Cisco

RASMUS JUEL NIELSEN

Datatekniker med speciale i Programmering

Indholdsfortegnelse

Dagbog

Dag 1: Læst og refereret Bogen ”Routing and Switching Essentials”.

Dag 2: Læst og refereret Bogen ”Routing and Switching Essentials”.

Dag 3: Læst og refereret Bogen ”Routing and Switching Essentials”.

Dag 4: Læst og refereret Bogen ”Routing and Switching Essentials”.

Dag 5: Læst og refereret Bogen ”Routing and Switching Essentials”.

Dag 6: Færdiggjort bogen. Arbejdet med OSI modellen.

Dag 7: Udarbejdet afsnit omhandlende subnetting, Packet Tracer og CLI. Finpudset rapport og skrevet konklusion.

Indledning

I rapporten skal der udarbejdes et referat af alle kapitlerne i bogen ”Routing and Switching Essentials”. Derudover skal der beskrives, udarbejdes og dokumenteres en række opgaver inden for emnerne: OSI-modellen, subnetting, VLSM, Packet Tracer samt CLI.

Kapitel 1 - Routing Concepts

Router Configurations

En router forbinder et netværk med et andet, og er ansvarlig for at levere data pakker over forskellige netværk, både lokalt og globalt. Når en host sender en pakke til en enhed på et andet IP netværk, bliver pakken leveret gennem en default gateway, da en host enhed ikke kan kommunikere direkte med en enhed uden for det lokale netværk. Default gateway er destinationen som kommunikerer fra det lokale netværk til enheder på fjerne netværk – oftest brugt til at koble et lokalt netværk til internettet.

Den hurtige kommunikation mellem netværk ville ikke være muligt uden routerens evne til at bestemme den bedste rute hvorved data pakkerne leveres til destinationen – dette sker vha. router tables.
Routere består af en processor og hukommelse (enten RAM eller ROM), og lagrer nødvendig data permanent for at udføre systemfunktioner (system initialization, routing functions og switching functions).

Router Memory

Memory	Description
Random Access Memory (RAM)	Volatile memory that provides temporary storage for various applications and processes including: • Running IOS • Running configuration file • IP routing and ARP tables • Packet buffer
Read-Only Memory (ROM)	Non-volatile memory that provides permanent storage for: • Bootup instructions • Basic diagnostic software • Limited IOS in case the router cannot load the full featured IOS
Non-Volatile Random Access Memory (NVRAM)	Non-volatile memory that provides permanent storage for the: • Startup configuration file
Flash	Non-volatile memory that provides permament storage for: • IOS • Other system-related files

Hvert netværk routeren er forbundet til kræver typisk et separat interface, som bruges til at forbinde en kombination af både LANs (Local Area Networks) og WANs (Wide Area Networks). Et LAN er typisk et Ethernet netværk bestående af enheder som printere, computere og servers, hvor et WAN forbinder netværk over store geografiske områder. WAN bruges f.eks. til at forbinde et LAN til Internet udbyderens netværk (ISP – Internet Service Provider).

Routere understøtter 3 packet-forwarding mekanismer:

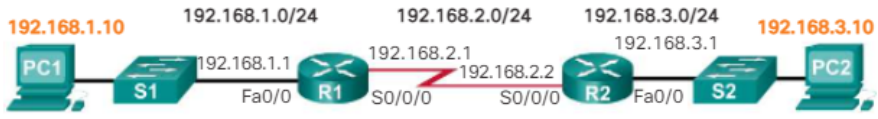
- **Process switching**

  Hver data pakke skal af CPU'en individuelt
- **Fast switching**

  Kun den første datapakke af et flow skal igennem CPU'en, hvorefter de resterende pakker tilføjes til Fast Foward Cachen, som hurtigere bliver bearbejdet.
- **Cisco Express Forwarding (CEF).**

  CEF bygger en Forwarding Information Base, ligesom i fast switching, samt en Adjacency table, som læser pakker på forhånd og derfor skaber et hurtigere flow.

For at skabe netværksadgang, skal enheder konfigureres med en IP-adresse plan for at identificere den rette IP-adresse (Identificerer den unikke host på et lokalt netværk), Subnetmaske (Identificerer hvilket netværks subnet hosten kan kommunikere med), default gateway (identificerer IP adressen på routeren som pakker skal sendes til, når pakker skal sendes til en destination uden for det lokale netværks subnet).



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.0	N/A
R2	Fa0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0	192.168.2.2	255.255.255.0	N/A
PC1	N/A	192.168.1.10	255.255.255.0	192.168.1.1
PC2	N/A	192.168.3.10	255.255.255.0	192.168.3.1

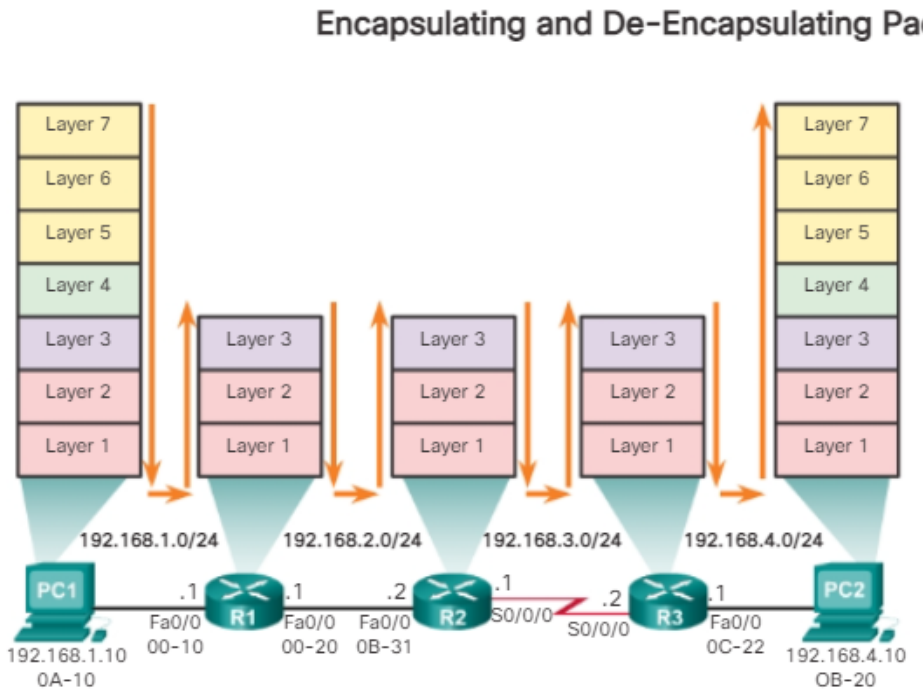
Denne figur viser hvordan man designer et nyt netværk eller mapper et allerede eksisterende. Det består af både en topologi (øverste del) og adresse tabel (nederste).

En host kan blive tildelt IP adresse information både statisk og dynamisk.
Statisk betyder at hosten manuelt får tildelt den korrekte IP adresse. Subnet maske og default gateway.
DNS (Domain Name System) serverens IP adresse kan og blive konfigureret.
Ved dynamisk routing bliver IP adresse informationen tildelt serveren ved brug af DHCP (Dynamic Host Configuration Protocol). Denne uddeler automatisk gyldige IP adresser, subnet masker og default gateway til enheder.

Routing Decisions

Den primære funktion for en router er at frembringe data pakker til deres destination, og gøres ved at routeren accepterer en pakke på et interface og sender den ud af et andet interface. Router switching's funktion er at indkapsle data pakker i den rigtige data link frame type for det udadgående data link. Router switching betyder at flytte pakker fra en source til en destination og skal ikke forveksles med funktionen hos en layer 2 Switch.

- **Step 1:** De-encapsulate layer 2 frame header og trailer for at fremvise layer 3 pakken.
- **Step 2:** Undersøger destinations IP adressen for IP pakken for at finde den bedste rute i routing tabellen.
- **Step 3:** Hvis routeren finder en rute til destinationen encapsulerer den layer 3 pakken ind i en ny layer 2 frame og frembringer framen ud af exit interfacet.



Det er normalt at pakker behøver en encapsulation i en anderledes type af layer 2 frame end den er modtaget. F.eks. kan en router modtage en ethernet encapsulation frame på et FastEthernet interface og derefter behandle den frame til at blive sendt ud af et seriel kabel.

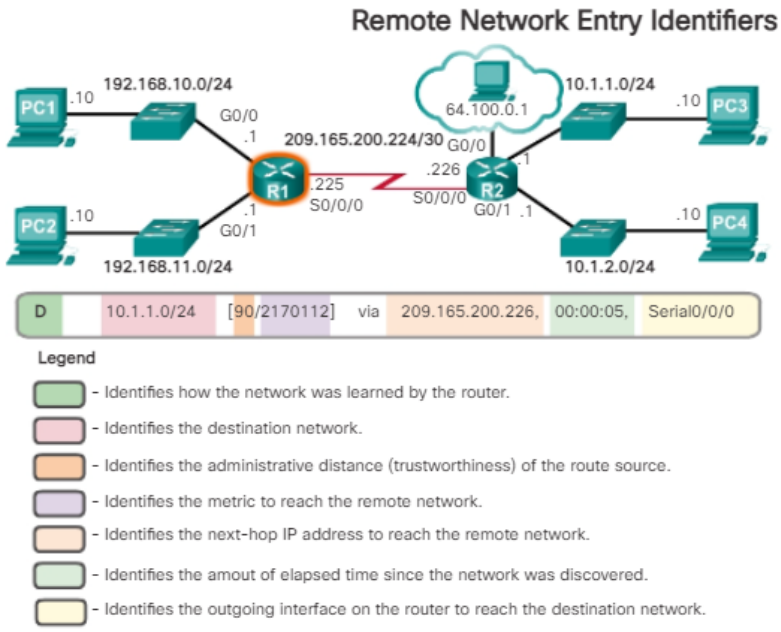
Routeren har også en funktion til at bestemme den bedste rute til at sende pakker på tværs af netværk. Det kan enten være i form af:

- **Directly Connected network** – destinationen og host adresserne er på det samme netværk som routerens interface
- **Remote Network** – hvis destinatonens IP adresse for pakken hører til et remote netværk, sendes pakken til en anden router.
- **No route determinded** – hvis destinations IP adressen ikke hører til et connected eller remote netværk leder routeren efter en Gateway of Last Resort.

Routeren overvejer mange ruter for at finde den korteste og hurtigste rute at sende en given pakke gennem. Hertil gives en række værdier som bestemmer om ruten er den mest effektive: **RIP (Routing Information Protocol)** bruger f.eks. antal hops (antal routere den skal igennem) for at bestemme den bedste rute, hvor **EIGRP (Enhanced Interior Gateway Routing Protocol)** tager faktorer som bredbånd, forsinkelse, belastning og pålidelighed i betragtning for at bestemme den bedste rute.

Router operations

Nedenstående figur viser en kørende routers routing table (vises ved at skrive ”show ip route” i CLI).



En ny router uden konfigurerede interfaces har en tom routing table, og før at den kan benyttes skal der tilføjes en IP adresse og aktiveres ved brug af **no shutdown** kommandoen i routeren **CLI (Command Line Interface).** Når interfacet kører ændres dens status til ”up” og netværket til det tilknyttede interface tilføjes til routing table.

Kapitel 2 - Static routing

Routere kan finde andre netværk på to måder, manuelt og dynamisk. Manuelt betyder at man taster netværk ind manuelt i routerens router table i form af statiske ruter. Dynamisk routing foregår automatisk ved hjælp af en dynamisk routing protokol. Mange netværk benytter en kombination af de dynamisk og statisk routing.

- **Fordele ved statisk routing:**

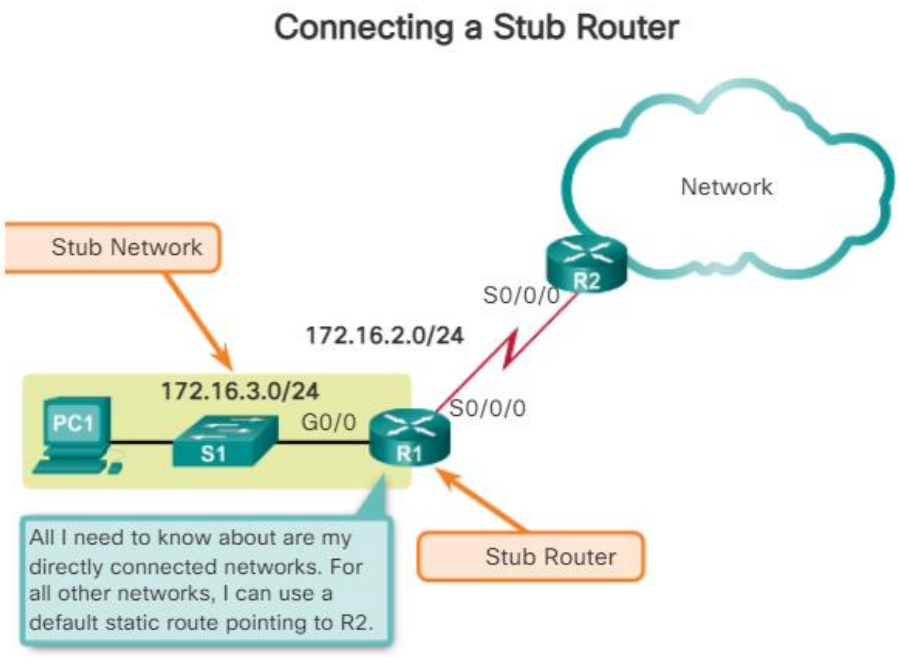
  Sikkerhed, bruger mindre båndbredde, bruger ikke CPU til at udregne kommunikations ruter og den rute statisk routing bruger til at sende data er kendt.

- **Ulemper ved statisk routing:**

  Tager tid at konfigurere og vedligeholde, der kan opstå fejl i opsætningen især i større netværk, skalerer ikke godt med voksende netværk og komplet kendskab til netværket er nødvendigt for optimal implementering.

Fordele og ulemper er omvendt for dynamisk routing.

Stub router



Når en router kun er forbundet til én anden router kaldes det en stub router, og her benyttes der default static routing. En default static route kan både læres dynamisk eller konfigureres manuelt, men er egentlig bare en statisk route med 0.0.0.0/0 som destinations IPv4 adresse.

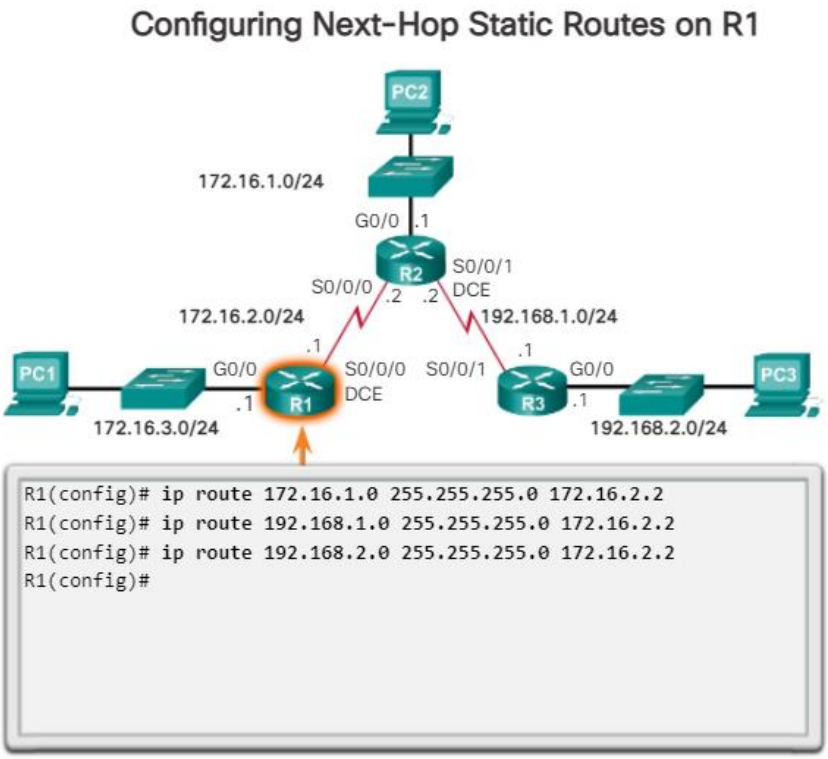
Ip route

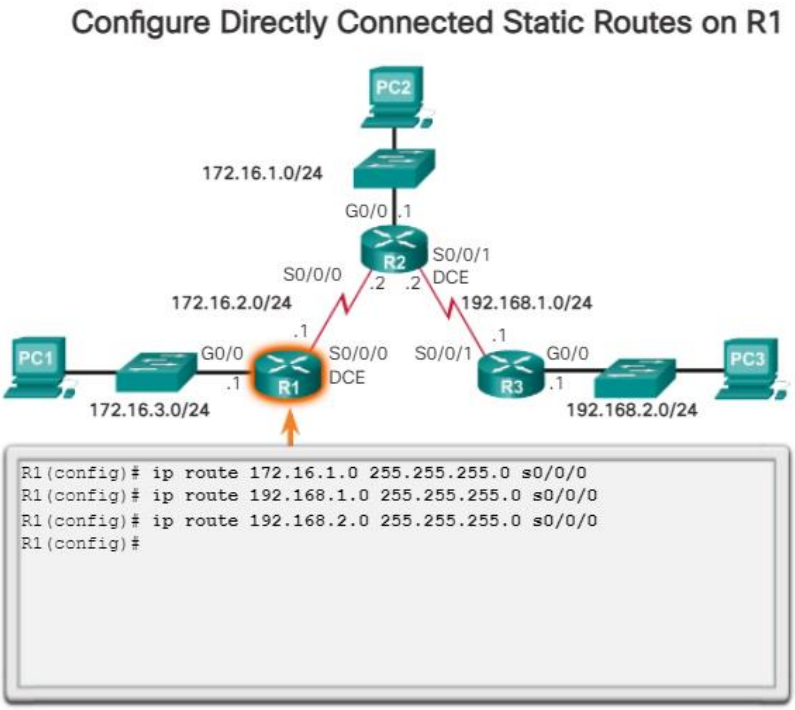
Statisk route konfigureres ved brug af ”ip route” kommando i gobal configuration:

```
Router(config)# ip route network-address subnet-mask
{ip-address | exit-intf}
```

Det kræver følgende parametre:

- **Netværks adresse** – destinatons netværks adressen af det remote netværk tilføjes til routing table, ofte refereret til som prefix.
- **Subnet-masken** – kan blive modificeret til at opsummere en gruppe af netværk.
- **IP-adresse** – next hop.
- **exit-intf** – outgoing interface, bruges til at sende pakker til next hop.





Man kan verificere den statiske rute ved at skrive ”**ping**”, ” **traceroute**”, ”**show ip route**” eller ”**show ip route static”**.

En floating static route kan blive konfigureret, som en backup af et main link, ved at manipulere dets administrative værdi.

Kapitel 3 - Dynamic routing

De primære komponenter i dynamic routing:

- **Data struktur** – routing protokoller bruger tables eller databaser til dets operationer, som lagres i RAM.
- **Routing protocol messages** – bruges til at opdage nabo routers, dele information og vedligeholde informationer om netværket.
- **Algorithm** – en liste af punkter til at fuldføre en opgave, bruger algoritmer til at komprimere information og bestemme den bedste rute.

Routing protocols gør det muligt for routere, dynamisk at dele information om remote networks og automatisk dele denne information til deres egen routing tables. Det bruger routeren til at bestemme den

bedste rute, denne rute installeres i routeren hvis der ikke er en anden rute med en lavere AD (Administrative Distance). F.eks. en statisk rute med en AD på 1 vil have højere prioritet over det samme netværk som den dynamiske routing protocol har lært.

Dynamic Routing Advantages and Disadvantages

Advantages	Disadvantages
Suitable in all topologies where multiple routers are required.	Can be more complex to implement.
Generally independent of the network size.	Less secure. Additional configuration settings are required to secure.
Automatically adapts topology to reroute traffic if possible.	Route depends on the current topology.
	Requires additional CPU, RAM, and link bandwidth.

Dynamic routing er den bedste løsning for et større netværk, da det kræver mindre konfiguration og administrering, men kræver dog stadig en dedikeret del af routerens ressourcer. Router protokollerne finder andre netværk og opretholder korrekt netværksinformation.

Når en router opdager flere ruter til et andet netværk, bruger routeren Administrative distance til at bestemme hvilken kilde den skal bruge. Jo mindre AD værdi jo større prioritering.

IPv4 router tables kan indeholde fire typer af routes: Ultimate routes, Level 1 routes, Level 1 parent route, Level 2 child route. IPv6 er classless og derfor er alle routes level 1 ultimate routes.

Kapitel 4 – Switched Networks

Alle avancerede tjenester afhænger af tilgængeligheden af en robust routing- og switching-infrastruktur, som de kan bygge på. Denne infrastruktur skal være omhyggeligt designet, implementeret og administreret for at give en stabil platform. Det er er her switches kommer ind og hjælper med netværkstrafikken og bruger MAC adressers information til effektivt at ”switche” data mellem hosts på netværket.

Borderless network

Cisco Borderless Network er en netværksarkitektur, der kombinerer innovation og design. Det giver organisationer mulighed for at understøtte et borderless netværk (netværk uden grænser), der kan forbinde enhver enhed, hvor som helst, når som helst, både sikkert, pålideligt og problemfrit.

Generel Switching i et netværk

Konceptet med at skifte og videresende frames er universelt inden for netværk og telekommunikation. Forskellige typer switches bruges i LANs, WANs og det offentlige telefonnetværk (PTSN). Det grundlæggende begreb om at switche refererer til, at en enhed træffer en beslutning baseret på to kriterier:

- **Indgangsport**
- **Destinationsadresse**

Beslutningen om, hvordan en switch videresender trafikken, træffes i forhold til flowet af trafikken.

MAC adresse i switching

Switches bruger MAC adresser til at dirigere netværkskommunikation gennem switchen, til den relevante port, mod destinationen.
Hver frame der sendes til en switch, undersøges for ny information, og gøres ved at switchen undersøger kildens frame MAC adresse og det port nummer, hvorpå framen går ind i switchen. Hvid MAC adressen ikke eksisterer, bliver den tilføjet til swtichens table sammen med port nummeret.

Store- and forward & Cut-through

Swtiches bruger enten store-and-forward eller cut-through switching. Store-and-forward læser hele rammen ind i en buffer og kontrollerer CRC, før rammen videresendes. Cut-through switching læser kun den første del af rammen og begynder at videresende den, så snart destinationsadressen er læst. Selvom dette er ekstremt hurtigt, foretages der ingen fejlkontrol på rammen før den videresendes.

Switches forsøger som standard at bruge full duplex-kommunikation. Switch-porte blokerer ikke for broadcast, og det at forbinde switches kan udvide størrelsen af broadcast-domænet, hvilket ofte resulterer i forringet netværksydelse.

Kapitel 5 – Switch Configuration

Switching configuration i CLI

This Syntax Checker activity reviews basic switch configurations.

Configure the switch hostname to be 'HQSw1'.

```
Switch# configure terminal
Switch(config)# hostname HQSw1
```

Configure the encrypted privileged EXEC password to 'class'.

```
HQSw1(config)# enable secret class
```

Set all line passwords to 'cisco' and require a login, starting with the console. Set vty lines 0 through 15.

```
HQSw1(config)# line console 0
HQSw1(config-line)# password cisco
HQSw1(config-line)# login
HQSw1(config-line)# line vty 0 15
HQSw1(config-line)# password cisco
HQSw1(config-line)# login
```

Exit to global configuration mode. Enter the command to encrypt the plain text passwords.

```
HQSw1(config-line)# exit
HQSw1(config)# service password-encryption
```

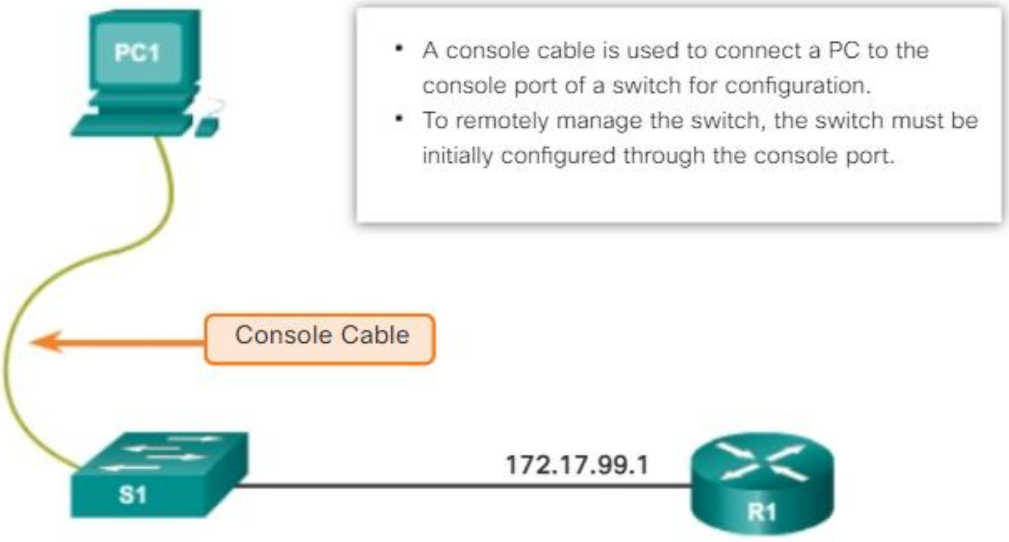
Configure VLAN 1 with the IP address 192.168.10.2/24 and activate the interface.

```
HQSw1(config)# interface vlan 1
HQSw1(config-if)# ip address 192.168.10.2 255.255.255.0
HQSw1(config-if)# no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up
```

Return directly to privileged EXEC mode and display the current configuration.

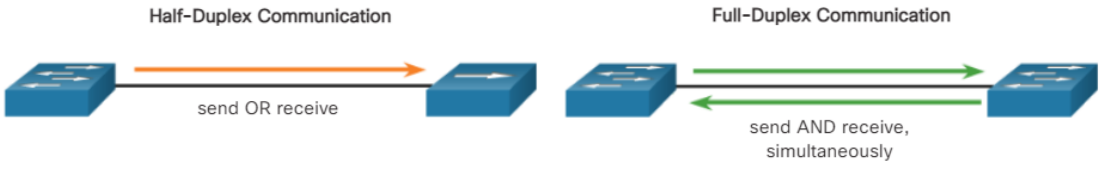
```
HQSw1(config-if)# end
HQSw1# show running-config
Building configuration...
```

Switches bruges til at forbinde flere enheder på det samme netværk. I et korrekt designet netværk er LAN-switches ansvarlige for at styre og kontrollere datastrømmen på access layer til netværksressourcer. Access layer er hvor klient netværksenheder er direkte forbundet til netværket, og IT-afdelinger ønsker ukompliceret netværksadgang for brugerne. Det er et af de mest sårbare områder på netværket, fordi det er så udsat for brugeren. Switche skal konfigureres til at være modstandsdygtige over for angreb af alle typer, mens de beskytter brugerdata og giver mulighed for højhastighedsforbindelser.



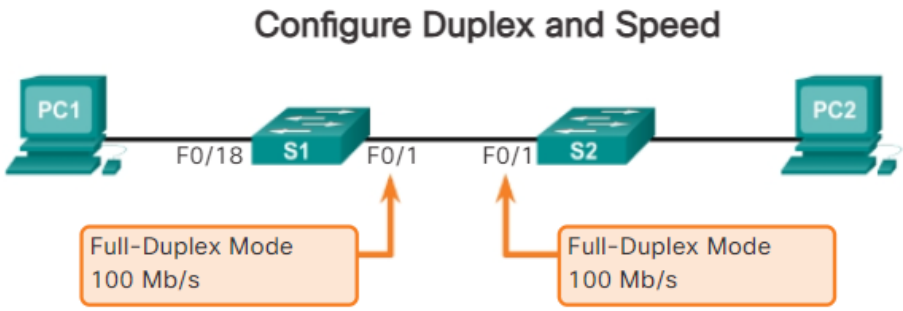
For at forberede en switch til remote management access skal switchen konfigureres med en IP-adresse og en subnet mask. For at administrere switchen fra et remote netværk skal switchen konfigureres med en default gateway.

Full-duplex & Half-duplex



Full-duplex kommunikation øger ydeevnen på et switched LAN ved at øge tillade begge ender af en forbindelse at transmittere og modtage data samtidig. Half-duplex kommuniakton er unidirectional hvorved det at sende og modtage data ikke foregår på samme tid, dette kan ofte resultere i kollisioner, og ses oftest på ældre hardware. Full-duplex benyttes dermed på de fleste nye hardware.

Duplex konfigureres på følgende måde og her kan man tilpasse hastigheden på switchen:



Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface FastEthernet 0/1`
Configure the interface duplex.	`S1(config-if)# duplex full`
Configure the interface speed.	`S1(config-if)# speed 100`
Return to the privileged EXEC mode.	`S1(config-if)# end`
Save the running config to the startup config.	`S1# copy running-config startup-config`

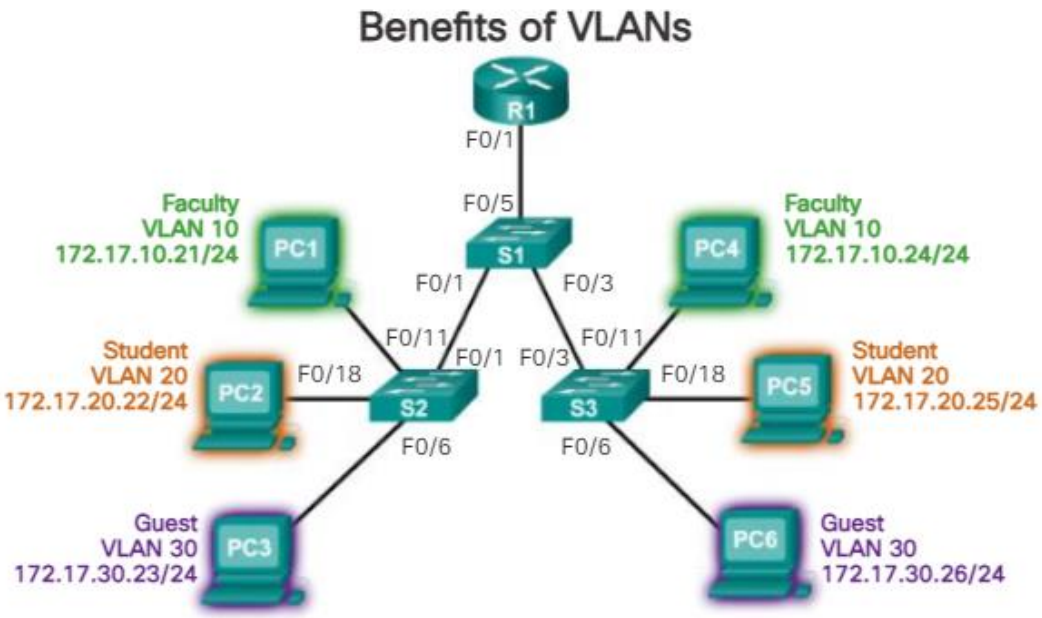
Switch port security

En switch kan konfigureres remotely, her er der brug for at default gateway er konfigureret ved brug af "ip default-gateway" kommandoen. Det anbefales at man bl.a. benytter beskyttelse i form af kryptering – f.eks. SSH (Secure Shell) i stedet for Telnet – så man undgår at uvedkommende kan tilgå passwords og brugernavne, og afværge angreb som MAC address Flooding og DHCP Spoofing.

Kapitel 6 – VLAN

VLANs er baseret på logiske forbindelser i stedet for fysiske forbindelser. Brugerproduktivitet og netværkstilpasningsevne er vigtige for virksomheders vækst og succes. VLAN'er gør det nemmere at designe et netværk, der understøtter en organisations mål. De primære fordele ved at bruge VLAN:

- **Sikkerhed** – Grupper med sensitiv data er separerede fra resten af netværket – f.eks Faculty VLAN 10, er fuldstændig separeret fra ”Student” og ”Guest” data trafikken (se nedenstående figur).
- **Reducerede omkostninger** – resultat af at der er mindre brug for dyre netværks opgraderinger.
- **Bedre ydeevne –** reducerer unødvendig trafik på netværket.
- **Reducerer størrelsen af broadcast domæner –** færre enheder på broadcast domænet.
- **Forbedret effektivitet for IT ansvarlige –** brugere med lignende netværks krav deler samme VLAN.
- **Simplere ledelse af projekter.**



Netværk uden VLANs – Når en switch modtager en broadcast frame på en af dens porte, fremsender den framen ud af alle andre porte undtagen den port hvorpå broadcasten var modtaget. Det betyder så også at alle på netværket vil modtagen framen.

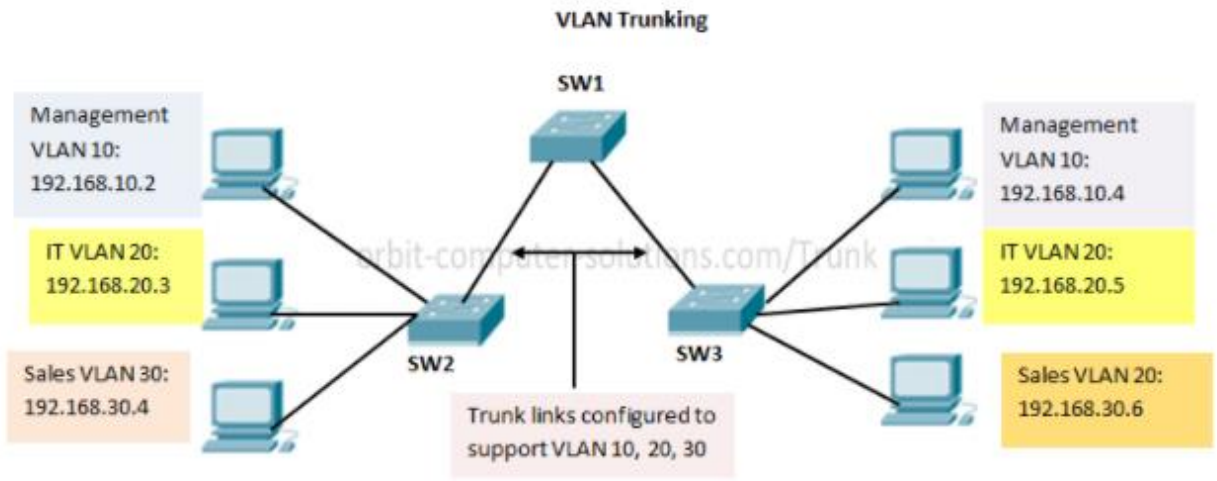
Trunks

Før i tiden var det vanskeligt at implementere VLANs på tværs af netværk. Hvert VLAN blev manuelt konfigureret på hver netværks switch. VLAN trunking blev udviklet for at hjælpe med at gøre det nemmere at administrere et stort switched netværk.

Man kan kontrollere og segmentere netværks broadcast med VLANs. VLAN trunking muliggør flytning af trafik til forskellige dele af netværket konfigureret som et VLAN.

En trunk er en point-to-point-forbindelse mellem to netværksenheder, der bærer mere end ét VLAN. Med

VLAN trunking kan man udvide sit konfigurerede VLAN på tværs af hele netværket. De fleste Cisco-switches understøtter IEEE 802.1Q, der bruges til at koordinere trunks på FastEthernet og GigabitEthernet.

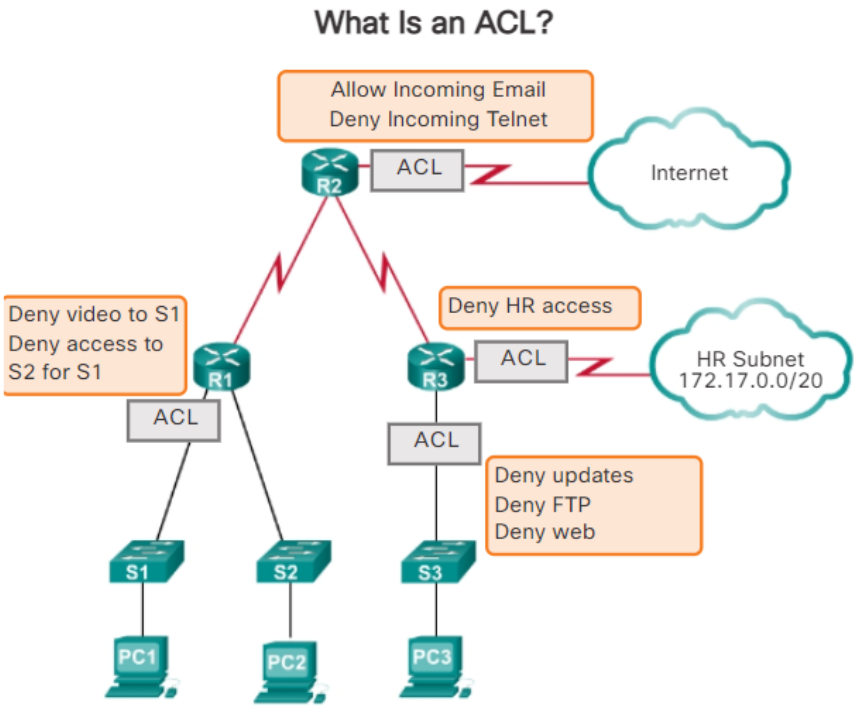


På ovenstående figur, i er linksne mellem SW1 ←→ SW2 og SW1 ←→ SW3 konfigureret som trunk links, for at aktivere trafik mellem VLAN 10, 20 og 30. Dette netværk ville ikke kunne virke uden VLAN trunks.

Kapitel 7 – Access Control Lists

Access Control Lists (ACL) er en række IOS kommandoer som kontrollerer om en router fremsender eller droppe pakker, baseret på informationen i ”headeren” på data pakken. ACL er ikke konfigureret som standard på en router, og filtrerer derfor ikke trafikken gennem routeren, hvis det ikke er konfigureret.

Pakke filtrering kontrollerer tilgængeligheden til et netværk, ved at analysere de pakker der kommer ind og sendes ud af routeren og baseret på opstillede kriterier, vurderes det om de skal sendes videre eller droppes. Disse kriterier kan baseres på IP adressen fra afsenderen eller destinationen, og den protokol der findes i pakken.



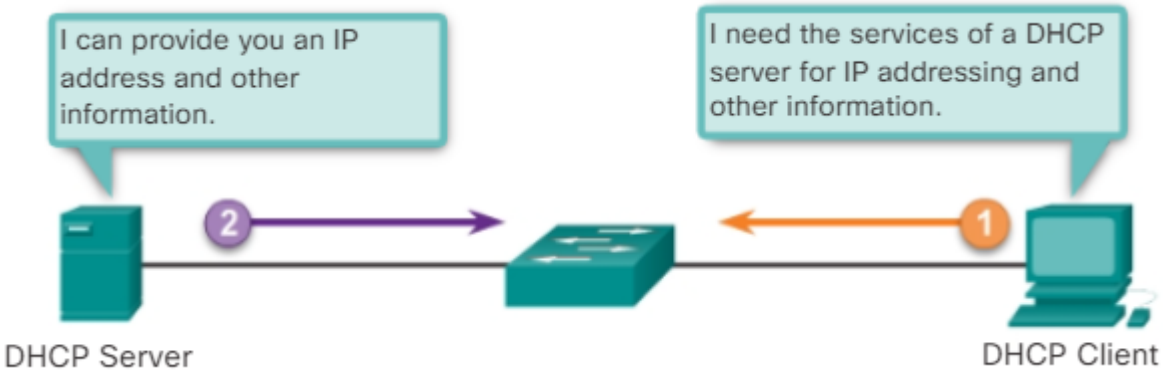
ACL er en sekventiel liste af "permit" og "deny" statements. Når netværkstrafikken passerer et interface som er konfigureret med ACL, sammenligner routeren informationen i pakken med hver indkommen information i sekventiel rækkefølge (en ad gangen), og beslutter dermed om pakken matcher en af de opstillede permit eller deny statements, hvis den gør det, så bliver pakken behandlet ud fra opsatte statements (se ovenstående figur).

Kapitel 8 – DHCP

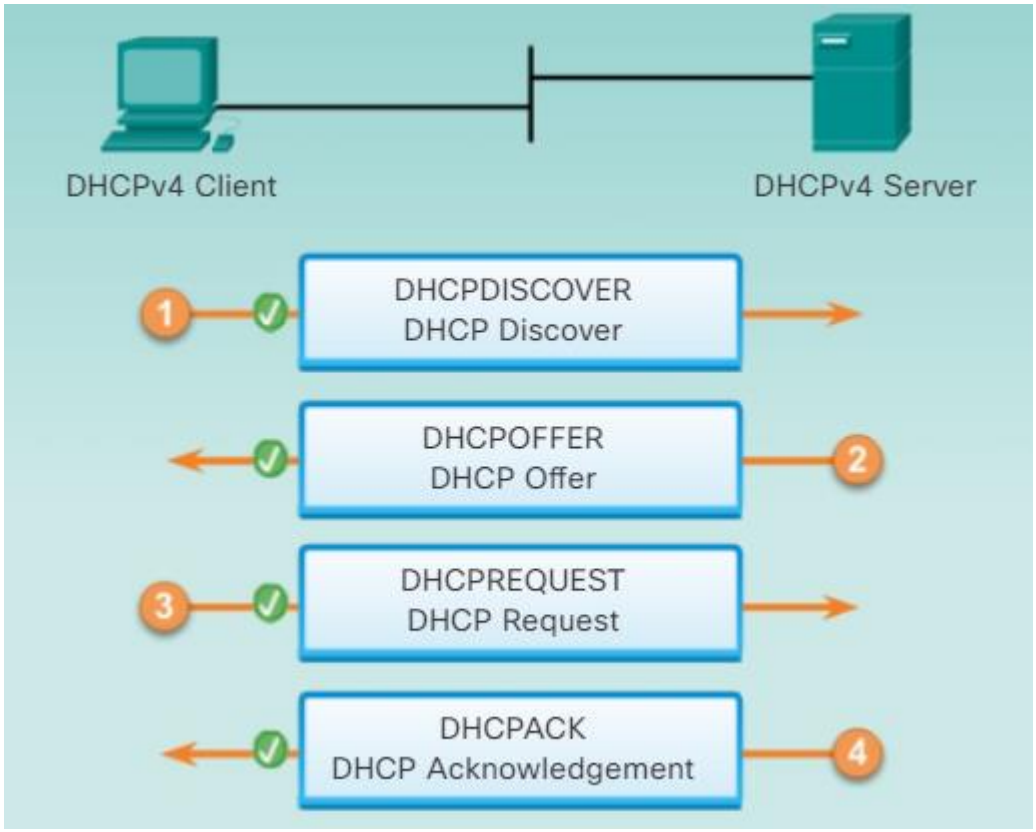
IPv4

Dynamic Host Configuration Protocol (DHCP) kan konfigureres på et lokalt netværk for at simplificere uddeling af IP adresser. En centraliseret DHCP server gør det muligt for en organisation at administrere alle dynamiske IP adresser fra en enkelt server og bruges især på store netværk. DHCP er både tilgængeligt for IPv4 og IPv6.

DHCPv4 serveren uddeler automatiske IP adresser fra en pulje af adresser i en begrænset periode som serveren bestemmer eller indtil klienten ikke længere har brug for adressen.



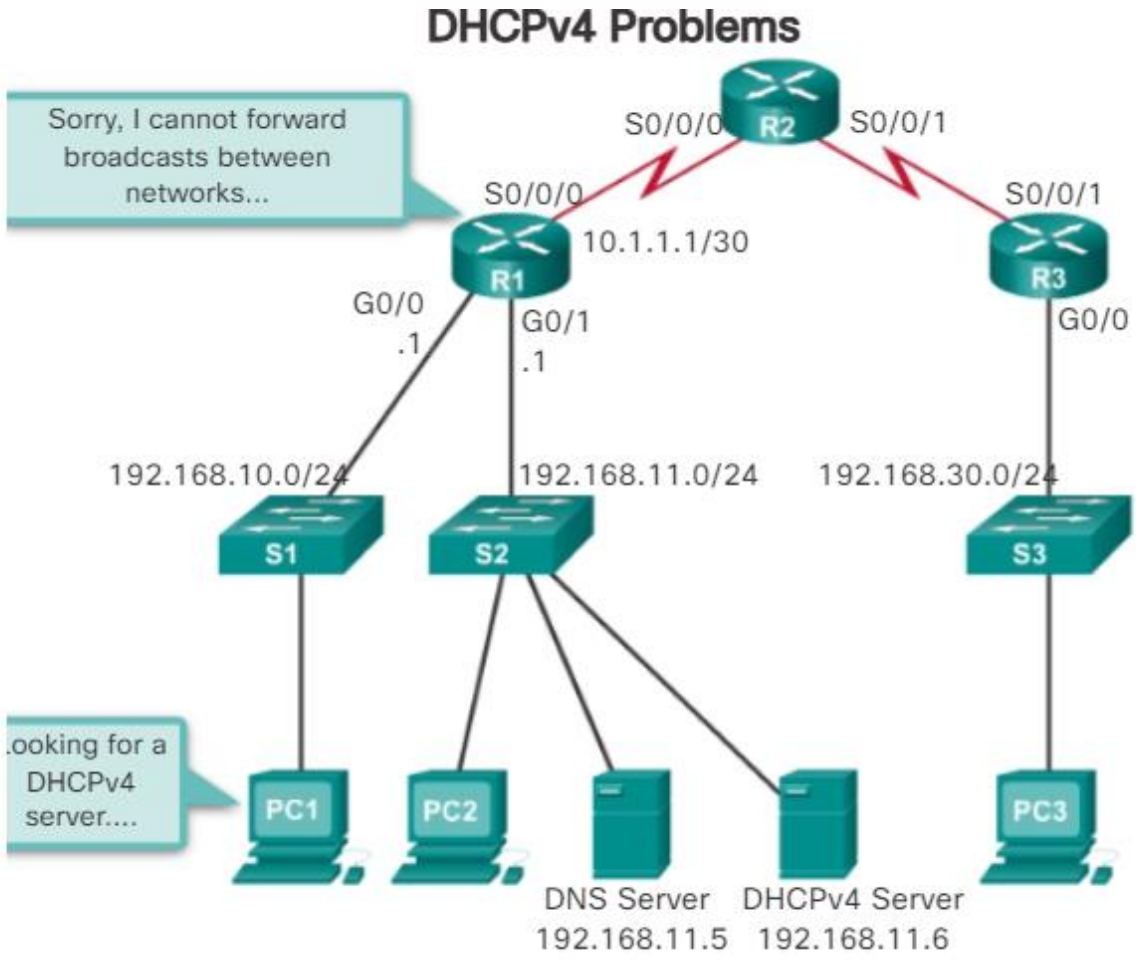
Uddeling af dynamisk IP adresse fra client til server, sted by step ser således ud:



En eller flere IP adresser kan ekskluderes fra adresse puljen, f.eks. da der typisk er nogle adresser der tildeles netværks enheder, som kræver statiske adresser. Dette gøres ved følgende kommando:

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
```

IP Helper address



Med udgangspunkt i ovenstående figur:

PC1 prøver at få deldelt en IPv4 adresse automatisk og sender et broadcast ud til en DHCPc4 server, men da routeren ikke kan forwarde broadcast møder PC1 modstand, da DHCPv4 serveren er på et anden netværk. Der er derfor brug for en ip helper adresse, som kan konfigueres på R1 – dette gør R1 til en DHCPv4 relay agent, og gøres ved følgende kommando:

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.11.6
<output omitted>
```

Nu kan R1 acceptere broadcast anmodninger for DHCPv4 service og frembringe de anmodninger som unicast til IP adressen 192.168.11.6, og dermed kan PC1 få tildelt en IP adresse.

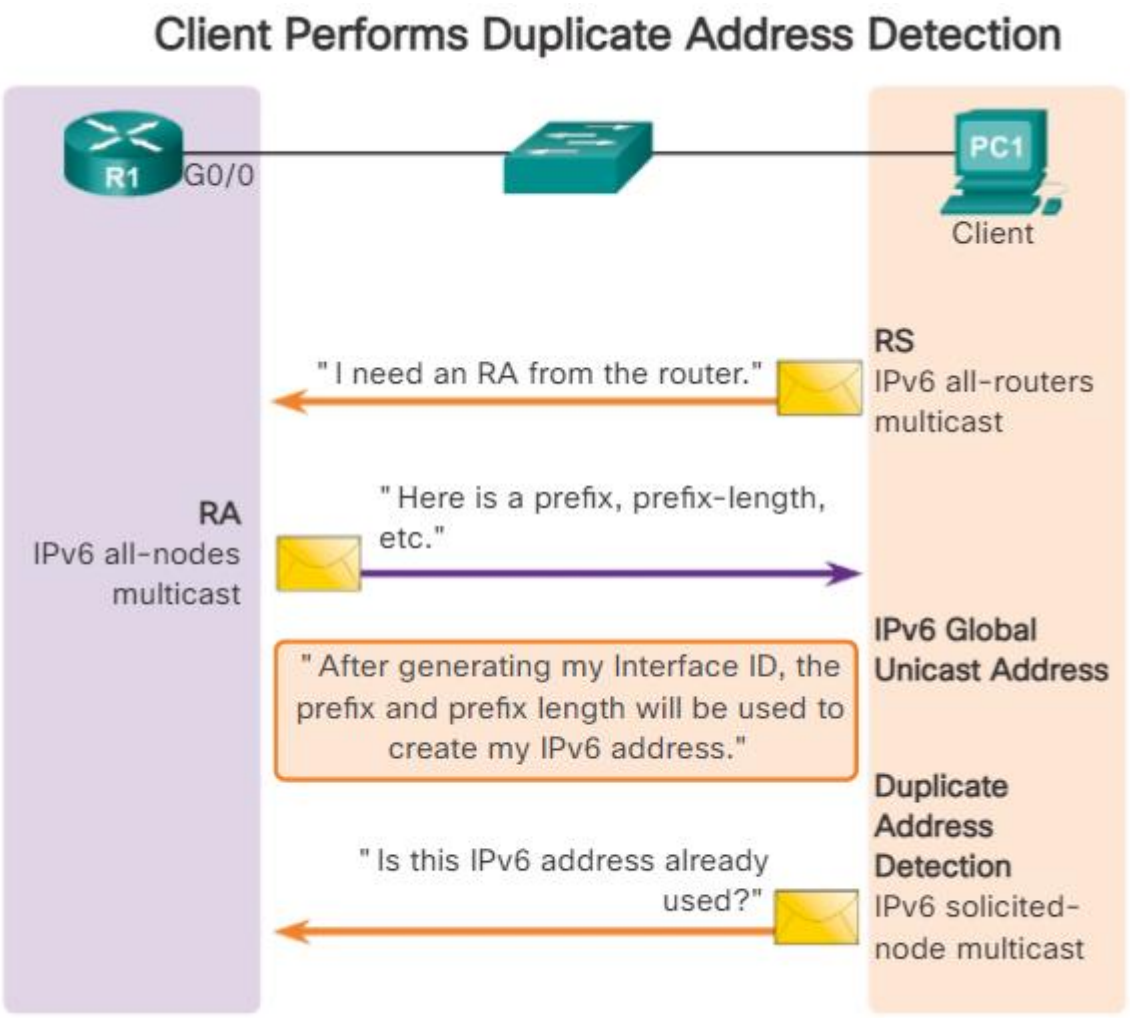
Routere kan også konfigureres som DHCPv4 clients, oftest i hjemmet eller mindre virksomheders netværk.

IPv6

Stateless Address Autoconfiguration

SLAAC er en metode hvor enheder kan få en IPv6 global unicast adresse uden en DHCPv6 server. Det er en stateless service som betyder at der ikke er en server som opretholder netværks adresse informationen, og en SLAAC server ved ikke, i modsætning til DHCP, hvilke IPv6 adresser der bruges og hvilke der er tilgængelige.

En router skal have IPv6 routing aktiveret for at kunne sende RA (Router Advertiement) beskeder.

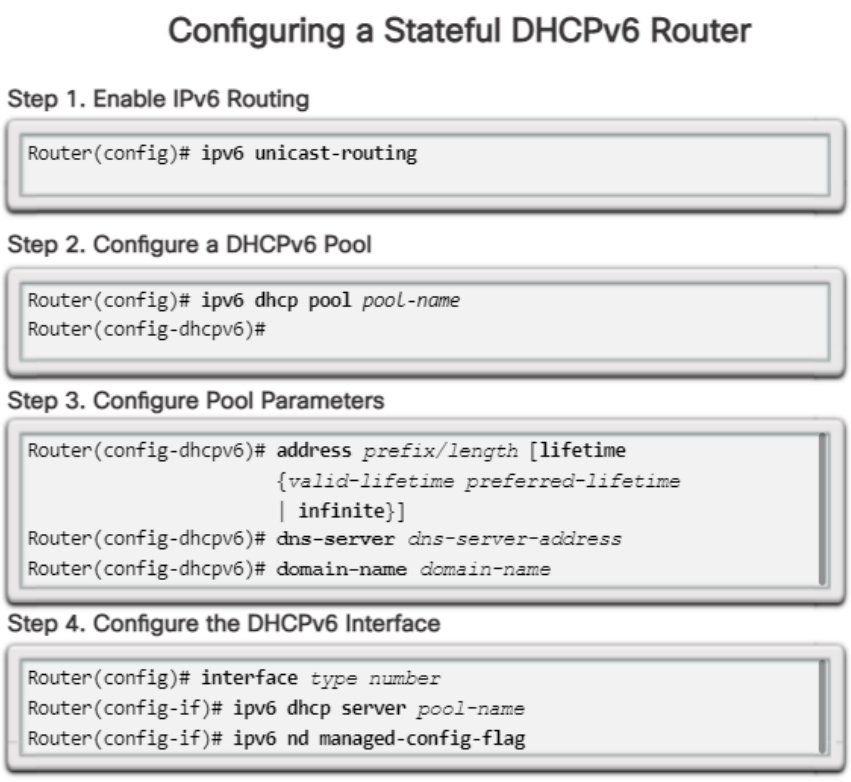


I figuren ovenfor er PC1 konfigureret til at få IPv6 adresse information automatisk, og efter PC1 starter op får den ikke en RA besked, så den sender en RS (Router Solicitation) besked til all-routerens multicast adresse for at informere den lokale IPv6 router at den mangler en RA.
Til sidst i figuren skal PC1 verificere at den nye IPv6 adresse er unik før den kan benyttes.

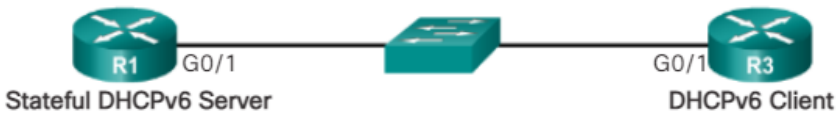
DHCPv6

Dette er en anden metode for dynamisk konfiguration af IPv6 global unicast adresser.

Hvor SLAAC er stateless, er DHCPv6 stateful. Stateful DHCPv6 ligner DHCPv4, og her informerer RA beskeden klienten om ikke at bruge informationen i RA beskeden. Al adresse- og DNS information fås fra en stateful DHCPv6 server.



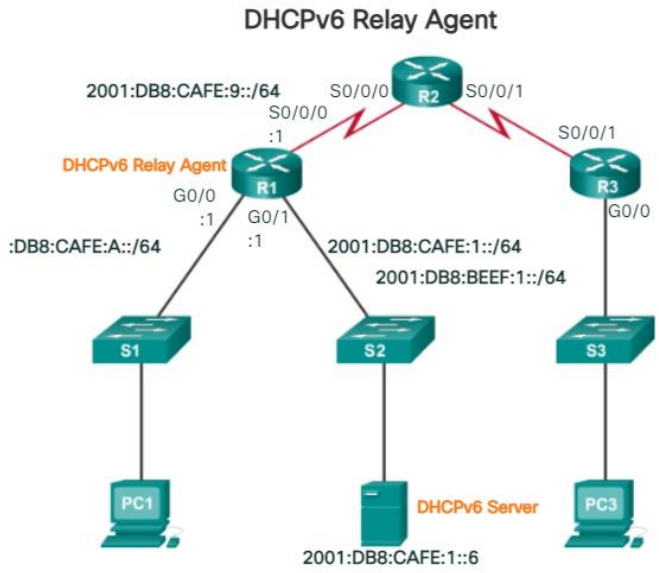
Configuring a Router as a Stateful DHCPv6 Client




```
R3(config)# interface g0/1
R3(config-if)# ipv6 enable
R3(config-if)# ipv6 address dhcp
R3(config-if)#
```

Relay

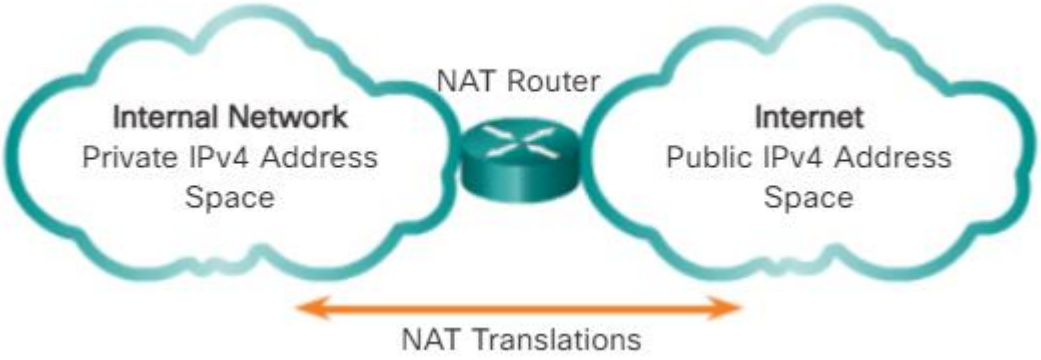
Hvis DHCP serverens er placeret på et andet netværks segment en DHCP klienten, er det nødvendigt at konfigurere en relay agent. Denne fremsender specifikke broadcast eller multicast beskeder inkl. DHCP beskeder, som kommer fra en host på en LAN segment, til en specifik server som ligger på et andet LAN segment. Det fungerer lidt ligesom ip helper adresse for IPv4.



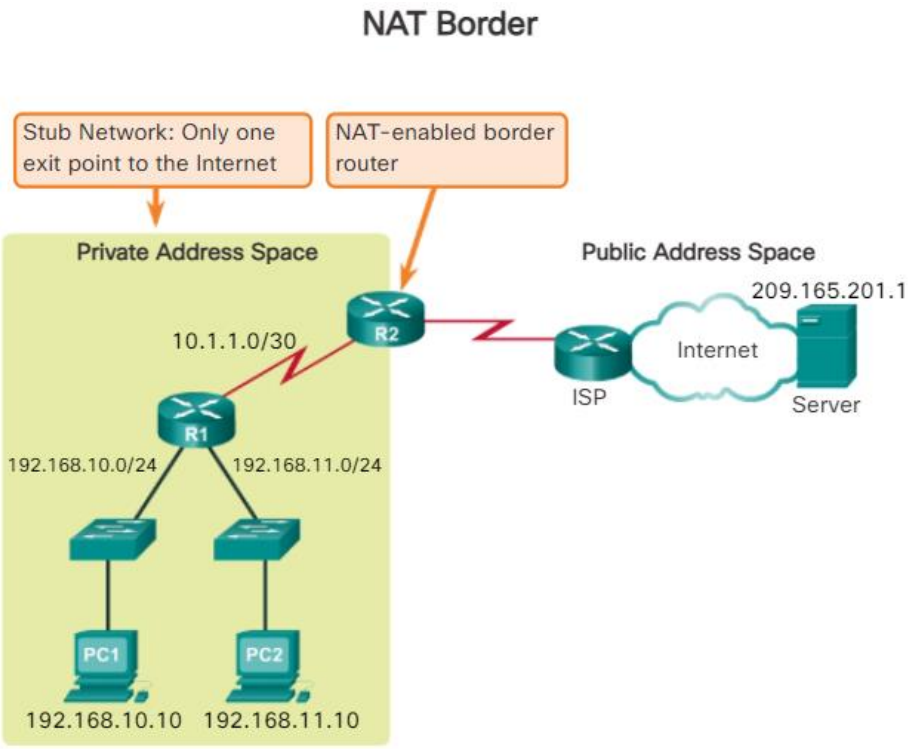

```
R1(config)# interface g0/0
R1(config-if)# ipv6 dhcp relay destination 2001:db8:cafe:1::6
R1(config-if)# end
R1# show ipv6 dhcp interface g0/0
GigabitEthernet0/0 is in relay mode
  Relay destinations:
    2001:DB8:CAFE:1::6
R1#
```

Kapitel 9 – NAT for IPv4

NAT gør det muligt at oversætte en privat IPv4 adresse til en public adresse, så de kan tilgå nettet uden for deres private netværk. Flere hundrede eller tusinder kan bruge den samme public adresse så længe de har konfigureret deres egen private IPv4 adresse, da man kun får tildelt en public adresse når man har brug for den. NAT har dermed reddet verden for at løbe tør på IPv4 adresser, uden den ville vi allerede før år 2000 være løbet tør for unikke adresser (Address Space) til alle de enheder som tilgår nettet.

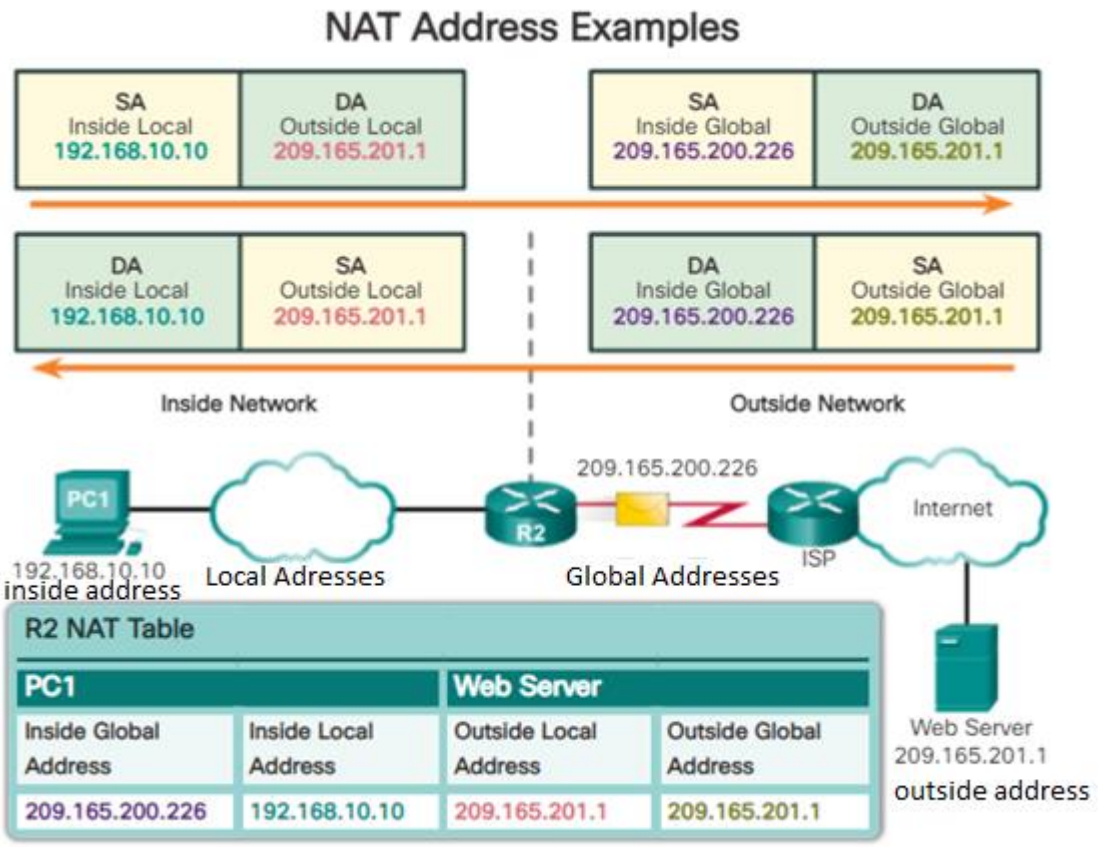


Der er dog en række begrænsninger for NAT. Disse begrænsninger sammen med den stadig stigende efterspørgsel på IPv4 adresser er grunden til at vi i sidste ende må overgå til IPv6.



NAT foregår på en NAT konfigureret router, typisk på grænsen af et ”stub netværk” (et netværk der kun har en enkelt indgang og udgang til netværket). NAT routeren konfigureres med en eller flere public IPv4 adresser, kendt som NAT pool. Når en enhed i Stub netværket vil kommunikere med en enhed uden for dens netværk bliver pakken sendt til ”grænse routeren”, som udfører NAT processen ved at oversætte den enhedens private adresse til en public adresse.

Eksempel på NAT networking:



Terminologi:

- **Inside Address -** Adressen på den enhed, der bliver oversat af NAT.
- **Outside Address -** Adressen på destinationsenheden.

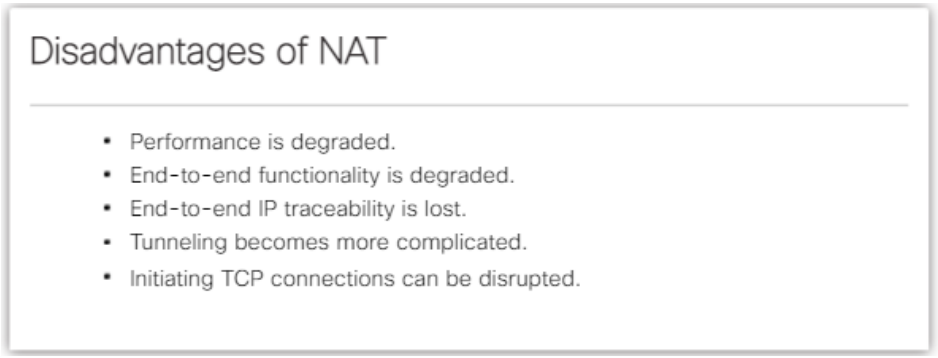
NAT bruger også begrebet lokal eller global med hensyn til adresser:

- **Local Address -** En lokal adresse er enhver adresse, der vises på den indvendige del af netværket.
- **Global Address -** En global adresse er enhver adresse, der vises på den ydre del af netværket.

Local og Global kombineres også med Inside og Outside, for at referere til specifikke adresser:

- **Inside local address -** Adressen på kilden set inde fra netværket.
- **Inside global address** - Kildens adresse set fra det eksterne netværk.
- **Outside global address** - Adressen på destinationen set fra det eksterne netværk.
- **Outside local address** - Adressen på destinationen set fra det indvendige netværk.

Ulemper ved NAT:



Kapitel 10 – Device Discovery, Management and Maintanance

Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) er en Cisco Layer 2-protokol, der bruges til at indsamle oplysninger om Cisco-enheder, der deler det samme datalink. CDP er medie- og protokol uafhængig og kører på alle Cisco-enheder, såsom routere, switches og adgangsservere.

Enheden sender periodiske CDP-advertisements til tilsluttede enheder, som så deler information om typen af enheden der opdages, som navnet og nummeret og typen af interfacet.

Med CDP aktiveret på netværket kan kommandoen show cdp neighbors bruges til at vise layouet på netværket.

Konfigurering af CDP:

Display the status of CDP on R1.

```
R1# show cdp
% CDP is not enabled
R1#
```

Enter Global Configuration mode to configure the following:

- **Enable CDP globally on R1.**
- **Disable CDP on interface S0/0/0.**
- **Use end command to exit Global Configuration mode.**

```
R1# configure terminal
R1(config)# cdp run
R1(config)# interface s0/0/0
R1(config-if)# no cdp enable
R1(config-if)# end
R1#
```

Display the list of CDP neighbors on R1.

```
R1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S1               Gig 0/1           122              S I   WS-C2960- Fas 0/5
```

Display more details from the list of CDP neighbors on R1.

```
R1# show cdp neighbors detail
```

Link Layer Discovery Protocol

Cisco-enheder understøtter Link Layer Discovery Protocol (LLDP), som er en neutral protokol til at opdage neighbouring netværk, og ligner CDP. LLDP fungerer med netværksenheder, såsom routere, switche og trådløse LAN-adgangspunkter. Denne protokol viser sin identitet og egenskaber til andre enheder og modtager oplysningerne fra en fysisk tilsluttet Layer 2-enhed.

LLDP konfigureres således:

Display the status of LLDP on R1.

```
R1# show lldp
% LLDP is not enabled
R1#
```

Enter Global Configuration mode to configure the following:

- **Enable LLDP globally on R1.**
- **Disable LLDP on interface S0/0/0.**
- **Use end command to exit Global Configuration mode.**

```
R1# configure terminal
R1(config)# lldp run
R1(config)# interface s0/0/0
R1(config-if)# no lldp run
R1(config-if)# end
R1#
```

Display the list of LLDP neighbors on S1.

```
S1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf     Hold-time  Capability      Port ID
R1                  Fa0/5          99         R               Gi0/1

Total entries displayed: 1
```

Display more details from the list of LLDP neighbors on S1.

```
S1# show lldp neighbors detail
```

Syslog

Den mest almindelige metode til at få adgang til systemmeddelelser er at bruge en protokol kaldet syslog.

Når visse hændelser opstår på et netværk, har netværksenheder funktioner til at underrette administratoren om detaljerede systemmeddelelser. Disse meddelelser kan enten være ikke-kritiske eller vigtige. Her har netværksadministratorer muligheden for at benytte syslog til at fortolke og vise disse beskeder og for at blive advaret om de beskeder, der kan have den største indvirkning på netværksinfrastrukturen.

Mange netværksenheder understøtter syslog, som routere, switches, servers og firewalls. For at se syslog beskeder skal der være installeret en syslog server på en arbejdsstation i netværket.

Syslog Severity Level

Severity Name	Severity Level	Explanation
Emergency	Level 0	System Unusable
Alert	Level 1	Immediate Action Needed
Critical	Level 2	Critical Condition
Error	Level 3	Error Condition
Warning	Level 4	Warning Condition
Notification	Level 5	Normal, but Significant Condition
Informational	Level 6	Informational Message
Debugging	Level 7	Debugging Message

Device maintenance

Enheds vedligeholdelse omfatter sikring af, at Cisco IOS-images (indeholder den systemkode, som routeren bruger til at fungere) og IOS-konfigurationsfiler sikkerhedskopieres på et sikkert sted i tilfælde af, at enhedens hukommelse beskadiges eller slettes, enten ondsindet eller utilsigtet.

OSI-modellen

OSI model		
Layer	**Name**	**Example protocols**
7	Application Layer	HTTP, FTP, DNS, SNMP, Telnet
6	Presentation Layer	SSL, TLS
5	Session Layer	NetBIOS, PPTP
4	Transport Layer	TCP, UDP
3	Network Layer	IP, ARP, ICMP, IPSec
2	Data Link Layer	PPP, ATM, Ethernet
1	Physical Layer	Ethernet, USB, Bluetooth, IEEE802.11

OSI-modellen (Open Systems Interconnection Reference Model) består af 7 lag som hver især beskriver kommunikation og netværksprotokoller mellem lagene.

- **Layer 1 – Det fysiske lag**, definerer alle de fysiske komponenter og rammer som netværks elementer består af. Dette kan være alt fra stik-type til netværkskortet i en enhed.
- **Layer 2 – Data Link**, består bl.a. af protokoller som PPP, ARP og LLDP. Dette lag gør det muligt at overføre data mellem netværks-enheder.
- **Layer 3 – Netværks laget**, består af protokoller som IP, ARP og ICMP. Laget gør det muligt at sende datablokke fra en kilde til en destination via et eller flere netværk, og er også her routere og layer 3 switche opererer.
- **Layer 4 – Transport laget**, består af protokoller som TCP, UDP og SCTP. Det er her dataoverførsler mellem brugere foregår og her tjekket pålideligheden af forbindelser via flowkontrol og fejlkontrol.
- **Layer 5 – Session**, består af protokoller som PPTP, SCP og NetBios, og fungerer som brugerens interface til netværket. Laget håndterer sessioner mellem applikationer og kontrollerer data transmissioner.
- **Layer 6 – Præsentations laget**, består af protokoller som SSL, TLS, AFP og NCP. Dette lag er måske det vigtigste i OSI-modellen, og konverterer data til et acceptabelt format som kan læses af applikations laget (Layer 7).
- **Layer 7 – Applikations laget**, består af protokoller som HTTP, FTP, DNS og DHCP. Det er dette lag der fungerer som brugerens interface til programmer så man har adgang til information på netværket.

Subnetting FLSM/VLSM

Subnetting er en måde hvorpå man kan opdele et IP netværk, og bruges bl.a. for at gøre det mere overskueligt, nemmere at administrere og mere effektivt at håndtere større netværk f.eks. i store virksomheder med mange netværksenheder.

Subnetting opdeles i to versioner: FLSM og VLSM. Ved FLSM (Fixed length subnet masking) opdeles netværket i lige store dele og hvert subnet har lige mange hosts, men ved brug af VLSM (Variable length subnet masking) kan netværket opdeles i forskellige størrelser så det tilpasses netværkets krav.

Subnet	**1**	**2**	**4**	**8**	**16**	**32**	**64**	**128**	**256**
Host	256	128	64	32	16	8	4	2	1
Prefix	/24	/25	/26	/27	/28	/29	/30	/31	/32
Subnet mask	.0	.128	.192	.224	.240	.248	.252	.254	.255

Denne tabel giver et overblik over hvor mange host der kan være i de respektive subnets, og kan defineres ud fra prefix/subnet mask. Der skal altid tages højde for at der bruges én host til netværket (den første) og én host til broadcast (den sidste) i hvert subnet. Dvs. en prefix /30 har plads til 4 host, men da to af dem allerede er afsat til netværks og broadcast adresse, er der kun to adresser tilbage til andre enheder.

Eksempel på subnetting med FLSM

Vi får tildelt netværksadressen 192.168.10.0/24 og skal opdele det i fire subnets. I tabellen finder jeg under subnet ”4”, og ser at der kan være 64 hosts på hvert af de fire netværk. Det betyder derfor at subnetmasken kommer til at hedde /26 for hvert subnet og subnetmasken kommer til at hedde 255.255.255.192. Tabellen for de fire subnets kommer til at se således ud:

Netværks navn	Number of Hosts	Prefix	Netværks adresse	Host Range	Broadcast adresse	Subnet Adresse
1	64	/26	192.168.10.0	192.168.10.1 - 192.168.10.62	192.168.10.63	.192
2	64	/26	192.168.10.64	192.168.10.65 - 192.168.10.126	192.168.10.127	.192
3	64	/26	192.168.10.128	192.168.10.129 - 192.168.10.190	192.168.10.191	.192
4	64	/26	192.168.10.192	192.168.10.193 - 192.168.10.254	192.168.10.255	.192

Eksempel på subnetting med VLSM

Vi får tildelt samme netværksadresse 192.168.10.0/24, men får nu at vide at netværket skal opdeles i 3 netværk. Det første netværk skal have plads til 32 hosts, det andet skal have 8 og det tredje skal have 30.

Man starter altid med det største netværk og fortsætter med det andetstørste, ned til til mindste netværk til sidst.

Da det største netværk skal bruge 32 hosts (netværk 1) skal vi afgøre hvor stort netværket skal være. Da der skal benyttes to hosts til netværksadressen og broadcast er det derfor ikke nok at bruge prefix /27, da det kun efterlader os med 30 brugbare hosts og er derfor nødsaget til at øge kapaciteten til den næste i rækken som er 64. Dette giver en prefix /26. Det næstestørste netværk kræver 30 hosts (netværk 3), og her er prefix /27 nok, og det sidste netværk (netværk 2) kræver en prefix /28 for at have plads til 8 brugbare hosts.

Vores subnets kommer dermed til at hedde følgende:

Netværks navn	Number of Hosts	Prefix	Netværks adresse	Host Range	Broadcast adresse	Subnet Adresse
1	64	/26	192.168.10.0	192.168.10.1 - 192.168.10.62	192.168.10.63	.192
3	32	/27	192.168.10.64	192.168.10.65 - 192.168.10.94	192.168.10.95	.224
2	16	/28	192.168.10.96	192.168.10.97 - 192.168.10.110	192.168.10.111	.240

Der skal typisk også indgå en eller flere routere for at netværkene kan kommunikere med hinanden og forbindes i form af WAN netværk som kræver 2 hosts. Derfor skal WAN'et bruge et netværk der rummer 4 hosts, som betyder et subnet .252 eller en prefix /30 (da der stadig skal taget højde for netværks adressen og broadcast adressen).

Når disse inkorporeres i tabellen kommer subnettet til at se således ud med tre routere, som forbinder LAN'ene gennem to WAN.

Netværks navn	Number of Hosts	Prefix	Netværks adresse	Host Range	Broadcast adresse	Subnet Adresse
LAN1	64	/26	192.168.10.0	192.168.10.1 - 192.168.10.62	192.168.10.63	.192
LAN3	32	/27	192.168.10.64	192.168.10.65 - 192.168.10.94	192.168.10.95	.224
LAN2	16	/28	192.168.10.96	192.168.10.97 - 192.168.10.110	192.168.10.111	.240
WAN1	4	/30	192.168.10.112	192.168.10.113 - 192.168.10.114	192.168.10.115	.252
WAN2	4	/30	192.168.10.116	192.168.10.117 - 192.168.10.118	192.168.10.119	.252

(måske er WAN ikke helt optimalt i forhold til hvad man burde gøre, kan være seperate WANs fra LANs, så de ikke er på 192.168.10.0 netværket)

Packet Tracer & CLI

Packet tracer er et program udviklet af Cisco Systems til at simulere alle aspekter af netværksopsætning. I programmet kan man bl.a. tilføje enheder som PC'er, routere og switche og konfigurere og forbinde dem som ønsket. Routere og switche kan f.eks. konfigureres via CLI (Command Line Interface). I CLI'en foregår kommandoerne i forskellige modes alt efter hvad der skal konfigureres:

- **User EXEC mode**, er standard mode efter man har startet routeren op, og vises ved "Router >"
- **Privileged EXEC mode**, tilgås ved "enable" kommandoen, vises ved "Router#".
- **Global Configuration mode**, tilgås via "configure termial" kommandoen, vises som "Router(config)#".
- **Interface Configuration**, tilgås ved at skrive "int" efterfulgt af det ønskede interface man vil konfigurere, så f.eks. "int s0/0/0" tilgår interfacet på serial 0/0/0, og vises som " Router(config-if)#".

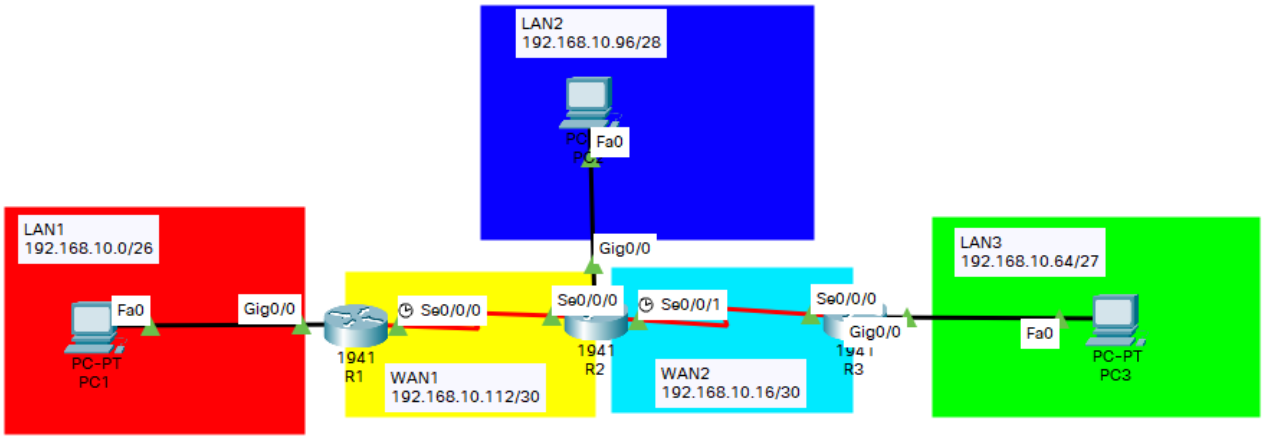
Eksempel på CLI konfiguration af router

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R3
R3(config)#int s0/0/0
R3(config-if)#ip add 192.168.10.118 255.255.255.252
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
```

Eksempel på topologi i Packet Tracer



Konklusion

Jeg har fået opfrisket alle emnerne fra grundforløbet, samt lært om nogle nye begreber og skrevet noter/referater af kapitlerne i bogen ”Routing and Switching Essentials”. OSI modellen er blevet gennemgået og derudover har jeg forklaret og lavet eksempler på Subnetting i form af FLSM og VLSM, samt demonstreret konfigurationer i CLI på en router i Packet Tracer.