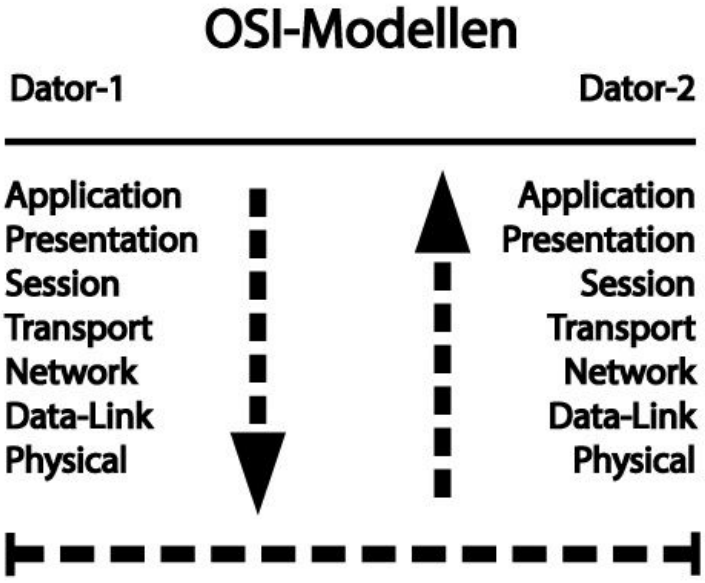
William Beinö
TE16B
Stockholm Science & Innovation School
2017-05-19

Nätverk - Essä

OSI-modellen:

OSI-modellen är en konceptuell modell av hur nätverk ska vara uppbyggda och eller hur de ska fungera. OSI står för Open Systems Interconnections vilket översätts till systemens-sammanlänkningar, OSI-modellen är en modell av precis detta, hur hostar sammankopplas och kommunicerar med varandra. I dagens samhälle är OSI-modellen en standard och därför välkänd i hela världen när det kommer till uppbyggnad och felsökning av nätverk. OSI-modellen bygger på sju lager: Physical layer, Data link layer, Network layer, Transport layer, Session layer, Presentation layer och Application layer. Dessa lager används konceptuellt hela tiden när datorn skickar och tar emot data, med andra ord när datorn och andra värdar byter information.



Physical layer:

Det fysiska lagret är det lager som transporterar datan genom fysiska kablar eller trådlöst genom radiovågor, datan skickas i en ström av ettor och nollor och är ofta representerade i volt där tex fem volt kan representerar en etta. Transportmediat alltså om datan transporteras trådlöst eller trådat kan också räknas till lager noll, detta lager har inget namn men håller koll på ifall enheten kör på ethernet eller wifi. Maskiner som fungerar på det fysiska lagret är hubbar som inte håller koll eller sparar någon typ av data utan skickar bara vidare informationen till alla tillgängliga enheter.

William Beinö
TE16B
Stockholm Science & Innovation School
2017-05-19

Data link layer:
Data link lagret ser till att en anslutning mellan enheter på det fysiska lagret är funktionalitet samtidigt som detta lager ser till att bara en enhet skickar information i taget. Data link layer använder protokoll som MAC(Media Access Control) för att veta vart information kommer ifrån eller till vilken enhet informationen ska till. Maskiner som använder MAC adresser är maskiner som fungerar på lager två eller högre alltså switchar och routrar. Data link layer använder också LLC(Logical Link Control) som en felrättning ifall enheterna t.ex. skulle skicka information samtidigt eller ifall informationen skulle vara skadad på olika sätt.

Protokoll:
MAC(Media Access Control): Mac adressen är en unik adress som bara finns på din dator, den fungerar som din dators fingeravtryck. Ingen annan dator har exakt samma adress som den, och därför kan adressen sparas på routrar och switchar för minska på bandbredden. Till skillnad från switcharna och routrarna som sparar mac adressen skickar hubbarna paketerna till alla enheter varje gång den får något.

LLC(Logical Link Control): LLC är ett protokoll som används av routrar och switchar när de skickar packets genom ethernet kabeln. Tex kan LLC se till att bara en enhet pratar över ethernet kabeln i taget, eller ifall kabeln stödjer multi channels kan LLC tillåta synkroniserade överföringar. Dessutom ifall det blir något fel under processen kan LLC säga till sendern att skicka paketen igen, eftersom datan kan vara skadad. Med andra ord fungerar LLC som en felrättning till enheter.

Network layer:
Nätverkslagret är precis som det låter, lagret som kopplar samman alla enheter med varandra samt internet med hjälp av IP(Internet Protocol). Maskiner som fungerar på nätverkslagret är routrar som introducerar och håller koll på ip adresser. Med hjälp av ip adresser kan datan veta destinationen samt källan som den ursprungligen skapats ifrån, detta för att datan ska kunna transporteras till destinationen och sedan kunna ta samma väg tillbaka. Ip är en standard för internet kommunikation och att inte ha ip adresser är som att ha bilar utan vägar att köra på. Med andra ord skulle inte det finnas någon destination för datorns packets utan ip adresser.

Transport layer:
Transportlagret är lagret som ser till att datan når sin destination, detta åstadkommer lagret med hjälp av TCP(Transmission Control Protocol) och UDP(User Datagram Protocol), två protokoll med samma huvudsyfte men helt olika funktioner. TCP och UDP är standarder för att skicka packets mellan datorer, alltså ett sätt att formatera datan för att alla enheter ska kunna förstå varandra. TCP är en ingående konversation mellan enheter som ser till att all data når fram till destinationen, dock använder detta extra bandbredd och tar längre tid. UDP är ett protokoll som inte bryr sig på samma sätt ifall datan kommer fram utan fortsätter bara skicka ny data hela tiden.

William Beinö
TE16B
Stockholm Science & Innovation School
2017-05-19

Session layer:
Sessions lagret är som håller koll på statusen av anslutningen, alltså ser lagret till att en anslutning skapas, underhålls och eller stängs på respektive enhet. Sessions lagret spelar därför en viktig roll på alla enheter, ifall ett fel uppstår i sessionslagret kan enheten fortsätta skicka packets till en host som är avstängd eller av andra skäl onåbar. Ifall det blir något fel i transportlagret brukar detta oftast avspegla sig i sessionslagret genom att anslutningen inte uppehålls, troligen avslutas den abrupt med någon typ av felmeddelande.

Presentation layer:
Presentationslagret är lagret som tar datan till eller från programmet, och däremellan ser lagret till att justera datan till det angivna formatet. Tex ifall din webbläsare gör en SQL-Request där den frågar om lösenordet stämmer med serverns databas, ska lösenordet självklart inte skickas utan kryptering, krypteringen sker därför i detta lagret. Med andra ord presenterar presentationslagret datan för applikationslagret som förståelig och proper formaterad data, ofta formaterad efter det angivna protokollet tex i form av en HTTP-Request.

Application layer:
Applikationslagret tillhör det tre övre lagrarna, detta lager är i direkt kontakt med programmet och använder sig därför av protokoll som DNS, FTP, HTTP, SSH, TELNET, SSL m.m. Dessa protokoll fungerar som ett eget språk mellan programmen och är därför den typen av data som ska transporteras till de andra hostarna. Applikationslagret har alltså som huvuduppgift är att generera data som presentationslagret kan formatera vidare. Ett exempel på applikationslagret i arbete, är när webbläsaren genererar en HTTP-Request till webbservern som ofta frågar servern om HTML formatet på den angivna adressen.

TCP-modellen:
TCP-modellen precis som OSI-modellen är en konceptuell modell av hur nätverk ska vara uppbyggda samt fungera. TCP-modellen är också väldigt lik OSI-modellen dock finns några få justeringar. TCP-modellen har till exempel slagit ihop den tre övre lagren, till ett stort så kallat Application layer samt slagit ihop de två första lagren till ett Network Interface layer. Alltså består TCP-modellen bara av fyra lager, dessa lager har samma funktioner men beskrivs på ett annorlunda sätt. När man beskriver nätverk med hjälp av TCP-modellen går man sällan lika ingående i enheter som Switchar, Hubbar och Routrar eftersom dessa enheter sammanfattas i ett och samma Physical layer.

DNS(Domain Name Server):
DNS servrar finns idag för att göra om simpla urlar till ip adresser som webbläsaren kan läsa och förstå, tex när vi skriver in www.google.com i sökfältet skickar webbläsaren iväg en fråga till DNS servern om ip adressen till hemsidan, efter att DNS servern svarat kan webbläsaren skicka iväg en HTTP-Request till webbservern.

William Beinö
TE16B
Stockholm Science & Innovation School
2017-05-19

FTP(File Transfer Protocol):
FTP är en okrypterad connection mellan FTP servern och en FTP client, FTP används för att föra över filer mellan enheter och nätverk. Tex kan man ha en FTP server på ett webbhotell för att tillåta användaren av webbhotellet att ladda upp ny version av sin hemsida på webbhotellet. SFTP(SSH File Transfer Protocol) kom några år senare och är precis samma sak som FTP dock krypterad och skriven över en ssh connection. FTP använder port 21 och SFTP port 22, portarna är olika för att nätverket ska veta vilket typ av protokoll som används.

Skolans nätverk:
På SSIS en skola med ca 200 elever måste man se till att alla enheter får internet, vi säger att alla elever har en skoldator samt mobil. Det resulterar i 400 enheter, vilket betyder att CIDR/23 bör räcka, alltså subnet-masken 255.255.254.0 som klarar av 2^9-2=510 enheter. Eftersom denna subnet-mask är klass B så skulle skolan kunna få subnet-idn 172.60.0.0 vilket skulle ge broadcast-adressen 172.60.1.255. Alla elevernas enheter skulle därför få lokala adresser mallen subnet-idn och broadcast-adressen. På en skola som SSIS bör åtta accesspunkter räcka, dessa kopplas samman med routern med ethernet kablar. Ifall det bara finns en våning eller en del av skolan som idag, bör detta räcka för en stabil trådlös internet anslutning. Men eftersom SSIS ska fördubblas i storlek och antal elever skulle subnet-masken behöva ändras samt vore det bra att installera två switchar mellan routern och accesspunkterna eftersom dessa switchar kopplas med routern och alla accesspunkter till sin dels switch. På grund av den dubbelt så stora ytan som ska täckas trådlöst bör dubbelt så många accesspunkter köpas. Efter konfigurering på alla switchar och accesspunkter ska det trådlösa internetet fungera felfritt i båda delarna av skolan.

Internet protokollet:
Internet protokollet är idag det viktigaste protokollet inom nätverk, eftersom det ser till att alla enheter har en egen/unik adress, något som inte längre går att underhålla. Problemet uppstår när man pratar om ip versioner, i ipv4 som är uppbyggt på 32-bitar finns det möjlighet för ~4 228 250 625 unika uppsättningar av adresser. Detta är på tok för lite med tanke på att vi är drygt ~7 miljarder människor på jorden och det flesta använder fler än en enhet. Lösningen till detta är ipv6 som bygger på 128-bitar och kan därför generera 2^128 unika uppsättningar av adresser. Genom att byta till ipv6 skulle man höja säkerheten både för privat ägare samt företag eftersom ipv6 tillåter tillräckligt många ip adresser för att alla enheter på internet ska kunna ha en peer-to-peer connection med varandra, vilket ger möjligheten för enheter att kunna kommunicera krypterat utan någon möjlighet för avlyssning. Enligt en undersökning av RIPE[1] fanns det den 16:e maj 2017 12.98 miljoner ip adresser kvar för ipv4. När routern tilldelar en enhet sin ipv4 adress sker detta genom ett protokoll som heter DHCP(Dynamic Host Configuration Protocol), protokollet fungerar som

[1] https://www.ripe.net/publications/ipv6-info-centre/about-ipv6/ipv4-exhaustion/ipv4-available-pool-graph

en brygga mellan enheten och routern och ser till att enheten blir konfigurerad med en ip, subnet-mask, m.m. Routern tilldelar en ip som matchar subnet-masken och ger därför en ip emellan subnet-idn och broadcast-adressen. Subnet-idn får den absolut lägsta ip adressen och är oftast på okonfigurarade routrar 192.168.0.0 precis under routerns host ip 192.168.0.1. Observera att dessa ip adresser använder 255.255.255.0 som subnet mer känd som klass C eller i CIDR(Classless Inter-Domain Routing) som /24. Broadcast adressen används när en enhet eller routern vill få kontakt med alla enheter på nätverket, broadcast skickar därför paketet till alla enheter.

Exempel:
Ifall ett företag med 3000 användare skulle behöva tilldelas ip adresser skulle man behöva en subnet mask som tillåter minst 3000 enheter. Det lättaste vore då att ändra nätverkets subnet mask till 255.255.0.0 vilket skulle tillåta 2^16 enheter, detta skulle ge subnet-idn 172.17.0.0 och broadcast-adressen 172.17.255.255. Så för nätverksteknikern ska han konfigurera routern på ip adressen 172.17.0.1. Ifall man skulle vilja sänka antalet enheter från 64K till 4K ska man ändra subnet-masken till 255.255.240.0/20 vilket skulle ge 2^12=4K hostadresser.

Konfigurera router:
Att konfigurera routern har aldrig varit lättare, de flesta routrar idag använder ett webbinterface för att konfigureras. Eftersom routern fungerar som mamman för nätverket brukar den placera sig på första lokala ip adressen(192.168.0.1). Så efter att routern har fått ström kan man ansluta med en enhet som en dator eller mobil. Webbinterfacet är oftast inte responsivt, så det brukar vara lättare att ansluta med en dator. När man har anslutit till routern kan man göra en HTTP-request till routerns ip, detta gör din webbläsare när du skriver in 192.168.0.1 i sökfältet. Efter att man kommit in på hemsidan finns oftast någon typ av wizard/snabb installation denna måste slutföras för att få igång internetet. Om man har erfarenhet med nätverk och en tydlig förståelse av ip adressen kan man konfigurera routern under en mer avancerad inställning. Denna undergrupp tillåter användaren att ändra subnätmasken samt default gateway.

På det flesta routrar är det också möjligt att reservera ip adresser till speciella mac-adresser(enheter). Alltså är det möjligt att reservera en local ip som till exempel 192.168.0.2 för en speciell enhet på nätverket.

Andra inställningar som går att göra på routern är tex ändra till en static ip, vilket resulterar i att routerns default gateway aldrig byts ut. Att routern aldrig byter default gateway kan fungera som en säkerhetsrisk för privatpersoner men är precis vad företag med servrar vill ha eftersom dns servrarna inte ska behöver uppdatera sin information.

Kryptering:

Kryptering är ett sätt att försöka gömma ett avsatt meddelanden eller text, ofta i syftet att andra än personer med en nyckel ska kunna läsa detta meddelande eller text. Kryptering används idag i väldigt stora mängder, tex är känslig data på iphone krypterad för att bara apple och dig själv ska ha tillgång till dina filer. Detta är super effektivt mot hackare eller andra personer som försöker få tillgång till din privata information. Eftersom din data är krypterad kan ingen hackare läsa den tillfrågade datan utan en nyckel, för att en hackare ska kunna avkryptera datan krävs flera timmar/dagar av brute force. Exempel på ställen där kryptering har tillämpats på grund av säkerhetsskäl kan vara hur http gått över till https vilket är ett krypterat protokoll. Detsamma har tillämpats för ftp som blivit sftp och telnet som för det mesta bytts ut mot ssh. Kryptering förr i tiden bestod oftast av att placera bokstäver i en annan ordning för att förvränga datan, men har idag fått hjälp av matten och räknas nu ut genom multiplikation av långa primtal. Något som är omöjligt att räkna ut utan den medskickade nyckeln, därför ifall man försöker hacka måste datorn gissa varje primtal som går att multiplicera till det når det önskade talet, även kallat brute force. Det finns massor av olika typer av kryptering i dagens samhälle där det vanligaste är AES(Advanced Encryption Standard) ofta i formen av AES256 vilket betyder att krypteringen ska bestå av 256 bytes.

William Beinö
TE16B
Stockholm Science & Innovation School
2017-05-19

Källor och Metod:
När jag från första början läste på om OSI-modellen läste jag på en av Ciscos egna hemsidor[2] sedan läste jag en artikel av Bradley Mitchell som heter “The Layers of the OSI Model”[3] skriven på *Lifewire* 7:e april 2017. Bradley Mitchell gav bra beskrivningar av vad det olika lagrena har i uppgift och hur de åstadkommer detta. Samtidigt som jag skrev om det enskilda lagrena så kollade jag ifall informationen stämde överens med vad som stod i IT-ords definitioner av lagrena[4]. Slutgiltigt ifall det var något som var oklart googlade jag och läste vidare på wikipedia. När jag skulle skriva om TCP-modellen läste jag Ciscos definition och beskrivning av TCP-modellen, vilket jag upplevde gav mig tillräckligt med förståelse om modellen[5]. Under tiden som jag skrev på denna essä, jobbade jag med James Summers och Leon Enshagen på ett projekt i datorteknik, vilket gav mig en övergriplig förståelse inom säkerhet på internet, speciellt inom PHP och HTML. Datortekniks projektet gick ut på att skapa ett webbhotell där användaren kan skapa sin eget konto. Detta ledde till att vi var tvungna att kryptera lösenorden för att spara dem i våran databas. När detta problem uppkom började jag läsa om hur kryptering fungerar och hur man implementerar det i php. Samtidigt jobbade jag med Niklas Rydkvist på ett webbutveckling projekt där jag programmerade all nätverkskod till ett spel i javascript. Projektet i webbutveckling fick mig att läsa på om TCP och UDP innan jag satte igång att programmera, något som var väldigt lärorikt när det kommer till transport av packets. Alla bilder är antingen gjorda eller tagna av mig, så inga källor på bilderna.

Reflektion:
Under arbetes gång har jag lärt mig massor, innan denna essä hade jag aldrig hört om OSI-modellen eller TCP-modellen och visste knappt skillnaden mellan ipv4 och ipv6. Med andra ord har jag lärt mig super mycket om nätverk och hur allting fungerar tillsammans. Tack vare att jag läst på olika sidor och testat mig fram genom att konfigurera en router samt ändrat windows nätverk inställningar har jag lärt mig mycket inom säkerhet och protokollen bakom nätverk. Jag upplever att uppsatsen kanske inte bör vara en så stor uppgift utan att webbutveckling projekten samt datortekniks projekten ska höra ihop med nätverk i form av att tex skicka packets över tcp eller udp samt kanske lära sig om kryptering i php.
Osi-modellen tror jag att jag kommer ha stor nytta av i framtiden så därför upplever jag att den fortfarande bör skrivas om av kommande elever. Det roligaste med den här uppgiften var att ta reda på hur allt fungerar tillsammans och lära sig massor av nya saker på vägen.

[2] https://learningnetwork.cisco.com/docs/DOC-15624
[3] https://www.lifewire.com/layers-of-the-osi-model-illustrated-818017
[4] https://it-ord.idg.se/
[5] http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13769-5.html#tcp