Datornätverk

Patric Fors

2004-05-29

»If you want to make an apple pie from scratch, you must first create the universe.«
Carl Sagan

Sammanfattning

Dokumentet ska i sin relativa korthet förklara hur datorer fungerar i nätverk. Fokus kommer att vara på själva nätverket och inte hur ett visst operativsystem konfigureras för att kopplas in på ett nätverk även om det kommer att nämnas en del i texten.

Ethernet är den vanligaste typen utav nätverk så texten kommer att lägga fokus där. Ethernet är på det så kallade »länkskiktet« som beskriver hur kommunikationen mellan nätverkskort sker. Fler skikt kommer att tas upp då de är en viktig del i hur datornätverk fungerar. De lager som kommer att beskrivas är ifrån tillämpnings- till länkskikt.

Även de komponenter som tillhör ett nätverk kommer att beröras, så som nätverkskort, hub, switch, router, brandvägg, binära tal, storlek, storheter, lite nätverktyg och en lagom skvätt säkerhet.

Innehåll

1 Grunder

1.1 Vad är ett nätverk?

Ett nätverk är flera datorer eller annan utrustning sammankopplade via ett gemensamt sätt att kommunicera. Det kan vara Internet eller till och med sitt lokala företagsnät med två datorer och en skrivare sammankopplade.

Man brukar sätta ett namn på den typ och storlek utav nätverk man pratar om, det kan vara namn så som »Internet«, »WAN«, »LAN« osv. Här kommer en förklaring på några utav dem.

Internet Datorer eller annan utrustning sammankopplade till *ett* gemensamt globalt nätverk.

WAN »Wide Area Network«, vanligen företag och institutioner uppkopplade till ett eget nätverk som går över ett stort område t ex mellan städer eller länder. Det vill säga mellan kontoren.

LAN »Local Area Network«, nätverket hemma och på kontoret räknas som ett LAN.

WLAN »Wireless Local Area Network«, trådlöst och vanligtvis radiobaserat LAN.

PAN »Personal Area Network«, ett betydligt mindre nätverk än de andra. Den utrustning man kopplar till ett PAN är fysiskt mycket nära en som kanske hörs på namnet. Det kan vara en blåtandsbaserad mobiltelefon eller kanske sin portabla handdator kopplad via USB till den stationära datorn. Med andra ord så är räckvidden högst ett par meter.

Ovanstående kan givetvis vara kopplade till varann, dvs ett WAN eller LAN till Internet. Men i tal och skrift så behöver man en benämning på just det nätverk man tar upp.

1.2 Vad behövs för att koppla in en dator till ett nätverk?

Det beror givetvis på vilken typ utav nätverk man vill koppla in sig i. Egen inkoppling till Internet utan internetoperatör kräver speciell utrustning, samt att det går utanför denna text, så det kommer vi inte att ta upp.

Köper man »färdig« internetkoppling via ett abbonemang till en internetleverantör så får man vanligtvis idag ett jack i väggen eller någon form utav xDSL-modem. Man kopplar då in sig i jacket eller modemet för access till Internet.

Ett WAN kräver nästan lika mycket som ett Internet om man ska sätta upp ett själv, men vanligast är det bara att koppla in sig i ett färdigt nätverk. Då behövs lika mycket utrustning som för ett LAN, dvs nätverkskort (inbyggt i de flesta datorer numera) samt kabel att koppla in sig med. Kabeln kopplas in i en hubb eller switch, mer om det i nästa del.

WLAN kräver lite annan typ utav nätverkskort, ett radiobaserat, samt att hubben eller switchen bytts ut mot en accesspunkt som har motsvarande funktion.

1.3 Vilka delar består ett nätverk utav?

Nätverkskort, kabel, hubb, switch samt accesspunkt har vi nämt ovan men vad har de för funktion samt vad mer behövs för att få ett nätverk att fungera.

Nätverkskort Används för att koppla in datorn till ett nätverk. Modernare nätverkskort har ofta en lysdiod för att tala om nätverket är inkopplat samt en annan lysdiod som blinkar för att visa att trafiken flyter.

Kabel Vanligtvis sk. »TP-kabel« där »TP« står för »Twisted Pair« och kontakterna heter »RJ-45«. Både kabel och kontakter är besläktade med vanlig telefonkabel, det syns väl. TP-kablar finns i två sorter, en för inkoppling utav dator till hubb/switch samt en som kallas »korsad« och används för att koppla samman två datorer. De kan vara svåra att skilja åt men ibland så är de korsade TP-kablarna markerade med en annan färg på kabel eller kontakter. Om inte markering finns så får man plocka fram förstoringsglaset och titta närmare på färgen på ledarna, de syns igenom kontakterna. Håll upp båda kontakterna på samma sätt. Är det samma ordning på färgerna så är kabeln »rad« annars är den »korsad«. Det finns även optisk kabel där signalerna i kabeln består utav ljus istället för elektriska impulser. De klarar betydligt högre hastigheter i kabeln, men kräver då dyrare och mer speciell utrustning för att kunna användas samt att fiberkabeln är betydligt mer känsligt för böjskador.

Hubb Används för att koppla samman flera datorer och annan utrustning. Vanlig rak TP-kabel används för inkoppling. En hubb har inte något minne över vem som är inkopplad i vilken port, så all trafik skickas till alla portar. Detta gör att den inte blir så effektiv då flera datorer skickar samtidigt trafik in i samma hubb. Något som kallas paketkollisioner (mer om paket i kapitel 2) sker då och de paket som krockade måste sändas igen. Om bara två utav portarna används så blir det minimal mängd paketkollisioner, men med varje extra port som används så ökar risken samt att hastigheten minskar. Nyare hubbar brukar ha en speciell port som kallas »uplink« eller något liknande namn. I den kan man koppla in en rak eller korsad TP-kabel. Om inte hubben har s.k. »auto crossing« så måste man ställa om en knapp för att inkopplingen till »uplink« porten ska kännas vid. Man kan likna en hubb med en förgreningsdosa.

Switch Samma funktion som en hubb men är betydligt smartare då den lär sig vem som inkopplat i varje port. Det innebär att trafik mellan t ex två datorer i samma switch endast berör de två portar där de är inkopplade i. Hastigheten blir då betydligt snabbare samt att paketkollisionerna blir till ett minimum. Även dessa har en uplink port likt hubbar. Man bör även

tänka på att switchar även har en intern begränsning på hur mycket trafik som kan flöda mellan alla portar samtidigt.

Accesspunkt Används för trådlösa nätverk där trafiken skickas med radiovågor. Funktionen är likt en hubb, dvs inkoppling utav flera datorer eller annan utrustning till ett nätverk. De brukar även inkludera andra funktioner så som brandvägg (kapitel 5.2.2), DHCP (kapitel 4.4). De frekvenser som används är 2,4 GHz, de mindre vanliga på 5,2 GHz och 5,5 GHz. Hastigheterna i trådlösa nätverk är inte lika höga som de som går i kabel.

Router En routers funktion är att skicka de paket den får till rätt mottagare på ett annat nätverk, med andra ord så kopplar den ihop nät. Den skapar en intern tabell med alla de olika vägar som leder till andra nätverk, samt att den har koll på vilka som är kortare/snabbare och vilka som fungerar. Detta gör den med hjälp utav andra routrar, de utbyter information med varann om hur deras nätverk ser ut. En router kan vara speciell hårdvara men även en vanlig hemdator kan göra samma sak om den har fler nätverkskort och programvara för det. Se mer om routrar i (kapitel 4.6)

TCP/IP Denna del är döpt efter två delar som ingår, »TCP« (kapitel 2) samt »IP«(kapitel 2). TCP/IP är en del utav alla vanliga operativsystem samt den mjukvara som styr ovanstående hårdvara. Man brukar kalla denna delen för »IP-stacken«, och är den del som skapar de flesta delarna i det nätverkspaket som skickas i ett nätverk.

2 TCP/IP

Ett protokoll beskriver hur något skall göras, och TCP/IP är inget undantag. TCP/IP är en hierarkisk protokollfamilj där varje skikt använder sig utav de undre som byggklossar, lite som de ryska dockorna där en mindre finns inuti den andra. Men i detta fallet kallas delarna för »paket« där »tillämpningsskiktet« (se nedan) är inslaget i »transportskiktet« som i sin tur är inslaget i »nätverksskiktet« osv.

Man har delat in det i skikt för att lättare kunna hantera komplexiteten. Varje skikt har sina egna protokoll för hur kommunikationen ska ske.

TCP/IP baserar sina skikt löst på en teoretisk modell som kallas för »OSI-referensmodell« (»Open System Interconnection Reference Model«). Den består utav sju stycken skikt medans TCP/IP endast består utav fem då man slagit ihop två utav dem. Vi börjar beskriva dem inifrån och går utåt..

Tillämpningsskiktet Detta är det mest synliga utav skikten i datorn fast det är mest »inbakat« bland de fem. Anledningen till att det är synligt är att dessa de protokoll som man som användare mest kommer i kontakt med. Exempel på protokoll är HTTP (3.3) för surfning på webben och SMTP (3.1) när man skickar e-post.

Transportskiktet Här finns två typer utav protokoll, »UDP« (»User Datagram Protocol«) samt »TCP« (»Transmission Control Protocol«). De har lite olika egenskaper och vilken man väljer när man skapar sitt program beror helt på vilken typ av kommunikation man söker. TCP verifierar att alla paket kommer fram till mottagaren samt gör omsändningar om så behövs. Detta sker med hjälp utav kontrollnummer som mottagaren kvitterar. UDP har inte den kontrollen utan skickar iväg paket på vinst och förlust. Man kan då undra varför något som UDP används när det finns risk att man tappar paket på vägen. UDP används för spel, internetbaserad telefoni och andra applikationer där det inte är så viktigt om man förlorar lite information eller där information som blivit »gammal« inte längre skulle vara värd att vänta på för omsändning. UDP är betydligt snabbare då den »bara slänger iväg« paket jämfört med TCP som hela tiden måste ha grym kontroll på vad som kommit fram och vad som inte klarat sig. Även något som kallas »portar« tillkommer i detta skikt, det är ett nummer som adresserar en viss tjänst. Många tjänster har ett bestämt portnummer så som »80« för HTTP (kapitel 3.3). Det finns 65536 st olika portar och de används både av sändare och mottagare utav ett TCP eller UDP paket. Avsändarporten brukar vara ett mer eller mindre slumpmässigt värde högre än 1024 medan mottagarporten är en fast port som vanligtvis ligger under 1024 då de vanligaste tjänsterna har sina portar där.

Nätverksskiktet I detta skikt så kommer själva »IP-paketet« som även den kanske känns bekant på grund av den så välkända IP-adressen. Den används för identifiering för sändare och mottagare i ett paket. En IP-adress består utav fyra stycken så kallade oktetter. En oktett är ett binärt (kapitel 4.1) tal med 8 bitar och ett värde mellan 0 och 255. Varje oktett i en IP-adress skiljs åt med en punkt, t ex »192.168.42.1«. Routrar (kapitel 4.6) jobbar på detta skikt.

Länkskiktet Här är det »Ethernet« protokollet som bestämmer. Ytterst sällan man behöver påverka eller undersöka något i detta skikt. Detta skikt står för kontakten mellan de nätverkskort som är direkt sammankopplade med varann i en hubb eller switch. Alla nätverkskort har ett unikt idnummer, en så kallad MAC-adress (»Media Access Control«) och den används för identifiering i Ethernet. Switchar och hubbar (kapitel 1.3) jobbar på detta skikt.

Fysiskaskiktet Detta är det skikt man kan »ta på« då det beskriver kontakter, kablar, signalstyrka, modulation och våglängder för signalen osv. Det finns även en så kallad RFC (kapitel **??**) hur man använder en brevduva som fysiskt skikt. RFC 1149 beskriver detta.

Man kan säga att de olika skikten paketeras in i ett större paket utav den del i kedjan där paketet befinner i. Som ett exempel kan vi ta webbläsaren som stoppar in paket av typen »HTTP« i tillämpningsskiktet, IP-stacken skapar

»TCP-paketet« med rätt portnummer i transportskiktet, samt stoppar in det i ett »IP-paket« med avsändar- och mottagar-IP-adress i nätverksskiktet. Nätverkskortet tar sedan hand om det och lägger alltihopa i ett »Ethernet« paket med en »MAC« adress i länkskiktet.

Under paketets väg så öppnas det fysiska samt länkskiktet för varje steg på vägen, samt att det packas in i nya med just det MAC-adress och typ utav fysiskt skikt. Ett paket kan t. ex. färdas igenom kopparkabel, vidare i optisk länk och därefter via radio och sen tillslut in i kopparkabel.

Det omvända sker på mottagarsidan, då öppnas paketen i tur och ordning och tillslut får, som i exemplet ovan, webbservern innehållet i »HTTP-paketet«.

3 Tillämpningsprotokoll

De flesta »servrar« använder tillämpningskiktet. En server är en programvara som bistår med en tjänst, det kan t ex vara webbsidor eller e-post. En »klient« är den dator eller annan utrustning som kopplar upp sig mot en server.

Alla protokoll nedan använder »TCP« paket.

3.1 SMTP

Alla har vi nog skickat iväg ett e-brev eller två, och då har vi omedvetet använt oss utav en del i »SMTP-protokollets« repertoar. SMTP är en förkortning för »Simple Mail Transfer Protocol«, och är det protokoll som används för att transportera e-post. Transporterna sker mellan din e-postklient och SMTP-servern själv samt mellan SMTP-servrar då de skickar vidare e-posten till mottagaren.

De maskiner som hanterar »SMTP« är vanliga datorer med programvara som förstår detta protokoll. När man ställer in sin e-postklient så skriver man in vanligtvis ett namn på den dator som ska få den e-post man skickar iväg, t ex »smtp.example.com«. Man brukar kalla tjänsten för »mailserver« eller »mejlrelä«.

Den port som en SMTP server jobbar på är vanligtvis »25«. Vi kommer nu att bekanta oss närmare med den porten när vi går igenom några bitar av protokollet. Vi ska även för egen hand skicka iväg ett e-brev med hjälp utav SMTP-protokollet.

Till detta så behöver vi använda oss utav programmet »telnet«, det finns med i alla moderna operativsystem och används ifrån kommandoläget (»command.exe« under Windows).

Den text som kommer från SMTP servern kan variera en del beroende på vilken mjukvara man använder som mailserver men den numreriska statuskoden följer en standard och det är den som ens »mailprogram« bryr sig om. Statuskod på »1xx«, »2xx« samt »3xx« betyder att det är »okej«, »4xx« är temporärt fel (»försök igen senare«) samt att »5xx« innebär att felet är permanent (»försök inte fler gånger«).

I detta exempel så kopplar vi upp oss mot en e-postserver som ligger på IP-adressen »217.215.109.190« och heter »mail.zro.se«, vi skickar ett e-brev ifrån »patric.fors@nollan.pp.se« till »patric@zro.se« med ärenderaden »Testar SMTP manuellt« och »Meddelandet i brevet...<nyrad>Mvh Patric« som innehåll.

Text ifrån SMTP servern är markerad i **fet** stil.

```
telnet mail.zro.se 25
Trying 217.215.109.190...
Connected to as5-4-6.sbn.s.bonet.se.
Escape character is '^]'.
220 mail.zro.se ESMTP
HELO
250 mail.zro.se
MAIL From: patric.fors@nollan.pp.se
250 ok
RCPT To: patric@zro.se
250 ok
DATA
354 go ahead
From: patric.fors@nollan.pp.se
To: patric@zro.se
Subject: Testar SMTP manuellt

Meddelandet i brevet...
Mvh Patric
.
250 ok 1075992163 qp 13641
QUIT
221 mail.zro.se
Connection closed by foreign host.
```

Nu ska vi gå igenom steg för steg i vad vi precis gjorde. Alla »SMTP« kommandon är endast fyra bokstäver långa så »HELO« är rättstavat.

1. »telnet mail.zro.se 25«, skapa en uppkoppling till SMTP servern på »mail.zro.se« med port »25«
2. Telnet skriver en del statusinformation innan uppkopplingen skett.
3. »220 mail.zro.se ESMTP«, här svarar SMTP servern med statuskod »220« som innebär att den är redo.
4. Vi skriver ett »HELO« som hälsningsfras tillbaka.
5. »250 mail.zro.se«, betyder »okej, fortsätt«. Nu börjar det som kallas för »envelope«, man kan likna det med kuvertet med mottagare- och avsändareadresser.
6. Vi fortsätter med »MAIL From: patric.fors@nollan.pp.se« som avsändare.
7. »250 ok«, användaren är godkänd, fortsätt.
8. Och vi fortsätter med mottagaren »RCPT To: patric@zro.se«.
9. »250 ok«, mottagaren är godkänd, fortsätt.
10. Nu slutar »envelope« och vi kliver in i själva e-brevet med »DATA«.

11. »354 go ahead«, dvs kör på med resten utav e-brevet. Nu lyssnar den inte efter kommandon längre så en ensam punkt (».«) först på en rad innebär att e-brevet är slut.

12. Nu kan man säga att vi skriver direkt på pappret i kuvertet, typ »Hej Patric!« och avsändaren uppe i höger hörn. Men på SMTP sätt skriver man »From: patric.fors@nollan.pp.se« och nästa rad blir »To: patric@zro.se« samt att raden under är ärendet för e-brevet »Subject: Testar SMTP manuellt«.

13. En tom rad skiljer ovan ifrån själva e-brevets innehåll.

14. Nu kan vi skriva på hur mycket som helst, detta är e-brevets innehåll.

15. En ensam punkt (».«) först på raden talar om att innehållet är slut, e-brevet skickas iväg samt att SMTP-servern nu lyssnar på SMTP-kommandon igen. Nu kan du skicka ett till e-brev om du vill.

16. »250 ok 1075992163 qp 13641«, e-brevet fick ett »okej« och några nummer som hamnar i SMTP-serverns loggar.

17. Vi skriver »QUIT« och hoppar ur då vi är klara med e-brevet.

En rätt konfigurerad SMTP-server hanterar endast e-post för sina användare/kunder. Den är inställd så att användarna kan skicka e-brev till alla mottagare, ett så kallad »mejlrelä«, samt att den endast tar emot e-brev utifrån till användarnas e-postadresser.

Detta är mest för att förhindra så kallad »spam« (kapitel 5.3.2). De flesta har nog fått oönskad e-post till sin låda med reklam och det mest underliga saker som de vill att man ska köpa eller webbsidor man ska besöka. Om en SMTP-server tillåter obehöriga skicka e-brev via sig för alla möjliga mottagare så kallas den för ett »öppet relä« och det är inte önskvärt för någon annan än de som skickar spam. En stor risk finns då att IP-adressen hamnar i svartalistor och får svårt att skicka e-post till de som filtrerar ut IP-adresser ifrån listorna.

Använd den SMTP server som du fått utav din internetleverantör om du vill testa ovanstående men med andra avsändare och mottagare utav e-brevet.

När bifogade filer läggs med så kodas de om ifrån att vara binära till ren text i ett speciellt format. Alla vanliga e-postklienter kan göra detta samt att de känner igen flera olika format som de kan göra den omvända processen till en binär fil.

3.2 POP3/IMAP

Även någon av dessa ställer man in i sin e-postklient enligt det man fått ifrån sin internetleverantör.

»POP3« är det protokoll som används för att hämta hem sin e-post. Förkortningen står för »Post Office Protocol« och version 3 utav den. POP3 använder sig utav port »110«.

»IMAP« har samma funktionalitet men är mindre vanlig hos internetleverantörer då man läser e-posten direkt ifrån servern istället för att hämta hem den. Det innebär att e-breven hela tiden tar plats på internetleverantörerns hårddiskar istället för sin egna.

Förkortningen »IMAP« står för »Internet Message Access Protocol«. IMAP använder port »143«.

Vi skulle kunna labba med protokollen manuellt likt det vi gjorde med SMTP, men det finns risk att förlora e-post så vi hoppar över laborationen.

3.3 HTTP

Detta protokoll borde vara en aning mer känt då namnet används för webbadresser, t ex »http://www.varmdo.fro.se«. Man kan då gissa rätt så enkelt att protokollet är det som all webbaserad trafik använder sig utav. »HTTP« står för »Hyper Text Transfer Protocol« och använder port »80«.

En webbserver är vanligtvis en vanlig dator med programvara för att hantera protokollet. En enda webbserver kan ta hand om flera företags och kunders webbsidor, t ex så kan »http://www.evensen.org« samt »http://www.svart.com« finnas på samma webbserver.

De som har en internetbank är vana att se »https://« före sin banks webbadress. »HTTPS"« är krypterad HTTP och förkortningen står för »Hyper Text Transfer Protocol Secure«.

HTTPS använder sig utav kryptografiska certifikat, och några pålitliga verifieringsföretags certifikat brukar finnas inbakade i webbläsaren. Dessa används för att på ett säkert sätt avgöra om man verkligen besöker rätt sida så måste webbläsaren verifiera certifikaten. Det gör den genom att jämföra webbsidans certifikat med verifieringsföretagets certifikat (på nätet) samt med den inbakade. Skulle den se något fel så meddelar webbläsaren det direkt. Var *noga* när ni läser felmeddelanden ifrån säkra webbsidor. När webbsidan är verifierad så kommer all kommunikation mellan den och din webbläsare vara krypterad, dvs oläsbar för obehöriga.

HTTPS använder sig av en annan port än HTTP, och den är »443«.

Vi ska titta närmare på HTTP och testa lite manuellt för att se lite hur protokollet fungerar. Även denna gång "telnet" så som när vi testade SMTP (kapitel 3.1). Text ifrån webbservern är i **fet** stil.

```
telnet www.varmdo.fro.se 80
Trying 212.75.79.22...
Connected to thorild.fro.se.
Escape character is '^]'.
GET /index.htm HTTP/1.1
Host: www.varmdo.fro.se

HTTP/1.1 200 OK
Date: Thu, 05 Feb 2004 16:23:44 GMT
Server: Apache/1.3.26 (Unix) Debian GNU/Linux AuthMySQL/3.1
PHP/4.1.2 mod_perl/1.26
Last-Modified: Sun, 25 Jan 2004 12:03:52 GMT
ETag: "16c011-a41-4013b0a8"Accept-Ranges: bytes
Content-Length: 2625
Content-Type: text/html; charset=iso-8859-1
```

```
<html xmlns:o="urn:schemas-microsoft-com:office:office"
xmlns:w="urn:schemas-microsoft-com:office:word"xmlns=
"http://www.w3.org/TR/REC-html40">
<head>
<meta http-equiv=Content-Type content="text/html; charset=
windows-1252"><meta name=ProgId content=Word.Document>
...och så vidare...
```

Även HTTP har statuskoder likt SMTP protokollet. »2xx« är »okej«, »3xx« är ompekare till annan webbplats, »4xx« visat att klienten gjort fel samt »5xx« som indikerar webbserverfel. De flesta känner nog till felmeddelandet »404 Not Found« som anger att den önskade sidan inte finns att tillgå.

1. »telnet www.varmdo.fro.se 80« skapar uppkopplingen till webbservern på destinationsport »80«.
2. Telnetklienten meddelar att den försöker skapa en uppkoppling samt hur man kommer ur den.
3. Vi skriver »GET /index.htm HTTP/1.1« som innebär hämta »index.htm« ifrån huvudkatalogen »/« samt med »HTTP« version »1.1«
4. Vi fortsätter med att skriva »Host: www.varmdo.fro.se« för att tala om vems webbsida vi vill hämta hem »index.htm« ifrån. Innan version 1.1 fanns utav HTTP-protokollet få fick varje domän ha en egen IP-adress. Man kan snabbt räkna ut att om det skulle fortsatt så skulle alla IP-adresser snart ta slut. Nu räcker det med en enda IP-adress per webbserver för alla domäners webbsidor.
5. För att tala om att vår begäran är färdig så behövs en tom rad med endast vagnretur, dvs tryck på RETURN eller ENTER knappen en gång extra.
6. Nu kommer information om vad det är för webbserver, vilka funktioner den stödjer samt själva HTML-koden[1] för webbsidan.
7. Efter en stund så »släpper« webbservern din förfrågan och du kommer tillbaka till kommandoläget. du kan även trycka »ctrl-c«[2] om du vill bryta den snabbare.

4 Mindre synliga delar

4.1 Binära tal

»Det finns 10 typer av personer, de som kan räkna binärt och de som inte kan.«
Okänd

[1] HTML står för “Hyper Text Markup Language” och är det sätt man beskriver hur en webbsida ska se ut.
[2] Håll inne “Ctrl” kappen och tryck sedan på “c”.

»Ettor och nollor« är ett utryck som nästan alla hört när det gäller datorer, och det är precis vad binära tal är.

De består utav ettor och nollor eftersom talbasen är »2« istället för »10« som den är för våra mer vanliga decimala tal. Exempel på binära tal: »1001« blir decimalt »9«, »11111110« blir »254«.

Vad menas då med »talbasen är 2«? Jo, det finns två (»0« samt »1«) möjliga kombinationer för varje position jämfört med vår decimala som har tio olika (»0« till »9«). »Deci-« betyder »tio« och »bi-« betyder »två«.

Varje position har även sitt värde, precis som i det decimala. En ensam trea (»3«) är inte lika mycket »värd« som en trea följt utav en nolla (»30«). Trean följt av nollan är ju tio gånger mer värd.

I binära tal så dubblas värdet för varje position, så en ensam etta (»1«) är värt ett, en etta följt utav en nolla (»10«) är värd två osv.

För att få hela värdet så summerar man värdet på alla positioner, precis som i de decimala. Exempel »39« är »30+9«, binära »11« är »10+01« (summan i decimalt blir »3«).

Varje position i ett binärt tal kallas för »bit«, åtta bitar kallas för en »byte« eller »oktett«. Man brukar gruppera binära tal i oktetter för läsbarhetens skull. Som en kort överkurs så kan jag även nämna att även hexadecimala tal är en vanlig gruppering i programmering, talbasen är då sexton och man går från 0 till 9 och fyller sedan på med A till F för att skapa 16 möjliga kombinationer per sifferposition.

Det maximala värdet som en byte kan ha är »255« och det minsta är givetvis »0«, dvs »256« olika värden. För att beskriva större tal så används flera bytes brevid varann, t ex två bytes blir sexton bitar och ett maxvärde på »65535« (»65536« olika värden).

När man beskriver storlekar och hastigheter så är det viktigt att man vet vilken storhet och enhet man menar. Det som har blivit praxis är att »B« står för »byte« och »b« för »bit«. Ett exempel på felaktig storlek är »200 mb hårdisk«, dvs »200 millibit hårddisk«, fyrtio stycken sådanna och vi är uppe i en hel bytes hårddisk.

Datatermgruppen[3] har som rekommendation att skriva »byte« eller »bit« för att förtydliga enheten.

Här följer en tabell med en bytes alla positioner och värden.

1	1	1	1	1	1	1	1
128	64	32	16	8	4	2	1

Exempel, »01101001« blir decimalt »105«:

0	1	1	0	1	0	0	1
0	64	32	0	8	0	0	1

64+32+8+1=105

En liten påminnelse, en IP-adress har 32 bitar uppdelat på fyra oktettet (mer i kapitel 2).

Lite vanliga storheter:

[3] http://www.nada.kth.se/dataterm/rek.html#a6

Storhet	Namn[4]	SI-värde[5]	Värde i datorvärlden[6]	Exempel
k-	kilo	1000	1024	56 kbit/s
M-	mega	1000 000	1 048 576	32 MByte
G-	giga	1000 000 000	1 073 741 824	80 GByte
T-	tera	1000 000 000 000	1 099 511 627 776	2 TByte

4.2 Hastigheten på nätverket

När man talar om hastigheter i ett nät så brukar man använda ordet »bandbredd«. Den hastighet man beskriver är »rå« hastighet i bitar per sekund. När man lägger på ett protokoll så som »TCP/IP« så tar även det en liten del av bandbredden. Protokollet tar plats därför det beskriver vad som kommer, t ex vem som ska ha paketet samt avsändaren, typ utav paket, ordningsnummer och så själva innehållet.

Om det står »10 M*bit*/s« så innebär det 1,25 M*byte*/s och med protokollet pålagt så kan man få ut en teoretisk maxhastighet på ca 1 M*byte*/s.

4.3 Storlek på nätverk

När man sätter upp ett datornätverk så är det inte bara den fysiska utrustningen som ska begränsa storleken på nätet, man sätter även en begränsning på hur många IP-adresser som det ska bestå utav.

Anledningarna till en begränsning kan vara många men en vanlig är för att hårdvara som jobbar på länkskiktet gör en så kallad »broadcast« för att få reda på MAC-adressen (kapitel 2) för en viss IP-adress i samma nät. Det finns även andra protokoll som gör broadcast för att få reda på information. Så med ett för stort nätverk så kommer det att svämma över utav alla dessa förfrågningar. Kallas lite elakt för »broadcast stormar«.

Det finns lite olika sätt att benämna storlekarna, det vanligaste för några år sedan var att man pratade om »A-«, »B-« och »C-nät«. Ett »C-nät« är minst med 256 st IP-adresser, »B-nät« har 65536 st och störst är »A-nät« med 16777216 st.

För att kunna veta vilken typ utav nätverk som beskrivs så behövs en »subnätmask«. Den ser ut som en IP-adress till skrivsättet men den beskriver med hjälp utav åtta (»255.0.0.0«) till tjugofyra (»255.255.255.0«) binära ettor ifrån vänster hur stort nätet är. De binära ettorna markerar hur stor del utav IP-adressen som är nätet.

En IP-adress tillsammans med en subnätmask anger hur stort datornätet är samt att den är en nätadress för den utrustning man kopplat in. Med andra ord så är en del av IP-adressen nätet, och subnätmasken beskriver hur stor den delen är.

Exempel.

Typ	IP-adress för nätet	Max IP-adresser	Nätmask
A	10.x.x.x	256*256*256=16777216 st	255.0.0.0
B	10.11.x.x	256*256=65536 st	255.255.0.0
C	10.11.12.x	256 st	255.255.255.0

Skalan inte är så flexibel om man har en nätstorlek som inte passar in i någon utav dem. IP-adresserna skulle snabbt ta slut om man inte löste flexibiliteten. Därför infördes något som kallas »klasslösa nät« som innebär att man delar upp näten i ytterligare mindre delar.

Nu fick »subnätmasken« även beskriva delar utav »A-«, »B-« samt »C-näten«. Denna gång så behöver man inte fylla på med åtta bitar åt gången utan man fyller bara på med så många binära ettor ifrån vänster så långt man behöver (glöm inte att en IP-adress har max 32 bitar).

Om ni minns hur man räknar ut binära tal (kapitel 4.1) så blir nätmasken enkelt att räkna ut. Åtta stycken ettor (»11111111«) blir »255« och är en vanlig oktett i en nätmask. Så om en nätmasks sista oktett är »11100000« så blir hela nätmasken »255.255.255.224« om vi skulle ha delat upp ett »C-nät«.

Hur stort skulle då vårt uppdelade »C-nät« bli, dvs hur många IP-adresser får vi i det nya mindre nätet? Det är rätt så enkelt att räkna ut det med. Man räknar summan på de positioner till höger i nätmasken som är nollor som om de vore ettor. Så i vårt exempel med »255.255.255.224« som nätmask så skulle vi få 32 st IP-adresser i det nätverket (fem nollor).

Nu kan vi inte använda oss utav alla 32 st, första och sista IP-adressen är reserverade för annat. Den första beskriver nätverket och används inte av tradition till maskiner även om det skulle kunna funka och den sista är broadcastadressen för nätet. Då blir det 30 st kvar att använda för datorer och annat.

Vi får inte glömma att vi även får fler små nät när vi delar upp större på detta sätt. Istället för att ha 256 st (254 st användbara) IP-adresser i *ett* C-nät så har vi nu utav samma nät fått 8 st nät med 32 st IP-adresser vardera, där 30 st går att använda. Det första nätet är »x.x.x.0« till »x.x.x.31«, nästa på »x.x.x.32« till »x.x.x.63« osv.

Om vi skulle dela upp det i ännu mindre bitar, t ex med en nätmask på »255.255.255.252« så skulle vi få 64 st nät med 4 st IP-adresser vardera. Precis som innan så kan inte första och sista IP-adressen användas så det lämnar oss med endast 2 st kvar per nät. Inte så många alls, då hela 128 st IP-adresser »försvinner« när vi delade upp det i så små bitar. Det finns tillfällen då dessa små nät är användbara.

Att ange en nätmask för att beskriva storleken blir lite otympligt efter en stund så ett annat skrivsätt finns som heter »CIDR«. CIDR står för »Classless Inter-Domain Routing« och anger de antalet bitar som står för storleken på nätverket. I vårt exempel ovan där nätmasken var »255.255.255.224« så skulle det stå som »/27« i CIDR benämning. Minns att en IP-adress består utav 32 st bitar så »/27« betyder att de första 27 st bitarna är nätstorleken och de 5 st som är kvar blir de IP-adresser som kan användas för utrustning. För att förenkla yttrligare så brukar man hoppa över att skriva de nollor som är givna, t ex »10.0.0.0/8« blir »10/8«.

Här är en tabell med nätmask, motsvarande CIDR samt hur många IP-adresser nätet består utav.

CIDR	Nätmask	Nätmasken i binär form	Antal IP-adr.
/8	**255.0.0.0**	11111111.00000000.00000000.00000000	16777216
/9	255.128.0.0	11111111.10000000.00000000.00000000	8388608
/10	255.192.0.0	11111111.11000000.00000000.00000000	4194304
/11	255.224.0.0	11111111.11100000.00000000.00000000	2097152
/12	255.240.0.0	11111111.11110000.00000000.00000000	1048576
/13	255.248.0.0	11111111.11111000.00000000.00000000	524288
/14	255.252.0.0	11111111.11111100.00000000.00000000	262144
/15	255.254.0.0	11111111.11111110.00000000.00000000	131072
/16	**255.255.0.0**	11111111.11111111.00000000.00000000	65536
/17	255.255.128.0	11111111.11111111.10000000.00000000	32768
/18	255.255.192.0	11111111.11111111.11000000.00000000	16384
/19	255.255.224.0	11111111.11111111.11100000.00000000	8192
/20	255.255.240.0	11111111.11111111.11110000.00000000	4096
/21	255.255.248.0	11111111.11111111.11111000.00000000	2048
/22	255.255.252.0	11111111.11111111.11111100.00000000	1024
/23	255.255.254.0	11111111.11111111.11111110.00000000	512
/24	**255.255.255.0**	11111111.11111111.11111111.00000000	256
/25	255.255.255.128	11111111.11111111.11111111.10000000	128
/26	255.255.255.192	11111111.11111111.11111111.11000000	64
/27	255.255.255.224	11111111.11111111.11111111.11100000	32
/28	255.255.255.240	11111111.11111111.11111111.11110000	16
/29	255.255.255.248	11111111.11111111.11111111.11111000	8
/30	255.255.255.252	11111111.11111111.11111111.11111100	4
/31	255.255.255.254	11111111.11111111.11111111.11111110	2
/32	255.255.255.255	11111111.11111111.11111111.11111111	1

Exempel 1:

Nätet »192.168.7.0« och nätmasken »255.255.255.0« kan skrivas »192.168.7.0/24«. Nätet har 256 st IP-adresser där »0« och »255« inte kan användas utav någon utrustning.

Exempel 2:

Ett »192.168.0.0/29« nät har nätmasken »255.255.255.248« samt består utav 8 st IP-adresser ifrån »192.168.0.0« till »192.168.0.7« där endast »192.168.0.1« till »192.168.0.6« kan användas. Nätverksdelen utav IP-adressen är markerad med **fet** stil.

IP-adress	IP-adressen binärt	Nätmasken binärt	Kommentar
192.168.0.0	...**00000**000	...**11111**000	Nätets adress
192.168.0.1	...**00000**001	...**11111**000	fri
192.168.0.2	...**00000**010	...**11111**000	fri
192.168.0.3	...**00000**011	...**11111**000	fri
192.168.0.4	...**00000**100	...**11111**000	fri
192.168.0.5	...**00000**101	...**11111**000	fri
192.168.0.6	...**00000**110	...**11111**000	fri
192.168.0.7	...**00000**111	...**11111**000	Broadcast adress

Så efterföljande »/29« nät blir då:

IP-adress	IP-adressen binärt	Nätmasken binärt	Kommentar
192.168.0.8	...**00001**000	...**11111**000	Nätets adress
192.168.0.9	...**00001**001	...**11111**000	fri
192.168.0.10	...**00001**010	...**11111**000	fri
192.168.0.11	...**00001**011	...**11111**000	fri
192.168.0.12	...**00001**100	...**11111**000	fri
192.168.0.13	...**00001**101	...**11111**000	fri
192.168.0.14	...**00001**110	...**11111**000	fri
192.168.0.15	...**00001**111	...**11111**000	Broadcast adress

4.3.1 Verktyg

Ovanstående omvandlingar, samt en hel del annat finns det hjälpverkyg för på denna webbsida:

```
http://library.mobrien.com/net.shtml
```

4.4 DHCP

Förkortningen »DHCP« står för »Dynamic Host Configuration Protocol« och är ett protokoll för att dela ut IP-adresser och andra inställningar på ett lokalt nätverk (LAN).

Man ställer in klienten för dynamisk konfiguration och kopplar in den på nätet. Den kommer då att göra en broadcast på LANet och en DHCP-server kommer att svara med inställningar för klienten.

Utan en DHCP-server så måste man själv konfigurera sin dator med rätt inställningar för att den ska kunna kommunicera med andra.

En DHCP-server finns som programvara i många operativsystem samt även i hårdvara (bredbands brandväggar). Den behövs konfigureras så att den ger ifrån sig rätt inställningar. Då det är olika sätt att göra det för varje server så kommer denna text inte att gå igenom hur det görs. Vanliga inställningar är DNS-servrar (kapitel 4.5), »default gateway« (kapitel 4.6), nätmask samt vilka IP-adresser den ska dela ut.

Klienten behåller IP-adressen tills halva lånetiden gått ut, den gör då en ny begäran om förnyelse direkt till DHCP-servern. Vanligtvis så får klienten samma IP-adress som innan eftersom DHCP-servern behåller en databas med vilken MAC-adress (kapitel 2) som fått IP-adressen, ofta även efter att klienten slutat förnya via DHCP. Först då många datorer är anslutna till samma DHCP-server och det är stor omsättning kan IP-adressen variera när man skickar ut en förfrågan om IP-adress.

4.5 DNS

När du skriver in en webbadress som t ex »http://www.sssa.nu« vet normalt inte datorn vartifrån den ska hämta webbsidan. Den behöver en IP-adress och

DNS fixar den biten.

»Domain Name System« eller mer känt som »DNS« kan liknas med nätverkets nummerupplysning. DNS översätter värdnamn så som »www.sssa.nu« till IP-adress samt tvärtom.

När man slår upp IP-adress till värdnamn så brukar man kalla det för »reversen« då det normala är att fråga efter IP-adress.

För att kunna använda en DNS-server så måste klienten ha en inställd i sina TCP/IP inställningar. Har man automatisk konfigurering med hjälp utav DHCP (kapitel 4.4) så får man normalt sett DNS-inställningarna därifrån.

DNS-strukturen är hierarkisk, där »root-domänen« är högst upp och vet vilka DNS servrar som har hand om »toppdomänerna«. En toppdomän är t ex ».se«, ».com« eller ».nu«. Toppdomän-DNSen vet i sin tur vem som har hand om domänerna som ligger under den, t ex »sssa.nu«. Sssa.nu-domänens DNS-server kan svara med IP-adressen för »www.sssa.nu«. Det är med andra ord många hänvisningar tills man kommer till den rätta »auktoritära DNS-servern« som har den information man frågar efter.

En DNS-server är en programvara som finns till alla operativsystem. Tjänsten använder sig utav UDP-paket på port 53, och består utav två delar, en så kallad »resolver« och en auktoritär del.

Auktoritära DNSer är de som har originalinformationen om en eller flera domäner, t ex »www.sssa.nu«. De har ingen kunskap om andra domäner än sina egna och svarar normalt sett inte på frågor som inte rör deras egna domäner.

»Resolvern« däremot är den del som tar alla typer av DNS-förfrågningar och ger sig ut och frågar auktoritära DNSer efter information. Den börjar med att se om den svarat på det nyligen genom att den letar i sin »cache« utav frågor och svar. Finns den inte där så följer den hierakin och fyller på sin cache med information. Inställningarna på sin dator för DNS är alltid en resolver.

Varje DNS-uppslag stannar inte i en resolver hur länge som helst, det finns en »bäst-före« tid som när den passerat ser till att den informationen slängs ifrån cachen.

En DNS-server lagrar inte bara domäner och IP-adresser utan även annan information som t ex vilken dator som hanterar e-post för domänen.

Det finns även idéer om att lagra information om telefonnummer och namn, precis som en riktig nummerupplysning. Man kan säga att DNS är mycket flexibel som uppslagsverk.

4.5.1 Verktyg

Nu ska vi testa och se vad man kan få ut utav en DNS-server. Verktygen vi ska använda heter »nslookup« och finns på alla operativsystem. Det är gammalt och kommer snart att ersättas med något bättre, men för våra tester så duger det utmärkt.

Börja med att gå till kommandoläget, ett »skal« under Unix och »command.exe« för Windows. Resultatet ifrån nslookup är markerat med **fet** stil.

Utskriften kan se lite olika ut beroende på vilken version utav »nslookup« som används.

Exempel 1:

Vi slår upp vilken IP-adress som »www.varmdo.fro.se« har.

```
nslookup www.varmdo.fro.se
Server:  192.168.42.1
Address: 192.168.42.1#53
Non-authoritative answer:
Name: www.varmdo.fro.se
Address: 212.75.79.22
```

En hel del information utöver den vi begärde, men var inte orolig det här reder vi ut.

Nslookup talar först om vilken DNS-resolver den frågat, med värdnamn och IP-adress. Därefter kommer informationen om att det är »non-authoritative«, dvs att DNS-resolvern inte är auktoritär utan endast en resolver för det man frågat. Och sist är själva svaret på vår fråga, »212.75.79.22«.

Exempel 2:

Nu ska vi slå upp reversen, dvs värdnamnet på den IP-adress vi fick ovan (»212.75.79.22«) innehar.

```
nslookup 212.75.79.22
Server:  192.168.42.1
Address: 192.168.42.1#53
Non-authoritative answer:
22.79.75.212.in-addr.arpa       name = thorild.fro.se.
```

Nu ser svaret lite mer komplicerat ut och ingenstans ser vi »www.varmdo.fro.se« som vi kanske trodde. Första delarna är de samma som i exempel 1, men själva svaret är inte det vi förväntade. Anledningen till det kan vara flera, dels så kan flera värdnamn peka på samma IP-adress eller så är uppslag och »reversen« konfigurerad att svara olika.

I detta fall så är det en webbadress så det troliga är att webbservern hanterar sidor för fler värdnamn än FRO Värmdö. Dvs många värdnamn pekar på samma IP-adress, men webbserverns »riktiga« värdnamn är »thorild.fro.se« som reversuppslagningen snällt berättar. Det är inte alls ovanligt att ett namn pekar på flera IP-adresser eller att flera namn pekar på samma IP-adress.

»in-addr.arpa« är toppdomänen för reversuppslagningar. Eftersom domäners och IP-adressers mest signifikanta del är spegelvänt mot varann så har man valt att vända på IP-adressen och lägga till »in-addr.arpa« som toppdomän.

Den mest signifikanta delen i »thorild.fro.se« är ».se« och för IP-adressen är det »212«. En uppslagning för en revers blir då detsamma som för ett domännamn. I detta fall så frågar resolvern vem som är auktoritär för »212.in-addr.arpa«, därefter »75.212.in-addr.arpa« osv.

4.6 Routing

Vi har nu gått igenom många protokoll och delar utav ett datornätverk, binära tal och annat som hör ihop. Men vi har ännu inte bekrivit hur en dator eller annan utrustning kan veta *vart* den ska skicka sina paket.

För att förenkla så använder vi liknelsen att varje IP-adress är en vanlig fysisk adress. När vi vet destinationen samt att vi redan kan vår egna adress så behöver vi en färdplan för resan. Routing är själva färdplanen. Är avsändare och mottagare utav ett IP-paket på samma nätverk så skickas paketet direkt till mottagaren. Där kommer nätmasken in i bilden, det är via nätmasken som klienten vet om den kan prata direkt med mottagaren eller om den måste få hjälp med transporten.

Nu är routing så smidigt att den anpassar färdplanen utefter vägen. Så om en »väg« plötsligt försvinner så kommer paketet ändå fram om alternativa vägar finns. Routing är faktiskt bättre än en färdplan eftersom varken avsändare eller paketet själv behöver ta reda på vart nästa riktning blir. Det gör hård- eller mjukvara som kallas »routrar« som finns i varje steg mellan avsändare och mottagare av paketet. De har en tabell som hela tiden uppdateras om vilken väg som är bäst just nu. Antalet steg, eller som det vanligtvis kallas »routerhopp«, varierar beroende på avstånd mellan nätverken.

En router kan vara hårdvara som enbart är gjort för routing, annan hårdvara som har fler funktioner utöver routing eller till och med som ett simpelt program i en dator.

När man konfigurerar sin dator så att den blir en del utav ett nät så ställer man även in något som brukar kallas »default gateway« eller »default router«. Det är dit som alla paket skickas om inte mottagaren finns på samma nät som man själv är på.

Om vi ska gå tillbaka till liknelsen med fysiska adresser så om jag ska ifrån Fisksätra till Gustavsbergs Centrum så går jag till min »default gateway« som i detta fallet är Saltsjöbanans station (vi leker med tanken att det endast är det transportsätt som finns att tillgå). Väl på Saltsjöbanan så får jag nästa destination som blir tag tåget till Slussen. Framme i Slussen så får jag nästa »hopp« som är buss 425 osv tills jag är framme vid resans mål.

Skulle det vara någon störning i trafiken så skulle »routern« ta reda på vilken väg som då blir snabbast. T ex stopp för Saltsjöbanan i Saltsjö-Järla och jag får en ny »route« att ta buss 422 därifrån till Gustavsbergs Centrum.

För att beskriva hur en router kan veta hur den bäst ska skicka paketet så behöver vi gå in lite i detaljer hur större nätverk kopplade till Internet är organiserade. Vi flyttar oss upp i fågelperspektiv och tittar mer på ett företags nätverk med alla dess komponenter som *en* enda enhet.

Nätverken på Internet är uppdelade i två delar, den »yttre« delen är den del som ansluter till andras nätverk och den »inre« är företagets alla egna nätverk och hanteras helt internt.

Hur »kopplar man in sig« i Internet? Vad är Internet? Det kanske låter som stora djupa frågor men svaret är rätt så enkelt. Det finns inte *en* punkt som är Internet utan det är massor med nätverk som är sammankopplade på flera

punkter. Vissa punkter är samlingspunkter för många nätverk, de kallas för »GIX« (»Global Internet Exchange«) eller »peeringpunkt«.

Alla nätverk kopplade till Internet som en stor internetleverantör, mycket stort företag eller organisation innehar är samlade i ett unikt »AS-nummer« (»Autonomous System«). AS-numret blir en typ utav samlingsadress för alla dess nätverk.

Nätverken utbyter AS-nummer med tillhörande IP-nät med varann där de är sammankopplade, kan vara på fler ställen. De utbyter även AS-nummer för andra nät än sig själv. Detta innebär att varje AS-nät får en tillgång till *alla* AS-nummer och hur långt bort de är.

Dessa tabeller blir unika för alla AS-nät och som ni förstår så uppdateras de konstant.

Om vi ska återgå ännu en gång till liknelsen med fysiska verkligheten så kan man likna en peeringpunkt med Arlanda där olika stora »nät« (länder) av trafik möts. Detta protokoll kallas för »BGP« där förkortningen står för »Border Gateway Protocol«.

Inom ett AS-nätverk så används en mer dynamisk och detaljerad bild hur allt är sammankopplat. Där utbyter routrarna information med ett annat protokoll t.ex ett som heter »OSPF« (»Open Shortest Path First«). Med vår liknelse igen så är detta Slussen eller T-Centralen, dvs information om trafikvägar inom landet.

BGP är med andra ord mer »grovt« och OSPF mer i detalj. Om du reser till London så är det OSPF till Arlanda med kollektivtrafik eller ArlandaExpress, och BGP till Heathrow i London (information om trafikvägar utomrikes).

Självklart så kan man även ställa en route manuellt, det kallas en »statisk route« och används bland annat då den inte ska förändras oavsett vad som händer i nätverket eller i de fall då det helt enkelt bara kan se ut på ett vis.

4.6.1 Verktyg

Kan man se hur ens routing ser ut? Givetvis är det möjligt med lite verktyg. Det verktyg vi ska använda först heter passande nog »traceroute«. Under Windows så är det förkortat till »tracert«. Starta »command.exe« under Windows eller valfritt skal under Unix. Resultatet ifrån traceroute är markerat med **fet** stil.

Traceroute exempel under Windows (med radbrytningar för vissa IP-adresser):

```
C:\>tracert aristotle.algonet.se
Tracing route to aristotle.algonet.se [213.150.135.238]
over a maximum of 30 hops:
  1    <1 ms    <1 ms    <1 ms  seven.bzt.dmz [192.168.42.1]
  2    27 ms    14 ms    13 ms  217.215.109.1
  3    14 ms    14 ms    13 ms  ar2sbk1-geth0-0-0.fre.skanova.net
[217.209.228.69]
  4    14 ms    13 ms    13 ms  fre-d2-geth7-1.se.telia.net
[217.209.228.65]
  5    13 ms    14 ms    13 ms  hy-c1-pos11-1.se.telia.net
[217.209.228.5]
  6    14 ms    14 ms    13 ms  hy-peer1-pos3-0.se.telia.net
[194.17.167.146]
  7    15 ms    14 ms    15 ms  netnod-ix-ge-b-sth.utfors.net
[194.68.128.66]
```

```
 8    15 ms    15 ms    15 ms  ge-0-0-0.se-sthms001-pe-1.tu.telenor.net
[212.105.101.198]
9    15 ms    16 ms    15 ms  ti600000b051-ge4-2.ti.telenor.net
[148.122.8.13]
10    16 ms    16 ms    15 ms  ti600000a180-ge2-3.ti.telenor.net
[146.172.116.131]
11    17 ms    16 ms    40 ms  213-150-130-42.telenor.se
[213.150.130.42]
12    17 ms    17 ms    17 ms  aristotle.algonet.se
[213.150.135.238]
Trace complete.
```

Ovan ser vi alla routrar som ett paket ifrån min dator till »aristotle.algonet.se« just nu tar sig igenom. Vägen tillbaka ifrån aristotle kan vara en helt annan, det kallas »assymetrisk routing« och är rätt så vanligt.

Med hjälp utav »netstat« så kan vi se den routing tabell som datorn har.

Att se sin routing tabell:

```
C:\>netstat -r
Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 d0 b7 06 b0 e8 ...... Intel(R) PRO/100+ Management Adapter - Pack
et Scheduler Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination       Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.42.1  192.168.42.210       20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
    192.168.42.0    255.255.255.0   192.168.42.210  192.168.42.210       20
  192.168.42.210  255.255.255.255        127.0.0.1       127.0.0.1       20
  192.168.42.255  255.255.255.255   192.168.42.210  192.168.42.210       20
        224.0.0.0        240.0.0.0   192.168.42.210  192.168.42.210       20
 255.255.255.255  255.255.255.255   192.168.42.210  192.168.42.210       1
Default Gateway:      192.168.42.1
===========================================================================
Persistent Routes:  None
```

Ovan så ser vi först en lista på alla anslutna »interface«, dvs nätverkskort, som datorn har. Därunder de nät och nätmask för näten samt vilken »Gateway« , dvs router, som är mottagare för det. En »Persistent route« är det samma som »statisk route«.

Kan ni se vilken IP-adress som min brandvägg har?

4.7 Speciella nät

Vi ska nu ta upp IP-adresser med lite speciell innebörd, så som »privata nät« och den »egna värddatorn«. Betydligt mer information om dessa speciella nät hittar du i RFC 3330[7].

4.7.1 Privata nät

»Privata nät« är precis som det låter, dvs de nät som inte routas på Internet utan endast i sitt egna nät. Det innebär att flera kan använda samma IP-adresser

[7] http://www.faqs.org/rfcs/rfc3330.html

utan att de »krockar« på Internet.

Privata nät är något som *alla*, även företag, kan använda på sitt nät så länge routing för dem inte annonseras utanför sina egna nätgränser. För att denna annonsering ska råka ske måste man konfigurera sin router väldigt felaktigt.

När man kopplar ett nätverk som använder privata adresser så måste man använda sid utav NAT (kapitel 5.2.1)

Här är den adressrymd som är allokerad för privat/internt bruk:

IP-rymd	CIDR	Antal IP-adresser
10.0.0.0 - 10.255.255.255	10/8	16777216
172.16.0.0 - 172.31.255.255	172.16/12	1048576
192.168.0.0 - 192.168.255.255	192.168/16	65536

4.7.2 127.0.0.1

IP-adressen »127.0.0.1« eller namnet »localhost« kanske ser bekant ut. Anledningen är rätt så enkel, all utrustning som använder IP-adresser har den som sin *egna* adress. Denna adress kallas för »loopback« då den pekar på sig själv.

Nu är det inte enbart 127.0.0.1 som har den speciella funktionen utan hela 127.0.0.0/8 nätet. Om ni inte minns CIDR så kan vi fuska lite och skriva på annat sätt: 127.0.0.0 till 127.255.255.255. Med andra ord så är det väldigt många IP-adresser som är loopback. Man har dock valt att använda »127.0.0.1«. Prova att »pinga« (se nästa kapitel) så ser ni.

Man kan undra vilken nytta en loopback adress har. Den underlättar mycket när man ska sätta upp tjänster som *endast* ska kunna gå att nå lokalt av utrustningen själv. Eller för »torrkörning« utav en tjänst som ska kunna bli nåbar via nätet.

4.8 ICMP

ICMP är ett statusprotokoll för IP-baserade nät. Den skickar information till avsändaren om något gått fel eller ett resultat om man begärt en test. Själva förkortningen står för »Internet Control Message Protocol«.

Vanligast är att man använder verktyget »ping« för att diagnostisera, då skickas ett ICMP »echo request« paket som får ett ICMP »echo reply« tillbaka. Andra ICMP meddelanden är »Destination Unreachable« som skickas när IP-paket skickats iväg men en router längst vägen inte hittar till mottagaren.

Något som alla IP-paket har är »time to live« (även kallat »TTL«) som är en siffra hur länge paketet får »leva« på nätet. Siffran sätts utav avsändaren och varje router paketet passerar minskar denna siffra med ett. När den är nere på noll och inte nått fram till mottagaren så skickas ett ICMP »Time Exceeded« tillbaka till avsändaren samt att IP-paketet slängs. Förklaringen till TTL är enkel, vilsna paket som skickas ska inte få leva i evigheter susandes fram och tillbaka utan hitta någon mottagare.

Traceroute går ut på att man skickar ett paket med TTL=1 och ser vilken router som angav att TTL numera hade nått 0, därefter ett paket med TTL=2

osv tills man når slutdestinationen.

ICMP paket skickas precis som UDP vind för våg, ingen kontroll om det kommit fram eller tappats bort på vägen.

4.8.1 Verktyg

Här ska »ping« få visa vad den går för. Även som i de andra labborationerna så behövs ett kommandoskal. Starta »command.exe« under Windows eller ditt favoritskal i Unix. Utskriften och växlarna för ping varierar efter operativsystem. Den jag valt i exemplet nedan är ifrån Windows. Resultatet ifrån ping är markerat med **fet** stil.

Exempel 1:

Vi börjar med att göra en enkel ping mot ett värdnamn eller IP-adress.

```
C:\>ping kairos.algonet.se
Pinging kairos.algonet.se [213.150.135.237] with 32 bytes of data:
Reply from 213.150.135.237: bytes=32 time=16ms TTL=245
Reply from 213.150.135.237: bytes=32 time=17ms TTL=245
Reply from 213.150.135.237: bytes=32 time=17ms TTL=245
Reply from 213.150.135.237: bytes=32 time=16ms TTL=245
Ping statistics for 213.150.135.237:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 17ms, Average = 16ms
```

Utskriften visar att det i snitt var 16 ms mellan min dator och den jag »pingade«. Fyra ICMP echo request paket skickades och lika många kom tillbaka, dvs »0% loss«. Skulle det vara hög belastning eller routingproblem i nät eller utrustning någonstans på vägen så kan man tappa paket, och det syns tydligt i svaret.

Exempel 2:

Vi kanske inte tycker att hela fyra paket är en bra grund för statistik eller diagnos så vi vill skicka fler. Denna ping kommer att fortsätta till man avbryter igenom att trycka ctrl-c .

```
C:\>ping -t kairos.algonet.se
Pinging kairos.algonet.se [213.150.135.237] with 32 bytes of data:
Reply from 213.150.135.237: bytes=32 time=17ms TTL=245
Reply from 213.150.135.237: bytes=32 time=16ms TTL=245
Reply from 213.150.135.237: bytes=32 time=17ms TTL=245
Reply from 213.150.135.237: bytes=32 time=16ms TTL=245
Reply from 213.150.135.237: bytes=32 time=16ms TTL=245
Reply from 213.150.135.237: bytes=32 time=16ms TTL=245
Reply from 213.150.135.237: bytes=32 time=16ms TTL=245
Reply from 213.150.135.237: bytes=32 time=17ms TTL=245
Reply from 213.150.135.237: bytes=32 time=16ms TTL=245
Reply from 213.150.135.237: bytes=32 time=16ms TTL=245
Reply from 213.150.135.237: bytes=32 time=17ms TTL=245
Ping statistics for 213.150.135.237:
    Packets: Sent = 11, Received = 11, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 17ms, Average = 16ms
Control-C^C
```

Nu har vi betydligt fler paket att bygga statistik på. Jag nämde inte att även storleken på dessa paket kan förändras, i detta fall är de 32 bytes, men det får ni klura själva.

5 Säkerhet

> »Security is a process, not a product.«
> Bruce Schneier

Vad är datorsäkerhet? Är det fysisk tillgång till datorn, vilka som får använda den eller är det utnyttjande av fel i program eller nätverk? Någon hindrar dina nättjänster? Datorns driftsäkerhet? Eller är det kanske att man spar en kopia av viktiga dokument på CD?

Det är allt ovan! Man vill inte att någon kommer åt sin personliga information, företagsfiler eller annat viktigt man spar på sin dator. Om datorn kraschar och man förlorar veckor eller månaders jobb så är man tacksam om man har en kopia sparad på annan plats.

Även om man inte har något alls på sin dator så drabbas man om den raderas helt. Man tappar tid som kunde utnyttjas till roligare saker. Eller det kan till och med vara så att sin egna dator används utav obehörig för att göra intrång eller annat obehagligt mot annan eller en själv. Vems IP-adress tror du då loggas?

De ämnen som kommer att tas upp nedan skiljer sig inte så mycket ifrån vardaglig säkerhet. De flesta har bra lås på ytterdörren och halvbra på bilen, de flesta har brand-, bil- eller huslarm, några har fått bluffakturor till sitt företag, vi får alla reklam med posten samt att vi stänger och låser alla dörrar när vi går hemifrån.

Det är också så att vi låser om oss av flera skäl på samma gång. Givetvis vill vi inte bli av med vår bil vi köpt för dyra pengar, men även om vi vunnit bilen på lotteriet så skulle vi inte vilja att någon stal den. I det mest extrema ytterlighetsfall där vi kunde få en ny bil gratis om den gamla försvann, så skulle ändå inte vilja att någon stal vår bil och använde den som flyktbil vid ett bankrån. På samma vis bör man se om sin dator och det data man har på den, för även om det kanske går att återskapa eller återinstallera det som finns där så ska man inte ge någon annan chansen att missbruka sin egen maskin.

5.1 Lösenord

Lösenord kan liknas med lås. Har vi endast ett kvastskaft lutat mot ytterdörren så är det ingen överraskning om tjuven kommer in utan problem.

Man ska byta lösenord ett par gånger per år eller då man har en liten misstanke om att det kanske kommit i orätta händer. Byt lösenord oftare om du använder det på internetkaffér eller om du varit utomlands och läst din e-post med ditt e-postprogram. Anledningen är att e-post använder vanligtvis lösenord i klartext samt att internetkaféer är utsatta platser för intrång.

Ett tips för att inte låsa sig ute, på grund av att man glömt bort lösenordet, är att skriva ner de på ett papper och stoppa ner det i ett kuvert som man förseglar och skriver sin namnteckning och datum på. Detta kuvert ska sedan låsas in på ett *säkert* ställe.

Här är några tips på hur man kan komponera ihop ett bra lösenord:

- Det är *inte* ett eller flera ord ifrån en ordbok oavsett språk eller ovanlighet.
- Det är *inte* ett ord följt utav eller påbörjas med nummer, slumpmässiga bokstäver eller tecken.
- Det är *inte* enbart siffror.
- Det är *inte* något mönster på tangentbordet.
- Det är *inte* din dators namn, märke eller modellnamn.
- Det är *inte* något inloggningsnamn.
- Det är *inte* någon halvhemlig information som t.ex personnummer...
- Det ska *inte* gå att gissa, som t.ex namn på en kändis, årstiden, månaden eller kombination utav månad och år.
- Det ska *inte* vara något med personlig anknytning, som t ex din hunds namn, favorit godis, registreringsnumret på bilen...
- Det ska *inte* vara benämnt som ett »bra lösenord« i någon bok, webbsida, dokument eller annat publicerat.
- Det är *inte* något som du skulle kunna skicka i klartext till någon, som t.ex användarnamn, e-postadress, kontonummer, postadress...
- Det är *inte* något utav ovan där bokstav eller siffra är utbytt mot liknande, som t ex »i« till »!«, »o« till »0« (noll), »V« till »5«...
- Det är *inte* något utav ovan i annan form så som spegelvänt, dubbelt eller annan förändring.
- Det *ska* vara längre än 8 tecken, helst längre än 12.
- Det *ska* innehålla gemener, versaler, andra tecken än bokstäver, siffror...

Populära papper att spara lösenord på är gula notispapper och favoritplatsen kan vara på skärmen eller under tangentbordet. Bästa platsen är som jag skrev ovan men om man inte orkar sprätta upp kuvertet hela tiden för att det är svårt att minnas alla 4711 st olika lösenord så kan man lägga de i krypterad form i sin dator.

Min rekommendation är »Password Safe« ifrån:

```
http://www.schneier.com/passsafe.html
```

5.2 Nätverk

5.2.1 NAT

»NAT« betyder »Network Address Translation« och är IP-adressöversättning med flera användningsområden.

Ett är att ansluta flera datorer till en internetanslutning när man har fått färre IP-adresser än vad man har datorer. NAT sker då i routern eller brandväggen som internetanslutningen är kopplad till. IP-adressen för avsändaren byts ut i paketet. Så trafiken ifrån routern kommer då att ha en annan IP-adress som avsändare än den riktiga lokalt på nätverket. Allt förs in i tabell och det omvända sker på vägen tillbaka.

Ett annat användningsområde för NAT är att gömma och skydda de riktiga IP-adresserna man har på sitt nätverk samt försvåra andra »utifrån« att ansluta sig till nätverket. Med andra ord en enklare brandvägg (se nästa kapitel).

Oftast så används privata nät (kapitel 4.7.1) på insidan routern.

5.2.2 Brandvägg

Någon sa att en brandvägg inte är något mer än en »router med attityd«. En kort men korrekt beskrivning.

Nu har inte en brandvägg alla finesser som en router har, men den har istället några andra funktioner som gör att namnet passar bra.

En brandväggs huvuduppgift är att stå emot intrångsförsök likt en »riktig« brandvägg ska stå emot brand. Den riktiga brandväggen är säkerhetsklassad att klara utav brand ett visst antal minuter, så parallellen med nätverksbrandväggen är att den inte stoppar allt...

Brandväggen stoppar allt utan regler. Dessa regler talar om vilken trafik som är tillåten samt åt vilket håll den får flöda. Beroende på hur avancerad brandväggen är så kan man konfigurera reglerna till att tillåta eller stoppa allt ifrån en IP-adress och port till vilket innehåll på webbsida som får visas.

- Personlig brandvägg, typ »ZoneAlarm«.
- Brandvägg på nätverksskiktet, dessa filtrerar på IP-adress samt port, typ »Packet Filter« i OpenBSD.
- Brandvägg på tillämpningsskiktet, dessa filtrerar på innehåll i webbsida eller e-brev, typ »webproxy« för surfning eller »Checkpoint Firewall-1« (som även jobbar på andra skikt).

En personlig brandvägg har redan en regeluppsättning som passar de flesta samt att den anpassar dessa regler med frågor till användaren. De jobbar på nätverksskiktet men för även en tabell på vilka applikationer som kommunicerar på nätverket. Man kan då se om »notepad.exe« plötsligt får för sig att skicka iväg paket till någon IP-adress på Internet (troligtvis har någon bytt ut originalet). Personliga brandväggar finns i gratis versioner att hämta hem ifrån Internet.

Brandväggar som jobbar på nätverkskiktet kräver nästan ingen processorkraft alls. De kan med lätthet klara utav en stor mängd trafik på den billigaste processorn idag. Även gamla 486:or jobbar idag som paketfiltrerande brandväggar.

Den dyraste och mest komplicerade brandväggen är den som jobbar på tillämpningsskiktet. Dels kostar mjukvaran en hel del samt att hårdvaran behöver vara betydligt snabbare än paketfiltrerande. Dessa brandväggar räknas som de bästa då man kan filtrera på tillämpningsskiktet samt att den har speciella tillämpningsprogram som jobbar som mellanhand samt analyserar protokollet efter fel.

5.3 E-post

5.3.1 Virus, maskar, trojanska hästar och annan ohyra

Dessa behöver knappast någon förklaring då alla någon gång fått eller hört talas om dessa elakingar. Kan dock ta upp några viktiga punkter som kanske är mer okända.

Jag buntar ihop virus, trojanska hästar, spionprogram och maskar i namnet »skadeprogram« (engelskans »malware«).

Antivirusprogram skyddar, men skyddar inte alltid. När ett nytt skadeprogram »släpps« ut i det fria så måste antivirusföretagen först få tag på det innan de kan stoppa in ett skydd i sin databas. De måste även analysera och skapa ett »fingeravtryck« samt uppdatera databasen för antivirusprogrammet. Det kan ta några timmar innan allt är gjort.

Du måste sedan uppdatera ditt antivirusprogram så att din dator får den senaste databasen. Detta bör göras dagligen om man vill ha skydd.

Skadeprogrammen kan orsaka en hel del mer än man kanske kan tro. Till en början så var de mer »ofarliga« än idag. För att nämna några saker som de kan göra idag, förutom att sprida sig via filer, nätverk, e-post och ICQ så är det:

- Öppnar upp möjligheten att skicka e-post via din dator. Några skadeprogram har även en helt egen e-postserver inbyggd.
- Spela in lösenord via tangentbordet och skicka de till skaparen av skadeprogrammet via e-post eller annat sätt.
- Radera filer, alla eller t.ex bara Office filer.
- Öppna portar så att datorn kan användas som mellanhand för surfning eller intrång. Din IP-adress står då som avsändaren i dessa paket.
- »DDoS« som står för »Distributed Denial of Service«. En mycket avancerad och kraftfull form utav tjänsteblockering. En DDoS attack består utav massor med infekterade datorer som styrs utav en »herre«. Dessa »slavar« kan då helt slå ut ett stort företags nätverk eller t.ex webbserver.
- Automatisk intrång hos andra i andra tjänster och sedan skicka resultatet tillbaka till skaparen av skadeprogrammet.

- Sprida dina filer via e-post till alla e-postadresser den får tag på.
- Radera BIOS så att datorn blir helt obrukbar.
- Tidsbomb, inget sker förrän ett visst datum och klockslag och sedan kan något utav ovan inträffa.

Spionprogram har en annan funktion än de jag beskrivit ovan. De kan rikta om länkar så att du kommer till deras webbsidor eller öppnar nya fönster med reklam. Ens webbsurf vanor analyseras och skickas till företag som använder det till att tjäna pengar. Dessa program ställer även till med sega ner surfningen samt krascher för program och operativsystem.

Som jag skrev i inledningen till detta kapitel så kan man inte skydda sig helt. Man måste dagligen uppdatera sitt antivirusprogram samt vara mycket vaksam på de filer man får skickat till sig även om det är ett känt namn. Är man minsta tveksam så är det bättre att ringa upp personen som står som avsändare eller vänta en vecka innan man tittar närmare på det.

Skadeprogram så som virus utnyttjar människans nyfikenhet, tillit och vilja att hjälpa till. Så var vaksam när får ett e-brev eller annat som tycker att du ska starta programmet för att det är så vackert, eller skicka ditt lösenord för att internetleverantören slarvat bort det.

Det finns enligt Symantec ~67000 olika virus varav den absolut största majoriteten är för Windows. Så om ni använder det operativsystemet så rekommenderar jag starkt att installera antivirusprogram.

Har ni inte råd till ett kommersiellt så finns det lite enklare att ladda ner utan kostnad ifrån dessa leverantörer:

- AVG Anti-Virus ifrån http://www.grisoft.com/
- AntiVir Personal Edition ifrån http://www.freeav.com/

Tyvärr så har inte många tillverkare utav antivirusprogram lagt med spionprogram till deras databas. Man måste då använda sig utav ännu ett till program för att »städa« i sin dator. »Spybot« och »Ad-aware« är namn på två utav dessa som kan städa upp i datorn. Även dessa program bör uppdateras, dock inte lika ofta som ett antivirusprogram.

- Spybot ifrån http://www.spybot.info/
- Ad-aware ifrån http://www.lavasoft.de/

5.3.2 Spam

Spam är även det något oönskat i sin e-brevlåda. Oönskad kommersiell reklam om sexprodukter eller piratkopierade program är inte helt ovanligt. Man önskar att man enkelt kunde sätta upp en »ingen reklam tack!«, och slippa allt.

Men så enkelt är det inte. Andra åtgärder är nödvändiga om man vill minska mängden »brus« i sin e-postlåda.

Från och med första april 2004 så är det förbjudet att skicka e-postreklam *inom* hela EU. Du kan anmäla överträdelser på:

`http://www.epostreklam.konsumentverket.se/`

För att minska mängden ännu mer så kan man använda sig utav en internetleverantör som filtrerar direkt i deras e-postservrar.

Det går även att filtrera själv om man använder t.ex »Mozilla«[8] som sin e-postklient. Dessa filter lär sig vad som är spam med hjälp utav statistisk analys utav orden. Då markerar bara de e-brev som du vet är spam och på det sättet lär sig programmet. Även andra e-postklienter har denna finess.

Även om det står i spam e-brevet att man ska anmäla utträdelse ut deras utskick så gör det *aldrig*! Det är bara ett sätt för dem att veta att just din e-postadress är en som någon läser.

Till och med spam med bilder gör att de vet att din e-postadress är valid. Bilderna ligger inte med i e-brevet utan på en webbserver samt att en unik kod läggs med i adressen till bilden. När du öppnar upp e-brevet så kommer din e-postklient att gå ut på Internet och hämta hem bilden ifrån just den adressen med unika koden. De kan då koppla din e-postadress med unika koden och på det sättet veta att e-postadressen är något att skicka mer till.

E-postadresserna får spammarna via webbsidor, inlägg i nyhetsgrupper, virus, direktmeddelandetjänster (ICQ, MSN) samt att de prövar sig fram genom att bygga ihop sannolika e-postadresser till redan kända domännamn.

5.4 Operativsystem

5.4.1 "Patcha"

Ett känt citat är »alla program över 10 rader har fel i sig«. Så man ska hålla sina datorer uppdaterade!

Att uppdatera program och operativsystem kallas »patcha«. Ordet kommer ifrån engelskans »patch« som betyder »lappa« och det är precis det man gör, man lappar över säkerhetshålen. Även patchar för driftsäkerheten finns med i dessa uppdateringar.

Skulle ytterdörren eller ett fönster plötsligt vara svårt att stänga så känner nog alla ett visst obehag. Men när det gäller datorer så är det svårare att märka om en säkerhetsbrist plötsligt finns där.

Gå med i e-postlistor för din viktiga mjukvara eller operativsystem. De flesta tillverkare har en som enbart används när en viktig produktuppdatering skett. Då kan man lättare veta att det är dags att hämta hem uppdateringar.

Vill man inte gå med i e-postlistor så får man besöka deras webbsidor med jämna mellanrum för att se om man måste göra någon åtgärd.

Hämta *inte* hem uppdateringar eller nya versioner av programvara ifrån andra än tillverkaren!

[8] http://www.mozilla.org/

5.4.2 Aktiva tjänster

Vindsfönstret, källardörren, köksingången eller balkongvägen är välkända vägar som tjuvar eller andra skurkar tar när de ska in i ett hus eller lägenhet.

Samma sak gäller för datorer, stäng alla onödiga tjänster som inte används eller används väldigt sällan.

Inget nytt hus har alla fönster och dörrar öppna när det står tomt, men några operativsystem har alla tjänster igång ifrån start.

Det innebär att det till och med kan bli svårt att hinna patcha det nya operativsystemet utan att få intrång under tiden, om man gör det via Internet.

Lär dig hur du stänger utav och slår på tjänsterna för det operativsystem du använder. En mycket kort lista på vart du hittar det för ditt operativsystem:

Windows Detta gäller »2000« samt »XP«. Klicka med höger musknapp på »My Computer« och välj »Manage«, expandera sedan »Services and Applications« och klicka på »Services«. För varje tjänst som du vill avaktivera så klickar då med höger musknapp och väljer »Disabled« under »Startup type«. Ett tips är att till en början endast stoppa tjänsten genom att klicka på »Stop« knappen. Det bör göras om man är osäker på vad tjänsten har för syfte.

Unix Eftersom det finns så många versioner utav Unix så tar jag bara upp det som vanligtvis är gemensamt för dem. Kommentera alla tjänster som inte ska vara aktiva i »/etc/inetd.conf« genom att skriva ett »#« först på raden. Spara filen och starta om »inetd« med en »kill -HUP *pid*« där *pid* är processid för »inetd«.

Mac Som numera kör under namnet »Mac OS X« och bygger på Unix. Väldigt få nåbara tjänster är igång efter installation så inget behövs stängas utav. Om du vill verifiera eller slå på tjänster så gå in i »Systeminställningar« och klicka på »Fildelning«. Även den interna brandväggen kan slås på där,

Notera även att några operativsystem slår på avstängda tjänster efter att man patchat operativsystemet.

5.5 Säkra sin utrustning

En kort checklista för nyinstallation:

1. Låt *inte* datorn vara inkopplad i något nätverk.
2. Installera operativsystem.
3. Patcha operativsystemet om möjligt via CD eller liknande (bränn patchar på CD).
4. Stäng av tjänster som aldrig eller sällan behövs.

5. Installera antivirusprogram om du kör Windows.
6. Uppdatera virusprogram via CD eller liknande.
7. Installera övrig mjukvara.
8. Verifiera än en gång att inte onödiga tjänster är aktiva.
9. Gör en viruskontroll utav hela hårddisken.
10. Koppla in datorn på nätverket.

6 Licens

7 Förändringar

Datum	Namn	Kommentar
2004-04-19	Patric Fors	Första riktiga utkast, allt är dock inte klart.
2004-05-20	Patric Fors	Små uppdateringar efter igenomläsning utav andra ögon.
2004-05-29	Patric Fors	Mindre förändringar, rensade bort lite

8 Tack för Er hjälp!

- Janne Johansson

- Christian Borén
- Peter Johnsson
- Örjan Sjelvgren
- Peter Stenberg
- Andreas Suojanen