Datakommunikation och nätverksteknik - del 1

För en komplett lista av aktuella kommandon, användning och förklaring, se då till `cheat cheat.pdf`.

Vecka 1

Introduktion

Datakommunikation handlar om principerna, så som hur "ettor och nollorna" tar sig mellan datorer. Nätverksteknik handlar om de praktiska delarna - förgreningskablar för ström, switchar och nätverkssladdar för att koppla ihop datorer etc.

Kursen består av fyra delar. Varje del innefattar en bok. Böckerna finns gratis online, givet tillgång.

1. Introduction to networks
2. Routing and switching essentials
3. Scaling networks
4. Connecting networks

Böckerna är uppbyggda av företaget Cisco som har ett helt utbildningskoncept som kursen följer i stort. Detta inkluderar laborationsmaterial etc.

I regel behandlar varje vecka tre kapitel ur aktuell bok. Varje del studeras över fyra veckor. Tyngden i kursen ligger i den första delen.

Föreläsningar läggs ut på läroplatformen. Ej obligatoriska laborationer utförs varje vecka. Laborationerna utförs individuellt och utgår efter skrivna instruktioner. Tillgång till laborationssal är ständig. Via portalen Cisco Academy - NetAcad fås tillgång till kursens innehåll. Vissa tillägg till kursen - utöver innehållet i Ciscos kurser kommer att inkluderas, så som socket-programmering. Kursen innefattar två praktiska tentamen och två teoretiska tentamen. Den praktiska tentamen utgår i laborationssalen under cirka två timmar - det finns då ingen tid att tänka ut strategier, utan det är något som ska "sitta". En frivillig del i kursen resulterar i ett diplom från Cisco. För att få diplomet måste man utföra ett kapiteltest efter varje kapitel ur boken. Testerna måste klaras med 80% godkänt. En slutgiltig examen under en och en halv timme avslutar testerna för att få diplomen. De två praktiska tentamen motsvarar den praktiska delen som måste avklaras för att få diplomet. Efter en kursutvärdering gentemot Cisco kan diplomet mottagas. Programvara som kommer att användas inkluderar PacketTracer (nätverkssimulering) och Wireshark ("sniffar" nätverkskortet).

Kapitel 1 - Introduktion

Introduktion

Globalisering får sin skjuts av nätverk. Arbete och studier förändras i takt med internets utveckling. Vissa jobb har försvunnit, andra tillkommit. Det finns fler kanaler för informationsflöde - bloggar, SMS, chat, wiki, podcaster, sociala medier etc. En demokratisering av samhället har upptstått till följd att alla kan hitta en plattform för att utrycka sina idéer och hitta likasinnade. Samhället är gränslöst - det finns alla möjligheter att kommunicera, jobba eller spela med människor från hela världen utan fördröjning. Underhållning har förändrats - böcker, filmer, musik etc. finns tillgängligt via så kallade streaming-tjänster. Filter-bubblor - sökresultat, mediaflöden etc. anpassas till egna preferenser, ibland utan användarens vetskap. Google, Youtube, Spotify, Netflix etc. är exempel på tjänster som anpassar sig.

Nätverk kommer i många olika storlekar.

- *Home Networks* - kopplar ihop några enheter med varandra och internet
- *Small Office / Home Office (SMOHO)* - kopplar ihop några enheter med fjärrskrivbord över internet etc.
- *Medium to Large Networks* - flera hundra eller tusen sammankopplade enheter över flera platser
- *World Wide Networks (WAN)* - hundratals miljoner sammankopplade enheter - så som internet.

Client-server-modellen

Varje dator som kopplas upp kallas för *host* eller *end device*. En *server* är en dator som delar ut information / funktioner. En *client* är en dator som ständigt skickar förfrågningar (*requests*) till en server.

Peer-to-peer-modellen

Kopplar samman datorer där alla agerar både klient och server. En fil kan ligga utspridd på flera datorer. Det finns ingen centraliserad konfigurering eller åtkomst till funktioner. Om en enhet kopplas från kan information eller funktioner begränsas eller helt försvinna ur nätverket.

Nätverkskomponenter

En *end device* är en enhet från vilken ett meddelande har sitt ursprung eller dit meddelandet ska. Meddelandet flyter (*flows*) genom nätverket. Varje enhet har vanligtvis en *Network Interface Card* (*NIC*) till vilken kopplingen till nätverket sker. Varje *NIC* har vanligtvis en unik address - hårdvaruadressen (*MAC*).

Network media (nätverksmedia) är länkarna mellan enheter. Vanligtvis kopparkablar, fiberoptik eller trådlöst. Man pratar ibland om *Cat 5*- och *Cat 6*-kablar etc.

Topologier (*topology*) är ett sätt att se nätverket på. Antingen en fysisk topologi som visar hur enheter är sammankopplade eller en logisk topologi som är mer fokuserad på nätverksaddresser, ingångar till enheter etc. Båda behövs, men i olika syfte.

Typer av nätverk

Local Area Network (*LAN*) finns över en liten geografisk yta. Hanteras vanlgitvis av en individ eller IT-personal. Vanligtvis mycket hög hastighet inom nätverket.

Wide Area Network (*WAN*) finns över stora geofrafiska ytor och involverar vanligtvis en *Internet Service Provider* (*ISP*). I grund och botten är syftet att koppla samman olika LAN-nätverk. Vanligtvis en långsammare hastighet mellan nätverken.

Metropolitan Area Network (*MAN*), *Wireless Local Area Network* (*WLAN*) är fler exempel på nätverkstyper.

Intranet hanterar den lokala informationen mellan medarbetare.

Extranet kan inkludera kunder, sammarbetspartner och återförsäljare.

Internet är en samling ihopkopplade WAN- och LAN-nätverk (hemnätverk, sjukhusnätverk, skolnätverk, företagsnätverk etc.). Internet ägs inte av en individ eller en grupp, men följande grupper har utvecklats för att upprätthålla dess struktur (DNS-servrar, domännamn, IP-adresser): IETF, ICANN och IAB. Det finns flera sätt att koppla upp sig på internet - kabelanslutning, (A)DSL, mobila tjänster, satelliter o.s.v. När det kommer till företag finns det mer säregna anslutningstyper så som dedikerade kopparkablar eller fiberkaplar mellan exempelvis huvudkontor och dotterbolag.

Konvergerade nätverk

Förr i tiden var nätverk seperarade, telefonnätverk, datornätverk, *broadcastnätverk (ex. TV, radio)* etc. var ej sammankopplade. Nu för tiden konvergerar alla nätverk ihop. Nätverk tenderar att kopplas samman över samma IP-baserade nätverk. Detta är gynnsamt då en och samma enhet tagit över roller som tidigare hölls av flertalet enheter. En mobiltelefon kan nu hantera det som tidigare en telefon, dator, radio och TV skötte.

Tillförlitliga nätverk

Hos ett pålitligt nätverk söker man:

- *Quality of Service (QoS)* - möjlighet att styra vilka trafikflöden som ska prioriteras. Exempelvis kan VoIP prioriteras över nedladdning av webbsidor. Prioritera realtidsapplikationer.
- *Scalability* - förbered för nya anslutningar. Det går snabbt att utöka support till nya användare och applikationer utan att negativt påverka prestanda för nuvarande användare.
- *Fault Tolerance* - redundanta anslutningar (multipla vägar), ej möjligt med kretskopplade nätverk (när en linje sammankopplar två punkter, så som telefonsamtal förr i tiden).
- *Security* - många olika delar. Infrastruktursäkerhet (fysisk säkerhet) - lås in routrar, larma. Informationssäkerhet - *end to end*, kryptering (ex. HTTPS). Tre mål med nätverkssäkerhet: *confidentiality* - enbart den tänkta mottagaren kan läsa data, *integrity* - datan ändras inte över nätverket, *availability* - pålitlig *access* för autentiserade användare.

Nätverkstrender

Nätverkets roll måste hela tiden justeras för att möta förfrågan och de nya enheter som hela tiden släpps. Andra termer som används: *Bring Your Own Device (BYOD)* - ta med egna enheter till företaget där man jobbar etc., *Online collaboration* - samarbete mellan individer över nätverk, *Video communications* - konferenser, möten, utbildningar, *Cloud computing* - spara filer / backup på servrar, editera bilder / filmer online. Småföretag gynnas av cloud computing - de slipper

dyra datacenter, servrar, lagringsmedia etc.

Teknologier kring smarta hem är en växande trend. Lampor kan tändas vid ankomst, dörrar kan låsas när hemmet lämnas. Bilen kan vara uppkopplad. Vanligtvis är dessa enheter kopplade till olika *molntjänster* där exempelvis biltillverkaren har en server som sköter bilen.

Nätverk via elnätet är ett alternativ till trådlösa nätverk. Det trådlösa nätverket är enklare att avlyssna.

Wireless Broadband - alternativa master till mobiltelefoninätverket så att hem kan kopplas trådlöst till internet utan att koppla på mobiltelefoninätverket.

Säkerhetshot

Externa hot:

- Virus, maskar (*worms*), trojanska hästar
- *Spyware*, *adware*,
- *Zero-day attacks*
- *Denial of Service (DoS) attacks*

Interna hot:

- BYOD-strategier gör företaget mer sårbart
- Studier visar att interna hot är vanligare än externa hot

Säkerhetslösningar

Nätverkssäkerhet måste lösas i flera olika lager. I hemnätverket är anti-virus och brandväggar vanliga lösningar. I företag finns det *Access Control List (ACL)*, *Intrusion Prevention Systems (IPS)*, *Virtual Private Network (VPN)*, dedikerade brandväggar etc.

Kapitel 2 - Cisco IOS

Ett praktiskt kapitel.

Operativssystem

Alla elektroniska enheter har ett operativssystem. Windows, macOS och Linuxvarianter för PC, iOS, Android för mobila enheter, Cisco IOS för nätverkskomponenter.

Denna kurs fokuserar på användning av Cisco IOS 15.x. Accessmetoder inkluderar en *console port*, -Secure *Shell (SSH)* (rekommenderat) och *Telnet*.

IOS navigation och kommandon

Den här delen förklaras bäst genom en översiktlig läsning av kursens powerpoint - del 1, kapitel 2, Navigate the IOS och vidare.

Se *cheat sheet* för en översikt över vanliga kommandon och kortkommandon.

OBS: under laboration används lösenordet `cisco` eller `class`!

Kapitel 3 - Nätverksprotokoll

All kommunikatiion har tre element som är lika:

- En källa eller avsändareen
- mottagare
- en kanal eller ett media.

Man måste komma fram till regler för att kunna kommunicera.

Regler för kommunikation

Hur kodar man meddelandet? Hur formaterar man paketet? Finns det någon speciell timing som man måste använda när meddelandet skickas?

Tänk bara på mänskliga språk.

Kodningen måste vara anpassad för det medium som meddelandet ska föras över på. I nätverk är meddelanden vanligtvis omkodade till bitar. Bitarna omkodas sedan till exempelvis ljud, ljus eller elektriska impulser - beroende på det medium som ska användas vid överförning. Mottagaren tar mot signalerna och kan tolka meddelandet.

Man behöver även formatera / paketera meddelandet. Tänk exempelvis på brev - vi behöver kapsla in meddelandet och addressera det i ett specifikt format. I nätverkssammanhang kallas detta för *frame*. I en frame finns addresser (fysisk / logisk) och ett inkapslat meddelande enligt ett strikt format. Dessa *frames* kodas till binär form och skickas över nätverket. Vanligtvis sköts detta automatiskt av operativssystemet.

Meddelandet bryts ner till mindre delar, precis som vi människor skriver - kapitel, sidor etc. Mottagaren rekonstruerar de flera paketen som mottas till det ursprungliga meddelandet.

Beroende på medium kan kollisioner uppstå. Detta löses ofta med *message timing*. Det finns flera olika timing-strategier, exempelvis kan man göra upprepade försök om nätverket är upptaget - med slumpmässiga väntetider.

Flow control används för att komma fram till en korrekt timing för att undvika att mottagaren blir överväldigad av information.

Det finns flera olika sätt att välja mottagare till meddelande:

- *unicast* - en till en (peer-to-peer)
- *multicast* - en till flera
- *broadcast* - en till alla (exempelvis för att fråga nätverket var en mottagare finns)

De viktiga reglerna för kommunikation:

- Använd ett gemensamt språk
- Vänta på din tur
- Signalera när du är klar

Nätverksprotokoll och standarder

Den här kursen fokuserar på protokollen *TCP (transmission control protocol)* och *IP (internet protocol)*. Ett annat vanligt protokoll är exempelvis *HTTP (hyper text transfer protocol)*. IP har två huvudsakliga versioner - *IPv4* och *IPv6*. Det finns ungefär fyra miljarder IP-addresser i IPv4. Dessa tog slut för flera år sedan, vilket leder oss till IPv6. Med IPv6 kan man mer eller mindre

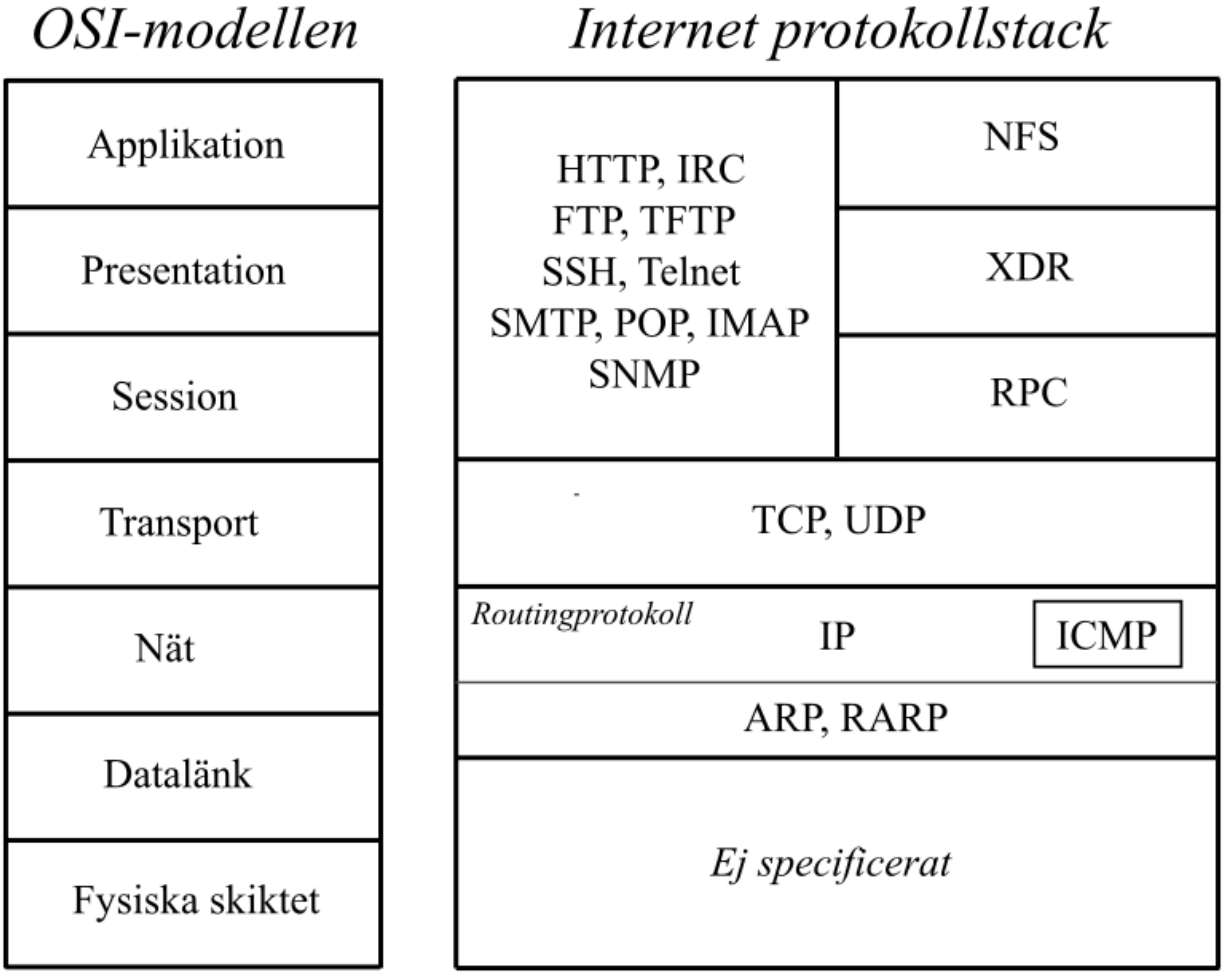
ansätta en address till varje gruskorn på jordens yta.

Det finns flera bilder och diagram som kan vara bra att skåda i tillhörande slide (*Protocols - Protocol Interaction* och vidare).

En *protocol suite* (stack) är en samling protokol som jobbar tillsammans för att kunna komunicera på nätet. Den vanligaste stacken är antagligen *TCP/IP*.

Ett exempel på lagerstrukturen av nätverk finns i tillhörande PowerPoint (*Organization of air travel*).

Internet protocol stack (ISO/OSI - modellen):



Vecka 2

Kapitel 4 - Nätverksaccess

Det fysiska lagret

Innan nätverk kan kommunicera måste en fysisk koppling sättas upp. Det kan röra sig om en sladd eller en trådlös koppling över radiovågor. En vanlig hemmarouter har vanligtvis både en switch man kan koppla LAN-kablar till och en *Wireless Access Point* (WAP) man kan ansluta trådlöst till.

Nätverksinterfacet (*Network Interface Card* alt. *NIC*) ansluter enheten till nätverket. Det kan som tidigare röra sig om antingen en trådbunden koppling eller en trådlös anslutning.

I en elektrisk (koppar-) signal ser man vanligtvis skillnaden på en etta och nolla beroende på strömstyrkan. I fiberoptik är det ljuspulser som tolkas. För trådlösa kopplingar rör det sig ofta om analoga signaler (så som FM, AM etc.). En vanlig funktion är sinus-funktionen, $Asin(\omega t + \Phi)$. Denna funktion går att *modulera* / påverka. På så vis går det att koda data till en naturlig funktion som lämpar sig för radiosänding. Man pratar ofta om amplitudmodulering och frekvensmodulering. I fallet amplitudmodulering ökar eller sänker man styrkan på signalen för att koda information, dock klarar sig inte signalen särskilt långt då styrkan sänks naturligt över längre avstånd. Frekvensmodulering ändrar frekvensen mellan två värden och håller kvar samma amplitud. Detta ger en bättre kvalité i exempelvis radio. Ett tredje sätt att koda in data i sinusfunktionen är *Phase Modulation* (PM), då justeras fasen i funktionen. Man sänder då två perioder av sinus, den ena i fas och den andra i fas 180. När den byter fas är det en logisk 1 och när fasen kvarhålls är det en logisk 0. Fasmodulering sägs vara mer kortvågig än andra modulationer. Fasmodulering kan även använda sig av fler än två olika faslägen, exempelvis 0, 90, 180, 270 och 360. På så vis kan man skicka två bitar samtidigt. Det går utöka detta till åtta olika lägen för att koda tre bitar samtidigt etc.

Dessa tre medium (elektroniska signaler, ljussignaler och radiosignaler) är de tre grundläggande medium för nätverkskommunikation.

Det fysiska lagret berör även termen *bandbredd*. Denna term benämner hur många bitar som skickas per sekund, ofta teoretisk hastighet. Vanligtvis används förkortningar så som Mb/s, Gb/s etc. Termen *throughput* är snarare den faktiska, möjliga hastigheten på nätverket. Termen *goodput* är throughput minus trafikens *overhead* för att skapa sessioner etc.

När det kommer till elektriska kablar så finns det flera saker som negativt kan påverka prestanda, så som *cross talk* (att kablarnas signaler sprids till andra kablar), elektromagnetiska störningar etc. För att motverka vissa av dessa negativa drag så tvinnas kablarna och ibland så skyddas dem av ett lager folie. Detta bidrar till att en högre hastighet kan uppnås. Den vanligaste kablen i nätverk är *RJ-45*. För analoga signaler används vanligtvis *coaxial*-kabel. Man använder den ofta till antenner av olika slag. Den traditionella klassifieringen av kablar är *Category 3,4,5,5e,6...* (*CAT*). Desto högre klassifiering desto högre bandbredd. Cat 5 ≈ 100-1000Mb/s, Cat 7 ≈ 1-10Gb/s. Raka kablar kopplar nätverk till en switch eller hub. Tvinnade kablar kopplar samman två nätverk, switch till switch eller router till router. Det finns verktyg för att testa om en kabel är tvinnad eller rak.

Fiberkablar är immun mot elektromagnetiska störningar, kan skicka data över längre distanser, är flexibel och har flera andra positiva karakteristiska drag. Den är däremot dyrare än traditionella kablar. Fiberkablar skickar pulser av ljus för att överföra data. *Single mode* skickar en signal rakt genom kabeln flera tusen meter. *Multimode* använder totalreflektion för att skicka flera signaler samtidigt, ökar bandbredden men sänker möjliga överförningsdistansen (några hundra meter). Det finns verktyg för att testa dessa kablars funktion (reflektometer). Fiber stöder 10Mb/s - 100Gb/s.

Trådlös media har blivit mycket populärt de senaste 10-20 åren. Nackdelar är täckningsområden, störningsrisk, säkerhet och det faktum att det är ett delat medium. Det finns flera olika standarded för trådlös överförning - Wi-Fi, Bluetooth etc. Wi-Fi jobbar likt ethernet på så vis att det väntar med att skicka data till nätverket är klart. Bluetooth är av typen *Wireless Personal Area Network* (WPAN). Distanser mellan 1-100m. *Wireless LAN* (WLAN) kopplar samman trådlösa enheter i ett nätverk. För detta nätverk står en WAP.

Media Access Control går att likna vid reglerna hur man tar sig med bil ut till motorvägen. Man måste ta hänsyn till andra på vägen. Man kan använda kugghjulsprincipen, man kan vänta på sin tur vid en stoppsignal, krockar man backar man och gör om igen efter en stund.

Topologier

Fysisk topologi är den fysiska strukturen så som att det i ett visst serverrum finns en rack där det i hylla 2 står en switch.

Logisk topologi är snarare hur enheter kopplas samman ur ett nätverksperspektiv, ip-adresser och nätmaskar är vanligt förekommande i en sådan topologi.

I IPv4 finns det tre nätmaskar som är tillägnade privata nätverk: *192.168.x.x*, *10.x.x.x* och *172.[16-31].x.x*.

Det finns även olika typer av underkategorier för topologier. *Point-to-point*-topologier visar hur två *end-nodes* sammankopplas antingen fysiskt eller logiskt. *Star*, *Extended Star*, *Bus* och *Ring* är andra vanligt förekommande topologier där Star och Extended Star är vanligt förekommande för nätverk, då vanligtvis med en switch/router i mitten.

Andra begrepp som är centrala i sammanhanget är *half duplex* och *full duplex*. Half duplex innebär att man kan skicka och ta emot data, men inte samtidigt. Full duplex klarar av att både skicka och ta emot data samtidigt.

Frame

En *frame* består av en *Header*, *Packet (data)* och *Trailer*. Headern består av *Frame Start*, *Addressing*, *Type* och *Control*. Trailern består av *Error Detection* och *Frame Stop*.

Frame start består av en byte som indikerar början på en frame och indikerar timingen och slutet för resten av paketet. Addressing tar hand om källa och destination av paketet. Type bestämmer lager 3-protokollet för data-fältet. Control stöder *control services* så som QoS. Data-delen innehåller *frame payload*:en (*packet header*, *segment header* och data).

Se bild i presentation *Data Link Frame - Layer 2 Addressing*.

Kapitel 5 - Ethernet

Ethernet är den mest använda LAN-tekniken idag. Stöder i praktiken mellan 10 Mb/s till 100 Gb/s. Ethernet arbetar i data-länk-lagret och det fysiska lagret. Ethernet förlitar sig på *Logical Link Control* (LLC) och *Media Access Control* (MAC) sublagren.

MAC-sublagret tar hand om att kapsla in datan. Kapsuleringen bygger upp framen gällande adressering och feldetektering.

Den minsta framen är 64 byte och maximum är 1518 bytes. Frames som är mindre än 64 bytes kastas alltid. De kallas *collision fragment* eller *runt frame*. Frames som är större än maximum kallas *jumbo* eller *baby giant frames*. Även denna typ av frame kastas (*drop frame*).

MAC-adressen är ett 48-bitars binärt tal som vanligtvis uttrycks med 12 hexadecimala siffror (4 bitar per hexadecimalt tal). Adressen skapades för att identifierar den faktiska källan och destinationen. De 24 första bitarna tilldelas företagen som skapar NICs så att skaparen kan identifieras. De sista 24 bitarna är upp till tillverkaren att bestäma så att värdet förblir unikt.

MAC-adressen kodas vanligtvis in i ett *Read Only Memory* (ROM) på enheten. De refereras vanligtvis till som *Burnt In Address* (BIA). Vid utskrift brukar de hexadecimala talen separeras med bindestreck eller kolon. Det finns olika slag av MAC-adresser så som *Unicast MAC Address* som används för att skicka ett meddelande till en enhet på nätverket (en-till-ett). Det finns även *Broadcast MAC Address* som används för att skicka ut till alla enheter på nätverket (så som DHCP, Avahi / Bonjour). Broadcast-adressen är *FF:FF:FF:FF:FF:FF* (48 binära ettor). *Multicast MAC-address* används för att skicka till flera enheter samtidigt. Då måste MAC-adressen börja med *01:00:5E* och IP-adressen måste vara i vidden *224.0.0.0-239.255.255.255* i IPv4. I IPv6 börjar adresserna på *FF00::/8*. IP-räckvidden / multicast-gruppen definieras av switchen.

Switchen

En *Layer 2 Ethernet switch* gör sina beslut enbart baserat på MAC-adresserna i lager 2. En nystartad switch har en tom så kallad *MAC address table* (*CAM table*) då den ännu inte har lärt sig vilken port som använder vilken MAC-adress. Switchen bygger upp tabellen dynamiskt. Switchen kollar på alla inkommande paket och tittar på:

- En ny MAC-adress sparas med tillhörande port
- En tidigare känd MAC-adress som skickas från eller till får ett nytt värde i *refresh timern* (se nedan)

Vanligtvis så håller switchen värden tabellen i 5 minuter innan det släpps (om inte en frame med adressen kommit in).

Finns inte destination-adressen i tabellen skickas framen ut till alla portar. När en enhet tar mot ett meddelande kontrollas framens destination-adress gentemot den egna MAC-adressen, om de matchar tas frame mot. En port kan tilldelas flera MAC-adresser. Exempelvis kan en switch A kopplas till en annan switch B. Alla enheter som kopplas till switch A är för switch B på samma port som switch A.

Det finns flera olika sätt på vilka frames skickas vidare till andra Cisco switchar (*Store-and-forward* och *cut-through*).

Switchen "pratar inte" IP (Lager 3 etc.). Om den behöver skicka till en viss IP måste den fråga nätverket via en *ARP-request* vilken MAC-adress som hör ihop med en viss IP-adress. Datorer håller en ARP-tabell över vilka IP-adresser som har vilka MAC-adresser. Tabellen hålls vanligtvis i två minuter. Ska en request till ett annat nätverk (ett annat *subnet*) så skickas den till *default gateway* (vanligtvis routern) istället.

Kapitel 6 - Nätverkslagret

Nätverkslagret sköter transport av data från nätverk till nätverk. Applikationslagret är snarare transport från process till process. De huvudsakliga protokollen som sköter detta är IPv4 och IPv6.

För att skicka datan måste IPn kapsuleras in. Dessa paket kallas vanligtvis *datagram* eller *IP-paket*. IP-headern förblir densamma från *source* till *destination*. IP designades som ett protokoll med *low overhead* som enbart tjänar syftet att ge de funktioner som krävs för att skicka ett paket från en källa till en mottagare. IP har ett läge som kallas *connectionless* då den inte bryr sig om om mottagaren kan läsa meddelandet, om det kommer fram etc. IP betraktas på det viset opålitligt, det kan inte garantera frakomst. Vi litar helt enkelt på att det går så bra som möjligt,

men routrarna får mindre att göra och kan lägga arbetet på att skicka vidare till bästa länk. I IPv6 har detta "renodlats" ännu mer, så att headern ska vara så lätt som möjligt att hantera. De överstående få raderna brukar sammanfattas med termen *best effort*. IPv4 *packet headern* består av 20 bytes. Exempelvis talar den om vilken version på protokollet som används, vilka prioritetsmöjligheter som finns, *Time-to-Live* (TTL) som berättar hur många steg paketet kan ta (hur många routrar som den passerar innan den försvinner), *protocol* som berättar vilket övre protokoll (ex. TCP) som använts, *header checksum* som kontrollerar att headern ej ändrats etc. IPv4 saknar *end-to-end connectivity* då man måste använda *Network Address Translation* (NAT) som kan dela ut en IP-adress på flera enheter (lokalt). Denna funktion sitter i routern. I IPv6 har man bytt ut 32-bitars-adressrymden från IPv4 till 128-bitars. Detta innebär 10^36 adresser. På varje kvadratmeter på jordens yta kan man alltså lägga ungefär 100 000 000 000 000 adresser. Lätt sagt finns det ungefär en IP-adress ber gruskorn på jorden. IPv6 har färre fält i headern och nödvändigheten av NAT är borttagen då alla enheter kan få en egen adress. Time to live har döpts om till *Hop Limit*. Checksumman har tagits bort. Mer om hur headern ser ut för IPv4 och IPv6 finns att se i presentationen - *IPv6 Packet - Encapsulating IPv6* och vidare.

Den viktigaste funktionen för nätverkslagret är att skicka paket mellan hosts. Man kan skicka paket till sig själv (*loopback interface*). *Local host* är en host på samma nätverk och *remote host* är en host på ett annat nätverk. För att veta vilka hosts som finns var eller för att hitta en väg ut upprättas en *host table*.

Vecka 3

Kapitel 7 - IP-adressering

IPv4 har 32 bitar som är representerade i 4 fält om 8 bitar.

Kapitel 8 - Subnetting

Den första möjliga adressen är "host-biten" och den sista är broadcast-adressen

Vecka 4

Kapitel 9 - Transportlagret

TCP har kontroll så att paketet verkligen kommer fram. Men mycket overhead - om paketet inte kommer fram så skickas det om etc. Diplomatisk - frågar nätverket och mottagaren om hur mycket som kan skickas / tas emot etc. Mäter *roundtrip*-tiden (från att ett meddelandet skickas till att mottagaren berättar att det är mottaget). Om det är snabbt kanske fler paket kan skickas samtidigt. Om ett paket däremot skickas och inte tas emot går sändningstakten vanligtvis ner till hälften.

..
....
.....
.....
FEL
....

TCP underlättar för applikationer då de inte behöver hantera stabiliteten i nätverket. HTTP, FTP, SMTP, Telnet, TCP etc.

UDP har få av egenskaperna som nämns ovan. Frågar inte om mottagaren finns (upprättar ingen kontakt). Ingen sekvenshantering etc. Man måste själv hantera att sortera paketen - utrymme för att de kommer fram i rätt tid. Användbart för streaming. Man har då en liten buffert så man hinner sortera datan innan den visas eller begära återsändning av paket. Litet och snabbt helt enkelt. Används för DHCP, RADIUS, VoIP, DNS etc. Enkla innehåll som rymms i ett paket.

Kapitel 10 - Applikationslagret

Applikationslagret består mer eller mindre av det vi stöter på i vardagligt bruk - webbservrar (HTTP, HTTPS) etc.

Sessions-hantering så som cookies, historik etc. Det finns en koppling till webbservern även när den direkta anslutningen är avslutad.

Applikationer använder ofta en av följande modeller:

- client-server (en klient ansluts till en server)
- peer-to-peer (varje enhet agerar både klient och server)

Kapitel 11 - Att bygga ett litet nätverk

Många små nätverk består av en enda router med en eller fler switchar. Vanligtvis har routern en enda WAN-anslutning via fiber eller ethernet. Att hantera nätverket involvera felsökning och att säkra nätverket.

Man behöver tänka på kostnaden, krav på hastighet och tillgänglighet, vilka operativsystem-egenskaper som bör inkluderas. En planering av IP-adresserna bör göras, vilka hostar som ska kunna kommas åt via internet eller döljas bakom NAT etc (fysisk och logisk topologi). Exempelvis kan servrar alltid läggas på 192.168.1.[50-100] så att det är enkelt i loggar att se vilken trafik som är till servrar. Man bör överväga felsäkerhet via exempelvis redundanta servrar, switchar etc. Dubbla NICs i servrarna kan användas etc. Termer så som lastbalansering kan även övervägas.

Trafikhantering berör QoS, så som att VoIP kan prioriteras över FTP.

Vanliga applikationer som är tänkta att användas kan studeras för att se hur nätverket kommer belastas.

Ett litet nätverk kan växa. Man bör dokumentera vilka IP-adresser som används, vilka enheter och vilken budget man har, trafikanalyser. Följ upp nätverket och var förutseende för när nätverket ska utökas. Man kan använda protokollanalys via Wireshark för att se vad som händer i nätverket. Man tittar på nätverksmönster - när inträffar viss typ av trafik.

De vanliga områden för nätverkssäkerhet bör tänkas över; informationssäkerhet, tillgänglighet av data och tjänster. Fysisk säkerhet så som hårdvaruhot, miljömässiga hot, elektriska hot och underhållning.

Man bör ha sparat ett *network baseline* där man samlar på sig grunddata för att ha koll på hur det vanligtvis ser ut på nätverket. På så vis kan man se förändringar på nätverket om något hänt.