Datorkommunikation

Marcus Rejås
Rejås Datakonsult AB

marcus@rejas.se

Datorkommunikation

av Marcus Rejås

Publicerad $Date: 2011-01-19 20:09:27 $

Denna bok är anpassad för gymnasieskolans kurs datorkommunikation med kurskoden DTR1201 (appendix B). Den kan naturligtvis användas även i andra sammanhang.

Du kan köpa tryckta böcker från Rejås Datakonsult AB, se http://www.rejas.se.

Revisionshistorik

Revision $Revision: 1.62 $
Utvecklingsversion

Dedikation

Denna bok vill jag tillägna mina barn.

In Memorian Daniel Lundblad 1995--2008.

Innehållsförteckning

Tabellförteckning

Förord

Tack till

Jag vill börja denna bok med att tacka alla som hjälpt mig med den. Framför allt då *Johan Hammar*, *Gunnar Sjöö*, *Jenny Ohlsson* och *Kalevi Nyman* som ställt upp med korrekturläsning och *XXXX XXXX* som ritat alla fina bilder. Utan er hade boken inte varit så bra som den är idag. Tack!

Jag vill också tacka dig som läser denna bok. Hittar du något som är fel eller som du tycker att man kan göra på något bättre sätt så tveka inte att höra av dig till mig. Min adress står i början av boken. Jag har mina begränsningar som författare men genom att släppa denna bok fri förväntar jag mig att du som läsare skall skicka mig kommentarer så att vi tillsammans kan göra den mycket bättre än vad jag och kanske du skulle ensamma. Några exempel på de som gjort detta är *Bengt Gördén* som gett mycket bra feedback om NAT, *Pär Lindskog* som gett bra feedback angående IMAP, *Jan Johansson* som bidragit med stycken om bryggor och repeatrar, *Torbjörn Ahlsén* som skrev och berättade att jag blandat ihop kablar och ledare, *Simon Schmidt* som hittade fel i kapitlet om Internet och *Marie Lundholm Janenge* som uppmärksammade att jag snurrat till det bland bilderna i kapitlet om datornätverk. Marie påpekade också att jag förkortat Media Access Unit felaktigt inte bara en eller två utan tre gånger. Tack alla för er hjälp!

Sist vill jag tacka min *Jenny* som står ut med att ha en datanörd hemmavid. Att skriva böcker för att ge bort dem samt att engagera sig i en massa öppna projekt vid sidan om mer än ett heltidsjobb tar sin tid och kräver mycket tålamod och förståelse av de nära. Allt det ger Jenny mig vilket jag är mycket tacksam för. Ni borde också tacka Jenny, utan Jenny -- ingen bok.

Några ord om denna bok

Jag vill också passa på att berätta lite om denna bok, varför jag skriver den, varför jag släpper den helt fritt och kanske varför den blev som den blev.

Det finns flera anledningar till att jag skriver denna bok. Den största anledningen är att jag till vardags håller bland annat denna kurs i en gymnasieskola. Jag har läst ett flertal böcker på området och tycker inte att någon lägger upp kursen på det sätt jag vill och vissa innehåller inte heller allt det som står i kursplanen. Jag har utgått från kursplanen när jag gjort denna bok så allt skall vara med. Man bör komplettera med labbar också eftersom kursplanen nämner en del praktiska moment. Det finns labbar att hämta på denna boks hemsida. Har du förslag på labbar, lektionsförslag, övningar eller annat så tveka inte att skicka dem till mig. Tillsammans kan vi göra ett suveränt kursmaterial som kan gagna både elever, lärare och skolor i framtiden.

Hur kommer det sig då att jag släpper denna bok fritt på Internet, med en licens som till och med låter andra ändra i den och/eller sälja den för att tjäna pengar? Jag brinner för något som kallas fri programvara. Fri programvara är programvara som du får använda fritt i vilket syfte du vill och vars källkod är öppen. Fri programvara har visat sig hålla mycket hög kvalitet och funktionalitet. Exempel på fri programvara är till exempel operativsystemet Linux, webbservern Apache och kontorsprogramsviten OpenOffice.org. Alla dessa tre har på sitt sätt hjälpt till att skapa och sprida denna bok. Till denna bok har uteslutande fria programvaror använts.

Även denna bok är fri. Du kan ladda ner den från Internet. Även de datafiler jag skrivit boken i finns där så att du kan förbättra den om du vill. Om du väljer att göra det så vill jag gärna veta det även om det inte är något tvång. Vad som däremot är ett tvång är att om du bygger vidare på denna bok så måste du släppa den lika fri som jag gjort (se licenstexten om du är osäker). Eftersom denna bok är skriven för och med fria programvaror så kommer de exempel som är i boken att vara för operativsystemet Linux och de program som brukar finnas med det. Använder du något annat operativsystem så kan du ändå ha nytta av boken.

Det finns naturligtvis andra skäl till att släppa en bok fritt på detta sätt. Det självklara är att alla kan hjälpas åt att göra den bättre, men det finns även mer praktiska fördelar. Det står skolan fritt att köpa denna bok i tryckt format. Tycker man att det är för dyrt eller tar för lång tid kan man trycka den själv. Man kan även läsa den online om man vill. Har någon elev glömt sin bok en dag så finns allt material fritt tillgängligt på Internet. Man får fritt kopiera hela eller delar av boken. Detta kan vara smidigt i händelse av att någon glömt sin bok eller om man bara vill behandla en liten del av den i en kurs. Hittas ett fel i boken kan detta rättas till och vara studenterna till hands redan nästa dag om man vill.

Men, som jag sagt, den största fördelen är att alla kan hjälpas åt för att göra denna bok bättre. Jag hoppas nu när jag skriver denna bok att det skall vara ett levande dokument som anpassas efterhand som tekniken förändras. Därför vill jag uppmuntra dig som läsare att skicka kommentarer, rättelser, nya avsnitt, förändrade avsnitt, m.m., m.m. till mig så för jag in dem i boken. Tillsammans kan vi göra en bok mycket bättre än vad jag själv skulle kunna åstadkomma. I gengäld får du ett bättre material och vad som brukar kallas för "credit", det vill säga ett omnämnande i boken för att visa vad du gjort. Att hjälpas åt på detta sätt för att göra det som blir bäst för alla, det är det som allt detta handlar om.

Marcus Rejås, Norrtälje 2004-01-11.

Kapitel 1. Inledning

I detta kapitel ges en liten introduktion till vad datorkommunikation är och går igenom några grundläggande begrepp.

Vad är data och vad är dator?

Det här är inte så lätt som man kan tro. Data är någon typ av fakta eller värden som kan bearbetas av människor eller maskiner men som ännu inte har tolkats. Till exempel så är en ström av bokstäver data. Man kan titta på bokstäverna utan att läsa ut vad de innebär, man kan flytta dem, skriva ut den, kopiera dem och så vidare. Bokstäverna kan bilda en mening men behöver inte nödvändigtvis göra detta för att vara data. På samma sätt kan en tabell med siffror utgöra data. Rätt tolkade kanske de utgör en viktig kalkyl för ett stort företag men utan att tolka dem så är det data.

En dator är en maskin som vi använder för att behandla data, till exempel en persondator eller en server i ett nätverk. Man hör ofta att någon säger "Jag slog på datan." när de egentligen menar, "Jag slog på datorn.", såvida de inte faktiskt stod och slog på cd-skivan eller vad det nu kan vara för något som innehåller data.

Vad är information?

Data som tolkats och förståtts av en människa kallas för information. Till exempel så är en bild som sparats på en disk data ända tills den presenterats av ett bildvisningsprogram för en människa som förstår bilden, då först är det information. På samma sätt så är strängen med bokstäver i exemplet ovan data tills dess att de läses av en människa som kan tolka dem. Då blir det information.

Några exempel kan vara på sin plats. 10 är data. Men om 10 sätts i ett sammanhang som man kan tolka, till exempel "lådan väger 10 kilo", så blir 10 information. På samma sätt är 23 data medan det blir information om man vet att det handlar om temperaturen i Pajala i Celsiusgrader.

Alltså data som presenteras (tolkats och givits en innebörd) på ett sätt som direkt kan förstås av en människa är information. Information kan inte flyttas mellan två datorer men data kan. Information kan inte sparas ned på en disk men data kan. Data kan, om den är rätt utformad, tolkas till information.

Vad är kommunikation?

Kommunikation är ett vitt begrepp. Vi använder det för att benämna till exempel ett samtal eller att vi själv förflyttar oss med till exempel tåg eller buss. Kommunikation kommer från det latinska ordet communicatio som betyder ungefär "att utbyta" eller "att delge". Ordet kommunikation kan, som du vet, användas på flera olika sätt och alla är riktiga. Men i denna bok och i ämnesområdet datorkommunikation betyder kommunikation att man utbyter information. Som vi konstaterat tidigare så kan inte information skickas mellan två datorer men data kan. Data plus regler för hur dessa data skall tolkas kan ju göras om till information.

Vad är datorkommunikation?

Datorkommunikation är ju vad denna bok skall behandla, så vad är det för något? Datorkommunikation är när människor utbyter information med varandra med hjälp av datorer. Som vi sett så kan bara datorerna utbyta data så det måste även finnas regler för hur denna data skall kunna tolkas till information i slutändan för att det skall vara någon mening med kommunikationen. Under kommunikationens gång kan data behandlas av system eller datorer som inte har vetskap om vad dessa data betyder. Dessa är en del av kommunikationsprocessen. Till exempel så är telefonen en del av ett telefonsamtal men det är inte telefonen som kommunicerar utan det är du och den som håller i luren på andra sidan som kommunicerar. Trots detta är telefonen, ledningar och telefonväxlar ett led i kommunikationen.

Sammanfattning

I detta kapitel har vi lärt oss vad några grundläggande begrepp inom datorkommunikationsämnet står för. Detta kapitel avslutas, liksom de resterande kapitlen i boken, med några kontrollfrågor eller övningsuppgifter som du kan använda för att kontrollera att du lärt dig det som kapitlet handlade om.

Kapitel 2. Dataöverföring

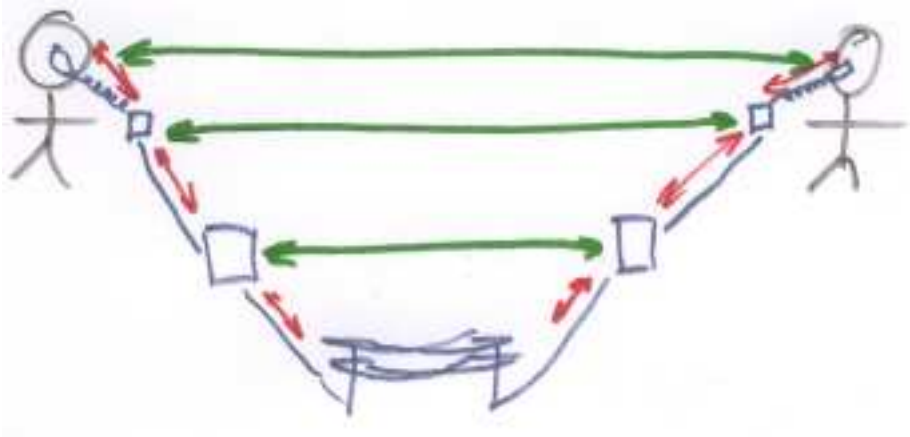
Detta kapitel behandlar hur data kan föras över mellan två olika noder i ett system genom en kabel eller på annat sätt som till exempel radio eller som infrarött ljus.

Inledning

I slutet på det förra kapitlet nämndes ett telefonsamtal som ett exempel på kommunikation. Två personer kommunicerar med varandra. Om man bryter ner samtalet i olika lager så ser vi att personerna egentligen inte talar med varandra utan de båda talar egentligen med sin telefon. Telefonerna i sin tur talar med varandra med hjälp av telenätet. Telefonerna utbyter data med varandra men är ovetande om innebörden. Telefonerna presenterar data i form av ljud som personerna som för dialogen förstår och omsätter till information. En hel del regler måste finnas och följas för att kommunikationen skall fungera.

I figur 2-1 visas en skiss på ett sådant telefonsamtal. Det är inte meningen att förklara hur telefonnätet fungerar. Häng inte upp dig på detaljerna utan fokusera på principen med de olika skikten. I figuren är alla protokoll ritade som pilar. Tänk på att de olika delarna upplever att de talar horisontellt med sin motpart på andra sidan när de egentligen talar nedåt eller uppåt på sin egen sida.

Figur 2-1. Ett telefonsamtal



Personerna som samtalar måste följa en mängd regler som båda känner till, och som de i förhand kommit överens om, för att samtalet skall ha någon mening. Till exempel så måste de komma överens om att tala en i taget och tala ett språk som de båda förstår och följa de regler som finns i detta språk. Man kan säga att detta är det *protokoll* som de följer.

Nu är det ju inte så att dessa två personer talar med varandra direkt, utan de talar ju egentligen med sina telefoner. Telefonerna i sin tur talar sedan med den andra telefonen med hjälp av en mängd komponenter som till exempel växlar och kablar. Alla dessa komponenter måste samarbeta enligt givna protokoll för att det skall fungera. Telefonerna skickar och tar emot elektriska strömmar som bildar ljud. Dessa måste se ut på ett visst sätt för att telefonerna skall förstå dem. Vidare måste alla delar i telefonnätet vara överens för att man skall vara så säker som möjligt på att de strömmar som kommer ur en telefons högtalare skall vara så lika som möjligt som de som kommer in i den andra telefonens mikrofon.

Om alla delar i denna kommunikation fungerar så kommer samtalet att vara givande.

Duplex, Simplex och Halv-duplex

Man kan dela in kommunikation beroende på i vilken rikting den kan gå. Simplex innebär att kommunikation bara kan ske åt ett håll. Ett bra exempel på det är TV eller radio-utsändningar. Du kan bara lyssna (och titta) på det som sägs, men inte säga något tillbaka. Duplex (kallas ibland även full-duplex) innebär att du kan svara och säga emot den du kommunicerar med det vill säga ni kan tala i munnen på varandra och kommunikationen kan flyta åt båda håll på samma gång. Ett exempel på duplex är ett vanligt telefonsamtal. Ett mellanting mellan simplex och duplex är halv-duplex. Med halv-duplex kan kommunikationen ske åt båda hållen, men bara åt ett håll i taget. Ett exempel på detta är kommunikationsradio där man inte kan tala i munnen på varandra utan en sänder och andra lyssnar.

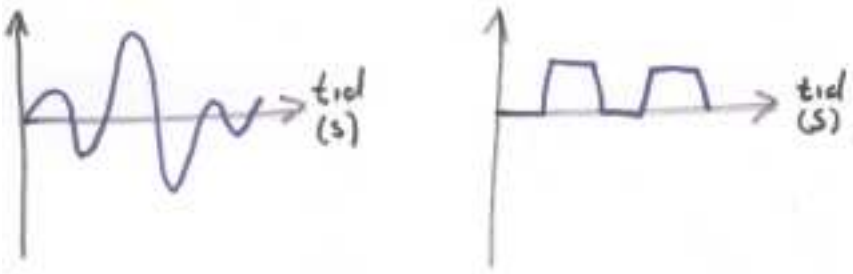
Analog och digital överföring

Data som förs över en ledning skickas som elektriska pulser eller signaler på ett eller annat vis. Beroende på vilket protokoll som används så kan data packas in i dessa strömmar på olika sätt. Till exempel så kan en hög spänning betyda en sak och en låg spänning något annat.

I telefonexemplet så var det ljud som fördes från en telefon till en annan. Ljud är exempel på analoga data [1]. Spänningen varierar beroende på vilket ljud som kommer i mikrofonen på den ena telefonen och spelas upp på motsvarande sätt i den andres hörtelefon. Man kan jämföra analoga signaler med en vattenkran. Om man öppnar mycket kommer mycket vatten och öppnar man den lite kommer det lite vatten. Man kan variera exakt hur mycket vatten man vill skall komma fram vid varje tidpunkt. Digitala signaler kan man istället jämföra med en strömbrytare som antingen kan slå på eller av strömmen. Man kan inte med en vanlig strömbrytare sätta på strömmen lite grann.

1. Även analoga data kan överföras digitalt bara man kommer överens om vilket protokoll som skall användas för att packa in dessa analoga data i ett binärt format.

Figur 2-2. Analoga och digitala signaler



Amplitud och frekvens

I figur 2-2 så ser vi exempel på en analog och en digital signal. Vi ser att båda två går upp och ned. Ibland är de höga och ibland är de låga. Avståndet mellan det höga läget och det låga läget kallas för signalens amplitud. I vilken enhet den mäts beror på vilken enhet som finns på y-axeln i diagrammet. Vanligt är att den mäts i Volt.

Hur många gånger per sekund en kurva växlar mellan lågt och högt värde kallas för frekvens. Den mäts i enheten Hertz (Hz) som är samma sak som antal per sekund. Vid höga frekvenser används Kilo Hertz (kHz), Mega Hertz (MHz) eller till och med Giga Hertz (GHz).

Mer om digital dataöverföring

När man talar om datorkommunikation menar man så gott som alltid digital dataöverföring. Datorn fungerar digitalt både inom en och samma maskin och när den kommunicerar med andra datorer.

Du har kanske hört att en dator bara känner till ettor och nollor. Detta verkar ju hänga bra ihop med liknelsen med en strömbrytare ovan eller att kurvan bara kan vara låg eller hög. Och visst hänger det ihop. En dator använder bara ettor och nollor för att hantera data och dessa representeras ofta av låga och höga spänningar, precis som i vårt lilla exempel ovan.

Men hur kan man få ut något av en etta eller en nolla? Jodå, det går alldeles utmärkt bara det finns många ettor och nollor. En datamängd som kan vara ett eller noll är den minsta möjliga datamängden. Den kallas för en *bit*. Alltså något som kan vara ett eller noll är en bit. Ordet bit kommer från engelskans *Binary Digit* som betyder binär siffra. Binär är samma sak som tvåfaldig. Men en bit har man ingen större nytta av. Oftast klumpar man ihop några bitar för att få en datamängd som är något större. Om man har en bit så finns det ju bara två alternativ (0 och 1), men har man 8 bitar så finns det betydligt fler alternativ (till exempel 11001010 och 01010111). Det är

vanligt att man jobbar med just 8 bitar som kallas för en *byte*. Ordet byte kommer från engelskans "By eight" En byte kan anta 2^8=256 olika kombinationer.

Något om talbaser

Normalt när vi räknar och talar om siffror så menar vi underförstått att vi använder talbasen 10. Vi bygger våra tal av 10 olika siffror (0-9) och grupperar upp ett tal i ental, 10-tal, 100-tal, 1000-tal och så vidare. 1, 10, 100 och 1000 är potenser av 10 10^0, 10^1, 10^2, 10^3. Precis på samma sätt kan man räkna med andra talbaser, till exempel 2 (binärt), 8 (oktalt) eller 16 (hexadecimalt).

Talet 13 kan beskrivas som $1*10^1+3*10^0$=13. Det vill säga ett 10-tal och 3 ental. I det binära talsystemet har vi bara två siffror (0 och 1) och istället för ental, 10-tal och så vidare så har vi ental, 2-tal, 4-tal, 8-tal, 16-tal och så vidare eller 2^0, 2^1, 2^2, 2^3, 2^4 och så vidare. Skall vi binärt skriva 13 så behöver vi, enligt samma principer som i vår decimalsystem, ett 8-tal, ett 4-tal, inget 2-tal och ett ental eftersom $1*2^3+1*2^2+0*2^1+1*2^0$=13. Talet 13 skrivs alltså som 1101 binärt.

Eftersom datorn bara jobbar binärt med bitar så hanterar datorn tal i binärform. Ofta när man jobbar inom datateknik och programmering så använder man sig av binära tal. Som vi sett så går det ju utmärkt att konvertera mellan det binära talsystemet och det vanliga decimala. Som vi också ser så är 1101 mycket längre och svårare att överblicka än till exempel 13. Det gör att man i praktiken sällan jobbar med binära tal. Ofta räknar man istället med talbasen 8 eller 16. Dessa är fortfarande potenser av 2 och passar bra in i datorsammanhang men talen blir mindre och enklare. Det vanligaste är talbasen 16 eller hexadecimala tal som det kallas. Eftersom vi har talbasen 16 måste vi ha 16 stycken siffror. Våra vanliga siffror räcker inte till utan man brukar lägga till bokstäverna A-F också och behandla dem precis som om de vore siffror. Vi har alltså siffrorna 0123456789ABCDEF. Vi bygger tal av ental, 16-tal, 256-tal, 4096-tal och så vidare. Eller om vi uttrycker det som ovan 16^0, 16^1, 16^2, 16^3 och så vidare. Skall man skriva talet 13 binärt så behöver vi bara D (=13) stycken ental. Talet 13 skrivs alltså D hexadecimalt.

Bit, Byte kByte, ...

Inom matematiken har vi sedan länge lärt oss att prefixen kilo (k), Mega (M) och Giga (G) betyder 10^3, 10^6 respektive 10^9. Inom datorvärlden där mycket utgår från binära tal så är inte dessa tal speciellt jämna. De tal som är jämna i ett binärt talsystem är, översatt till decimaltal, talen 4, 8, 16, 32, 64, 128, 256, 512, 1024, osv. Kanske känner du igen dessa tal om du någon gång köpt till exempel minne till din dator. Detta har också gjort att man inom datorvetenskapen definierat om våra vanliga prefix. Kilo betyder istället för 1000 (10^3) i sammanhanget kByte istället 1024 (2^{10}). Mega betyder 1024*1024 eller 2^{20} eller som det blir decimalt, 1048576. Detta leder förstås till en del missförstånd, men eftersom talen ligger relativt nära varandra så blir det sällan några större problem.

Men det kan vara svårt att veta om man till exempel köpt en hårddisk på 1 GByte om den rymmer 10^9=1000000000 eller 2^{30}=1073741824 bytes.

Märk också, när vi har enhetsförväxlingar på tapeten, att dataöverföringshastigheter oftast mäts i bitar/sekund och inte i bytes/sekund. Där gör det större skillnad eftersom skillnaden är ungefär en faktor 10.

ASCII-tabell

Vi har nu sett att man binärt kan uttrycka tal. Till exempel så var ju 1101 talet 13. Ofta så vill man istället för tal representera text eller bokstäver. Detta går till på så sätt att man låter olika tal representera olika bokstäver enligt en tabell. Ett exempel på en sådan tabell är ASCII-tabellen. ASCII står för *American Standard Code for Information Interchange* och är en standard för hur tecken skall representeras binärt i form av siffror från standardiseringsorganet ANSI. Ett exempel på en (utökad) ASCII-tabell visas i tabell C-1.

Sammanfattning

I detta kapitel har vi behandlat på vilket sätt olika protokoll kan jobba både beroende till varandra och oberoende av varandra i en och samma kommunikationsmodell. Vi har också tittat på vad som menas med analog och digital överföring och vilka karakteristiska egenskaper dessa har. Vi har lärt oss ytterligare några begrepp och lite om matematiken med olika talbaser och varför man i datorvärlden så ofta uttrycker tal hexadecimalt.

Kapitel 3. Seriell och parallell kommunikation

Här behandlas seriell och parallell dataöverföring. Vad skiljer dem åt och hur fungerar det.

Seriell och parallell kommunikation

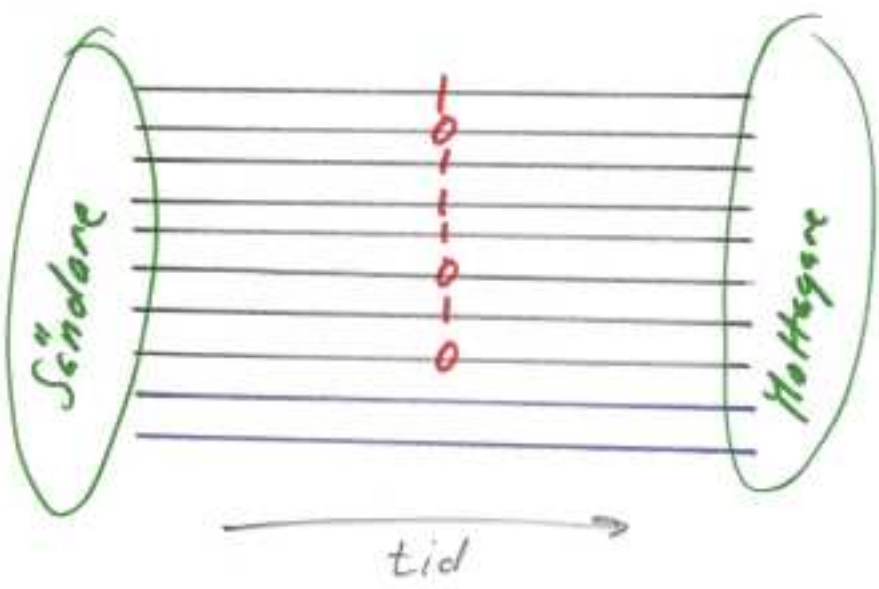
Skillnaden mellan seriell och parallell kommunikation hörs nästan i namnet. Vid seriell kommunikation skickas bitarna i en rad efter varandra och vid parallell kommunikation skickas flera bitar i bredd, samtidigt. Det kan naturligtvis inte finnas flera bitar på en ledning samtidigt utan de åtskiljs av tiden. Ledningen kan ju bara i ett ögonblick vara antingen 0 eller 1. Men liknelsen fungerar i alla fall.

Seriell kommunikation lämpar sig bäst då data skall transporteras längre sträckor och parallell kommunikation används bara för att transportera data kortare sträckor.

Parallell kommunikation

Parallell kommunikation innebär som tidigare nämnts att data-bitarna skickas parallellt i grupper. Detta innebär att några förutsättningar måste finnas. Får det första så måste det finnas en ledning för varje bit som skall åka i bredd. Tänk på en motorväg, fyra bilar lastade med ettor eller nollor kan bara åka parallellt om det finns fyra filer på vägen. Vidare så måste filerna vara likvärdiga för att en grupp bilar ska komma fram samtidigt. Om en fil är långsammare än de andra så kommer överföringen att bli långsammare och om det blir problem på en fil så kommer överföringen naturligtvis att hindras. Se figur 3-1.

Figur 3-1. Parallell överföring



När vi talar om datorkommunikation är det naturligtvis inte filer på en motorväg vi talar om utan om ledningar. Ju fler ledningar i bredd desto snabbare dataöverföring. Eftersom parallell överföring lämpar sig bäst för korta avstånd är det denna typ av kommunikation som används inuti en dator för att flytta data mellan minnet, processorn och andra enheter som till exempel diskar och minnen. Vanligtvis idag så har dessa databussar, som det kallas, 32 ledningar i bredd men 64 blir allt vanligare. Även 8 och 16 ledningar förekommer men det är inte lika vanligt.

Eftersom en ledning med 32 kablar i bredd kan överföra 32 bitar i taget brukar en sådan ledning kallas för en 32-bitars buss.

Som nämnts tidigare så används parallella anslutningar oftast inom datorn men det kan också användas för att ansluta yttre enheter. Vanligaste enheten som ansluts till en dator parallellt är en skrivare men även lagringsenheter, skannrar och annat förekommer med parallell anslutning. Den parallella anslutning som finns på de flesta PC kallas normalt för parallellport eller skrivarport. figur 3-2 visar hur en parallellport eller skrivarport ser ut.

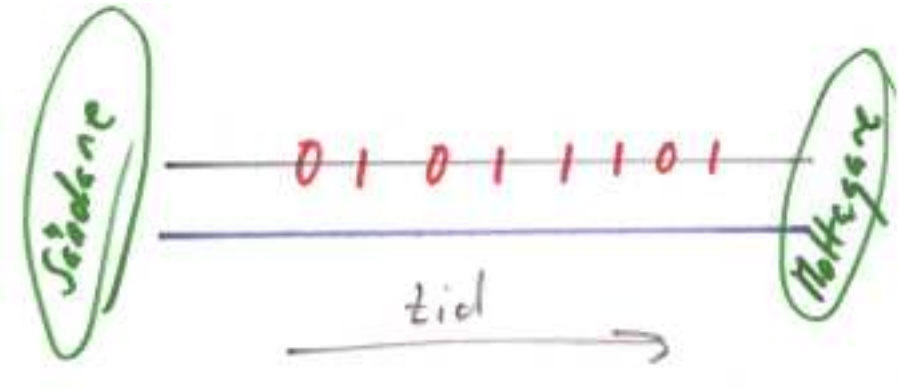
Figur 3-2. Parallellport eller skrivarport

Den största nackdelen med att ansluta utrustning till datorn via en parallellkabel är att denna kabel måste hållas kort. För skrivare som inte är så krävande kan den vara omkring 5 meter medan den om man har mer krävande utrustningar som till exempel diskar bara kan ha en kabel på omkring en meters längd.

Seriell kommunikation

Till skillnad från parallell kommunikation så behövs det i seriell kommunikation egentligen bara en ledare. I praktiken så behövs det oftast åtminstone två men man kan se det som en. Ofta har man en ledare för trafik i den ena riktningen och en för trafik i den andra riktningen plus några ledare för kontrollsignaler.

Figur 3-3. Seriell överföring



Seriell överföring är normalt långsammare än parallell överföring men är inte lika störningskänslig och man kan ha kablar som är upp till 40 meter långa.

På en PC kan det finnas lite olika seriella portar. En lite äldre som normalt kallas en serieport eller som den lite mer strikt heter RS-232 (Recommended Standard 232, från ett Amerikanskt standardiseringsförbund). Denna kan se ut på två olika sätt, antingen med 9 poler eller med 25. Dessa två fungerar likadant men ser olika ut. Den med 25 poler blir mindre och mindre förekommande eftersom den tar större plats.

Något som blir vanligare och vanligare både på PC och bland tillbehör är något som kallas för USB (Universal Serial Bus) som används för att koppla tillbehör till en dator. Den har mycket högre överföringskapacitet än den äldre RS-232. Även USB finns i två utföranden. Den större är vanligast att man hittar på datorer och i kopplingar medan den mindre ofta hittas på utrustningar som till exempel kameror, skannrar och diskar där utrymmet ofta är mindre. I figur 3-4 visas de vanligaste typerna av serieanslutningar och motsvarande kablar. De två uttagen till vänster är RS-232 portar. Dessa kallas vanligvis bara för serieportar. De två till höger är USB-anslutningar. Under alla portar visas motsvarande kabel.

Figur 3-4. Olika seriella portar och motsvarande kablar

För att seriell överföring skall fungera så måste data skickas på ett visst sätt genom kabeln. Annars fungerar det naturligtvis inte. Man skiljer på två olika sätt att överföra data seriellt, nämligen *synkront* och *asynkront*. Att skicka data asynkront är det vanligaste.

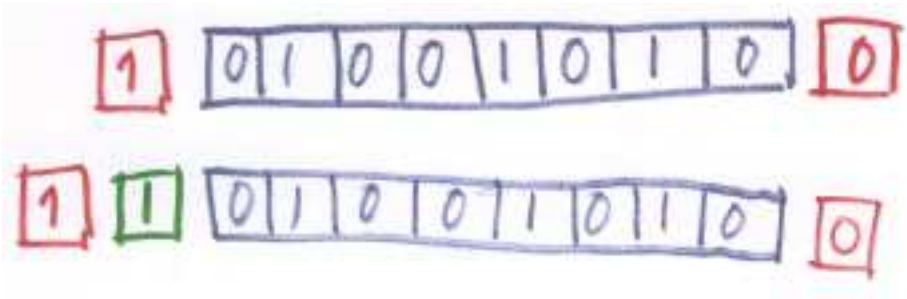
Synkron överföring

Synkron överföring innebär att databitarna skickas i så kallade datablock. Varje datablock kan innehålla hundratals bitar. Hur många framgår av de regler (protokoll) som gäller för överföringen. För att de parter som utbyter data på en synkron förbindelse skall veta var de är så måste de ha en gemensam klocka så att parterna kan hålla takten. Vidare så måste båda parterna ha tillgång till ett buffertminne för att kunna samla upp datablock och kontrollera dem. Parterna måste också kunna förbereda ett datablock för sändning.

Asynkron överföring

Det vanligaste när man talar om seriell kommunikation är asynkron överföring. Med asynkron överföring skickas data tecken för tecken och inte block för block. Det ger lite större *overhead* eftersom varje tecken måste kontrolleras. Med overhead menas sådan trafik som inte direkt är nyttig men som krävs för överföringen. Mycket overhead ger större slöseri med bandbredd än lite overhead. Man kanske kan jämföra med ett lastfartyg. Skall man flytta säd eller kaffe över jorden måste man även transportera bränsle till fartyget och mat till besättningen. Denna last måste vara med för att skeppet skall komma fram men ingår inte i den last för vilken någon betalar. Bränslet och maten utgör då overhead.

Figur 3-5. Start- och stoppbit



Schematisk bild över ett tecken . Den första biten kallas startbit. Sedan kommer de databärande bitarna och sist kommer det en stoppbit. Startbiten och stoppbiten utgör overhead.

I figur 3-5 visas hur ett tecken som skall skickas över en asynkron seriell förbindelse kan se ut. Lägg märke till att bilden kan verka felvänd, den första biten som skickas är den som är längst till höger i bilden. Först skickas en startbil som alltid är en 0:a, sedan kommer de bitar som utgör det data som skall skickas, det är normalt 7 eller 8 stycken. Sist kommer eventuellt en paritetsbit om vi kommer att behandla längre fram och en eller eventuellt två stoppbitar. Startbiten, stoppbiten och eventuell paritetsbit utgör overhead.

Om bara en start och en stoppbit används så kommer det att innebära att två bitar ber byte är overhead. Det är ganska mycket men de fördelar som finns, bland annat billiga utrustningar och möjligheter att ha långa kablar, gör att det ändå är värt denna overhead.

Man kan använda sig av något som kallas *paritet*. Syftet med paritet är att lägga till en enkel felkontroll på överföringen. Det fungerar så att man läggar till en bit innan stoppbiten eller stoppbitarna. Man skiljer på *udda* och *jämn paritet*. Vid jämn paritet skall summan av alla ettor, inklusive paritetsbiten utgöra ett jämnt tal och vid udda paritet ett udda tal.

Sändaren beräknar och lägger till paritetsbiten när tecknet skickas och mottagaren beräknar och

kontrollerar paritetsbiten. Om den inte stämmer överens med det förväntade har något fel inträffat i överföringen.

En enklare form av paritet kallas etta eller nolla. Då lägger man till en paritetsbit som alltid är en etta eller nolla.

Sammanfattning

I detta kapitel har vi tittat på seriell och parallell kommunikation. Vi har lärt oss vad som skiljer dem åt och vilka för- respektive nackdelar de har. Vi har lärt oss att seriell kommunikation i huvudsak kan gå till på två olika sätt och hur dessa fungerar. Vi har också lärt oss begreppet overhead och dess betydelse vid seriell kommunikation.

Kapitel 4. Datornätverk

Att ansluta datorer till nätverk är idag regel snarare än undantag. Alla nya datorer som säljs kan kompletteras med nätverkskort och de flesta har det som standard redan från början.

I detta kapitel tittar vi närmare på hur ett datornätverk byggs upp, vad topologier är och hur de ser ut och hur man kan sammanbygga flera mindre nät till ett stort.

Inledning

I det förra kapitlet tittade vi på seriell och parallell överföring. Vid sådan kommunikation är det alltid två parter som talar med varandra. I detta kapitel tittar vi lite längre upp ser hur man bygger mer avancerade kommunikationsnät med en mer avancerad struktur där datorer efter givna regler kan kommunicera med varandra. Dessa nät kallar vi kort och gott för datornät.

Ett datornätverk är ett system som består av två eller flera datorer som kopplats ihop så att det kan utbyta data med varandra. Ett litet nätverk kan kopplas ihop med ett annat för att bilda ett större nätverk. Det största nätverket som finns är Internet som består av extremt många nätverk, både stora och små.

LAN, WAN, MAN

Man kallar nätverken för olika saker beroende på hur stort område de sträcker sig över. Det vanligaste är det som kallas för *LAN, Local Area Network* som är ett nätverk som oftast håller sig inom samma byggnad. Det finns dock inget som hindrar att även ett LAN utbreder sig mellan flera byggnader eller ett campus. På svenska säger vi lokalt nätverk eller just LAN som är den engelska förkortningen. Allt från små hemmanätverk till ganska stora företagsnätverk hör till denna grupp.

Ett nätverk som sträcker sig mellan flera byggnader, inte sällan långt från varandra, eller mellan olika städer kallas för ett *WAN, Wide Area Network*. Ett WAN består oftast av två eller flera LAN som kopplats ihop till ett större WAN. Ett exempel på ett WAN är Internet.

Storleksmässigt mellan LAN och WAN finns något som kallas för *MAN, Metropolitan Area Networks*. Ett MAN är större än ett LAN och kopplar ihop LAN inom ett begränsat område, till exempel en stad, med hög kapacitet. I Sverige är stadsnäten exempel på olika MAN. MAN är ett

nyare begrepp än de andra två och används inte så ofta. Det är inte fel att säga WAN om ett MAN eftersom ett MAN också består av flera LAN.

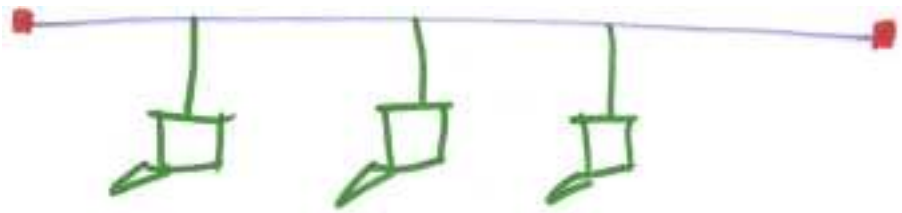
Topologier

Ett lokalt datornätverk (LAN) kan byggas på en mängd olika sätt. Både logiskt och fysiskt kan man välja olika lösningar. Hur ett nätverk strukturellt är uppbyggt kallar vi för *topologi*. En topologi kan beskriva både hur nätet ser ut fysiskt (hur kablar är dragna) och hur det ser ut logiskt. De topologierna som används är: *bussnät*, *stjärnnät* och *ringnät*.

Bussnät

I ett bussnät finns det en kabel till vilken alla datorer är kopplade. Till den gemensamma kabeln (kallas för backbone) kopplas datorerna med så kallade drop-cables. I figur 4-1 visas en schematisk bild av ett bussnät. Överst i bilden är backbone-kabeln med terminatorer i ändarna. Från den går så kallade drop-cables till de olika datorerna på nätverket.

Figur 4-1. Bussnät



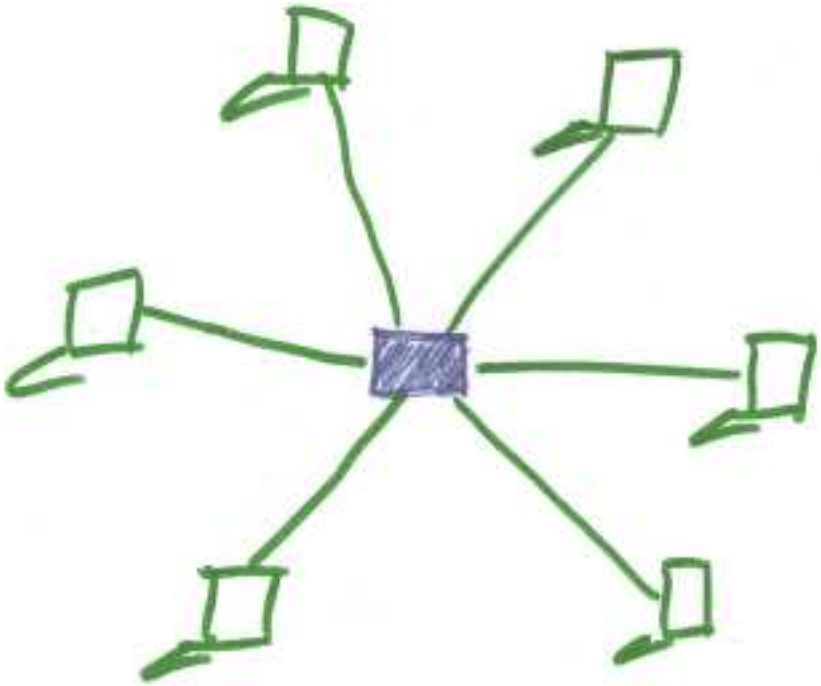
Bussnätverk är relativt billiga att installera. Ett problem med dem är att alla delar av nätet är beroende av backbone-kabeln. Bara en dator i taget kan sända ut data på nätet. Detta leder till att nätverket blir långsammare ju fler datorer som ansluts. För att signaler på backbone-kabeln inte skall kunna studsa fram och tillbaka (och så på sätt ockupera nätet längre än nödvändigt) så måste backbone-kabeln ha *terminatorer* i båda ändarna. Terminatorn är egentligen ett motstånd som dämpar signalen.

Stjärnnät

I ett stjärnnät kopplas alla datorer till en central punkt som kallas för *hub*. Hub, som brukar försvenskas till hubb, är engelska och betyder nav. I figur 4-2 visas ett stjärnnät. Om man tittar på

bilden och jämför hubben med navet på ett hjul så förstår man varför den kallas hubb och varför topologin kallas stjärnnät.

Figur 4-2. Stjärnnät



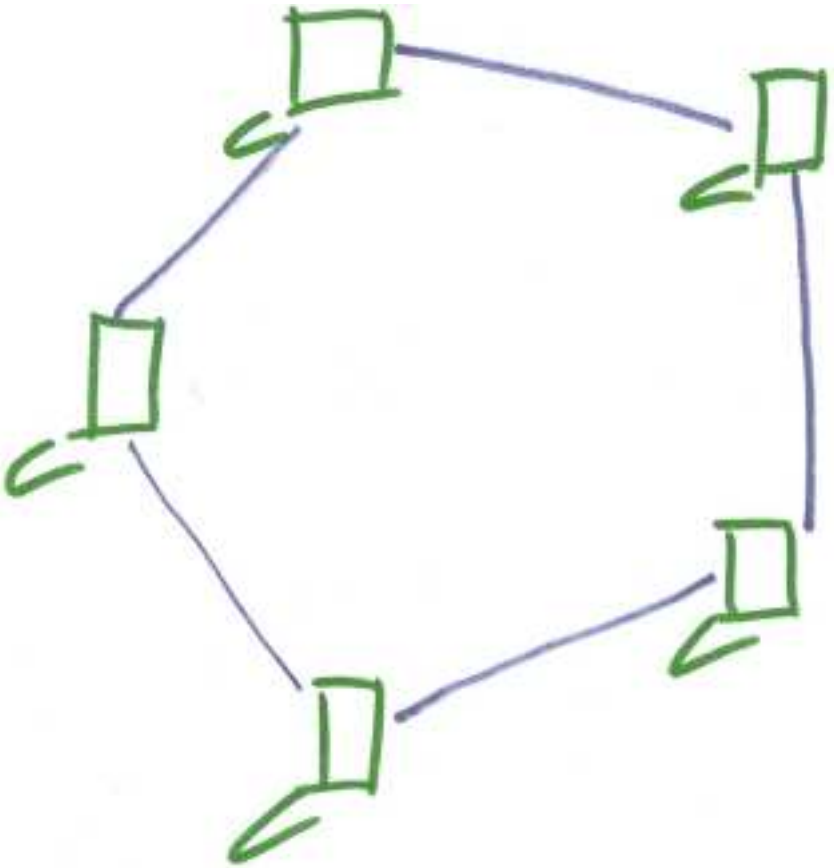
Stjärnnät är den vanligaste topologin i nyinstallerade nätverk idag. Den är billig att installera och om någon del av nätverket fallerar behöver inte nödvändigtvis hela nätet påverkas. Hubben i mitten fungerar så att en dator sänder och alla andra lyssnar, bara den datorn som meddelandet är avsett för sparar och behandlar meddelandet. Om någon dator faller ur nätverket så spelar det ingen roll för de övriga. Hubbar ersätts idag ofta med switchar. En switch fungerar som en hubb men håller reda på till vilken dator som ett meddelande skall. På så sätt kan flera maskiner utbyta data samtidigt oberoende av varandra. Det gör att nätverkets kapacitet ökar markant.

Ringnät

I både bussnät och stjärnnät så finns det en central del som alltid måste fungera (backbone respektive hubben). I ett ringnät behövs inte detta utan noderna (datorerna) är kopplade till varandra utan någon central enhet. Detta är möjligt eftersom alla datorer har två anslutningar, en från föregående dator och en till nästa dator. När cirkeln av datorer är sluten har man fått en ring, därav namnet ringnät. I figur 4-3 ser vi ett exempel på ett ringnät. Observera att ringen ofta består av en så kallad MAU, *Media Access Unit*. Denna MAU innehåller en logisk ring och påminner till utseendet om en hubb

eller switch. Med en MAU får en ringnät samma fysiska topologi om ett stjärnnät.

Figur 4-3. Ringnät



En nackdel med ringnät är att de är relativt känsliga för störningar. Om cirkeln bryts kommer kommunikationen inte att fungera. Detta försöker man undvika genom att skydda kablarna så mycket som möjligt och ibland drar man även dubbla cirklar. Ringnät är inte speciellt vanliga idag utan idag byggs i huvudsak stjärnnät när man bygger ett nytt nätverk.

Accessmetoder

I alla tre topologier som vi gått igenom måste det finnas regler för vilken dator som får sända när. I inget av näten kan alla datorer prata i munnen på varandra på samma kabel. Det går inte eftersom det inte fysiskt fungerar. För att detta inte skall ske och för att det inte skall bli katastrof om det sker så finns det vissa regler för hur datorerna får tala. Dessa regler kallas för accessmetoder och är i själva verket protokoll som säger vilken dator som för tillfället har rätt att använda det gemensamma

mediet (kabeln). Om du skall ringa till din kompis så får du en upptaget-ton om han eller hon talar i telefonen, du får försöka igen lite senare. Det är ett exempel på en relativt enkel accessmetod.

Den vanligaste accessmetoden är en med det krångliga namnet *CSMA/CD* som betyder: *Carrier Sense Multiple Access / Collision Detection*[1]. Vi tar det steg för steg. Carrier Sense innebär att en dator innan den sänder måste känna efter om det är någon som använder nätet. Är det det så måste datorerna vänta tills det blir ledigt. Multiple Access betyder att alla får använda nätet men inte samtidigt. Collision Detection innebär att om två stycken eller flera börjar sända samtidigt så skall detta detekteras och de får sända en i taget. I praktiken så fungerar det så att om en kollision upptäcks så slutar alla inblandade att sända och väntar en slumpvis tidsperiod. På så sätt minimeras risken att de börjar sända samtidigt igen. Naturligtvis gör kollisioner att trafiken i systemet går långsammare. På hubbar brukar det ofta finnas lampor som indikerar att en kollision har inträffat. CSMA/CD används i nätverksprotokollet Ethernet.

En variant på CSMA/CD är *CSMA/CA*. Alla bokstäver står för samma sak (och samma innebörd) utom då CA som står för *Collision Avoidance*. Det fungerar så att en dator innan den börjar sända skickar ut ett litet meddelande för att kontrollera att nätverket är ledigt och om det är det skickar ut riktiga data. Det gör att kollisioner inte behöver ske med riktiga data utan bara med de små "provskotten". CSMA/CA används i LocalTalk som är ett nätverksprotokoll från Apple och i de flesta av våra trådlösa nätverk.

CSMA/CD och CSMA/CA passar när nätverket består av ett gemensamt media, till exempel en kabel eller en hubb. I fallet med ringnät passar inte detta eftersom det är olika kablar i de olika delarna av nätverket (studera figur 4-3). I ett ringnät kan man istället använda en accessmetod som heter *token passing*. Token passing går ut på att en token cirkulerar runt i nätverket ungefär som en stafettpinne. Varje dator får stafettpinnen och skickar den vidare. Det finns bara en stafettpinne och bara den dator som har stafettpinnen får sända data. Dessa data och stafettpinen skickas vidare. Alla datorer skickar vidare och den som aktuella data är avsedd för kopierar dessa data och skickar vidare. När dessa data kommer tillbaka (med stafettpinnen) till avsändaren tar den bort dessa data från nätet och skickar stafettpinnen vidare. Detta gör att kollisioner helt kan undvikas. Token Passing används i nätverksteknologin Token Ring från IBM.

Sammanfattning

I detta kapitel har du lärt dig vad ett datornätverk är. Du har lärt dig de olika topologierna och hur de ser ut och fungerar. Du skall även veta vad accessmetoder är, vad de vanligaste heter och hur de fungerar.

1. Datorkommunikation är ett underbart ämne med underbara förkortningar!

Kapitel 5. Nätverkskomponenter

För att kunna bygga de nätverk som beskrevs i det förra kapitlet måste man ha något att bygga av. Nätverken byggs naturligtvis upp av datorer, men även andra komponenter behövs för att kunna, dels koppla ihop datorerna i nätverk och även kunna koppla ihop olika nätverk med varandra.

Noder

Det kan vara på sin plats att först beskriva termen *nod*. En nod är en generell adresserbar nätverkskomponent. Det kan vara en arbetsstation, en router, en brandvägg eller något annat. Är den adresserbar i nätverket så kallas den ofta för en nod.

Man kan säga att ett nätverk byggs upp av noder som i sin tur är olika komponenter.

Datorer/Servrar

Datorer kan anses som de viktigaste komponenterna i ett datornätverk. Utan dem blir det inte mycket till nätverk. Det minsta nätverk man kan bygga är med hjälp av två datorer med något typ av kommunikationskort och en kabel.

Den vanligaste typen av kommunikationskort eller gränssnitt man använder på en dator är ett *nätverkskort*. Den vanligaste typen av nätverkkort idag är ethernet-kort. Dessa har oftast ett uttag för en kabel med ett kontaktdon som kallas för RJ-45. RJ-45 ser ungefär som den koppling som finns på en del telefoner. Den kontakt som sitter på telefonen heter RJ-11 och har fyra ledningar medan RJ-45 har åtta. RJ-11 kallas även för modulärkontakt. RJ står för Registered Jack.

Varje nätverkskort har en unik adress. Denna kallas för kortets *hårdvaruadress* eller *MAC-adress*. MAC står för *Media Access Control* och är nödvändig för att kunna identifiera de olika datorerna på nätverket. MAC-adresserna är alltså unika på alla nätverkskort som säljs. Detta samordnas centralt av en organisation som heter *IEEE*. IEEE (uttalas "i-triple-e") är en förkortning för Institute for Electric and Electronic Engineers och är en organisation av personer och företag inom elektricitet, elektronik och datorer.

En dator kan ha flera olika roller i ett nätverk. Den kan vara till exempel en arbetsstation vid vilken någon sitter och jobbar. Det kan också vara en *server*. En server är en dator som förser nätverket med

en eller flera tjänster (Eng. services). Egentligen är en server inte en hårdvara utan själva programvaran som implementerar tjänsten men det har blivit så att man även kallar själva datorn som kör servern eller servrarna för en server. Det finns speciella datorer som kallas servrar. Det som skiljer dessa från vanliga datorer är att de brukar vara kraftigare byggda och ha mer påkostade fläktar och diskar. Funktionsmässigt är det ingen större skillnad så länge det rör sig om samma datorarkitektur.

En dator kan också vara en *terminal*. En terminal är brukar kallas för en "dum" terminal och är en dator som inte själv har så mycket resurser utan är knuten till en server vars tjänster terminalen är helt beroende av. Terminalerna bestod tidigare av bara en skärm och ett tangentbord som var kopplade direkt till en dator antingen via en vanlig kabel eller via telefonnätet eller andra större nätverk. De hade alltså ingen egen datorkapacitet. Idag är detta inte så vanligt. Använder man terminalsystem idag så är det oftast så att man kör ett terminalemulerningsprogram på sin PC.

Det har dock på senare tid blivit vanligt med tunna klienter. Dessa fungerar ungefär som terminalerna gjorde men en tunn klient har lite egna resurser men kör alla program direkt från en server. Det har flera fördelar. För det första så blir dessa tunna klienter mycket billigare och har längre livslängd än PC-datorer. En andra fördel är att service och uppgraderingar av programvaror lättare kan skötas centralt. Alla klienter kör ju samma programvaror från servern så om denna uppgraderas så har alla klienter uppgraderats på en gång.

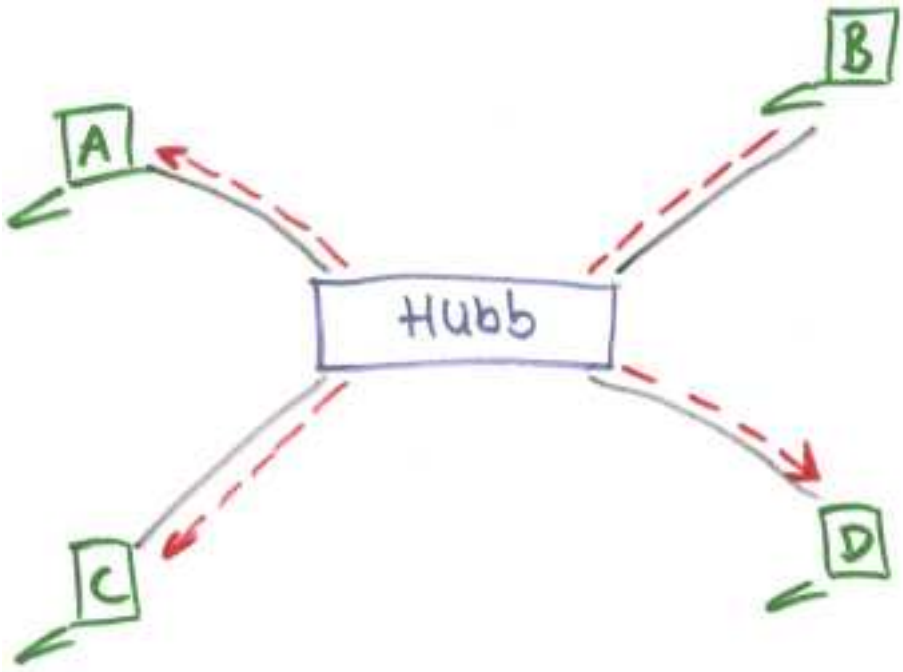
Hubb[1]

En hubb, från engelskans hub (= nav), är namnet på den centrala knytpunkten, nätnavet, i ett stjärnnät. Det är också namnet på en nätverkskomponent som används just i detta syfte. En hubb fungerar som en grenkoppling. Alla signaler som kommer in på ett uttag på hubben skickas ut på alla andra uttag på samma gång. En nackdel med detta är att bara en ansluten nod i taget kan sända. Sänder en så skickas det till alla andra på en gång och hela nätet blir således upptaget. Det är väldigt vanligt med kollisioner i ett nät där man har just en hubb som nätnav. De flesta hubbar har en lysdiod som indikerar när det är en kollision på nätet. Denna lampa kan man använda som en indikator för att se hur många kollisioner det är på nätverket. Många kollisioner gör att nätverket får minskad kapacitet och upplevs som långsamt. Man kan då välja att segmentera nätverket eller skaffa en switch (se nästa stycke). Ett annat relaterat problem är att eftersom all trafik kommer fram till alla datorer kan en ond användare ta del av information som inte är avsedd för henne vilket är en säkerhetsrisk.

I figur 5-1 visas kommunikation över en hubb. När dator B sänder data över nätverket så når det inte bara avsedd mottagare utan även alla andra anslutna till hubben. Det gör att bara en kan sända i taget vilket gör att fler kollisioner uppstår och att nätverket kan gå långsammare.

1. Se även brevet från Jan Johansson i appendix K

Figur 5-1. Kommunikation över en hubb



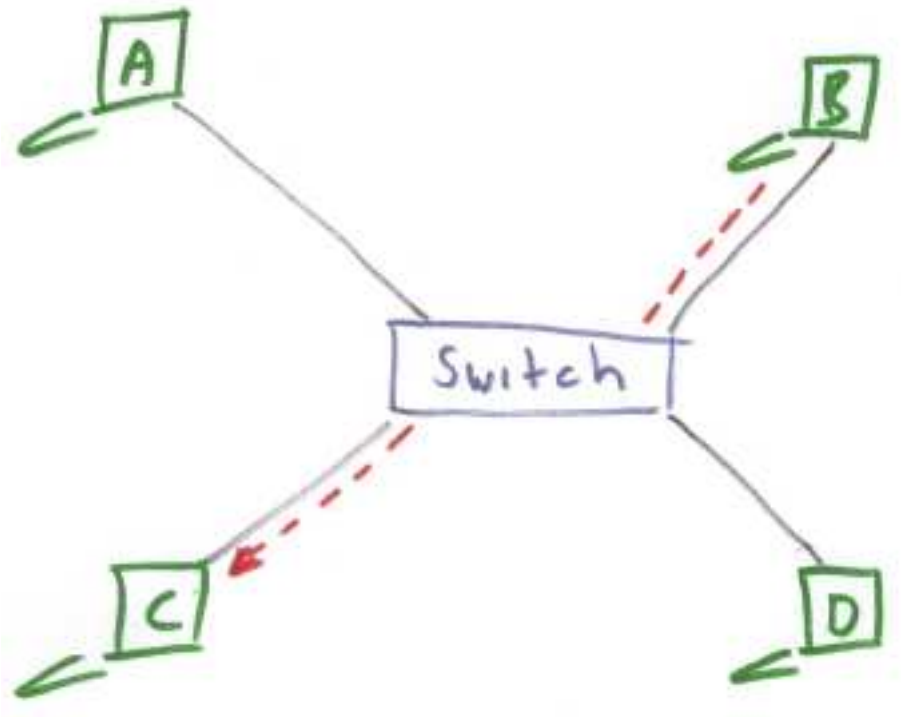
Switch[2]

En switch är också en komponent som används som nätnav i ett stjärnnät. Till skillnad från hubben så håller switchen reda på vilka datorer som sitter på vilket uttag och skickar bara informationen till den dator som den är avsedd för. Det gör att inte nätet fylls med trafik så fort någon av datorerna skickar data. Alltså kan kommunikation ske mellan två par datorer oberoende av varandra på samma gång på samma switch. Säkerheten ökas också eftersom det blir svårare att komma åt information som inte är avsedd för den aktuella datorn.

Studera och jämför bilderna figur 5-1 och figur 5-2. I figur 5-2 visas kommunikation över en switch. När dator B sänder data över nätverket till C så når dessa data bara dator C. Eftersom B och C får en egen kanal genom switchen kan de kommunicera utan att resten av nätverket störs. Samtidigt skulle A och D kunna kommunicera på samma sätt.

2. Se även brevet från Jan Johansson i appendix K

Figur 5-2. Kommunikation över en switch



I mer avancerade switchar kan man konfigurera exakt på vilket sätt olika noder får tala med varandra. Man kan skapa så kallade *virtuella LAN* (VLAN) på en switch. Det går till så att man kopplar ihop portar i grupper så att varje grupp fungerar som en egen switch. Det finns även flera funktioner på dyrare switchar.

Repeater[3]

En repeater kan jämföras med en förstärkare. En repeater har ingångar och utgångar, den lyssnar på ingångarna och förstärker signalerna och skickar dem på utgångarna. En repeater har ingen intelligens alls utan förstärker bara det den hör och skickar vidare. En repeater används vid kommunikation över större avstånd och för att koppla ihop olika nätverkssegment i ett nätverk.

Brygga[4]

En brygga fungerar ungefär som en repeater så tillvida att den är en ganska enkel apparat med två anslutningar. Där slutar dock likheten. En brygga används för att koppla ihop olika nätverk, eller

3. Se även brevet från Jan Johansson i appendix K
4. Se även brevet från Jan Johansson i appendix K

segment av samma nätverk. Bryggan släpper bara igenom den trafik som skall till nätet på andra sidan. På så sätt minskas onödig trafik i de båda näten eller segmenten.

Brouter

Namnet brouter är en lek med ord. Det är en sammanslagning av de engelska orden Bridge (brygga) och Router. Den fungerar som en brygga men kan koppla ihop flera nätverk, eller nätverkssegment, som en router (se nedan). Den är dock enklare än en router och jobbar på samma nivå som en brygga.

Router

En router är en nätverkskomponent som kopplar samman olika nätverk. Den kopplar inte samman näten så blint som en brygga eller repeater utan en Router läser nätverkstrafiken och bedömer vilken trafik som skall till vilket nät. En router kan vara ansluten till flera nät. Att läsa nätverkstrafik och skicka den vidare åt olika håll beroende på deras destination kallas för att *routa* på klingande svengelska. För att veta åt vilket håll inkommen nätverkstrafik skall använder sig en router av en *routingtabell* där det finns listat var olika datorer och nätverk finns. Routingtabellen kan vara statisk, det vill säga sparad på en disk i routern och ändras inte, eller dynamisk. En dynamisk routingtabell uppdateras automatiskt utifrån hur omgivningen ser ut.

Gateway

En gateway används för att koppla samman nätverk av olika typ. Man kan se det som en konverterare. Namnet gateway används ibland, felaktigt, på en maskin som som sitter mellan ett lokalt nät och Internet även om samma nätverksprotokoll används. I det fallet är router en riktigare benämning.

Brandvägg

En router mellan till exempel ett lokalt nätverk och Internet kombineras ofta med en brandvägg (eng. Firewall). En brandvägg är en speciell sorts router som bara routar vidare den trafik som uppfyller vissa krav. Trafik som inte uppfyller kraven kastas bort vilket gör att mottagaren av den "förbjudna" trafiken skyddas från den.

Oftast har man en brandvägg mellan ett lokalt nätverk och Internet men man kan även ha brandväggar på det interna nätet. Ibland har man brandväggar på själva den datorn som skall

skyddas. Den fungerar på samma sätt som en vanlig brandvägg med den enda skillnaden att den inte routar till och från ett helt nätverk utan bara till och från den aktuella datorn.

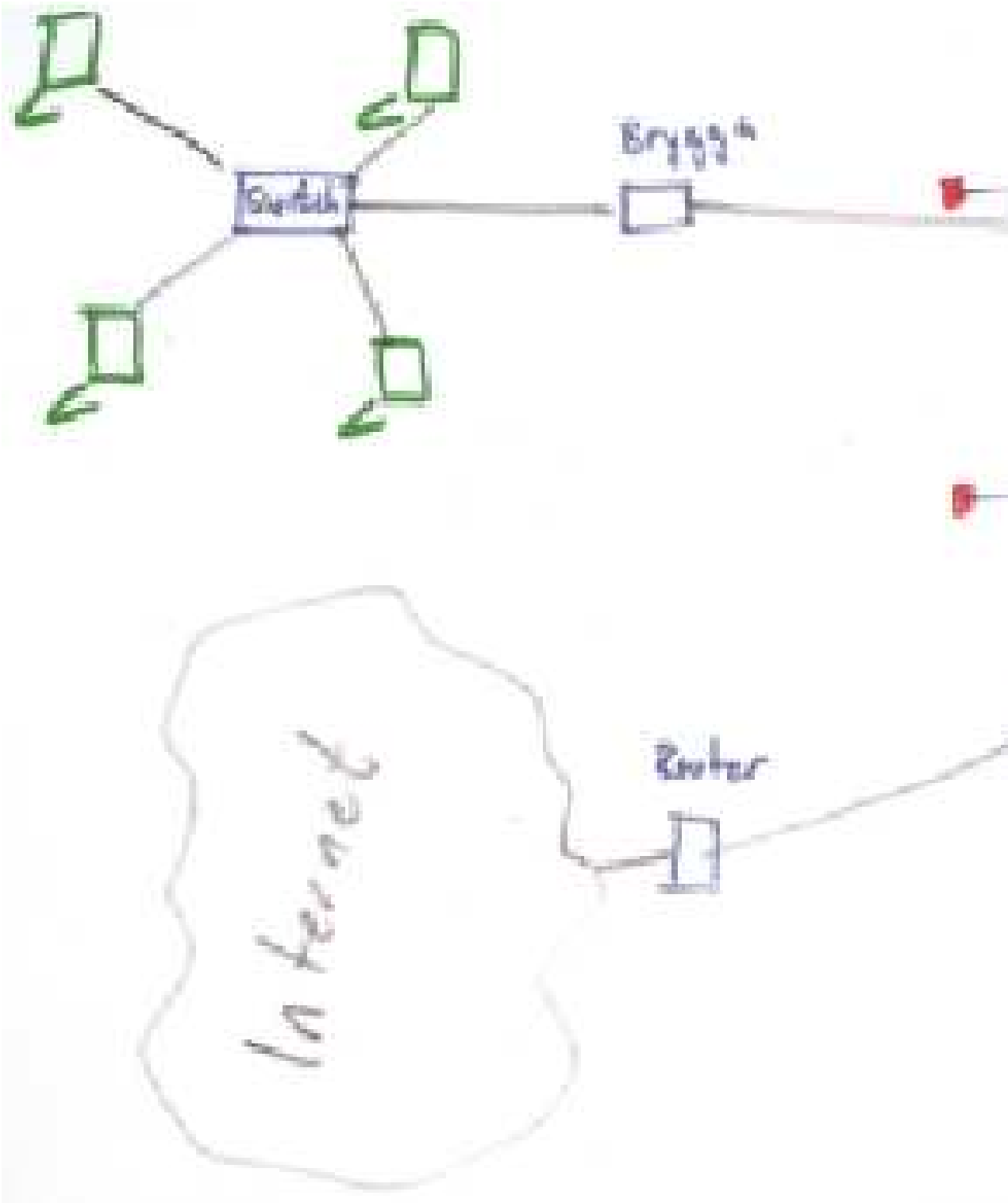
Det som avgör om en viss trafik skall släppas igenom eller inte kallas för *brandväggsregler* eller bara regler om det inte råder några tvivel om vad man talar om.

Vi kommer att tala mer om brandväggar i kapitel 14.

Sammanhängande exempel

I figur 5-3 visas en en ganska krystad bild på ett nätverk där de flesta av komponenterna vi behandlat finns med. Switchen hade lika gärna kunnat vara en hubb. I exemplet finns det en kombinerad router och brandvägg vilket inte alls är ovanligt.

Figur 5-3. Exempel på nätverk



Sammanfattning

I detta kapitel har vi gått igenom en mängd nätverkskomponenter. Du skall nu känna till vad dessa gör och hur de fungerar. Till exempel switch, router och brandvägg.

Kapitel 6. Kablar och icke-kablar

Vi har tidigare tittat på hur man kan "förpacka" data för att skicka det på olika sätt i olika kablar. I detta kapitel skall vi titta mer på själva kablarna och lite på de trådlösa alternativ som finns.

Inledning

Det finns massor av olika kablar. De flesta kablar finns naturligtvis för att de är speciellt bra på någonting men det finns också de som finns för att de en gång i tiden var bra på något. Det vill säga vissa kablar finns kvar på grund av att de varit vanliga en gång i tiden. Idag finns det dessutom en hel del trådlösa alternativ såsom radio, IR och Mobiltelefonnätet. Jag kallar dessa trådlösa alternativ för icke-kablar. Detta för att de på många sätt påminner om kablar och gör ofta samma sak men en del av själva finessen med dem är att de just inte är kablar.

I detta kapitel tittar vi närmare på kablarna och icke-kablarna och deras egenskaper.

Kabelegenskaper

En kabel har en mängd olika egenskaper. Alla påverkar på olika sätt hur bra den är i olika sammanhang. En kabel för att leda starkström mellan ett kärnkraftverk och någon typ av ställverk eller mellan två kontinenter har vid en första anblick inte mycket gemensamt med en ledning mellan två olika delar i ett elektroniskt armbandsur. Men om man tänker efter så är flera olika saker direkt jämförbara även om deras mätvärden inte ens kommer i närheten av varandra.

Båda kablarna har som uppgift att leda en ström. Den gigantiska kabeln från kärnkraftverket eller mellan kontinenterna måste kunna leda en enormt stor ström. Den måste också tåla väder och vara utformad så att man inte kan skada sig på den. Kabeln i klockan skall också leda en ström. Denna ström är bara en bråkdel av strömmen i den stora kabeln. Kabeln i klockan måste i stället vara tillräckligt tunn för att rymmas i klockan, den måste dessutom vara utformad så att den tål eventuella stötar som klockan kan komma att utsättas för.

Även om dessa kablar inte liknar varandra ser vi att samma storheter spelar in på dem. De skall leda en viss ström (Ampere). De får inte ha för stort motstånd (Ohm) och så vidare.

En annan aspekt på kablar som man måste tänka på är brandfarligheten. Ofta när man drar nätverk i

större hus så blir det väldigt tjocka kabelbuntar i väggar och på skenor under tak. Ur brandsynpunkt finns det två material att välja på. PVC och Plenum, PVC är mer brandfarligt och kan utveckla giftig rök när det brinner. Plenum däremt är mindre brandfarligt. Plenum-kablar är betydligt dyrare än PVC-kablar.

De kanske viktigaste egenskaperna för kablar när det gäller datorkommunikation är att de har rätt antal ledare, att de inte har för stort motstånd över den längd de är avsedda för och att de inte är störningskänsliga så att de klarar de frekvenser de kommer att utsättas för. Det finns en mängd olika kablar.

Kablar till periferiutrustning

För att ansluta periferiutrustning till en dator finns det idag i huvudsak tre olika kabeltyper. Seriekabel, parallellkabel och USB-kabel.

Parallellkabel

Parallellkabeln kallas också för skrivarkabel och används huvudsakligen för att ansluta skrivare till en dator. Man kan också använda den till att ansluta andra saker som till exempel flyttbara hårddiskar, skannrar, och annat. Man kan även koppla ihop två datorer med en parallellkabel för till exempel filöverföring. Man skall tänka på att en parallellkabel inte kan vara speciellt lång (se avsnittet *Parallell kommunikation* i kapitel 3).

Seriekabel

Seriekabeln används oftast för att ansluta modem men den kan även användas för en mängd olika saker, som till exempel att ansluta en digitalkamera eller överföra filer. Seriekablar kan vara väldigt långa.

USB-kabel

USB *Universal Serial Bus* är ett gränssnitt som blir allt vanligare. I många fall ersätter det både seriekablar och parallellkablar. Både modem, kameror och skrivare ansluts allt oftare via USB. Det finns flera skillnader mellan den vanliga seriekabeln och USB. Den största skillnaden är att USB, som namnet antyder, är ett bussystem. Det gör att man inte har en kommunikation bara mellan två punkter utan man kan koppla in flera enheter på samma uttag.

Kablar till datornätverk

Det blir allt vanligare att man kopplar ihop flera datorer i ett datornät. De allra flesta nya datorer idag har nätverkskort eller modem och ansluts till ett nätverk.

Fortfarande är kablar det vanligaste sättet att bygga ett datornätverk även om trådlösa alternativ kommer starkt.

Twisted-pair (TP)

Twisted-pair eller partvinnad kabel, kallas vardagligt för TP-kabel, är den vanligaste typen av kabel i installationer inom byggnader. TP-kabel är är lätt att dra i byggnader och är ekonomiskt fördelaktig.

I en vanlig TP-kabel finns det 4 par ledare. Det finns dem med bara två par också men de används inte så ofta för datornätverk utan används oftast bara till telefontrafik. Som namnet antyder är ledarna i varje par tvinnade om varandra. Man kan känna detta om drar fingrarna längs en TP-kabel och man ser det tydligt om man klipper upp en bit kabel. Anledningen till att man tvinnar dem är att minska känsligheten för störningar, både för störningar utifrån, så kallad interferens, och inre störningar i kabeln, så kallad crosstalk. Kanske minns ni från fysiken hur ett elektromagnetiskt fält vrider sig runt kabeln. Genom att tvinna två kablar tar dessa magnetfält ut varandra och minskar risken för störningar.

Det finns två typer av TP-kabel, skärmad och oskärmad. Den skärmade varianten kallas för STP och den oskärmade för UTP. TP-kabel klarar överföringar på 10 - 155 Mbit/s. Det finns även de som klarar 1000Mbit/s.

Oskärmad TP-kabel (UTP)

Oskärmad TP-kabel brukar kallas UTP. Det kommer från engelskans Unshielded Twisted Pair. Den har normalt 8 ledningar (4 par). UTP kabel är mycket mjuk och följsam vilket gör den lätt (och billig) att installera i en byggnad.

Skärmad TP-kabel (STP)

Skärmad TP-kabel kallas STP som i Shielded Twisted Pair. Trots att ledarparen är tvinnade så är UTP-kabel känslig för störningar. Därför finns STP. Den ser likadan ut som UTP men har en skärm mellan ledarna och ytterhöljet. Denna skärm består oftast av aluminiumfolie eller kopparväv. STP

blir, tack vare skärmen, lite stelare och svårare att installera. Men den är ändå relativt lättinstallerad. STP är också dyrare är UTP.

Koaxialkabel (Koax)

Koaxialkabel är en kabel med en ledare i mitten. Runt denna finns en isolator och utanpå den en skärm. Ytterst finns ett skyddande och isolerade hölje. Ledningarnas centrumaxel sammanfaller vilket är bra eftersom den elektromagnetiska strålningen, som kan störa, blir minimal.

Koaxialkabel är styvare än TP-kabel och är därför svårare att installera. Svårare är i detta fall lika med dyrare.

Fiberoptisk kabel (Fiber)

Fiberoptisk kabel har en kärna av glas eller plast som släpper igenom ljus mycket bra. Ljus i ena änden på kabeln tar sig blixtsnabbt igenom kabeln och kan registreras på andra sidan.

Fiberoptisk kabel är billig och har en enorm kapacitet som vida överstiger de andra kablarna. Dock är fiberoptisk kabel svårare att hantera, till exempel behövs speciella verktyg för att skarva kabeln. Ledaren är extremt känslig, både för böjning och för slag. Fiberoptisk kabel skall installeras av proffs.

Fiberoptisk kabel är det vanligaste alternativet idag vid snabbare internetförbindelser.

Trådlösa alternativ

Kablar har många nackdelar. Till exempel så kostar de en hel del. Även om kostnaden för kabeln kanske inte är så stor så kostar den att installera. Vidare är kablar svåra att dölja vid en installation. Man vill ju inte ha kablar kors och tvärs överallt i en lokal. Kablar är inte heller så flexibla för användaren. Skall man gå från sitt skrivbord till soffan eller fika-bordet och vill ha sin laptop med sig blir det krångligt med sladdar. Har man trådlöst nätverk till sin dator underlättar det avsevärt.

Och sist men inte minst. Sladdar och kablar kan inte ligga still bredvid varandra utan att bilda trassel, bara det kan motivera ett byte till trådlösa alternativ. Man skall dock vara medveten om problemen.

Trådlös kommunikation kan låta som himmelriket men är förknippat med en hel del problem. För det första får man räkna med att kapaciteten minskar mot kabelalternativ och framför allt att säkerheten som regel minskar. Man måste ta detta i beaktande innan man beslutar sig för att upprätta en trådlös kommunikation.

Infrarött ljus (IR)

Infrarött ljus kan användas för att överföra data mellan olika enheter som stödjer detta. Vanligast är att det används för att föra över information mellan små enheter som till exempel handdatorer. Det är också vanligt att det används för att ansluta pereferienheter, framför allt skrivare, till bärbara datorer för att slippa hålla på med kablar. Det går också att använda IR för att föra över filer mellan bärbara datorer. En nackdel med IR är att det måste vara fri sikt mellan sändaren och mottagaren och att dessa är ganska riktingskänsliga. Det blir vanligare och vanligare att Bluetooth tar över där IR tidigare varit vanligt.

Radio

Radio är det vanligaste alternativet när det gäller att sätta upp trådlösa nätverk, så kallade *Wireless LAN* eller *WLAN*. Eftersom man oftast använder radio till dessa kallas de ibland för radio-LAN. De standarder som är vanligast inom detta område kommer från *IEEE* (http://www.ieee.org/) och är en familj av protokoll under namnet *IEEE 802.11* (http://www.ieee802.org/11/). Kapaciteten beror på vilken standard man använder sig av. Vanligast idag är IEEE 802.11b som tillåter 11 Mbit/s men betydligt snabbare finns.

Till 802.11 togs en standard fram för att höja säkerheten. Den kallas WEP *Wireless Equivalence Privacy* och följer med de flesta produkter. Namnet antyder syftet med den, den är avsedd att höja säkerhetsnivån till den som motsvaras av ett kabelburet nätverk. Det vill säga, inte perfekt, men bra nog för de flesta. Tyvärr har det visat sig att den har stora brister varför WEP enbart inte räcker för att göra ett trådlöst nät speciellt säkert.

Bluetooth (Blåtand)

Bluetooth, eller Blåtand som det också kallas, är en standard som från början togs fram av Ericsson. Nu styrs standarden av ett större organ med över 100 medlemmar.

Bluetooth är inte direkt menat för datornätverk även om det idag kan användas till det. Bluetooth är avsett för det som brukar kallas personliga nätverk. Det vill säga nätverk som bara används av en person. Det kan vara till exempel mellan en telefon och ett headset, mellan en handdator/ljudspelare

och hörlurar eller mellan en dator och en datormus. Eftersom det är avsett för dessa små nätverk har Bluetooth väldigt begränsad räckvidd. Upp till 10 eller 100 meter beroende på utrustning.

Bluetooth är idag mycket vanligt i till exempel mobiltelefoner och handdatorer. I vanliga datorer är det ännu inte lika vanligt men väntas komma där med.

Mobiltelefon

Ofta vill man komma åt sina nätverk var man än befinner sig. I dagsläget är det enda rimliga alternativet för detta att använda sig av mobiltelefonnätet. Det finns flera sätt att ansluta till ett datornätverk via mobiltelefonen. Till exempel kan man använda den som en helt vanlig telefon och ringa upp ett modem precis som med en vanlig telefon. Dock skall man tänka på att hastigheten i det fallet inte blir lika snabb som med en vanlig telefon eftersom mobiltelefonnätet inte förmedlar lika mycket information (bandbredd).

Eftersom man inte kan utnyttja mobiltelefonnätet så bra för datorkommunikation på traditionellt sätt så har nya tekniker tagits fram som nyttjar samma infrastruktur. Det vanligaste idag är GPRS. GPRS är ett paketförmedlat system som kan användas samtidigt som man talar i telefonen. Det har en hastighet på 9-160 kbit/s beroende på belastning i systemet.

I det nya mobiltelefonnätet *UMTS*, även kallat 3G. UMTS använder ett mycket större frekvensområde än dagens mobiltelefoner *GSM* och är bland annat mer lämpligt för datatrafik.

Sammanfattning

Det finns en mängd olika kablar som alla är bra på olika saker. Inom datorkommunikationen har vi flera olika alternativ. I dag är olika typer av TP-kabel och fiberoptisk kabel det vanligaste.

Kapitel 7. Trådlösa nätverk, WLAN

I förra kapitlet behandlades kablar och några trådlösa alternativ. Det vanligaste trådlösa alternativet idag är WLAN och det är vad vi skall behanda i detta kapitel.

Detta kapitel behandlar trådlösa nätverk. En del av detta kapitel kommer från Wikipedia, Den fria encyklopedin.

Trådlös frihet

Det finns massor av skäl att välja trådlösa nätverk idag. Tekniken är mogen och snabb och fungerar mycket bra. Att sätta upp ett trådlöst nätver går på ett kick om lokalen inte är för stor och användarna för många. Tidigare har det kritiserats väldigt mycket för att vara osäkert men dagen teknik gör att det är enkelt att få det åtminstone lika säkert som trådbundna nätverk.

Att man slipper dra kablar gör installationen enkel och billig. Har de som skall använda nätverket bärbara datorer och kan flytta sig så är det också bra med trådlöst nätverk. Men finns det kablar att tillgå är det nästan alltid snabbare och mer tillgängligt att använda dem, men fördelarna med trådlöst nätverk är många.

Trådlöst LAN

Trådlöst LAN eller WLAN (av engelskans Wireless Local Area Network) är ett samlingsnamn för olika typer trådlösa lokala datornätverk.

Den vanligaste typen är IEEE 802.11-familjen som bland annat kan användas för att koppla ihop en central accesspunkt (AP) med klienter i form av datorer, IP-telefoner, handdatorer, smarta mobiltelefoner, mediaspelare och annan utrustning i kontors- eller hemmiljö.

Trådslösa LAN använder sig av teknologi baserad på radio eller mikrovågor (vid radio-LAN), och förr även infraröda vågor, för att kommunicera med andra enheter inom en begränsad radie. Detta ger användaren möjligheten att röra sig fritt inom detta område och fortfarande vara ansluten till nätverket. Radio-LAN har på senare tid blivit mer och mer populär bland annat på grund av den låga investeringskostnaden jämfört med trådbundet LAN.

De standarder som idag används för radio-LAN ger tillgång på upptill 54Mb/s i delad överföringshastighet, det vill säga hastigheten delas av samtliga klienter i nätverket. Inom en förmodligen snar framtid kommer dock nya standarder som skall stödja 100Mb/s och mer och skall även ge längre räckvidd med samma utsända effekt.

Teknik

Som tidigare sagts är trådlösa lan byggda på radiovågor. Dessa går igeom väggar och har ganska bra räckvidd. Upp till 30-50 meter brukar gå bra och även längre om man har bra utrustning. Även i ett trådlöst nätverk uppstår kollisioner (se avsnittet *Accessmetoder* i kapitel 4). Som accessmetod används CSMA/CA för att undvika och göra kollisionerna så snabba som möjligt.

Säkerhet

Trådlösa nätverk är ur säkerhetssynpunkt mer utsatta än trådbundna nätverk. Detta beror på att någon som vill utnyttja ett nät inte behöver komma i fysisk kontakt med det utan det räcker att denna är i närheten, till exempel i samma hus eller på gatan nedanför.

Oerfarna WLAN ägare begår ofta misstaget att inte skydda åtkomsten till nätverket med hjälp av kryptering. En stor andel av trådlösa nätverk står därför öppna utan något som helst skydd. Dessa kan vem som helst som har en dator och ett trådlöst nätverkskort ansluta sig till. Detta fenomen, att använda andras nät utan tillstånd, brukar man kalla Snyltning. Snyltarna kan till exempel göra olagligheter på någon annans bredbandsuppkoppling eller bara använda den för normalt bruk och då slippa betala för en egen. De flesta jurister verkar numera överens om att sådant uppsåtligt olovligt nyttjande av både oskyddade och skyddade nätverk är olagligt.

För att skydda sig mot snyltning och andra typer av intrång, tillämpas olika typer av skydd. Det vanligaste är att man krypterar nätverket. Det finns olika typer av kryperingsmetoder, de vanligaste är WEP, WPA och WPA2. WPA och WPA2 är en nyare och bättre standarder, men WEP-krypteringen dominerar fortfarande p g a att många accesspunkter inte stöder något annat.

Det finns även andra sätt att skydda sitt trådlösa nätverk från intrång, till dessa hör MAC-adressbegränsning, MAC-filtrering och att stänga av SSID-broadcast. Dessa skydd bör bara användas som komplement till kryptering då de är mycket lätta att komma förbi och deras huvudsakliga uppgift är att stänga ute oavsiktlig användning. Snyltare kommer förbi dem ändå genom att bland annat använda spoofing. Att stänga av SSID-broadcast ger egentligen inget skydd alls eftersom SSIDet fortfarande finns i all trafik på det aktuella WLANet.

Kapitel 8. Modem

För bara några år sedan kom internet-boomen till Sverige. Alla skulle koppla upp sig. I början fanns det bara ett sätt att skapa en förbindelse mellan kunderna och deras internetleverantör (ISP, Internet Service Provider). Det var genom att skicka digital datatrafik som analoga signaler över telefonnätet. Till detta används en uppfining som är mycket äldre än så och som använts i datorkommunikationssammanhang sedan 1960-talet, nämligen modemet.

I detta kapitel tittar vi närmare på modem. Vad ett modem är och hur det fungerar.

Introduktion

Som vi sagt tidigare så är vissa medier, till exempel telefonnätet, gjorda för att transportera analoga signaler. Ofta vill man transportera digital data över en analog förbindelse. Till detta används en utrustning som kallas för *modem*. Modem är en förkortning för *Modulator/Demodulator* och kommer från modemets huvudsakliga funktion. Att modulera innebär att man översätter digitala signaler till analoga och att demodulera innebär att man reverserar processen genom att omvandla de analoga signalerna tillbaka till digitala.

Modem har traditionellt varit det vanligaste sättet för privatpersoner att ansluta sig till Internet. Alla Internetleverantören (Internet Service Provider, ISP) erbjuder tjänsten uppringt Internet, det vill säga Internet via ett modem anslutet till telenätet. I dag blir detta dock allt mindre vanligt då nya snabbare tjänster erbjuds. Mer som dessa kommer i kapitlet om Internet (kapitel 11).

Olika sätt att modulera

När ett modem modulerar en digital signal finns det flera olika sätt att göra det på. I slutändan blir det någon typ av ljud med olika egenskaper. Man kan välja att ändra den analoga signalen på flera olika sätt för att kunna koda in digitala signaler i den.

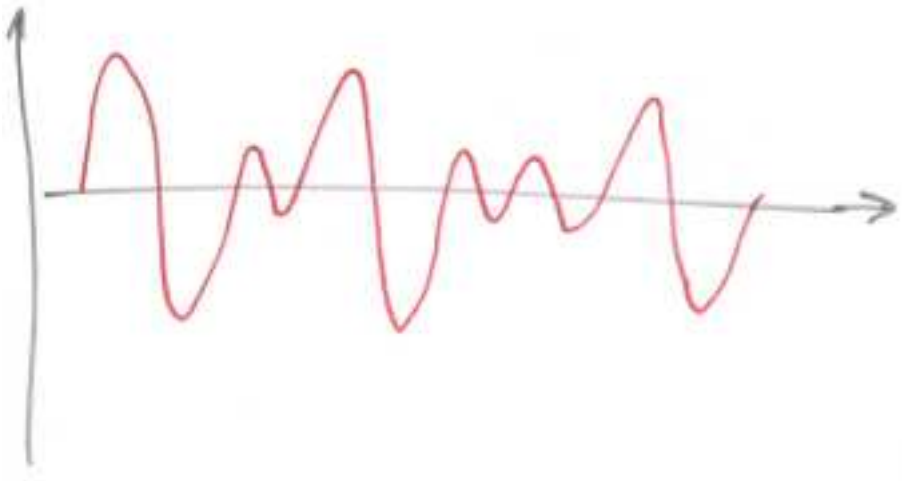
Amplitudmodulering

Amplitudmodulering innebär att man genom att ändra amplituden i signalen kan man baka in data i signalen. Det vill säga 1:or ges en amplitud och 0:or en annan. Denna metod är inte så effektiv,

eftersom den till exempel är väldigt beroende av att signalen inte dämpas på vägen, och användes i de första modemen.

I figur 8-1 visas amplitudmodulering. I figuren innebär till exempel en högre amplitud en 1:a och en lägre en 0:a. Denna metod är dock väldigt känslig för till exempel att signalen blir dämpad och användes bara i de första modemen.

Figur 8-1. Amplitudmodulering

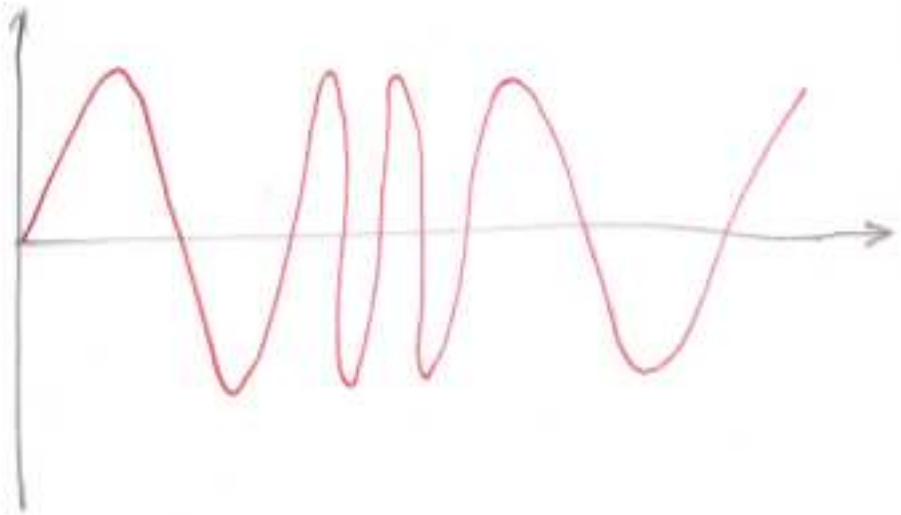


Frekvensmodulering

Frekvensmudulering innebär att man skickar en signal med konstant amplitud men att frekvensen ändras. Denna metod är bättre än amplitudmodulering.

I figur 8-2 visas frekvensmodulering. Vid frekvensmodulering används olika frekvenser för att bära antingen 1:or eller 0:or. I figuren innebär till exempel en högre frekvens en 1:a och en lägre en 0:a.

Figur 8-2. Frekvensmodulering

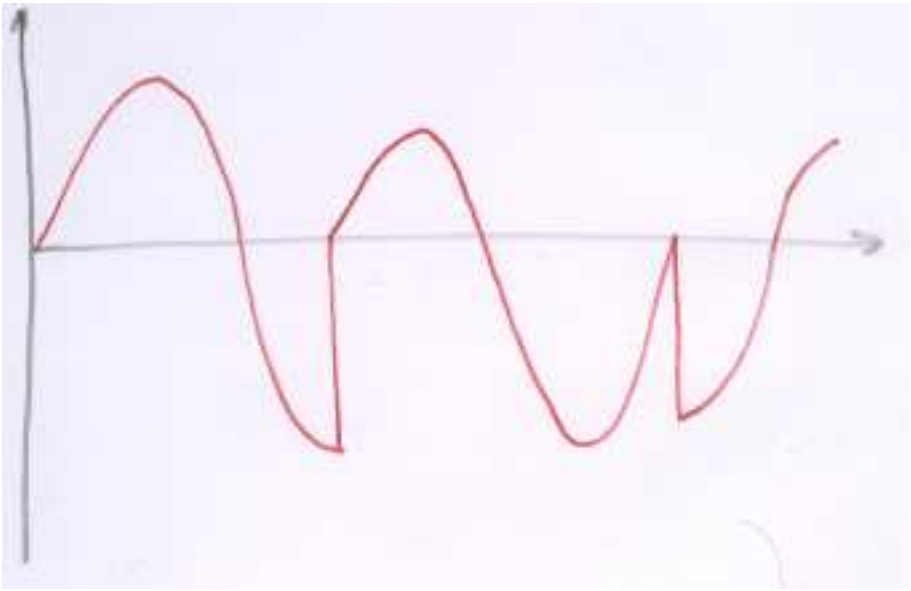


Fasskiftesmodulering

Ett tredje sätt att bädda in digitala signaler i en analog är att använda sig av fasskiftesmodulering. Det innebär att man utgår från en sinusformad signal och bestämmer att ett fasskifte har en viss innebörd. Eftersom man kan välja att byta fas vid olika ställen (vinklar) så kan man skicka mer information än 1:or och 0:or. Till exempel kan man bestämma att vissa lägen betyder 00, 01, 10 och 11.

I figur 8-3 visas fasskiftesmodulering. Vid fasskiftesmodulering utgår man från en sinusformad kurva och låter den byta fas vid bestämda lägen. Ett fasskifte på ett visst ställe i cykeln betyder en viss sak, till exempel en 1:a eller 0:a. Det finns också utrymme för att specificera följder av tecken, till exempel 00, 01, 10 eller 11.

Figur 8-3. Fasskiftesmodulering



Handskakning

Innan två modem kan börja tala med varandra (det är alltid två modem) så måste modem komma överens om hur de skall skicka information. Det gör de i en procedur som kallas *handskakning* (eng. Handshake). I handskakningen, som föregår det egentliga datautbytet, kommer modemen överens om exempelvis överföringshastigheten.

För att ett modem skall kunna kommunicera med så många olika modem som möjligt så kan de flesta modemen skicka och ta emot data i en mängd olika hastigheter. När två modem kommer överens om överföringshastigheten så är det alltid det långsammaste modemet som bestämmer i vilken hastighet de skall utbyta data.

Hayes-kommandon, (AT-kommandon)

Modem avsedda för telenätet var oftast så kallade akustiska modem. De bestod av en liten låda med en sladd och en telefonlursliknande sak med gummimuffar som passade på en vanlig telefonlur. Modemet innehöll alltså ingen telefon utan man ringde manuellt upp det nummer man skulle ringa och sedan kopplade man på modemen på varje sida genom att montera modemets mikrofon och högtalare på telefonluren. Detta var naturligtvis inte speciellt praktiskt. Man ville ju kunna

programmera modemet från datorn så att datorn själv kunde till exempel ringa upp ett annat modem. Modemet borde ju dessutom kunna svara själv.

Det första modemet som kunde detta var ett modem från ett företag som heter *Hayes Communications*. Modemet hette *Hayes Smartmodem* och lanserades 1981. Detta modem kunde man kontrollera helt från datorn. Man kunde alltså ringa ett nummer, ändra inställningar, lägga på luren med mera från datorn utan att röra modemet. I övrigt var Smartmodem inget fartunder utan det skickade data i blygsamma 300 bit/s vilket var ganska vanligt på den tiden.

För att styra modemet så införde företaget ett system med olika kommandon som man använder för att säga åt modemet att göra olika saker. Dessa kommandon började alla med *AT* som är en förkortning för engelskans "attention". På grund av detta kallas dessa kommandon för AT-kommandon eller Hayes-kommandon. Det är ingen formell standard men de flesta modem som finns idag är *Hayes-kompatibla*. det vill säga de stöder hela eller delar av Hayes uppsättning AT-kommandon. Flera modemtillverkare lägger till egna kommandon utöver de vanliga. I tabell 8-1 listas några vanliga AT-kommandon. Är du intresserad så finns det en mer komplett lista på http://en.wikipedia.org/wiki/Hayes_command_set.

Tabell 8-1. Vanliga Hayes-kommandon (AT-kommandon)

Kommando: (AT+)	Gör
DT1111111	Ringer upp 1111111 med tonval
DP1111111	Ringer upp 1111111 med pulsval
M0	Stänger av modemets högtalare
H0	Lägger på luren
Z0	Återställer modemets sparade konfiguration

Sammanfattning

Modem är en gammal uppfinning. Modem är en förkortning för *Modulator/Demodulator*. Sändande modem modulerar och mottagande demodulerar. Man kan modulera på flera sätt och det vanligaste idag är fasskiftesmodulering.

Innan två modem kan börja utbyta data kommer de överens om i vilken hastighet detta skall ske. Denna procedur kallas handskakning och det är alltid det långsammaste modemet som bestämmer.

Kapitel 9. Publika telenätet

Över det publika telenätet kan man använda en hel del olika tjänster. Här tittar vi på ett urval av dessa, vad de är och hur de fungerar. Vi tar inte upp snabba och moderna Internetuppkopplingar i detta kapitel utan dessa behandlas i kapitel 11.

Telenätets uppbyggnad

Vi skall inte gå in på detaljnivå i denna bok hur telenätet är uppbyggt. Det finns säkert andra böcker som behandlar detta. Vi nöjer oss med att titta på de mesta karakteristiska egenskaperna.

Stamnät och accessnät

Man delar in det publika telenätet i två olika delar: *stamnät* och *accessnät*. Stamnät brukar man kalla stora nätverk som används som backbone i nätverksstrukturer och så är det även i fallet med telefonnätet. Stamnätet är alla de kablar som utgör telefonnätet mellan städer och kopplingsstationer i Sverige. Accessnät kallas det nät som förbinder alla abonnenter med stamnätet. Det vill säga den kabeln som går från ditt telefonjack till kopplingsstationen. Telefonnätet består till största delen av kopparkabel som i många fall är 50 år gammal. När man skall bygga snabba datornät över telenätet är det oftast här man stöter på problem. Detta gamla kablage är naturligtvis inte avsett för att köra snabba, moderna datornät över. Men det finns tekniker där man anpassat modern teknik efter gammal lägre standard. Ett bra exempel på det är xDSL som är ett snabbt sätt att kommuninicera med datatrafik över gamla kopparledningar. I Sverige är ADSL vanligast inom det området idag.

Kretskopplade nät

Man skiljer på kretskopplade och paketförmedlande nät. I kretskopplade nät fungerar förbindelsen så att man har en fysisk koppling mellan de två parterna. Denna är konstant öppen och stängs inte förrän parterna bestämmer det. Precis så fungerar ett telefonsamtal. Detta har både fördelar och nackdelar. De kommunicerande har en konstant koppling till varandra, de känner dess kapacitet och vet att ingen annan tar den i anspråk. Å andra sidan är det ett enormt slöseri med resurser när dessa parter inte utbyter någon data. Då är ju linjen uppbokad så att ingen annan kan nyttja den men den används inte till något. Alltså måste parterna koppla ner förbindelsen när den inte skall användas på en längre tid.

Det vanligaste protokollet för krestskopplade nätverk är X.21.

Datex

Ett exempel på ett kretskopplat datornät är Datex. Datex lanserades av Televerket 1982 (oktober), det var då ett av de första publika datanäten i världen. Datex har idag fått ge vika för andra, nyare tekniker.

Paketförmedlande nät

Ett paketförmedlat nät är ett nät där trafiken delas upp i små paket som skickas genom nätet. Det gör att flera kan nyttja nätet på samma gång. Om man jämför kretskopplande nät med ett telefonsamtal så kan man jämföra ett paketförmedlande nät med en transportfirma eller posten. Flera personer kan skicka massor av paket samtidigt. Posten eller transportfirman ser till att alla paket kommer dit de skall. Paketen delar lastbilar och annat på vägen.

Standarden för paketförmedling i dessa nät kallas *X.25*.

Datapak

Ett exempel på ett paketförmedlande (X.25) datanät är Datapak. Datapak marknadsförs av bland annat Telia och används till exempel för bankomater, kassasystem, företagsnät och telefonsystem.

Uppringt Internet

Vi kommer att tala mer om olika sätt att ansluta sig till Internet i kapitel 11. Men det passar här att i alla fall nämna att telenätet är ett av de vanligaste sätten att ansluta sig till Internet eller använda sig av datorkommunikation. Använder man en uppringd förbindelse till Internet eller till någon annan dator eller tjänst så behöver man inget annat än en vanlig telefonanslutning och ett modem i båda ändar av förbindelsen. Detta fungerar sedan som ett vanligt telefonsamtal. Man skall tänka på att man har en kretskopplad förbindelse mellan modemen. Modemens prestanda är väldigt beroende av hur bra denna förbindelse är. Har man en dålig förbindelse kan det löna sig att koppla ner och sedan koppla upp igen och hoppas på en bättre koppling mellan modemen.

Sammanfattning

Kapitel 10. Protokoll

Protokoll är en uppsättning regler som de olika systemen måste känna till för att kunna kommunicera med varandra. Man kan säga att ett protokoll är det språk på vilket kommunikationen sker. Jag skriver detta på Svenska. Eftersom du känner till de regler som gäller för Svenska så förstår du vad jag skriver. Vi kommunicerar med Svenska som protokoll.

Inledning

Minns ni telefonsamtalet (figur 2-1) som var ett exempel tidigt i denna bok? För att telefonsamtalet skall fungera krävs att väldigt många olika regler följs. Man kan dela kommunikationen i ett flertal olika lager. Om Kalle talar i telefon med Kajsa så talar de ju enligt en uppsättning olika regler. De måste vara överens om vilket språk de talar och även inom vilket ämne de talar. Talar de om helt olika saker finns det en stor risk att de missförstår varandra.

Om man studerar samtalet i detalj så ser man att Kalle egentligen inte talar med Kajsa. För honom är det som om han gör det men egentligen så talar han med sin telefon. Telefonen i sin tur tror att den "talar" med Kajsas telefon men den talar egentligen med en telefonväxel och så vidare. Varje nivå i vårt exempel tror att de talar med en motpart på samma nivå medan de egentligen talar med en nivå upp eller ner på sin sida av figuren. Överallt i alla pilar i figur 2-1 finns det regler för hur det skall gå till för att allt skall fungera. Märk också att de tvärgående pilarna fungerar precis lika även om de underliggande pilarna ändras. Till exempel så behöver inte Kalle och Kajsa tala på ett annat sätt om samtalet går via satellit istället för kopparkabel bara de lager det berör gör sitt.

Kort sagt så kan man säga att om man skall kommunicera på ett eller annat sätt så måste de som kommunicerar göra det efter vissa givna regler. Ett datornätverk skulle inte fungera om inte alla enheter höll sig till en uppsättning regler. Hur skulle alla 1:or och 0:or på Internet kunna komma rätt om alla datorer gjorde som de ville?

Olika protokoll till olika saker

Nu är det inte så att det bara finns ett protokoll. Det finns inte heller bara ett protokoll per nätverk utan det finns massor av protokoll, i alla delar av kommunikationen. Tänk på telefonsamtalet igen. Kalle och Kajsa talar ett språk med varandra, det är ett protokoll. Den som ringde upp slog ett nummer med sin telefon, detta nummer tolkades av en telefonväxel enligt ett visst protokoll, osv. På

samma sätt är det ett virrvarr av protokoll i ett datornätverk och även mellan datorer och tillbehör, som till exempel skrivare.

Protokoll finns mellan alla parter som utbyte av data sker. Detta gäller både horisontellt och vertikalt i vår telefonmodell (figur 2-1). Vi har ju tidigare tittat på till exempel hur data kan skickas över en seriell förbindelse som är ett exempel på ett protokoll.

Följer alla sina protokoll så kommer det att fungera. För att alla skall kunna följa samma protokoll så måste ju dessa protokoll finnas tillgängliga för alla som vill vara med och prata. Dessutom måste det ju finnas någon som ser till att protokollen hålls uppdaterade och att de är korrekta.

Vem styr över protokollen och hur tillkommer nya?

Det finns flera företag och organisationer som hanterar olika standarder. De flesta välanvända protokoll finns dokumenterade i någon typ av standard. När det gäller Internet så har flera standarder kommit till på ett lite annorlunda sätt. Internet är ju ett öppet nät som inte någon kontrollerar, därför har standarder under Internets uppväxt kommit till på i den andan. På Internet finns en typ av dokument som heter *Request For Comments, RFC*. RFC-Dokument fungerar så att någon publicerar ett RFC som beskriver något protokoll eller annat som kan beröra flera. Om inte någon protesterat inom en vis tid antas att RFC:n kan fungera som standard. I dag är som regel ett RFC-dokument redan klart när det publiceras. Vi kommer att titta mer på Internet i kapitel 11, det finns också en tabell över RFC:er som berör det vi talar om i denna bok i appendix J.

Det finns naturligtvis även protokoll och standarder som kontrolleras av företag och organisationer på traditionellt vis. Exempel på organisationer som hanterar standarder är i Sverige till exempel *Post och Telestyrelsen, PTS* som kontrollerar bland annat radio och teletrafiken i Sverige och *Standardiseringen i Sverige, SIS* som är en del av *ISO, International Organization for Standardization* som är en organisation som lyder under FN och har medlemmar från 147[1] länder. Ett annat organ som kan vara bra att känna till är *IEEE* som är ett Amerikansk samling av ingenjörer som tar fram standarder för bland annat lokala nätverk.

Standarder som tas fram av oberoende organisationer kallas för *formella standarder*. I de oberoende organisationerna sitter ofta flera av de företag som berörs av starndarderna men eftersom de alla har samma tillgång till standarderna så kallas de ändå oberoende. Ganska många standarder tas fram på så sätt att ett företag utvecklar en produkt som skall fungera på ett viss sätt. Blir denna populär så kommer konkurrenterna att anamma samma format för att kunna utbyta information med denna produkt. Till slut har man en "standard" som alla följer men som ett enda företag (det som inledningsvis tog fram det) kontrollerar och utvecklar. Dessa standarder kallas för *de-factostandarder*

1. http://www.iso.ch/iso/en/aboutiso/introduction/

eller industristandarder och skall inte förväxlas med formella standarder eftersom företagen inte konkurrerar på samma villkor kring en industristandard vilket de kan kring en formell standard.

OSI-modellen

I de fall där man skall implementera datorkommunikation så stöter man oftast på problem som är väldigt likartade. Oftast så kan man specificera problemet i en modell som inte är helt olik den i vårt telefonsamtal (figur 2-1). Likheten är att man kan dela upp kommunikationen i olika lager med samma lager på både sändar- och mottagarsidan. Precis som i telefonsamtalet upplever varje lager som om det kommunicerar med motsvarande lager på andra sidan när det i själva verket egentligen bara talar med det underliggande och överliggande lagret.

På under slutet av 1970- och början på 1980-talet kom den internationella standardiseringsorganisationen, ISO på en modell för att på ett standardiserat sätt beskriva hur datorkommunikation går till. Anledningen till detta är att alla som jobbar med datorkommunikation skall ha en gemensam modell att jobba kring. Modellen som ISO togs fram kallas för *Open Systems Interconnect (OSI)*.

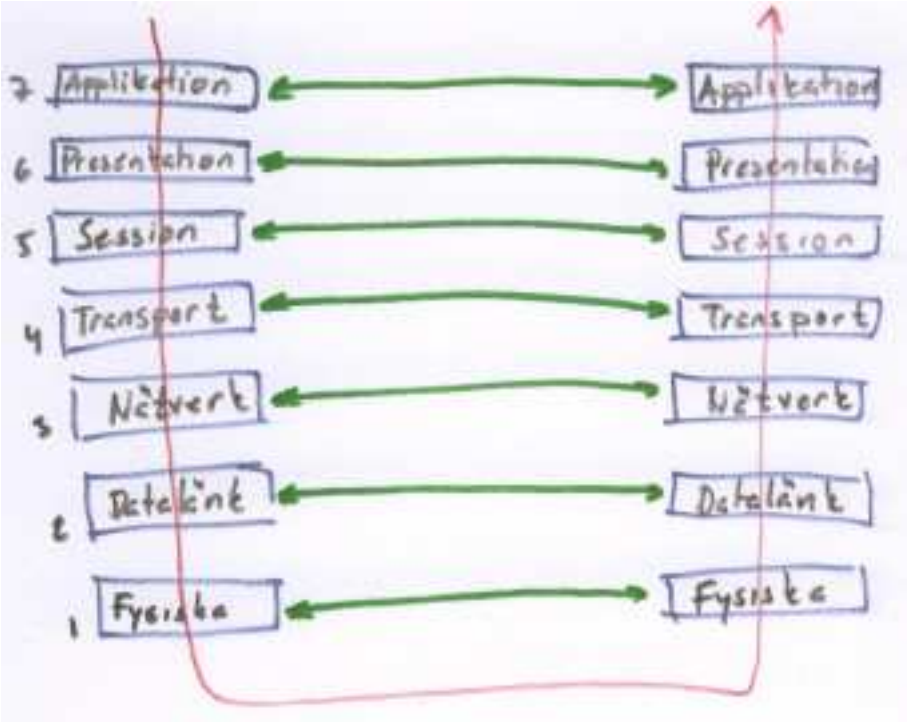
OSI-modellen har sju lager. Den nedersta lagret är närmast hårdvaran och det översta närmast användaren. Man numrerar lagren från 1 till 7 och börjar nerifrån. Så här ser lagren ut.

7. Applikation (Application)
6. Presentation (Presentation)
5. Session (Session)
4. Transport (Transport)
3. Nätverk (Network)
2. Datalänk (Datalink)
1. Fysiska (Physical)

För att komma ihåg de olika lagren är det smidigt att lära sig en lite ramsa. Den ramsa jag lärde mig en gång i tiden var *Please Do Not Teach Such Petty Acronyms* men du kan hitta på en egen ramsa eller leta efter en på Internet, det finns massor.

Vi skall nu studera OSI-modellen lite mer i detalj. För att det skall gå så lätt som möjligt så börjar vi med en liten figur.

Figur 10-1. OSI-modellen



I figuren (figur 10-1) ser vi OSI-modellens sju lager. Då ett meddelande skall gå från den ena sidan till den andra börjar meddelandet högst upp på den ena sidan. All data förbereds för att skickas till samma nivå på den andra sidan och skickas sedan till lagret under. Detta lager lägger på den information som skall till motsvarande lager på andra sidan och skickar nedåt. Så fortsätter meddelandet på sändarsidan tills det nått det nedersta lagret. Det nedersta lagret ser till att meddelandet hamnar längst ned på mottagarsidan. Nu har meddelandet en resa framför sig upp på mottagarsidan. Varje lager behandlar den information som var avsedd för det lagret (från sin kompis på andra sidan) och tar bort denna information innan meddelandet skickas uppåt. Så fortgår det tills meddelandet nått toppen på mottagarsidan och ser ut som det gjorde innan det började sin resa.

Vi skall ni titta lite närmare på varje lager:

Applikationslagret

Detta är lagret närmast programvarorna som användaren ser. Det är med detta lager som program som använder nätverket jobbar. Exempel på protokoll från detta lager är FTP, HTTP, och olika protokoll för att dela filer.

Presentationslagret

Används inte så ofta. I detta lager formateras data om utan att förändras. Till exempel om man skall kryptera eller komprimera data i överföringen så sker det i detta lager.

Sessionslagret

Detta lager används inte så ofta. Detta lager håller reda på hur sessioner startas och avslutas. En session kan till exempel vara att ett program har en koppling till en terminal eller databas.

Transportlagret

I detta lager delas data i flera mindre paket. Det gör att nätskiktet lättare kan arbeta. På mottagarsidan ansvarar detta lager för att sätta ihop paketen igen i rätt ordning så att ursprungsstrukturen återfås. I detta skikt hittar vi TCP som används flitigt på Internet och på LAN.

Nätverkslagret

Detta lager ansvarar för vägval och och vidarebefordring av paketen i datanätet. Här jobbar till exempel routrar. Det finns massor av protokoll i detta skikt och det viktigaste i dag borde vara IP som används på Internet och i de flesta LAN.

Datalänklagret

Här hittar vi de accessmetoder vi lärt oss. Till exempel CSMA/CD och Token Passing. Utrustning som jobbar här är till exempel bryggor.

Fysiska lagret

Det fysiska lagret hanterar det fysiska. Det vill säga det som man kan ta på. Här hittar vi kablar, kontakter, spänningar och strömmar. Exempel på utrustning här är STP, UTP, Koax och RJ45. Vanliga enheter är Volt, Ampere och Herz.

Sammanfattning

Kapitel 11. Internet

Internet är utan tvekan det viktigaste datanätet som finns. Internet kan man komma åt från världens alla hörn och tjänsterna på Internet blir fler och fler för varje dag. I detta kapitel tittar vi på hur Internet kom till, hur det fungerar och vad det erbjuder.

Internet är inte heller bara Internet. Den teknik som används på Internet blir allt vanligare även i andra betydligt mindre datornät. Till exempel är det vanligaste nätverksprotokollet i lokala nätverk idag TCP/IP som är samma protokoll som används på Internet.

Internets historia och utveckling

Internet har en väldigt intressant historia i många avseenden. För det första är det väldigt roligt att tala om historia när hela Internet inte ens är 50 år gammalt. En intressant sak med Internets utveckling och historia är att det har utvecklats på ett öppen sätt med bidrag från massor av företag och provatpersoner. Ingen äger internet och väldigt många ser till att det fungerar.

Internets historia

Det vi idag kallar för Internet har även det varit ett litet projekt en gång i tiden. Alla har vi ju varit små. Internet började sin bana som ett forskningsprojekt inom den amerikanska universitetsvärlden. Syftet var att kunna ansluta datorer till varandra över ett stort avstånd. I mitten på 1960-talet var en av pionjärerna J.C.R. Licklider som anses vara den första som kommit på idén med ett världsomspännande nätverk. Han blev sedan chef för ett forskningsprojekt som kallades *DARPA, Defense Advanced Research Projects Agency* som var ett projekt inom dataforskningen där han fick medel till att utvärdera och utveckla sina idéer.

Inom det Amerikanska försvaret hade man liknande tankar som de som utvecklades inom forskarvärlden. Man var sedan länge beroende av kommunikationer över långa sträckor och hade börjat fundera på hur dessa skulle kunna hållas fungerande under krig. Det ultimata problemet man ställdes inför var dåtidens rädsla för atombomber.

Man insåg att kretskopplade nät som till exempel telenäten var väldigt känsliga för störningar. Klipper man av en kabel så försvinner förbindelsen. Kunde man uppfinna ett nätverk där data kunde delas upp i mindre delar och sedan skickas ut i ett nätverk där det fanns flera olika vägar fram och

tekniken själv ser till att alla paket kommer fram, även om det innebär att paketeten tar olika vägar. På så sätt kan systemet hämta sig även om några kommunikationsvägar slås ut.

Det första nätet som byggdes byggdes inom ett projekt som kallades ARPANET. ARPANET var ett paketförmedlat nät, precis som Internet, men från början mycket, mycket mindre. Vissa tjänster utvecklades tidigt, till exempel så kom e-post att bli väldigt populärt i början av 1970-talet.

Allt fler intresserade sig för ARPANET och fler datorer och nätverk anslöts. Ju större det blev desto mer intressant blev det och fler och fler ville ansluta sig. Försvaret hade redan tidigt bestämt sig för att nätverket skulle utvecklas öppet. De hade nämligen inga resurser att utveckla det själva utan måste ta hjälp från universiteten. Detta var en ovanlig situation för en militär organisation där all utveckling i normala fall är topphemlig. Allteftersom nätverket sprider sig blir det mer och mer okontrollerbart och är till slut inte längre intressant för militären. De övergav till slut Internet och började utveckla ett eget nätverk som de kom att kalla MILNET.

Word wide web, WWW

Det som många idag förknippar med Internet är *World wide web* eller WWW som det brukar förkortas eller webben som det populärt kallas. Webben är egentligen bara en funktion av väldigt många på Internet men för många är den, parallellt med e-post, den funktion som är viktigast. När man talar om att "surfa på nätet" är det WWW som man avser.

Ett centralt begrepp på webben är hypertext. Hypertext är text som innehåller hyperlänkar. En hyperlänk är en koppling mellan en viss del av en text eller bild till en helt annan, men relaterad, text eller bild antingen på samma server eller på ett helt annat ställe, kanske på andra sidan jordklotet. Konceptet med hypertext har funnits mycket länge, långt innan tanken på Internet föddes, men har inte före Internet fått en så betydande användning.

Som WWW’s fader anses Tim Berners-Lee. Han var forskare på CERN när han hittade på de första prototyperna av HTTP och HTML. Han bildade sedare (1994) W3C (http://www.w3.org). W3C, som är en förkortning för *World Wide Web Consortium* är ett konsortium som jobbar med standarder och protokoll för webben.

Det största som hänt Internet bör vara när den första grafiska webbläsaren, *Mosaic*, skapades. Den gjorde det möjligt att på ett enkelt sätt navigera bland all den information som gjordes tillgänglig på Internet. Programvaran var så pass enkel att vem som helst skulle kunna använda den. Ett mål med den, och hela Internet, var att det skulle fungera oavsett vilken sorts dator man använde. Redan tidigt hade det bestämts att alla datorer skulle kunna ansluta till nätet bara de följde de protokoll som gäller.

Idag är det vanligaste webbläsarna *Internet Explorer*, *Netscape* och *Mozilla*.

Svensk Internethistoria

Man kan välja att börja den svenska internethistorien vid lite olika tidpunkter. Den kanske mest logiska är att börja den 1988 när *SUNET* kopplades upp mot Internet. SUNET är en förkortning för *Swedish UNiversity computer NETwork*. På den tiden vara bara universitet och högskolor anslutna till SUNET. Sedan anslöts några stora företag till Internet.

Den stora internetboomen i Sverige kom senare. Det var i mitten på 1990-talet då Tele2, precis före Telia, startade ett kommersiellt nät, till vilket vem som helst kunde ansluta sig.

RFC-Dokument

Som sagts tidigare så måste alla aktörer och användare följa samma regler. Eftersom ingen bestämmer enväldigt över Internet så måste man på något sätt ta fram de regler som gäller. För att styra upp Internet så har en rad organisationer upprättats som organiserar olika delar av regelverket som styr Internet. I början var den huvudsakliga vägen att styra regelverket på Internet de så kallade *RFC-dokumenten*. RFC står för Request For Comments som betyder ungefär "Förfrågan om kommentarer" och det fungerade ungefär så här. En organisation, företag eller forskare kommer på ett bra protokoll eller program och skriver en RFC om detta. Denna RFC läses av alla intresserade och de har möjlighet att kommentera den. Alla har, i demokratins anda, möjlighet att läsa, och kommentera, dokumenten. Då ett dokument kommenterats och uppdaterats tills alla ha blivit nöjda anses det vara en standard som gäller.

Idag fungerar det lite annorlunda. De RFC:er som publiceras idag är oftast redan färdiga standarder men likväl kan de läsas av alla så att alla skall ha samma chans att skriva programvaror som följer de standarder som specificeras i dokumenten.

I appendix J finns länkar till några av de RFC:er som behandlar det vi tagit up i denna bok samlade.

Att ansluta till Internet

Det finns idag så många sätt att ansluta till Internet att man kan tycka att det är svårt att välja. I praktiken är det dock nästan aldrig några problem eftersom urvalet kraftigt styrs av var du bor eller var företaget ligger och hur mycket man är villig att betala, det vill säga vilket behov man har.

Privatpersoner och mindre företag

Som sagt så kan man ansluta till Internet på en uppsjö av olika sätt. Man kan till exempel använda ett vanligt telefonabonnemang och en dator med modem. Denna metod kallas vardagligt för uppringt Internet. Uppringt Internet är väldigt enkelt och fungerar överallt där det finns telefon. Denna metod är väldigt vanlig bland de som inte använder Internet så ofta eller av dem som bor på ett ställe där inga alternativ ges. Använder man Internet väldigt lite är detta det i särklass billigaste sättet.

Nackdelen med uppringd Internet är att det är ganska långsamt och att det oftast är förknippat med en samtalsavgift. Det vill säga du betalar för den tid du är ansluten till Internet även om du inte använder anslutningen. Detta inbjuder till att man kopplar ner sin anslutning till Internet när man inte använder den. Ytterligare en nackdel är då att det tar en stund att koppla upp sig igen. För inte alls många år sedan var detta det enda sättet en privatperson kunde ansluta sin dator till Internet. Den maximala anslutningshastigeheten ligger på ungefär 56 kbit/s med ett vanligt modem.

Det finns snabbare sätt att ansluta till Internet via telefonlinjen. Men till skillnad från modemet ovan så ställer dessa metoder mer krav på telefonförbindelsen och kräver installationer såväl i hemmet som i telefonsystemet. De metoder som avses är ISDN (Integrated Services Digital Network) och olika varianter av DSL (Digital Subscriber Line). De vanligaste ISDN linjer man ansluter hemma kallas för en basanslutning. Den gör så att man får två stycken linjer till sitt jack (som måste vara ett specialjack) dessa två kan man antingen använda till data eller till samtal. Använder man en till data klarar den maximalt 64 kbit/s och använder man båda till data så kommer man upp i maximalt 128 kbit/s. Använder man bara den ena så kan man tala i telefonen samtidigt som man använder Internet men det går naturligtvis långsammare än om man använder båda. ISDN är oftast, precis som med ett vanligt modem, förknippat med en avgift som är beroende på hur länge man är uppkopplad men till skillnad från vanliga modem så går en uppkoppling med ISDN väldigt fort. Det gör att man kan koppla upp och ner mer frekvent med ISDN. En annan fördel med ISDN är att det är något snabbare än ett vanligt modem.

DSL tekniken är en modernare teknik än ISDN. Men den kräver ytterligare lite till av telenätet och går därför inte att installera överallt där man kan få ISDN eller använda ett vanligt modem. Den vanligaste varianten av DSL som använde i Sverige är ADSL (Asymmetric Digital Subscriber Line) det innebär att hastigheten man kan komma upp i skiljer sig beroende på om man skickar eller tar emot data. Vanligtvis så går det snabbare att hämta data från Internet än vad det gör att skicka data till Internet. Eftersom man oftast hämtar data från Internet så har detta oftast ingen större praktisk betydelse. Hur snabbt det kan gå med ADSL beror på hur lång ledning du har från ditt hem till en telestation. Ledningens kvalitet påverkar också. Med ADSL ligger hastigheten för nedladdning någonstans mellan 1 och 8 mbit/s och uppladdning någonstans mellan 0,5 och 1 mbit/s. Observera att din Internetleverantör (ISP) kan sätta en lägre hastighet än den teoretisk möjliga.

Med DSL-teknik är man normalt uppkopplad hela tiden med samma hastighet. Man betalar antingen

ett fast pris per månad eller så betalar man beroende på hur mycket man använder anslutningen, det vill säga hur mycket data man skickar och hämtar.

Företag

Det sätt vi behandlat hittills passar privatpersoner. De kan naturligtvis även användas av företag som företaget inte har större behov. Företag har annars flera andra sätt att ansluta till Internet beroende på vilka behov de har.

Oftast använder företag någon typ av fast förbindelse till Internet. Det vill säga att de har en konstant koppling till en av Internetleverantörernas routrar och får på så sätt en stabil koppling till Internet. Inte sällan har större företag två eller flera kopplingar för att inte vara beroende av en enda. De kan till exempel ha en förbindelse mellan två kontor i olika städer och sedan en Internetförbindelse i varje stad. Går den ena Internetförbindelsen ner så märker inte användarna det utan surfar vidare genom förbindelsen till det andra kontoret och ut på Internet via deras Internetförbindelse.

När det gäller kapaciteten på Inernetanslutningar för företag och skolor så finns det egentligen inga begränsningar. Bara priset sätter gränsen. Hur mycket man är villig att betala beror naturligtvis på vilket behov man har. Behovet beräknas utifrån vilken verksamhet man bedriver och hur många samtidiga användare man har. Anslutningar från 10mbit/s och upp till hundratals mbit/s är vanliga.

Ytterligare metoder att ansluta till Internet

Det har länge funnits ett behov av snabba billiga Internetanslutningar i Sverige. Ett stort behov medför många förslag på hur det skall tillgodoses. Detta gör att det finns ett otal andra sätt att ansluta sig till Internet.

Man kan till exempel koppla upp sig mot Internet via kabel-tv-näten. Denna metod är relativt vanlig i de städer där kabeltv finns. Man kan även på vissa ställen i landen använda elnätet för att koppla upp sig. Man kan även använda radio för att ansluta ett avlägset hus eller villaområde. På vissa ställen kan man få fiberkabel ända in till huset eller till ett område vilket ger en mycket snabb och bra Internetförbindelse.

Även på det mobila området förekommer mycket nytänkande. Man kan till exempel utan problem koppla upp sig mot Internet med de flesta moderna mobiltelefoner. Man kan också i vissa butiker koppla upp sig mot Internet via Bluetooth eller radio-LAN.

Vanliga tjänster, program och protokoll på Internet

Det säger sig självt att om så många datorer skall fungera ihop så måste de använda ett och samma protokoll. Vidare verkar det kanske uppenbart att ett så stort och mångfaldigt nätverk som Internet måste ha flera protokoll.

En annan sak som säger sig självt är att när en massa datorer kopplas ihop och en massa människor börja använda dem så skapas en marknad för en mängd olika tjänster. Dessa tjänster kräver i sin tur sina egna program och sina egna protokoll.

TCP/IP

Det protokoll som är absolut viktigast på Internet är TCP/IP. TCP/IP är standardprotokollet på Internet. Namnet TCP/IP är egentligen en hel familj protokoll. Namnet TCP/IP kommer från två av de ingående protokollen, nämligen IP och TCP. IP står för Internet Protocol och är det protokoll som ansvarar för hur alla datorer skall hitta varandra på Internet. Alla datorer på Internet har en så kallad IP-adress. Denna adress är unik och det är tack vare denna som paket som skall till din dator kommer fram just till din dator. Om vi jämför med OSI-modellen (avsnittet *OSI-modellen* i kapitel 10) som vi tittat på tidigare så ligger IP i nätverksskiktet.

Vi kommer inte att behandla TCP/IP så mycket i detta kapitel. Det kommer mer om det längre fram i boken. Vi skall i detta kapitel titta på de protokoll och program som används högre upp i modellen.

WWW (HTTP)

World Wide Web (WWW) var det system som satte riktig fart på Internet. WWW paketerades med snygga program som var lätta att använda. WWW är det system som vi använder när vi "surfar" på nätet. Det verktyg som man använder kallar för webbläsare (eng. browser). Det protokoll som används heter *Hypertext Transport Protocol (HTTP)*. Med hypertext menas text som innehåller hyperlänkar. Men hyperlänk menas en koppling från det man läser till relaterad text någon annanstans. Det är genom att följa hyperlänkar som man surfar på nätet.

Hypertext är inget som kommit till i och med Internet utan det har funnits tidigare i vissa programvaror och begreppet som sådant har använts, om än inte i samma utbredning som nu, sedan andra värdskriget.

För att använda WWW måste man ha en webbläsare. Vänliga webbläsare är Netscape Navigator, Internet Explorer och Mozilla. I figur 11-1 visas en webbläsare som heter Konqueror och är en

grafisk webbläsare. Grafiska webbläsare är enormt populära och finns till i princip alla operativsystem. Den som visas på bilden heter Konqueror.

Figur 11-1. Den grafiska webbläsaren Konqueror

Filöverföring (FTP)

När man använder http (se ovan) så hämtar man ju filer från servern för att visa dem i sin webbläsare. Men eftersom http är tänkt för att användas av webbläsare så saknar det mycket av den funktionalitet som man vill ha i ett protokoll för filöverföring. Till exempel så är det bökigt att ladda upp filer till servern med http och det går inte att byta namn eller radera en fil på servern med http. Eftersom man tidigt kom fram till att man vill flytta filer mellan datorer på ett nätverk så skapades ett speciellt protokoll för detta. Man kallade protokollet för *File Transfer Protocol (FTP)*. Ftp har stöd för alla funktioner man förknippar med att flytta filer mellan datorer. Det finns flera program för att använda ftp och ftp stöds dessutom av flera vanliga filhanterare.

Nyhetsgrupper, Usenet News (NNTP)

Usenet news eller nyhetsgrupper är ett hörn av Internet som många glömmer bort. En nyhetsgrupp har inte så mycket med nyheter att göra utan handlar om diskussioner. Usenet News fungerar lite som e-postlistor. Det finns hundratusentals nyhetsgrupper världen över. De flesta speglas mellan servrarna så på din newsserver kommer även postningar från andra länder. Alla grupper har ett

specifikt ämne. Vissa har ett speciellt språk. Till exempel så finns det grupper som behandlar olika datorsystem på svenska. Om det inte framgår vilket språk som gäller så är det alltid engelska.

Det går till så här. När någon postar ett meddelande i en grupp så kan alla som prenumererar på gruppen se detta i sitt nyhetsläsarprogram (många e-postprogram kan också hantera news). De andra ser bara rubriken och kan själva välja om de vill ladda ner och läsa meddelandet.

Usenet News eller nyhetsgrupper är faktiskt äldre än Internet självt. Från början, innan Internet, användes ett protokoll som heter UUCP (Unix to Unix Copy Protocol), men detta ersattes senare med ett protokoll som var bättre anpassat för Internet. Det protokollet heter NNTP (Network News Transfer Protocol) och används än idag.

Fjärrinloggning (TELNET/SSH)

Ett operativsystem som utvecklades väldigt mycket på samma tid som Internet och med nätverk i åtanke var Unix. Det gör att Unixsystem fungerar väldigt bra i nätverk. Till exempel så kan man på en Unixdator jobba flera personer på samma gång och man kan göra det över nätverket precis som om man satt direkt vid datorn. Låter det modernt? Det har man kunnat i Unix sedan 1970-talet. En modern Uniximplementation är Linux. Linux har ärvt dessa egenskaper från sin föregångare och har alltså haft dessa möjligheter från starten

För att kunna logga in på en server över nätverket måste man naturligtvis ha ett protokoll för hur det skall fungera. Ett vanligt, ganska gammalt, protokoll är telnet. Telnetklienter följer med de flesta operativsystem.

Telnet används idag mindre och mindre. Den största anledningen är att det är ett så kallat klartextprotokoll. Informationen som skickas mellan server och klient krypteras inte. Det gör att den kan avlyssnas. Det finns massor av klartextprotokoll som används på Internet och i de flesta gör det ingenting om trafiken kan avlyssnas. I fallet med telnet däremot är trafiken väldigt känslig. Anledningen är att användarnamn och lösenord skickas i början av en session. Om någon avlyssnar kommunikationen får får denne kompletta kontouppgifter och kan logga in på servern.

Ett nyare protokoll som heter SSH (Secure SHell) som erbjuder samma funktionalitet som telnet men som är mycket säkrare. Klienter finns till de flesta operativsystem men installeras inte alltid som standard vilket telnet ofta gör.

Om nu SSH är så mycket säkrare, varför finns telnet kvar? Telnet har fortfarande ett användningsområde. Till exempel används ofta telnet för att konfigurera hårdvara, till exempel switchar. Då används det på ett internt nätverk där risken för avlyssning bedöms som liten. Till

exempel en ensam kabel mellan server och klient.

Internets framtid

Vad som kommer att hända med Internet i framtiden är naturligtvis svårt att säga. På sista tiden har de största förändringarna skett bland rena konsumentprodukter såsom fildelning och direktmeddelanden (IM, Instant Messaging).

Vad som kommer i framtiden går bara att gissa. Det har talats om tekniska förändringar i Internets struktur. Bland annat finns planer på att byta ut en så grundläggande del som IP (Internet Protocol, se nästa kapitel) för att bland annat råda bot på bristen på IP-adresser. Som det ser ut nu är detta inte att vänta de närmaste åren. Utan nyheterna kommer högre upp i strukturen, på applikationsnivån.

Det som "bubblar" nu är olika telefontjänster. Att man kan tala med varandra över Internet. Det kommer som en naturlig förlängning på IM-tjänsterna och kommer förmodligen att bli väldigt vanligt.

Smarta-hemtjänster var väldigt hett för ett par år sedan men blev ingen hit. Jag tror att dessa kommer att komma igen när marknaden mognat. Exempel på tjänster är att till exempel kunna titta in hemma med hjälp av kameror från jobbet eller på semestern. Andra tjänster kan vara larmtjänster där man meddelas via e-posts, SMS eller varför inte till sin IM-programvara om något händer hemma.

En sak jag med säkerhet kan säga är dessa nya tjänster kommer att kräva mer och mer bandbredd. Och mer bandbredd kommer att finnas. Det kommer att bli enklare att koppla upp sig och med mer bandbredd än vad vi är vana med idag. Snabba uppkopplingar med mobila enheter kommer också att bli vanligare.

Sammanfattning

Kapitel 12. Mer om Internets teknik

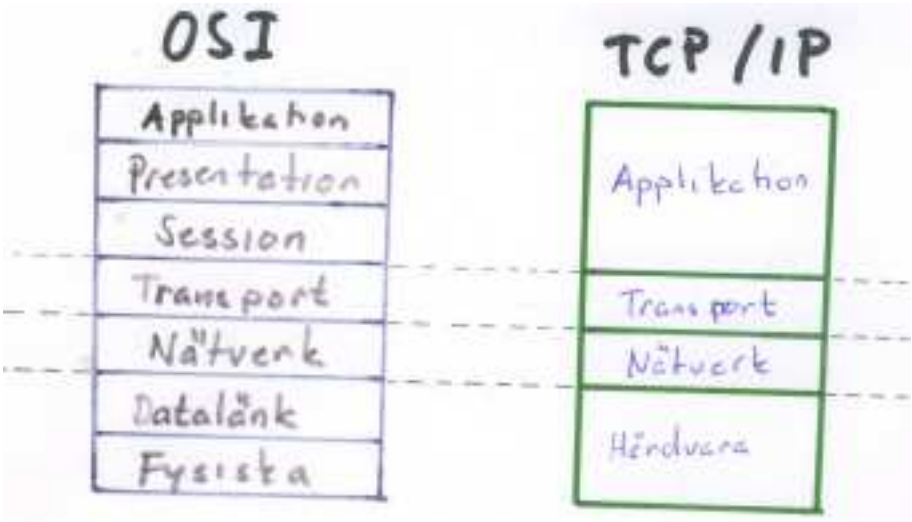
Vi har i föregående kapitel tittat på Internet och hur det används. I detta kapitel skall vi titta närmare på tekniken som gör Internet möjligt. Efter att ha läst detta skall du förstå hur Internet fungerar och kunna utföra enklare felsökning.

TCP/IP

TCP/IP är en grundläggande teknik som används på Internet. TCP/IP är det protokoll, eller riktigare, den familj av protokoll som bygger upp Internet. TCP/IP står för *Transmission Control Protocol/Internet protocol*. Standarden TCP/IP har fått sitt namn av två av dess ingående protokoll, nämligen TCP och IP. Andra protokoll som ingår i standarden och som vi kommer att bekanta oss med är UDP, ICMP och ARP. Vi kommer även att titta på protokoll på lite högre nivå, till exempel FTP, HTTP, SMTP, och DNS.

Precis som OSI-modellen (se avsnittet *OSI-modellen* i kapitel 10) så är TCP/IP-modellen uppdelad i lager enligt samma princip som modellen från ISO. I TCP/IP-modellen har man slagit ihop några av lagren för att få enklare implementationer. I figur 12-1 visas en figur över modellerna och hur deras lager är relaterade till varandra. Vi ser även exempel på protokoll i de olika lagren. Till vänster ser vi OSI-modellens sju lager. Till höger ser vi att TCP/IP har 4 lager och hur de är relaterade till OSI-modellen. Vissa delar upp TCP/IP-stacken i 5 skikt. Då är det nedersta lagret uppdelat på samma sätt som i OSI-modellen.

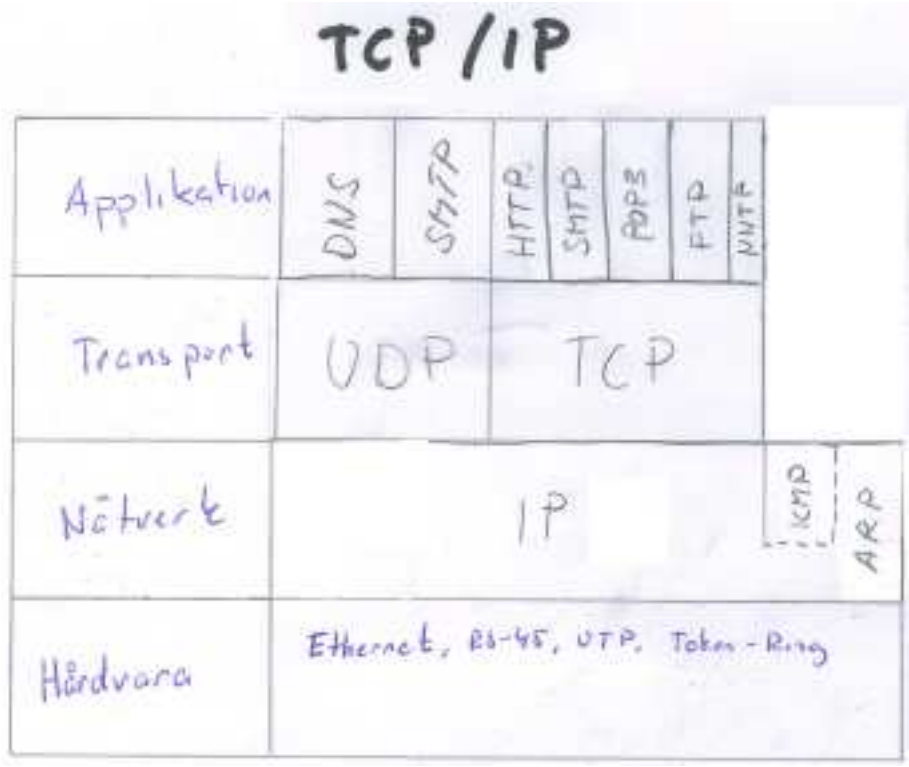
Figur 12-1. OSI modellen kontra TCP/IP



Några av protokollen i TCP/IP

I detta avsnitt behandlas de olika protokollen mycket kortfattat. Vissa kommer inte att behandlas mer och andra kommer vi att gå igen lite djupare på andra ställen i boken. Du kan också komma att stöta på dem i laborationskursen.

Figur 12-2. Några av protokollen i TCP/IP



IP

IP är en förkortning för *Internet Protocol*. IP är det protokoll som ser till att data kommer från en nod till en annan. IP är vad man brukar kalla för ett *connectionless* protokoll. Det innebär att det inte finns en koppling mellan sändare och mottagare utan paketen skickas ut i nätet och kommer fram om det kommer fram. Man kan jämföra det med att skicka ett brev med posten. Man skriver det och skickar iväg. Det finns ingen direkt förbindelse mellan sändare och mottagare. Kommer brevet fram så gör det, annars inte. Vill man veta att brevet verkligen har kommit fram måste man be mottagaren bekräfta detta vilket görs i en del av protokollen ovanför IP i OSI-modellen. IP hittas i nätverksnivån i OSI-modellen.

TCP

TCP står för *Transmission Control Protocol*. TCP är det vanligaste transportprotokollet på Internet. TCP är vad man brukar kalla för *connection oriented*, det vill säga det skapas en koppling (connection) mellan sändare och mottagare, precis som under ett telefonsamtal. Vi inser ju att den bara är virtuell eftersom den bygger på IP, men alla överliggande lager ser det som en koppling. I TCP finns funktioner som ser till all data som sänds mellan noderna kommer fram och att den inte blir förstörd. På IP-nivån kan detta åstadkommas genom att paketen som skickas måste kvitteras. Precis på samma sätt som jag kan veta säkert att ett brev kommit fram om jag ber mottagaren bekräfta det.

UDP

UDP är också ett vanligt protokoll på Internet. UDP är en förkortning för *User Datagram Protocol*. Till skillnad från TCP så är det *connectionless*, vilket betyder att det fungerar som det underliggande IP i det avseendet. I UDP finns alltså ingen garanti för att alla paket kommer fram. UDP används till exempel till DNS och i många program som streamar media av något slag där det är viktigare att data kommer fram i tid än att alla data kommer fram.

ICMP

ICMP som är en förkortning för *Internet Control Message Protocol* är ett protokoll som används för ruting och annan funktionalitet samt för kontroll och felmeddelandehantering i ett TCP/IP-nät. Programmen "ping" och "traceroute" är exempel på program som använder ICMP. ICMP är, precis som UDP, connectionless så man kan inte garantera att paketen kommer fram.

ARP

ARP (Address Resolution Protocol) använs för att en nod skall kunna hitta MAC-adressen[1] till en annan nod. Detta är nödvändigt eftersom nätverkslagret inte använder samma typ av adresser som underliggande lager. För att de skall kunna tala behöver noden veta den andres IP-adress som är känd från nätverkslagret och uppåt (mer om IP-adresser nedan) men för att de faktiskt skall kunna prata måste den veta dess MAC-adress som används i de underliggande lagren. För att hitta den används ARP. Det fungerar så att den dator som skall sända skickar ut en *broadkast*-förfrågan (en broadkastförfrågan kommer till alla datorer på nätverket) där den ber noden med den aktuella IP-adressen att svara. När den svarar får den nod som skickar redan på dess MAC-adress. För att varje nod inte skall behöva göra ARP-förfrågningar varje gång den skall sända sparas MAC-adresserna i en tabell på varje nod.

1. MAC-adress kallas även Fysisk adress eller hårdvaruadress

IP-adresser

För att man skall hitta alla datorer i ett TCP/IP nät så måste de ha en unik adress. Precis som alla telefoner anslutna till ett globalt telefonnät måste ha unika telefonnummer. Precis som i telefonfallet kan olika datorer ha samma nummer men de kan inte sitta på samma nät. Två telefoner kan ha nummer 12345 men de kan ju inte finnas på samma riktnummer. Skulle de sitta på samma riktnummer så får de inte finnas inom samma land utan måste skiljas åt med olika landsnummer. Huvudsakligen är att det totala telefonnummret är unikt. IP-adresserna byggs upp av olika delar, precis som ett telefonnummer.

Man delar upp en IP-adress i datoradress (host address) och nätverksadress (network address) för att, på samma sätt som i telefonnätet, kunna dela upp nätverket (Internet) i mindre delar. För att man skall hitta fram mellan de olika delarna använder man en teknik som kallas routing. Vi kommer att tala mer om det senare i denna bok.

En IP-adress består av ett tal som är 32 bitar stort. Detta tal brukar delas upp i fyra delar om vardera 8 bitar. Man brukar ange delarna decimalt. Det vill säga med basen tio som vi är vana. 8 bitar ger 256 olika kombinationer så varje del i en IP-adress kan vara mellan 0 och 255. De fyra delarna åtskiljs med . (punkt). Exempel på en giltig IP-adress är 192.168.100.10. Precis som med telefonnummer så består denna IP-adress av olika delar. En del är datornamnet och en annan del är adressen till det nätverk där datorn finns. Till skillnad från telefonnummer så är avgränsningen mellan datornamn och nätverksnamn lite mer flytande och syns inte direkt i adressen.

Vilken del av adressen som är nätadress och vilken som är datoradress beror på vilket nätverk man sitter på. Traditionellt så delar man in nätverken i tre olika klasser, A, B och C. Det finns även D och E men dessa behandlas inte i denna bok. Om man delar in IP-adressen i dess fyra talgrupper w.x.y.w så gäller tabell 12-1.

Tabell 12-1. Nätverksklasser

Klass	Nätadress (N)	Datoradress (D)	Nätmask	Antal nätverk	Datorer / Nätverk
A	N.X.X.X	X.D.D.D	255.0.0.0	126	16 777 214
B	N.N.X.X	X.X.D.D	255.255.0.0	16 384	65 534
C	N.N.N.X	X.X.X.D	255.255.255.0	2 097 152	254

Det är alltså med hjälp av nätmasken som man avgör hur stort ett nätverk är. Med hjälp av IP-adressen och nätmasken kan man lista ut vilken del av en IP-adress som är datoradress (host address) och vilken del som är netverksadress (network address). Ett förenklat sett att förklara det är att man genom att titta på nätmasken kan se vad som är nätadress och datoradress. Den del av IP-adressen som består av 255:or är nätverksadressen och de som består av 0:or är datoradressen (hosta ddress). Detta är en förenkling av verkligheten, se appendix I om du vill veta mer.

Den observanta läsaren har redan insett att antalet tillgängliga nätverk inte kommer att räcka till alla datorer som finns på Internet. Det finns flera lösningar på detta. Ett sätt är att dela in adresserna i fler mer finfördelade klasser än A, B och C. Detta gör man redan idag för att få fler nätverk. Man kan till exempel ha nätverk med bara 8 eller 32 IP-adresser. Läs med om detta i appendix I. Det finns också en teknik som kallas NAT *Network Address Translation* som gör att man kan gömma hela nätverk bakom en enda IP-adress. Genom att använda denna teknik så kan man ha samma IP-adresser på flera datorer bara de sitter på ett nätverk som använder NAT för att komma ut på Internet. Läs mer om detta i avsnittet *Routing* . Detta är idag det vanligaste sättet att ansluta företagsnät. Det har flera fördelar, till exempel så höjs säkerheten eftersom datorerna inne på nätverket har adresser som inte finns på Internet. Det finns speciella adress-serier för detta som vi ser i avsnittet *Routing* . En annan uppenbar fördel är att företaget bara behöver några få publika IP-adresser. Det finns också nackdelar med denna metod, till exempel om någon av datorerna på det interna nätet av någon anledning behöver göras tillgänglig på Internet. Men det är som regel inget som förekommer i lokala nät som drivs av säkerhetsmedvetna administratörer[2].

Det finns också en mer permanent lösning på problemet. Det finns en helt ny version av IP-protokollet som heter IP version 6. Med IP version 6 kommer det inte att råda någon brist på vare sig IP-adresser eller nätverksadresser. Problemet är att bytet från nuvarande version, IP version 4, till den nya inte är enkel och kommer att skapa problem. IP version 6 behandlas inte i denna version av denna bok.

Portnummer och tjänster

Som vi sagt tidigare så kan en och samma dator tillhandahålla en mängd olika tjänster. Till exempel så kan en dator vara både webbserver, e-postserver och DNS-server på samma gång. För att inte trafiken till de olika tjänsterna skall krocka med varandra så måste man på något sätt dela upp den. Till exempel så förstår ju inte en webbserver den trafik som är menad till en e-postserver även om de körs på samma dator. För att komma till rätta med detta så har man infört i protokollet något som kallas för portar. Man skulle kunna jämföra det med ett hyreshus. Hela huset är datorn och varje lägenhetsdörr är en port. I varje lägenhet bor en tjänst. I lägehet nummer 80 bor till exempel webbtjänsten så om någon pratar med port 80 på datorn så pratar den bara med webbtjänsten. Portar är alltså inte något fysiskt på datorn utan bara en logisk uppdelning av tjänsterna. Varje tjänst är kopplad till en port på datorn. En dator kan ha ungefär 65000 portar.I lägehet nummer 80 bor till exempel webbtjänsten så om någon pratar med port 80 på datorn så pratar den bara med webbtjänsten. Portar är alltså inte något fysiskt på datorn utan bara en logisk uppdelning av tjänsterna. I lägehet nummer 80 bor till exempel webbtjänsten så om någon pratar med port 80 på datorn så pratar den bara med webbtjänsten. Portar är alltså inte något fysiskt på datorn utan bara en logisk uppdelning av tjänsterna.

2. Se även brevet från Bengt Gördén i appendix K

För att man skall veta bakom vilken port som en viss tjänst finns (jämför lägenhetsdörr) så har man kommit fram till vissa standardportar som brukar användas. Till exempel så körs nästan alltid webbservern på port 80 och e-postservern på port 25. I appendix G finns en lista av de vanligaste portarna och vad de används till. Där finns även en referens till var man hittar fler.

URL Uniform Resource Locator

En URL är en adress som används för att referera till en viss tjänst på en viss dator någonstans i världen (Internet). En URL består av tre olika delar. Vi tittar på en URL: *http://www.se.linux.org:80/support*. Den första delen är det som kommer före *://*, i vårt fall *http*. Http står för *Hypertext Transfer Protocol* och används för att läsa webbsidor från en webbserver. Andra exempel på vanliga protokoll i URL:er är ftp och https som är för filöverföring respektive säker överföring av webbsidor. Den andra delen är datornamnet, se kapitlet om DNS längre fram i boken. Om datornamnet har ett kolon i sig så är det som kommer efter ett portnummer. Normalt sett så behöver man inte ange portnummer om tjänsten man skall komma åt körs på sin standardport, men om den körs på en icke-standardport så måste man tala om detta. Den sista delen är en adress till något på den dator man ansluter till. I vårt fall en webbsida.

Routing

På Internet finns en otrolig mängd datorer. Du kan blixtsnabbt läsa en sida på en dator i Australien för att nästa sekund läsa en på en dator i USA. Att detta fungerar och går så fort är inget under utan ingenjörskonst. I detta avsnitt skall vi behandla hur det går till.

Paketförmedling

Till att börja med så är en del i hemligheten att Internet (TCP/IP) är ett paketförmedlande nät. Det betyder som vi sagt tidigare att all trafik mellan två datorer delas upp i små paket som skickas oberoende av varandra igenom nätverket.

För att alla paket, eller åtminstone så många som möjligt, skall komma fram används en teknik som kallas för routing.

Routing i korthet

På Internet finns en mängd olika routrar. De fungerar som små postkontor som tar emot paket från olika håll och beroende på vart de skall skickar dem vidare åt olika håll. Varje router står i kontakt med andra routrar och de samarbetar så att varje router vet vilka delar av nätet som varje router kan

komma åt. På så sätt kan en router välja vilken av sina grannar som bäst kan förmedla det aktuella paketet. Det finns flera alternativa väger för ett paket att komma fram så om någon router går ner så märker dess granne detta och letar efter en annan router som kan komma åt de delar av nätet som den som gick ned. Det kan innebära att paketen får ta en liten omväg men de kommer i alla fall fram. Det kan även hända att den kortaste vägen för tillfället är överbelastad. Då kan en router välja att skicka paketeten en annan väg.

Systemet består alltså av en mängd olika routrar som känner till sin omgivning genom att de med hjälp av bestämda protokoll samarbetar med sina grannar om de olika möjliga vägarna till olika mål och därefter tar emot och skickar datapaket åt olika håll beroende på var de skall.

Time to live (TTL)

Man kan lätt tänka sig att det kan uppstå problem i detta system. Tänk om någon router får fel information av någon anledning och börjar att skicka paket åt fel håll eller tänk om ett paket har en konstig adress som ingen vill veta av. För att förhindra att paket åker runt i all evighet på Internet så har varje paket ett fält med ett heltal som kallas för *Time To Live (TTL)*. Detta fält börjar på ett tal och minskas av varje router som tar i paketet med ett. Om paketet kommer till en router med TTL=0 så kastar denna router bort paketet. På så sätt kommer inget paket att åka runt för evigt.

Statisk routing, default gw

Vi har i tidigare kapitel talat om nätmasker (netmask). Anledningen till att man har en sådan är just routing. Man måste veta lite om det nätverk som man tillhör för att veta om en dator eller nod man söker finns på det nätet eller på ett annat.

Studera exemplet i figur 12-3.

Figur 12-3. Nätverksexempel

Till vänster i denna bild syns ett lokalt, internt nätverk. Det har nätverksadressen 192.168.0.0 och nätmasken 255.255.255.0. På det nätverket finns maskinerna 192.168.0.1 och 192.168.0.2 samt en router på 192.168.0.254. Denna router har en publik IP-adress som är 10.0.0.9. Routern är kopplad till Internet (eller i själva verket till ytterligare en router) och där, på Internet, finns bland annat datorn se.linux.org (213.141.74.169).

I figuren figur 12-3 så kan 192.168.0.1 direkt få kontakt med 192.168.0.2. De sitter ju på samma nätverk och kan tala med varandra direkt. Skall 192.168.0.1 däremot komma åt se.linux.org (213.141.74.169) så måste paketen går via 192.168.0.254. Detta sker med hjälp av den så kallade routingtabellen som finns på alla nätverksanslutna datorer.

Routingtabellen på 192.168.0.1 och 192.168.0.2 ser ut så här:

```
Destination   Netmask          Gateway           Interface
192.168.0.0   255.255.255.0    0.0.0.0           eth0
0.0.0.0       0.0.0.0          192.168.100.253   eth0
```

Routingtabellen fungerar så att varje paket som skall skickas iväg från en maskin kontrolleras mot en routingtabell. Paketet jämförs med varje rad. Om IP-adressen passar in i kombinationen av destination och nätmask (det vill säga skall det det nätet) är det den regeln som gäller. Routingtabellen läses uppifrån och ner och den första raden som stämmer blir den som gäller. Hittas ingen regel som stämmer kan inte paktet levereras. För att undvika detta brukar man ha en regel i slutet som gäller för alla adresser. Det vill säga, har inget annat passat så gäller denna. En sådan regel för man om man använder nätmasken 0.0.0.0 eftersom en sådan markerat ett nätverk som består av hela Internet.

Skall man skicka ett paket till något annat ställe än det interna nätet så måste man använda en router, eller gateway som det brukar kallas på ett Internt nätverk. Man kan bara skicka ett paket till en nod man har kontakt med, det har man med en gateway och den kan skicka paketen vidare. Den router som pekas ut i den sista regeln, den som fångar upp alla paket som inte hittat rätt i tidigare regler brukar kallas för *Default Gateway*, det vill säga den gateway som man skall kontakta för att lämna det lokala nätet.

I exemplet tittar vi på datorer på ett lokalt nätverk. Dessa har vad man brukar kalla *statiska routingtabeller*. En dator kan antingen konfigureras i nätverksinställningarna att använda en speciell routingtabell eller så får den tabellen av en en server på nätet. Sedan ändras inte denna tabell utan den är statisk. Routrar på Internet som inte gör annat än att routar har som regel dynamiska routingtabeller. Som vi sagt tidigare är en av fördelarna med Internet att ett paket kan ta flera olika vägar för att komma fram. Om alla routrar på vägen hade statiska routingtabeller skulle alla paket mellan två platser alltid gå samma väg, precis som de alltid går via samma gateway i exemplet. Istället för statiska tabeller använder routrarna på Internet ett speciellt protokoll för att deras

routingtabeller alltid skall vara aktuella. De håller ständigt reda på sina grannar och vet vilken väg de skall skicka paket för att nå olika nät. I övrigt fungerar routrar enligt precis samma princip som routingtabellen i din dator.

NAT, Network Address Translation[3]

Som vi nämnt tidigare så finns det inte oändligt med IP-adresser på dagens Internet. Det gör att företag idag inte får hur många IP-adresser som helst. Ett sätt att spara adresser är att använda sig av privata adresser på sitt interna nätverk och sedan använda en router eller gateway som har en publik adress på Internet. Denna router översätter sedan de interna adresserna så att alla datorer på den interna nätverket använder en och samma adress när de ansluter till Internet.

Det finns, som nämnts tidigare, flera fördelar med detta än att man sparar IP-adresser. En annan fördel är att säkerheten höjs för de datorer som är på det interna nätverket eftersom de har IP-adresser som inte syns på Internet, de göms ju bakom routern.

Eftersom IP-adresserna på det interna nätverket aldrig kommer att synas på Internet så kan dessa vara vilka adresser som helst. För att man inte skall riskera att använda adresser på det interna nätet som finns på Internet (då skulle man ju inte komma åt den datorn eftersom deras adresser skulle kollidera) så finns det speciella adresser som bara är avsedda att användas på Interna nät. Dessa kallas ibland för svarta adresser eftersom man aldrig skall stöta på dessa på Internet. Dessa adresser specificeras i RFC 1918 (se appendix J) och är:

10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Som vi ser så är det olika stora nätverksklasser. Till exempel så är det lämpligt att använda 10.X.X.X om man behöver ett klass A nät, 172.16.x.x om man behöver ett klass B nät och 192.168.0.x om man behöver ett klass C nät. Men inget hindrar att man använder ett klass C nät som börjar på 10 eftersom man gör som man vill med dessa adresser.

Observera att vissa ISP:er använder dessa adresser i sina nät. Till exempel använder telia 10.0.0.0 till sina kunder. Tänk på att kolla detta innan du väljer att använda dessa adresser.

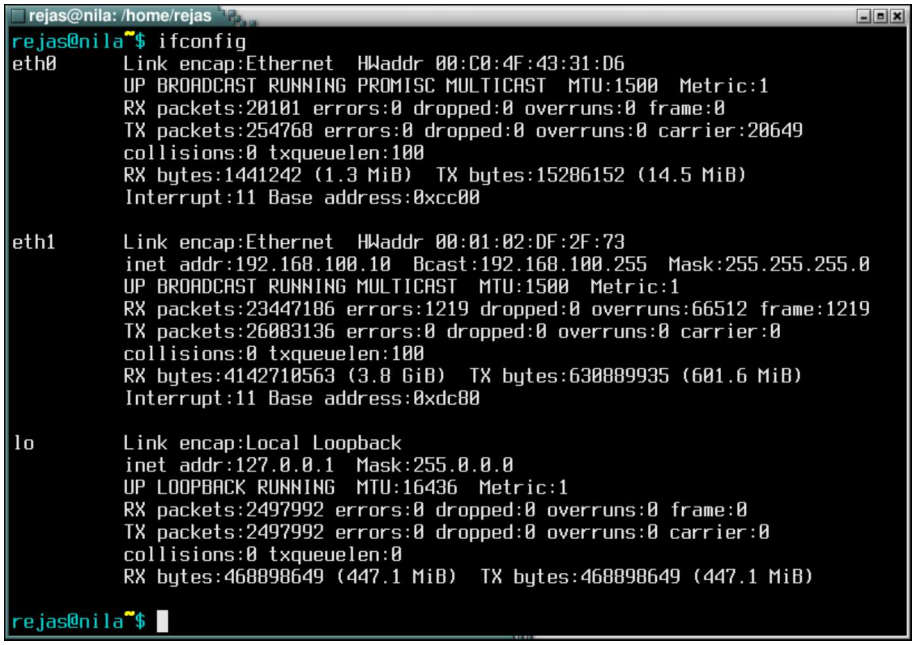
Felsökning i TCP/IP-nätverk

3. Se även brevet från Bengt Gördén i appendix K

Ifconfig

Ifconfig[4] är ett program som visar, eller ändrar de nätverksgränssnitt som finns på datorn. Vi skall i detta avsnitt inte ändra på nätverkgränssnitten utan bara titta på dem.

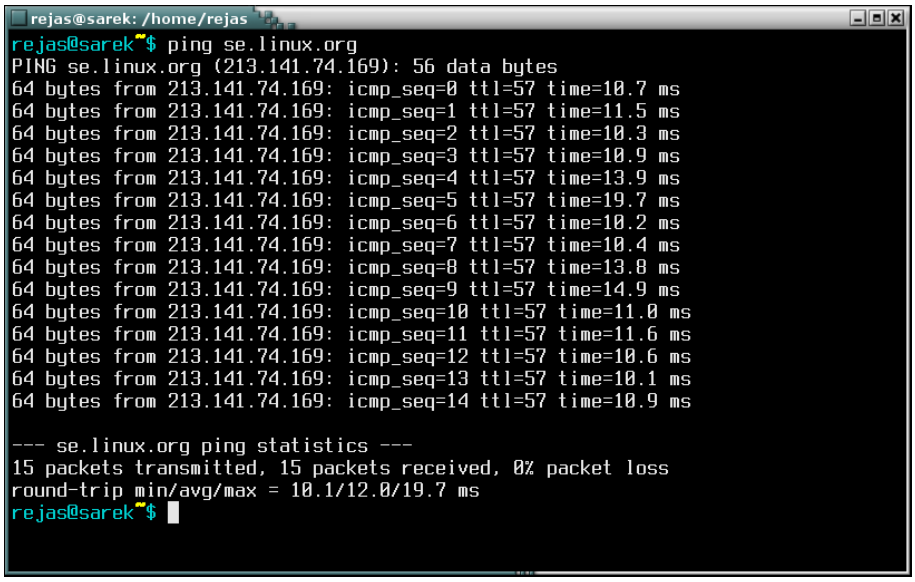
Figur 12-4. Skärmdump: ifconfig på Linux



Ping

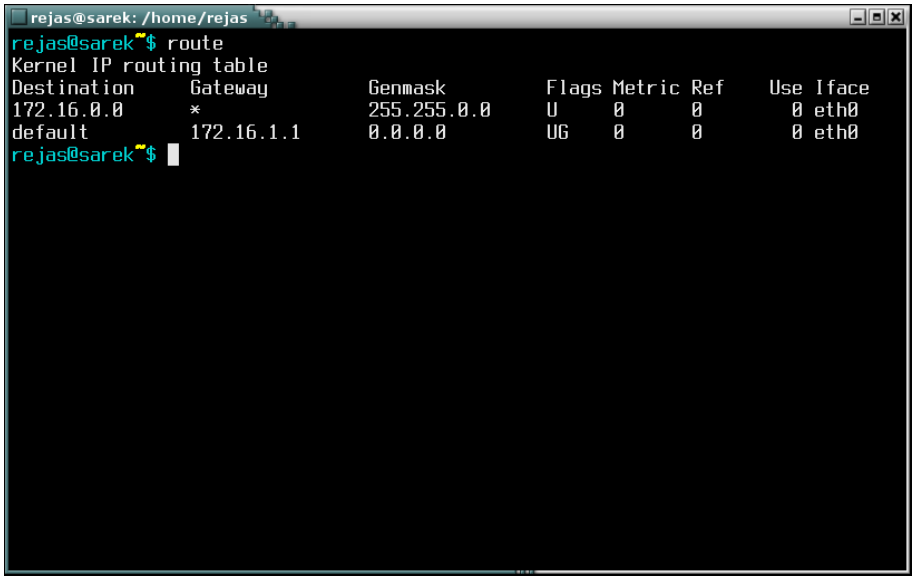
4. Se appendix F ifall du använder ett annat operativsystem än Linux

Figur 12-5. Skärmdump: ping på Linux



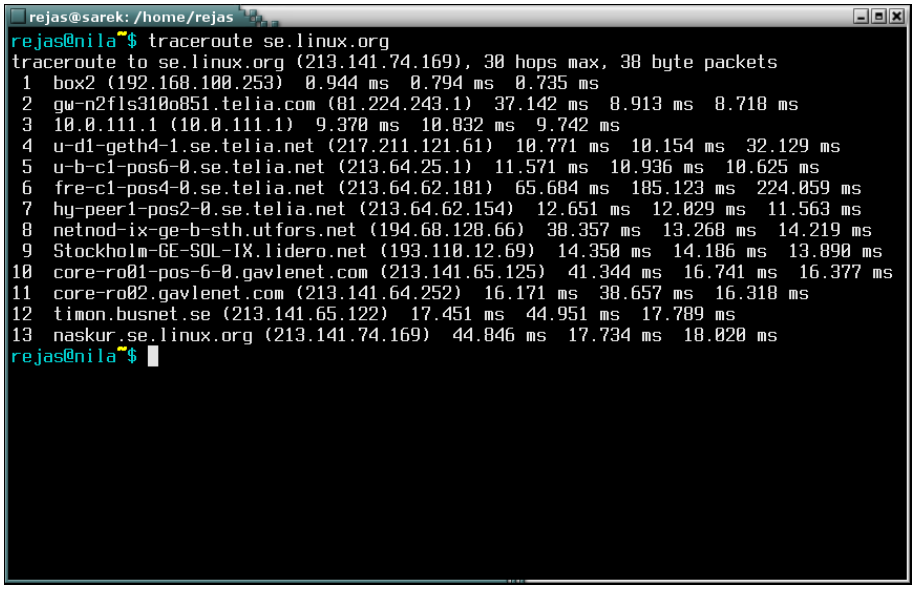
Route

Figur 12-6. Skärmdump: route på Linux



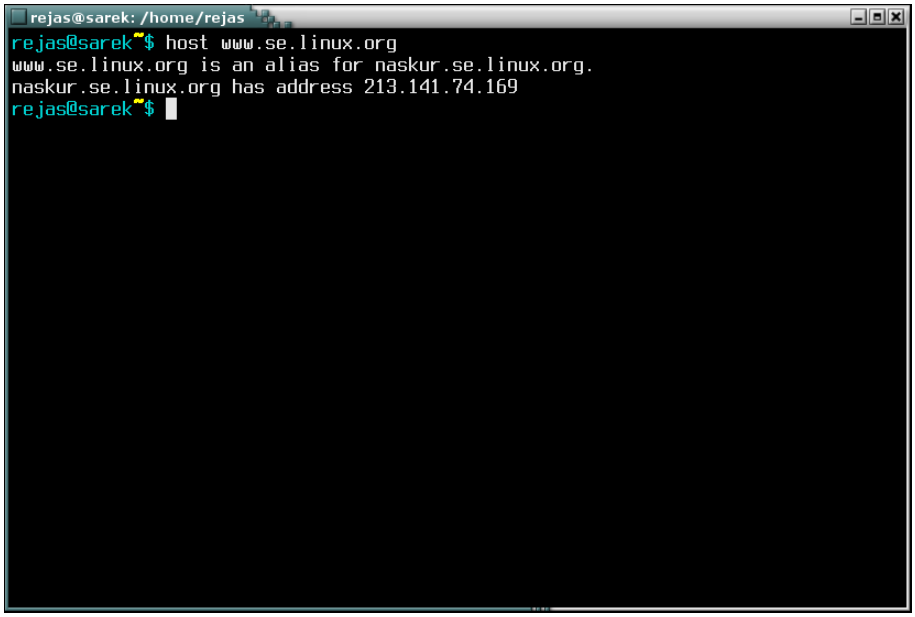
Traceroute

Figur 12-7. Skärmdump: traceroute på Linux



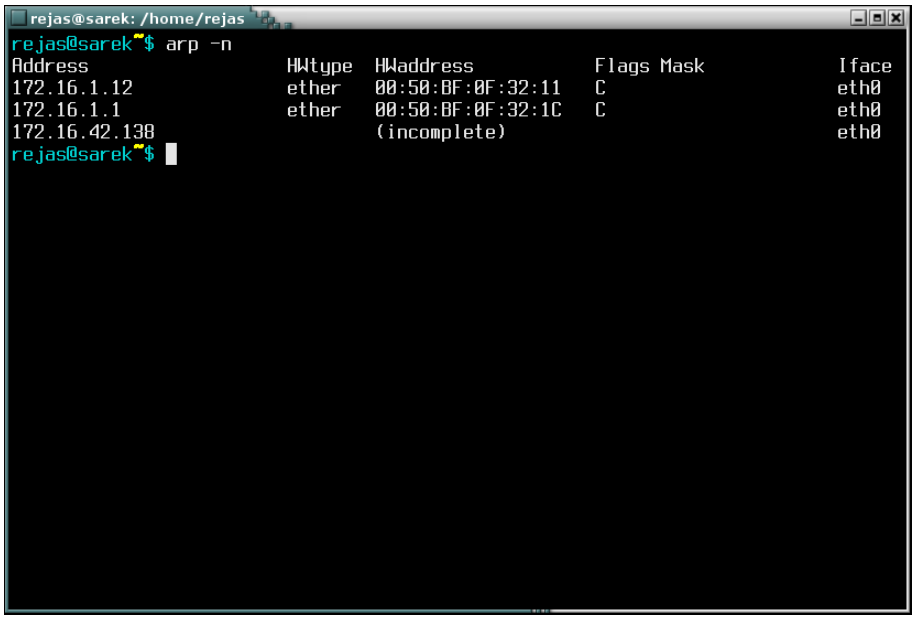
Host

Figur 12-8. Skärmdump: host på Linux



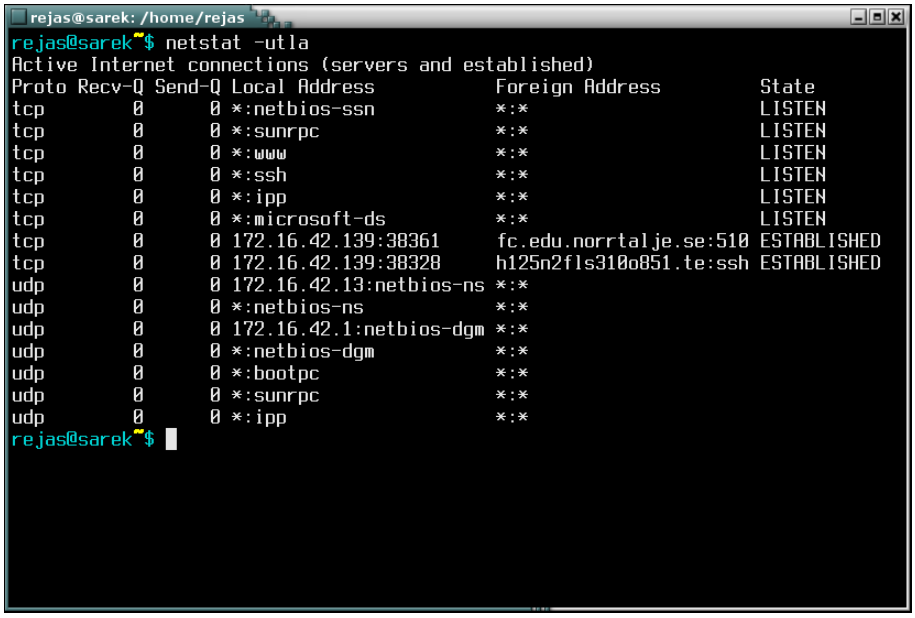
Arp

Figur 12-9. Skärmdump: arp på Linux



Netstat

Figur 12-10. Skärmdump: netstat på Linux



Domännamnssystemet (DNS)

Domännamnssystemet *Domain Name System, DNS* är ett av de viktigaste systemen på Internet. Utan detta system skulle visserligen det mesta av Internet fungera men inte många skulle kunna använda sig av det. Både fysiska användare och olika system på Internet skulle sluta fungera om DNS skulle sluta att fungera en dag.

Domännamnssystemets huvudsakliga uppgift är att översätta datornamn (hostname), till exempel www.se.linux.org till en IP-adress, 213.141.74.169. Den huvudsakliga anledningen till detta är att det skall vara lätt för människor att komma ihåg namnen på olika servrar. I exemplet så är ju datornamnet mycket lättare för en människa att lägga på minnet än vad IP-adressen är. Dessutom är det bra att använda ett alias, datornamnet, när man adresserar en dator eftersom man då kan flytta datorn, vilket oftast medför en ny IP-adress, utan att man behöver uppdatera alla som skall använda datorn, det räcker ju att uppdatera DNS-namnet.

När Internet inte var så stort behövde man inte använda något system som DNS. På samma sätt behöver man inte använda det om man har ett mindre lokalt nätverk. Men så snart man skall använda Internet eller skall hantera ett lite större nätverk så är det väldigt bra att använda ett DNS-system. Från början på Internet använde man så kallade hosts-filer på varje dator. I denna fil fanns det en lista med datornamn och motsvarande IP-adresser. Detta system kan man fortfarande använda om man vill men fungerar bara så länge som nätverket är litet. Det blir snabbt ohållbart att hålla alla dessa hosts-filer uppdaterade med varandra. Precis som man upptäckte så snart som Internet började växa.

Hierarkiskt system

DNS kan jämföras med en gigantisk distribuerad databas med datornamn och IP-adresser. DNS är ett hierarkiskt system. Det vill säga det finns en mängd olika nivåer där varje nivå har en master. Det kan jämföras med en hierarkisk företagsstruktur med en VD överst och under denne en rad chefer som under sig har kanske andra chefer som under sig har arbetare. Varje chef ansvarar för sina underhuggare och lyder närmast överliggande chef. Ungefär på samma sätt fungerar DNS.

Denna hierarkiska struktur används i DNS av precis samma skäl som det används i företag. Den högsta chefen kan inte personligen hålla reda på alla arbetare i företaget. Precis som en enda dator inte kan hålla reda på alla datorer på Internet och hantera frågor om dem.

DNS har inte en master eller topp-chef utan i dagsläget 13 stycken (http://www.root-servers.org/). Under dessa finns alla dns-servrar som hanterar *toppdomäner*.

Vi har tidigare sett att ett datornamn består av flera olika delar. Det längst till höger är det mest

signifikanta och är den så kallade toppdomänen. I det finns två olika typer av toppdomäner, dels de så kallade *generiska* som är de äldsta. De vanligaste generiska toppdomänerna är .com, .org, och .net. Dessa kom till när Internet var litet och i princip bara fanns i USA. Då var det mest logiskt att dela upp datornamnen efter vilken funktion de tillhörde. Sedan när Internet växte insåg man att man måste dela upp ytterligare, då blev det mest logiska att dela upp efter land. Så kom de nationella toppdomänerna till. Exempel på nationella domäner ät .se, .no, och .dk. Märk att de nationella domänerna är bundna till land medan de generiska kan användas överallt. USA, där användandet av generiska toppdomännamn är vanligast har det nationella toppdomännamnet .us. Märk också att även om nationella toppdomännamn är bundna till länder så finns det inget som hindrar att landet säljer dessa till utlandet. På så sätt har det till exempel blivit väldigt vanligt att svenskar använder det nationella toppdomännamnet .nu som tillhör landet Niue.

I Sverige har vi den nationella toppdomänen se. Den styrs av ett företag som heter Nic-SE. Nic-SE ägs till 100% av en stiftelse som heter *Stiftelsen för internetinfrastruktur (II-stiftelsen)*. Fram till april 2003 var det väldigt avancerat att få ett domännamn under se-domänen, till exempel så måste man då ha ett företag registrerat hos Patent och Registreringsverket (PRV). Bland annat detta ledde till att toppdomänen nu blev så populär bland svenskar. Nu är det betydligt enklare och vem som helst kan skaffa en se-domän.

I appendix H finns en komplett lista över de generiska och nationella toppdomänerna.

Domännamnsförfrågan

Som vi sa tidigare så ansvarar DNS för att översätta datornamn till IP-adress. Så vad händer när du skall hitta en dator. Säg att du vill kontakta datorn www.se.linux.org för att till exempel titta på de webbtjänster som den erbjuder. Du knappar in http://www.se.linux.org i din browser, vad händer sedan?

Det första som händer är att din dator frågar den DNS-server som du angett som standard, det är vanligtvis den server som är DNS på ditt lokala nätverk eller den som din internetleverantör tillhandahåller. Så din dator frågar alltså denna efter www.se.linux.org. Vi antar att denna DNS inte vet vad www.se.linux.org har för adress så denna DNS måste fråga någon annan. Eftersom det är en .org adress (generisk toppdomän) så frågar den den server som ansvarar för .org. Vet den inte vilken server vilken det är så måste den fråga någon av root-servrarna vilken server[5] som hanterar .org. Denna server känner inte heller till hela adressen men den kan fråga linux.org som den känner till. Alla känner ju till de som ligger direkt under dem. linux.org känner se.linux.org som i sin tur hittar www.se.linux.org. På så sätt så hittas adressen till den dator du sökte. Varje fråga som ställs sparas (cachas) i den maskin som ställde frågan så det skall gå snabbare nästa gång. Så nästa gång du frågar

5. Dessa stora domäner hanteras av flera servrar men man kan se de som en enda.

så vet redan din lokala DNS vilken adress det är du söker. Utan denna funktion skulle Internet snabbt svämma över av bara namnförfrågningar.

DNS-servrar

En DNS-server är en funktion i en dator. De större DNS-servrarna är datorer som bara är DNS-servrar och inget annat. Mindre DNS-servrar till exempel i lokala nätverk kan ha flera funktioner, man kan till exempel ha en dator som både DNS-server och webbserver. Det finns DNS-serverprogramvaror till i princip alla operativsystem. Den vanligaste finns till Unix-system, även Linux och heter *BIND, Berkeley Internet Name Daemon*.

Round Robin DNS

Om man har en server där prestanda blir lidande av för stor belastning kan man använda en teknik som heter Round Robin DNS. Den fungerar så att DNS-servern inte returnerar samma IP-adress varje gång den frågas efter ett datornamn. Det gör att man kan ha två eller flera servrar, gärna utspridda på olika håll som servar samma domännamn. Eftersom DNS-servrarna sprider ut svaren på domännamnsfårgorna så kommer lasten att balanseras över de olika servrarna.

Sammanfattning

Kapitel 13. E-post

Från Wikipedia, den fria encyklopedin.

E-post, förkortning för "elektronisk post". En av de ursprungliga typerna av meddelanden som vidarebefodras över Internet och som kännetecknas av högre tillförlitlighet än andra typer av elektroniska meddelanden. Tillkomsten av fenomen som spam (oönskad skräppost) och datavirus har gjort e-post mindre användbar på senare år, men den är fortfarande den dominerande standarden för att skicka meddelanden över Internet.

E-post

E-post är den tjänst som av många räknas som den viktigaste på Internet. Utan e-post står många företag stilla. I detta avsnitt skall vi behandla e-post och hur det fungerar lite närmare.

I svenskt tal och skrift bör man använda ordet e-post före till exempel e-mail eller bara mail. Framför allt bara mail eller försvenskat till mejl är olyckligt eftersom det redan har en annan betydelse på engelska, nämligen papperspost. Ytterligare information om detta finns hos Svenska Datatermgruppen[1].

E-post var den tjänst som många såg som den mest användbara när Internetliknande teknik presenterades i slutet på 60-talet. De första e-postsystemen fungerade så att man hade en fil som flera datorer kunde komma åt. I denna fil kunde man skriva meddelanden som andra kunde läsa. Detta system var dock inte så bra när man ville ha ett system där alla datorer skulle kunna skicka meddelanden till varandra oavsett var de fanns och oavsett vilket system de körde. Man utvecklade det vi i idag kallar e-post.

Från början när det inte fanns så många datorer skickade man breven till en viss användare på en viss dator. Efter ett tag, när e-posten utvecklades kom man på den notation som vi fortfarande använder i e-post adresser. Den med ett @ mellan användarnamnet och datornamnet. Från början så var det just ett användarnamn och ett datornamn som avsågs. Då hittade man som regel den man sökte på en viss dator i systemet. I dag är det oftast så att det som står före @ mostvarar ett namn och det som står efter @ är i regel ett domännamn som mostvarar ett företag eller en ISP.

E-postadresserna så som vi är vana att se dem idag kom till 1971. Den som hittade på det var Raymond Tomlinson (1941-). Han kom på det när han jobbade med att anpassa dåtidens e-post till

1. http://www.nada.kth.se/dataterm/

Arpanet.

Vad är då @? Detta tecken kallas för "at" på engelska. Det betyder ungefär "på" eller "vid". Adressen rejas@se.linux.org skulle då utläsas "rejas på se.linux.org" vilket stämmer bra. På svenska kallas @ för snabel-a men den har också en mängd olika smeknamn[2].

Flera protokoll

När du skickar ett e-brev till någon så kommer flera protokoll att ha används innan mottagaren har läst brevet. Förutom TCP/IP, DNS med mera används även minst ett par olika protokoll för själva brevskickandet.

Simple Mail Transport Protocol, SMTP

Det viktigaste protokollet som används är *Simple Mail Transport Protocol, SMTP*. Det är med SMTP som brevet transporteras över Internet från dig till mottagaren. Man kan säga att det är med SMTP som man skickar e-post.

Du startar ditt e-postprogram på din dator. Normalt så har du ingen SMTP-server på din dator utan när du skickar brevet så pratar ditt e-postprogram med en SMTP-server på ditt nät som antingen tillhandahålls av din ISP eller av IT-avdelningen på det företag du jobbar. Det protokoll som används mellan e-postprogram och servern är SMTP.

När brevet nått din SMTP-server måste det skickas vidare. Mottagaren har ju inte tillgång till din SMTP-server, och även om mottagaren hade det så kan han eller hon inte veta att post väntar på just din server. Istället så skickar din SMTP-server brevet vidare till den SMTP-server som hanterar posten för det domännamn som du angav i mottagarens e-postadress (det som står till höger om "@" i e-postadressen). Information om vilken server som ansvarar för e-posten för just den aktuella domänen får din server från DNS-systemet. När brevet kommit dit så finns det förhoppningvis på en server som mottagaren har tillgång till. I vissa fall så hoppar brevet flera steg till innan det nått den servern som just din mottagare kommer åt.

Nu återstår det bara för din mottagare att hämta och läsa brevet från dig. Det finns flera olika sätt att göra det. De vanligaste sätten är via protokoll som POP eller IMAP, men det blir vanligare och vanligare att man använder något som kalls för webbmail som är ett system för att, med hjälp av en webbläsare läsa sin post direkt från SMTP-servern.

2. Se svenska datatermgruppen på http://www.nada.kth.se/dataterm/rek.html#a17

Post Office Protocol, POP

Ett ganska gammalt, men fortfarande väldigt vanligt, sätt att hämta sin e-post är att använda ett protokoll som heter *Post Office Protocol, POP*. Med hjälp av POP hämtar du posten från din POP-server till lokala dator. De flesta e-postprogram klarar att hämta post med POP. Märk att SMTP har används hela tiden för att transportera brevet men sista biten används andra protokoll. I det här fallet POP. När brevet flyttats (kallas ibland för poppats) till din dator tas det oftast bort från POP-servern och lagras nu lokalt på din hårddisk.

IMAP

Se även brevet från Pär Lindskog i i appendix K angående IMAP.

IMAP är en forkortning för *Internet Message Access Protocol* är ett protokoll för att läsa e-posten med ett e-postprogram. Till skillnad från POP så är IMAP avsett för att läsa, sortera och söka bland breven på servern. (POP var ju avsett för att hämta breven från servern till den lokala datorn.) Fördelarna med IMAP är uppenbara, all e-post lagras centralt på en server. Användarna kan komma åt från vilken plats som helst. Till skillnad från POP så kan man med IMAP också skapa mappar på servern och sortera breven i dem. Nackdelen är kanske också uppenbar, att man läser breven från servern gör att man är beroende av denna och måste ha en fungerande anslutning till det nät där servern finns. Det finns program som löser detta genom att spara en synkroniserad kopia på den lokala datorn och synkronisera denna med servern när programmet har kontakt med den.

Webmail

En nackdel med POP och IMAP är att det krävs inställningar på den dator man skall läsa sin post ifrån. Många vill idag kunna läsa sin post på vilken dator som helst eftersom de ofta reser eller använder flera olika datorer.

Det enklaste sättet att göra detta på är att använda sig av en webbmail. Det är ett system då man istället för att hämta sin post från leverantörens eller företagets SMTP-server med POP eller IMAP, läser den direkt från servern med hjälp av en webbmailprogramvara. Vad denna programvara gör är att möjliggöra att man läser sin post via HTTP och ett vanlig webbläsare. Eftersom nästan alla datorer idag har en webbläsare och är anslutna till Internet kan man läsa sin post nästan varifrån som helst.

Att kunna läsa sin post varifrån som helst och att slippa spara sina brev på den egna datorn är stora fördelar som gör att många använder webbmail. Det finns flera företag som använder gratis

webbmailtjänster som gör att du kan skaffa dig en e-postadress alldeles gratis utan att ens ha en internetansluten dator. Men det finns också nackdelar med webbmail.

Webbmail har flera nackdelar. Att hantera sin post med en webbläsare är oftast krångligare och långsammare än att göra det med ett vanligt e-postprogram. En annan nackdel är att du måste vara uppkopplad hela tiden du skall läsa din post. Om du hämtar posten med POP eller IMAP behöver du ju bara vara ansluten till Internet just när du hämtar posten, sedan kan du ju läsa den i lugn och ro även om du inte är uppkopplad. En annan nackdel är att de flesta företag som erbjuder webbmail har en gräns för hur mycket post du får spara på deras server. Det gör att du men jämna mellanrum måste slänga dina brev för att få plats med nya. Detta gäller i första han gratistjänster men det är inte ovanligt att även sådana man betalar för eller de inom företag har liknande gränser (om än oftast lite högre).

E-post och säkerhet

I nästa kapitel kommer vi att tala om säkerhet men det är ändå på sin plats att tala lite om det redan nu när vi hanterar e-post. E-post är nämligen en tjänst på Internet som skall betraktas som osäker. En tumregel som är bra är att man inte skall skriva någonting i ett e-brev som man inte skulle skriva på ett vykort. Vill man skicka någonting som är lite hemligt skall man använda sig av något verktyg för att kryptera sitt brev så att obehöriga inte kan läsa det.

Kapitel 14. Datasäkerhet och lagstiftning

Stora öppna nät som till exempel Internet är naturligtvis bra för kommunikationen men det öppnar även för onda personer som kan missbruka denna öppenhet. I detta kapitel behandlar vi datasäkerhet. Hur farligt är Internet och vilka metoder finns för att skydda sig?

Man kan säga att säkerhet är de metoder och verktyg som vi kan ta till för att uppnå trygghet.

Syftet med datasäkerhet

Syftet med all säkerhet är att man skall skapa trygghet. Alla som berörs av systemet skall känna sig trygga med att den information som ligger i systemet bara kan komma i rätta händer. En stor bov i detta spel är faktiskt också trygghet. En människa som känner sig väldigt trygg slutar ofta att tänka på säkerheten. Det värsta är det vi kallar falsk trygghet.

Det finns flera exempel när tryggheten som man vill uppnå motarbetar säkerheten i sig. Till exempel så kan ett brandlarm göra att man struntar i att kontrollera att alla ljus är släckta innan man går och lägger sig. Risken att huset skall brinna ner är då betydligt större än utan brandvaranare. Man har installerat ett skyddssystem men inte skyddat sig mot själva faran.

Falsk trygghet kan vara om till exempel brandvarnaren i exemplet ovan inte fungerar. Du sjunker säkerheten i huset avsevärt, men de som bor där känner sig tryggare än någonsin.

För att skapa trygghet inom databehandling måste följande tre krav vara uppfyllda.

- Sekretess
- Integritet
- Tillgänglighet

Sekretess

Med sekretess menas att bara rätt personer skall kunna komma åt en viss information. Informationen behöver inte vara hemlig eller sekretessbelagd utan även annan information kräver viss sekretess. Till exempel dina dokument på din dator, de är inte sekretessbelagda, men en viss sekretess vill du

ändå ha på dem så att inte vem som helst kan läsa dem. Inom vården, polismyndigheten och även företag ställs det väldigt höga krav på sekretessen.

Integritet

Integritet i det är fallet handlar inte om människors integritet utan om datas integritet. Med detta menas att de data som finns i ett system skall vara riktiga och inte förändrade av någon obehörig. Till exempel så måste polisen och läkaren vara säker på att det som står i register och journaler är riktigt och inte förändrat av någon. Detsamma gäller naturligtvis även företagarens rapporter. Så god sekretess förhindrar insyn och god integritet förhindrar förändring. Se även spårbarhet nedan.

Tillgänglighet

Med tillgänglighet menas att data skall finnas tillhanda för rätt personer i rätt tid och på rätt plats. Ett system är värdelöst om det är så säkert att inte ens de legitima användarna kan nyttja det.

Spårbarhet

Spårbarhet tar många upp som en egen punkt ovan. Jag gör det inte eftersom jag tycker att den hänger ihop med den andra punkten (Integritet) och att det inte är ett säkerhetsmål i sig. Data blir inte säkrare av spårbarhet, men det är lättare att i efterhand verifiera data med hjälp av spårbarhet. Med spårbarhet menas att man i efterhand skall kunna reda ut vad som hänt med vissa data och vad som hänt i ett system. Man skall kunna se vem som gjort vad och när det hände. Detta gör man oftast med hjälp av olika loggar.

Hur farligt är Internet?

Internet och andra stora nätverk är i sig är inte farliga. Det är de som använder näten som potentiellt kan vara farliga. Det är viktigt att tänka på vilka uppgifter man lämnar ifrån sig och hur man skyddar sådant som man vill hålla för sig själv.

Människan är ofta rädd för det som är okänt. Det gör att man kanske är mer rädd för att använda sitt kontokort på Internet än vad man är för att använde det i en butik. I själva verket är det lika farligt att använda det i en butik om den som står bakom disken i butiken har onda avsikter.

Hur kan jag skydda mig?

Det finns massor av sätt att skydda dig. Vanligt sunt förnuft räcker väldigt långt. Här kommer ytterligare några tips.

Var försiktig med e-post och bilagor

Med e-post finns möjligheten att skicka brev med bilagor. Bilagorna kan vara till exempel en bild som illustrerar innehållet i brevet. Det går också att bifoga filer som kan vara program. Om du kör dessa program ger du programmet (och då naturligtvis den som skrev det) samma rättigheter som du själv har på din dator. Om du inte vet var programmet kommer från skall du inte köra det. Öppna aldrig filer från personer du inte känner. Även om du känner personen i fråga så kan det vara fråga om ett virus. Kontrollera gärna en extra gång med den personen som skickat brevet innan du öppnar några bifogade filer.

Ladda hem saker från Internet med försiktighet

Precis som med filerna i e-posten så måste man passa sig för filer man får ner till sin dator på andra sätt. Det är på samma sätt här, kör du filen så ger du den som gett dig filen samma rättigheter på din dator som du själv har. Extra farligt är så kallade filbytartjänster eller -nätverk, där du inte alls vet vem som lagt upp de filer du tankar hem.

Använd bra lösenord

Den första kontakten de flesta har med datasäkerhet är användarnamn och lösenord. Användarnamnet använder du för att det aktuella systemet skall veta vad då får och inte får göra och se. Det kallas får identifiering. Lösenordet används för att du skall kunna bevisa att du verkligen är du. Detta kallas autenticering. Ibland behövs ingen autenticering och ibland behövs det autenticering som är starkare än bara ett användarnamn och ett lösenord. Ett lösenord är något som man *vet* ibland kan det också krävas att man *har* något, till exempel ett kort eller en nyckel.

Ett system som använder lösenord är relativt säkert. Det största problemet med ett sådant system är användarna och de lösenord de väljer eller hur de handskas med lösenorden. Ett lösenord som är lätt att gissa eller som står uppskrivet på skärmen eller under skrivbordsunderlägget gör ingen större nytta. En grundläggande regel som man kan jobba efter är att: *Lösenord skall man hantera som underkläder. Man lånar inte ut dem, låter dem inte ligga framme, och byter dem då och då.*

Hur hittar man då ett lösenord som man skall kunna komma ihåg (det är aldrig bra att ha lösenord nedskrivna) men som inte är lätt att gissa? En grundregel är att inte ta något som är kopplat till ens person. Till exempel är namnet på barn, barnbarn, hundar och katter extremt vanliga lösenord. Helst skall man undvika alla ord och helst också blanda små bokstäver, stora bokstäver och siffror. Ett bra lösenord är till exempel *Jsk2KgP* men hur skall man komma ihåg ett sådant lösenord? Jo, det är enkelt. Lösenordet är taget från frasen *Jag skall köpa 2 Kg Potatis* som är lätt att komma ihåg. Ofta är det lätt att komma ihåg fraser. Man kan också utgå från ord och byta ut vissa tecken mot bokstäver, till exempel så kan *potatis* bli *p0t4t1s* som är ett bra lösenord.

Anledningen till att man skall ha bra lösenord är att det finns vissa program som är till föra att knäcka lösenord genom att testa alla möjliga tänkbara lösenord. Dessa program utgår från listor med vanliga lösenord och tar sedan ord från ordböcker och liknande. De kan utan problem testa alla svenska ord. Har du då ett svenskt ord som lösenord så skyddar det dig inte alls.

Uppdatera ditt system

Datorsystem måste uppdateras för att vara säkra. Inget system är säkert över tiden. Även om systemet var säkert när du installerade det så hittas hela tiden nya säkerhetsproblem. De flesta operativsystem har en funktion för att uppdaterara sig automatiskt. Använd denna så håller sig ditt system så säkert som möjligt. Detsamma gäller naturligtvis antivirusprogram, brandväggar och andra program.

Välj inte de "dansande grisarna"

En säkerhetsexpert som heter Bruce Schneier har konstaterat att användarna alltid kommer att välja dansande grisar före säkerhet. Med detta menar han att hur mycket man än utbildar dem som använder systemen så kommer de så fort de ser något lockande att göra tvärt emot. Så gör inte saker du vet är fel!

Brandväggar

Allmänt

Brandväggar är en central del i ett säkert datornätverk. Man skall dock passa sig för att ge dem en allt för central roll. Det finns risk att man när man har installerat en brandvägg känner sig trygg och slarvar med säkerheten på det interna nätverket. Det kan leda till att många nätverk till och med blir osäkrare efter att man har installerat en brandvägg. Men rätt använd är en brandvägg oumbärlig när det gäller att skydda sin dator eller sitt nätverk från oönskad trafik.

Namnet brandvägg kommer naturligtvis från det som vi kallar brandväggar i eller mellan två byggnader. En brandvägg är en, oftast murad eller gjuten, vägg och den får inte ha några hål. Dess syfte är att hindra att en brand sprids mellan husen eller delar av ett hus.

Brandväggar kan arbeta på olika lager i OSI-modellen. De vanligaste jobbar i nätverksskiktet och kallas för paketfiltrerande brandväggar. En annan typ kallas proxy-servrar och de jobbar i applikationslagret. De som jobbar på nätverkslagret kan naturligtvis bara titta på ip-adresser och portar medan de som jobbar högre upp i OSI-modellen även kan titta på den trafik som är i paketen. Inte sällan kombinerar man båda typerna i en och samma brandvägg.

Paketfiltrerande

En paketfiltrerande brandvägg tittar bara på ip-adresser och portar. Den arbetar på nätverkslagret och kan därför inte säga något om innehållet i trafiken. Det finns två typer av paketfiltrerande brandväggar, de som är *stateful* och de som är *stateless*. De som är stateful kommer ihåg de paket den har behandlat och kan sätta in paketen i ett sammanhang medan de som är stateless ser varje paket som en egen händelse.

Paketfiltrerande brandväggar kombineras oftast med en router. De har två eller fler gränssnitt mellan vilka trafiken dirigeras med en routingtabell. Utöver detta finns det även brandväggsregler som säger vilken trafik som får passera branvädggen. Ett enkelt sådant regelverk kan vara:

```
Tillåt trafik från insidan till webbservrar (port tcp/80) på utsidan
Tillåt trafik från insidan till dnsservrar  (port udp/53) på utsidan
Tillåt trafik till 84.243.2.149 port tcp/6667 (selinux, irc)
Tillåt ingen annan trafik från insidan till utsidan
```

En paketfiltrerande brandvägg har sina begränsningar men är väldigt effektiv och används idag på i proncip alla nätverk och nästan alla datorer som används på Internet.

Proxies

En proxyserver är också en typ av brandvägg men den jobbar ända uppe på applikationsnivån i OSI-modellen. Det gör att den har andra möjligheter än en paketfiltrerande brandvägg. En proxyserver kan till exempel titta på url:er och till och med på innehåll i http-trafik (surfning).

Man kan alltså kontrollera vilka webbplatser som kan besökas och man kan till och med kontrollera vilka filnamn som kan hämtas. Man kan filtrera på innehåll och till exempel sortera bort sidor som innehåller vissa ord.

Inte sällan kombineras en patetfiltrerande branvägg med en proxy. En nackdel med proxyservern är att den är något långsammare eftersom den måste ända upp i applikationslagret och dessutom har ett mer avancerat regelverk.

Personlig brandvägg

Det är ganska vanligt att man utrustar även klientdatorerna, alltså de som användarna sitter vid, med lokala brandväggar och till och med proxys. Detta för att de skall vara skyddade mot varandra och när de flyttas runt mellan olika nät. Det är en bra säkerhetsprincip att varje nod skall i sig vara säker. Man skall aldrig lita på att något runt om kring är säkert.

Man skall heller aldrig lite för mycket på en brandvägg. Tänk på hur fungerar och att de i princip inte alls fungerar mot virus och trojaner och annat som kan lista sig in i din dator utan att du vet om det, men enligt brandväggens regler.

Kryptering

En sak som är grundläggande när det gäller att hålla saker hemliga är kryptering. Kryptering har man använt i princip lika länge som människor har kommunicerat. Man vet att vi använt kryptering sedan minst 4000år. Man kallar även att kryptera för att chiffrera som betyder att dölja något. Den okrypterade texten brukar kallas för klartext och den krypterade brukar kallas chiffer. För att kryptera och dekryptera använder man någon algoritm och i vissa fall en eller flera nycklar. Information som är krypterad med en bra krypteringsalgoritm kan man klassa som helt skyddad.

En väldigt gammal krypteringsalgoritm som de flesta använt som barn är det så kallade *Caesars Chiffer*. Det går ut på att man helt enkelt byter ut bokstäverna i alfabetet mot en annan bokstav x positioner längre fram i alfabetet. Till exempel så kan E bli H och R bli U om man hoppar 3 steg. I det fallet är krypteringsalgoritmen Caesars Chiffer och nyckeln är 3.

```
||| <- Nyckel = 3
   ABCDEFGHIJKLMNOPQRSTUVWXYZÅÄÖ
       |  |  |      |||       |
ABCDEFGHIJKLMNOPQRSTUVWXYZÅÄÖABC
```

Krypterar man ordet *säkerhet* med denna krypteringsalgoritm så blir det *vbnhukhw*. Denna krypteringsalgoritm är naturligtvis väldigt lätt att knäcka men man kan säga att det är grundprincipen för hur kryptering fungerar.

En nackdel med Caesars Chiffer är att bokstaven S alltid blir V om man krypterar enligt ovan. Det gör att chiffret blir väldigt lätt att knäcka. Om man istället använder till exempel 5 olika nycklar om varandra så blir det mycket svårare att knäcka. Är det optimalt så bör bokstaven S bli olika bokstäver varje gång den krypteras.

Symmetrisk och asymmetrisk kryptering

Det går att dela in vanliga krytperingsalgoritmer i två famljer, *symmetrisk* och *asymmetrisk*. Symmetrisk kryptering använder en nyckel och asymmetrisk två.

Caesars Chiffer som vi såg ovan använder sig av en nyckel (3 i exemplet). Det är ett så kallat symmetriskt chiffer. Man använder samma nyckel för att kryptera som man använder för att dekryptera meddelandet.

Programvara som implementerar symmetriska krypteringsalgoritmer kan göras väldigt snabba. Det är relativt lätt att kryptera med symmetrisk kryptering. Men det finns ett stort problem, nämligen hur man skall dela nyckeln mellan sändare och mottagare. Vill jag kunna ta emot krypterade meddelanden från människor så måste jag ju först träffa dem för att vi skall kunna komma överens om en nyckel vi skall använda. Nyckeln måste vi ju båda känna till och den är lika hemlig som meddelandet. Nyckeln kan man ju också bara använda för att skicka meddelanden mellan två personer. Skall man skicka ett annat meddelande till en annan person så måste man skapa en nyckel till och byta den på något sätt. Till slut inser man att om man måste byta en nyckel varje gång man skall skicka ett meddelande så kan man lika gärna lämna meddelandet på en gång.

En lösning på detta är något som kallas asymmetrisk kryptering. Det går till så att man använder ett par av nycklar. En för att kryptera och en för att dekryptera. Med hjälp av denna förändring kan man lösa många av problemen som vi visat på ovan.

Paret av nycklar använder man på så vis att man håller den ena för sig själv och sprider den andra så att den är väl tillgänglig för alla som vill ha den. Man kallar den man skyddar för privat nyckel och den som alla kan nå för publik nyckel. Eftersom den ena nyckeln krypterar och den andra dekrypterar så kan en person som vill skicka ett meddelande till mig använda min publika nyckel för att kryptera meddelandet. När det är krypterat kan det bara öppnas med min privata nyckel, alltså bara av mig.

Signering

Ofta behöver man inte kryptera meddelandet utan det räcker med att signera det. En signatur är något som man applicerar på sitt meddelande så att mottagaren vet att det är du som skickat det.

Signering går att lösa med flera asymmetriska krypteringsalgoritmer. Eftersom nycklarna jobbar i par där en kan kryptera och den andra kan dekryptera[1] så kan man välja att kryptera meddelandet med sin hemliga nyckel. När man gjort det så kan vem som helst dekryptera det med motsvarande publika nyckel. Eftersom vem som helst kan dekryptera meddelandet så är det inte skyddat för insyn. Men man kan vara säker på att det kommer från den person det utges komma ifrån för man vet vems publika nyckel man använder och då måste det ju vara krypterat med motsvarande, hemliga nyckel. Inte heller den här gången behöver man avslöja sin hemliga nyckel.

Relevanta lagar

Personuppgiftslagen (PUL)

Från Wikipedia, den fria encyklopedin.

PUL, eller Personuppgiftslag (1998:204) som den egentligen heter, är den svenska implementationen av ett EU-direktiv. Syftet med lagen är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Lagen gäller för personuppgiftsansvariga som är etablerade i Sverige. Lagen tillämpas också när den personuppgiftsansvarige är etablerad i tredje land men för behandlingen av personuppgifter använder sig av utrustning som finns i Sverige. Straffet är böter eller fängelse i högst sex månader eller, om brottet är grovt, till fängelse i högst två år.

Sammanfattning

Datasäkerhet är viktigt. Tänk dig för när du läser e-post och surfar på Internet. Man kan med hjälp av kryptering skicka meddelanden eller annan data säkert över internet. Antingen använder man symmetrisk kryptering där båda parterna har en egen nyckel, eller så använder man en asymmetrisk då man har olika nycklar och aldrig behöver avslöja den ena.

Håll dina system uppdaterade och var försiktig med filer du laddar hem från Internet så kommer du att klara dig mycket bättre från problem. Och du! Välj aldrig de dansande grisarna före säkerheten.

1. Det är inte alla asymmetriska krypteringsalgoritmer som har denna egenskap men de vanligaste man använder i samband med till exempel e-post har det.

Appendix A. Övningsuppgifter

I detta appendix finns övningsuppgifter till alla kapitel i boken. Har du förslag på fler uppgifter, gärna både lätta och fördjupningsuppgifter så uppskattar jag om du skickar dem till datorkommunikation@rejas.se.

Datorkommunikation: Inledning

1. Förklara skillnaden mellan data och dator.
2. Förklara skillnaden mellan data och information.
3. Diskussionsuppgift: Kan man spara information?

Datorkommunikation: Dataöverföring

1. Vad är skillnaden mellan digitala och analoga signaler?
2. Vad är skillnaden mellan en bit och en byte?
3. Hur många bitar går det på en byte?
4. Hur många värden kan en byte respektive en bit anta?
5. Vad blir talet 36 hexadecimalt?
6. Vilket tal motsvarar bokstaven A enligt ASCII-tabellen i tabell C-1?

Datorkommunikation: Seriell och parallell kommunikation

1. Vad är skillnaden mellan parallell och seriell kommunikation?
2. Vilka är fördelarna med asynkron överföring?
3. Hur lång tid tar det att föra över en fil på 1MByte över en seriell förbindelse med kapaciteten 28800 bit/s om man använder asynkron överföring med en stopp-bit och ingen paritet?

Datorkommunikation: Datornätverk

1. Förklara begreppen LAN, WAN och MAN. Berätta vad de betyder och vilka som är vanligast.
2. Vad är en topologi?
3. Varför behövs terminatorer i ett bussnät?
4. Vad är en accessmetod (åtkomstmetod)?
5. Förklara accessmetoderna CSMA/CA och CSMA/CD.

Datorkommunikation: Nätverkskomponenter

1. Förklara begreppen dator och server. Vad har de för relation till varandra?
2. Vad är skillnaden mellan en hubb och en switch?
3. Vad är, och hur jobbar en router?
4. Vad är en brandvägg (i datorkommunikationssammanhang)?

Datorkommunikation: kablar och icke-kablar

1. Av vilken anledning finns det två olika material till kabelhöljen (pvc och plenum) att välja på?
2. Vilken typ av kabel är det vi normalt kallar för skrivarkabel?
3. Vad är skillnaden mellan UTP och STP?
4. Vilka är för- och nackdelarna med trådlösa nätverk?

Datorkommunikation: Modem

1. Vilken moduleringssform är vanligast idag?
2. Vad gör två modem under den så kallade handskakningen (handshake)?

Datorkommunikation: Publika telenätet

1. Vad är datapak?

Datorkommunikation: Protokoll

Övningar kommer snart ...

Datorkommunikation: Internet

Övningar kommer snart ...

Datorkommunikation: Mer om Internets teknik

Övningar kommer snart ...

Datorkommunikation: Datasäkerhet

Övningar kommer snart ...

Appendix B. DTR1201 - Datorkommunikation

100 poäng, inrättad 2000-07 SKOLFS: 2000:28

Mål

Mål för kursen

Kursen skall ge grundläggande kunskaper om datorkommunikation och utveckla färdigheter inom området. Kursen skall också ge kunskaper om principer, begrepp, standarder och utveckling inom området.

Mål som eleverna skall ha uppnått efter avslutad kurs

Eleven skall

kunna upprätta, underhålla och felsöka seriell och parallell kommunikation mellan persondatorer och deras kringutrustning

kunna upprätta och konfigurera förbindelser med olika typer av modem

kunna ansluta, konfigurera och använda digitala tjänster

känna till det publika telenätets anslutningsmöjligheter, prestanda, begränsningar och tjänster samt egenskaper för de vanligaste modemstandarderna

ha kunskap om principer och prestanda för olika typer av överförings- transport- och transmissionsprotokoll

känna till begreppen ledningsegenskaper och kapacitet samt deras praktiska innebörd vid datakommunikation med olika överföringsmedier

känna till funktion och prestanda hos olika digitala förbindelser

ha kunskap om gällande datalagstiftning och förstå datasäkerhetens betydelse

ha kunskap om referensmodeller som beskriver struktur och funktion för datorkommunikation

ha kunskap om de vanligaste protokollen och programmen på internet samt hur de används

kunna använda programvaror för enklare diagnostisering, spårning och felsökning på internet

ha kunskap om internets historik, uppbyggnad och kommunikationsteknik

ha kunskap om olika sätt att skydda information vid dataöverföringar.

Betygskriterier

Kriterier för betyget Godkänd

Eleven upprättar kommunikation mellan datorer med olika operativsystem i lokala nät och telenät.

Eleven utför med viss handledning felsökning i förbindelser mellan persondatorer och kringutrustning.

Eleven söker upp den information som behövs för arbetsuppgifterna.

Eleven beskriver grundläggande begrepp, funktioner och standarder för datorkommunikation.

Eleven redovisar ledningsegenskapers betydelse vid datorkommunikation.

Eleven ger exempel på hur kravet på datasäkerhet och datalagstiftning påverkar arbetet.

Kriterier för betyget Väl godkänd

Eleven utför på egen hand och inom rimlig tid de arbetsuppgifter som ingår i datorkommunikation.

Eleven hämtar på egen hand information från olika källor och tillämpar denna i olika arbetsuppgifter och situationer.

Eleven tillämpar kunskaperna om datasäkerhet och datalagstiftning i arbetet.

Kriterier för betyget Mycket väl godkänd

Eleven utför sina arbetsuppgifter på ett närmast yrkesmässigt sätt.

Eleven löser självständigt problem med metoder som tar hänsyn till datasäkerhet och ekonomi.

Eleven beskriver samband och ser helheten i komplexa datakommunikationsmodeller.

Skolverket 2002-04-09

Appendix C. Exempel på ASCII-tabell

Tabell C-1. ASCII-tabell

Specialtecken			Standardtecken						Utökade tecken (8-bitar)							
Dec	Ctrl	Tkn	Dec	Tkn	Dec	Tkn	Dec	Tkn	Dec	Tkn	Dec	Tkn	Dec	Tkn	Dec	Tkn
0	ctrl-@	NUL	32	Spc	64	@	96	‘	128	€	160		192	À	224	à
1	ctrl-A	SOH	33	!	65	A	97	a	129		161	¡	193	Á	225	á
2	ctrl-B	STX	34	"	66	B	98	b	130		162	¢	194	Â	226	â
3	ctrl-C	ETX	35	#	67	C	99	c	131		163	£	195	Ã	227	ã
4	ctrl-D	EOT	36	$	68	D	100	d	132		164		196	Ä	228	ä
5	ctrl-E	ENQ	37	%	69	E	101	e	133		165	¥	197	Å	229	å
6	ctrl-F	ACK	38	&	70	F	102	f	134		166	¦	198	Æ	230	æ
7	ctrl-G	BEL	39	’	71	G	103	g	135		167	§	199	Ç	231	ç
8	ctrl-H	BS	40	(	72	H	104	h	136		168	¨	200	È	232	è
9	ctrl-I	HT	41	)	73	I	105	i	137		169	©	201	É	233	é
10	ctrl-J	LF	42	*	74	J	106	j	138		170	ª	202	Ê	234	ê
11	ctrl-K	VT	43	+	75	K	107	k	139		171	«	203	Ë	235	ë
12	ctrl-L	FF	44	,	76	L	108	l	140		172	¬	204	Ì	236	ì
13	ctrl-M	CR	45	-	77	M	109	m	141		173		205	Í	237	í
14	ctrl-N	SO	46	.	78	N	110	n	142		174	®	206	Î	238	î
15	ctrl-O	SI	47	/	79	O	111	o	143		175	¯	207	Ï	239	ï
16	ctrl-P	DLE	48	0	80	P	112	p	144		176	°	208	Đ	240	ð

Specialtecken			Standardtecken						Utökade tecken (8-bitar)							
Dec	**Ctrl**	**Tkn**	**Dec**	**Tkn**	**Dec**	**Tkn**	**Dec**	**Tkn**	**Dec**	**Tkn**	**Dec**	**Tkn**	**Dec**	**Tkn**	**Dec**	**Tkn**
17	ctrl-Q	DC1	49	1	81	Q	113	q	145		177	±	209	Ñ	241	ñ
18	ctrl-R	DC2	50	2	82	R	114	r	146		178	²	210	Ò	242	ò
19	ctrl-S	DC3	51	3	83	S	115	s	147		179	³	211	Ó	243	ó
20	ctrl-T	DC4	52	4	84	T	116	t	148		180	´	212	Ô	244	ô
21	ctrl-U	NAK	53	5	85	U	117	u	149		181	µ	213	Ö	245	õ
22	ctrl-V	SYN	54	6	86	V	118	v	150		182	·	214	Ö	246	ö
23	ctrl-W	ETB	55	7	87	W	119	w	151		183	·	215	×	247	÷
24	ctrl-X	CAN	56	8	88	X	120	x	152		184	¸	216	Ø	248	ø
25	ctrl-Y	EM	57	9	89	Y	121	y	153		185	¹	217	Ù	249	ù
26	ctrl-Z	SUB	58	:	90	Z	122	z	154		186	º	218	Ú	250	ú
27	ctrl-[	ESC	59	;	91	[	123	{	155		187	»	219	Û	251	û
28	ctrl-\	FS	60	<	92	\	124	|	156		188	¼	220	Ü	252	ü
29	ctrl-]	GS	61	=	93	]	125	}	157		189	½	221	Ý	253	ý
30	ctrl-^	RS	62	>	94	^	126	~	158		190	¾	222	Þ	254	þ
31	ctrl-_	US	63	?	95	_	127	DEL	159		191	¿	223	ß	255	

Appendix D. Tabell för att översätta mellan Hexadecimala och Decimala tal

Tabell D-1. Hexadecimal -> Decimal

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	000	001	002	003	004	005	006	007	008	009	010	011	012	013	014	015
1	016	017	018	019	020	021	022	023	024	025	026	027	028	029	030	031
2	032	033	034	035	036	037	038	039	040	041	042	043	044	045	046	047
3	048	049	050	051	052	053	054	055	056	057	058	059	060	061	062	063
4	064	065	066	067	068	069	070	071	072	073	074	075	076	077	078	079
5	080	081	082	083	084	085	086	087	088	089	090	091	092	093	094	095
6	096	097	098	099	100	101	102	103	104	105	106	107	108	109	110	111
7	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
8	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
9	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
A	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
B	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
C	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
D	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
E	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
F	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

Appendix E. Tabell för att översätta mellan Decimala och binära tal

Detta är en tabell för att översätta de första 256 talen i vårt vanliga talsystem med basen tio till det binära med basen två. I boken behandlas hur man, istället för att hämta ur en tabell, räknar fram dessa värden. Det är bättre att lära sig räkna fram dem. Använd denna tabell på det sätt du tycker passar.

Tabell E-1. Decimal -> Binära

Dec	Bin	Dec	Bin	Dec	Bin	Dec	Bin
0	00000000	64	01000000	128	10000000	192	11000000
1	00000001	65	01000001	129	10000001	193	11000001
2	00000010	66	01000010	130	10000010	194	11000010
3	00000011	67	01000011	131	10000011	195	11000011
4	00000100	68	01000100	132	10000100	196	11000100
5	00000101	69	01000101	133	10000101	197	11000101
6	00000110	70	01000110	134	10000110	198	11000110
7	00000111	71	01000111	135	10000111	199	11000111
8	00001000	72	01001000	136	10001000	200	11001000
9	00001001	73	01001001	137	10001001	201	11001001
10	00001010	74	01001010	138	10001010	202	11001010
11	00001011	75	01001011	139	10001011	203	11001011
12	00001100	76	01001100	140	10001100	204	11001100
13	00001101	77	01001101	141	10001101	205	11001101
14	00001110	78	01001110	142	10001110	206	11001110
15	00001111	79	01001111	143	10001111	207	11001111
16	00010000	80	01010000	144	10010000	208	11010000
17	00010001	81	01010001	145	10010001	209	11010001
18	00010010	82	01010010	146	10010010	210	11010010
19	00010011	83	01010011	147	10010011	211	11010011
20	00010100	84	01010100	148	10010100	212	11010100
21	00010101	85	01010101	149	10010101	213	11010101
22	00010110	86	01010110	150	10010110	214	11010110
23	00010111	87	01010111	151	10010111	215	11010111
24	00011000	88	01011000	152	10011000	216	11011000
25	00011001	89	01011001	153	10011001	217	11011001
26	00011010	90	01011010	154	10011010	218	11011010
27	00011011	91	01011011	155	10011011	219	11011011
28	00011100	92	01011100	156	10011100	220	11011100
29	00011101	93	01011101	157	10011101	221	11011101
30	00011110	94	01011110	158	10011110	222	11011110

Dec	Bin	Dec	Bin	Dec	Bin	Dec	Bin
31	00011111	95	01011111	159	10011111	223	11011111
32	00100000	96	01100000	160	10100000	224	11100000
33	00100001	97	01100001	161	10100001	225	11100001
34	00100010	98	01100010	162	10100010	226	11100010
35	00100011	99	01100011	163	10100011	227	11100011
36	00100100	100	01100100	164	10100100	228	11100100
37	00100101	101	01100101	165	10100101	229	11100101
38	00100110	102	01100110	166	10100110	230	11100110
39	00100111	103	01100111	167	10100111	231	11100111
40	00101000	104	01101000	168	10101000	232	11101000
41	00101001	105	01101001	169	10101001	233	11101001
42	00101010	106	01101010	170	10101010	234	11101010
43	00101011	107	01101011	171	10101011	235	11101011
44	00101100	108	01101100	172	10101100	236	11101100
45	00101101	109	01101101	173	10101101	237	11101101
46	00101110	110	01101110	174	10101110	238	11101110
47	00101111	111	01101111	175	10101111	239	11101111
48	00110000	112	01110000	176	10110000	240	11110000
49	00110001	113	01110001	177	10110001	241	11110001
50	00110010	114	01110010	178	10110010	242	11110010
51	00110011	115	01110011	179	10110011	243	11110011
52	00110100	116	01110100	180	10110100	244	11110100
53	00110101	117	01110101	181	10110101	245	11110101
54	00110110	118	01110110	182	10110110	246	11110110
55	00110111	119	01110111	183	10110111	247	11110111
56	00111000	120	01111000	184	10111000	248	11111000
57	00111001	121	01111001	185	10111001	249	11111001
58	00111010	122	01111010	186	10111010	250	11111010
59	00111011	123	01111011	187	10111011	251	11111011
60	00111100	124	01111100	188	10111100	252	11111100
61	00111101	125	01111101	189	10111101	253	11111101
62	00111110	126	01111110	190	10111110	254	11111110
63	00111111	127	01111111	191	10111111	255	11111111

Appendix F. Tabell över kommandon i olika operativsystem

I denna bok utgår vi från att du har tillgång till ett Linux eller Unixsystem. Har du inte det så finns det i detta kapitel en tabell över alla kommandon som nämnts i boken och deras motsvarighet i olika operativsystem.

För att få reda på exakt hur de fungerar så rekommenderas att du läser manualen till just ditt operativsystem.

Tabell F-1. Kommandotabell

Kommando	Linux/Unix	Windows 9x	Windows 2000/XP	MacOS
"Pinga" en adress	ping	ping	ping	
Lista nätverksgränssnitt	ifconfig	ipconfig	ipconfig	
Skriva ut routingtabellen	route	route /print	route /print	
Spåra en rutt (route)	traceroute	tracert	tracert	
DNS-uppslag	host eller nslookup	nslookup	nslookup	
Lista arp-tabell	arp -a	arp -a	arp -a	
Lista aktiva nätverksanslut-ningar	netstat	netstat	netstat	

Appendix G. Portnummer och tjänster

I detta appendix listas en del tjänster och deras motsvarande portnummer i urval. Man kan naturligtvis köra tjänster på vilken port som helst men vill man göra det lätt för sina användare så använder man dessa portar. Vill du se flera skall du läsa RFC 1700.

```
Keyword         Decimal    Description
-------         -------    -----------
echo              7/tcp    Echo
echo              7/udp    Echo
daytime          13/tcp    Daytime (RFC 867)
daytime          13/udp    Daytime (RFC 867)
chargen          19/tcp    Character Generator
chargen          19/udp    Character Generator
ftp              21/tcp    File Transfer [Control]
ftp              21/udp    File Transfer [Control]
ssh              22/tcp    SSH Remote Login Protocol
ssh              22/udp    SSH Remote Login Protocol
telnet           23/tcp    Telnet
telnet           23/udp    Telnet
smtp             25/tcp    Simple Mail Transfer
smtp             25/udp    Simple Mail Transfer
time             37/tcp    Time
time             37/udp    Time
domain           53/tcp    Domain Name Server
domain           53/udp    Domain Name Server
finger           79/tcp    Finger
finger           79/udp    Finger
http             80/tcp    World Wide Web HTTP
http             80/udp    World Wide Web HTTP
pop3            110/tcp    Post Office Protocol - Version 3
pop3            110/udp    Post Office Protocol - Version 3
sunrpc          111/tcp    SUN Remote Procedure Call
sunrpc          111/udp    SUN Remote Procedure Call
auth            113/tcp    Authentication Service
auth            113/udp    Authentication Service
nntp            119/tcp    Network News Transfer Protocol
nntp            119/udp    Network News Transfer Protocol
ntp             123/tcp    Network Time Protocol
ntp             123/udp    Network Time Protocol
netbios-ns      137/tcp    NETBIOS Name Service
netbios-ns      137/udp    NETBIOS Name Service
netbios-dgm     138/tcp    NETBIOS Datagram Service
netbios-dgm     138/udp    NETBIOS Datagram Service
netbios-ssn     139/tcp    NETBIOS Session Service
```

```
netbios-ssn     139/udp    NETBIOS Session Service
imap            143/tcp    Internet Message Access Protocol
imap            143/udp    Internet Message Access Protocol
ups             401/tcp    Uninterruptible Power Supply
ups             401/udp    Uninterruptible Power Supply
https           443/tcp    http protocol over TLS/SSL
https           443/udp    http protocol over TLS/SSL
isakmp          500/tcp    isakmp
isakmp          500/udp    isakmp
syslog          514/udp
printer         515/tcp    spooler
printer         515/udp    spooler
ldp             646/tcp    LDP
ldp             646/udp    LDP
silc            706/tcp    SILC
silc            706/udp    SILC
rsync           873/tcp    rsync
rsync           873/udp    rsync
imaps           993/tcp    imap4 protocol over TLS/SSL
imaps           993/udp    imap4 protocol over TLS/SSL
ircs            994/tcp    irc protocol over TLS/SSL
ircs            994/udp    irc protocol over TLS/SSL
pop3s           995/tcp    pop3 protocol over TLS/SSL (was spop3)
pop3s           995/udp    pop3 protocol over TLS/SSL (was spop3)
```

Appendix H. Topdomäner

Toppdomänerna är den översta nivån i DNS-hierarkin. I detta appendix listas de generiska och de nationella toppdomänerna. Dessa uppgifter kommer från Internet Assigned Numbers Authority (IANA, http://www.iana.org).

Generiska (gtld)

aero, Reserverad för medlemmar av flygtransportindustrin, sponsrad av Société Internationale de Télécommunications Aéronautiques (SITA).
biz, Begränsad till företag, drivs av NeuLevel, Inc.
com, Drivs av VeriSign Global Registry Services.
coop, Reserverad för kooperativa föreningar, sponsrad av Dot Cooperation LLC.
info, Drivs av Afilias Limited.
museum, Reserverad för museum, sponsrad av Museum Domain Management Association.
name, Reserved för privatpersoner, drivs av Global Name Registry.
net, Drivs av VeriSign Global Registry Services.
org, Drivs av Public Interest Registry. Avsedd för icke-kommersiella verksamheter men finns tillgänglig för alla.
pro, Under uppbyggnad, drivs av RegistryPro.
gov, Reserverad enbart för den amerikanska regeringen. Drivs av US General Services Administration.
edu, Reserverad för amerikanska skolväsendet
mil, Reserverad för det amerikanska försvaret.Drivs av US DoD Network Information Center.
int, Används bara av oraganisationer som etablerats av olika regeringar. Drivs av IANA .int Domain Registry.

Nationella (cctld)

ac, Ascension Island. *ad*, Andorra. *ae*, United Arab Emirates. *af*, Afghanistan. *ag*, Antigua and Barbuda. *ai*, Anguilla. *al*, Albania. *am*, Armenia. *an*, Netherlands Antilles. *ao*, Angola. *aq*, Antarctica. *ar*, Argentina. *as*, American Samoa. *at*, Austria. *au*, Australia. *aw*, Aruba. *az*, Azerbaijan. *ba*, Bosnia and Herzegovina. *bb*, Barbados. *bd*, Bangladesh. *be*, Belgium. *bf*, Burkina Faso. *bg*, Bulgaria. *bh*, Bahrain. *bi*, Burundi. *bj*, Benin. *bm*, Bermuda. *bn*, Brunei Darussalam. *bo*, Bolivia. *br*, Brazil. *bs*, Bahamas. *bt*, Bhutan. *bv*, Bouvet Island. *bw*, Botswana. *by*, Belarus. *bz*, Belize. *ca*, Canada. *cc*, Cocos (Keeling) Islands. *cd*, Congo, Democratic Republic of the. *cf*, Central African Republic. *cg*, Congo, Republic of. *ch*, Switzerland. *ci*, Cote d'Ivoire. *ck*, Cook Islands. *cl*, Chile. *cm*, Cameroon. *cn*, China. *co*, Colombia. *cr*, Costa Rica. *cu*, Cuba. *cv*, Cap Verde. *cx*, Christmas Island.

cy, Cyprus. *cz*, Czech Republic. *de*, Germany. *dj*, Djibouti. *dk*, Denmark. *dm*, Dominica. *do*, Dominican Republic. *dz*, Algeria. *ec*, Ecuador. *ee*, Estonia. *eg*, Egypt. *eh*, Western Sahara. *er*, Eritrea. *es*, Spain. *et*, Ethiopia. *fi*, Finland. *fj*, Fiji. *fk*, Falkland Islands (Malvina). *fm*, Micronesia, Federal State of. *fo*, Faroe Islands. *fr*, France. *ga*, Gabon. *gd*, Grenada. *ge*, Georgia. *gf*, French Guiana. *gg*, Guernsey. *gh*, Ghana. *gi*, Gibraltar. *gl*, Greenland. *gm*, Gambia. *gn*, Guinea. *gp*, Guadeloupe. *gq*, Equatorial Guinea. *gr*, Greece. *gs*, South Georgia and the South Sandwich Islands. *gt*, Guatemala. *gu*, Guam. *gw*, Guinea-Bissau. *gy*, Guyana. *hk*, Hong Kong. *hm*, Heard and McDonald Islands. *hn*, Honduras. *hr*, Croatia/Hrvatska. *ht*, Haiti. *hu*, Hungary. *id*, Indonesia. *ie*, Ireland. *il*, Israel. *im*, Isle of Man. *in*, India. *io*, British Indian Ocean Territory. *iq*, Iraq. *ir*, Iran (Islamic Republic of). *is*, Iceland. *it*, Italy. *je*, Jersey. *jm*, Jamaica. *jo*, Jordan. *jp*, Japan. *ke*, Kenya. *kg*, Kyrgyzstan. *kh*, Cambodia. *ki*, Kiribati. *km*, Comoros. *kn*, Saint Kitts and Nevis. *kp*, Korea, Democratic People's Republic. *kr*, Korea, Republic of. *kw*, Kuwait. *ky*, Cayman Islands. *kz*, Kazakhstan. *la*, Lao People's Democratic Republic. *lb*, Lebanon. *lc*, Saint Lucia. *li*, Liechtenstein. *lk*, Sri Lanka. *lr*, Liberia. *ls*, Lesotho. *lt*, Lithuania. *lu*, Luxembourg. *lv*, Latvia. *ly*, Libyan Arab Jamahiriya. *ma*, Morocco. *mc*, Monaco. *md*, Moldova, Republic of. *mg*, Madagascar. *mh*, Marshall Islands. *mk*, Macedonia, Former Yugoslav Republic. *ml*, Mali. *mm*, Myanmar. *mn*, Mongolia. *mo*, Macau. *mp*, Northern Mariana Islands. *mq*, Martinique. *mr*, Mauritania. *ms*, Montserrat. *mt*, Malta. *mu*, Mauritius. *mv*, Maldives. *mw*, Malawi. *mx*, Mexico. *my*, Malaysia. *mz*, Mozambique. *na*, Namibia. *nc*, New Caledonia. *ne*, Niger. *nf*, Norfolk Island. *ng*, Nigeria. *ni*, Nicaragua. *nl*, Netherlands. *no*, Norway. *np*, Nepal. *nr*, Nauru. *nu*, Niue. *nz*, New Zealand. *om*, Oman. *pa*, Panama. *pe*, Peru. *pf*, French Polynesia. *pg*, Papua New Guinea. *ph*, Philippines. *pk*, Pakistan. *pl*, Poland. *pm*, St. Pierre and Miquelon. *pn*, Pitcairn Island. *pr*, Puerto Rico. *ps*, Palestinian Territories. *pt*, Portugal. *pw*, Palau. *py*, Paraguay. *qa*, Qatar. *re*, Reunion Island. *ro*, Romania. *ru*, Russian Federation. *rw*, Rwanda. *sa*, Saudi Arabia. *sb*, Solomon Islands. *sc*, Seychelles. *sd*, Sudan. *se*, Sweden. *sg*, Singapore. *sh*, St. Helena. *si*, Slovenia. *sj*, Svalbard and Jan Mayen Islands. *sk*, Slovak Republic. *sl*, Sierra Leone. *sm*, San Marino. *sn*, Senegal. *so*, Somalia. *sr*, Suriname. *st*, Sao Tome and Principe. *sv*, El Salvador. *sy*, Syrian Arab Republic. *sz*, Swaziland. *tc*, Turks and Caicos Islands. *td*, Chad. *tf*, French Southern Territories. *tg*, Togo. *th*, Thailand. *tj*, Tajikistan. *tk*, Tokelau. *tm*, Turkmenistan. *tn*, Tunisia. *to*, Tonga. *tp*, East Timor. *tr*, Turkey. *tt*, Trinidad and Tobago. *tv*, Tuvalu. *tw*, Taiwan. *tz*, Tanzania. *ua*, Ukraine. *ug*, Uganda. *uk*, United Kingdom. *um*, US Minor Outlying Islands. *us*, United States. *uy*, Uruguay. *uz*, Uzbekistan. *va*, Holy See (City Vatican State). *vc*, Saint Vincent and the Grenadines. *ve*, Venezuela. *vg*, Virgin Islands (British). *vi*, Virgin Islands (USA). *vn*, Vietnam. *vu*, Vanuatu. *wf*, Wallis and Futuna Islands. *ws*, Western Samoa. *ye*, Yemen. *yt*, Mayotte. *yu*, Yugoslavia. *za*, South Africa. *zm*, Zambia. *zw*, Zimbabwe.

Appendix I. Tabell över CIDR-nät

Som vi sett i boken så delar man upp nätverksklasser i A-, B- och C-nät. Så var det från början på Internet. Skulle du ansluta ditt företag fick du välja om de behövde ett A-, B- och C-nät. Eftersom det är ganska stora steg mellan dem så blev det ett väldigt slöseri med IP-adresser. Varje företag måste ju skaffa ett nät som var större än det antal datorer de ville ansluta till Internet för att det skulle räcka. Man insåg snabbt att antalet adresser på Internet skulle ta slut om man inte kom på ett effektivare sätt att fördela dem på.

Teknikst så fungerar nätmasken så här. Både nätmasken och IP-adressen representeras (som allt annat) i binär form. Till exempel så blir nätmasken 255.255.255.0

11111111.11111111.11111111.00000000

naturligtvis är inte punkterna med men jag tar med dem ändå i exemplen för att det skall bli lättare att se.

En IP-adress, till exempel 192.168.0.1 ser ut så här i binär form

11000000.10101000.00000000.00000001

För att få fram nätverksadressen använder man den logiska (Booleska) operanden AND på varje bit i nätmasken med varje bit i IP-adressen. Detta kallas bitvis AND. AND fungerar enligt följande:

1 AND 1 = 1
1 AND 0 = 0
0 AND 1 = 0
0 AND 0 = 0

Det vill säga AND är bara 1 om båda termerna är 1.

Om man AND-ar nätmasken med IP-adressen får man fram nätadressen. Se nedan:

11111111.11111111.11111111.00000000
11000000.10101000.00000000.00000001 AND
11000000.10101000.00000000.00000000

Alltså är 11000000.10101000.00000000.00000000 = 192.168.0.0 nätverksadressen.

I exempler ät nätmasken 24 bitar stor (24 ettor). Man säger att det är ett /24-nät. Vilket är samma sak som ett C-nät eller ett nät med nätmasken 255.255.255.0.

Tekniskt så finns det inget som hindrar att man gör nät med andra nätmasker än de som hör till A-, B- och C-näten. Man införde ett koncept som kallas för CIDR (Classless Inter-Domain Routing) som är en metod för mer finmaskig uppdelning av ett IP-nät. Istället för att ange nätadressen som 192.168.0.0/255.255.255.0 så anger man den som nätadress/1-24 där 1-24 kallas IP-prefix eller nät-prefix och motsvarar nätmaskens storlek i bitar. Nät-prefixen 8, 16 och 24 motsvarar A-, B- och C-nät. Prefixet 32 motsvarar en nodadress (host).

Tabellen tabell I-1 visar alla CIDR nät. I kolumnen med anatelt adresser bör man beakta att det som regel "går bort" två adresser. Det är för att man behöver en broadcastadress och en nätverksadress.

Tabell I-1. CIDR nätadresser

Nätmask	CIDR-notation	Antal adresser	Kommentar
0.0.0.0	n.n.n.n/0	4 294 967 296	Hela Internet
128.0.0.0	n.n.n.n/1	2 147 483 648	128 A-nät
192.0.0.0	n.n.n.n/2	1 073 741 824	64 A-nät
224.0.0.0	n.n.n.n/3	536 870 912	32 A-nät
240.0.0.0	n.n.n.n/4	268 435 456	16 A-nät
248.0.0.0	n.n.n.n/5	134 217 728	8 A-nät
252.0.0.0	n.n.n.n/6	67 108 864	4 A-nät
254.0.0.0	n.n.n.n/7	33 554 432	2 A-nät
255.0.0.0	n.n.n.n/8	16 777 216	A-nät
255.128.0.0	n.n.n.n/9	8 388 608	128 B-nät
255.192.0.0	n.n.n.n/10	4 194 304	64 B-nät
255.224.0.0	n.n.n.n/11	2 097 152	32 B-nät
255.240.0.0	n.n.n.n/12	1 048 576	16 B-nät
255.248.0.0	n.n.n.n/13	524 288	8 B-nät
255.252.0.0	n.n.n.n/14	262 144	4 B-nät
255.254.0.0	n.n.n.n/15	131 072	2 B-nät
255.255.0.0	n.n.n.n/16	65 536	B-nät
255.255.128.0	n.n.n.n/17	32 768	128 C-nät
255.255.192.0	n.n.n.n/18	16 384	64 C-nät
255.255.224.0	n.n.n.n/19	8 192	32 C-nät
255.255.240.0	n.n.n.n/20	4 096	16 C-nät
255.255.248.0	n.n.n.n/21	2 048	8 C-nät
255.255.252.0	n.n.n.n/22	1 024	4 C-nät
255.255.254.0	n.n.n.n/23	512	2 C-nät
255.255.255.0	n.n.n.n/24	256	C-nät

Nätmask	CIDR-notation	Antal adresser	Kommentar
255.255.255.128	n.n.n.n/25	128	128 Noder (1/2 C-nät)
255.255.255.192	n.n.n.n/26	64	64 Noder (1/4 C-nät)
255.255.255.224	n.n.n.n/27	32	32 Noder (1/8 C-nät)
255.255.255.240	n.n.n.n/28	16	16 Noder (1/16 C-nät
255.255.255.248	n.n.n.n/29	8	8 Noder (1/32 C-nät)
255.255.255.252	n.n.n.n/30	4	4 Noder (1/64 C-nät)
255.255.255.254	n.n.n.n/31	2	2 Noder (1/128 C-nät)
255.255.255.255	n.n.n.n/32	1	1 Nod (hostadress)

Appendix J. Tabell över några av de RFC:er som berör boken

Tabell J-1. Exmpel på RFC:er som är relaterade till boken

RFC	Titel	URL
RFC 768	User Datagram Protocol (UDP)	http://www.faqs.org/rfcs/rfc768.html
RFC 2060	Internet Message Access Protocol (IMAP)	http://www.faqs.org/rfcs/rfc2060.html
RFC 792	Internet Control Message Protocol (ICMP)	http://www.faqs.org/rfcs/rfc792.html
RFC 977	Network News Transfer Protocol	http://www.faqs.org/rfcs/rfc977.html
RFC 854	Telnet Protocol Specification	http://www.faqs.org/rfcs/rfc854.html
RFC 1631	The IP Network Address Translator (NAT)	http://www.faqs.org/rfcs/rfc1631.html
RFC 1918	Address Allocation for Private Internets	http://www.faqs.org/rfcs/rfc1918.html
RFC 2822	Internet Message Format	http://www.faqs.org/rfcs/rfc2822.html

Appendix K. Kommentarer från läsare och experter

Brev från Bengt Gördén

Date: Thu, 11 Mar 2004 23:42:25 +0100
From: Bengt Gördén <bengan (snabel-a) sunet.se>
To: marcus@rejas.se
Subject: ang. NAT

Hej!

Ang. Datorkommunikation och kurs DTR1201.

Trevlig läsning (även om jag inte lyckats ta mig genom allt :-).

Nu till lite spörsmål ang. NAT.

Ditt avsnitt om NAT är inte riktigt rättvisande, om man utgår från att kapittlet egentligen handlar om IP-routing. IETF har under flera år varit rejält bekymrade ang. NAT. Anledningen är helt enkelt att NAT slår sönder det fundament varpå IP bygger. Det finns några få kriterier som måste uppfyllas för att Internet skall fungera. Ett av dem är "unik adresserbarhet". Genom att NAT (främst den varianten där man i hög grad bygger adresseringen på transportnivå) förhindrar detta så är det förkastligt att använda det.

Det är för övrigt ingen fördel att spara adresser då man konserverar en modell och bygger dåliga lösningar runt den. Speciellt i USA och Europa har vi inget adressproblem. Det finns så mycket adresser att vi kan gödsla med dem. Att få ut nya adresser är heller inte svårt. Det är bara de stora ISP:erna som anför annledningen att det är dåligt med adresser så att de bara kan dela ut 1 till varje hushåll. Den egentliga annledningen är att de inte vill att du har mycket burkar på ditt hemnät som aggerar servrar. Och kanske framför allt inte att du ska köra IP-telefoni (de stora ISP:erna är ju egentligen telekombolag).

Jag vet inte om du har tänkt skriva något om detta i din kurs men som "Old Internet Fart" (tm) så skulle jag råda dig till att skriva in ett stycke där man förklarar just grunden för IP och varför det är dumt att slå sönder den.

Brev från Pär Lindskog

Date: Sun, 30 May 2004 23:33:55 +0200
From: Pär Lindskog <lindskog (snabel-a) imapcenter.net>
To: marcus@rejas.se
Subject: Rättelse/tillägg Datorkommunikation

Hej

Surfade runt lite på se.linux.org och fastnade en stund på din bok om datorkommunikation. Mycket bra skrivet, verkligen välgjord.
Nu har jag inte läst hela boken (hoppas jag hinner till sommaren) men jag upptäckte en sak på kapitlet om E-post. Det står att med protokollet IMAP lagras all e-post lokalt... CENTRALT borde det vara? Sen har jag ett tillägg på IMAP-protokollet som kan vara värt att nämna, nämligen risken med backuper då mailen lagras centralt, man måste vara medveten om att man är helt och hållet i händerna på leverantören (motsv.) då det gäller backup av sina mail. Många av de leverantörer som specialicerat sig på IMAP har möjligheten att ladda ner allt innehåll i en mapp som tex. en zip-fil.

En stor fördel med IMAP är möjligheten till ett kommando som heter IDLE, vilken ser till att "pusha" ut mailen istället för att ställa in mailprogrammet att aktivt "gå" och hämta nya mail med visst intervall (som POP-mail). Om IDLE supportas av servern och klienten har jag mailet i min mailklient samtidigt som det kommer till servern. Man kan visserligen ställa tiden för hämtning av POP-mail lågt men det tar ganska stora resurser i anspråk (logga in, kolla, logga ut) så det kan lätt bli överbelastning på servern om många gör det...

Vidare under webmail står det att webmail ofta har begränsat utrymme på servern, som det står skrivet kan man tolka det som att utrymmet är obegränsat då man använder sig av någon mailklient (POP/IMAP), borde nog förtydligas lite, speciellt om man använder sig av IMAP då man måste rensa själv på servern.

Ändra/lägg till det du önskar eller tycker är relevant i sammanhanget, jag återkommer säkert med fler synpunkter i framtiden.

--
Mvh
/Pär Lindskog

Brev fån Jan Johansson

Date: Tue, 30 Nov 2004 16:27:10 +0100
From: "Jan Johansson" <jan.johansson (snabel-a) ragunda.se>
To: marcus@rejas.se
Subject: datorkommunikation

Hej Marcus
Jag har jobbat flera år som lärare och håller fullständigt med när det gäller svårigheten att hitta lämpliga böcker för kursen datorkommunikation. Kul att du har tagit detta initiativ! Boken är skriven på ett lättfattligt och lättläst sätt, men tenderar kanske att bli ytlig i en del avsnitt.

Jag brukar ta upp lite mer när det gäller repeatrar och bryggor. Bryggan är viktig att förstå eftersom den är grunden till hur switchen fungerar. Fortsätter sedan med att ta upp layer 2 funktionen, broadcast, switchar finns i olika utföranden mm. Begreppen simplex, halv- och full-duplex måste också förklaras.

Repeatrar
Är en kvarleva från bussnätens tid. Trots att koaxialkabeln i 10base2 (thinnet) kunde sträckas ut nästan 200meter och 10base5 (thicknet) ca 500 meter behövdes signalerna i koaxialkablarna förstärkas med hjälp av repeatrar så att man kunde forsätta ännu längre sträckor. Eftersom det var glest mellan datorerna på den tiden och de skulle dessutom sammanbindas med samma kabel blev det snabbt långa krokiga snirklingar med kablarna.

Med stjärnnäten blev repetrarna var mans egendom eftersom det sitter en förstärkare (repeater) på varje port i en hubb. Vi skulle kunna säga att hubben är en "multirepeater" som isolerar varje kabelsegment så att ett kabelfel (kortslutning, avbrott eller missanpassning) på ett ställe inte slår ut de andra anslutningarna (portarna) i hubben.

Bryggor
Har haft en lika tynande tillvaro som repeatrar men har nu börjat göra comeback i trådlösa nät. Bryggan används ofta för att minska onyttig trafik i nät där trafiken ökat för mycket. Egentligen så minskar man ej trafiken utan ser med bryggan till att hålla "onödig trafik" sk broadcast lokalt inom mindre områden. Genom att lagra nätverkskortens hårdvaruadresser "MAC-adresser" i ett litet minne, lär sig bryggan på vilken sida av bryggan som olika datorer finns. Bara den trafik som behöver komma till andra sidan av bryggan släpps sedan igenom. I nät med hubbar och Windows datorer kan broadcast och elections ta upp en stor del av bandbredden. För att lätta upp situationen är en brygga lättare

att sätta in än att dela nätet med en router.

I nät med switchar uppstår inte behovet av att sätta in bryggor eftersom switchar har en bryggfunktion i varje port. Därför kan vi likna switchen vid en "multibrygga". I dagens trådlösa nät har vi oftast en bryggfunktion inbygd i den trådlösa accesspunkten. Bryggan har i det fallet i uppgift att brygga samman det trådade nätet med det trådlösa.

Skall försöka återkomma med mera när jag får tid över. Du får använda/förändra som du vill.

Mvh
Jan Johansson

Appendix L. GNU Free Documentation License

Version 1.2, November 2002. Svensk översättning av Marcus Rejås och Alexander Nordström, Januari 2004.

This is an unofficial translation of the GNU Free Documentation License into Swedish. It was not published by the Free Software Foundation, and does not legally state the distribution terms for documentation that uses the GNU FDL -- only the original English text of the GNU FDL does that. However, we hope that this translation will help Swedish speakers understand the GNU FDL better.

Detta är en inofficiell översättning av GNU Free Documentation License till svenska. Den har inte publicerats av Free Software Foundation och är inte juridiskt gällande för spridning av dokumentation som använder GNU FDL -- bara den engelska originaltexten i GNU FDL gäller. Vi hoppas att denna översättning skall hjälpa svensktalande att förstå GNU FDL bättre.

0. BAKGRUND

Syftet med denna licens är att göra en handbok, bok, eller annat praktiskt och användbart dokument "fritt" som i frihet: att försäkra var och en den faktiska friheten att kopiera och sprida det vidare, med eller utan förändringar, antingen kommersiellt eller ideellt. Sekundärt bevarar denna licens ett sätt för författaren och förläggaren att få ära för deras arbete utan att de anses vara ansvariga för förändringar gjorda av andra.

Denna Licens är en sorts "copyleft", vilket betyder att derivativa verk av detta dokument själva måste vara fria på samma sätt. Den kompletterar GNU General Public License, som är en copyleft-licens utformad för fri programvara.

Vi har utformat denna licens för att den skall användas för handböcker till fri programvara, eftersom fri programvara behöver fri dokumentation: ett fritt program bör ha en handbok som erbjuder samma friheter som programmet gör. Men denna licens är inte begränsad till programvaruhandböcker; den kan användas för vilket textverk som helst oavsett ämne eller huruvida det är en utgiven, tryckt bok. Vi rekommenderar denna licens huvudsakligen för alla verk vars syfte är instruktion eller referens.

1. TILLÄMPNINGSOMRÅDE OCH DEFINITIONER

Denna licens [det engelska originalet] gäller för varje handbok eller annat verk, oavsett uttrycksform, som innehåller ett meddelande där upphovsrättsinnehavaren stadgat att verket kan spridas enligt villkoren i GNU Free Documentation License. Ett sådant meddelande ger en internationell frihet utan krav på ersättning och utan tidsbegränsning att använda verket under villkoren i denna licens [det engelska originalet]. "Dokument" nedan syftar på godtycklig handbok eller verk. Var och en är licenstagare och benämns som "du". Du accepterar villkoren i GNU Free Documentation License om du kopierar, modifierar eller sprider verket på ett sådant sätt att det kräver tillstånd enligt gällande upphovsrättslagstiftning.

En "förändrad version" av dokumentet avser varje verk som innehåller dokumentet eller en del av det, antingen ordagranna kopior, eller med ändringar och/eller översatt till ett annat språk.

Ett "sekundärt avsnitt" är en märkt bilaga eller förord till dokumentet som exklusivt behandlar förhållandet mellan dokumentets förläggare eller författare och dokumentets huvudsakliga ämne (eller till relaterade ämnen) och som inte innehåller något som direkt faller under det huvudsakliga ämnet. (Således, om dokumentet delvis är en lärobok i matematik så får ett sekundärt avsnitt inte förklara någon matematik.) Förhållandet kan vara en historisk koppling till ämnet eller något relaterat, eller en juridisk, kommersiell, filosofisk, etisk eller politisk ställning till det.

De "oföränderliga avsnitten" är sekundära avsnitt vars titlar är angivna som oföränderliga avsnitt i meddelandet som stadgar att dokumentet är utgivet under denna licens [det engelska originalet]. Om ett avsnitt inte innefattas av den ovanstående definitionen av sekundärt så är det inte tillåtet att ange det som oföränderligt. Dokumentet behöver inte innehålla några oföränderliga avsnitt. Om dokumentet inte anger några oföränderliga avsnitt så finns det inga.

"Omslagstexterna" är speciella korta ordföljder som är listade som framsidestexter eller baksidestexter i meddelandet som stadgar att dokumentet är utgivet under denna licens [det engelska originalet]. En framsidestext kan vara som mest 5 ord och en baksidestext kan vara som mest 25 ord.

En "transparent" kopia av dokumentet är en maskinläsbar kopia, representerad i ett format vars specifikation finns tillgänglig för allmänheten, som lämpar sig för att revidera dokumentet på ett enkelt sätt med generella textredigeringsprogram eller (för pixelbaserade bilder) generella grafikprogram eller (för ritningar) något väl tillgängligt ritprogram, och som är passande som indata till textfomaterare eller för automatisk konvertering till en mängd format som passar som indata till textformaterare. En kopia i ett för övrigt transparent filformat vars markeringar, eller avsaknad av markeringar, har ordnats för att hindra eller motverka att vidare förändring vidtas av läsare är inte transparent. Ett bildformat är inte transparent om det används för någon betydande del text. En kopia som inte är "transparent" kallas "opak".

Exempel på passande format för transparenta kopior innefattar ren ASCII utan markeringar, Texinfo indataformat, LaTeX indataformat, SGML eller XML som använder en publikt tillgänglig DTD, och standardenlig HTML, PostScript eller PDF utformat för mänsklig förändring. Exempel på transparenta bildformat innefattar PNG, XCF och JPG. Opaka format innefattar leverantörsspecifika format som bara kan läsas och editeras med leverantörsspecifika ordbehandlare, SGML eller XML för vilket DTD och/eller verktyg för behandling inte finns allmänt tillgängliga, och den maskingenererade HTML, PostScript eller PDF som produceras av vissa ordbehandlare enbart avsett som utdata.

"Titelsidan" innebär, för en tryckt bok, titelsidan själv, och sådana därpå följande sidor som krävs för att göra det material som enligt denna licens skall synas på titelsidan läsbart. För verk i sådana format som inte har någon egentlig titelsida, avses med "titelsida" den text som är närmast den mest framstående förekomsten av verkets titel, föregående den huvudsakliga textmassan.

Ett avsnitt "med titeln ÅÄÖ (XYZ)" avser en namngiven del av dokumentet vars titel är exakt XYZ eller innehåller XYZ inom parentes efterföljande text som översätter XYZ till ett annat språk. (Här står XYZ för ett speciellt namn på ett avsnitt nedan, som till exempel "Acknowledgements", "Dedications", "Endorsements" eller "History" [och ÅÄÖ för lämplig översättning, till exempel "tillkännagivanden", "dedikationer", "endossering" respektive "historik"].) Att "bevara titeln" på ett sådant avsnitt när du ändrar dokumentet innebär att det förblir ett avsnitt "med titeln ÅÄÖ (XYZ)" enligt denna definition.

Dokumentet får innehålla garantiavsägelser invid meddelandet om att denna licens [det engelska originalet] gäller för dokumentet. Dessa garantiavsägelser skall anses vara inkluderade per referens i denna licens, men bara för att friskriva från garantier. All annan innebörd dessa garantiavsägelser kan ha är ogiltiga och påverkar inte på något sätt innebörden i denna licens.

2. ORDAGRANN KOPIERING

Du äger kopiera och sprida dokumentet på valfritt medium, antingen kommersiellt eller ideellt, förutsatt att denna licens [det engelska originalet], upphovsrättsklausul, och meddelandet som stadgar att GNU Free Documentation License gäller för dokumentet finns med på alla kopior, och att du inte lägger till några som helst andra villkor än de som ingår i denna licens. Du äger inte vidta tekniska åtgärder för att begränsa eller kontrollera läsande eller vidare kopiering av de kopior du skapar eller sprider. Dock äger du ta emot kompensation i utbyte mot kopior. Om du sprider tillräckligt många kopior måste du också följa villkoren i paragraf 3.

Du äger också låna ut kopior, under samma villkor som ovan, och du äger visa kopior offentligt.

3. OMFATTANDE KOPIERING

Om du publicerar tryckta kopior (eller kopior i medier som normalt har tryckta omslag) av dokumentet, i en upplaga överstigande 100 exemplar, och dokumentets licensmeddelande kräver omslagstexter, så måste du förse kopiorna med omslag som, klart och tydligt, visar alla omslagstexter: framsidestexter på framsidan och baksidestexter på baksidan. Båda omslagen måste klart och tydligt identifiera dig som utgivare av dessa kopior. Framsidan måste presentera dokumentets hela titel, med alla ord i titeln lika framträdande och synliga. Du äger lägga till ytterligare stoff på omslagen. Kopiering med förändringar gjorda bara på omslaget, så länge som de bevarar dokumentets titel och i övrigt uppfyller dessa krav kan anses vara ordagrann kopiering i andra avseenden.

Om de obligatoriska texterna för något omslag är för omfattande för att rymmas i läsbart skick skall du placera de första (så många som får plats) på det egentliga omslaget, och fortsätta med resten på de direkt intilliggande sidorna.

Om du publicerar opaka kopior av dokumentet i upplagor om mer än 100, måste du antingen bifoga en maskinläsbar transparent kopia med varje opak kopia, eller ange i eller med varje opak kopia en nätverksadress som är tillgänglig för den allmänna nätverksanvändande massan där man, med öppet standardiserade protokoll, kan ladda ner en komplett transparent kopia av dokumentet, utan extra material. Om du väljer det senare alternativet, måste du vidta skäliga åtgärder, när du börjar sprida opaka kopior i kvantitet, för att denna transparenta kopia skall förbli tillgänglig på angivna platsen till åtminstone ett år efter den sista gången du spred en opak kopia (direkt eller via ombud eller återförsäljare) av den utgåvan till allmänheten.

Det är önskvärt, men inte ett krav, att du kontaktar författarna till dokumentet i god tid innan du sprider något större antal kopior, för att ge dem en chans att förse dig med en uppdaterad version av dokumentet.

4. FÖRÄNDRINGAR

Du äger kopiera och sprida en förändrad version av dokumentet under de villkor som beskrivs i paragraf 2 och 3 av GNU Free Documentation License, förutsatt att du släpper den förändrade versionen under exakt denna licens, och att den förändrade versionen antar dokumentets roll, och således medger spridning och förändring av den förändrade versionen till envar som erhåller en kopia av den. Utöver detta måste du göra följande med den ändrade versionen:

A. På titelsidan (och omslagen om det finns några) använda en titel skild från den som [original]dokumentet har, och skild från tidigare versioners titel (som skall, om det finns några,

finnas listade i historikavsnittet i dokumentet). Du äger använda samma titel som det föregående dokumentet om den ursprungliga utgivaren ger sitt tillstånd.

B. Lista, som författare, en eller flera personer eller juridiska personer som ansvarat för förändringarna i den ändrade versionen, tillsammans med minst fem av de huvudsakliga författarna av dokumentet (alla dess huvudsakliga författare, om det har mindre än fem), såvida de inte ger dig tillstånd att bortse från detta krav.

C. Ange namnet på utgivaren av den ändrade versionen, som utgivare, på titelsidan.

D. Bibehålla dokumentets alla upphovsrättsklausuler.

E. Lägga till en upphovsrättsklausul för dina förändringar angränsande till de andra upphovsrättsklausulerna.

F. Direkt efter upphovsrättsklausulerna innefatta ett meddelande som ger allmänheten tillstånd att använda den ändrade versionen under villkoren i denna licens [det engelska originalet] i den form som visas i Tillägg nedan.

G. I meddelandet om licensen bevara den fullständiga listan över oföränderliga avsnitt och obligatoriska omslagstexter som finns i dokumentets meddelande om licensen.

H. Inkludera en oförändrad kopia av denna licens [Det är den engelska originalversionen som avses].

I. Bevara avsnittet med titeln "historik (History)", bevara dess titel och lägg i avsnittet till en post med åtminstone titeln, året, nya författare och utgivaren av den modifierade versionen så som angivet på titelsidan. Om det inte finns något avsnitt med titeln "historik (History)" i dokumentet så skapa en med titeln, året, författare och utgivaren av dokumentet så som det står på [original]dokumentets titelsida. Lägg sedan till en post som beskriver den förändrade versionen så som beskrivits ovan.

J. Bevara den nätverksadress, om det finns någon, angiven i dokumentet till den allmänt tillgängliga transparenta kopian av dokumentet, och likaså nätverksadresserna till de föregående versioner som dokumentet baseras på. Dessa får placeras i avsnittet "historik (History)". Du äger utelämna en nätverksadress för ett verk som är publicerat mer än fyra år före dokumentet självt, eller om den ursprunglige utgivaren vars verk nätverksadressen hänvisar till ger sitt tillstånd.

K. För alla avsnitt med titlarna "tillkännagivanden (Acknowledgements)" eller "dedikationer (Dedications)", bevara titeln på avsnittet, och bevara allt innehåll och prägel på alla tillkännagivanden och/eller dedikationer gjorda av varje bidragare.

L. Bevara alla oföränderliga avsnitt i dokumentet oförändrade till text och titel. Avsnittsnummer eller motsvarande anses inte tillhöra avsnittets titel.

M. Radera varje avsnitt med titeln "endossering (Endorsements)". Ett sådant avsnitt får inte inkluderas i en modifierad version.

N. Inte byta titel på något existerande avsnitt så att det blir "endossering (Endorsements)" eller så att titeln kan förväxlas med något oföränderligt avsnitt.

O. Bevara varje garantiavsägelseklausul.

Om den förändrade versionen innehåller nya framsidestexter eller bilagor som är att anses som sekundära avsnitt och inte innehåller något material kopierat från dokumentet, så äger du, om du vill, benämna några eller samtliga av dessa som oföränderliga. För att göra detta, lägg deras titlar till listan över oföränderliga avsnitt i den förändrade versionens licensmeddelande. Dessa titlar måste vara skilda från alla andra avsnitts titlar.

Du äger lägga till ett avsnitt med titeln "endossering (Endorsements)", förutsatt att det inte innehåller något annat än endosseringar för din modifierade version från olika aktörer -- till exempel, meddelanden om utförd korrekturläsning eller att texten har godkänts av en organisation som en officiell definition av en standard.

Du äger lägga till ett textavsnitt på upp till fem ord som framsidestext, och ett textavsnitt på upp till 25 ord som baksidestext i listan över omslagstexter i den modifierade versionen. Bara ett textavsnitt med framsidestexter och ett med baksidestexter får läggas till av (eller genom försorg av) en enda juridisk person. Om dokumentet redan innehåller en omlagstext för något av omslagen, tidigare tillagd av dig eller genom försorg av samma juridiska person som du företräder, äger du inte lägga till en till, men du äger ändra den gamla med tillstånd från den tidigare utgivaren som lade till den förra.

Författaren (författarna) och utgivaren (utgivarna) av dokumentet ger inte via denna licens sitt tillstånd att använda sina namn för publicitet eller för att lägga till eller antyda endossering av någon modifierad version.

5. KOMBINERA DOKUMENT

Du äger kombinera dokumentet med andra dokument som är utgivna under denna licens, under de villkor som definieras i paragraf 4 av GNU Free Documentation License för modifierade versioner, förutsatt att du, i det kombinerade dokumentet, innefattar alla oföränderliga avsnitt från originaldokumenten, omodifierade, och listar dem som oföränderliga avsnitt i ditt kombinerade verk i dess licensklausul, och att du bevarar alla deras garantiavsägelseklausuler.

Det kombinerade verket behöver bara innehålla en enstaka kopia av denna licens [engelska originalversionen], och flera identiska oföränderliga stycken kan ersättas med en kopia. Om det finns flera oföränderliga stycken med samma namn men olika innehåll, se till att titeln på varje sådant avsnitt är unik genom att i slutet på den, inom parentes, lägga till namnet på den ursprunglige författaren eller utgivaren av det avsnittet om dessa är kända, annars ett unikt nummer. Gör samma justeringar av titlarna i listan över oföränderliga avsnitt i licensklausulen i det kombinerade verket.

I det kombinerade verket måste du kombinera alla avsnitt med titlarna "historik (History)" i de ursprungliga dokumenten, till ett avsnitt med titeln "historik (History)"; på samma sätt skall alla

avsnitt med titlarna "tillkännagivanden (Acknowledgements)", alla avsnitt med titlarna "dedikationer (Dedications)" kombineras. Du måste ta bort alla avsnitt med titlarna "endossering (Endorsements)".

6. SAMLINGAR AV DOKUMENT

Du äger skapa en samling bestående av dokumentet och andra dokument som är släppta under GNU Free Documentation License, och ersätta individuella kopior i dokumenten av denna licens med en enda kopia [av den engelska originalversionen] som inkluderas i samlingen, förutsatt att du följer villkoren för ordagrann kopiering i denna licens för varje inkluderat dokument i alla andra avseenden.

Du äger lyfta ut ett dokument från en sådan samling, och sprida det enskilt under GNU Free Documentation License, förutsatt att du lägger till en kopia av denna licens [den engelska originalversionen] i det utlyfta dokumentet, och följer villkoren för ordagrann kopiering i denna licens för det utlyfta dokumentet i alla andra avseenden.

7. SAMMANSLAGNING MED OBEROENDE VERK

En samling av dokumentet eller av dess derivat med andra separata och oberoende dokument eller verk, på eller i en lagringsvolym eller ett spridningsmedium, kallas för en "sammanslagning" om den sammanslagna upphovsrätten inte används för att begränsa samlingens användares rättigheter som de enskilda dokumenten medger. När dokumentet ingår i en sådan sammanslagning, gäller inte denna licens de andra verken i samlingen som inte själva är deriverat av dokumentet.

Om kravet på omslagstexter enligt paragraf 3 är tillämpligt på dessa kopior av dokumentet, så kan dokumentets omslagstexter, om dokumentet utgör mindre än hälften av hela samlingen, placeras på det omslag som omger dokumentet inuti samlingen, eller den elektroniska motsvarigheten till omslag om dokumentet är i elektronisk form. Annars måste de synas på det omslag som omger hela samlingen.

8. ÖVERSÄTTNING

Översättning anses vara en sorts förändring, så du äger sprida översättningar av dokumentet enligt de villkor som sätts i paragraf 4. Oföränderliga avsnitt som ersätts med översättningar kräver tillstånd från deras upphovsrättsinnehavare, men du äger inkludera översättningar av alla eller vissa av dessa oföränderliga avsnitt tillsammans med originalversionerna av dessa oföränderliga avsnitt. Du äger inkludera en översättning av denna licens, och alla licensklausuler i dokumentet, och alla

garantiavsägelser, förutsatt att du också innefattar den engelska originalversionen av denna licens och originalversionerna av dessa klausuler. Skulle det finnas skillnader mellan översättningen och originalversionen av denna licens eller någon klausul så gäller originalversionen.

Om ett avsnitt i dokumentet har titeln "tillkännagivanden (Acknowledgements)", "dedikationer (Dedications)", eller "historik (History)", kommer kravet (paragraf 4) att bevara dess titel (paragraf 1) vanligtvis att kräva att själva titeln ändras.

9. UPPHÖRANDE

Du äger inte kopiera, förändra, omlicensiera eller sprida dokumentet annat än enligt villkoren i GNU Free Documentation License. Alla övriga försök att kopiera, modifiera, omlicensiera, eller sprida dokumentet är ogiltiga och kommer automatiskt medföra att du förlorar dina rättigheter enligt denna licens. Tredje man som har mottagit kopior eller rättigheter från dig enligt dessa licensvillkor kommer dock inte att förlora sina rättigheter så länge de följer licensvillkoren.

10. FRAMTIDA VERSIONER AV DENNA LICENS

Free Software Foundation kan publicera nya, reviderade versioner av GNU Free Documentation License då och då. Sådana nya versioner kommer att vara likadana i andemening som den nuvarande versionen, men kan skilja i detalj för att behandla nya problem eller angelägenheter. Se http://www.gnu.org/copyleft/.

Varje version av licensen ges ett unikt versionsnummer. Om dokumentet stadgar att en specifik numrerad version av denna licens "eller valfri senare version" gäller för det, så äger du rätten att följa villkoren enligt antingen den angivna versionen eller vilken senare version som helst som publicerats (inte som utkast) av Free Software Foundation. Om dokumentet inte anger en version av denna licens, äger du välja vilken version som helst som publicerats (inte som utkast) av Free Software Foundation.

TILLÄGG: Hur du använder denna licens för dina dokument

För att använda GNU Free Documentation License för ett dokument du har skrivit, inkludera en kopia av licensen [det engelska originalet] i dokumentet och placera följande copyrightklausul omedelbart efter titelsidan:

> Copyright (c) ÅRTAL DITT NAMN. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".
>
> [Översättning:] Copyright (c) ÅRTAL DITT NAMN. Var och en äger rätt att kopiera, sprida och/eller förändra detta dokument under villkoren i licensen "GNU Free Documentation License", version 1.2 eller senare publicerad av Free Software Foundation, utan oföränderliga avsnitt, utan framsidestexter och utan baksidestexter. En kopia av denna licens finns med i avsnittet med titeln "GNU Free Documentation License".

Om du har oföränderliga avsnitt, framsidestexter och baksidestexter, ersätt "with...Texts." ("utan...texter.") med följande:

> with the Invariant Sections being LISTA DERAS TITLAR, with the Front-Cover Texts being LISTA, and with the Back-Cover Texts being LISTA.
>
> [Översättning:] med de oföränderliga avsnitten LISTA DERAS TITLAR, med framsidestexterna LISTA, och med baksidestexterna LISTA.

Om du har oföränderliga avsnitt utan omslagstexter, eller någon annan kombination av de tre, slå samman dessa två alternativ så att det passar den uppkomna situationen.

Om ditt dokument innehåller icke-triviala exempel med programkod, så rekommenderar vi att du släpper dessa exempel parallellt under en, av dig vald, fri programvarulicens, som till exempel GNU General Public License, för att möjliggöra deras användning i fri programvara.

Appendix M. GNU Free Documentation License (Originaltext)

Version 1.2, November 2002

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it,

either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in

formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work’s title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document’s license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document’s license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version’s license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add

another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> Copyright (c) YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

> with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.