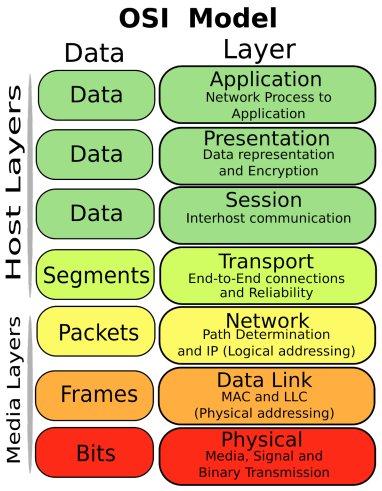
Nätverkskommunikation Essä

Bakgrund

På 60-talet utvecklades det första prototypen av vad vi idag skulle kalla internet. ARPANET, som det då kallades, var ett forskningsprojekt för det amerikanska försvaret för att kommunicera med andra forskningsinstitut i landet i fall ett kärnvapenkrig skulle utlösas mellan stormakterna. På den tiden använde man ARPANET för att fördela filer och för att kunna logga in och använda andra forskningsinstituts datorer. Redan i ett tidigt stadie fick man problem med att kommunikationsmetoderna inte var standardiserade och att de inte fanns några centrala protokoll att gå efter, då olika datorer inte kunde kunde kommunicera över nätet med datorer av olika fabrikat och typ. Alla datortillverkare hade olika sätt att tillverka sina datorer och hur de kommunicerade med varandra. I början och i mitten av 70-talet började man utveckla e-posten som blev en av dem första sättet att normalisera kommunikation över nätet. På denna tid var det oftast bara amerikanska universitet som använde sig av ARPAnet, men redan tidigt i utveckling insåg man att man var tvungen att sätta standard för nätverkskommunikation för att effektivisera kommunikationen. Det är här då bland de första protokollen kliver in i form av TCP/IP, som kommer tas upp mer om senare i uppsatsen, som skapades just för att finna en internationell standard för kommunikation över nätet. Efter ett antal statliga infrastruktursatsningar på ökad bandbredd i USA hade man tillslut skapat fundamentet för det internet vi känner till idag. På mitten av 90-talet kom även ett annat protokoll: HTTP (HyperText Transport Protocol), som tillsammans med World Wide Web (WWW) möjliggjorde vårt behov av att finna information på ett enklare sätt genom att skapa det vi idag finner i olika Webbläsare: det moderna internet som vi känner till. Det var också runt denna tid som OSI-modellen kom in i bruk som en riktlinje för bland annat kommunikationsfelsökningar och bearbetning av dessa problem. På senare år har även en del andra protokoll tillkommit för att effektivisera informationens väg till olika användare på internet.

OSI Modellen



Fysiskt lager

Det fysiska lagret omfattar alla fysiska komponenter som krävs för att två datorer ska kommunicera. Vid detta lager överförs bits, i form av datapaket (Data packets), med fysiska medel. Detta omfattar allt från kablar till hubs och repeterare, alltså datornätverkshårdvaran. Det är även det första lagret i OSI-modellen.

Datalänkslager

Datalänkslagret tillhandahåller datapaketen som det fysiska lagret ger ifrån sig och omvandlar det till bits. Detta skikt ser även över att om det skett något fel i det fysiska lagret och fastställer att signalen har kommit fram. Denna signal kan även ta form av en Broadcastmeddelande. Ett Broadcastmeddelande är ett medelande som skickas till alla datorer på samma Lan (Local Area Network), och kan bland annat användas när en dator vill ta kontakt med en DHCP server för att få tag i sin IP-adress (Kommer mer om IP-Adresser senare). Datalänkslagret har också två så kallade Sublayers: En *Media Access Control* (MAC) och en *Logical Link Control* (LLC)

MAC: Mac-lagret tar hand om den information som ges från det första lagret: Det fysiska lagret. Mac har även en så kallad Mac-adress som används för att identifiera ett unikt nätverkskort. Kort sagt kontrollerar MAC hur de olika nätverksnoderna får access till det fysiska lagret i OSI-modellen

LLC: LLC-lagret tar hand om den information som det övre lagret ger: Nätverkslagret. Några av LLC främsta uppgifter är att använda sig av Multiplexera samt demultiplexera, det vill säga att sortera de olika protokollinformationerna från olika protokoll från lagret ovan. Den ser till så att rätt information hamnar i rätt kanal.

Datalänkslagret är det andra lagret i OSI-modellen och har tillsamans med det fysiska lagret en del protokoll. Dessa protokoll handlar delvis of ethernet som bland annat IEEE 802.2 LLC IEEE 802.3 som är en standard för vad som kan kallas för ethernet.

Nätverkslager

Nätverkslagret ser till så att hitta den optimala vägen för informationen att ta, även kallat "Routing". IP (Internet protocol) infinner sig även här och hjälper till att adressera mottagaren såväl källan av informationen för att effektivisera rutten. Nätverkslagret sköter även om omvandlingen från logiska adresser till fysiska adresser i form av MAC adresser.
Nätverksslagret är det tredje lagret i OSI-modellen och har även en del protokoll. Bland annat befinner sig IS-IS (Intermediate System-to-Intermediate) och ES-IS (End System-to-Intermediate) som hjälper med dirigeringen (routing) av information

IP

Ip adress motsvarar din plats på internet. IP systemet liknar till stor del vårt postsystem, där alla adresser inom ett visst geografiskt område har en unik adress. Detsamma gäller våra datorer. Alla datorer eller andraapparater uppkopplade till internet har alla en unik IP-adress, och likväl vårt telefonsystem, avgränsas dessa av geografiskt område. Ingen kan ha samma telefonnummer, om dem inte är i ett annat land exempelvis, och detsamma gäller även för IP-adresser. IP-adresser används för att hitta en dator och kunna skicka data till denna utan att riskera att datan hamnar någon annanstans. Ip-adresser är skrivna i binär kod och är uppdelat i 32 bits. Dessa bits är i sin tur uppdelade i 4 lika stora delar, alltså blir det 8 bits per indelning. Ett vanligt exempel på en IP-adress är 192.168.1.1. och skrivs binärt 11000000.10101000.00000001.00000001. Det går högst att uppnå 255 i det binära systemet är 11111111 eller 255. Notera att varje siffra i den binära koden är ett bit och att det då existerar 32 siffror över 4 sektioner.

IP-adresser brukar oftast delas in i tre kategorier: A, B och C. Dessa olika grupper påverkar antalet unika Ip-adresser som kan finnas på nätverket. Det som skiljer dessa åt är de så kallade nätmaskerna. Nätmaskerna kan se ut såhär:

Klass:	Nätmasksadress	Antalet möjliga unika IP-adresser
A	255.0.0.0	16 777 214
B	255.255.0.0	65 534
C	255.255.255.0	254

255:orna motsvarar alltså hur stort IP-nätet är och 0:orna är möjliga IP-adresser

A, B och C klasserna har också förutbestämda startnummer där:

Klass	Möjliga starnummer
A	0.0.0.0 - 127.255.255.255
B	128.0.0.0 - 191.255.255.255
C	192.0.0.0 - 223.255.255.255

Det finns även fler klasser under dessa tre men dem används sällan

Det finns även så kallade "Broadcast Adress" som använts för att skicka information till alla datorer på samma nätverk, istället för att individuellt skicka informationen till alla individuella datorer på nätverket. Detta liknar väldigt mycket hur man använder sig av Broadcast meddelanden på samma nätverk. Broadcast adressers nätmask ser lite annorlunda ut där 255.255.255.255 indikerar att meddelandet skickas till alla IP-adresser på nätverket.

Några Exempel:

Om man ska använda sig av några exempel som man fått skåda i uppgiften kan vi inledningsvis börja med arbetsplatsen med 2500 människor med IP-adressen 172.17.5.1. Det vi kan inspektera redan nu på IP adressen är att den tillhör B klassen som kan ha upp emot 65 534 (256 * 256 - 2) eftersom startnumret är 172. Detta innebär att de två sista sektionerna är unika IP-adresser. Ett exempel på hur man skulle kunna dela ut dessa skulle kunna vara att fylla upp alla systematiskt. Det vill säga att man fyller ut från lägsta till högsta. Dock krävs det en så kallad "Default Gateway" som oftast brukar vara en router som klarar upp emot 254 individuella IP-adresser. Därför blir den första adressen Default Gateway. Tillgängliga adresser blir således:
172.17.1.2 - ….1.254
172.17.2.2 - ….2.254
Och så vidare tills alla IP adresser är fyllda

Det andra exemplet som man fick skåda var 192.168.1.1. Denna adress tillhör klass C och kan således bara ha 254 unika IP-adresser. Det är också ett så kallat privat nätverk som då enbart kan kommunicera med datorerna med samma IP-nät och inte ut på internet. Eftersom vi tidigare etablerade att nätverket är att klassen C har vi därav bara en sektion för IP-adressen. Eftersom nätverket för övrigt är privat krävs det ingen "Default Gateway".

Nätverket kommer fördelas som följande:
192.168.1.1 - …1.25

Transportlager

Transportlagret innefattar allt som har med transport av data att göra som inte är av fysiska komponenter. Transportlagret bryter ner alla data i mindre så kallade segment (Segments), fixar så att all information förses i samma ordning som den kom in i och förser andra lager med "End-to-end" leverans. I transportlagret finner vi protokollen TP0-TP4 som alla möjliggör uppkopplad samt trådlös transport. Transportlagret är det fjärde lagret i OSI-modellen.

Sessionslagret

Sessionslagret används för att skapa en direktkontakt mellan två datorer i en så kallad session. Ett exempel på en av dessa sessioner är bland annat filöverföringssession. Detta lager initierar också kontakten mellan de två datorerna. Sessionslagret används dock inte så mycket nu för tiden, som informationen om lagret är knapp. Sessionslagret är det femte lagret i OSI-modellen och dess protokoll handlar främst om "Session-service users" alltså ett förfrågan om hjälpa av sessionslagret. Protokollen kallas Session Service/Session Protocol.

Presentationslager

I detta lager omformateras data utan att ändra på dess innehåll. Här krypteras och komprimeras data i överföringen. Här hanteras även de språk som används mellan presentationslagret och applikationslagret (tillämpningslagret). Operativsystem jobbar på denna nivå, bland annat Microsoft DOS. Protokollen som finns här handlar främst om kommunikationen mellan lagret och exempelvis operativsystemet. Presentationslagret är det sjätte lagret i OSI-modellen

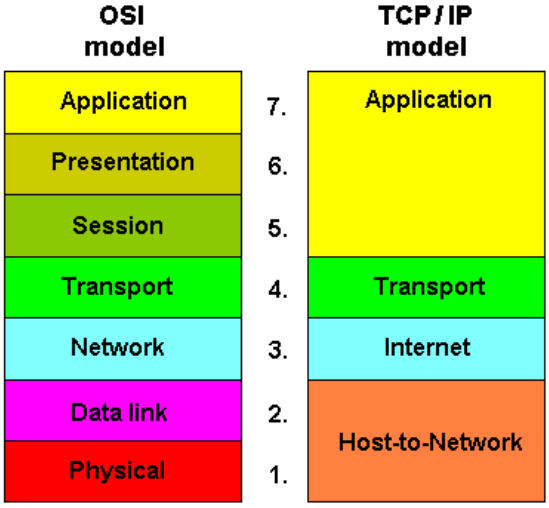
Applikationslager

Här finns de program som använder internet och som hanteras direkt av oss användare, där användaren kommer i kontakt med programvaran. Applikationslagret kan även ses som ett slags fönster mellan sändaren och mottagaren. HTTP är ett protokoll som infinner sig här bland annat, men det finns också många protokoll på detta lager, exempelvis

- **DNS** (Domain Name System)
- **DHCP** (Dynamic Host Configuration Protocol) som primärt används för att konfigurera nätverksanslutningar.
- **BitTorrent**, som används för fildelning

Applikationslagret är det sjunde, och sista, lagret i OSI-modellen.

TCP/IP



TCP/IP eller Transmission Control Center/Internet Protocol har likt OSI-modellen också lager och ett flertal av OSI-modellens lager finns även i TCP/IP såsom applikationslagret och transportlagret, bara med lite olika namn med liknande samma funktion. TCP/IP modellen är också således lik OSI-modellen då båda står i grund som riktlinjer för hur information bör överföras från dator till dator. TCP/IP är förvisso den äldre av dem två, och är mer väletablerat som en regel inom data- och nätverkskommunikation, medans motsvarigheten i OSI-modellen ännu inte är lika väletablerat, men används fortfarande som riktlinjer för exempelvis spårning av kommunikationsfel. TCP/IP har bara fyra Lager:

- Applikationslagret, med alla protokoll, motsvarar lager 5-7 i OSI-modellen
- TCP samt UDT (“Host to Host”), som även kallas Transportlagret, motsvarar Transportlagret i OSI-modellen, alltså lager 4
- IP, även kallats Nätverkslagret, som motsvarar nätverkslagret, lager 3 i OSI-modellen
- Länklagret som motsvarar lager 1 samt 2 i OSI-modellen

TCP/IP fungerar som sådant att **applikationslagret** interagera med exempelvis den webbläsare du använder genom en bunt olika protokoll såsom HTTP (HyperText Transfer Protocol), DNS (Domain Name System) och SMTP (Simple Mail Transfer Protocol). Denna, exempelvis webbläsare, skickar data till användaren, alltså datorn i detta fall, genom att använda sig av TCP/IP. Denna data hamnar först i applikationslagret och skickas sedan vidare till transportlagret genom så kallade portar (Ports) som har olika nummer beroende på vilket protokoll som användarlagret har interagerat med på exempelvis webbläsaren. Ett av dem vanligaste protokollen är HTTP som använder port 80. I transportlagret fördelas datan i små paket (Packets) för att effektivisera tiden det tar för datan att nå användaren. I transportlagret finns det två protokoll med detta arbetsområde, nämligen TCP och UDP (User Datagram Protocol). Skillnaden mellan TCP och UDP är att TCP lägger till en så kallad “header” på varje paket med instruktioner om vart den ska någonstans och i vilken ordning den ska ligga i när den ankommer till användaren. Detta garanterar att ens data eller meddelande alltid kommer komma till rätt plats eller kommer komma fram. UDP effektiviserar tiden genom

att skippa att sortera datan i ordning samt att man också förlorar garantin på att datan kommer ankomma till rätt plats. Risken för korruption av datan finns också, men UDP går väldigt mycket snabbare än TCP och används också vid låg latens (Low Latency) applikationer såsom Onlinespel.

Efter denna process fortsätter paketen vidare till nätverkslagret där IP infinner sig. Detta lager sätter ditt IP adressen för både ursprungsdatorn och destinationsdatorn för att paket ska nå rätt destination. Efter detta fortsätter paket till Länklagret där exempelvis MAC (Media Access Control) finns. Detta ser till att informationen i form av paketet når rätt fysisk adress såväl som att konverterar datan till så kallade elektriska impulser i de fysiska ethernetkablarna

Konfigurera router:

För att exempelvis kunna få din router att kommunisera ned resteande nätverkskomponenter krävs det att man konfigurerar den. För att göra detta så behöver man en dator med en fungerande webbläsare och en router som antingen är uppkopplade till nätverket eller är trådlös. Som tidigare har påpekats har denna Default Gateway också en IP-adress som står med på dokumentationen som medföljer vid köp av en router, och för att då konfigurera routern så skriver man in denna IP i URL:n som exempelvis http://192.168.0.1. När man väl kommer in på sidan brukar det medföljas en mindre guide på hur man konfigurera router, som ibland kan skifta beroende på tillverkare. Här kan du även till exempel:

- Sätta på din routers brandvägg
- Sätta på DHCP (Dynamic Host Configuration Protocol)
- Ställa in SSID (Service Set Identifier) som blir namnet på ens router.

Kryptering

Kryptering är en metod som hjälper att skydda känslig information genom att kryptera informationen antingen på din dator eller på annan uppkopplad apparat. När du bland annat skriver in dina kortuppgifter på datorn krypteras denna information när den checkas om den är korrekt. Detta för att förhindra att människor ska kunna ta den informationen under tiden som den transporteras. Hur man kan kryptera informationen varierar kraftigt och det finns många olika versionerna av kryptering. En av de äldsta metoderna för krypteringen är den så kallade "Caesars nyckel" som fungerar så att alla bokstäver i alfabetet hoppade 4 steg framåt. Ordet "Hej" blir istället "Khm". För utomstående blir denna information meningslös och det är precis det man vill uppnå. Man kan även kryptera individuella filer på datorn och även hela hårddiskar, men de senare alternativet rekommenderas att avstå ifrån då det är svårt att återfå informationen om hårddisken skulle korrumperas. Kryptering är därav väldigt viktigt när man ska skydda känslig information eller filer.

Trådlöst nätverk

Ett trådlöst nätverk är ett nätverk som kommunicerar mellan noder med hjälp av radio. Traditionellt sätt har man använt sig av ethernet sladdar för att kommunicera elektriska impulser från nod till nod, men med hjälp av det trådlösa nätverket har man kunnat framställa en ny typ av internetdelning. Även här träder det tidigare

nämnda ämnet kryptering in då det spelar stor roll i fördelning av information över det trådlösa nätverket. Det finns olika typer av trådlösa nätverk. Ad-hoc-nätverk kännetecknar när enbart två noder kommunicerar med varandra, medans meshnätverk kännetecknas av att flera noder är ansluta till varandra. Så kallade accesspunkter är ett trådlöst nätverk med en central nod som alla andra noder är ansluna till. Noderna kan i sen också anslutas till internet vilket då möjliggör internetuppkoppling.

Olika protokoll

HTTP:
HyperText Transport Protocol används för att överföra data från HTML:n som finns bevarade på hemsidan för att kunna läsa av informationen som finns på hemsidan. Sedan en tid tillbaka har man även implementerat in kryptering i HTTP och då har man även lagt till Secure på slutet av protokollnamnet, alltså HTTPS.

SMTP
För att skicka ett mejl krävs det ett protokoll vid namn SMTP eller Simple Mail Transfer Protocol. Detta protokoll möjliggör att datorer och andra apparater kan ta emot och skicka mejl med hjälp av en internetadress. Protokollet för att kunna ta emot mejl är Post office protocol (POP) och det finns även en nyare version av den vid namn POP3. Det finns även Interactive Mail Access Protocol (IMAP) som kan hantera mejl på individuella maillådor och som oftast används i jobbsammanhang.

FTP:
File Transport Protocol är ett protokoll som hanterar upp- och nedladdning från internet. Det är ett sätta att kopiera filer trådlöst över internet. FTP är en av de äldsta protokollen som fortfarande används aktivt idag. FTP fanns redan innan konceptet av WWW hade skapats.

IPV4-IPV6

Det finns ett ökande problem med vårt Nuvarande IP-adressystem: IP-adresserna räcker inte till och håller på att ta slut.

IPv4 Skrivs i 32 bit. Detta innebär att det enbart går att åstadkomma max 32 nollor och ettor. Eftersom Ipv4 är skrivet i binärt blir alltså uträkningen för antalet IP adresser 2^{32} vilket blir cirka 4 miljarder unika adresser. Men vi är ju som sagt snart 8 miljarder på vår planet, och den uppkopplade delen av världen kommer snart nå maxantalet för antalet unika adresser eftersom man oftast äger mer än en uppkopplad apparat. Man har försökt stoppa detta genom att bland annat använda sig av NAT (Network Address Translation) där ett lokalt nätverk delar på en IP-adress istället för exempelvis 4 olika. Detta har dock inte slagit igenom så mycket som man hade hoppats och det är här IPv6 kliver in. Om Ipv4 var skrivet i 32 bitar så är IPv6 skrivet i 128 bitar vilket möjliggör för ett nästintill oändligt antal IP-adresser. Övergången mellan dessa IP-adresser är dock svår, men det finns en del förslag på hur man skulle kunna göra det:

- Man kan använda sig av något som kallas "Dual Stack Routers" som använder sig av båda IP versionerna samtidigt, alltså både IPv4 och v6, på en specialkonfigurerad router.
- man kan använda sig av något som kallas "Tunneling" som kan användas för att möjliggöra att man kan kommunicera mellan två olika nätverkstyper med hjälp av olika protokoll
- Man kan även här använda sig av det som kallas NAT. Med hjälp av en NAT-PT (....Protocol Translation) kan man som användare fortfarande ha IPv4 och sen låta NAT-PT översätta adressen till IPv6 genom att ta bort v4 "Header" som finns på paket och ersätta det med en v6 "Header".

Ökad säkerhet

Att öka säkerheten av internet är en frågeställning människor ställer sig var dag och det är så internet utvecklas dagligen. För företag eller andra webbsidor som erbjuider tjänster via internet är det viktigt att försvåra krypteringen och täck upp säkerhetsluckor i sina system. Detta görs redan i stor grad, men det hindrar inte andra människor från att försöka får tag i exempelvis känslig information. Som privatperson kan man se till att uppdatera spel och webbläsare så snabbt en uppdatering kommer ut, då även dessa saker präglas av luckor i systemen som alltid måste täppas igen. Man kan även skydda allt som har med internet att göra genom att exempelvis kryptera känsliga filer eller lösenordsskydda routrar och liknande. Även att utbygga stadgar för hur internet bör bedrivas ökar säkerheten i systemet då alla kan jobba på samma sätt och utveckla produkter som är kompatibla med en standardisering.

Gymnasieskola - SSIS i Kista

För att bygga upp ett nätverk på vår skola måste man först estimera hur många människor som kommer använda detta nätverk. Om vi antar att varje person nästa termin kommer använda nätverket med 2 olika apparater, en skoldator och sin egna mobil, blir det på ett ungefär 400-500 olika uppkopplingar. Detta är alldeles för många för ett klass C nätverk att hantera, och det rör sig nästan om ett gränsfall för 2 klass C nätverk som ungefär skulle nå till strax ovanför 500 individuella uppkopplingar. Då skolan kan nu uppemot 700-800 uppkopplingar om cirka 3 år finns det även en risk för att investera i 3 Klass C nätverk. Dessvärre är det svårt att få fram kostnaden för de olika nätverkskalssern och deras routrar, men jag har en viss aning om att även 3 starka Klass C router kommer kosta en hel del. Dessa trådlösa routrar skulle även kräva en hel del förstärkare för att nå runt i hela skolan och därav skulle kostnaden blir väldigt hög. Men jag vill se att det ändå skulle bara billigare än att köpa ett klass B nätverk.

Slutsats

Internet har alltid varit kompliserat, och har därav krävt centrala stadgar för att effektiversa arbete. Det är därför man finner så många protokoll och liknande som visar på hur viktigt det är att man sätter standard för bland annat nätverkskommiunikation. Om man exempelvis skulle göra en jämförelse med biltrafiken kan man se att utan centrala regler skulle allt bli så mycket krångligare och ineffektivare. Om det inte fanns en regel för vilken sida av vägen man skulle åka eller hur snabbt man fick åka skulle systemet gå ihop. Det är lite samma princip med nätverkskommunikation. Om man inte hade haft centrala stadgar och regler hade man aldrig kunnat effektivisera datahastigheten och vi skulle därav få ett långsammare internet. Sen kan man även se att skyddandet av information har blivit bättre om ett mer central ämne på internet. Man har nu förstått vikten i att skydda information. Det innebär också att risken för att människor skulle vilja få tag i denna information skulle ökar den med.

Metod

Jag har främst sök upp min fakta på min webbläsare, där jag har använt diverse olika källor för att få fram min information. Jag har även tittat på en del videos om exempelvis

TCP/IP för att få det verbalt förklarat för mig då text ibland kan har blivit lite jobbigt att läsa igenom.

Referenser:

Bakgrundshistoria:

- https://www.oxit.se/internets-historia-och-utveckling/

OSI:

- https://sv.wikipedia.org/wiki/OSI-modellen
- https://www.youtube.com/watch?v=HEEnLZV2wGI&t
- https://www.youtube.com/watch?v=0Rb8AkTEASw
- https://www.lifewire.com/layers-of-the-osi-model-illustrated-818017
- http://www.webopedia.com/quick_ref/OSI_Layers.asp
- http://www.learnify.se/learnifyer/ObjectResources/d740e0ac-7ac3-4988-8615-beeaf23f8693/datorkommunikation1_33.html
- http://sv.nous-utile.info/article/vad-ar-natverkslagret
    - **IP**: https://www.fixanatet.se/

TCP/IP

- http://www.electronicdesign.com/what-s-difference-between/what-s-difference-between-osi-seven-layer-network-model-and-tcpip
- https://www.youtube.com/watch?v=PpsEaqJV_A0
- https://sv.wikipedia.org/wiki/TCP/IP
- https://www.cyberciti.biz/faq/key-differences-between-tcp-and-udp-protocols/

Konfigurera Router:

- http://www.dummies.com/computers/computer-networking/networking-components/configure-a-router/

Kryptering:

- http://lifehacker.com/a-beginners-guide-to-encryption-what-it-is-and-how-to-1508196946
- https://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/

Trådlösa Nätverk:

- https://sv.wikipedia.org/wiki/Tr%C3%A5dl%C3%B6st_n%C3%A4tverk

Olika Protokoll:

- http://vlaurie.com/computers2/Articles/protocol.htm
- https://sv.wikipedia.org/wiki/Hypertext_Transfer_Protocol

Ipv4/Ipv6

- https://www.tutorialspoint.com/ipv6/ipv6_ipv4_to_ipv6.htm
- https://www.kjell.com/se/fraga-kjell/hur-funkar-det/natverk/terminologi-och-anslutningar/ipv6-ny-standard-for-ip-adresser
- https://en.wikipedia.org/wiki/IP_tunnel

Ökad säkerhet:

- http://www.mjukvara.se/surfa-sakert

Bilder:

- Sida 1 https://commons.wikimedia.org/wiki/File:Osi-model-jb.svg
- Sida 4 https://commons.wikimedia.org/wiki/File:OSIandTCP.gif
- Sida 5 https://en.wikipedia.org/wiki/Wireless_network#/media/File:Wifi.svg
- Sida 7 https://sv.wikipedia.org/wiki/Fil:Kista_Science_Tower.jpg