

Cisco Rapport

Navn - Jonas Barigo Østergaard

Uddannelse - DataTekniker med speciale i Programmering

Instruktør - Simon Nicolas El Hanafi



Indhold

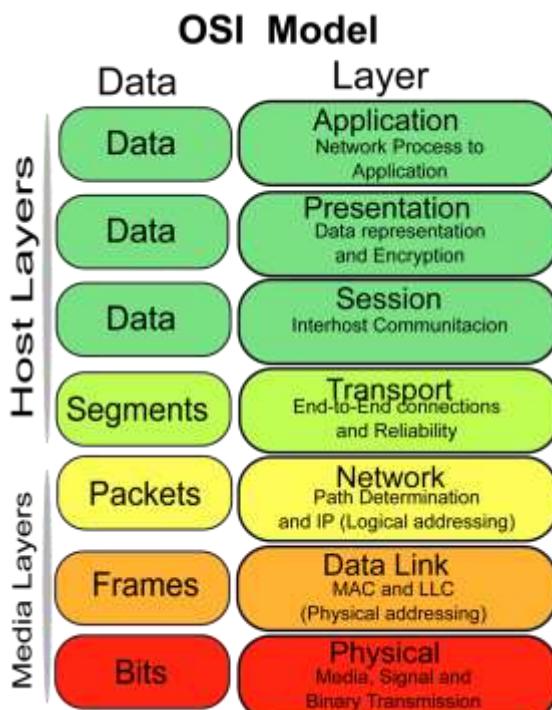
Indledning	3
Dokumentation.....	4
Osi modellen	4
Subnetting	5
Packet-tracer & CLI	7
Referat af Kapitler.....	7
Kapitel 1 Routing Concepts	7
Kapitel 2 Static Routing.....	7
Kapitel 3 Dynamic routing.....	8
Kapitel 4 Switched networks	8
Kapitel 5 switch configuration.....	9
Kapitel 6 VLANs	9
Kapitel 7 Access Control Lists.....	10
Kapitel 8 DHCP	11
Kapitel 9 NAT	11
Kapitel 10 Device Discovery, Management, and Maintenance	11
Konklusion	12

Indledning

I denne opgave har jeg skulle læse bogen Routing and Switching Essentials, lave et referat af dette og udføre packet tracer opgaver. Derudover har jeg skulle beskrive OSI modellene der er centralt for alle netværk. Jeg har også skulle beskrive Subnetting og VLSM, samt at komme med eksempler på hvordan disse anvendes. Dette gøres for at få en bredere forståelse inden for netværk og hvordan netværker fungere.

Dokumentation

Osi modellen



OSI modellen består af 7 lag som ses på figuren.

Modellens første lag er det fysiske-lag, som beskriver de fysiske komponenter af et netværk. I det fysiske lag findes komponenter så som internet kabler og NICs. Det er også her at bits bliver omdannet til diverse signaler for at kunne kommunikere med andre enheder.

Modellens andet lag er datalinklaget. På dette lag bliver data frames transporteret mellem netværks-enheder der er forbundet til det fysiske lag. Desuden bliver data link laget brugt i switch funktioner, herunder arp og mac-adresser.

Det tredje lag er netværkslaget. Netværkslaget står for at overføre packets fra netværk til netværk, det er altså her at routere befinner sig. Netværkslaget gør desuden brug af protokoller så som Rip og NAT som jeg har skulle læse om i bogen Routing and Switching Essentials.

Det fjerde lag er transportlaget. Transportlaget står for at transportere packets og segments over netværk. Her bliver protokollerne UDP og TCP brugt alt afhængigt af hvor pålidelig data overførslen skal være.

Det femte lag er Sessionslaget. Sessionslaget står for at åbne og lukke for kommunikationen mellem end-devices, med andre ord åbnes en session mellem end-devices.

Det sjette lag er Præsentationslaget. Præsentationslaget formaterer data til et format der kan læses af programmer i applikationslaget. Præsentationslaget håndterer data encryption, decryption, compression, decompression mm.

Det syvende og sidste lag er Applikationslaget. Applikationslaget er det der er nærmest brugerne og er her applikations / programmer findes. Eksempler kunne være en internet browser eller microsoft word.

Subnetting

Et subnet er et netværk inde i et netværk. Et subnet er med til at øge sikkerheden, idet et subnet ikke kan få adgang til et andet subnet, der er mindre netværkstrafik end hvis der ikke var subnets, og det er muligt for internet udbydere kun at give en IP-adresse til en lokation, da netværket kan opdeles (desuden bruges NAT til at oversætte et lokalt netværk med subnets til en offentlig IP-adresse). Alt afhængig af hvordan man subnetter kan netværkene variere i størrelse, dette gøres med variable length subnet mask eller VLSM.

Da der er ipv4 adresse mangel, er subnetting nødvendigt for at alle kan få en IP-adresse inden vi overgår til ipv6. Derudover er der også fordele ved at kunne subnette som nævnt tidligere.

Eksempel på subnet scenarie:

Vi skal subnette IP-adressen 192.168.0.0, der er skal oprettes 3 subnets som skal kunne indeholde henholdsvis 10 30 og 60 hosts.

Her starter jeg med at se på det subnet hvor der er flest hosts, altså det subnet med 60 hosts.

Derefter finder jeg det subnet mindste subnet hvor der kan være 60 hosts. I dette tilfælde vil det være /26 eller subnet maske 255.255.255.192 som kan indeholde 62 hosts. For at finde subnet masken skal man tælle de bits som subnetmasken oktet består af.

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

Her kan man se en tabel hvori bits opgøres og derved kan bruges til at udregne decimal værdien af subnetmasken. Her er der sat et 1 tal ved 128 og 64 da det er disse pladser vi bruger i subnetmasken. Altså alle tal fra start af til og med de antal hosts vi skal bruge. 64 kommer fra de 64 adresse pladser der findes og heraf er 2 reserveret til Network og broadcast, altså er der 62 host pladser som nævnt tidligere. 128 + 64 giver desuden 192 som svare til subnetmaskens sidste oktet.

Nu hvor vi ved at subnettene er opdelt i 64 pladser, ved vi dermed også at der må være 4 subnets i det hele. Subnet et der strækker sig fra 0-63, subnet to der strækker sig fra 64-127, subnet tre der

strækker sig fra 128 til 191, og subnet fire der strækker sig fra 192 til 255. Her har vi altså 4 subnet hvor der er 64 adresser og 62 host pladser i hver. Nu skal vi blot tildele de forskellige hosts til hvert sit subnet, dette gøres ved at bruge IP-adressen efterfulgt af subnet masken. Eg. 192.168.0.61 255.255.255.192. Dette kunne være adressen på en host i subnet 1. hvis vi skulle tilføje hosts til subnet 2 ville vi skulle sætte den sidste del af ip adressen til at være lig med den host-range som subnettene råder over. Derfor ville vi skulle sætte en IP-adressen på en host i subnet 2 til at være 192.168.0.65-126 255.255.255.192.

For VLSM laver man et subnet der svare til det antal hosts man skal bruge på hvert subnet og ikke kun det største. Så man kan have et subnet med 62 hosts og et subnet med 14 hosts i på den samme IP-adresse. Før inddelte jeg subnettene i lige store subnets.

Eksempel på VLSM:

	128	64	32	16	8	4	2	1
Subnet 1	1	1	0	0	0	0	0	0
Subnet 2	1	1	1	0	0	0	0	0
Subnet 3	1	1	1	1	0	0	0	0

Jeg tager her udgangspunkt i det forrige scenarie hvor der var 60, 30 og 10 hosts i hver deres subnet. Her starter jeg med at finde subnettet for 60 hosts igen, da dette er det største. Som det kan ses ud fra tabellen har de 3 subnets forskellige værdier på subnetmasken. Subnet 1 har slutning 192, subnet 2 har slutningen 224, subnet 3 har slutningen 240. Man starter desuden her med det største subnet fordi dette forhindre overlapning af subnettene.

Subnettene vil derfor se således ud:

Subnet 1: (IP-adresse) **192.168.0.1-62** (Subnetmask) **255.255.255.192**

Subnet 2: (IP-adresse) **192.168.0.65-94** (subnetmask) **255.255.255.224**

Subnet 3: (IP-adresse) **192.168.0.97-110** (Subnetmask) **255.255.255.240**

Tal-Tal repræsentere en ip range.

VLSM sørger for at så få host adresser som muligt går til spilde. I det forrige eksempel havde vi et subnet med 62 host pladser men kun 10 hosts. Her er de 10 hosts placeret i et subnet med 14 host pladser.

Packet-tracer & CLI

Packet tracer er et program udviklet af cisco. Packet-tracer bruges som et virtuelt læringsmiljø hvori man kan konfigurere netværk. Packet-tracere brugere desuden kun cisco enheder og software. På nogle af enhederne I packet-tracer kan anvende en CLI (Command Line Interface). Denne bruges til at indskrive kommandoer, der har til formål at konfigurere den valgte enhed. Her kan man bl.a konfigurere ip adresser på en router eller switch. Derudover kan man også konfigurere sikkerhed.

For dokumentation af packet-tracer opgaver, se mappen "packet tracer opgaver"

Referat af Kapitler

Kapitel 1 Routing Concepts

Kapitlet omhandler funktionen af en router, herunder hvilke dele en router består af, hvordan man forbinder en router på forskellige måder, hvordan en router udvælger den bedste vej til destination, routerens rolle i forhold til osi modellen, samt diverse kommandoer der kan bruges til konfiguration af router, samt kommandoer til at vise hvad routeren er forbundet til og på hvilken måde.

Kapitel 2 Static Routing

Static routing vs dynamic routing, AD table dictates static routing is the preferred choice.

Default static route 0.0.0.0 0.0.0.0 last resort gateway – bruges når en packet ikke matcher en destination ip i routing tabellen.

Default static route ipv6: ::/0

Floating static routes er en static route der fungere som en backup af en primary static route eller dynamic route. Her skal man configurerer den floating route til at have en højere værdi i AD tabellen / have en længere administrative distance.

Derudover har jeg også lært om troubleshooting af routere og hvordan man genopretter netværksadgang.

Kapitel 3 Dynamic routing

Router Rip, network network-address, version 2, show ip protocols, show ip route, no auto-summary, passive-interface {interface}, passive-interface default, no passive-interface {interface}, Propagate a default route in rip, the edge router must be configured with a default static **route ip route 0.0.0.0 0.0.0.0** command. Then use the **default-information originate** command in **router rip**.

Longest matching prefix. En ip-adresse kan være valid i flere subnets, når en router skal sende en packet, vælger routeren derfor ip adressen med det længste prefix.

Dynamisk routing bliver brugt til at udveksle data mellem routere, denne data anvendes til at opdage netværk, opdatere routing tables, vælge den bedste vej til destination og finde en ny bedste vej til destination, hvis den forrige ikke virker.

Dynamisk routing opdatere sig selv, og bruger derfor mere cpu kraft og netværks bandwith.

Kapitel 4 Switched networks

3 Lags designet fordeler netværket i core, distribution og access lag og giver mulighed for optimering af hver deres specifikke funktionalitet. Her bliver der sørget for modularitet, modstandsdygtighed og fleksibilitet der alle er med til at tilføje sikkerhed, mobilitet og fælles kommunikationsfunktioner.

Netværks switch benytter tabeller til at gemme mac-adresser som benyttes til at bestemme hvor packets skal føres hen. Switch kan benytte en flood funktion til at opdatere tabellen med gemte mac-adresser, dette gøres hvis en packet indeholder en destinations MAC-adresse der er ukendt.

Switch kan enten benytte store-and-forward eller cut-through teknologier. Store-and-Forward læser hele packeten og tjekker den for fejl før den sendes videre, hvorimod cut-through kun tjekker den første del af packetten før den sendes videre.

Kapitel 5 switch configuration

I dette kapitel har jeg lært om cisco switcher og hvordan man konfigurerer dem, herunder har der især været fokus på at konfigurer sikkerhed for switcher.

Når en switch tændes går den igennem 5 trin før den er klar. Først kører switchen en selv test der hedder POST. POST tjekker: CPU, DRAM, og FLASH. I trin 2 loader switchen bootloader software, dette gøres så snart POST er kørt uden fejl. I trin 3 bliver CPU'en initialiseret. I trin 4 bliver FLASH initialiseret. I trin 5 loades IOS operativ systemet af bootloaderen og giver kontrollen til IOS.

Til selve konfigurationen af switchen, har kapitlet omhandlet hvordan man konfigurerer SSH og hvordan man ikke skal bruge telnet, da det ikke krypterer plain-text. Derudover har kapitlet beskrevet hvordan man skaber sikkerhed for de enkelte switchporte via switchport port-security commandsne, hvori man kan bestemmer statiske mac-adresser der er tilknyttet portene.

Kapitel 6 VLANs

I dette kapitel har jeg lært om routes på routeren, oprettelse af vlans, hvordan man tilføjer vlans til interfaces, hvordan man opretter trunking, hvornår man skal oprette trunking, hvad native vlan bruges til, hvad switchport mode er og hvordan man bruger access og trunk til dette, hvordan man konfigurerer subinterfaces på en router så man kan pinge mellem flere forskellige vlans.

Kapitel 7 Access Control Lists

ACL, router kommandoer der bestemmer om packets må forwardes eller om de bliver droppet.

Packet filtering sker på lag 3 og 4 I osi modellen, network og transport.

Show access-list, show run | section interface.

Oprettelse af access-list (conf t): access-list {number} eller ip access-list standard {name}.

Herefter kan man oprette regler for det oprettede access-list.

Permit/Deny (host) ip-address (wildcard-mask)

Wildcard-mask bliver brugt til ip-ranges hvorimod host bliver brugt til enkelte ip adresser.

Hvis man vil slette en konfiguration kan man skrive no {ace number}

Desuden er det implicit at alt bliver denied, derfor skal man skrive permit any, efter at man har lavet et deny statement.

Hvis man vil slette en hel access-list kan man skrive:

No access-list {number} eller no ip access-list standard {name}

Hvis man vil tilknytte en access-list til et interface skal man først vælge sit interface og derefter bruge kommandoen: ip access-group {navn} {in/out}.

Her bestemmer in/out om det er indgående eller udgående trafik der skal filtreres.

Man kan også bruge access-class til at konfigurere lines (eg. line vty 0 15) for at filtrere adgange igennem ssh eller telnet.

Kapitel 8 DHCP

DHCP eller Dynamic Host Configuration Protocol sørger for at tildele ip adresser automatisk og gør derved jobbet lettere for netværksadministratorer. DHCP kan benyttes på både ipv4 og ipv6, man kan desuden konfigurere en server til at tildele ip-adresserne til de forskellige enheder på netværket, ud over en server kan en router også bruges til dette formål. Når en ip adresse skal tildeles udveksler enheden der skal have en ip adresse og DHCP serveren meddeleser, der har til formål at validere adresse informationer og endeligt tildeling af adressen.

Ved ipv6 bruges SLACC og Stateful DHCP.

SLACC bruger information Router Advertisement til at udvælge og konfigurere ip adresser.

Stateful Bruger derimod en DHCP server til at udvælge og konfigurere ip adresser.

Hvis en DHCP server er op et andet netværk en enheden bliver man nødt til at anvende en relay agent, der sørger for at DHCP udvekslingen kan ske over andre netværk.

Kapitel 9 NAT

I dette kapitel har jeg lært om NAT der er et system som blev implementeret fordi der er ipv4 adresse mangel. Nat sørger for at oversætte lokale IP adresser til offentlige ip adresser. Derudover har jeg lært om konfigurering af NAT på routere, fejlfinding af NAT problemer og PortForwarding og hvordan man tilgår en routerens indstillinger via en lokal IP adresse.

Kapitel 10 Device Discovery, Management, and Maintenance

Cdp bruges til at tilgå information om andre enheder forbundet til den enhed man ser på. Eg. en router kan tilgå informationer om en switch som er forbundet til routeren. Her kan man bl.a. se hvilket interface enheden er forbundet til, enhedens navn og enhedens ip adresse. Lldp gør nogenlunde det samme, lldp er dog ikke en cisco specifik feature og bruges derfor når cisco enheder skal finde ikke-cisco enheder på netværket.

Derudover har jeg lært at konfigurere NTP der bruges til at synkronisere tid mellem forskellige enheder. Desuden kan syslog beskeder tildeles et tidspunkt hvor en begivenhed opstod.

Til sidst har jeg lært om IOS versioner, installation af image til flash, backup af image og fjernelse af image. Jeg har her også lært om software licens og hvordan dette konfigureres på cisco enheder.

Konklusion

I denne opgaver har jeg lært om routing concepts, static routing, dynamic routing, switched networks, switch configuration, VLANs, Access Control Lists, DHCP, NAT og Device Discovery, Management, and Maintenance, som det fremkommer af mine referater. Derudover har jeg lært om subnetting, med og uden VLSM, OSI modellen, Packet tracer og dets funktioner, herunder CLI og diverse kommandoer dertil.