

MAGISTERUPPSATS I INFORMATIK
VID INSTITUTIONEN FÖR DATA- OCH AFFÄRSVETENSKAP
1997:M01

Översättning av nätverksadresser

- en kostnadseffektiv lösning för små och
medelstora företag att ansluta sig till Internet

Johan Sanneblad

Handledare: Fil. Dr. Bertil Lind

vt 1998



HÖGSKOLAN
I BORÅS

Sammanfattning

För varje dag som går ansluter sig en ständig ström nya företag och privatpersoner till det gigantiska nätverket Internet. Syftet med denna rapport är att finna en möjlighet för små och medelstora företag att låta samtliga anställda ha tillgång till onlinetjänsterna över Internet, till en låg kostnad. En explorativ studie har gjorts för att finna en lämplig plattform som kan användas som bas, varefter en utforskande undersökning har genomförts som förklarar bakomliggande tekniker och teorier. Ett system har implementerats och testats i skarp miljö hos tre företag med skilda behov i syfte att granska både systemets funktionalitet och de anställdas Internetanvändande. Resultatet visar att en majoritet av de involverade personerna som utvärderat systemet ökade sitt Internetanvändande, även om de redan tidigare hade tillgång till en anslutning. Programvaran som används för studien är gratis och en bilaga till rapporten visar samtliga steg som krävs för att själv installera och anpassa en egen länk mot omvärlden.

Nyckelord Internet, Internetanslutning, översättning av nätverksadresser, network address translation, NAT, kostnadseffektivitet, lokala nätverk

Förord

Jag vill först och främst tacka samtliga inblandade på de företag som deltagit i studien. Detta projekt hade ej varit genomförbart utan Er hjälp, och det är också Er vilja att ställa upp som fört vidare konceptet med fri tillgänglig programvara, från de tekniskt orienterade utvecklingsmiljöerna till det mindre företaget med funderingar på att ansluta sig till Internet!

Jag vill även att tacka Jürgen Claussen och Bill Andersson på Institutionen för Data- och Affärsvetenskap som lånade ut de fem datorsystemen till mig som krävdes för studien. Även om endast tre av dem användes, så var det lika bra att vara ordentligt förberedd.

Min verksamhet på Högskolan som utvecklare och administratör av kursplanssystem och Högskolans hemsidor på Internet hade ej möjliggjorts om det ej var för Per Zaring, som är föreståndare på forskningscentret ITCentrum. Den kunskap jag här inhämtade om Unix och Internet kom väl till nytta vid genomförandet av denna studie.

Slutligen vill jag rikta ett varmt tack till min handledare Bertil Lind och min studiekamrat Göran Golcher, som båda varit ett ovärderligt diskussionsstöd för att ventiler mina tankar och idéer kring det som idag formats till denna rapport. Detsamma gäller även mina föräldrar Karin och Peter Sanneblad, som frivilligt tagit sig an uppgiften att korrekturläsa de olika revisioner som sammanställts av rapporten. Jag hade inte kunnat genomföra rapporten på utsatt tidsram utan någon av Er!

Johan Sanneblad

Borås, den 14 april 1998

Innehållsförteckning

1	INLEDNING	1
1.1	BAKGRUND	1
1.1.1	<i>Datorn som kommunikationsmedium</i>	2
1.1.2	<i>Framtidens systemutvecklingsmiljöer</i>	3
1.1.3	<i>Att ansluta ett företag till Internet</i>	4
1.1.4	<i>Konsten att dela på en Internetadress</i>	5
1.2	PROBLEMFÖRMULERING	6
1.3	PROBLEMAVGRÄNSNING	7
1.4	SYFTE OCH MÅLGRUPP	7
1.5	FÖRVÄNTAT RESULTAT	8
1.6	EGNA RELATIONER OCH FÖRUTSÄTTNINGAR	8
1.7	DEFINITIONER	9
2	TEORETISK BAKGRUND	13
2.1	RELATERAT ARBETE	13
2.1.1	<i>Request for Comments (RFC)</i>	14
2.1.2	<i>IPng</i>	14
2.1.3	<i>Linux</i>	15
2.1.4	<i>Dial on Demand</i>	17
2.2	TEORIER AV BETYDELSE	18
2.2.1	<i>Nätverksadressering</i>	18
2.2.2	<i>OSI-modellen</i>	24
2.2.3	<i>Olika nätverksprotokoll</i>	26
2.2.4	<i>Nätverkssäkerhet</i>	33
2.3	PERSPEKTIV OCH TEORIVAL	34
3	METODVAL OCH METODBESKRIVNING	37
4	GENOMFÖRANDE	39
4.1	PLANERING	39
4.2	PRAKTISKT ARBETE	40
4.2.1	<i>Teknisk inventering</i>	40
4.2.2	<i>Litteraturstudie</i>	41

4.2.3	<i>Test</i>	41
4.3	PROBLEM	45
5	RESULTAT	47
5.1	INSAMLAT MATERIAL.....	47
5.1.1	<i>Teknisk utvärdering</i>	47
5.1.2	<i>Kostnadsmodell</i>	48
5.1.3	<i>Enkät</i>	49
5.2	RESULTATANALYS.....	51
5.2.1	<i>Personliga erfarenheter</i>	52
5.2.2	<i>Programvara och systemproblem</i>	52
6	SLUTSATSER	55
6.1	GENERELL METODUTVÄRDERING.....	56
6.2	SAMMANFATTANDE UTVÄRDERING AV ARBETET.....	57
6.3	EGNA REFLEXIONER.....	57
6.4	IDÉER FÖR FORTSATT FORSKNING	58

Figurförteckning

2.1	Adressintervaller för IP-adresser	19
2.2	Subnätsindelning av en klassC-adress	20
2.3	Två exempel på subnätmask i olika klassC-nät	20
2.4	Rekommenderade nätverksadresser för lokala nätverk	21
2.5	Översättning av nätverksadresser – ett exempel	23
2.6	Protokollsviten TCP/IP tillsammans med protokollsviten PPP	25
2.7	Inkapsling av data enligt TCP/IP-sviten	26
2.8	IP-fragmentering av ett TCP-paket	29
2.9	Inkapsling av ICMP-meddelanden i ett IP datagram	30
2.10	Inkapsling av UDP	31
2.11	Inkapsling av TCP-data i ett IP datagram	31

Bilagor

A	Enkät	2s
B	Installationsanvisningar	23s

1 Inledning

1.1 Bakgrund

”Internet åt folket” är en slogan som använts flitigt vid annonsering av Internetabonnemang de senaste åren. För att idag ansluta sig till Internet räcker det med en vanlig persondator och en telefonlinje, där övrig utrustning levereras i färdiga paket. Då datorerna blir allt snabbare till ständigt lägre priser blir det allt mer vanligt med ett flertal datorer även i små företag. Frågan uppstår då hur man skall gå tillväga för att ansluta samtliga dessa datorer till Internet, vilken teknik som krävs, och hur mycket det kommer att kosta?

Större företag har idag möjligheten att investera i fasta anslutningar som är tillgängliga dygnet runt, men de höga månadskostnaderna kan ibland vara svåra att motivera. För små och medelstora företag är situationen än mer problematisk, och det är inte ovanligt att det endast är en anställd på arbetsplatsen som har tillgång till Internet via en dator. Problemet ligger i att dagens Internetabonnemang endast kan nyttjas av en användare i taget.

Detta kapitel kommer först att nämna olika orsaker till varför en Internetanslutning kan vara till nytta för de flesta organisationer oavsett storlek, redovisa tänkbara orsaker till varför dagens abonnemang endast fungerar med ett modem, och kommer sedan slutligen att ta upp olika lösningar på problemet ”en dator, ett Internetabonnemang”.

Mycket forskning bedrivs idag med inriktning på hur Internet kan vara till fördel för organisationer av varierande storlekar, och jag kommer nedan att fokusera på i huvudsak två områden. Det första området är datorn som kommunikationsmedium, och hur detta synsätt på tekniken påverkar våra vardagliga arbetsuppgifter. Den ständiga frågan om huruvida det är tekniken som påverkar människans arbetsuppgifter med sina möjligheter, eller om det är människan som med hjälp av tekniken finner nya möjligheter och arbetsmoment är alltid aktuell (se Daniels, Spiker och Papa (1996) för mer infor-

mation kring detta), och påverkar i högsta grad beslut inför graden av införandet av modern informationsteknik. Då allt fler arbetsuppgifter förläggs till en datorbaserad miljö, kan man idag se hur kompletta administrationsverktyg dyker upp på marknaden som ofta är tillräckligt omfattande för att täcka en medarbetares samtliga arbetsmoment. Eftersom människors sociala behov är lika stora oavsett i vilken miljö de befinner sig i, kommer datorn till slut att även ta på sig rollen som kommunikativ transparent länk mellan olika individer inom organisationen (se t.ex. Nurminens (1988) sammanfattning av det humanistiska perspektivet).

Det andra området som kommer att redovisas är hur olika systemutvecklingsstrategier påverkas av en ökad Internetspridning bland företag. Traditionell systemutveckling av programvara är något som håller på att förändras, just med tanke på att datorn mer och mer tar på sig rollen som kommunikativt medium. Istället för att skapa verktyg som människan använder för vissa arbetsmoment, ställs numera krav på kompletta miljöer för att utföra samtliga arbetsuppgifter. Denna situation skiljer sig radikalt från traditionella utvecklingsmiljöer, och ställer stora krav på väldokumenterade och föränderliga system. En lösning som fler och fler företag tar till hjälp är konstruktionen av lokala Intranät, vilket även leder till att anställda, om de har tillgång till en Internetanslutning, arbetar i en homogen miljö oavsett om de hämtar lokal information från Intranätet eller från ett externt webshotell över Internet.

1.1.1 Datorn som kommunikationsmedium

Att den nya informationstekniken kan påverka både arbetsuppgifter och miljö råder det inga tvivel om. Mycket forskning relaterar dock till frågan *hur* den påverkar oss, och *varför*. Enligt Daniels et al. (1996) så finns det experter inom området som påvisar att tekniken på grund av sin effektivitet kommer att resultera i massiva arbetslöshetsciffror, likväl som övriga experter hävdar att med tanke på att tekniken ej lett till större arbetslöshet idag, så finns det ingen orsak att det skulle inträffa den närmaste tiden heller. Daniels et al. (ibid) fastställer dock att det idag är omöjligt att förutspå effekterna av datorns påverkan på arbetsmiljö och uppgifter, främst med tanke på att pappersbaserad information fortfarande är det dominerande sättet för informationsspridning. Utopin om ett papperslöst kontor fortsätter att hägra, och det är idag tveksamt om vi någonsin kommer att nå ända dit.

Även om målet ej sätts till att helt ersätta papper som distributionsmedium, så finns det vinster att göra genom att nyttja datorn till grupparbete för att öka effektiviteten. Enligt Warner (1996) så söker sig individer till grupparbete främst på grund av fyra orsaker: möjligheterna att kunna fokusera på arbetsuppgifter som är relevanta för individen, att åstadkomma en social

identitet, att skapa en social stödsmechanism samt att tillfredsställa det inbyggda behovet av tillhörighet. Om arbetsuppgifterna förläggs till en mer datoriserad miljö, är det då inte rimligt att man borde sträva efter att bibehålla gruppens funktion även i denna datorbaserade form? Många anser detta, och det har på sistone dykt upp en särskild term just för programvara inriktad på grupparbete. Den engelska termen är *groupware*, och har som funktion att understödja kommunikationen mellan individer för att utföra gemensamma arbetsmoment. Dessa arbetsmoment behöver ej endast gälla mekaniska arbetsuppgifter, utan enligt Daniels et al. (1996) används även avancerade system för omröstningar, gemensamma gruppbeslut och administrativ övervakning.

Grupprogramvaran idag hade kanske aldrig nått så pass långt i sin utveckling om det inte vore för Internet. Istället för att som tidigare förlita sig på ett flertal verktyg med olika gränssnitt finns det nu möjlighet att använda sig av ett enda gränssnitt för att underhålla samtliga informationsmängder. Denna transparens mellan information och dess fysiska lokalisering gör att definitioner såsom LANs (Local Area Network) och WANs (Wide Area Network) håller på att försvinna (se Ringo (1994)). Tidigare användes dessa beteckningar till att fysiskt beskriva ett nätverks omfattning, då ett företag idag anslutet till Internet kan komma åt hela världen utan begränsning. Nya beteckningar som införts istället är Intranet och Extranet, beroende på vem som skall ha tillgång till informationen. Var informationen lagras, hur den ser ut i rå form samt hur den sammanställs är kunskap som endast är tillgänglig för ett fåtal individer, systemadministratörerna. Detta synsätt på information gäller även över Internet, och en åtkomstmöjlighet till denna enorma kunskapsbank kan leda till ökade konkurrensfördelar i en ständigt föränderlig global affärsmarknad.

1.1.2 Framtidens systemutvecklingsmiljöer

Även om det kan skönjas fördelar i en ökad användning av datorn som kommunikationsmedium, så återstår fortfarande problem i att utveckla programvara som tillåter detta. Sanneblad (1997) påvisade att många av dagens mest använda metoder för systemutveckling endast involverar ett fåtal medarbetare i utvecklingsprocessen. En paradox uppstår då programvaran tar på sig rollen som arbetsmiljö, där en majoritet av medarbetarna ej har någonting att säga till om avseende utseende, utformning eller funktionalitet. Lundeborg, Sundgren (1996) anser att bristande kommunikation mellan systembeställare och systemleverantör kan vara orsaken till varför de implementerade systemen ej lever upp till användarnas förväntningar. Problemet är dock att kommunikation tar tid, och Lundeborg et al. (ibid.) markerar gärna att kraven på verksamheten förändras lika snabbt som de möjliga sätten att uppfylla kraven.

Även om det föreligger problem vid utveckling av programvara, så håller programvaran i sig på att förändras. Brooks (1995) har granskat utvecklingsstrategier de senaste två decennierna, och funnit att vi är en lång väg från den optimala utvecklingsprocessen. Trots det så innebär en allt större utbredning av Internet att fler applikationer placeras i detta medium, framförallt på grund av fördelar som homogena gränssnitt och dataoberoende. Dessa applikationer konstrueras distribuerat, och skiljer sig radikalt från tidigare 4GL-verktyg på grund av att det ej existerar någon större etablerad standard inom området. Nya tekniker skapas för varje vecka som passerar, och krav på ökad interaktivitet orsakar förändring i redan driftsatta miljöer.

Det finns dock fördelar med denna nya variant av utvecklingsmiljöer. Shiller (1990) menar att produktutveckling idag går från att ha varit en fasinriktad process, där underhåll följt som ett sista steg i utvecklingsarbetet, till en situation där underhåll räknas som en vital komponent i allt utvecklingsarbete, redan från start. I underhåll inräknas här även mindre användarstyrda förändringar. Det ställs även högre krav på kommunikation programmerare emellan, då globala företag med distribuerade system spridda via Internet kan använda sig av ett flertal utvecklingsbyråer. Både Brooks (1995) och Shiller (1990) hävdar bestämt att fler programmerare ej innebär en linjär ökning av produktutvecklingshastigheten, just med tanke på den komplexitet som uppstår i arbetsmiljön.

I en situation där samtliga användare, utvecklare och administratörer har tillgång till Internet skulle kommunikationen dem emellan kunna effektiviseras, just med tanke på den ökade tillgängligheten. Användare kan direkt se hur prototypen utvecklas till färdigt system, posta kommentarer i speciella forum och statistik över produktanvändning kan föras parallellt med färdigställandet. Om detta leder till bättre system, snabbare utvecklingstider och mer anpassningsbara miljöer är än så länge bara spekulationer, klart är dock att Internet fortsätter att breda ut sig, och de organisationer som väljer att stå utanför kan riskera att hamna i ett sämre läge ur konkurrenssynpunkt.

1.1.3 Att ansluta ett företag till Internet

Många som har en dator hemma eller i det mindre företaget vet ungefär hur man bär sig åt för att komma åt den enorma informationsbank som finns tillgänglig via Internet. Man införskaffar ett så kallat abonnemang, ansluter ett modem till datorn och ringer upp ett speciellt telefonnummer, varefter man kan komma åt informationen med korrekt klientprogramvara. För att förstå problematiken som föreligger i att ansluta ett flertal datorer till Internet och varför det plötsligt kostar stora summor för fasta förbindelser, räcker det inte att härröra kostnaderna till endast samtalstaxor. Jag kommer i kapitel

2 att diskutera de tekniska aspekterna av problemet i detalj, och kommer nedan att sammanfatta några aspekter relativt kortfattat.

All trafik som sker över Internet använder sig av någonting som kallas för *protokoll*. Dessa styr dataflödet mellan olika datorer, och kapslar in data som skickas i något vi kallar *paket*. Den mest utbredda protokollstandarden som nyttjas över Internet kallas IP, och står för Internet Protocol. Den del av protokollet som leder till problem är den där sändare och mottagare definieras. Då Internet är konstruerat av en oräknelig mängd datorer måste varje klient tilldelas ett unikt nummer för att mottagaren av paketen skall veta vart svaret skall returneras. När denna standard konstruerades 1978 var det endast ett fåtal datorer som var anslutna till det nätverk vilket så småningom skulle bli det globala system idag kallat Internet. Eftersom denna enorma tillväxt var svår att överblicka, tillsammans med en strävan att optimera nätverkstrafiken, begränsades antalet tillgängliga adresser till ungefär 4 miljarder datorer. Denna standard döptes till IP version 4 (IPv4) och används fortfarande. Problemet är att landsindelningar har skett av numren, och bland andra Huitema (1996) förutspår att det inom en snar framtid även kommer att finnas ett behov av adresstilldelning till hushållsmaskiner och övrig teknisk utrustning. Visionen är ett maskinellt samhälle där apparater själva rapporterar fel, programmeras om och får ny information över ett ännu mer utbredd Internet. Hur skall då adresserna räcka till?

Internetleverantörer har idag köpt ett antal av de adresser som tilldelats respektive landskod. Då en användare ringer in via sitt modem blir han tilldelad ett av dessa nummer av en dator hos leverantören. Detta betyder att om han ringer in med två datorer, så behöver han bli tilldelad två nummer, och så vidare. Då ett företag väljer en fast anslutning via permanent kabel mot Internet blir företaget tvunget att prenumerera på så många nummer som det finns datorer. De löpande kostnaderna för att inneha ett nummer ökar i takt med att numren börjar ta slut, och Huitema (1996) är en av de forskare som kommit fram till att vi behöver en ny standard, IPng (IP next generation). Detta protokoll befinner sig fortfarande i testfas och kommer att ta flera år att implementera. Väl driftssatt på en global nivå så löser det dock samtliga adresseringsproblem.

1.1.4 Konsten att dela på en Internetadress

Teorin bakom en lösning på problemet med begränsade Internetadresser är ganska enkel. Man dedikerar en dator inom företaget till att sköta all nätverkstrafik mot Internet, via modem eller ISDN. Denna dator hämtar sedan alla paket i det lokala nätverket ett efter ett och granskar mottagaradressen. Om paketet skall levereras utanför det lokala nätverket ansluter den först automatiskt till Internet, byter ut sändaradressen i paketet till det dynamiskt

tilldelade numret av Internetleverantören, och lagrar samtidigt ett extra portvärde i paketet som gör att datorn vid svar vet vilken dator i det lokala nätverket som skickade det. Vid svar från datorn över Internet byts återigen svarsadressen ut till datorn i det lokala nätverket och paketet returneras. Datorn i det lokala nätverket upplever det som om den hade direkt åtkomst till fjärrdatorn över Internet. Då ingen dator begärt åtkomst till Internet under en begränsad tidsperiod kopplas förbindelsen ner och systemet är vilande.

Det finns redan sådana här system i drift, och beskrivs bland annat av Graham (1997). På sistone har man även kunnat se en ökad försäljning av så kallade "black box", eller slutna system till salu som sköter just ovan nämnda procedur utan att utsätta användaren för onödig teknisk information. Problemet är att de flesta av dessa system endast fungerar med en teknik, antingen modem eller ISDN, vilket gör det svårt att testa systemet i liten skala först för att senare skala upp miljön. Det finns även problem med uppkopplingen, om man till exempel vill att den dedikerade datorn ej skall tillåta anslutningar till Internet under kvällar, helger och semestertider. Alternativet till dessa system är att skapa en egen "crystal box", eller öppet system, där all kontroll är fritt tillgänglig och man kan konfigurera systemet efter individuella önskemål. Övriga fördelar med att välja strategin med öppna system är att samma dator även kan fungera som brandvägg mellan Internet och det lokala nätverket, vilket skyddar mot obehöriga angrepp. Ett exempel på ett öppet system är gratisoperativsystemet Linux, som finns distribuerat av en mängd företag runt om i världen.

Även om företaget vid en sådan här implementation fortfarande måste "ringa upp" Internet, sker detta automatiskt och utan insyn från användarna. Skillnaderna mot en permanent uppkoppling minimeras, och vid användandet av en ISDN-anslutning ligger uppkopplingarna på cirka en sekund, vilket är tillräckligt kort tid för att transparens skall kunna uppnås. Användarna blir ej medvetna om att det är en dator som kontinuerligt ringer upp och kopplar ner anslutningen.

1.2 Problemformulering

Då Internet kan leda till positiva aspekter för företag och dess medarbetare är det säkert många inköpsansvariga som har begrundat möjligheten till en anslutning av företagets datorer, men avskräckts på grund av att kostnaden för att abonnera på IP-adresser och kabeldragningar är för hög. Vi söker därför en kostnadseffektiv lösning som tillåter ett företags samtliga datorer att anslutas till Internet, helst genom ett öppet system tillsammans med en brandväggsimplementation. Programvaran bör vara gratis, så att kostnaden endast förläggs till priset på datorhårdvara, modem och ett vanligt Interneta-

bonnemang. För att fastställa det månatliga priset för telefonförbindelsen bör hänsyn tagas till att datorn kopplar ner förbindelsen då det ej föreligger någon trafik.

För att sammanfatta problematiken som föreligger fås följande punkter:

- Hur väl fungerar ett dedikerat system i syfte att hjälpa en organisations medarbetare att ansluta sig till Internet, med hänsyn till överföringshastighet, transparens och användarvänlighet?
- Leder den eventuella transparens som uppstår mot Internet med automatiska uppkopplingar till ett ökat Internetanvändande hos dem som tidigare var tvungna att ansluta sig manuellt?
- Vad finns det för bakomliggande teknik och program som understödjer denna implementation, och finns det funktioner som förhindrar uppkoppling baserat på tid och datum?
- Tillåter system av den här typen möjligheten att vid behov skala upp anslutningen från modem till ISDN?
- Finns det någon begränsning i vilka program som kan nyttjas hos företagets datorer med hjälp av denna lösning?
- Hur stor kan den månatliga anslutningskostnaden till Internet förväntas bli?

1.3 Problemavgränsning

En avgränsning kommer att göras i det att olika system ej kommer att sättas i förhållande mot varandra. Så fort ett system har hittats till minimal kostnad och uppfyller de krav vilka definierats i problemformuleringen kommer det att implementeras och driftsättas omgående för att utvärdera dess funktionalitet. Färdigkonfigurerade slutna system kommer att utelämnas helt, dels eftersom de innebär en hög anskaffningskostnad, dels på grund av att de generellt sett erbjuder begränsade möjligheter för anpassning och underhåll.

1.4 Syfte och målgrupp

Studien kommer att ha två huvudsakliga syften. För det första att finna ett kostnadseffektivt tekniskt system som alla mindre och medelstora företag kan nyttja för att komma ut på Internet. Implementationen skall vara säker och förhindra intrång, samtidigt som den skall möjliggöra Internetåtkomst utåt för företagets samtliga program. För det andra så skall detta system praktiskt testas och utvärderas hos olika företag med varierande behov, produkter och antal anställda. Utvärdering kommer att ske genom granskning av de eventuella problem som uppstår under evalueringstiden, tillsammans med

användarnas upplevelser av hur väl systemet motsvarade deras förväntningar.

Den tilltänkta målgruppen är inköpsansvarig, teknisk och övrig personal i små och medelstora företag som vill vidga sina möjligheter till kostnadseffektiv och skalbar Internetåtkomst.

1.5 Förväntat resultat

Det förväntade resultatet är ett tekniskt system som löser ovan nämnda problem. Detta system skall ha utvärderats i skarp miljö ett antal veckor före resultatsammanställningen, och bör ha minimala krav på underhållsarbete för att väl konfigurerat även kunna brukas som ett slutet system. Baserat på antalet samtalstimmar och uppkopplingskostnader kommer även en modell för kostnads kalkyler att redovisas, som visar maximal månadskostnad för ett iordningsställt system. Utöver detta så kommer även användares erfarenheter och upplevelser kring det implementerade systemet att redovisas.

1.6 Egna relationer och förutsättningar

När forskare i slutet av 1960-talet använde Multics-apparater (Multics stod för Multiplexed Information and Computing Service) för att på fritiden engagera sig i spelet Space travel fanns det hela tiden en strävan att möjliggöra för flera personer att nyttja en gemensam nätverksanslutning. Det största problemet med dåtidens datormiljöer var att det räckte med ett fåtal personer anslutna till systemet (gränsen 1969 gick vid tre personer) för att det skulle överbelastas helt. Enligt Salus (1994) ledde detta till att Multicsprojektet lades ner, och forskarna Ken Thompson och Dennis Ritchie bestämde sig då för att utveckla det som så småningom skulle bli ett nytt operativsystem, UNIX (Uniplexed Information and Computing Service).

Denna strävan efter att kunna arbeta flera personer över en och samma nätverksanslutning finns fortfarande, och jag stöter dagligen på folk som hunnit skaffa sig minst två datorer till antingen hemmet eller företaget, men ej vet hur de skall bära sig åt för att ansluta dem till Internet. Som tur är så finns det fortfarande människor i den här världen som liksom Ken och Dennis bedriver omfattande arbetsprojekt på sin fritid, för att komma ett större antal människor till nytta. Ett av dessa projekt är operativsystemet Linux, som är en variant av operativsystemet UNIX. Linux utvecklas av ett hundratal programmerare över hela världen, och programvaran släpps sedan fritt för folk att nyttja den efter egna intressen. Då det ej ligger affärsmässiga intressen bakom programvaran så var det först ganska nyligen det började distribueras

versioner av Linux som faktiskt riktade sig till den ovana UNIX-användaren. Detta, tillsammans med det faktum att det började formas företag som tar betalt för att hjälpa folk installera denna fria programvara, ledde till mitt ökande intresse för Linux som en lösning till problemet med att ansluta företag till Internet.

Parallellt med mina studier på Högskolan i Borås har jag varit verksam i forskningscentret ITCentrum, vid Institutionen för Data- och Affärsvetenskap. Jag har här fått möjligheten att administrera och underhålla både UNIX- och Windowsmiljöer vilket fått mig att inse vilken betydelse ett fritt tillgängligt operativsystem kan ha för mindre företag. Det är också viktigt att här markera att jag ej själv ämnar utföra någon form av produktutvecklingsarbete i studien, utan strävar efter att använda färdiga programvaror utvecklade av denna unika skara människor som hela tiden verkar växa i antal. Studien hade varit omöjlig att genomföra utan deras tillskott till denna fria programvaruflorea.

1.7 Definitioner

Black box. Ett system vars inre funktion ej är synligt för användaren. Även om det är möjligt att via ett gränssnitt administrera och konfigurera systemet så är det omöjligt att få en inblick i bakomliggande teorier och strukturer. För att undvika den engelska beteckningen kommer jag i texten att referera till denna typ av system som *slutna system*.

Brandvägg. Den engelska titeln på denna term är *firewall*, och används vanligtvis på föremål som hindrar eld från att sprida sig från en position till en annan. En liknelse som Chapman (1995) använder sig av istället är dock en vindbrygga på ett medeltida slott. Denna vindbrygga har följande funktionalitet:

1. Den begränsar ingående människor till en enda noggrant kontrollerad punkt
2. Den förhindrar angripare från att komma nära övriga försvarsområden
3. Den begränsar utgående människor till en enda noggrant kontrollerad punkt

Enligt Chapman (ibid.) är ovanstående kriterier även direkt anpassningsbara på brandväggar i datorsammanhang, där en Internetbrandvägg oftast installeras vid den punkt där det skyddade lokala nätverket skall anslutas till Internet.

Crystal box. Denna term används på system som är motsatsen till blackbox-varianten som illustreras ovan. Användaren har full översikt över samtliga interna strukturer, och dessa system brukar på engelska även benämnas *white box*, just för att extra tydligt illustrera skillnaden. I rapporten kommer jag i fortsättningen att använda mig av benämningen *öppet system*.

Gateway. Traditionellt sett kallas ofta routers för gateways, då de fungerar som en port ut mot omvärlden. Enligt Ringo (1994) är dock denna beteckning på väg bort på grund av främst OSI-modellens ökade inflytande, tillsammans med ett pågående arbete för att standardisera nätverksbegreppen inom industrin. Just detta standardiseringsarbete leder enligt Graham (1997) till att en gateway idag beskrivs som en router vilken är verksam i OSI-modellens lager 4 till 7 (ovanför nätverkslagret). En gateways uppgift blir då som protokollöversättare, exempelvis från TCP/IP till IBM SNA. Då detta förslag ej ännu är fastslaget används beteckningen gateway i texten som identisk med router, men bara då en markering vill göras för att stärka bilden som port mot Internet.

GNU. Den fullständiga engelska titeln på GNU är Gnu's Not Unix, och kännetecknar ett licensavtal skapat för att fritt kunna distribuera programvara internationellt där upphovsrättigheterna kvarhålls hos utvecklaren. Ordet fritt står här för programvarans frihet, ej dess pris. Programvara som levereras under GNU's avtal GNU Public License behöver ej vara gratis, även om det förespråkas. Avtalet är från början skapat av en forskare på MIT, Richard Stallman.

ISDN. ISDN står för Integrated Services Digital Network, och är en internationell standard för att kommunicera digitalt över ett publikt telefonnät. Då standarden är helt digital innebär det att uppkopplingen mellan två adaptrar sker på någon sekund, till exempel genom anslutning mot Internet. Till skillnad från modem som används över analoga telefonförbindelser är ISDN en synkron standard som har möjlighet att skicka och ta emot en kontinuerlig ström av data. De flesta externa adaptrar har också möjligheten att ansluta sig till en asynkron seriell port som finns på de flesta personatorer, vilket då gör dem helt kompatibla med övriga modem förutsatt att korrekta inställningar görs i programvaran. Överföringshastigheten via en så kallad BRI-kanal (Basic Rate Interface) är 64 kbit/sekund, och används för all kommunikation. Det finns på nya adaptrar möjlighet att med hjälp av särskild programvara sammankoppla två stycken BRI-kanaler för att totalt komma upp i en hastighet av 128kbit/sekund.

Modem. Modem är en förkortning på termen Modulator Demodulator, vilket är en beteckning på en särskild form av adaptrar med två funktioner. Dels konverteras en digital asynkron signal till en analog variant som skickas via bärvåg över telefonnätet, dels konverteras sedan denna signal tillbaka till en digital variant. Denna metod är asynkron vilket innebär att endast ett tecken i taget skickas, och på grund av begränsningar i telefonnätet kan endast hastigheter upp till 56kbit användas. Då det finns en stor flora av adaptrar med olika hastigheter på marknaden måste modemen vid en anslutning med varandra först bestämma vilka protokoll samt vilken hastighet som skall användas genom en procedur som på engelska kallas för *handshaking*, vilket tar ungefär 30 sekunder.

Paket. För att utbyta information mellan olika datorer i ett nätverk delas informationsflödet upp i någonting som kallas för paket (termen *datagram* används också i vissa sammanhang). Orsakerna till att informationen delas upp i olika paket är många, där den främsta är att flera datorer tillåts kommunicera över en gemensam kopplingspunkt. Då de noder som bygger upp Internet vidarebefordrar informationspaket från en stor mängd datorer, innebär det att ju mindre paketen är desto bättre kan noderna, eller routrarna, fördela belastningen. Storleken på paketen brukar ofta vara ganska små, under 1000 tecken per styck, vilket ger möjligheten att införa felkontroll vid nyttjandet av protokoll som inkapslar informationen. Enligt Ringo (1994) så kan det uppstå ett fel per en miljon skickade bitar information. Det innebär ungefär 10 fel vid överföring av en megabyte data. Ju fler paket som används, desto mindre paket behöver skickas om vid eventuellt fel vid överföringen.

Protokoll. Protokoll används för att koordinera informationsutbytet mellan olika nätverksenheter. Om data skulle sändas i sin rena form mellan olika datorer så skulle den vara utan mening, och protokollen verkar för att etablera en mekanism som registrerar och separerar relevant information från övriga data. Detta sker genom att kapsla in datan med ett informationshuvud, så att samma protokoll hos mottagaren förstår och kan tyda innehållet. Då det ej är garanterat att paketen anländer i korrekt kronologisk ordning, vilket kan inträffa vid överföring över långa distanser, hjälper även protokollen till att sammanställa och felkontrollera paketflödet så att korrekt information fås hos mottagaren.

Router. Enligt Ringo (1994) används en router till att hitta den bästa ruten mellan två eller flera nätverk. För att göra detta lagras samtliga kringliggande datorers adresser i någonting som kallas *routingtabell*, som används för att vidarebefordra ankomna paket till en korrekt destination. Då en router behöver tillgång till aktuella nätverksadresser som

lagras i paketen eller datagrammen gör det den mycket protokollspecifik. Skulle en router påträffa ett paket med ett protokoll den ej stödjer, slängs paketet direkt, vilket innebär att införandet av nya protokoll över Internet kommer att kräva förändring i de flesta system. Den process där nätverkspaket styrs mot sin destination med hjälp av en router kallas för *routing*, eller vidarebefordring som jag även nämner på en del ställen i texten.

UNIX. För att förstå och kunna beskriva vad UNIX står för idag måste man känna till historiken. Projektet UNIX påbörjades i slutet av 1960-talet, som en revolt mot det då nedlagda projektet Multics. Multics var från början konstruerat som ett system vilket skulle möjliggöra för ett flertal användare att nyttja resurser från en gemensam server, men lades ner då förväntningarna ej kunde uppnås. Namnet på projektet var från början Unics, just för att markera skillnaden mot Multicssystemet.

Från början byggdes UNIX enligt Andréasson, Skansholm (1993) som ett operativsystem i språket PDP-7, men skrevs om fullständigt 1973 i programspråket C. Denna standard innebar att operativsystemet blev portabelt och enkelt kunde flyttas till vilken dator som helst, förutsatt att denna kunde kompilera C-källkod. Då källkoden publicerades fritt byggde olika forskningscentrum sina egna versioner, och några av de varianter som utvecklats med tiden är System V, Berkeley, Xenix, Ultrix, SunOS, AIX m. fl. Skillnaderna mellan operativsystemen är idag relativt stora, och de är ej längre fullt kompatibla med varandra som det var tänkt från början.

Några distributioner som används idag och bygger på ovan nämnda varianter är operativsystemen Solaris (SunOS), Linux (System V) och FreeBSD (Berkeley). Det finns enligt Andréasson, Skansholm (1993) idag en strävan att sammanföra de olika varianterna till en gemensam standard för att återupprätta portabiliteten av programvara, vilket begränsas av att det bildats två oberoende, konkurrerande leverantörskonsortier som förhindrar arbetet (Open Software Foundation och Unix International).

2 Teoretisk bakgrund

2.1 Relaterat arbete

Datorprogram skapade av utvecklare som står utanför forskningsvärlden kan vara svåra att få gehör för inom akademiska kretsar. Då ett flertal av dessa datorprogram och miljöer är helt behovsstyrda, kan det vara mycket svårt att se en vetenskaplig koppling till existerande system. Trots att många utvecklare inom denna genre har en vetenskaplig anknytning har de själva insett problematiken med att få sitt fritidsintresse godkänt som vetenskapligt arbetsmaterial och har således blivit tvungna att utveckla intresset som en ren hobby.

Ett system som baserar sig på programvara av den här typen riskerar att befinna sig långt ifrån internt utvecklade akademiska miljöer, främst avseende referenser till tidigare utfört arbete, metodval och perspektiv vid utveckling av systemet samt möjligheter till validering av empiriska data. För att höra en utvecklares åsikter kontaktades Fil. Dr. Eric Schenk, som har skapat ett flertal program för operativsystemet Linux. Ett av Schenks mer kända program är DialD, vilket används för att låta routers behovsprövat ansluta sig till Internet. Vid frågan om hur han anser att specifika tekniker vuxit fram i denna utvecklingsmiljö var svaret: "My impression is that it just kind of evolved over time in discussion with various contributors to the networking core of the kernel." Att spåra eventuella vetenskapliga tillskott och tester av programvaran kan således anses vara mycket svårt.

Det finns ett flertal forskningsgrupper som bidrar till att sätta standards inom Internetsamhället, så kallade RFC's. Detta avsnitt kommer att behandla dessa standards och hur idéer växer fram etappvis över Internet och kommer sedan att redovisa en datormiljö som kan användas för att realisera möjligheten att ansluta ett flertal datorer via en Internetanslutning, operativsystemet Linux. Orsaken till att fokusering sker på just Linux är att det finns företag som specialiserat sig på att förenkla installation och underhåll av programva-

ran genom specialskrivna verktyg. Det finns säkerligen ett antal andra operativsystem som skulle klara uppgiften minst lika bra, och jag vill här återigen understryka att fokus för rapporten är att hitta en lösning som kan användas av de flesta företag, inte att finna alla tänkbara varianter som kan tänkas utföra uppgiften på ett acceptabelt sätt.

2.1.1 Request for Comments (RFC)

Internet är en global företeelse, utan vare sig styrning eller maktcentralisering. Det finns inga myndigheter som fattar gemensamma lagar, och standards växer fram behovsprövat. För att få ordning i kaoset formades enligt Stevens (1994) fyra större grupper, samtliga med uppgiften att godkänna och granska nya standards. De olika grupperna är Internet Society (ISOC) som stödjer och förespråkar Internet som en global infrastruktur för att understödja forskning, Internet Architecture Board (IAB) som koordinerar och ser över tekniska aspekter, Internet Engineering Task Force (IETF) vilka är en grupp som särskilt fokuserar på att fastslå kortsiktiga standards samt Internet Research Task Force (IRTF) som genomför långtgående projekt. Det finns idag även en mängd mindre grupper som organiserar specialiserade projekt, till exempel ROAD gruppen som forskar i problem kopplade till begränsningar i dagens IP protokoll (se Dixon (1993)).

Samtliga förslag till standards publiceras via en anslagstavla som kallas för Request for Comments (RFC). Dessa RFC's finns självklart tillgängliga via Internet, och det är här förslag till nya standards postas. Posterna granskas av ovan nämnda grupper och övriga användare, vilket leder till diskussion och synpunkter. Eftersom Internet i sig är så pass föränderligt flyttas aldrig dessa förslag från listan, utan varje standard är ständigt utsatt för både kritik och förslag om förbättringar. Då förändringar sparas som revideringar till äldre RFC's leder detta till att det idag finns en stor kunskapsbank som innehåller förklaringar till samtliga begrepp och tekniker som används eller har använts över Internet.

2.1.2 IPng

Ett flertal RFC's kretsar idag kring utvecklingen av nya Internetprotokoll, främst på grund av de problem som idag föreligger med den etablerade standarden IP version 4. Ett flertal varianter har presenterats och versioner upp till IPv9 finns dokumenterade. Den standard som vunnit flest sympatier är version 6, som i dagligt tal kallas för IPng (IP next generation). Enligt Dixon (1993) så är de största problemen relaterade till sättet nätverksadresser hanteras. Dels så finns det för få adresser tillgängliga, dels så är strukturen av

adresserna icke-hierarkisk vilket leder till en platt fördelning som försvårar vidarebefordring av nätverkspaketen. Även om det inkommit flera förslag på temporära lösningar genom att förlänga paketstorlekarna med extra information, så är de flesta överens om att det förr eller senare kommer att krävas en global implementation av denna nya standard IPng.

Den person som arbetat mest för att realisera IPng är Christian Huitema, som skrev det första utkastet inför Internet Architecture Board (IAB) 1992, vilket strax därefter presenterades inför Internet Engineering Task Force (IETF). Parallellt postades enligt Huitema (1996) ett antal RFC's över Internet som reaktion på det faktum att världen inom mindre än tjugo år skulle få slut på nätverksadresser, vilket framkom efter en studie som startades på initiativ av Internet Architecture Board (IAB) 1991. En orsak till detta är spekulationerna om att varje individ kommer att ha tillgång till en mängd datorer i form av hushållsmaskiner och övrig elektronik som var och en kommer att kunna kommunicera med varandra över Internet. En annan orsak är den platta strukturer som idag råder över adressfördelningen. Om man räknar med att Internet fortsätter att växa i samma hastighet som idag, och ritar upp denna kurva på ett logaritmiskt ark, så finner man enligt Huitema (ibid.) att antalet adresser tar slut helt mellan år 2005 och 2015. Om hushållsmaskiner och övrig teknisk apparatur får Internetadresser kommer detta stopp att inträffa mycket tidigare.

Året efter det att Huitema presenterade sitt första utkast sammanställde IETF-gruppen på Harvard University (1993) en begäran om viktiga kriterier internetanvändare ansåg att IPng borde uppfylla. I och med detta kunde vanliga användare hjälpa till att forma strukturen och framväxten på den standard som idag håller på att realiseras i allt större testsystem. Från att ha varit en anarki utan styrning formas Internet idag av dess användare, i vad som endast kan kallas för den idealiska demokratin.

2.1.3 Linux

Våren 1991 arbetade en 22-årig forskarstudent vid Helsingfors Universitet med att utveckla och förbättra kontrollen över sin dator. Studenten hette Linus Torvalds och datorn var en då modern Intel 386-baserad klon. Linus ville se hur mycket kontroll man kunde ta över datorsystemet och skrev till en början drivrutiner för att kontrollera bland annat hårddisk och grafikkort. Det hela började så småningom att likna ett komplett operativsystem baserat på UNIX-varianten SystemV, och redan i oktober samma år hade den första versionen av operativsystemet Linux v0.02 demonstrerats inför allmänheten. Linux levererades vid det här laget med färdiga program som kommandotolk, programkompilatorer och verktyg för att komprimera data. Om man sedan följer utvecklingen så gick den i rasande fart. Våren 1992 klarade Li-

nux av att exekvera grafiska applikationer, varefter så många personer kom att bli involverade i utvecklingen att den första stabila versionen 1.0 följde endast tre år efter det att den ursprungliga idén hade formats, det vill säga 1994.

För att få en komplett kronologisk översikt av Linuxutvecklingen så har Aaron Thies (1998) sammanställt en tidslinje som visar samtliga händelser i detalj, varifrån mycket av informationen i denna sektion är hämtad. I övrigt så finns det mycket lite information sammanställd om just utvecklingen av detta operativsystem, vilket även återspeglas i den problematik Salus (1994) upplevde då han begav sig att dokumentera framväxten av UNIX som operativsystem de senaste 25 åren. Salus (ibid.) var tvungen att personligen intervjua nyckelmännen bakom programmen då antalet sammanställda dokument var så få att det ej gick att framställa en övergripande struktur.

Linux har från det att den första versionen producerades 1991 distribuerats under ett avtal som innebär att vem som helst får modifiera programvaran efter egna behov. I januari 1992 antog Linus det generella GNU public license-avtalet för distributionen, vilket innebär att företag kunde ta betalt för att sprida programvaran vidare. Detta innebär i sin tur att företaget Redhat Software redan ett halvår efter det att Linux v1.0 släpptes 1994, marknadsförde sin distribution av operativsystemet vid namnet Redhat Linux. Distributionen innehöll programvara för att installera Linux, färdiga program för att skapa dokument och bilder tillsammans med grafiska konfigurationsverktyg. Hela paketet var byggt kring den stabila kärnan i Linux och försäljningssuccen var ett faktum. Då RedHat Software släppte sin distribution enligt GNU public license innebär det att den fritt gick att ta hem över Internet. Det enda företaget tog betalt för var tryckning av användardokumentation och CD-Skiva. Redhat Software säljer fortfarande sin distribution, och den används bland andra av Linus själv.

Då Linux bygger på en UNIX-arkitektur har målet med portabilitet satts högt. Linux finns idag tillgängligt för en bred flora av datorarkitekturer, allt ifrån vanliga PC-datorer till större Sun Sparc-system. Just det faktum att systemen är så pass anpassningsbara är enligt Salus (1994) den största skillnaden mellan UNIX-baserade operativsystem och de system som tillverkas endast för en datorarkitektur (t. ex. Microsoft Windows). Nackdelarna med denna portabilitet är att det kan vara problematiskt att utveckla kommersiell programvara då det finns så många hårdvaruplattformar att stödja. Att utveckla ett program i exempelvis Microsoft Windows-miljö för endast en datortyp innebär mindre arbete och en långt större marknad. Den senaste tidens debatt kring programspråket Java är någonting som skulle kunna förändra denna situation. Java är som bekant en utvecklingsmiljö för att skapa datorprogram som går att starta under vilket operativsystem som helst, på vilken datorarkitektur som helst (med vissa restriktioner).

2.1.4 Dial on Demand

Linux är uppbyggt kring en så pass öppen standard att vem som helst kan utföra vilka förändringar i systemet som helst. Hela källkoden till operativsystemet finns fritt tillgängligt via Internet, vilket innebär att användare kan få full kontroll över sin dator. Då själva kärnan i Linux är relativt liten, krävs det program för samtliga operationer som en användare kan tänkas utföras vid datorn. Som exempel på detta är kommandotolken för att starta program en applikation i sig, vilket leder till att när man diskuterar Linux så är det egentligen styrsystemet (engelska *kernel*) som diskuteras.

Även om de olika distributionerna av Linux som nämnts ovan innehåller en mängd färdiga applikationer för att arbeta med en dator i nätverksmiljö, så finns det ett flertal program för speciella situationer som ej levereras i pake-ten. Ett exempel på en sådan applikation är programmet DialD (Dial on Demand) som automatiskt ansluter datorn till Internet då användaren behöver det. Programmet är skrivet av Fil. Dr. Erik Schenk (1998) och fungerar även då datorn står fristående i ett nätverk. Detta skulle kunna innebära att programmet DialD tillsammans med inbyggda funktioner för översättning av nätverksadresser i Linux som en helhet kan utgöra det system vi avser att implementera. I likhet med övriga program för Linux så är även DialD distribuerat enligt avtalet GNU public license, vilket leder till att det både är gratis och fritt går att modifiera.

Enligt Schenk (ibid.) fungerar DialD enligt följande: DialD startas på den dator i nätverket som har tillgång till Internet. Så fort ett nätverkspaket anländer till datorn granskar DialD vem som skickat paketet, vem mottagaren är samt aktuellt klockslag. På detta sätt är det möjligt att bygga regeltabeller som förhindrar datorn att ansluta sig till Internet vid speciella klockslag eller datum. Paketet skickas sedan vidare till Linux inbyggda så kallade *routing-tabell*, som ser till att distribuera samtliga nätverkspaket till korrekt mottagare, varefter DialD ansluter datorn till Internet om paketet ej skulle till en mottagare i det lokala nätverket. Datorn ansluts ej till Internet om regeltabeller är definierade som förhindrar trafik att nå dit vid aktuellt klockslag eller datum. Om DialD ej uppmätt någon trafik mot Internet under ett specificerat antal minuter kopplas förbindelsen ner automatiskt.

Det går också att begränsa rättigheterna i DialD så att endast ett fåtal datorer har möjlighet att komma åt Internet, till ett begränsat antal webhotell. DialD är skalbart och lagrar konfigurationsfiler även för hur de olika paketen är strukturerade, vilket innebär att om en ny standard på nätverkspaket införs (exempelvis IPng) är det mycket enkelt att lägga till en konfigurationsfil som beskriver hur denna standard ser ut. Systemet övergår då omedelbart till att klara av även dessa nya paket.

All denna kontroll leder snabbt till att det blir en stor mängd konfigurationsfiler som måste skapas för att få systemet att fungera, vilket kan avskräcka den ovane användaren. Det har då vuxit fram ett program för att skapa just dessa filer kallat Diald-config vilket lägger ett abstraktionslager över informationen. Detta verktyg är framställt av Karl Pinc (1998) som är anställd på företaget The Meme factory, vars verksamhetsområde bland annat är att informera företag om hur de kan kunna nyttja Linux, DialD och DialD-config för att ansluta sin datorpark till Internet.

2.2 Teorier av betydelse

Som nämnts innan så finns det standards även i Internetsamhället, och en del av dem kommer att redovisas nedan. De tekniker som nedan kommer att redovisas motsvarar den minimala mängd teoretisk kunskap som krävs för att kunna förstå sig på hur det implementerade systemet kommer att fungera.

Det som kommer att redovisas i detta stycke är först och främst hur nätverk är strukturerade, hur olika datorer hittar varandra samt vad det innebär att översätta nätverksadresser. Efter det kommer den berömda OSI-modellen (Open System Interconnection) att visas. Denna modell visar kopplingen mellan en dator, dess program och programmens kommunikation med varandra över nätverksförbindelser och ligger till grund för många av dagens nätverksprotokoll (som ibland även kallas för OSI-protokoll enligt Graham (1997)). Dessa protokoll, som bestämmer hur information skall skickas mellan olika datorer, kommer sedan att granskas ingående för att ge en inblick i hur kommunikationen datorer emellan struktureras. Hela kapitlet avslutas med ett stycke som sammanfattar några för rapporten väsentliga säkerhetsaspekter.

2.2.1 Nätverksadressering

Datorer som kommunicerar mellan varandra är organiserade i olika nätverk. Termen nätverk i sig har egentligen ingenting med datorer att göra utan används mest för att illustrera den komplexitet som ett nät innebär. Varje dator ansluten till Internet måste ha en så kallad IP-adress, vilket är den adress protokollet IP (som förklaras senare) använder för att leverera information till en mottagare. Adressen består av ett 32 bitar långt nummer, vilket möjliggör drygt fyra miljarder kombinationer (2^{32}). Då nätverksadressen som används består av fyra bytes (32 bitar), brukar den ofta skrivas som fyra decimalnummer med en punkt som separator, vilket benämns decimalpunkts-notation. Då varje byte har 255 olika kombinationer (2^8), kan antalet

möjliga nätverksadresser även beräknas som 255^4 . Ett exempel på en sådan adress är numret till ITCentrums webserver, som idag är 193.10.174.6.

De teorier som redovisas i detta stycke är specifika för standarden IPv4, som är begränsad till 32-bitars adresser. De problem som existerar idag med att dessa adresser håller på att ta slut kommer dock att upphöra så snart IPng tas i drift, eftersom detta protokoll kommer att möjliggöra 128-bitars adressering. För att få en uppfattning av hur många datorer detta rör sig om beskriver Huitema (1996) det som möjligheten att ansluta en kvadriljon datorer (10^{15}) till en triljon (10^{12}) olika nätverk.

Nätverksklassificering

Utan en organisering av alla nummer skulle i värsta fall ett paket behöva söka igenom samtliga fyra miljarder adresser för att till slut hitta sin mottagare, vilket har lett till att en standard för indelning av numren i olika nätverksklasser har skett. Det finns idag fem olika nätverksklasser som används, klass A, B, C, D och E. Det enklaste sättet att se vilken nätverksklass en dator tillhör är att titta på den första siffran i decimalpunkts-notationen och sedan jämföra den med de intervall som är redovisade i figur 2.1.

Klass	Omfång	
A	0.0.0.0 till	127.255.255.255
B	128.0.0.0 till	191.255.255.255
C	192.0.0.0 till	223.255.255.255
D	224.0.0.0 till	239.255.255.255
E	240.0.0.0 till	247.255.255.255

Fig 2.1, Adressintervaller för IP-adresser, fritt översatt till svenska efter Stevens (1994)

Då varje dator ansluten till Internet måste ha en unik adress har det bildats en central myndighet för tilldelning och organisation av dessa klasser. Myndigheten kallas för på engelska *Internet Network Information Center*, eller *InterNIC*. Den ser till att jämnt fördela de olika nätverksadresser som finns tillgängliga mellan större myndigheter inom respektive land, vilka i sin tur ansvarar för att distribuera adresser till företag och Internetleverantörer. Nätverksadresserna som InterNIC bestämmer över är de första två siffrorna i decimalpunkts-notationen. När man ringer upp sin Internetleverantör via modem för att ansluta sig till Internet, blir man automatiskt tilldelad ett klientnummer från leverantörens hyrda lista av klientadresser.

Subnät

Om man antar att man skulle ansluta ett maximalt antal datorer till nätverksklass A skulle det innebära totalt 2^{24} stycken. Detta i sig är bättre än 2^{32} datorer, men det är fortfarande alldeles för många för att kunna administreras centralt. Det har då utformats en lösning där samtliga nätverksklasser i sig skall kunna delas upp i olika så kallade subnät för att ytterligare dela in datorerna. Bruket av decimalpunkts-notation blir nu än mer användbar, där de två första siffrorna bestämmer nätverksidentifikation, den tredje siffran subnät och den sista siffran klientadress, se figur 2.2.

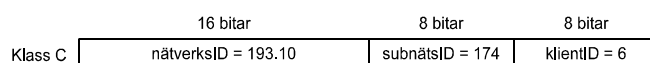


Fig 2.2, Subnätsindelning av en klassC-adress

Subnätmask

För att systemet skall veta hur många bitar av nätverksadressen som används som definition av subnät och vilka som används som klientadress, nyttjas en så kallad subnätmask. Ett system känner till sin egen adress tillsammans med subnätmasken och kan direkt avgöra om ett IP datagram (se förklaring till datagram under beskrivningen av protokollet IP) skall levereras till antingen (1) en dator på det egna subnätet, (2) en dator på ett annat subnät men på samma nätverk eller (3) en dator på ett annat nätverk. Subnätmasken består liksom övriga adresser av 32 bitar, innehållandes värdet 1 för nätverksid och subnätid, och 0 för klientid. För datorn i figur 2.2 skulle subnätet bli 255.255.255.0, och sättet detta räknas ut är redovisat i figur 2.3.

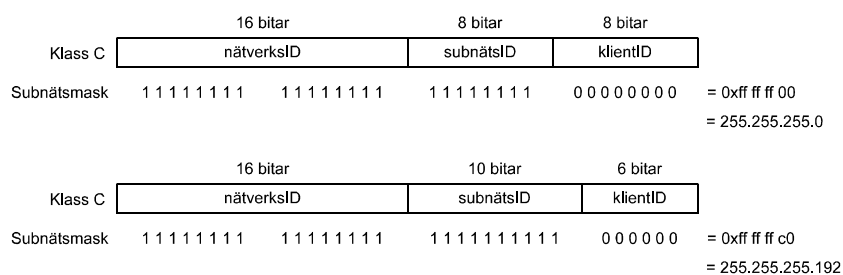


Fig 2.3, Två exempel på subnätmask i olika klassC-nät

Adresstilldelning i lokala nätverk

Då TCP/IP på sistone blivit populärt även i lokala nätverk har Rekhter, Moskowitz, Karrenberg och de Groot (1994) presenterat ett förslag som innebär att tre globala nätverksadresser (en klass A, en klass B och en klass C) reserveras endast för detta ändamål. Intresset för denna reservation är enkel – används en nätverksadress i det lokala nätverket som existerar någon annanstans över Internet kan datorerna i det lokala nätverket aldrig nå ut till det främmande nätverket. Datorn (som kontrollerar sin adress och subnätmask) tror då att destinationen befinner sig på det egna nätverket. Detta gäller även vid fristående arbetsstationer som har tillgång till Internet. Väljs ett felaktigt nätverksnummer finns det risk att man ej kommer åt vissa nätverk. De rekommenderade adresserna redovisas i figur 2.4.

Klass	Omfång	
A	10.0.0.0 till	10.255.255.255
B	172.16.0.0 till	172.31.255.255
C	192.168.0.0 till	192.168.255.255

Fig 2.4, Rekommenderade nätverksadresser för lokala nätverk

Allokering av nätverksportar

Vid det här laget bör strukturen över hur datorer finner varandra vara ganska tydlig. Frågan kvarstår dock hur datorn vet att ta hand om den mängd paket som ankommer till nätverkshårdvaran och hur varje applikation får rätt data. Jag ger här ett praktiskt exempel: En klientdator i det lokala klass C-nätverket med adress 192.168.1.7 skall anslutas till en den lokala Intranätservern på adress 192.168.1.50. För båda datorerna gäller att subnätmasken är satt till 255.255.255.0, vilket visar på att de befinner sig på samma subnät. Klientdatorn startar tre webläsare parallellt vilka i sin tur begär information från tre olika websidor hos servern. Dessa sidor skickas sedan som inkapslade TCP paket från klienten till servern. Servern svarar då genom skicka tillbaka informationen i sidorna till klienten, även här genom inkapslade TCP-paket, men hur vet klientdatorn vilken applikation som skulle ha respektive information?

Svaret på frågan är att varje klient allokerar en nätverksport på datorn som är unik för applikationen. Varje webläsare hos klienten har då skapat tre stycken tillfälliga portar, som är aktiva så länge strömmen av TCP-paket är aktiv. För att klienten skall veta till vilken port på servern begäran om att hämta information skall skickas, finns det ett antal fast reserverade portar just för detta, där exempelvis ftp-servers använder port 21, och webbservers använder port 80. Reservation av dessa portar sker av *Internet Assigned Numbers Aut-*

hority (IANA) och inbegriper intervallet mellan 1 och 1023. De portar som skapas på klienten kallas för temporära portar (eng. *ephemeral ports*) och placerar sig enligt Stevens (1994) vanligtvis mellan 1024 och 5000. Det finns dock en typ av system som använder portnummer över 32768, vilket kommer att redovisas nedan.

Översättning av nätverksadresser

Översättning av nätverksadresser är en teknik som kan användas om man ej vill att omgivningen skall få information om vilka eller hur många datorer som existerar i det lokala nätverket. Tekniken kan även användas då det lokala nätverket endast har en dator som är ansluten till Internet, då man låter den sköta samtliga datorers Internetkommunikation över en förbindelse. Några av fördelarna med denna teknik är enligt Egevang, Francis (1994) dels att den kräver få förändringar till den nuvarande datorparken, dels att den kan installeras inkrementellt med ett fåtal anslutna datorer som sedan skalas upp i antal efter behov. För att slippa den långa beteckningen "Översättning av nätverksadresser" existerar det idag en mängd olika namnvarianter, där den mest originella är den som ofta brukas i Linuxsamband, "IP masquerading".

I korthet fungerar tekniken så att en dator dedikeras till att sköta vidarebefordran av samtliga nätverksdatagram som skickas över nätverket. Datorn betecknas *gateway* eller, beteckningen som jag i fortsättningen kommer att bruka, *router*. Router granskar sedan samtliga IP-datagram som anländer till nätverkshårdvaran. De datagram som är adresserade till det egna subnätverket skickas omgående vidare, medan övriga placeras i en särskild kö. Det som sedan händer är gemensamt för alla varianter av nätverksadressöversättare, och jag kommer här att redogöra för hur det fungerar i Linux enligt Vos, Konijnenberg (1996) som medverkat till utvecklingen av masqueradefunktionerna.

Enligt Vos, Konijnenberg (ibid.) nyttjas de lokala nätverksprotokollen på routern till att analysera och förändra innehållet i respektive datagram. Först hämtar protokollet IP paketets sändare och mottagare, varefter dessa adresser registreras beroende på vilken typ av transportprotokoll som använts (TCP eller UDP). Routern allokerar då en ny port hos sig själv och ersätter sedan sändarens IP-adress med sin egen adress, varefter den byter ut sändarens portnummer mot det nya, allokerade portnumret. Dessa portnummer allokeras i intervallet 32768-65535, för att separera portarna från routerns egen trafik. Detta nya portnummer lagras tillsammans med sändarens adress och portnummer i ett register hos routern, vilket den sedan använder då den får svar från mottagaren till att återigen ersätta i det här fallet mottagarens adress och portnummer till den ursprungliga sändarens. Datorn i det lokala

nätverket märker aldrig att detta kontinuerliga utbyte av adresser sker, och upplever det som om den hade direkt förbindelse med mottagaren. Mottagaren i sin tur upplever hela det lokala nätverket som endast en dator, routern, som har ett flertal applikationer startade vilka använder portnumren 32768-65535.

Ett exempel som Vos, Konijnenberg (ibid.) illustrerar är försändelsen av ett paket från en dator i det lokala nätverket med adressen 192.168.37.15, till en extern server som har adressen 10.42.17.8, genom routern som har adressen 192.168.37.1. Paketet kommer då att förändras som redovisas i figur 2.5.

	Sändare		Mottagare	
	IP adress	Port	IP adress	Port
Ursprungligt paket	192.168.37.15	1027	10.42.17.8	23
Översatt paket	192.168.37.1	60005	10.42.17.8	23
---Väntan på svar---				
Svarspaket	10.42.17.8	23	192.168.37.1	60005
Återställt paket	10.42.17.7	23	192.168.37.15	1027

Fig 2.5, Översättning av nätverksadresser – ett exempel

Olika utökningar till denna funktion kan vara att låta routern först kontrollera så att den verkligen är ansluten till Internet för att kunna vidarebefordra paketet, eller att samtidigt låta den fungera som brandvägg genom att plocka bort de paket ur kön som ej anses vara säkra nog att passera. Då det vid snabba nätverksförbindelser kan komma att passera miljontals paket i sekunden genom routern, väcks säkert frågan hur mycket långsammare trafiken går med denna funktion aktiverad. Enligt Schenk (1998) märks ingen hastighetsskillnad över långsamma seriella förbindelser såsom modem eller ISDN, där en liten skillnad kan mätas upp då routern är fast ansluten till nätverket genom permanenta förbindelser.

De fördelar som redovisats med nätverksadressöversättning, bland annat möjligheten att dölja samtliga datorer i det lokala nätverket, kan enligt Egevang, Francis (1994) samtidigt vara till en nackdel. Det finns vissa fall då man vill tillåta externa användare att komma åt datorer i det lokala nätverket, vilket är helt omöjligt då en översättare av nätverksadresser är inkopplade. Likväl påpekar Egevang, Francis (ibid.) att det samtidigt innebär ökade möjligheter till skydd för en eventuell angripare som kan gömma sig bakom en annan dator utan att bli upptäckt. En dator med funktionen som översättare av nätverksadresser kan anslutas var som helst mot Internet, och behöver ej befinna sig i direkt anslutning till angriparens egen dator. En person skulle till exempel i hemlighet kunna installera ett sådant system i en av datorsalarerna på Högskolan i Borås, varefter han senare skulle kunna koppla upp sig mot denna dator från en modemförbindelse. Högskolan i Borås har för tillfället inte någon brandvägg som begränsar åtkomst till eller från Internet,

vilket gör att det skulle se ut som om en dator på Högskolan gör intrånget fastän personen som utför attacken kanske sitter i ett annat land ansluten via ett modem.

2.2.2 OSI-modellen

OSI-modellen, eller modellen för Open System Interconnection beskriver hur en dators nätverksarkitektur är uppbyggd och den är skapad av International Organisation for Standardisation (ISO). Modellen visar i detalj hur kommunikation sker i ett datorsystem, och ur denna mycket generella modell har ett flertal protokoll skapats, bland andra PPP och protokollsviten TCP/IP. Orsaken till att TCP/IP kallas för protokollsvit är att standarden består av en mängd olika protokoll, som tillsammans går under beteckningen TCP/IP.

Kommunikationen sker i lager, från den elektriska strömmen som leder till att nätverkskommunikation sker, till applikationen som nyttjas av användaren. Varje lager bestämmer funktionaliteten hos de protokoll som existerar där, beroende på dess roll i kedjan. De sju lager som beskrivs enligt OSI-modellen är enligt Graham (1997) följande:

- Fysiskt lager (lager 1): Det fysiska nätverksmediet. Exempel på detta är koaxialkablar och radiofrekvenser som används för nätverkskommunikation.
- Länklagret (lager 2): Här definieras protokollstandarderna för att ansluta till det fysiska nätverksmediet. Exempel på sådana protokoll är Token Ring, PPP och Frame Relay.
- Nätverkslagret (lager 3): De här protokollen används för att vidarebefordra paket mellan två slutnoder, och exempel på ett sådant protokoll är IP.
- Transportlagret (lager 4): Dessa protokoll används för transport av data mellan två slutnoder, och är antingen pålitliga eller opålitliga. Några protokoll som sköter detta är TCP och UDP.
- Sessionslagret (lager 5): Här finns protokoll för att upprätthålla en förbindelse mellan två slutnoder.
- Presentation (lager 6): Protokoll i detta lagret sköter konvertering av data från ett format till ett annat, exempelvis mellan ASCII och EBCDIC.
- Applikationslagret (lager 7): Användarapplikationerna.

TCP/IP-sviten innehåller protokoll i fyra av dessa ovanstående lager: länklagret, nätverkslagret, transportlagret och applikationslagret (se figur 2.6). Observera att OSI-lager 5 och 6 i figuren endast är med för att redovisa hur kopplingen mellan applikation och protokoll är definierad via så kallade sockets, och dessa lager har ingenting att göra med TCP/IP-svitens fyra lager

av protokoll. Huruvida lager OSI-lager 1 skall inräknas i TCP/IP-sviten verkar vara beroende av olika författares åsikter, Stevens (1994) anser att den ej skall inkluderas i TCP/IP-svitens lager då Graham (1997) anser att den skall göra det. PPP som kommer att redovisas senare befinner sig helt i länklagret, eftersom den definierar hur kommunikationen mellan en dator och ett modem skall ske. En orsak till att just TCP/IP har blivit en så populär standard, även för kommunikation inom lokala nätverk är enligt Stevens (1994) dels att standarden släppts helt fri, dels den stora tillväxt Internet märkt av de senaste åren.

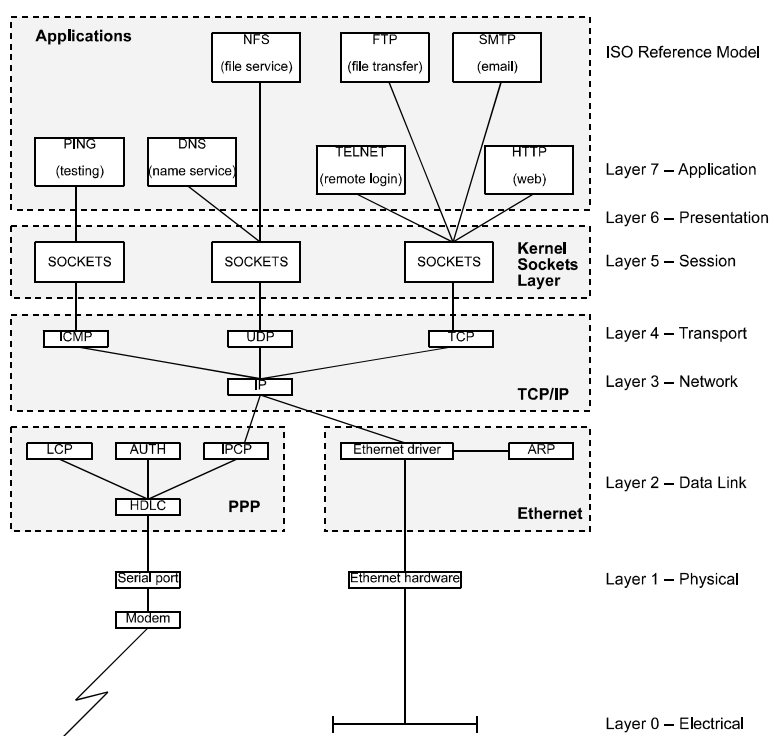


Fig 2.6, Protokollsviten TCP/IP tillsammans med protokollsviten PPP enligt Carlson (1998)

Eftersom ett protokoll verkar för att inkapsla data och ge den en funktion, så väcks säkert frågan hur inkapslingen sker mellan de olika lagren i OSI-modellen. Faktum är att det sker en mängd olika inkapslingar av data, och det ursprungliga datapaketet som levererades i applikationslagret kommer att ha minst tre olika inkapslingar innan det levereras till den fysiska nätverkskabeln (se figur 2.7). Detta leder till att det för varje paket som sänds läggs till en mängd kontrolldata som huvud, vilket kanske inte leder till någon större belastning över en permanent uppkoppling mot Internet, men blir desto mer märkbart då en temporär modemförbindelse används. Om ett da-

tapaket blir för stort vid sändning fragmenteras det automatiskt i ett antal mindre paket, vilket i sig kan leda till att onödiga resurser går åt till att kontrollera dataflödet i varje steg genom OSI-modellen. Det finns dock möjligheter att begränsa paketstorlekarna redan i sessionslagret så att inget paket kommer att fragmenteras senare i inkapslingskedjan, vilket kommer att diskuteras i detalj nedan då de olika TCP/IP protokollen kommer att redovisas.

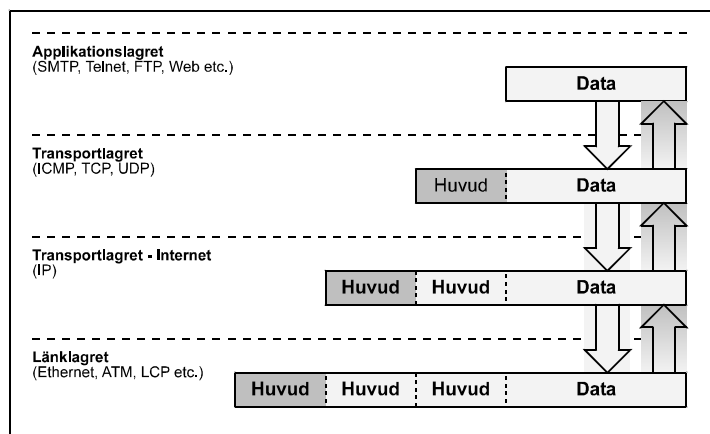


Fig 2.7, Inkapsling av data enligt TCP/IP-sviten, fritt översatt till svenska från Chapman (1995)

Vid kommunikation inom ett lokalt nätverk kan det tyckas onödigt att lägga till huvud för vidarebefordring av paket (eng. *routing*), genom IP protokollet. IP innehåller också en mängd information som är nödvändig för att skicka paket över stora distanser, men som aldrig kommer till sin rätt när datorerna är kopplade med en fast förbindelse i direkt anslutning till varandra. Det finns en mängd övriga protokoll på marknaden, såsom Appletalk och Novells IPX/SPX som är speciellt optimerade för denna situation. De använder mindre huvuderna för att kapsla in data, och huvuderna i sig innehåller ingen onödig information som ej kan komma att användas. Den senaste tidens stora tillväxt av applikationer som endast stödjer nätverkstrafik över TCP/IP kan leda till att många företag tvingas använda TCP/IP-sviten även i sitt lokala nätverk för att kunna bibehålla ett homogent användargränssnitt.

2.2.3 Olika nätverksprotokoll

Även om det vid det här laget borde te sig ganska klart vilken avgörande roll olika protokoll spelar vid överföring av data mellan olika nätverksenheter, så finns det trots allt ett behov av att klassificera och beskriva några av protokollen i detalj för att få inblick i hur översättning av nätverksadresser sker i

praktiken. De protokoll som kommer att nämnas nedan är dels protokoll som ingår i TCP/IP-sviten och befinner sig i OSI-lager 3 och fyra (nätverk och transport), dels protokollsviten PPP som befinner sig i OSI-lager 2, datalänken. När vi i fortsättningen diskuterar kring protokoll och deras uppgift att förmedla information mellan olika nätverksenheter kommer protokollen att betecknas transporttjänster (eng. *transport services*). I huvudsak finns det två typer av transporttjänster, pålitliga och opålitliga.

De pålitliga transporttjänsterna verkar enligt Graham (1997) i korthet för att skapa en fast anslutning till mottagaren, precis som ett vanligt telefonsamtal. Telefonsamtalet kan gå genom ett oändligt antal datorer och kablar på vägen, även om användaren upplever det som om det verkligen existerade en permanent anslutning mot mottagaren. Då information skickas i paket verifierar de pålitliga tjänsterna varje mottaget paket med hjälp av ett extra meddelande som skickas tillbaka till sändaren (detta meddelande använder i sig protokollet ICMP, se nedan). När informationen anlant till mottagaren felkontrolleras den sedan med hjälp av extra information som lagrats i huvudet på paketet, och returnerar vid fel ett meddelande om paketet skulle vara defekt. Pålitliga transporttjänster har även inbyggd flödeskontroll som ser till att ingen dator blir tvungen att ta emot fler paket än den hinner behandla. De ser även till att reorganisera paketen om dessa skulle ha anlant i fel kronologisk ordning. Ett exempel på en pålitlig transporttjänst är protokollet TCP.

Till skillnad från de pålitliga transporttjänsterna, så garanterar de opålitliga tjänsterna inte någonting. För att beskriva de opålitliga tjänsterna använder Graham (ibid.) liknelsen med postverket och proceduren med att skicka ett vanligt brev. En person skriver brevet (sammanställer informationen), lägger det i ett kuvert med mottagarens adress (inkapsling via protokoll) och lägger det i brevlådan (överföring). Efter det tar postverket över arbetet med att leverera brevet (vidarebefordring eller *routing*). Sändaren har ingen aning om hur lång tid det tar för brevet att ankomma till sin destination utan blir tvungen att uppskatta tiden baserat på tidigare erfarenhet. Sändaren vet heller inte om mottagaren får brevet överhuvudtaget, eller om han bekymrar sig om att läsa innehållet. I datorvärlden kallas paket som levereras genom opålitliga transporttjänster för *datagram*. Denna term har använts tidigare som namnet på en typ av paket, och detta är förklaringen. Eftersom det ej föreligger en fast förbindelse mellan sändare och mottagare så är det också möjligt att skicka samma datagram till flera mottagare (eng. *multicast* och *broadcast*).

Eftersom de opålitliga tjänsterna ej kan garantera leverans inom utsatt tid och ej har stöd för flödeshantering, vilket kan leda till att mottagarens system ej kan ta emot samtliga datagram, kan det vara svårt att se en nytta av dessa transporttjänster. Ett exempel då datagram verkligen kommer till nytta är genom programmet ICQ. Detta program skickar från klienten regelbundna datagram mot en central dator som registrerar att du är ansluten till Internet,

vilket gör att vänner och bekanta snabbt kan få tag på dig om du tillåter det. Det faktum att det idag finns över 10 miljoner användare av programmet innebär att det ej skulle vara möjligt att använda pålitliga transporttjänster, främst på grund av att det inte finns något datorsystem i världen som skulle kunna hantera denna mängd anslutningar. Nu kan centraldatorn istället skicka ut datagram via multicast till samtliga anslutna användare, och om den ej fått svar inom rimlig tidsåtgång och upprepade försök registreras användaren som bortkopplad från Internet. Detta illustrerar även det faktum att det är applikationerna som själva blir tvungna att sköta flödeshantering och bekräftelse på mottaget paket. Denna typ av transporttjänster lämpar sig också mycket bra för datorspel som kräver snabb överföring över ofta långsamma förbindelser, där programmerarna ej har något emot att skriva egna rutiner för att hantera dataförlust. Exempel på opålitliga protokoll är IP och UDP.

Nedanstående förklaringar av respektive protokoll kommer att hållas så kortfattade som möjligt så att uppsatsen i sin helhet ej domineras av en utmärkande teknisk karaktär. Detta för att den breda målgrupp som är definierad i första kapitlet på ett lättillgängligt sätt skall kunna tillgodogöra sig tillräckligt med kunskap för att förstå den tekniska diskussionen som kommer till en följd av implementationen.

IP

IP står för Internet Protocol, och är kärnan för all kommunikation i TCP/IP-sviten. All kommunikation som skickas via övriga protokoll såsom TCP, UDP eller ICMP inkapslas alltid av IP före det att datagrammet skickas vidare genom OSI-lagren. Vakna läsare märkte återigen beteckningen datagram istället för paket, vilket förtydligar det faktum att IP är en opålitlig transporttjänst. Skulle ett system ej ha möjligheten att ta emot eller skicka vidare ett paket så försöker det istället skicka tillbaka ett felmeddelande via transporttjänsten ICMP till källan.

Som beskrivet av Postel (1981a), så innehåller ett normalt IP-huvud 20 bytes data med information. Häri specificeras bland annat versionsnummer (IPv4 för närvarande), det aktuella datagrammets längd, livstid, checksumma för felkontroll, valt protokoll för den inkapslade datan, sändare- och mottagaradress samt identifikationsnummer. Identifikationsnumret används, eftersom det ej är garanterat att paketen anländer i kronologisk ordning, och ökas med ett för varje paket den sändande datorn skickar iväg. Felkontrollen i IP sträcker sig endast över det egna huvudet, då det är upp till de inkapslade protokollen (vilken typ av protokoll specificerades i huvudet) att själva ta hand om detta.

En utmärkande funktion för IP är datafragmentering, som används vid leverans av en stor mängd data till en gemensam mottagare. Då en mottagare enligt Stevens (1994) aldrig kan förutsättas att ta emot datagram större än 576 bytes, vilket kommer att rapporteras via felkoder över ICMP, riskerar fragmentering att ske ofta över förbindelser som på grund av dålig linjekvalitet begränsat datagramstorleken. Hur stora datagram ett system tillåts skicka går under beteckningen MTU (eng. *maximum transmission unit*), och den största tillåtna storleken på mottagna datagram går under beteckningen MRU (eng. *maximum receive unit*). Sättet IP-fragmentering fungerar på tillsammans med ett inkapslat TCP paket är redovisat i figur 2.8.

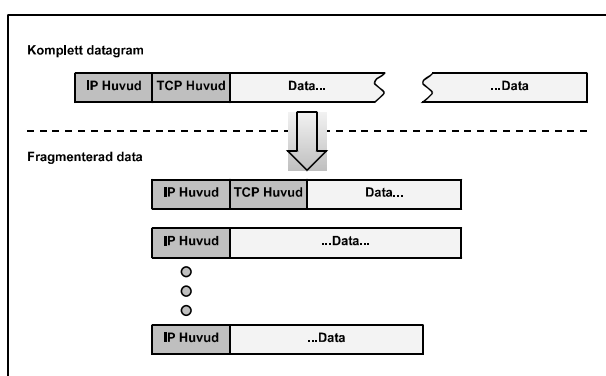


Fig 2.8, IP-fragmentering av ett TCP-paket, fritt översatt till svenska från Chapman (1995)

ICMP

ICMP är ett protokoll i transportlagret med uppgift att bland annat rapportera fel, då något av de övriga protokollen i transport- eller nätverkslagren ej kan leverera sin information till mottagaren. Övriga uppgifter ICMP har är att ständigt se till att sändaren använder en uppdaterat route till mottagaren. Ett exempel på detta är då ett datagram skickas via en router till en mottagare, och routern känner till en bättre väg. Routern skickar då automatiskt denna bättre väg till sändaren via ICMP-meddelanden.

ICMP-meddelanden är inkapslade i IP-datagram enligt figur 2.9, och innehåller i sig själva ett mycket litet huvud om endast fyra bytes, som redovisats av Postel (1981b). Detta huvud är placerat först i meddelandet, och innehåller först två bytes som kategoriserar meddelandets typ och vilket meddelande som redovisas, efter detta ges en checksumma på innehållet. Hur innehållet sedan är strukturerat beror på meddelandetypen, exempel på meddelanden som skickas över ICMP är ekosvar (pingsvar), meddelanden om att

destinationen ej kunde nås, omredigering av rutt samt begäran om eko (pingbegäran).

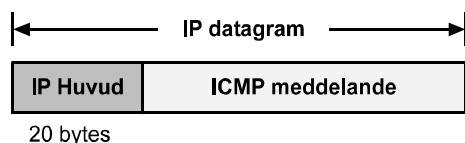
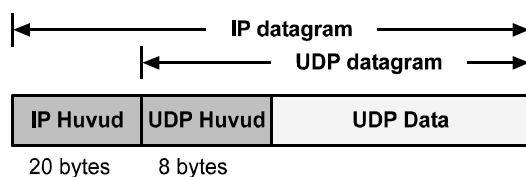


Fig 2.9, Inkapsling av ICMP-meddelanden i ett IP datagram efter Stevens (1994)

UDP

UDP är ett enkelt, datagramorienterat protokoll i transportlagret. UDP står på engelska för User Datagram Protocol, vilket fritt skulle kunna översättas till ungefär användarstyrt datagramprotokoll. Till skillnad från TCP som skickar data i flöden, är program som utnyttjar UDP tvungna att skicka exakt ett datagram i taget och sköta flödeshanteringen manuellt. UDP är ett typexempel på en opålitlig transporttjänst – datagrammen skickas direkt till nätverkslagret (IP) utan någon som helst garanti för att de når sin destination. Som nämnts tidigare vad gäller fördelar vid opålitliga transporttjänster så finns det orsaker att använda även UDP, som är en av övriga huvudkomponenter i TCP/IP-sviten.

Huvudet i UDP är konstruerat för att vara så litet som möjligt. Som nämnts tidigare under nätverksadressering krävs det för att en dator skall kunna ta emot paket att sändaren vet vilken nätverksport den skall skicka informationen till, samt hur mycket data som skickats. Postel (1980) fastställer således UDP huvudet till att innehålla just detta, sändarens- och mottagarens portnummer, längden på datablocket och en två byte lång checksumma som kontrollerar innehållets integritet, totalt åtta bytes (se figur 2.10). Notera här också skillnaden mot IP huvudets checksumma, som endast kontrollerar huvudet. Orsaken till detta är att det förutsätts att transportprotokollen ger möjlighet till kontroll av datan med hjälp av checksumma, även om man i vissa protokoll kan välja bort funktionen. Det sistnämnda gäller vid utnyttjande av UDP, då användaren kan välja att ej skapa eller kontrollera checksumman för att ytterligare öka hastigheten på överföringen, till skillnad från TCP som alltid kräver att checksumman beräknas och verifieras.

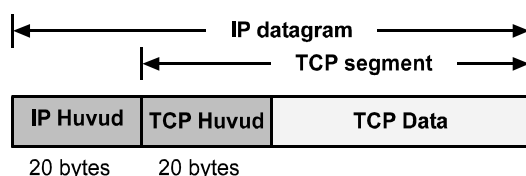


2.10, Inkapsling av UDP efter Stevens (1994)

TCP

TCP står på engelska för Transmission Control Protocol, vilket fritt översatt till svenska skulle kunna innebära protokoll för att kontrollera överföringen. Även om TCP använder samma nätverkslager som UDP (IP), så innebär bruket av TCP en helt annan service mot applikationslagret än UDP. Sammanfattat erbjuder TCP uppkopplingsorienterade, pålitliga tjänster där data överförs med hjälp av flödeskontroll. Med uppkopplingsorientering menas att två applikationer som skall utbyta data med hjälp av TCP (en typisk klient-server modell) först måste fastställa en TCP-anslutning med varandra innan de kan utbyta data (se liknelsen med telefonsamtalet under beskrivningen av pålitliga tjänster ovan).

TCP är först beskrivet av Postel (1981c), och fördelarna med detta protokoll är många. I likhet med IP, och till skillnad från UDP, har även TCP möjligheten att fragmentera data. Storleken på ett TCP-paket kallas vanligtvis för segment, och finns redovisat i figur 2.11. Denna fragmentering innebär att applikationer ej behöver bekymra sig om att separera datan i olika block, utan kan skicka en kontinuerlig ström data till transportlagret. Liksom UDP och alla andra protokoll i transportlagret har även TCP funktioner för att beräkna checksumma på innehållet. Till skillnad från UDP så beräknas alltid denna summa även om det ibland innebär onödig bearbetning (till exempel vid bruk av TCP i lokala nätverk med mycket låg brusfrekvens). Då TCP vid mottaget paket rapporterar till sändaren, finns det också inbyggt stöd för flödeshantering. Detta innebär att det ej finns någon risk för att en mottagare belastas med fler paket än systemet kan klara av att bearbeta.



2.11 Inkapsling av TCP-data i ett IP datagram efter Stevens (1994)

Just på grund av flödeshanteringen, inbyggda funktioner för fragmentering och den uppkopplingsorienterade strukturen på TCP är också huvudet större än UDP. Liksom UDP innehåller även detta huvud information om sändarens och mottagarens portnummer och checksumma, men istället för att som UDP specificera hur stort utrymme datan tar i bytes definierar TCP istället så kallad fönsterstorlek (eng. *window size*). Detta är helt enkelt den storlek på paketen som mottagaren kan tänka sig att använda vid överföring, och som nämnts tidigare så är denna alltid lika med eller över 576-20 bytes (IP's huvud borträknat). När en bidirektionell överföring sker kan denna fönsterstorlek förändras, även om det i vissa operativsystem är möjligt att låsa fönsterstorleken vid ett fast värde.

PPP

Det sista protokollet som nämns är PPP, som på engelska står för *Point-to-Point protocol*. Point-to-point är en speciell typ av nätverk där två enheter står i direkt anslutning till varandra, och används enligt Ringo (1994) mest för situationer där överföringshastighet är den viktigaste aspekten. Exempel på sådana miljöer kan enligt Carlson (1998) vara en personlig anslutning via modem mot Internet och storskaliga miljöer som satellitkommunikation och integrerade stordatormiljöer. PPP är alltså ej ett protokoll endast för modemförbindelser, även om den verkar över bidirektionella seriella kopplingar.

PPP är egentligen en protokollsvit, lika mycket som TCP/IP, och består i sig av ett flertal protokoll (se figur 2.6). Sviten består enligt Simpson (1993) av fyra grundläggande komponenter, där den första är möjligheten att kapsla in IP-datagram över en seriell länk, genom antingen synkron eller asynkron överföring. I figur 2.6 redovisas ett av dessa, IPCP som står för *IP Control Protocol*. Nästa komponent är det inbyggda protokollet för att hantera länken mellan noderna (eng. *link control protocol*, LCP), som innehåller funktioner för att fastställa, konfigurera och testa uppkopplingen. Den tredje, och kanske viktigaste komponenten är de inbyggda protokollen för att kontrollera nätverkstrafiken (eng. *network control protocols*, NCP). HDLC-protokollet som i figur 2.6 redovisas som ett sista steg före det att data skickas till serieporten är en ISO-standard (eng. *high-level data link control*), och definierar sätt att strukturera paket för överföring via en seriell uppkoppling, med hjälp av bland annat start- och stopbitar tillsammans med checksumma.

Skillnaderna mellan de olika varianterna av synkron och asynkron överföring som nämnts ovan ligger i hur data överförs. Asynkron hårdvara (kallas ofta för UART, eng. *universal asynchronous reciever/transmitter*), kan endast skicka och ta emot ett tecken i taget. Synkron hårdvara, som ibland även kallas för USART, kan ta emot en ström av tecken i en följd. Utöver dessa

två standards, så nämns ibland även duplex vilket betecknar möjligheten att ta emot och skicka data parallellt. Full duplex innebär att en adapter kan skicka och ta emot data samtidigt.

Även om LCP sköter säkerställandet av linjekvaliteten, så finns det ingen garanti för att obehöriga ej ansluter sig mot en av datorerna då den seriella linjen är nedkopplad. PPP-sviten innehåller då protokoll för användaridentifikation, som används vid den första LCP-anslutningen. De vanligaste protokollen som används för identifikation idag är PAP och CHAP, där mindre skillnader dem emellan enligt Carlson (1998) gör att det är omöjligt att utsluta den ena, eller säga att en standard är bättre än den andra. Carlson (ibid.) anser dock att ett bra system bör klara båda standards, trots att det verkar som om PAP är på väg ut från marknaden (Uppdaterade RFC's som behandlar PPP-identifikation nämner endast CHAP). Microsoft har även konstruerat en egen standard kallad MS-CHAP, som enligt Carlson (ibid.) i sig inte har några fördelar jämfört de andra systemen, utan istället inför en rad säkerhetsrisker. Med MS-CHAP är det till exempel tillåtet att ändra lösenord på fjärrdatorn.

2.2.4 Nätverkssäkerhet

Enligt Ringo (1994) så är det en omöjlighet att definiera ett datorsystem som säkert eller ej. Istället används olika säkerhetsnivåer som tilldelas operativsystemet genom en metod som bygger på tillit (eng. *trust*). Ett system med stora krav på tillit förhindrar samtliga försök till angrepp, men innebär samtidigt ökad komplexitet för de personer som verkligen är tilltrodda och har legitim rätt till åtkomst av information. Enligt Ringo (ibid.) så finns det i datorsammanhang fyra olika säkerhetsnivåer, vilka representeras av bokstäverna A till D, där D innebär största möjliga tillit inför sina användare. Varje nivå delas sedan in i ytterligare grupper såsom A1, A2, A3 och så vidare, där högre nummer visar på högre säkerhet. Ett exempel på ett säkerhetssystem som når upp till A-nivå är en dator inlåst i ett kassaskåp utan vare sig ström eller användare, där vi i andra änden av spektrat finner operativsystemet Microsoft Windows95 som ligger på D-nivå. Windows95 har inga säkerhetsfunktioner alls, och tillåter vem som helst som har tillgång till datorn att utföra vilka operationer som helst. Alla övriga operativsystem ligger någonstans däremellan, och för att nämna ett exempel så placerar sig Linux på C2 nivå tillsammans med många andra UNIX-baserade operativsystem. Detta anses idag vara en bra säkerhetsnivå, då det enligt Ringo (ibid.) ej existerar något kommersiellt operativsystem som når upp till B-nivå.

Om man ej kan fastställa att ett system är helt säkert mot intrång, hur kan man då verka för att öka säkerhetsnivån? Ett sätt är att låta samtliga paket i ett lokalt nätverk passera en router innan de lämnar nätverket, vilket gör att

programvaran på routern kan verifiera både ingående och utgående pakets behörighet. Routern tar då på sig rollen som brandvägg, och om systemet samtidigt översätter nätverksadresserna inom det lokala nätverket mot Internet före det att paketen levereras externt, blir det mycket svårt för en eventuell angripare att spåra de datorer som är anslutna till det interna nätverket. Egevang, Francis (1994) påpekar dock att det finns vissa nackdelar med nätverksadressöversättning, främst det faktum att det ej går att kryptera TCP-huvudets checksumma när denna teknik används. Å andra sidan menar Egevang, Francis (ibid.) att funktionaliteten i sig som förhindrar insyn i det lokala nätverket, tillsammans med det faktum att applikationsbaserad kryptering fortfarande fungerar kan räcka för att rekommendera nätverksadressöversättning som teknik för att öka säkerheten i mindre nätverk.

De flesta Internetleverantörer idag erbjuder inte möjligheten för företag och privatpersoner att alltid få samma IP-adress vid anslutning till Internet. Den uppringande datorn tilldelas alltid ett nytt, dynamiskt nummer från den lista adresser leverantören har reserverat. Detta leder i sig till en högre säkerhet än en ständigt ansluten dator eftersom det är omöjligt för en eventuell angripare att på förhand veta vilken adress klienten ansluter sig till.

När dessa tekniker verkar tillsammans, brandvägg med paketanalys som tilldelas en ny adress varje gång den ansluter till Internet samt översättning av nätverksadresser före paketleverans mot Internet, fås en miljö som i sig är mer säker än om en dator ansluts direkt mot Internet över en fast förbindelse. Det finns teorier som ej nämnts i detta kapitel som kan verka för att ytterligare öka säkerheten mot Internet, men då de skulle innebära att alltför många applikationsprotokoll skulle sluta fungera har jag valt att utelämna dem.

2.3 Perspektiv och teorival

När man inser hur mycket arbete som ligger bakom de produkter som idag finns tillgängliga gratis ställs naturligtvis frågan om man kan ta betalt för att informera om programmets möjligheter. Det säljs idag slutna system som uppfyller en del av de säkerhetsaspekter som nämnts innan, samtidigt som det finns företag som hyr ut konsulter vilka hjälper klienter att installera och konfigurera dessa fria program.

Personligen hamnade jag i ett moraliskt dilemma där jag för ett ögonblick ej kunde avgöra hurvida jag verkligen skall redovisa *samtliga* steg som krävs för att installera och konfigurera ett system som lever upp till de säkerhetsaspekter som diskuterades i stycke 2.2.4. Det finns uppenbarligen pengar att tjäna på att hemlighålla denna kunskap, men frågan är om det är etiskt försvarbart? I USA finns en större organisation kallad Association for Compu-

ting Machinery (ACM) som har sammanställt etiska regler och riktlinjer som kan tillämpas över hela IT-industrin. Generellt sett så har etiska normer enligt Forester, Morrison (1994) varit alltför generella som "Jag skall undvika att skada andra" och "Jag skall alltid vara ärlig och pålitlig". ACM's nya yrkesetiska riktlinjer är enligt Forester, Morrison (ibid.) starkt förbättrade eftersom de redovisar situationer specifika för IT-industrin.

Riktlinje 2.7 i ACM's lista över etiska normer för yrkesverksamma IT-expertter har fritt översatt från Forester, Morrison (1994) rubriken "Öka förståelsen för databehandling och dess konsekvenser hos allmänheten". I kort innebär denna norm att dataexperter bör verka för att dela med sig av sin tekniska kunskap till allmänheten, inklusive den eventuella påverkan data-systemet kan ha tillsammans med dess begränsningar. Då jag än så länge ej arbetar under ett kontrakt som hindrar mig från att dela med mig av min kunskap, är det enda etiskt försvarbara valet att redovisa all uppnådd kunskap på ett så tydligt sätt som möjligt.

I övrigt så är det enligt min uppfattning svårt att skydda ett lokalt nätverk mer än som beskrivits i stycke 2.2.4. En bekant som är anställd på Ericsson här i Borås beskrev hur de hade kopplat tre stycken brandväggar i sekvens för att skydda det lokala nätverket. Även om det teoretiskt är möjligt att gissa sig till lösenordet hos den första brandväggen med tillräckligt många försök är det tidsmässigt omöjligt att ta sig igenom samtliga tre routers före det att angreppet kan spåras.

Eftersom det system jag ämnar implementera använder en dynamisk tilldelning av nätverksadresser varje gång systemet ansluts Internet, hindras angripare så fort datorn kopplar ner förbindelsen. I övrigt så är det som sagt omöjligt att få kontakt med datorer inom det lokala nätverket då översättning av nätverksadresser används, vilket kan leda till slarv med nätverkssäkerheten. Företaget Telia råkade ut för detta 1997, då de lokalt hade delat ut samtliga filer till alla användare som kunde se dem. Telia hade endast en brandvägg ansluten till Internet och hade ej utfört nödvändiga åtgärder på denna för att försvåra externa angrepp. Därför tog det inte lång stund förrän en attack ledde till att en utomstående angripare hade fått full kontroll över hela brandväggen. Han kunde härifrån sedan enkelt komma åt de kataloger där Telias hemsidor lagrades och bytte ut dem mot egna varianter. Då angriparen innan han lämnade brandväggen raderade alla spår av intrång gick det ej att se hur attacken hade skett, och attacken kunde sedan upprepas ett flertal gånger där angriparen till sist fick fram en reaktion efter att ha hämtat all intern personlig epost och hotat med offentlig publicering.

3 Metodval och metodbeskrivning

Valet av metod påverkar sättet en studie utförs på, vilket i sin tur påverkar resultatet. Då problemformuleringen i denna studie bygger på behovet att finna ett tekniskt hjälpmedel som svarar mot människors kommunikationsbehov, räcker det ej med att endast granska kvantitativa, mätbara effekter i det implementerade systemet. Det är samtidigt av yttersta relevans att systemet i sig motsvarar de förväntningar som människor kan tänkas ha, där dessa åsikter i sig leder till behovet av en kvalitativ ansats.

Kraven för att en studie skall kunna benämnas som kvantitativ är enligt Andersen (1994) att den information som studeras skall vara möjlig att mäta. Sättet informationen inhämtas på beror på vald undersökningsform, och detta angreppssätt bör specificeras så tydligt att det är möjligt för andra forskare att objektivt uppnå liknande resultat. Precisionen i resultatet hos en kvantitativ studie beror på hur stor mängd information som granskats. För att kunna mäta det tekniska systemets tekniska kvalitéer och se huruvida dessa motsvarar tidigare nämnda problem kommer det att vara nödvändigt med en kvantitativ studie, där genomförandet av denna bör vara så tydligt specificerad att det skall vara möjligt för en utomstående forskare att upprepa försöket.

I problemformuleringen ingår även kvalitativa benämningar som används för att fastställa hur människorna upplevde systemet. Eftersom detta ej är någonting mätbart som genom en ny studie objektivt kan upprepas utan istället fokuserar på helhetsbilden och kunskapens karaktär, passar detta väl in på ett kvalitativt angreppssätt som beskrivits av Andersen (ibid.). För att kunna sammanställa en kvalitativ studie krävs det att man på något sätt kommer nära människorna och låter dem få möjlighet att fritt uttrycka sina egna perspektiv, vilket kan göras genom antingen deltagande observationer på plats eller olika former av intervjuer och enkäter. Tidsbegränsning förhindrar

möjligheten att granska människornas reaktioner och upplevelser, och med hänsyn tagen till detta kommer enkätform kommer att väljas.

För att konstruera det tekniska system som ligger till grund för studien kommer ett flertal undersökningsmetoder att utföras. För att använda de beteckningar som Lundahl, Skärvad (1982) redovisar skulle studien kunna klassificeras som en *explorativ, beskrivande* och *utvärderande* undersökning. En explorativ ansats passar ypperligt till att granska de möjligheter till implementation som existerar idag, genom relaterat arbete. För att förstå bakomliggande funktioner används en beskrivande undersökning där informationen inhämtas genom en större litteraturstudie och redovisas som teorier av betydelse. Då beskrivningsspråket vid denna typ av studie ej är av relevans annat än för att förtydliga, ligger istället tyngdpunkten i att omsortera all den mängd data som finns tillgänglig för att forma strukturen. För att slutligen mäta effekterna av det implementerade systemet kommer en utvärderande undersökning att utföras genom studie av empiriska testdata och svarsenkäter, vilket tillsammans kommer att verka för att forma resultatet.

4 Genomförande

4.1 Planering

När jag via diskussionsgrupper över Internet läst om personer vilka redovisat olika tekniska lösningar som samtliga kan tänkas leva upp till de krav som formulerats i problemformuleringen, visste jag att det skulle vara möjligt att nå fram till ett utvärderande resultat. Frågor som kvarstod var hur mycket tid det skulle ta att sätta sig in i de olika tekniker som finns tillgängliga, hur den bakomliggande tekniken fungerade samt vilka av dessa system som skulle kunna tänkas leva upp till förväntningarna. Det stod då klart att jag först skulle vara tvungen att via den explorativa ansatsen finna och beskriva de program som skulle kunna användas. Efteråt då programmen var utsedda skulle en detaljerad litteraturstudie utföras som beskriver och förklarar programmets bakomliggande funktionalitet, följt av en systemimplementation för att kunna utvärdera dess funktionalitet.

För att utvärdera det tekniska systemet måste företag kontaktas som är beredda att upplåta sin datorparks säkerhet till detta testsystem, vilket innebär att om problem uppstår riskerar företaget att vara helt utan Internetförbindelse, eller med en Internetförbindelse som är uppkopplad dygnet runt. Företagen måste även vara beredda att upplåta sitt användarlösenord för att ansluta sig mot Internet till mig, eftersom detta kommer att sparas lokalt på datorn för att sedan automatiskt hämtas vid varje ny anslutning.

För att praktiskt utföra testet kommer jag att använda mig av de riktlinjer för genomförande av testprojekt som Mynatt (1990) anser vara relevanta, vilka är speciellt lämpade för olika studentprojekt. Riktlinjerna innebär i korthet att man på ett tidigt stadium fastställer vad som skall mätas och varför testet utförs. Efter detta fastslås angreppssättet för hur testet kommer att utföras, följt av en komplett beskrivning av testets upplägg och innehåll. Före det att testet sedan realiserar bör man som en sista förberedelse definiera hur det förväntade eller korrekta resultatet av testet bör se ut, för att enligt Mynatt

(ibid.) undvika situationer som ”Det här resultatet är tillräckligt bra”, då resultatet kanske innehåller ett eller flera fel. Svaret från testet kommer sedan att jämföras med detta förutspådda resultat för att se hur väl testprojektet föll ut.

För att få reda på användarnas perspektiv på systemet kommer även en enkät att förberedas som svarar mot delar av problemformuleringen i första kapitlet. Denna enkät kommer bland annat att användas för att se om systemet med sin transparenta koppling mot Internet leder till att människor utnyttjar Internet mer ofta när de manuellt slipper utföra proceduren att ringa upp och koppla ner förbindelsen.

4.2 Praktiskt arbete

Det praktiska arbetet har delats upp i tre faser, där var och en använder en unik undersökningsmetod. Den första fasen är en explorativ studie i syfte att finna ett system som kan tänkas uppfylla de behov som är specificerade i problemformuleringen. Efter det skall systemet funktionsmässigt beskrivas med hjälp av en omfattande litteraturstudie som förklarar alla termer och begrepp, och den sista fasen behandlar testförfarandet med hjälp av en utvärderande ansats.

4.2.1 Teknisk inventering

För att välja det operativsystem med tillhörande programvara som skulle användas i testet påbörjades arbetet med att söka upp all information om nätverksadressöversättning och behovsprövade uppkopplingar mot Internet. Den lösning som efter mycket sökande över Internet subjektivt verkade populärast var operativsystemet Linux, med tillhörande programvaran DialD. Till Linux finns även drivrutiner för att ansluta ISDN-adaptrar vilket skulle göra det möjligt att skala upp systemet från modem till ISDN vid behov. För att välja distribution av Linux granskades de mest sålda paketen från Caldera och Redhat i avseendet antal tillgängliga, färdigkonstruerade program. Då de skilda distributionerna använder sig av olika program för att installera programvara kan användaren i värsta fall bli tvungen att själv skapa programmet med en kompilator, vilket ej är önskvärt. Efter en snabb granskning upptäcktes att samtliga nödvändiga program fanns installerbara till Redhat Linux 5.0, som tillsammans med första versionen av programmet Diald-config släpptes endast några veckor före det att sökningen påbörjades. Just det faktum att programvaran var så pass ny ledde till att testfasen fick uppskjutas till våren 1998 i väntan på felkorrigerade versioner.

Även om det hade varit möjligt för mig att konstruera systemet med en äldre version av Redhat Linux och jag således hade kunnat påbörja testfasen tidigare, var dessa miljöer alldeles för komplexa för att det skulle vara möjligt att redovisa samtliga nödvändiga förändringar som gjorts i datormiljön. Det nya abstraktionslagret till DialD som levereras med Diald-config leder till att antalet förändringar som krävs i operativsystemet kan hållas vid ett absolut minimum och även kan utföras av personer med begränsad erfarenhet av UNIX-baserade operativsystem.

4.2.2 Litteraturstudie

De program som valts för att konstruera systemet levererades med minimal dokumentation, vilket ledde till att en omfattande litteraturstudie fick utföras. Även om det finns viss information om hur programmen i sig fungerar, så förutsätter ofta författarna att läsaren redan har all nödvändig kunskap om nätverksteorier. Då jag som systemvetare hittills mest varit involverad i metodologiska projekt ledde detta till att jag var tvungen att inhämta en stor mängd information parallellt med genomförandet av testet. Det faktum att det under de senaste månaderna kommit ett antal program som abstraherar den bakomliggande tekniken från användaren gjorde att jag kunde vänta med stora delar av litteraturstudien till efter det att systemtestet påbörjats.

4.2.3 Test

För att kunna genomföra testet i skarp miljö hos olika företag var jag först tvungen att installera systemet på min egen dator för att få fram minimala krav på hårddiskutrymme och RAM. Efter att ha minskat datorns primärminne till 16mb fann jag att det räckte med ett hårddiskutrymme på 200mb för att installera all nödvändig programvara. Högskolan kontaktades då och de erbjöd mig att låna fem arbetsstationer för att kunna genomföra testet, vilka var utrustade med en processor av typen 486-66mhz, 16mb primärminne och 200mb sekundärminne.

För att testet skall vara kvantitativt upprepningsbart har samtliga steg som gjorts vid installationen redovisats i bilaga B, som på grund av sitt omfång använder en egen sidnumrering och innehållsförteckning. Denna bilaga användes även vid installation och konfiguration av de olika systemen för att garantera en homogen miljö över samtliga datorer.

Företagskontakt

Högskolan i Borås är medlem i stiftelsen STIS (Stiftelsen för Teknikutveckling i Sjuhärad), vilken strävar efter att öka samarbetet mellan Högskolan och det lokala näringslivet. Vid kontakt med Högskolans representant i STIS Hans Holmqvist erhöles telefonnumren till ett antal företag och kontaktpersoner vilka kunde tänkas vara relevanta för projektet. Vid kontakt med dessa hade merparten redan införskaffat eller planerade att installera en fast förbindelse mot Internet, och av listan blev det till slut endast ett företag kvar. Detta företag, Helge Nyberg AB, visade sig mycket positiva till projektet eftersom de själva övervägde att ansluta sig till Internet, men hade svårt att motivera kostnaden till en fast förbindelse, då anslutningen endast skulle användas för epost och inhämtning av produktinformation.

Då endast ett företag ej skulle räcka för att utvärdera systemets funktionalitet var jag tvungen att söka upp fler företag. Till slut fann jag företagen Davita Konsult och Torslanda Stål och Mekaniska AB vilka båda hade ett litet antal datorer i företaget, men tillräckligt många för att Internetåtkomst var önskvärd för samtliga anställda samtidigt. Företaget Davita Konsult använder idag Internet via en dator till distansarbete, distansutbildning, diskussionsareor samt epost, och efter kontorstid finns det intresse av att kunna spela datorspel över förbindelsen. Torslanda Stål och Mekaniska AB använder Internetförbindelsen till aktiehandel, bankärenden, epost samt inhämtning av nyheter.

Samtliga företag hade helt skilda arbetsmiljöer vilket i sig skulle verka för att sätta systemet till test. Helge Nyberg AB hade sedan tidigare både en UNIX-server och en WindowsNT-server installerade på nätverket, tillsammans med en ISDN-box ansluten till en router för ingående dataförbindelser från ett distanskontor. Deras huvudsakliga ekonomisystem arbetade via en TCP-förbindelse mot den redan existerande UNIX-servern, och ett införande av Linuxsystemet i denna komplexa nätverksmiljö skulle innebära att samtliga paket som genererades av de sju datorer som idag var anslutna till nätverket skulle behöva passera genom Linuxservern. Utöver datorerna så var även en nätverksskrivare ansluten till nätverket, vilket tillsammans förleder misstankar om en hårt belastad Linuxserver.

Davita Konsult har ett mindre nätverk med endast två sammankopplade datorer, så belastningen här är mindre. Denna belastning ökar dock på kvällstid då dataspelen ibland plockas fram, och Davita Konsult har lovat att pröva även de mest nätverksintensiva spel för att belasta Linuxsystemet. Torslanda Stål och Mekaniska AB använder ett nätverk som innehåller två stationära datorer för ekonomiärenden, tillsammans med två bärbara datorer för distansarbete. Dessa bärbara datorer ansluts emellertid ofta till nätverket för att

synkronisera informationen, och används också för vissa specialapplikationer.

Kriteriesammanställning

För att genomföra testet enligt Mynatt's riktlinjer (1990) fastställdes först vad som skulle uppmätas med hänsyn tagen till problemformuleringen. Då överföringshastigheten som tidigare nämnts enligt Schenk (1998) ej påverkas när Linuxsystemet är anslutet till en så pass långsam nätverksenhet som modem eller ISDN, finns det inget intresse av att utvärdera denna faktor. Det som är intressant är att verifiera att systemet ej ansluter vid icke tillåtna tider, vilket kommer att möjliggöras genom användandet av utökade loggningsfunktioner som beskrivs i bilaga B. Då det för att verifiera att samtliga användares program som skall leda till Internetanslutning får Linuxservern att ansluta sig krävs deltagande observationer, och går ej att sammanställa kvantitativt (samtliga nätverkspaket som någon gång passerat genom Linuxsystemet skulle behöva sparas) kommer denna kontroll att ske genom en enkätfråga. Nackdelen med detta undersökningssätt är att orsakerna bakom problematiken kan vara svåra att utröna. Det förväntade resultatet av denna tekniska utvärdering bör då vara ett system som endast ansluter vid specificerade tider, vilket kommer att vara kravet för att systemet skall anses ha fallit väl ut.

Om detta kriterium uppfylls blir det samtidigt mycket enkelt att kalkylera en maximal månatlig avgift för samtalsaxan, då denna som mest motsvaras av telefonkostnaden för ett vanligt telefonsamtal den tiden systemet tillåts koppla upp sig. Då systemet har en nedkopplingstid efter inaktivitet som standard satt till två minuter behöver ej heller uppkopplingskostnaden tas med i beräkningarna. I övrigt så tillkommer denna kostnad ej då företag använder sig av en ISDN-adapter istället för modem, vilket samtidigt leder till att uppkopplingstiden för att ansluta datorn till Internet minskar från 30 till 2 sekunder.

Genomförande

När systemet konfigurerades togs hänsyn till en mängd aspekter som skulle påverka dess funktionalitet. Brandväggen skulle vara öppen för både ICMP-, TCP- och UDP-paket, och TCP-segmentens fönsterstorlek tillsammans med IP's MTU/MRU skulle behöva begränsas för att förhindra att en användare skulle kunna ta för mycket systemresurser i anspråk av förbindelsen. Eftersom det inom företagen ej existerade en sådan situation att det fanns misstanke att anställda skulle missbruka Internetanslutningen, konfigurerades systemet till att vidarebefordra samtliga utgående paket. För att granska de

val som gjorts hänvisas till bilaga B, även om den på sina ställen håller en hög teknisk nivå.

Systemet hos företagen som genomförde testet skulle uppfattas som ett slutet system och därför planerades ingen tid under testperioden till att verifiera dess funktionalitet. Testperioden sattes till åtta veckor, vilket med kontinuerlig belastning borde generera tillräckligt med empiri för att genomföra undersökningen.

Enkät

För att få svar på frågor som ej kan uppmätas genom en tekniskt kvantitativ analys kommer användarnas uppfattningar om implementationen att inhämtas via en enkät. Frågorna i enkäten som redovisas i bilaga A svarar direkt mot problemformuleringen och enkäten skickades ut till samtliga personer som under testperioden haft tillfälle att utvärdera anslutningen.

En fråga som kan uppfattas som tvetydig är den där användaren vid ökat Internetanvändande fritt får ange en tänkbar orsak till varför detta har skett. Formuleringen har valts för att ej styra in användaren på problemformuleringens beteckning av termen "transparent Internetförbindelse", vilket är en av de viktigare aspekterna vid implementationen av systemet. Upplever ej medarbetarna systemet som en transparent länk mot Internet så framkommer detta ändå med önskvärd tydlighet.

Resultatsammanställningen av enkäten kommer att utföras genom en kvantitativ resultatredovisning, som sedan kommer att analyseras kvalitativt. Svaren kommer att struktureras i tre olika grupper, där den första kategorin kommer att behandla användarnas personliga erfarenheter av Internetanslutningen. Då dessa upplevelser i frågeformuleringen ej är relaterade till företagsspecifika aspekter kommer svar från samtliga intervjuade att användas. De två övriga grupperna är programvara och systemproblem, som är helt beroende av vilken datormiljö och applikationsprogramvara som används inom respektive företag. En kategorisering kommer därför att genomföras där svaren kommer att redovisas var för sig under respektive organisation.

De tre kategorier som valts svarar direkt mot de två första frågorna i problemformuleringen som ställdes i kapitel 1, och frågornas fördelningen mellan kategorierna kommer att vara enligt följande. Frågorna 1 – 3 tillsammans med fråga 8 och 10 kommer att placeras i kategorin erfarenheter av Internetanslutningen. Fråga 4 och 5 kommer att ligga till grund för den programtekniska delen, där fråga 6, 7 och 9 formar kategorin systemproblem.

4.3 Problem

Att få ett företag att erkänna en students kunskaper kan ibland uppfattas som svårt. Att få ett företag att förlita hela sin interna datorsäkerhet till en students kunnande skulle troligen avfärdas som en ren utopi av många säkerhetsansvariga. Jag befann mig i den situationen att företagets samtliga nätverkspaket var tvungna att passera Linuxsystemet för att en adressanalys skulle kunna ske, vilket samtidigt innebar att ett felaktigt konfigurerat system skulle kunna få ödesdigra komplikationer. Som om detta inte var nog var de involverade företagen även tvungna att delge mig sina användaridentifikationer och lösenord för att ansluta datorn till Internet, och om datorn slutar fungera står plötsligt hela datorparken inte bara utan Internetåtkomst, utan även helt utan nätverksåtkomst (då även de lokala nätverkspaketen skickas via Linuxservern). Jag blev emellertid mycket positivt överraskad av responsen jag erhöll, och testförfarandet innebar inte några tillitskonflikter överhuvudtaget.

När systemet väl satts i drift upptäckte personal på företaget Helge Nyberg AB en sen fredagseftermiddag att Linuxservern ej ville koppla ner förbindelsen mot Internet. Orsaken till detta var ej känd, men en teori är att någon dator kontinuerligt begärde uppdaterad information genom exempelvis en webbläsare. Då jag ej hade tid att bege mig till företaget, som ligger några mil utanför Borås, guidade jag istället Patrik Ingnell, som är anställd på företaget, genom proceduren att ansluta sig till Linuxservern över nätverket, få den att koppla upp sig till Internet, för att sedan redovisa vilken dynamisk IP-adress den blivit tilldelad. Allt detta sköttes över telefon. Jag kunde sedan via Högskolan ansluta till Linuxserverns IP-adress för att förändra en parameter i systemets tidsbegränsning, som skulle leda till att datorn ej kopplade upp sig mot Internet på varken kvällar eller helger. Denna metod användes även mot företaget Torslanda Stål och Mekaniska för en parameterändring och upplevdes mycket positivt av samtlig involverad personal. Då systemet är byggt på en mycket öppen arkitektur kan tidsbegränsningen även användas för att förhindra Internettrafik på större helger och semestrar.

5 Resultat

5.1 Insamlat material

Efter den genomgångna testperioden om åtta veckor, som varade mellan den första februari till den första april 1998, var det dags att granska resultatet. Enkäterna som finns redovisade i bilaga A skickades ut till den personal som använt Internetanslutningen och respektive systems logfil inhämtades därefter för att kunna verifiera uppkopplingsstatistiken. Detta kapitel kommer först att redovisa svaren från den tekniska undersökningen för att verifiera att uppkopplingar ej skett på oönskade tider, varefter en kostnadsmodell kommer att presenteras baserat på denna statistik. Efter detta sammanställs och struktureras enkätsvaren, varvid dessa kommer att analyseras i detalj.

5.1.1 Teknisk utvärdering

Då en parameter avseende tidsbegränsningen mot Internet var felaktigt satt från början av testperioden ledde detta till att endast sex veckor av utvärderingsperioden kunde användas för att granska de uppkopplingar som skett. Logfilerna visade vid insamling och granskning att datorerna hade stängts av eller startats om minst en gång i veckan, vilket skett genom att användare tillfälligt brutit strömtillförseln. Detta var en nödvändig handling då systemen levererades till företagen utan vare sig skärm eller tangentbord, och således ej kunde stängas av mjukvarumässigt.

Eftersom tidsbegränsningen implementerats vid olika tider hos de olika företagen (två av dem var tvungna att utföra omfattande kvällsarbete) gick det ej att tidsbestämma en generell uppkopplingsstatistik av logfilerna. Det som gick att utläsa var att systemet, då det skett en korrigerings i konfigurationsfilen som sköter tidsbegränsningen, aldrig anslöt sig vid oönskade tider mot Internet, även om användaren begärde detta. Systemet anses därför ha klarat det tekniska provet, och det går således att bestämma en maximal uppkopp-

lingskostnad baserad på det antal arbetstimmar som systemet skall vara tillgängligt per dag, vilket betyder att kostnaden slipper räknas på 24-timmars dygn.

5.1.2 Kostnadsmodell

Om ett slutet system som ej innehåller några tidspärrar sköter uppkopplingen mot Internet finns det en risk att anslutningen är uppe 24 timmar om dygnet. Är företaget stängt på större helger och över semestertider finns det ej heller något intresse av att ansluta mot Internet sig under dessa perioder. Eftersom tidsbegränsningen i det implementerade systemet fungerade enligt specifikationen blir det relativt enkelt att beräkna den maximalt största rörliga månadskostnaden för systemet enligt formeln:

$$\text{Maximal månadskostnad} = K + D \cdot (H1 \cdot R1 + H2 \cdot R2) \cdot 60$$

K = Fast månatlig kostnad för möjlighet till Internetanslutning

D = Antal veckodagar per månad som anslutning skall vara möjlig

H1 = Antal timmar per veckodag mellan 08-18 som anslutning skall vara möjlig

H2 = Antal timmar per veckodag mellan 18-08 som anslutning skall vara möjlig

R1 = Anslutningsavgift per minut för Internetanslutningen mellan 08-18

R2 = Anslutningsavgift per minut för Internetanslutningen mellan 18-08

I kostnaderna R1 och R2 bör även vanlig samtalstaxa läggas till om anslutning ej sker mot ett 020-nummer. Uppkopplingsavgift har ej redovisats i modellen, främst på grund av en sådan ej existerar om en ISDN-adapter används. Används modem så går denna markering trots allt till samtalstid, och då systemet har en nedkopplingstid på två minuter som diskuterats under kap4 Genomförande bör denna kostnad ej vara märkbar.

För att få en bild av hur stor denna kostnad blir med dagens telefontaxor mätt, kan timbegränsningen som företaget Helge Nyberg AB använde sig av granskas. Timbegränsningen var här satt mellan klockan 07-18 vardagar, vilket ger parametrarna D=20, H1=10h, H2=1h. Den svenska Internetleverantören Telia kontaktades för dagsaktuella prislistor 98-04-14, varvid månadskostnaden K=150kr och samtalsavgifterna R1=0,2kr/min och R2=0,1kr/min kunde fastställas för en modemförbindelse. Förutsatt att systemet är anslutet till Internet all tillgänglig tid blir den maximala månadskostnaden 2670kr som beräknas enligt:

$$150\text{kr} + 20 \cdot (10 \cdot 0,2 + 1 \cdot 0,1) \cdot 60 = 2670\text{kr} \text{ inklusive mervärdesskatt}$$

Skulle en ISDN-adapter användas istället skulle parametrarna bli $H1=10\text{h}$, $H2=1\text{h}$, $K=230\text{kr}$, $R1=0,16/\text{min}$ och $R2=0,08\text{kr}/\text{min}$, och kostnaden uppgår då istället till 2246kr per månad:

$$230\text{kr} + 20 \cdot (10 \cdot 0,16 + 1 \cdot 0,08) \cdot 60 = 2246\text{kr} \text{ inklusive mervärdesskatt}$$

Jag vill till sist påpeka ytterligare en gång om att detta rör sig om maximal månadskostnad. Används Internet endast hälften av all arbetstid, halveras även kostnaden (exklusive anslutningsavgiften).

5.1.3 Enkät

Efter det att den åtta veckor långa testfasen var avslutad skickades således enkäten ut till de personer som haft möjlighet att använda systemet. Resultatet kategoriserades i de tre huvudgrupperna som nämnts tidigare; intervjudeltagarnas erfarenheter av Internetanslutningen (fråga 1-3, 8, 10), programvara (fråga 4,5), och systemproblem (fråga 6,7,9). Erfarenheterna av programvaran som används och eventuella problem som uppkommer är beroende av företagets specifika datormiljö och därför kommer dessa kategorier att redovisas individuellt för respektive företag. Antalet erhållna svar på enkäten var åtta stycken, vilka var fördelade med tre svar från företaget Davita Konsult, två svar från företaget Torslanda Stål och Mekaniska AB samt tre svar från företaget Helge Nyberg AB.

Intervjudeltagarnas erfarenheter av Internetanslutningen

Av de åtta som svarade hade fem personer tillgång till Internet sedan tidigare. Trots detta svarade totalt sju personer att de upplevt en ökad Internetanvändning när systemet tagits i drift. På frågan vilka tänkbara orsaker som kan ligga bakom denna ökning av Internetanvändandet svarade tre personer att det berodde på upplevelsen att vara "fast uppkopplad" samt att tillgängligheten innebar att de nu fritt kunde följa upp idéer de fått genom att koppla upp sig direkt utan att behöva vänta. En person tyckte att det var snabbheten och enkelheten med vilken man kunde ansluta sig till Internet som ledde till ökningen, medan en annan person ansåg att det berodde på möjligheten att själv kunna arbeta med flera datorer parallellt. Känslan av att ha en egen anslutning kopplad till datorn angavs av en anställd. En person angav ej någon orsak till ökningen.

Vid frågan vad de ansåg vara tillfredsställande med Internetanslutningen ansåg tre personer att det främst var tillgängligheten och upplevelsen att vara

”fast uppkopplad”. Resterande svar var relativt spridda där två personer mest uppskattade den snabbhet vilken man kunde ansluta sig till Internet med samt de säkerhetsaspekter som brandväggen tillsammans med den automatiska nedkopplingen medförde. En person ansåg att upplevelsen av en ”egen anslutning” var det som var mest tillfredsställande, medan en annan ansåg att kostnaden för abonnemang och brevlådor för epost vägde mest. Värt att notera är att samtliga intervjuade personer var tillfredsställda med anslutningen. Den siste som svarade angav ej någon specifik orsak men uppgav dock att väl installerat fungerade ”allting” bra.

Samtliga intervjuade skulle kunna tänka sig att fortsätta använda ett system av den här typen. Tre personer svarade att deras företag redan beställt ett ISDN-abonnemang för fortsatt användning av systemet. På frågan varför de skulle kunna tänka sig vidare användning gav samtliga personer ekonomiska orsaker till nyttjandet. Utöver de ekonomiska aspekterna ansåg tre personer att de upplevde att det hade fungerat bra att ansluta samtliga datorer till Internet och två andra tyckte det var bra med möjligheten att spara både tid och pengar genom att flera kunde arbeta samtidigt mot Internet över en via brandväggen säker förbindelse.

Davita Konsult

Davita Konsult använder anslutningen både för distansarbete och distansutbildning, tillsammans med Internetspecifika program såsom diskussionsareor, webläsare, epost och spel (efter arbetstid). Ingen på företaget kunde i enkäten rapportera om något program som hade fungerat innan men ej fungerade då systemet togs i drift, och det fanns ej heller någon lokal programvara som hade slutat fungera.

Ingen kunde heller rapportera om några problem som uppkommit under testperioden, och den enda nackdelen samtliga anställda redovisade var att hastigheten över Internetanslutningen snabbt minskade då två personer parallellt överförde stora mängder data.

Helge Nyberg AB

Helge Nyberg AB använde sin anslutning till Internet för både ekonomiärenden, epost och möjligheten till att hämta produktinformation över webläsare. Två personer rapporterade att det ibland uppkom problem med att ansluta till vissa websidor, där det till och med var vissa sidor som ej gick att komma åt överhuvudtaget då systemet tagits i drift. En anställd hade synpunkter om att längre hemtagningar av filer hade en tendens att avbrytas mitt i överföringen, tillsammans med problemet att hemtagning av epost var

tvunget att utföras två gånger då det första försöket alltid misslyckades. Det ekonomisystem som används över det lokala nätverket hade ej påverkats av Linuxserverns intåg, och samtliga övriga program hade även då projektet startats fortsatt fungera.

Övriga problem som uppkommit var relaterade till Internetsystemet som sådant. Två användare påpekade att det vid upprepade tillfällen föll sig så att Linuxservern ej ville ansluta sig till Internet även om den teoretiskt sett skulle göra det. Datorn fick då startas om genom att man temporärt bröt strömtillförseln varefter systemet fungerade tillfredsställande igen. En annan anställd rapporterade om problemet då en ny dator skulle anslutas till Linuxservern, men den ej var registrerad hos serverns datorlista. Kontakt togs med mig och på tidigare beskrivet sätt anslöt jag mig över Internet mot servern för att lägga till datorns IP-adress till filen */etc/hosts* (se bilaga B för en redovisning av denna fil). Alla problem som uppkom gick emellertid enligt samtliga som svarade på enkäten mycket enkelt att åtgärda. Ett problem som dock var svårare att åtgärda, vilket en anställd påpekade, var att det tog lång tid för systemet att ansluta sig första gången till Internet då ett modem alltid kräver minst 30 sekunder för att fastställa en uppkoppling.

Torslanda Stål och Mekaniska AB

Torslanda Stål och Mekaniska AB använder Internet för att sköta aktiehandel, bankärenden, epost samt inhämtning av nyheter via webläsare. Ingen av de intervjuade hade stött på några mjukvaruproblem, vare sig vad gäller Internetprogram eller övriga lokala applikationer.

Liksom personalen på Davita Konsult hade ingen anställd rapporterat om något problem som uppkommit med anknytning till Internetförbindelsen, och de intervjuade kunde ej heller finna någon nackdel med systemet.

5.2 Resultatanalys

För att kunna värdera testdeltagarnas perspektiv som redogjorts i enkätsvaren, kommer en analys att utföras på de tre valda kategorierna personliga erfarenheter, programvara och systemproblem. De två sista kategorierna kommer här ej att fördelas under respektive företag. En jämförande analys kommer istället att utföras mellan företagen med hänsyn tagen till datorantal och nätverksbelastning.

5.2.1 Intervjudeltagarnas erfarenheter

Att de personer som ej haft tillgång till Internet före projektstarten ökat sitt Internetanvändande när systemet togs i drift var kanske ingen överraskning, men att fyra av dem som redan tidigare hade tillgång till Internet via sin persondator ökade sitt användande var märkligt. Eftersom anslutningstiden för att koppla upp sig mot Internet fortfarande var ungefär 30 sekunder vid bruk av modem så fanns det i sig inga större tidsvinster att uppnå. Ändå svarade personer som redan tidigare haft tillgång till Internet att de nu på grund av snabbheten och enkelheten hade möjlighet att ansluta sig oftare. Några ansåg också att det berodde på upplevelsen att vara fast uppkopplad. Några av de som uttalade sig om väntetider hade troligtvis tidigare varit tvungna att fysiskt vänta på sin tur vid en gemensam arbetsstation ansluten till Internet, och där borde tidsvinsterna varit mycket stora. Hur många av dem som räknade detta alternativ som en tidigare möjlighet till Internetåtkomst är oklart.

En jämförelse kan göras med de automatiska dörrar man träffar på i sin vardagliga livsmedelsbutik. När kunden väl handlat sina matvaror och är på utgående öppnar sig vanligtvis dessa dörrar automatiskt via en fotocell, och fotgängaren är allt som oftast ej medveten om att det från början ens fanns en dörr i vägen. Kunden vill ta sig ut från butiken på enklast möjliga sätt. Om där istället hade stått en vanlig dörr, hade kunden kanske tillfälligt fått ställa ner kassarna, öppna dörren, för att sedan gå ut. Just denna faktor att ej behöva tänka på att det överhuvudtaget finns en dörr som blockerar utfarten skulle kunna betecknas som transparent port mellan butiken och dess omgivning, likaväl som Linuxsystemet erbjuder en transparent brygga mot Internet. De automatiska dörrarna i butiken leder även, liksom fleranvändarmöjligheten hos Linuxservern, till att olika kösystem effektivt förhindras.

5.2.2 Programvara och systemproblem

I de två företagen med de minsta datorparkerna existerade inte ett enda problem med någon programvara. Det uppkom inga märkbara problem, och systemet anslöt och kopplade ner Internetförbindelsen precis som förväntat. Däremot stötte företaget Helge Nyberg AB på en mängd problem, där vissa Internetsidor ej gick att hämta. Systemet vägrade ansluta sig eller kopplade ner sig för tidigt, och det var ibland nödvändigt att upprepa vissa operationer, som att läsa epost, då hemtagningen alltid misslyckades vid första försöket.

Då Helge Nyberg AB hade sjutton datorer anslutna till nätverket som dagligen arbetade via detta med det lokala ekonomisystemet uppstod en stor mängd kontinuerlig nätverkstrafik. När testperioden var slut hade det redan

kommit två nya revisioner av programvaran DialD, vilka enligt upphovsmakaren skall korrigera sådana fel som gör att systemet ej ansluter sig då det skall göra det, eller att det kopplar ner förbindelsen för tidigt. Om den nya revisionen av programmet hade fungerat bättre i företags miljö är omöjligt att förutsäga, det är dock klart att den stora mängd nätverkstrafik som uppstod ledde till felaktigt beteende hos Linuxservern. Vid problemen som personalen på Helge Nyberg AB redovisade, där eposten ej ville hämtas första gången, kan en möjligt orsak ha varit en inställning i mailprogrammet som rapporterar fel då svar från brevlådan via Internet ej erhållits inom 30 sekunder, vilket är den tid modemmet tar på sig för att ansluta. De oönskade nedkopplingar som uppstod ledde även till att vissa dynamiska websidor fungerar dåligt, då servern som lagrar websidorna identifierar användaren via dess TCP-session som bryts då systemet kopplar ner. Problemet med att vissa websidor ej gick att hämta alls var unikt för företaget Helge Nyberg AB, och orsaken till detta är okänd.

6 Slutsatser

För att sammanfatta det resultat som framkommit kommer här återigen att redovisas de ursprungliga frågeformuleringarna, tillsammans med passande resultatdel. Då även kapitel 2 i rapporten är en del av resultatet från undersökningen kommer frågor som rör tekniska förklaringar, möjligheter och begränsningar att hämtas härifrån.

Hur väl fungerade systemet i syfte att hjälpa en organisations medarbetare att ansluta sig till Internet, med hänsyn till överföringshastighet, transparens och användarvänlighet?

Samtliga intervjuade personer ansåg att de var tillfredsställda med hur systemet fungerade, och alla kunde även tänka sig ett fortsatt användande. Fördelar som nämndes var bland annat känslan av en ”fast uppkoppling” vilket ledde till att användarna nu fritt kunde följa upp idéer utan att behöva vänta, samt att brandväggen i sig innebar en trygghet tillsammans med vetskapen om att systemet automatiskt stängde ner förbindelsen när det ej längre existerade någon trafik. Överföringshastigheten var begränsad till modemets konfiguration, och ett av företagen hade redan före testets slut beställt hem ett ISDN-abonnemang för vidare systemutnyttjande.

Leder den eventuella transparens som uppstår mot Internet med automatiska uppkopplingar till ett ökat Internetanvändande hos de som tidigare var tvungna att ansluta sig manuellt?

Ja, av de fem personer som tidigare haft tillgång till Internet angav fyra att de märkt ett ökat Internetanvändande.

Vad finns det för bakomliggande teknik och program som understödjer denna implementation, och finns det funktioner som förhindrar uppkoppling baserat på tid och datum?

Den bakomliggande tekniken som valdes är det fria operativsystemet Linux och programvaran DialD. För att anpassa och konfigurera DialD användes även verktyget DialD-config. DialD har utöver funktioner för att begränsa uppkoppling baserad på tid och datum även möjlighet att begränsa anslutning baserat på veckodagar. Det innebär att det krävs få anpassningar för att definiera vilka timmar under respektive arbetsdag Internet skall vara tillgängligt för de anställda.

Tillåter system av den här typen möjligheten att vid behov skala upp anslutningen från modem till ISDN?

Ja, då Linux tillåter användaren att bestämma modeminställningar för att ansluta ISDN-adaptrar via datorns seriella port (se bilaga B). Det finns även drivrutiner att installera för interna ISDN-kort vilket tillåter datorn att ansluta till Internet med 128kbit. Tyvärr innebär dessa drivrutiner idag att funktionen som ringer upp till Internet vid behov ej längre fungerar (se även här bilaga B).

Finns det någon begränsning i vilka program som kan nyttjas hos företagets datorer med hjälp av denna lösning?

Nej, systemet har testats med ett flertal applikationer, bland annat för bankaffärer, distansundervisning, distansarbete, epost, dataspel och webläsare.

Hur stor kan den månatliga anslutningskostnaden till Internet förväntas bli?

Kostnaden varierar beroende på hur mycket Internet används. Den totala månadskostnaden då ett företag är ansluten konstant mot Internet mellan 07.00-18.00 med ett abonnemang av typen Telia Internet 020 hamnar på 2670kr inkl. moms för modem, och 2246kr inkl. moms för ISDN. Används Internet endast hälften av all tillgänglig arbetstid halveras kostnaden (exkl. fast månadsavgift för abonnemanget).

6.1 Generell metodutvärdering

Den explorativa ansatsen som användes vid genomsökning av Internet efter tänkbara lösningar fungerade mycket bra. Även om denna undersökning tog mycket tid fann jag till slut både existerande system och tänkbara problem tydligt förklarade. Den beskrivande undersökningen som sedan påbörjades blev mycket omfattande, främst på grund av det breda ämnesområde som utsetts. Då olika författare har olika uppfattningar om beteckningar och standarder på grund av de ständigt föränderliga RFC's som existerar, innebar det

att det ej räckte med att inhämta endast en författares förklaring på ett beskrivet fenomen för att fastställa dess relevans.

Den utvärderande undersökningen som utfördes med hjälp av enkät föll väl ut, men då öppna frågor valts upplever jag idag att svaren hade kunnat preciseras ytterligare med hjälp av intervju eller observation. Ett exempel är frågan som löd ”Hade du tillgång till Internet före det att projektet startades”. En tänkbar tolkning av denna fråga är att personen i fråga hade *möjligheten* att tidigare ansluta sig till Internet, till exempel via en företagsgemensam dator, även om innebörden i frågan var tänkt som ”Var din personliga arbetsstation tidigare ansluten till Internet”. Detta hade kunnat förklaras vid en personlig intervju. Då resorna till och från företagen redan ätit upp det mesta av mitt sparade kapital fanns det tyvärr ej möjlighet att genomföra detta, och området är därför fortfarande intressant för vidare forskningsarbeten.

6.2 Sammanfattande utvärdering av arbetet

Samtliga involverade i projektet nämnde kostnaden som en viktig aspekt vid användandet av systemet. Det är lätt att bortse från att systemet i sig måste installeras och konfigureras före användning, vilket måste utföras av en kvalificerad person. Det har därför idag vuxit fram ett flertal företag som specialiserat sig på just installation av denna typ av system, bland annat företaget Meme Factory (<http://www.meme.com/>) som skapat verktyget DialD-config, och företaget Virtual World Network (<http://www.virtualworld.net/>) som säljer systemet Net2Net.

Denna rapport redovisar dock samtliga nödvändiga steg som krävs för en fungerande installation, vilket gör att det nu är möjligt även för personer med begränsad UNIX-vana att installera och anpassa den fria programvaran, vilket även begränsar anskaffningskostnaderna av systemet. Förhoppningsvis leder detta till att fler företag till låg kostnad kommer att ha möjligheten att ansluta sig till Internet.

6.3 Egna reflexioner

Eftersom problem uppstod under testperioden vid en komplex nätverksmiljö blir det ändå relevant att fråga sig om det verkligen är värt besväret som det innebär att nyttja ett system av den här typen mot att använda en permanent Internetförbindelse mot företaget. För att kunna sätta kostnaden i perspektiv mot den eventuella vinst som görs vid ökad tillgänglighet skulle ytterligare en studie behöva genomföras som lyfter fram dessa aspekter. För små företag med ett fåtal datorer inkopplade i nätverket uppstod inte ett enda pro-

blem, varvid den diffusa gräns som uppstår mellan vad som kännetecknas av en enkel och en komplex nätverksmiljö är svår att specificera.

Då denna teknik för att ansluta företaget till Internet trots allt är väldigt ny (DialD och DialD-config) är det rimligt att stöta på problem vid större lokala nätverk som Helge Nyberg AB använder sig av. Det kommer ständigt nya uppdateringar till programmen och då utvecklarna ej tar något betalt för verktygen har man som användare ej heller möjligheten att ställa krav.

Om företag överväger att använda informationen som finns redovisad i denna rapport för att själva sälja färdigkonfigurerade system vill jag bara än en gång påpeka att projektet ej hade varit möjligt att genomföra utan dessahängivna programmerare som utan tanke på ersättning fortsätter att förbättra sina datorprogram som användes i studien. Självklart är det rimligt att ta ut en skälig ersättning för att installera programvaran till kund, men då tiden detta tar i anspråk ej överstiger en timmas arbetstid finns det ej heller skäl att ta ut orimliga kostnader. Använd gärna fritt kunskapen i detta dokument, men gör det på ett sätt som kommer så många människor till nytta som möjligt!

6.4 Idéer för fortsatt forskning

Då denna studie visar hur ett system konstrueras som tillåter organisationer att kostnadseffektivt ansluta sig till Internet tillsammans med effekterna av detta, skulle det vara intressant att granska de kommunikativa aspekterna då Internetanvändandet ökat på en arbetsplats. Upplever personalen att deras arbetsmiljö förbättrats, produceras bättre resultat samt har arbetstakten ökat? En sådan studie skulle ej behöva befatta sig med de tunga tekniska aspekterna av systemet utan skulle kunna istället helt kunna följa mina anvisningar för att skapa ett flertal slutna system för evaluering.

För att bygga vidare på de tekniska aspekterna skulle det vara intressant med ett fullständigt installationsprogram och en specialgjord CD-skiva som automatiskt installerar Linux och DialD efter användarstyrda önskemål. Detta skulle sedan kunna säljas som ett färdigt "Internetanslutningspaket" innehållandes floppydisk och skiva för en rimlig summa. Då Linux är så pass öppet i sin struktur är det fullt möjligt att anpassa installationsprogrammet till att klara detta, och det finns idag färdiga Internetservers och brandväggar som är byggda på precis detta sätt.

Referenslitteratur

Andersen, H., ed. (1994). "*Vetenskapsteori och metodlära*",
Studentlitteratur

Andréasson, T., Skansholm, J. (1993). "*UNIX och X från början*",
Studentlitteratur

Bradner, S., Mankin, A. (1993). "*IP: Next Generation (IPng) White Paper Solicitation*", RFC 1550

Brooks, F. P. (1995). "*The Mythical Man-Month*",
Addison-Wesley Publishing Company

Carlson, J. (1998). "*PPP Design And Debugging*",
Addison Wesley Longman

Chapman, D. B., Zwicky, E. D. (1995). "*Building Internet Firewalls*",
O'Reilly & Associates

Daniels, T. D., Spiker, B. K., Papa, M. J. (1996). "*Perspectives on organizational communication*", Brown & Benchmark publishers

Dixon, T. (1993). "*Comparison of Proposals for Next Version of IP*",
RFC 1454

Egevang, K., Francis, P. (1994). "*The IP Network Address Translator (NAT)*", RFC 1631

Forester, T., Morrison, P. (1994). "*Computer Ethics*",
Massachusetts Institute of Technology (MIT)

- Graham, B. (1997). *"TCP/IP Addressing"*, Academic Press
- Huitema, C. (1996). *"IPv6 – The New Internet Protocol"*, Prentice Hall PTR
- Lundahl, U., Skärvad, PH. (1982). *"Utredningsmetodik för samhällsvetare och ekonomer"*, Studentlitteratur
- Lundeberg, M., Sundgren, B. (1996). *"Att föra verksamheten framåt"*, Studentlitteratur
- Mynatt, B. T. (1990). *"Software Engineering with Student Project Guidance"*, Prentice Hall
- Nurminen, M. L. (1988). *"People or Computers"*, Studentlitteratur
- Pinc, K. (1998). *"DialD-config"*,
<ftp://ftp.meme.com/pub/software/diald-config>
- Postel, J. B. (1980). *"User Datagram Protocol"*, RFC 768
- Postel, J. B. (1981a). *"Internet Protocol"*, RFC 791
- Postel, J. B. (1981b). *"Internet Control Message Protocol"*, RFC 792
- Postel, J. B. (1981c). *"Transmission Control Protocol"*, RFC 793
- Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. (1994). *"Address Allocation for Private Internets"*, RFC 1597
- Ringo, T., ed. (1994). *"Inside TCP/IP"*, New Riders Publishing
- Salus, P. H. (1994). *"A Quarter Century of UNIX"*, Addison-Wesley Publishing Company
- Sanneblad, J. (1997). *"Användarmedverkan vid systemutveckling"*, Högskolan i Borås

Schenk, E. (1998). "*The Diald home page*",
<http://www.loonie.net/~eschenk/diald.html>

Shiller, L. (1990). "*Software Excellence*",
Prentice Hall

Simpson, W.A. (1993). "*The Point-to-Point Protocol (PPP)*",
RFC 1548

Stevens, W. R. (1994). "*TCP/IP illustrated vol. 1 – The Protocols*",
Addison-Wesley Publishing Company

Thies, A. (1998). "*Linux Time Line*",
http://www.acsu.buffalo.edu/~thies/Linux/Time_Line.html

Vos, J., Konijnenberg, W. (1996). "*Linux firewall facilities for kernel-level packet screening*", <http://www.xos.nl/linux/ipfwadm/paper/>

Warner, T. (1996). "*Communication Skills for Information Systems*",
Pitman publishing

Samtliga referenser mot Internet är kontrollerade 1998-04-14

Bilaga A – Enkät

Hej!

Som Du kanske vet så har det på Din arbetsplats skett ett studentprojekt med koppling till Högskolan i Borås. Målet med projektet har varit att hjälpa små och medelstora företag att ansluta sina datorer till Internet, och Ditt företag har varit en av deltagarna.

Då systemet som tillåter Internetåtkomst idag fortfarande befinner sig i utvecklingsfas är det mycket viktigt med just Dina synpunkter för att Din Internetåtkomst skall kunna förbättras och anpassas efter Dina individuella behov. Jag har därför sammanställt nedanstående enkät med 10 frågor som hjälper både Ditt företag och andra organisationer genom att påverka strukturen av det färdiga systemet. Jag skulle uppskatta om Du tog dig tid att svara på samtliga frågor, och vill samtidigt lyfta fram hur viktigt det är med alla synpunkter, även de av icke-teknisk karaktär.

Denna enkät bör helst fyllas i av samtliga på arbetsplatsen som fått tillgång till anslutningen mot Internet. Svaren kommer att vara konfidentiella, och endast sammanställningar och generella tolkningar av resultaten kommer att redovisas i den slutliga rapporten.

Tack på förhand,

Johan Sanneblad
Högskolan i Borås

Namn: _____

Företag: _____

Befattning: _____

Använder Internet för att: _____

1. Hade Du tillgång till Internet före det att projektet startade?
2. Upplever Du att Internetanvändandet har ökat efter projektets start?
3. Om du svarade JA på både fråga 1 och 2, vad tror Du denna ökning i Internetutnyttjande beror på?
4. Var det någon Internetapplikation som ej fungerade med det färdiga systemet?
5. Var det någon programvara som slutade fungera då systemet togs i drift?
6. Uppstod det några problem under testperioden?
7. Om det uppstod problem under testperioden, ungefär hur lång tid tog det att lösa dem, och var Du tvungen att begära hjälp från Johan Sanneblad för att komma tillrätta med problemen?
8. Vad upplevde Du fungerade tillfredsställande med Internetanslutningen?
9. Vilka nackdelar upplevde Du med Internetanslutningen?
10. Skulle Du idag kunna tänka Dig att fortsätta använda ett system av den här typen för att ansluta Ditt företag till Internet? Varför?