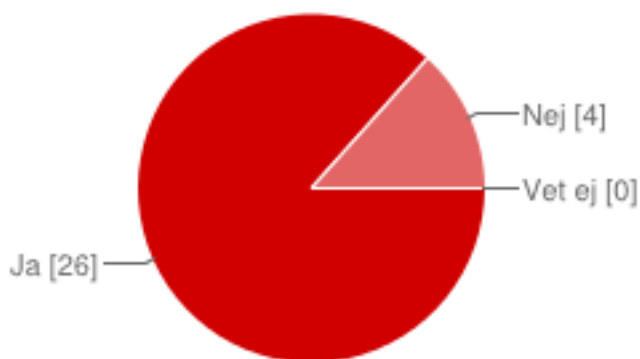


Figur 15 IPv6 utbildning

Av de 30 respondenter som svarat på frågan om de genomgått någon form av utbildning som berör IPv6, har hela 70 procent ja (figur 15). Detta innebär att tillförlitligheten för administratörernas svar i denna enkät ökar.

På frågan som berör hur länge respondenten arbetat som systemadministratör, har totalt 30 personer svarat på frågan där åldrarna sträcker sig allt från 4 till över 25 år (inget diagram). Av de 30 respondenter som svarat, har 50 procent arbetat som systemadministratörer i 15 år eller längre. Hälften har alltså en lång erfarenhet av yrket som systemadministratör, vilket ökar trovärdigheten för svaren.

Administrerar du eller har du administrerat nätverk där övergångsmekanismer till IPv6 används?

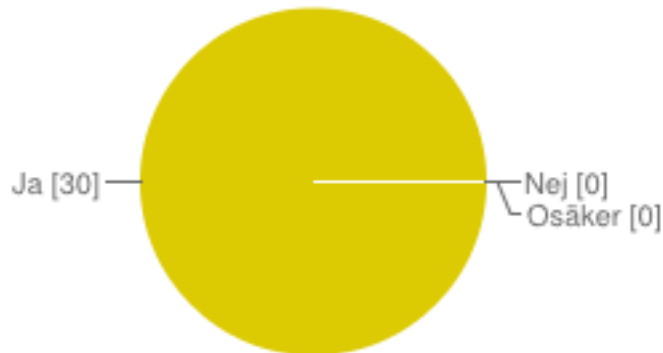


Figur 16 Administration av nätverk gällande övergångsmekanismer

På frågan angående om administratören har administrerat eller administrerar nätverk där övergångsmekanismer till IPv6 används, har hela 26 respondenter av 30 svarat ja. Endast fyra respondenter har svarat nej (figur 16). Även detta resultat medför en större tillförlitlighet för senare resultat då 87 procent av deltagarna har erfarenhet av IPv6-protokollet.

Respondenterna har även fått möjlighet att utveckla svaret på frågan ovan, där kommentarerna kommer att sammanfattas i en sammanfattande analys längre fram i arbetet.

Känner du till att övergångsmekanismer kategoriseras i följande kategorier?



Figur 17 Kännedom av kategorisering av övergångsmekanismer

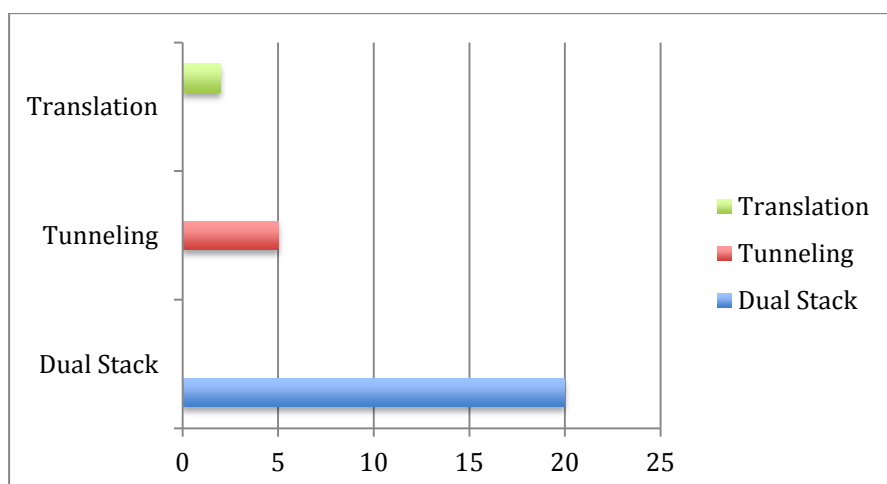
På frågan som undersöker om administratörerna känner till att övergångsmekanismer kategoriseras som Dual Stack, Tunneling och Translation, har samtliga 30 respondenter svarat ja (figur 17). Denna kännedom underlättar för följdfrågorna som bygger på kategorisering, där administratören även kan utveckla sina svar. Endast en respondent har kommenterat att det är tveksamt att kalla dual stack för en övergångsmekanism. En direkt kommentar till denna fråga är att organisationens driftpersonal har fått intern IPv6-utbildning via externt företag. Detta tyder på att en del myndigheter hyr in utomstående konsultföretag för att utbilda sin personal om IPv6. Eftersom svaret är en direkt vidareutveckling frågan, tyder det på att utbildningsinnehållet även har omfattat kategorisering av övergångsmekanismerna.

6.2.2 Enkät Del 2

Denna del av enkäten riktar sig mot de organisationer som inte har uppnått en fullbordad övergång dvs. en eller endast två av de tre grundläggande tjänsterna har implementerats. 20 av 30 deltagare har svarat på del 2 för enkäten.

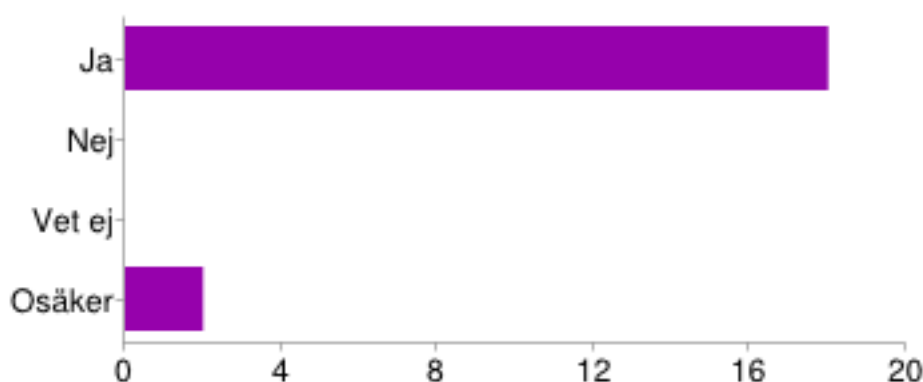
På frågan om vilken eller vilka typer av övergångsmekanismer organisationer använder, har samtliga 20 respondenter svarat dual stack (figur 18). Detta innebär att 100 procent har svarat dual stack, där 25 procent av dessa även använder tunnlingstekniker och tio procent använder någon form av översättningsteknik. Detta överensstämmer med det som Amoss & Minoli (2008) hävdar att dual stack är den mekanism som idag är vanligast.

Vad för typ av övergångsmekanism/övergångsmekanismer använder ni?



Figur 18 Vilken/vilka övergångsmekanismer som mest används

Känner ni till potentiella säkerhetsproblem som kan uppstå vid en övergång från IPv4 till IPv6?

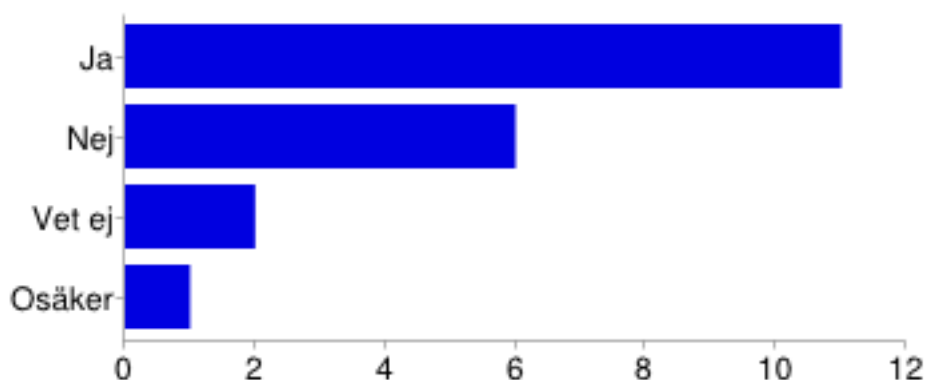


Figur 19 Kännedom om säkerhetsproblem

På frågan om administratören känner till säkerhetsproblem som kan uppstå vid en övergång till IPv6, har 18 respondenter svarat ja (figur 19). Detta tyder på att det finns en klar medvetenhet om säkerhetsproblemen för de olika mekanismerna. Endast två respondenter har markerat att de är osäkra.

Utvecklade svar till denna fråga, som att tekniken 6to4 har inaktiverats och att man inte känner till alla men är samtidigt väl medveten om säkerhetsproblemen vid tunnling och dual stack, tyder på att 90 procent verkar även relativt säkra på sitt svar.

Har er organisation upplevt säkerhetsproblem som kan relateras till övergångsmekanismer?

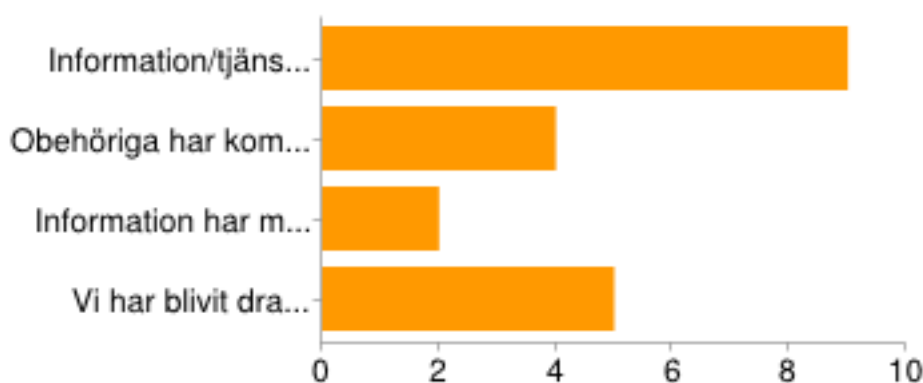


Figur 20 Antal upplevda säkerhetsproblem relaterade till övergångsmekanismer

En mycket intressant del i enkäten är frågan om organisationen har upplevt säkerhetsproblem som kan relateras till övergångsmekanismer. I enkäten förklaras det att problem kan innebära allt från *DDos*-attacker till upptäckta sårbarheter i nätverket eller t.ex. IPv6-IPv4 tunnlar som används för att kringgå IPv4-paketfiltreringen, både internt eller externt.

Här har hela 55 procent av 20 respondenter svarat ja (figur 20). Det är alltså en stor andel av de tillfrågade som har haft problem med övergångsmekanismerna. Endast 30 procent svarade nej och tio procent "Vet ej". En respondent dvs. fem procent, markerade valet "osäker". Svaret tyder på att systemadministratörerna verkar väldigt medvetna om säkerhetsproblemen, samt att säkerhetsproblemen inte direkt verkar vara en ovanlig del av vardagen för systemadministratörer.

Om du har svarat Ja eller Osäker på föregående fråga



Figur 21 Antal drabbade gällande informationssäkerhet

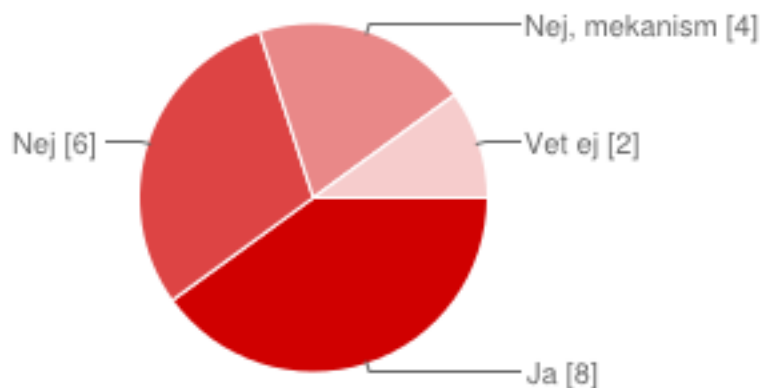
Information/tjänst har varit otillgänglig	9	45 %
Obehöriga har kommit åt information	4	20 %

Information har modifierats av obehöriga	2	10 %
Vi har blivit drabbade men väljer att inte avslöja några detaljer	5	25 %

Denna fråga bygger direkt på frågan ovan beroende på om man har svarat ja eller ”osäker”. Här mäts informationssäkerhetens tre egenskaper, vilka är tillgänglighet, integritet och konfidentialitet och hur organisationen har påverkats enligt dessa. 15 respondenter dvs. 75 procent har blivit drabbade och markerat olika alternativ (figur 21). Här har ytterligare ett val som ger respondenten möjlighet att svara om de har blivit drabbade men samtidigt väljer att inte avslöja detaljer. Syftet med detta val är att undersöka om frågan är av känslig karaktär för systemadministratörer. Hela 25 procent av de som svarat på denna fråga, har markerat detta alternativ, vilket tyder på att ämnet tycks vara känsligt för en del administratörer.

Respondenterna gavs även möjlighet att själva utveckla problemsituationen ovan, vilket kommer att presenteras i en sammanfattande analys senare. En överraskande aspekt för denna enkät är att många har valt utveckla en del av svaren själva, vilket ändå kan tyda på att ämnet är intressant, trots att enkätundersökningar generellt inte ses som intressanta.

Har övergångsmekanismen/mekanismerna på något sätt haft en negativ inverkan på nätverket/organisationen?



Figur 22 Antal upplevda övergångsmekanismer med negativ inverkan

Ja	8	40 %
Nej	6	30 %
Nej, mekanismerna har enbart haft positiv inverkan	4	20 %
Vet ej	2	10 %

Denna fråga undersöker om administratörerna på något sätt upplevt att mekanismerna i sin helhet skulle haft en negativ inverkan på nätverket eller organisationen (figur 22). Det intressanta är att föregående fråga visade att 55 procent har upplevt säkerhetsproblem men 40 procent upplever att de påverkats negativt. Det är en hög siffra för denna undersökning och tyder på att nästan hälften av organisationerna runtom i landet kan ha påverkats negativt. Endast 20 procent svarade att mekanismerna enbart haft en positiv påverkan.

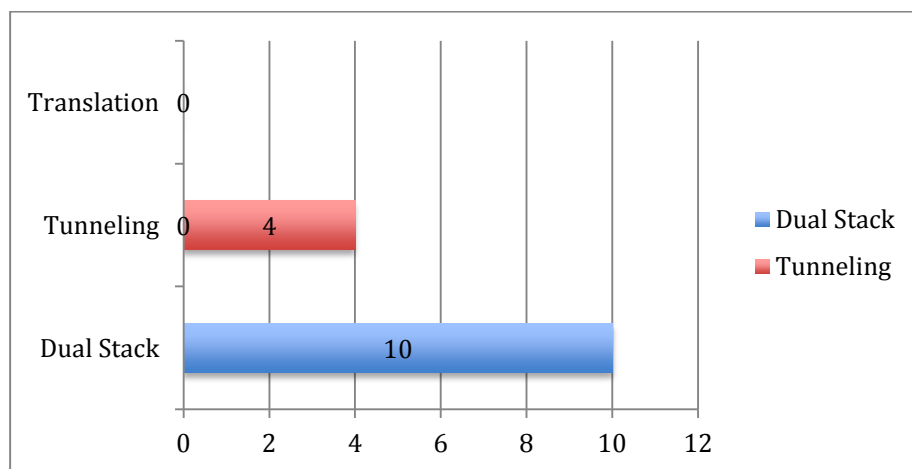
I slutet av del 2 hade respondenterna möjlighet att tillägga övriga åsikter och en del har kommenterat b.l.a. att leverantörer av hårdvara är en bromsfaktor för en fullskalig säker IPv6-implementation. En annan har kommenterat att deras IT-verksamhet finner det väldigt krävande i form av arbete och tid, att underhålla dubbla uppsättningar av säkerhetskfigurationer, t.ex. access-listor i dual stack-system för både IPv4 och IPv6. Detta räknas som en negativ inverkan orsakad av övergångsmekanismer.

6.2.3 Enkät del 3

Denna del av enkäten riktar sig mot de organisationer där övergången räknas som fullbordad och innebär att samtliga av de tre, enligt PTS, grundläggande tjänsterna är implementerade. Frågorna från del 2 finns också med i del 3 eftersom enkäten fortfarande undersöker vilka övergångsmekanismer som används, hur man upplevt eventuella problem som relateras till övergångsmekanismer samt kännedom om potentiella säkerhetsproblem. Resultaten som anges här är enbart för de deltagare som svarat på del 3.

På frågan som berör vilka övergångsmekanismer som används, dominerar användning av dual stack även här. Av de tio deltagare som svarat på denna fråga använder samtliga tio dual stack (figur 23). 40 procent av dessa använder även mekanismen tunnling.

Vad för typ av övergångsmekanism/övergångsmekanismer använder ni?

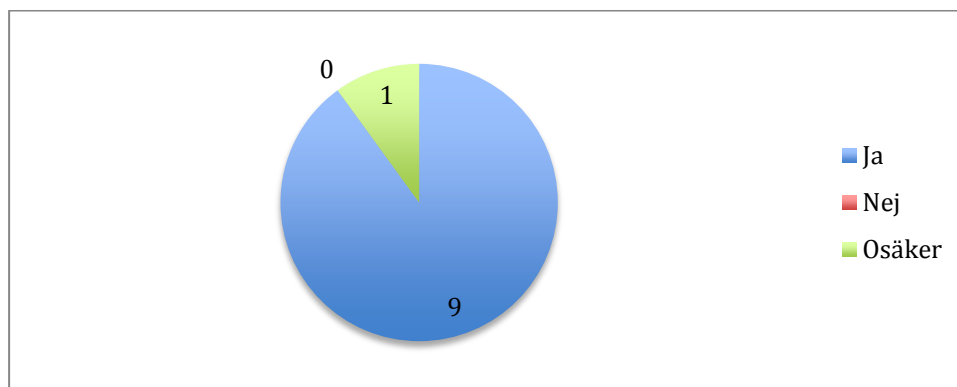


Figur 23 Vilken/vilka övergångsmekanismer som mest används

Dual Stack	10	100 %
Tunneling	4	40 %
Translation	0	0 %
Osäker	0	0 %

Frågan om kännedom om potentiella säkerhetsproblem som kan uppstå vid en övergång, har samtliga 10 svarat ja. Ingen av dessa använder översättning som mekanism (inget diagram).

Känner ni till de problem som kan uppstå vid en samexistens mellan IPv4 och IPv6?

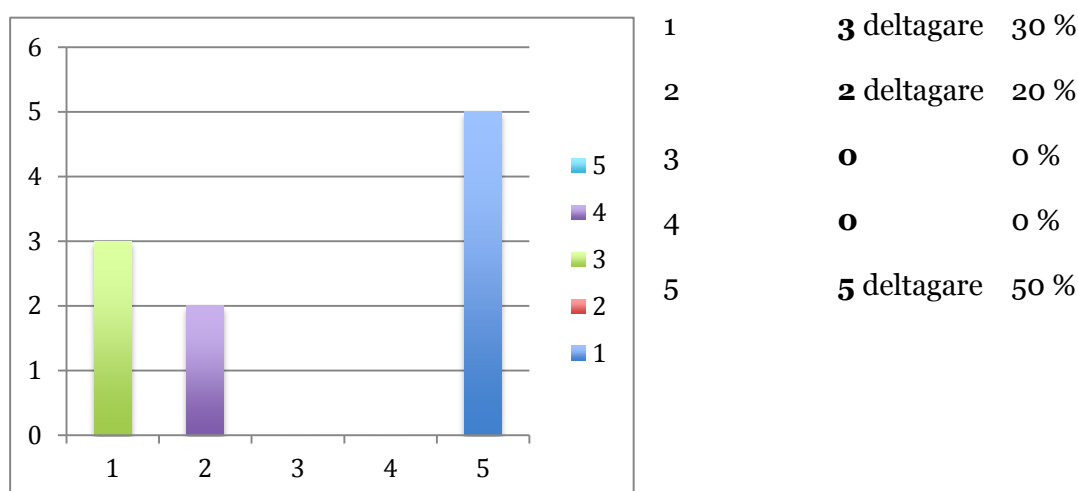


Figur 24 Kännedom om problem vid samexistens mellan IPv4 och IPv6

Frågan undersöker om administratörer känner till problem som kan uppstå vid en samexistens mellan IPv4 och IPv6. Här har 9 respondenter svarat ja och en har markerat "osäker" (figur 24). Eftersom 90 procent svarade ja till denna fråga tyder detta på att administratörerna verkar ha god kännedom om problemen för samexistens mellan IPv4 och IPv6, så som de presenteras av b.l.a. Wu et al. (2013) och Bi et al. (2007).

Ja	9	90 %
Nej	0	0 %
Osäker	1	10 %

De implementerade övergångsmekanismerna har orsakat problem för organisationen

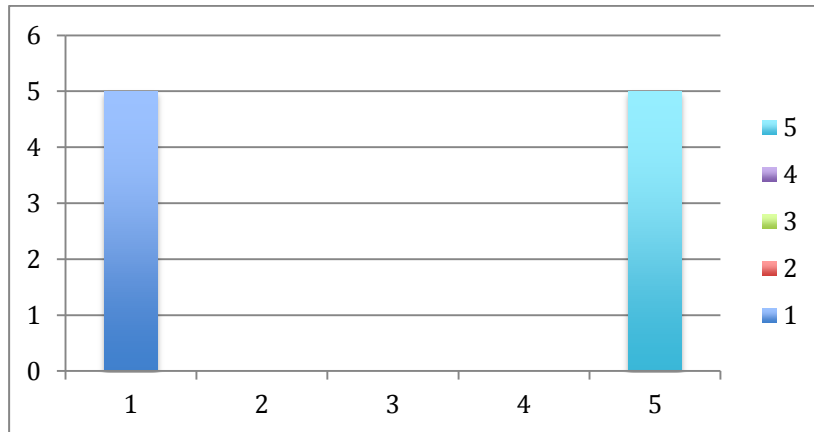


Figur 25 Antal personer som anser att mekanismerna orsakat problem för verksamheten

När det gäller om de implementerade övergångsmekanismerna har orsakat problem för organisationen verkar det som att det råder en delad mening. Hälften anser att detta

stämmer väldigt bra medan resterande inte håller med alls om att övergångsmekanismerna har orsakat problem (figur 25).

Uppgradering av hårdvara och mjukvara har varit nödvändig för samexistensen av protokollen IPv4 och IPv6



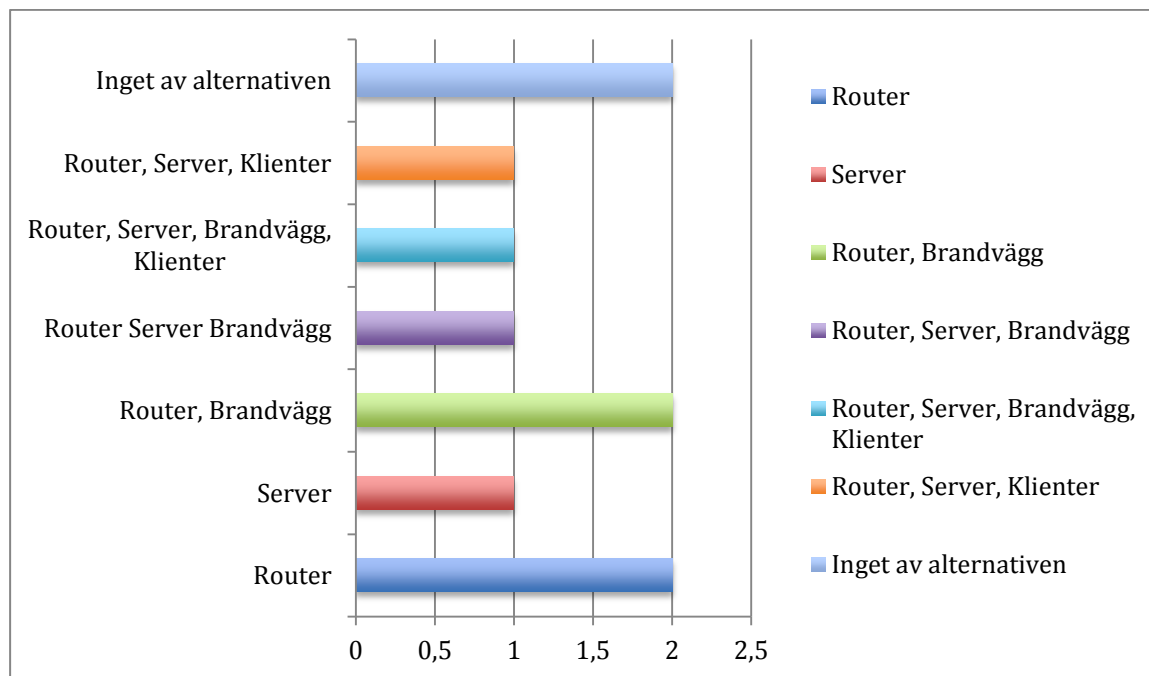
Figur 26 Uppgradering av hårdvara och mjukvara

1	5 deltagare	50 %
2	0	0 %
3	0	0 %
4	0	0 %
5	5 deltagare	50 %

För detta påstående får administratören svara om uppgradering av hårdvara och mjukvara varit nödvändig för samexistensen av IPv4 och IPv6. Även här får administratörerna möjlighet att välja hur bra påståendet stämmer från 1 till 5. 1 betyder att det inte stämmer alls och 5 stämmer väldigt bra. I det här fallet råder det en delad mening även för detta påstående (figur 26). 50 procent hävdar att uppgradering har varit nödvändig. Men samtidigt förefaller det rätt naturligt med tanke på resultatet från påståendet innan. Påståendet ovan relaterar direkt till nästa fråga där administratören får möjlighet att mer konkret ange på vilket sätt övergångsmekanismerna orsakat problem, genom att ange vad som behövt bytas ut eller uppgraderas. Detta är en flervälsfråga och här har respondenterna dock markerat olika. Det har varit byte eller uppgradering av enbart router eller router tillsammans med något av de övriga alternativen som är server, brandvägg, klienter eller inget av alternativen. Detta bekräftar det som Wu et al. (2013) hävdar att det kan uppstå problem ur olika synvinklar med routrar, servrar och brandväggar, som kan behöva en eventuell uppgradering eller byte. Resultatet i detta fall tyder på att routern har en dominerande roll och är den som är mest utsatt under en samexistens. 70 procent av deltagarna har med routern i sina alternativ.

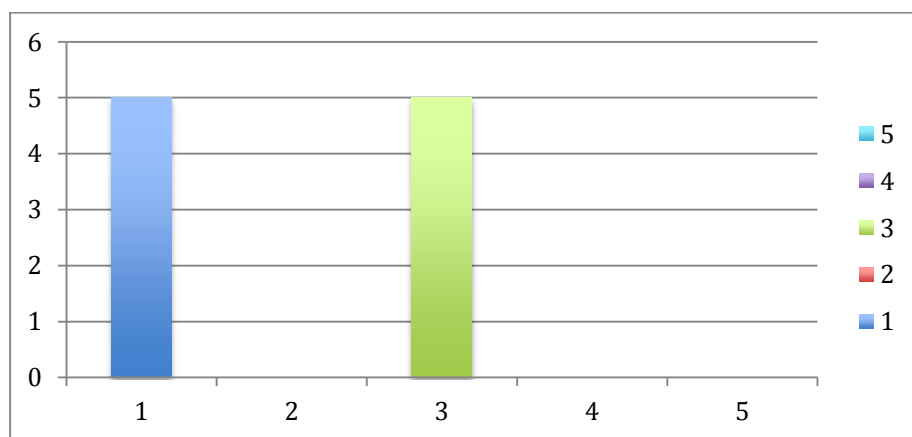
Figur 27 nedan illustrerar fördelningen kring hur respondenterna har drabbats gällande uppgradering/byte av de olika alternativen.

Följande utrustning har krävt byte eller någon form av uppgradering av nedanstående alternativ



Figur 27 Fördelning av byte/uppgradering hårdvara och mjukvara

Extra resurstilldelning har varit nödvändig för att garantera likvärdig tjänst åt både IPv4- och IPv6 nätverket



Figur 28 Fördelning av extra resurstilldelning

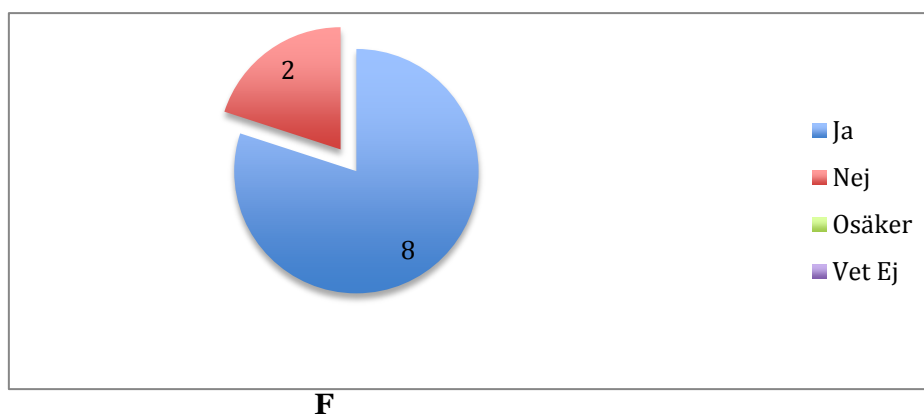
Wu et al. (2013) skriver att i en blandad nätverksmiljö behöver extra resurstilldelning i form av t.ex. bandbredd övervägas så att både IPv4 och IPv6-nätverket kan garanteras likvärdiga tjänster. Till detta påstående har deltagarna svarat olika. I detta fall har 50 procent (figur 28) av deltagarna uttryckt sig tillfredsställande där de ställer sig mer neutrala till påståendet och att det stämmer, vilket tyder på att någon form av omstrukturering i nätverket ändå har gjorts. En har valt att kommentera på följande sätt till detta påstående:

”Vi har vart tvungna att byta och omstrukturera hårdvara efter virus attack.”

Denna kommentar ger dock en missvisande effekt av resultatet till påståendet. Om man kan utgå från att respondenten kommenterat på rätt ställe i enkäten, bör resultatet sett annorlunda ut. Dock har 50 procent svarat att det inte stämmer alls med kommentarer som:

”Vi är så små så det har varit mycket enkelt att implementera” och ”fick hjälp att sätta upp miljön”

Har er organisation upplevt säkerhetsproblem som kan relateras till övergångsmekanismer?

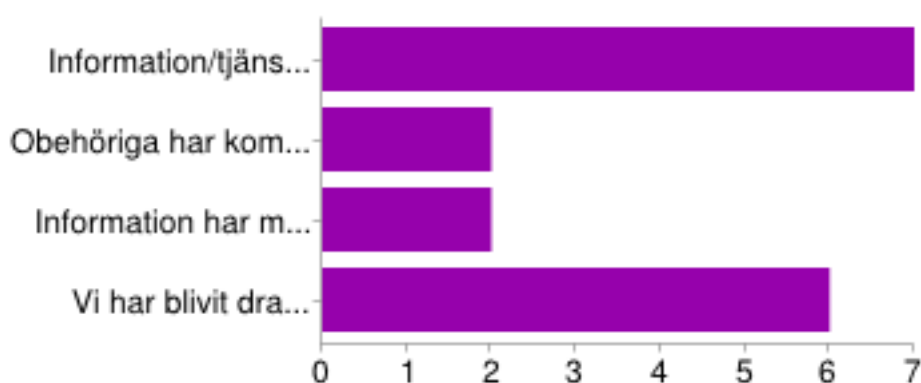


Figur 29 Antal upplevda säkerhetsproblem

Även i del 3 ställs frågan om organisationen har upplevt säkerhetsproblem relaterade till övergångsmekanismer. Frågorna har strukturerats på det här sättet eftersom organisationen även i denna fas kan drabbas av samma problem, men också för att få ett mer enhetligt resultat från alla respondenter. Till skillnad från del 2 är resultatet för del 3 anmärkningsvärt. Här har hela 80 procent av respondenterna svarat ja medan endast 20 procent har svarat nej. Figur 29 illustrerar resultatet för upplevda säkerhetsproblem.

Precis som i del 2 har respondenterna även här i del 3 fått möjlighet att välja alternativ för informationssäkerhet beroende på vad de har svarat i föregående fråga. Skillnaden här är att respondenterna har markerat flera alternativ. Vissa har t.ex. markerat alternativet ”Information/tjänst har varit otillgänglig men samtidigt också markerat ”Vi har blivit drabbade men väljer att inte avslöja några detaljer”. Det sistnämnda har även valts av respondenter som ett enda alternativ ett flertal gånger. Detta beteende tyder återigen på att ämnet tycks vara väldigt känsligt för deltagarna men ändå intressant. Figur 30 nedan illustrerar resultatet.

Om du har svarat Ja eller Osäker på ovanstående fråga



Figur 30 Antal drabbade gällande informationssäkerhet

Information/tjänst har varit otillgänglig	7	41 %
Obehöriga har kommit åt information	2	12 %
Information har modifierats av obehöriga	2	12 %
Vi har blivit drabbade men väljer att inte avslöja några detaljer	6	35 %

6.3 Sammanfattning Enkät

För att få en mer klar och total bild av hur respondenterna har svarat, slås båda delarna för enkäten ihop och presenteras tillsammans för de frågor som är gemensamma för både del 1 och del 2. En annan anledning till denna sammanslagning är att resultaten för frågorna inte skiljer sig mycket mellan delarna, dvs. oavsett vilken fas i övergången till IPv6 organisationen befinner sig i.

Vad för typ av övergångsmekanism/övergångsmekanismer använder ni?

Här har samtliga 30 deltagare uppgett att de använder dual stack-mekanismen. 30 procent av dessa använder även tunnling. Endast sju procent använder någon form av översättningsteknik.

Känner ni till potentiella säkerhetsproblem som kan uppstå vid en övergång från IPv4 till IPv6?

Totalt har 28 respondenter svarat ja på denna fråga. Endast två respondenter har svarat att de är osäkra.

Har er organisation upplevt säkerhetsproblem som kan relateras till övergångsmekanismer?

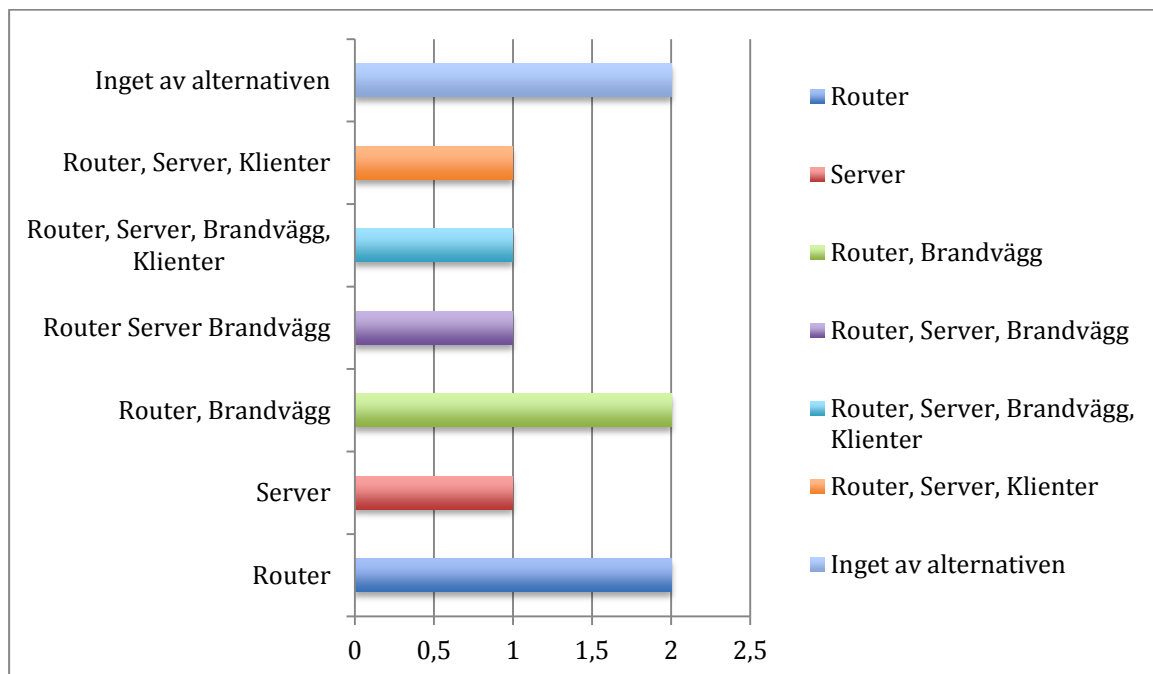
Här har 19 respondenter svarat ja och 8 respondenter har svarat nej. Två var osäkra och en visste inte. Tillförlitligheten till svaren ökar eftersom respondenterna vet vad för typ av problem som enkäten undersöker. Problemen till frågan har beskrivits på följande sätt: ”Problem i detta fall kan innebära allt från DDos-attacker till upptäckta sårbarheter i nätverket eller t.ex. IPv6-IPv4 tunnlar som används för att kringgå IPv4-paketfiltreringen, både från internt eller externt”.

Om du har svarat Ja eller Osäker på föregående fråga

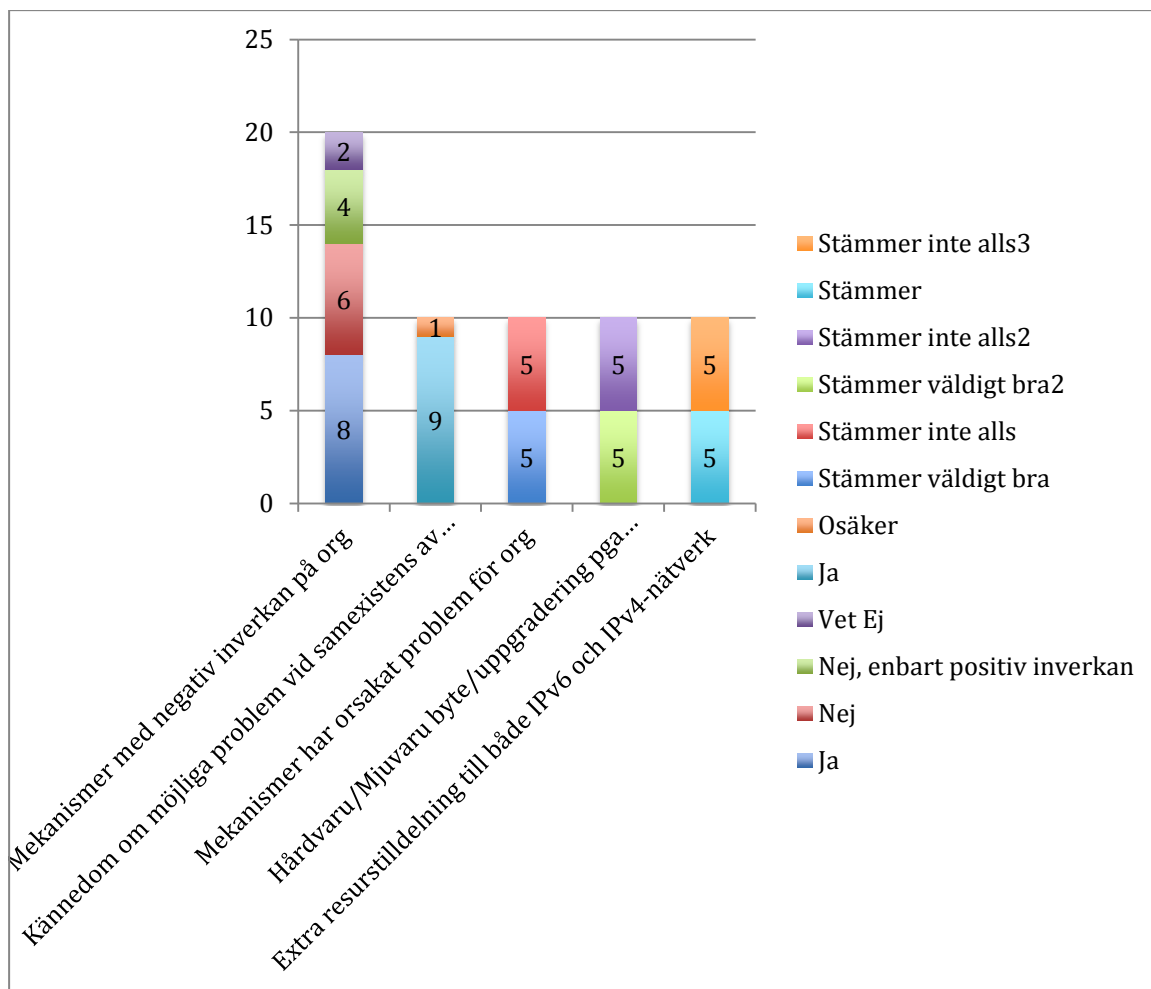
Detta är en följdfråga till föregående fråga beroende på om respondenten svarat ja eller nej.

Information/tjänst har varit otillgänglig	53 %
Obehöriga har kommit åt information	20 %
Information har modifierats av obehöriga	13 %
Vi har blivit drabbade men väljer att inte avslöja några detaljer	37 %

Ungefär en tredjedel av respondenterna har återigen svarat att de inte vill avslöja detaljer. Tillgängligheten verkar också vara den egenskapen som vanligtvis drabbas. Detta kan ha ett samband med en del av kommentarerna, där respondenterna har skrivit om problem med routern, som verkar vara nyckeln till många problem gällande tillgängligheten. Övriga frågor är sammanfattade nedan i figur 31 och 32.



Figur 31 Fördelning av utrustning som krävt byte/uppgradering pga. samexistensen



Figur 32 Sammanfattning av svar från respondenter för frågor i del 3

6.4 Intervju för delmål 3

Målet med intervjuerna som utförts var att de skulle komplettera enkätundersökningen genom att förse undersökningen med djupa, utvecklade och tydliga svar. Planen var att ställa fasta fixerade frågor som den intervjuade hade fått svara på, där sedan varje svar följs upp av en diskussion. Tanken var även att diskussionen skulle öppna för nya frågor. Totalt genomfördes två intervjuer.

Tyvärr har målen med intervjuerna inte fått den genomslagskraft man hade hoppats på utan kommer istället att ge en mer generell bild av situationen för de båda företagen. Det innebär att intervjuerna inte har bidragit till mer utvecklade svar rörande säkerhetsproblemen. Vid båda besöken var först någon form av kontrakt angående konfidentialitet tvungen att skrivas under. Företagens motivering till detta var företagets sekretesspolicy och att förhindra eventuellt avslöjad känslig information från att läcka ut. Denna händelse var oväntad då båda intervjuerna planerades via telefonsamtal, där det avslöjades vad som kommer att diskuteras och reaktionen till detta var då positiv.

De intervjuade från båda företagen har dessutom uttryckt att de önskar total anonymitet både för sig själva och företaget som organisation. Dessa krav har försvårat arbetet med undersökningen och kommer därmed inte att bidra med några djupare diskussioner rörande säkerhetsproblemen och deras påverkan. Dock kan det avslöjas att säkerhetsproblemen som

diskuterats i intervjun, liknar mycket de som har presenterats i detta arbete. Vidare fick frågorna som var planerade ändras till mer generella frågor under pågående intervju med båda företagen.

Båda företagen har varit utsatta när det gäller säkerhetsproblem som kan uppstå vid en övergång. Det som presenteras här har företagen i efterhand via telefonsamtal gett sitt medgivande till. Företagen kommer att kallas för A och X. Både företag A och X har sina huvudkontor i Västra Götalands Län. Företagen har totalt över 100 000 anställda runt om i världen och är globala koncerner. Det som b.l.a. kan avslöjas är att båda företagen använder för sina nätverk en nätverksarkitektur, som är väldigt lik detta arbetes kategorisering av övergångsmekanismer.

Representanter för företag X har uttryckt en stark negativ påverkan som relateras till övergångsmekanismer. Företaget har varit utsatt för angrepp som har lett till negativ påverkan för alla egenskaper inom informationssäkerheten dvs. tillgänglighet, konfidentialitet och sekretess. Trots utarbetade strategier för en övergång till IPv6 och analyser av risker för eventuella säkerhetsproblem, har företaget som de själva uttryckt det, *"fallit i en grop"*. Representanterna själva för företaget tror att en anledning till detta misslyckande kan bero på att för många parter har varit inblandade vid analysen för riskerna och planeringen, både internt och från externt håll. Även otillräcklig kompetens kan ha varit en bidragande orsak.

Företaget X har påverkats negativt på flera olika sätt. Påverkan har yttrat sig b.l.a. i form av tid och utbildningskostnader rörande IPv6 och övergångsmekanismer för personal från externt håll. Angreppet mot företag X har resulterat i omstrukturering i stora delar av nätverket samt bidragit till kostsamma byten av hårdvara och mjukvara. Ekonomin är alltså ett stort problem här, där representanterna hävdar att enbart intrånget rörande informationssäkerhet, har kostat företaget hundratusentals kronor.

Även representanter för företag A har uttryckt en negativ påverkan som kan relateras till övergångsmekanismer. Framförallt har säkerhetsproblemen orsakat produktionsbortfall för företaget, vilket i sin tur har lett till ekonomiska förluster. Dock hävdar representanterna att de ekonomiska förlusterna för det här fallet är minimala. Det som däremot varit kostsamt är uppgraderingen av hårdvara inför övergången till IPv6 samt säkerhetsåtgärder för de säkerhetsproblem som uppstått och en uppföljning av dessa. Även tiden som behövt avsättas för detta har påverkat IT-personalen och ekonomin negativt. Till exempel långa perioder av personalbrist är en effekt där resterande intern IT-personal upplevt ett högre tryck i verksamheten. Detta kan härledas till kommentarer från enkätundersökningen som till exempel:

"Vi har varit tvungna att byta och omstrukturera hårdvara efter virus attack."

Detta tyder på att det finns ett samband och likhet i den negativa påverkan mellan de intervjuade företagen och myndigheterna i enkätundersökningen.

6.5 Analys

Denna delsektion har som syfte att analysera svaren från onlineenkäten och intervjuerna i sektion 6.

6.5.1 Bakgrund och erfarenhetsanalys del 1 onlineenkät

Sammanlagt markerade 22 respondenter i enkätens del 1 att de har en högskoleutbildning, vilket innebär 73 procent av respondenterna är utbildade på en högre nivå. 70 procent har dessutom svarat att de genomgått någon form av IPv6-utbildning. Detta möjliggör att svaren i enkäten kan tolkas som mycket trovärdiga. Dessutom har 50 procent av respondenterna en över 15 år lång arbetslivserfarenhet inom IT. Dessutom har 87 procent av systemadministratörerna uppgett att de administrerar eller har administrerat nätverk med övergångsmekanismer. Samtliga 30 respondenter känner även till kategoriseringen av övergångsmekanismerna. Dessa resultat ökar tillförlitligheten och trovärdigheten för systemadministratörernas svar i enkäten.

6.5.2 Sammanfattande analys

Utifrån korta analyser av onlineenkätens svar och intervjuerna kan slutsatsen dras att en klar majoritet av deltagarna för undersökningen har utsatts och påverkats negativt av övergångsmekanismer. Organisationerna har påverkats negativt gällande ekonomi och informationssäkerheten har påverkats negativt av övergångsmekanismerna samt att den dyrbara tiden och arbetet även har påverkats negativt. Negativ inverkan kan även härledas till att samtliga använder dual stack-mekanismen. Respondenter har kommenterat problem med dual stack som:

*”Det vi upplever som mest krävande i form av arbete/tid är underhållande av dubbla uppsättningar säkerhetskonfigurationer, främst access-listor, för både IPv4 och IPv6.”,
”Kan kort avslöja att vår org varit utsatta för virusangrepp som har ett samband med dual stack arkitekturen”*

Detta kan ha ett samband med det som Liu et al. (2009) skriver att det finns specifika maskar som kan angripa mål i dual stack-nätverk. Vidare kan detta även härledas till angreppet på företag X som troligen använder dual stack. Dock kan detta inte styrkas eftersom det saknas bekräftelse på om de verkligen använder en sådan arkitektur. Här har även tid och arbete uppgetts som en negativ aspekt, vilket har en koppling till det som Taib & Budiarto (2007) skriver, att tjänster som t.ex. brandväggar bör stödja versionerna av protokollet.

Närmare 64 procent av myndigheterna har upplevt säkerhetsproblem som relateras till övergångsmekanismer, där 53 procent angett att tillgängligheten till information påverkats. 37 procent har angett att de blivit drabbade men väljer att inte avslöja detaljer.

Detta är det mest anmärkningsvärda resultatet som framkommit i undersökningen. Representanterna för företagen hade en väldigt kall och känslig inställning till ämnet i fråga, vilket i helhet påverkade hela undersökningen negativt. Denna inställning kan bero på och vara ett negativt resultat av att organisationerna utsatts för säkerhetsproblem, närmare bestämt 64 procent. Effekten av detta kan vara en spridning om negativ påverkan till organisationer som inte har påbörjat övergång än. Dessa problem kan mycket väl vara en bidragande orsak till varför många myndigheter än idag väntar med att gå över till IPv6.

Dock kan denna känsliga inställning knytas till enkätundersökningen, där 37 procent är en stor siffra för 30 respondenter. Vidare har denna känslighet gjort det mycket svårt att jämföra säkerhetsproblemen för övergångsmekanismerna, där majoriteten av respondenterna från enkätundersökningen inte har avslöjat detaljer. Kommentarer som kan härledas till informationssäkerheten är följande:

”Vi har använt tunnling för vissa tjänster fram till nyligen och slutat med det eftersom 6to4 arkitekturen har orsakat problem med säkerhet och hårdvaran”, ”kortare avbrott pga routingfel”, ”Vi hr haft en del routingfel tack vare mekanismen samt 6to4 har orsakat problem på routingen och brandväggsfunktionerna. Mer väljer vi att inte avslöja.” ”På grund av felaktig routing så har vissa tjänster varit otillgängliga via IPv6 och med fördröjning då det ofta tar tid innan klienter försöker med IPv4 när IPv6 inte är nåbart.”, ”Problemen har orsakat bla anställda har inte kommit åt sina program samt att konfidentiell information blivit tillgänglig. Känslig fråga.” ”epost från epost-system med ipv6 aktivt har läckt igenom icke-intrimmade filter i border-router.”

Dessa kommentarer tyder på att det finns ett samband mellan beskrivna säkerhetsproblem som handlar t.ex. om tunnlingstekniken 6to4 och litteraturstudien. I litteraturstudien framgår det som Bi et al. (2007) skriver, nämligen att 6to4 kan skapa säkerhetsproblem. Vidare bekräftar resultaten och kommentarerna att mer än hälften av myndigheterna har drabbats negativt med den negativa inverkan som säkerhetsproblemen kan ha på informationssäkerheten.

Svaren från undersökningen tyder på att majoriteten av organisationer dvs. både de intervjuade företagen och myndigheternas respondenter, har påverkats negativt. För företagen har en negativ påverkan inneburit förlust av tid, driftstopp, kostsamma byten av hårdvara och mjukvara, vilket tyder på att ekonomin påverkats mycket som en följd av detta. Vidare kan detta knytas till många av respondenternas svar och kommentarer, vilka har angett att ekonomin påverkats negativt samt byte av hårdvara. Exempel på kommentarer:

”Väljer att inte gå in på detaljer men vi har blivit drabbade där brister i säkerheten rörande mekanismer slutligen haft negativ inverkan på främst ekonomin.”, ”Hårdvaruleverantörerna är en bromskloss för att vi ska kunna köra ipv6 ordentligt”, ”Vi har använt tunnling för vissa tjänster fram till nyligen och slutat med det eftersom 6to4 arkitekturen har orsakat problem med säkerhet och hårdvaran”, ”Problemen vi haft har orsakat ekonomiska och it relaterade besvär för vår organisation”, ”Byte av hårdvara och ekonomiska följder”

I dagsläget där IPv4 och IPv6 samexisterar har 70 procent uppgett att de påverkats negativt pga. övergångsmekanismerna genom byte eller uppgradering av hårdvara, vilket bekräftar det som Wu et al. (2013) skriver, nämligen att routrar, servrar och brandväggar kan behöva bytas eller uppgraderas som en negativ konsekvens av övergångsmekanismerna.

7 Slutsats

Denna sektion presenterar de slutsatser för resultaten och analysen från sektion 6. De kommer att diskuteras utefter problemfrågeställningen och delmålen för problemet samt huruvida dessa har uppfyllts.

7.1 Slutsats och delmål

Detta arbetes problemfråga löd på följande sätt:

Vilka säkerhetsproblem gällande informationssäkerhet kan uppstå vid olika övergångsmekanismer från IPv4 till IPV6 och hur påverkar de organisationen?

Problemfrågan fick brytas ner till 5 delmål.

7.1.1 Delmål 1

Syftet med delmål 1: *Identifiera de säkerhetsproblem gällande informationssäkerhet som kan uppstå vid olika övergångsmekanismer.*

De resultat som presenterats i sektion 6, tyder på att det finns en del säkerhetsproblem som kan relateras till olika övergångsmekanismer. Säkerhetsproblemen kan uttrycka sig i form av maskar, felaktig konfiguration i dual stack-nätverk eller paketförfalskning och DDoS-attacker vid tunneling och translation. Det har framkommit i undersökningen att dessa problem kan ha en mycket allvarlig effekt på organisationer med en direkt påverkan på informationssäkerhetens tre grundstenar: Tillgänglighet, integritet och sekretess. Då en mängd säkerhetsproblem har identifierats, har delmål 1 uppfyllts. Dock finns säkerligen en hel del andra säkerhetsproblem också men de som fick flest träffar genom litteratursökningen i databaserna har istället valts.

7.1.2 Delmål 2

Syftet med delmål 2: *Undersökning om hur stor kunskap och erfarenhet organisationens systemadministratörer har gällande övergångsmekanismer och IPv6.*

Resultaten för detta delmål tyder på att administratörernas förmåga att svara på frågor rörande övergångsmekanismer och säkerhetsproblem, kan räknas som trovärdig där svaren kan anses vara tillförlitliga. Anledningen till detta är administratörers arbetslivserfarenhet, erfarenhet av IPv6-nätverk, utbildning och kunskap om t.ex. kategorisering av övergångsmekanismer. Resultaten för dessa aspekter har varit mycket tillfredsställande och därmed har delmål 2 uppfyllts.

7.1.3 Delmål 3

Syftet med delmål 3: *Undersöka hur övergångsmekanismer och relaterade säkerhetsproblem kan påverka organisationen gällande informationssäkerhet.*

Här har undersökningen avslöjat en hel del intressanta resultat. Resultaten från intervjuerna visar att ämnet som undersöks, är väldigt känsligt för organisationerna, i synnerhet de två företag som intervjuats. Man vill inte gå in på detaljer utan svarar så ytligt som möjligt. Ändå har det framkommit att företagen har utsatts för angrepp. Företagen har påverkats negativt av övergångsmekanismer med främst ekonomiska konsekvenser, byte av hårdvara och mjukvara, samt avsatt tid för omstrukturering av nätverk. Även enkäten har visat ungefär samma resultat i de flesta fall fast med en mer tydlig inblick i hur informationssäkerheten har

påverkats. En fördel är de många kommentarer som getts till svarsalternativen. Dock har de flesta som kommenterat inte valt att avslöja detaljer, vilket följer en ungefärligt likadan trend som med de intervjuade företagen. Delmål 3 har uppfyllts genom att en onlineenkät har skapats och skickats ut för att undersöka problemfrågan.

7.1.4 Delmål 4

Syftet med delmål 4: *Undersöka om systemadministratörer idag i en fas av samexistens mellan IPv4 och IPv6 upplever problem/säkerhetsproblem.*

Undersökningen för delmål 4 har fått en egen del i onlineenkäten där resultaten tyder på att hälften av respondenterna upplever problem med övergångsmekanismerna. Dessa problem innebär uppgradering av hårdvara och mjukvara, där hälften har angett att det stämmer väldigt bra. Resurstilldelningen har däremot enligt hälften av respondenterna varit rimlig medan de resterande 50 procenten angivit att detta inte alls stämmer. Eftersom onlineenkäten har berört problem i fasen av samexistens mellan IPv4 och IPv6, har delmål 4 uppfyllts.

7.1.5 Delmål 5

Syftet med delmål 5: *Jämföra och sammanställa resultat från organisationerna och de föregående delmålen för att sedan analysera och dra slutsatser utifrån dessa delmål.*

Resultaten från onlineenkäten har jämförts med intervjuerna och litteraturstudien och sammanställts där dessutom slutsatser har dragits. I och med detta har det femte delmålet uppfyllts. Det har varit svårt att dra konkreta slutsatser och föra djupa analyser eftersom en del deltagare i undersökningen har varit tillbakadragna i sina svar, i synnerhet representanterna från de två företagen som intervjuats.

7.1.6 Sammanfattning

Det här arbetet har påvisat att majoriteten av deltagarnas organisationer har blivit negativt påverkade av övergångsmekanismerna, där egenskaperna för informationssäkerheten kan drabbas. Tillgängligheten är den egenskap som verkar mest utsatt. Det som dessutom har framkommit av intervjuerna och enkätundersökningen är att ämnet är väldigt känsligt att diskutera och organisationerna vill helst inte gå in på detaljer gällande negativ påverkan.

Problemet med varför myndigheter väljer att dröja med en övergång till IPv6 kan bero just på att övergångsmekanismerna orsakar mycket problem, där konsekvenserna i form av omstrukturering, ekonomi och informationssäkerhet kan få allvarliga följder. Eftersom alla organisationer i undersökningen kände till övergångsmekanismerna och säkerhetsproblemen, kan detta tyda på att de som inte har påbörjat en övergång, redan känner till de potentiella problemen och därför undviker en övergång till IPv6.

Genom detta arbete kan organisationer, som inte har påbörjat en övergång få en mer klar bild över situationen med övergångsmekanismerna och de relaterade säkerhetsproblemen. Rapporten medför en ökad förståelse och kunskap om övergångsmekanismerna och hur allvarliga säkerhetsproblemen och följderna av dessa kan vara. En ökad förståelse och kunskap kan då underlätta för systemadministratörer inför och under en övergång till IPv6. Ett exempel på detta är den beskrivna dual stack-mekanismen, som kan vara en guide för administratörer till att undersöka brandväggsfiltrering för båda protokollen i ett nätverk. Det här arbetet kan användas som underlag för beslutsfattare när det kommer till frågor om att fatta viktiga beslut inför en övergång till IPv6.

8 Diskussion

Rapporten har visat att övergångsmekanismer kan orsaka säkerhetsproblem som i sin tur har påverkat mer än hälften av myndigheterna som undersökts. Trots att en majoritet av administratörer som har erfarenhet och kännedom övergångsmekanismer och relaterade säkerhetsproblem, har ändå mer än hälften av alla undersökta myndigheter drabbats. Detta tyder på att det kan finnas ett ökat behov av att utbilda systemadministratörer med en klar fokus på övergångsmekanismer och säkerhetsproblemen.

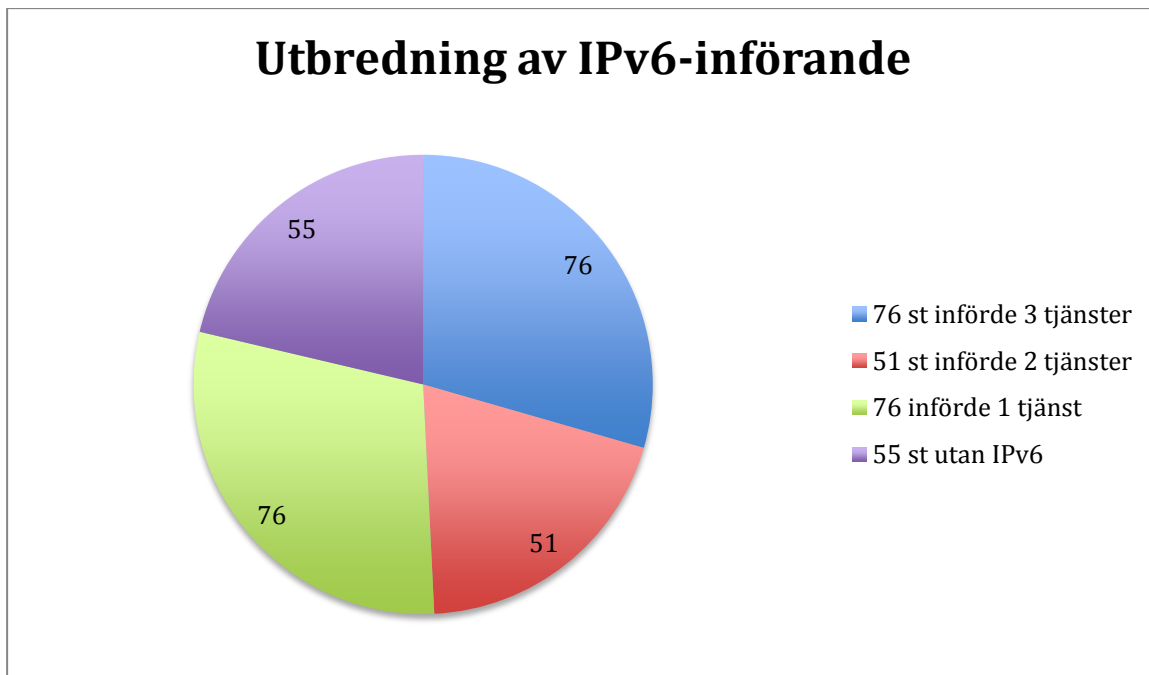
Vidare är det en överraskande bild som de intervjuade företagen har gett gällande negativ påverkan, i synnerhet de ekonomiska summorna. Dock har inte intervjuerna gett mer förväntade tydliga resultat i förhållande till enkätundersökningen. Den negativa påverkan med eventuella ekonomiska följder kan mycket väl vara ett avskräckande exempel för andra organisationer, som inte har påbörjat en övergång än, samt en bidragande orsak till varför en övergång dröjer.

Detta arbete har använt tre metoder, vilka var litteraturstudie, enkätundersökning och intervjuer. Enkätundersökningar som vanligtvis har en låg svarsfrekvens, har i detta fall istället haft en relativt rimlig svarsfrekvens på 20 procent med 30 deltagare som genomfört onlineenkäten. Det är fortfarande en låg svarsfrekvens men med tanke på administratörernas bakgrund, erfarenhet, kunskap och utbildning, kan resultaten ändå räknas som tillförlitliga.

Trots detta har inte allt för stora slutsatser kunnat dras med tanke på att svaren inte har varit så detaljerade som man hade hoppats på. Vidare har deltagarna i undersökningen förmedlats om syftet med undersökningen genom en inbjudan till enkäten, där syftet beskrivs som endast en undersökning om IPv6, övergångsmekanismer och relaterade säkerhetsproblem. Deltagarna har getts full frihet att svara på enkäten om de vill som de önskar, förutom att de antingen måste välja del 2 eller del 3. Deltagarna har även blivit meddelade om full anonymitet.

Frågorna i enkäten skulle säkerligen kunnat ha utformats på ett annat sätt så att deltagarna t.ex. inte skräms bort eftersom ämnet i fråga nu har visat sig vara så extremt känsligt. Dock finns i skrivande stund inga förslag till andra typer av frågor. Frågorna som var utformade för intervjuerna var relativt lika de frågor som utformats för enkäten, fast med skillnaden att mera detaljer efterlystes i frågorna för intervjuerna. Dessa frågor fick överges vid påbörjandet av intervjun på begäran de intervjuade och de nya frågorna fick istället ställas löpande under intervjuerna. Detta var en högst oväntad reaktion och händelse för båda intervjutillfällena.

Resultaten som presenterats kan mycket väl vara en bidragande orsak till att övergången inte sker i den takt som regeringen och PTS hade hoppats på. Övergången till IPv6 är i dagsläget fortfarande en pågående process, dock fortfarande långsam. Figur 33 nedan visar hur fördelningen av ett infört IPv6-protokoll ser ut i dagsläget. Siffrorna är hämtade från PTS, där informationen uppdateras dagligen (PTS E-tjänster, 2013)



Figur 33 Utbredning av IPv6-införandet för svenska myndigheter. Texten är tagen från (PTS E-tjänster, 2013)

8.1 Framtida arbeten

I denna delsektion framförs exempel på framtida undersökningar som eventuellt skulle kunna komplettera denna rapport.

- En undersökning om IPv6 gällande övergångsmekanismer och relaterade säkerhetsproblem, fast på en global nivå. En enkätundersökning som kanske kan täcka in något av eller alla de skandinaviska länderna för att jämföra med situationen där.
- En studie som undersöker hur frekventa problemen, som orsakats av övergångsmekanismer, har varit för de organisationer som redan gjort en heltäckande övergång till IPv6.
- Undersöka hur man på bästa sätt kan förhindra att en del eller alla redan nämnda övergångsmekanismer orsakar säkerhetsproblem för organisationerna.

Referenser

- Amoss, J. J. & Minoli, D. (2008). *Handbook of IPv4 to IPv6 Transition: Methodologies for Institutional and Corporate Networks*. Boca Raton, FL: Auerbach Publications.
- Berndtsson, M., Hansson, J., Olsson, B. & Lundell, B. (2008) *Thesis Projects: A Guide for Students in Computer Science and Information Systems* (andra utgåvan). London: Springer Verlag.
- Bi, J., Wu, J. & Leng, X. (2007) IPv4/IPv6 Transition Technologies and Univer6 Architecture. *International Journal of Computer Science and Network Security*, 7(1), 232-243. Tillgänglig på Internet: http://paper.ijcsns.org/07_book/200701/200701B06.pdf [14-03-21].
- Cho, K. & Bae, K. (2010) *The Problems and their solutions when using SIP in NAT Environment*. 5th international conference, Computer Sciences and Convergence Information Technology (ICCIT), Seoul, December 2010. s. 997-1000.
- Cisco (2005) *IP Routing: TCP/IP Overview*. Tillgänglig på Internet: <http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13769-5.html> [14-03-02].
- Cisco (2009) *CCNA Exploration 4.0: Network Fundamentals*. Cisco Networking Academy. Cisco Systems Inc.
- Comer, D. E. (2014) *Internetworking With TCP/IP Vol I: Principles, Protocols, and Architecture* (6:e upplagan). Upper Saddle River: Pearson Education.
- Das, K. (2008a) *Network Adress Translation (NAT) Pros & Cons*. Tillgänglig på Internet: <http://www.ipv6.com/articles/nat/NAT-Pros-and-Cons.htm> [14-03-02].
- Das, K. (2008b) *IPv6 – The History and Timeline*. Tillgänglig på Internet: <http://www.ipv6.com/articles/general/timeline-of-ipv6.htm> [14-03-02].
- Das, K. (2008c) *IPv6 Header Deconstructed*. Tillgänglig på Internet: <http://www.ipv6.com/articles/general/IPv6-Header.htm> [14-03-27].
- Das, K. (2008d) *ICMPv6 - Tech Details Advantages*. Tillgänglig på Internet: <http://www.ipv6.com/articles/general/ICMPv6.htm> [14-03-27].
- Davies, E., Krishnan, S. & Savola, P. (2007) *IPv6 Transition/Co-existence Security Considerations. Request for Comments 4942*. Tillgänglig på Internet: http://www.hjp.at/doc/rfc/rfc4942.html#sec_3 Hämtad [14-03-19].
- Dobrijevic, O., Svedek, V. & Matilasevic, M. (2012) *IPv6 Deployment and Transition Plans in Croatia: Evaluation Results and Analysis*. Zagreb: University of Zagreb. Tillgänglig på Internet: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6347659&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D6347659 Hämtad [13-12-16].

Gont, F. (2011) *IPv6 security issues: IPv6 transition mechanisms*. Tillgänglig på Internet: <http://searchsecurity.techtarget.com/tip/IPv6-security-issues-IPv6-transition-mechanisms> [14-03-02].

Govil, J., Govil, J., Kaur, N. & Kaur, H. (2008) An Examination of IPv4 and IPv6 Networks: Constraints and Various Transition Mechanisms. *Proceedings of the 2008 IEEE Southeastcon Symposium. SECON '08. Huntsville, AL, USA, IEEE*. s. 178–185.

Hagen, S. (2006) *IPv6 Essentials* (2:a upplagan). Sebastopol, CA: O'Reilly.

Halsall, F. (2005) *Computer Networking and the Internet* (5:e upplagan). Harlow: Pearson Education Limited.

Huitema, C. (2006) *Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)*. Tillgänglig på Internet: <http://www.ietf.org/rfc/rfc4380.txt> Hämtad [14-04-05].

IETF (1981a) *Internet Protocol". Request for Comments 791*. Tillgänglig på Internet: <http://www.ietf.org/rfc/rfc791.txt> Hämtad [13-11-01].

IETF (1981b) *TRANSMISSION CONTROL PROTOCOL*. Tillgänglig på Internet: <http://www.ietf.org/rfc/rfc793.txt> Hämtad [14-03-21].

IETF (2007) Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status. Tillgänglig på Internet: <http://tools.ietf.org/html/rfc4966> [14-03-27].

IETF (2012) *Dual-Stack Hosts Using "Bump-in-the-Host"*. Tillgänglig på Internet: <http://tools.ietf.org/html/rfc6535> [14-03-27].

Informationssäkerhet.se *IPv6: Att införa IPv6 är också en fråga om säkerhet*. Tillgänglig på Internet: <https://www.informationssakerhet.se/sv/vagledning/IPv6-och-DNSSEC/> [14-03-23].

Lewis, D. & Che, X. (2010) *IPv6: Current Deployment and Migration Status*. International Journal of Research and Reviews in Computer Science, 1(2). Swansea: Faculty of Applied Design and Engineering.

Liu, T., Guan, X., Zheng, Q. & Qu, Y. (2009) A New Worm Exploiting IPv6 and IPv4-IPv6 Dual-Stack Networks: Experiment, Modeling, Simulation, and Defense. *Network, IEEE*. 23 (5), s. 22–29.

Magnusson, A. (2011a) Nu är IPv4-adresserna slut. Tillgänglig på Internet: <https://www.idg.se/2.1085/1.366370> [14-03-02].

Magnusson, A. (2011b) IPv6.övergång dras med risker. Tillgänglig på Internet: <http://techworld.idg.se/2.2524/1.366887/ipv6-overgang-dras-med-risker> [14-03-02].

Palmer, C. (2012) Building Windows 8: *Connecting with IPv6 in Windows 8*. Tillgänglig på Internet: <http://blogs.msdn.com/b/b8/archive/2012/06/05/connecting-with-ipv6-in-windows-8.aspx> [14-03-29].

Parkhurst, W. R. (2004) *Internet Addressing and Routing First Step*. Tillgänglig på Internet: <http://www.ciscopress.com/articles/article.asp?p=348253&seqNum=7> [14-03-20].

Pfleeger, C. P. & Pfleeger, S. L. (2006) *Security in Computing*. s. 375-388. (4:e upplagan) Upper Saddle River: Pearson Education.

PTS (2011) *Att införa IPv6 - PTS-ER-2011:18*. Tillgänglig på Internet: <http://www.pts.se/sv/Dokument/Rapporter/Internet/2011/Att-infora-IPv6---PTS-ER-201118/> [14-03-29].

PTS (2013) *Myndigheter I otakt kring IPv6-införande*. Tillgänglig på Internet: <http://www.pts.se/sv/Nyheter/Pressmeddelanden/2013/Myndigheter-i-otakt-kring-IPv6-inforande/> [14-03-13].

PTS E-tjänster (2013) *Myndigheter med IPv6*. Tillgänglig på Internet: <http://e-tjanster.pts.se/internet/ipv6> [14-03-13].

SecurityFocus (2010) *SecurityFocus*. Tillgänglig på Internet: <http://www.securityfocus.com/glossary/P> [14-03-21].

Taib, A.H.M. & Budiarto, R. (2007) Security Mechanisms for the IPv4 to IPv6 Transition. *The 5th Student Conference on Research and Development. SCORED '07. Selangor, Malaysia, IEEE Xplore*. s. 1–6.

Wu, P., Cui, Y., Wu J., Liu, J. & Metz, C. (2013) Transition from IPv4 to IPv6: A State-of-the-Art Survey . *Communications Surveys & Tutorials, IEEE, 7(1)*, 1407-1424.

Zagar, D. & Grgic, K. (2006) IPv6 Security Threats and Possible Solutions. *Automation Congress. WAC '06. Budapest, Hungary*. s. 1-7.

Appendix A - Onlineenkät

IPv6: Övergångsmekanismer och säkerhetsproblem

Hej

Denna enkät består av 3 delar. Totalt är det två delar som besvaras beroende på om övergången till IPv6 är fullbordad eller inte.

Med fullbordad övergång menas att webbtjänst, e-post och DNS-tjänsten är nåbar med IPv6. Undersökningen tar cirka 10 minuter.

Del 1: Denna del är avsedd för alla svarsdeltagare och undersöker administratörens erfarenhet och bakgrund.


Del 2: Denna del är endast avsedd för er som har påbörjat ett införande av IPv6.

Del 3: Denna del är avsedd för er där övergången räknas som fullbordad och kör en samexistens med IPv4 och IPv6-protokoll.

Undersökningen är fullständig anonym och det är viktigt att ni svarar ur organisationens perspektiv och så utförligt som möjligt.

Om ni upplever att vissa frågor inte går att svara på, kan ni antingen stänga undersökningen och avvakta tills ni vet svaret, eller helt enkelt hoppa över frågan ni är osäkra på och svara på de andra frågorna så gott det går.

[Fortsätt »](#)

Tillhandahålls av
 Google Forms

Det här innehållet har varken skapats eller godkänts av Google.
[Anmäl otillåten användning](#) - [Användarvillkor](#) - [Ytterligare villkor](#)

IPv6: Övergångsmekanismer och säkerhetsproblem

Del 1 Inledande frågor

Vilken utbildningsnivå har du?

Du kan välja fler än ett alternativ

- Grundskola
- Gymnasium
- Högskola/Universitet
- Vet ej

Har du gått någon IT-utbildning som berör IPv6?

- Ja
 Nej

Hur länge har du arbetat som nätverks/systemadministratör?

Administrerar du eller har du administrerat nätverk där övergångsmekanismer till IPv6 används?

- Ja
 Nej
 Vet ej

Här kan du utveckla ditt svar om du har svarat Ja eller Vet ej på ovanstående fråga

Känner du till att övergångsmekanismer kategoriseras i följande kategorier?

Dual Stack (Dubbla lager) - Tunneling - Translation (Översättning)

- Ja
 Nej
 Osäker

Här har du möjlighet att utveckla ditt svar från föregående fråga

[« Bakåt](#)

[Fortsätt »](#)

IPv6: Övergångsmekanismer och säkerhetsproblem

Del 2

Svara endast på dessa frågor om ni har påbörjat en övergång till IPv6 eller tryck på "fortsätt" längst ner på sidan för att komma till del 3. I del 3 finns även knappen "skicka" som avslutar och skickar in enkäten.

Vad för typ av övergångsmekanism/övergångsmekanismer använder ni?

Flera alternativ kan väljas eftersom övergångsmekanismer kan kombineras

- Dual Stack (Dubbla Lager)
- Tunneling (Tunnling)
- Translation (Översättning)
- Vet ej

Utveckla gärna kortfattat vilken teknik/tekniker ni använder för övergångsmekanismerna

T.ex. 6to4, Teredo, NAT-PT eller endast IPv6-IPv6 och IPv4-IPv4-kommunikation

Känner ni till potentiella säkerhetsproblem som kan uppstå vid en övergång från IPv4 till IPv6?

T.ex. säkerhetsproblem som kan uppstå i samband med dual stack, 6to4, NAT-PT, ISATAP mm.

- Ja
- Nej
- Vet ej
- Osäker

Här har du möjlighet att utveckla ditt svar på ovanstående fråga.

Har er organisation upplevt säkerhetsproblem som kan relateras till övergångsmekanismer?

Problem kan innebära allt från DDos-attacker till upptäckta sårbarheter i nätverket eller t.ex. IPv6-IPv4 tunnlar som används för att kringgå IPv4-paketfiltreringen, både från internt eller externt

- Ja
- Nej
- Vet ej
- Osäker

Om du har svarat Ja eller Osäker på föregående fråga

Det eller de problem som drabbat vår organisation har påverkat följande:

- Information/tjänst har varit otillgänglig
- Obehöriga har kommit åt information
- Information har modifierats av obehöriga
- Vi har blivit drabbade men väljer att inte avslöja några detaljer

Beskriv gärna själv kortfattat om något av alternativen ovan inte passar in för er problemsituation

Har övergångsmekanismen/mekanismerna på något sätt haft en negativ inverkan på nätverket/organisationen?

- Ja
- Nej
- Nej, mekanismerna har enbart haft positiv inverkan
- Vet ej

Här har du möjlighet att utveckla ditt svar från föregående fråga

Har du något övrigt att tillägga?

« Bakåt

Fortsätt »

IPv6: Övergångsmekanismer och säkerhetsproblem

Del 3

Svara endast på dessa frågor om ni har fullbordat er övergång till IPv6

Vad för typ av övergångsmekanism/övergångsmekanismer använder ni?

Flera alternativ kan väljas eftersom övergångsmekanismer kan kombineras

- Dual Stack (Dubbla Lager)
- Tunneling
- Translation (Översättning)
- Vet ej

Här har du möjlighet att utveckla ditt svar från ovanstående fråga

T.ex. 6to4, Teredo, NAT-PT eller endast IPv6-IPv6 och IPv4-IPv4-kommunikation

Känner ni till potentiella säkerhetsproblem som kan uppstå vid en övergång från IPv4 till IPv6?

T.ex. säkerhetsproblem som kan uppstå i samband med dual stack, 6to4, NAT-PT, ISATAP mm.

- Ja
- Nej
- Osäker

Känner ni till de problem som kan uppstå vid en samexistens mellan IPv4 och IPv6?

- Ja
- Nej
- Osäker

De implementerade övergångsmekanismerna har orsakat problem för organisationen?

1 2 3 4 5

Stämmer inte alls Stämmer väldigt bra

Uppgradering av hårdvara och mjukvara har varit nödvändig för samexistensen av protokollen IPv4 OCH IPv6

Med detta kan menas om ni t.ex. har varit tvungna att uppgradera utrustning som t.ex. brandväggar, routrar mm.

1 2 3 4 5

Stämmer inte alls Stämmer väldigt bra

Följande utrustning har krävt byte eller någon form av uppgradering av nedanstående alternativ

Välj ett eller flera alternativ

- Router
- Server
- Klienter
- Brandvägg
- Inget av ovanstående alternativ

Extra resurstilldelning har varit nödvändig för att garantera likvärdig tjänst åt både IPv4- och IPv6 nätverket

Med resurser menas t.ex. bandbredd

1 2 3 4 5

Stämmer inte alls Stämmer väldigt bra

Här har du möjlighet att utveckla ditt svar från föregående fråga

Har er organisation upplevt säkerhetsproblem som kan relateras till övergångsmekanismer?

Problem i detta fall kan innebära allt från DDos-attacker till upptäckta sårbarheter i nätverket eller t.ex. IPv6-IPv4 tunnlar som används för att kringgå IPv4-paketfiltreringen, både från internt eller externt

- Ja
- Nej
- Vet ej
- Osäker

Om du har svarat Ja eller Osäker på ovanstående fråga

Det eller de problem som drabbat vår organisation har påverkat följande:

- Information/tjänst har varit otillgänglig
- Obehöriga har kommit åt information
- Information har modifierats av obehöriga
- Vi har blivit drabbade men väljer att inte avslöja några detaljer

Har du något övrigt att tillägga?

Skicka aldrig lösenord med Google Formulär

Appendix B - Enkätinbjudan

Hej!

Mitt namn är Dorian Mandic. Jag studerar Nätverks- och Systemadministration på Högskolan i Skövde. Just nu skriver jag ett examensarbete som handlar om IPv6: övergångsmekanismer och hur relaterade säkerhetsproblem kan påverka en organisation.

Jag vänder mig till Er i förhoppning om att ni kan hjälpa mig genom att svara på frågorna gällande införandet av IPv6 i er organisation. Jag vore oerhört tacksam om ni kunde ta er tid för att svara på frågorna så grundligt och uppriktigt som möjligt så att jag kan slutföra mitt examensarbete.

Undersökningen tar ca 10 min och er organisation är fullkomligt anonym.

Tack på förhand!

Dorian Mandic, Högskolan i Skövde

Enkäten finns tillgänglig på följande länk:

https://docs.google.com/forms/d/19DUely2B6wYT1HjauUVvw4mWl24NBIES3vXkqA5-iVA/viewform?usp=send_form

Appendix C - Enkätdata

Enkätdata i form av respondenternas kan läsas i ett separat dokument.