

# Netwerk Fundamentals

## Les 1

- Circuit-switched network
  - o Één pad gekozen voor elke verbinding
  - o Alle data gaat langs zelfde pad
- Packet-switched network
  - o Pakket bevat adres en kan zelf een weg door het netwerk vinden
  - o Meerdere pakketten van verschillende gebruikers langs zelfde route
  - o Meerdere paden naar bestemming mogelijk
    - Als één pad wegvalt, zijn de andere nog beschikbaar
    - Lading verdeling over verschillende paden
  - o Pakketten komen niet in volgorde aan, wat nadelig is
- Eigenschappen van een goed netwerk
  - o Fault Tolerance
  - o Scalability
  - o Quality of Service (QoS)
  - o Security
- QoS: Quality of Service
  - o Geeft aan welke pakketten zeker moeten doorkomen, voorrang krijgen
    - Vb.: bij het laden van een webpagina en het streamen van een video, heeft het streamen een voorkeur

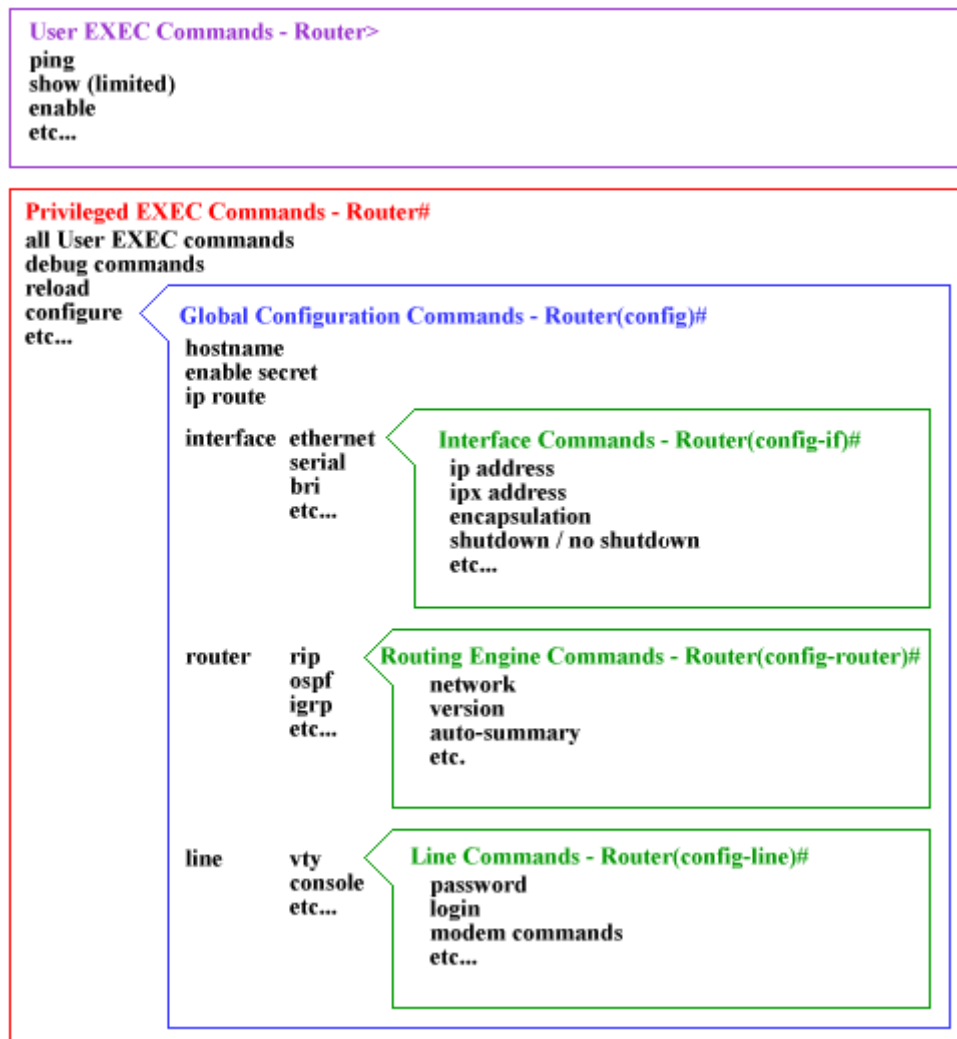
## Les 2

- Regels in een netwerk
  - o All devices within a network must have the same network address
  - o All devices within a network must have a different host address
  - o All devices within a network must have the same subnet mask
- Subnet mask CIDR notation: geeft weer hoeveel enen er zijn aan het begin de van de ip adres in bits
- Adres waar alle host bits 0 zijn (vb.: 192.168.1.0) kan niet worden gebruikt. Dit is het netwerk adres.
- Adres waar alle host bits 1 zijn (vb.: 192.168.1.255) kan ook niet worden gebruikt. Dit is het broadcast adres.
- Ping kijkt eerst of het ip adres op zijn eigen netwerk ligt door te kijken naar de subnet mask.
- Als je verbinding wilt maken buiten je eigen netwerk, moet je door de default gateway. In de meeste gevallen is dit je router.
- Je router heeft twee ip adressen omdat de router twee netwerken met elkaar gaat verbinden (heeft twee netwerk interfaces).
- WeTransfer Server verdeelt de data in kleine pakketjes.
  - o Door andere pakketjes er tussen te plaatsen kan de gebruiker meerdere dingen doen over dezelfde lijn.
  - o Aan de pakketjes wordt extra data toegevoegd.
  - o Alle pakketjes kunnen hun eigen weg vinden via het netwerk. Daarom is een volgordenummer nodig wanneer de pakketjes weer worden samengesteld.

- Deze server krijgt veel pakketjes binnen en zal eerst kijken of de bestemming voor zijn server is of niet.

### Hoofdstuk 3: Introduction to Cisco IOS (internetwork operating system)

- De poorten van de router staan standaard dicht als ze niet zijn ingesteld. Die van een switch staan wel open.
- L3 switchen zijn iets intelligenter en hebben zowel switch capaciteiten als router capaciteiten.
- Toegang tot software van switch via seriële kabel, dan van serieel naar USB (er is een speciale service port hiervoor aanwezig RJ45, maar is geen netwerk kabel, vaak achteraan de switch aanwezig (CONSOLE PORT))
- telnet gaat via plain tekst en is niet veilig -> beter SSH gebruiken
- AUX is een netwerk waarom je kan inbellen voor als het netwerk via de console port (SSH of telnet) niet meer toegankelijk is.
- Modes: symbool duidt aan in welke mode je zit
  - User mode (Router>): kan enkel ping doen en wat simpele dingen bekijken
  - Privileged mode (Router#): vooral voor de configuratie te bekijken of te debuggen
  - Configuration mode (Router(**config**)#)
    - Config: globale config
    - Config-if: configuratie voor een bepaalde interface; elke interface heeft zijn naam; config-if-NAAM
    - Config-line: configuratie van de binnenkomende lijnen
- Labo: altijd **cisco** of **student** als wachtwoord gebruiken
  - Privileged mode: switch>enable
  - Config mode: switch#conf t (of configure terminal)
- Wachtwoord staat er als gewone tekst in -> service password encryption
- Switch gaat alle commando's van de configuratie een voor een uitvoeren
  - running-config (staat op ram)
  - startup-config (staat op vast geheugen)
  - als de switch uitvalt, zal de running-config weg zijn en zal de startup-config op de ram worden gezet
  - je kan de running-config ook opslaan als startup-config
- OS van switch word op RAM gezet, daarom duurt het zo lang om een switch te starten
  - Eerst worden er nog enkele testen uitgevoerd
- #reload: running-config zal weg gaan en startup-config zal worden geladen
- #write erase: verwijdert de startup-config -> dit is altijd de eerste stap bij het labo -> reload om de running-config van de RAM te verwijderen
- Switch werkt standaard niet met Ip adressen en heeft zelf ook geen IP
  - Wel zijn er virtuele interfaces (Vlan)
- Backup maken van config-bestand kan via Putty of tftp server



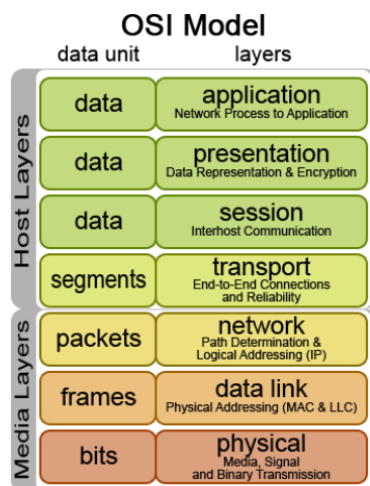
## Les 3

### Hoofdstuk 4: network protocols

- Pakketjes moeten worden encapsuled
  - o Extra data toevoegen aan pakketjes
- Als twee mensen op hetzelfde moment beginnen te praten: collision
  - ➔ Stop alle twee met praten en probeer opnieuw
- Je kan de pakketjes groter maken, maar kunnen te groot worden
  - ➔ Flow control: zorgen dat iedereen de pakketjes kan ontvangen (niet te snel, niet te traag)
- Response als pakketje is ontvangen, maar timeout om niet te lang blijven wachten. Het kan sneller zijn om een nieuw pakketje te sturen dan te blijven wachten
  - ➔ Response timeout
- Soorten message delivery options
  - o Unicast: one to one
  - o Broadcast: one to all
  - o Multicast: one to many (vb. videostreaming)
    - Aanmelden bij multicast adres zodat de source ook de pakketjes naar dat toestel gaat sturen.

- Bij sluiten van stream zal er weer een berichtje naar de source worden gestuurd en wordt de verbinding verbroken.
  - Anycast: one to closest
    - Vooral bij ipv6
    - Meerdere ip adressen met zelfde adres -> gaat op zoek naar een ip dat het dichtste bij de source zit
- Verschillende protocols
  - Networking protocols: HTTP, HTTPS, IP, FTP, DHCP, DNS, ...
    - DNS: netwerkadressen omzetten in IP-adressen
  - TCP: transmission control protocol
    - Betrouwbaar: zorgt er voor dat elk pakket wordt ontvangen door een bevestiging terug te sturen als het pakketje is ontvangen
    - Hierdoor is het wat trager want er worden ook pakketjes teruggestuurd
  - UDP: User Datagram Protocol
    - Stateless
    - Geen pakketjes teruggesturen
    - Gewoon snel de pakketjes blijven sturen (vb. videostreaming)
- Slide 17: voor volgend jaar
- OSI model: elke laag heeft zijn eigen verantwoordelijkheid
  - Application protocol: protocollen die door applicaties kunnen worden gebruikt (HTTP)
    - Hier is het niet belangrijk hoe de enen en nullen worden verzonden.
    - HTTP maakt gebruik van TCP
    - Werkt van applicatie naar applicatie, weet niet wat er tussen zit
    - Chrome (of besturingssysteem) zet HTTP pakketje om naar TCP pakketje
  - Transport protocol: TCP
    - Werken met poortnummers die gelinkt zijn naar bepaalde applicaties
      - Source poort: geeft de OS een bepaalde poort
      - Destination port is standaard 80 (op de dataserver)
    - Maakt gebruik van IP
  - Network protocol: IP
    - Ipv4 of ipv6
    - Is verantwoordelijk voor de communicatie tussen 2 IP-adressen
    - Maakt gebruik van Ethernet
  - Data link protocol:
    - Is verantwoordelijk voor de communicatie tussen de verschillende toestellen (vb.: router -> DNS -> DNS -> router -> webserver)
    - Dit is de Ethernet
  - Fysieke laag
- OSI packet header: extra informatie toevoegen
  - Chrome genereert een pakketje met HTTP protocol
  - TCP gaat poortnummers toevoegen voor te bepalen van welke applicatie komt mijn pakketje en naar welke applicatie moet het heen
  - IP gaat IP-adressen toevoegen
  - Ethernet gaat MAC adres toevoegen (dit adres is toestel gebonden)
    - MAC adressen worden gebruikt in eigen netwerk
- Bij return van data zullen de poorten en IP-adressen worden omgewisseld (source <-> destination)

- Slide 20
  - o ICMPV4 gebruikt bij ping berichten
  - o Niet alle protocollen kennen op afbeelding
- SMTP: email versturen
- POP, IMAP: email ontvangen
- TFTP: werkt via TCP met plain tekst (onveilig)
- Voice over IP: gaat eerst DHCP server zoeken en krijgt TFTP server terug met extra info over belserver, ...
- Slide met protocollen niet allemaal uit het hoofd leren
- Slide 36
  - o Eerste kijken of destination ip-adres op eigen netwerk zit
    - Werken met data link addresses (MAC adressen)
  - o Zoniet doorsturen naar default gateway = router
    - router is verbinding met het internet
    - router kijkt naar MAC adres en ziet dat het zijn MAC adres is, maar niet zijn IP adres
    - de router zal de destination MAC adres verwijderen en een nieuwe MAC adres toevoegen
    - MAC adres van pakketje wordt dus de hele tijd gewisseld



- The application layer provides the means for end-to-end connectivity between individuals in the human network using data networks.
- The presentation layer provides for common representation of the data transferred between application layer services.
- The session layer provides services to the presentation layer to organize its dialogue (dialog control) to manage data exchange.
- The transport layer defines services to segment, transfer, and reassemble the data for individual communications between the end devices.
- The network layer provides services to exchange the individual pieces of data over the network between identified end devices.
- The data link layer protocols describe methods for exchanging data frames between devices over a common media.
- The physical layer protocols describe the mechanical, electrical, functional, maintain, and de-activate physical-connections for bit transmission to and from a network device.

## Les 4

### Hoofdstuk 5: Network access and the physical layer

- Gaat nu over enen en nullen. Er zijn drie vormen van media:
  - o Koper: hoog laag
  - o Vezel: signaal patronen
  - o Draadloos: frequentie modulatie

#### koper

- Hoe enen en nullen doorsturen
  - o Encoding
    - **Manchester:** opgaande is 1; neergaande is 0
      - Dit is oud

- Nadeel is dat voor 2 enen of nullen na elkaar er dus een puls nodig is
  - Beter: **Non-Return to Zero**
- Er is ook een bepaalde tijd nodig dat er van 1 -> 0 en van 0 -> 1
- Hierdoor kan je de signalen niet heel dicht bij elkaar zetten
- Modulatie (draadfrequentie nodig waar signaal op wordt gezet)
  - Dit zorgt voor minder invloed van storing (ruis)
  - Signalen met een lagere frequentie hebben een lagere energie en kunnen minder ver gaan
  - Signalen met een hoge frequentie hebben een hogere energie en kunnen verder
  - Meerdere signalen over een kabel
    - Luisteren naar een bepaalde frequentie waar jouw data op zal komen
  - Am
    - Draaggolf heeft lage frequentie, signaal heeft hoge frequentie
    - Het is mogelijk om een bepaalde amplitude te filteren en daarvan de amplitude te bekijken
  - FM
    - De frequentie zal wijzigen
  - Fase modulatie
    - Bij 1 gaan de golf eerst omhoog (of omgekeerd)
- Bij internet gaat download en upload over een verschillende frequentiebereik (bandbreedte)
- Bandbreedte gaat over bits per seconde; dit is de theoretische datasnelheid
- Throughput: wat je effectief over je kabel krijgt (als de verliezen er af zijn)
- Goodput = de snelheid waarmee data wordt verstuurd, zonder alle headers enzo
- Kabels zijn rond elkaar gedraaid om storingen (ruis) te verminderen
  - Als ze niet gedraaid zijn kan het zijn dat de kabel die het dichtst bij een storingsbron licht heel veel storing krijgt
  - Bij gedraaide paren zal de ruis afwisselend op de ene als op de andere kabel gaan
  - UTP: unshielded
  - STP: shielded -> connector moet van metaal zijn zodat deze kan verbonden worden met de ground
    - **U = Unshielded (niet afgeschermd)**
    - **F = Foil shielded (afgeschermd met folie)**
    - **S = Braided shield (gevlochten scherm)**
    - **TP = Twisted pair (getwiste aders)**
- Er zijn verschillende categorieën van kabel
  - Categorie bepaald door de eigenschappen van de kabels
    - Dikte van de kabels
    - Hoe dicht ze op elkaar zijn gedraaid

### Fiber kabels

- Werkt met lichtpulslen
- Zit glas in -> nooit knikken maken
- Je hebt ook multimode kabels (MMF en SMF)

- Van plastic
- Er zijn rechtgaande en botsende signalen
- Wachten op botsende signalen
- Iets trager
- Deze kabels worden aan elkaar gelast

### **Verschil**

- Waar mensen niet aan kunnen zullen fiber gebruikt worden, ander kopen

### **Draadloos**

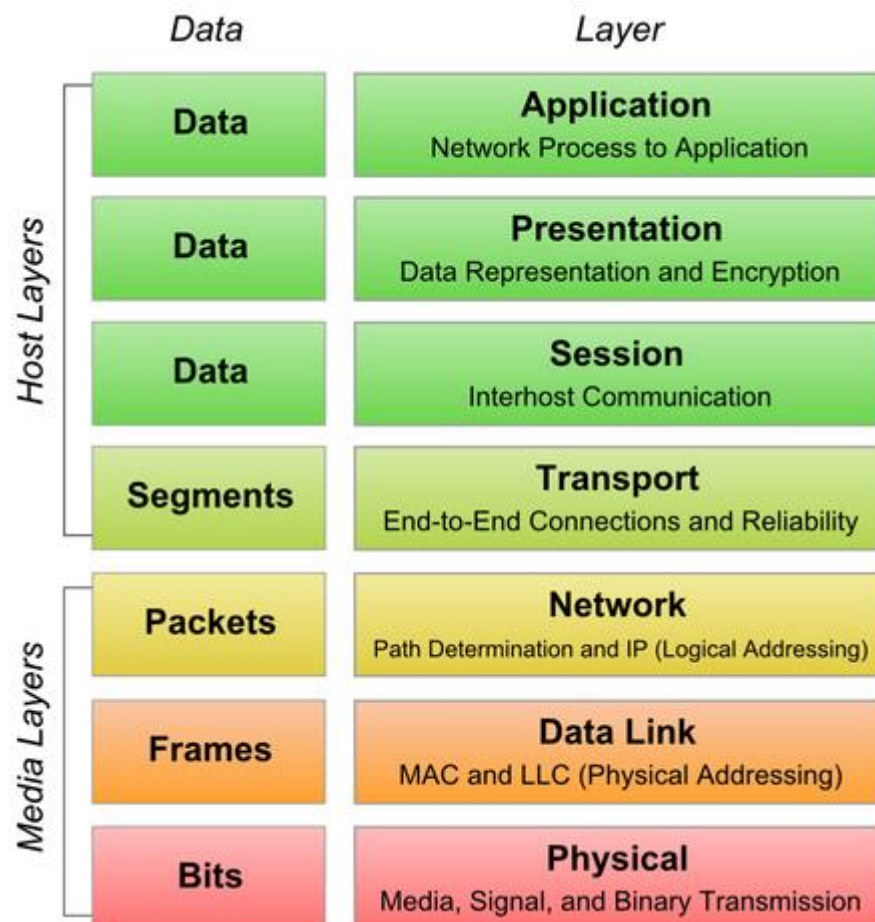
- Elektromagnetische straling
- Twee gebruikte frequentiebanden: 2.4GHz en 5GHz
- Er zijn verschillende standaarden: bepalen de snelheid
- Er zijn verschillende kanalen die je kan gebruiken, elk heeft zijn eigen draaggolf (SLIDE 44)
  - Alles wat onder de cirkel zit kan worden gebruikt
  - Er is hierbij wel overlap
    - Bij de overlapping weet men niet uit welk kanaal het kwam
    - Daarom kunnen er maar drie kanalen worden gebruikt zodat er geen overlap is (1, 6 en 11)
    - Overlap zoveel mogelijk vermijden in een gebouw door verschillende kanalen te kiezen (1, 6 of 11)

**Wat je moet weten is het verschil tussen UTP, FTP, STP kabel, het verschil tussen mono mode en multi mode fiber kabels en dat deze bestaan uit een glazen of plastiek fiber met een bescherming er rond ...**

### Hoofdstuk 6: data link layer and Ethernet

- Laag 1
  - Physical layer
  - Bits
- Laag 2
  - Overbrugging tussen fysieke laag en data link laag
- Ethernet protocollen: er zijn meerdere protocollen (SLIDE 8)
  - LLC (Logic Link Control) sublaag is de overgang met de OS (drivers)
    - Communicatie tussen software en fysieke hardware
    - Hier kan niet veel worden veranderd en wordt bepaald door OS
  - MAC (media access control) sublaag gaat over de software op fysieke controller (netwerk kaart)
    - Is verantwoordelijk voor het encapsuleren van de data die afkomstig is van de bovenliggende lagen
    - Deze zal encapsulation doen (toevoegen van de Ethernet header met onder andere de MAC adressen) en de-encapsulation (verwijderen van de Ethernet header). Wanneer een frame wordt verstuurd over een router zal deze router de het destination ip adres bekijken, in de routing table (waarin routes door het netwerk staan vermeld aan de hand van ip adressen) kijken naar welk ip adres dit moet worden doorgestuurd, in de arp table kijken welk mac adres hierbij hoort, en het nieuwe destination mac adres toevoegen aan het packet

- Verschillende toestellen op hetzelfde netwerk identificeren met een MAC adres: 48 bits, 12 hexadecimale getallen
- ➔ Header toevoegen met onder andere source en destination mac adressen
- ➔ Mac adressen zijn de adressen die op het niveau van de datalinklaag gebruikt gaan worden om frames te verzenden
  - Hier is er wel ruimte voor wijzigingen

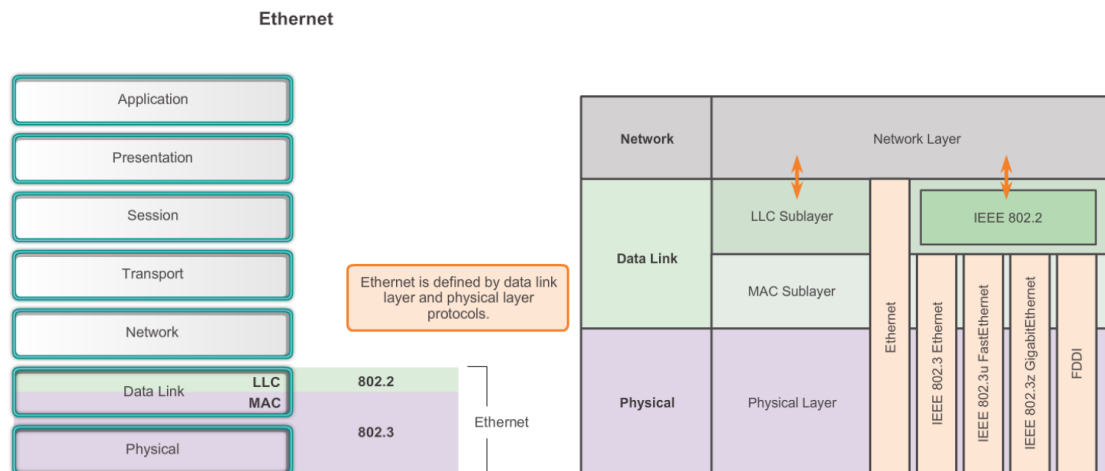


- SLIDE 22: type: verteld aan data link laag of het moet worden doorgestuurd naar IPv4 of IPv6
- 1500 bytes is een standaard maximale grootte
  - Do not fragment: pakket mag niet is stukken worden gedeeld
- MAC adressen
  - Zijn in principe ingebakken in de netwerk kaart
  - Adres van 48 bits of 12 hexadecimale getallen
    - Eerste 6 hex zijn fabrikant specifiek
    - Twee helft wordt door de fabrikant zelf bepaald
  - Deze adressen zijn altijd uniek
  - Drie vormen
    - Unicast MAC adres
      - Binnen één netwerk
    - Broadcast MAC adres: FF-FF-FF-FF-FF-FF
    - Multicast MAC adres
      - Begint met: 01-00-5E



## Toevoegingen

- Ethernet operates in the lower two layers of the OSI model: the Data Link layer and the Physical layer.



- Ethernet separates the functions of the Data Link layer into two distinct sublayers:
  - the Logical Link Control (LLC) sublayer
    - handles the communication between:
      - the upper layers (the networking software)
      - the lower layers (typically the hardware)
    - takes the network protocol data, which is typically an IPv4 packet, and adds control information to help deliver the packet to the destination node (frames the Network Layer packet)
    - identifies the Network Layer protocol
    - LLC communicates with the upper layers of the application and transitions the packet to the lower layers for delivery
  - the Media Access Control (MAC) sublayer
    - = the lower Ethernet sublayer of the Data Link layer
    - Media Access Control is implemented by hardware, typically in the computer Network Interface Card (NIC).
    - The Ethernet MAC sublayer has two primary responsibilities:
      - Data Encapsulation
      - Media Access Control
        - Responsible for the placement of frames on the media and the removal of frames from the media
        - Communicates directly with the physical layer
        - If multiple devices on a single medium attempt to forward data simultaneously, the data will collide resulting in corrupted, unusable data
        - Ethernet provides a method for controlling how the nodes share access through the use of a **Carrier Sense Multiple Access (CSMA)** technology
- There are two basic media access control methods for shared media:
  - **Controlled Access** (token ring, FDDI)
    - Toestellen mogen om de beurt data versturen
    - Mechanisme die bepaalt wie er wanneer mag zenden
      - Extra verkeer over netwerk nodig

- **Contention-based Access** (ethernet)
  - Alle toestellen zullen zelf kijken of er data over de kabel wordt verstuurd
  - Allow any device that has data to send to try to access the medium
  - To prevent complete chaos on the media, these methods use a Carrier Sense Multiple Access (CSMA) process to first detect if the media is carrying a signal
  - Possible that two devices or two nodes transmit at the same time
    - a data collision Data of both devices
    - corrupted and need to be resend
  - CSMA/COLLISION DETECTION (CSMA/CD)
    - all devices stop sending data
    - both devices wait each a random period of time
    - after this period of time (different!) each device looks again if the media is free
  - CSMA/COLLISION AVOIDANCE
    - used for wireless networks
    - If a data signal is present
      - media is not free
      - device waits for a random period of time and tries again
    - If a data signal is absent
      - media free
      - device sends a notification across the media to notify everyone that he will send data across the media
      - The device then sends the data
      - **Collisions are avoided!!**
        - Collisions van notifications kunnen wel voorkomen, maar geen collisions van data

→ Otherwise too much collisions

- LAYER 2 FRAME STRUCTURE
- **Header:** Contains control information, such as addressing, and is located at the beginning of the PDU.
  - Start Frame field: Indicates the beginning of the frame.
  - Source and Destination Address fields: Indicates the source and destination nodes on the media.
  - Type field: Indicates the upper layer service contained in the frame.
- **Data:** Contains the IP header, transport layer header, and application data.
- **Trailer:** Contains control information for error detection added to the end of the PDU.
  - **FCS** this field is used for error checking. The source calculates a number based on the frame's data and places that number in the FCS field. The destination then recalculates the data to see if the FCS matches.
  - Stop frame indicates the end of the frame when transmitted.

## Les 5: 17/03/2020 (video 1)

Hoe wordt data over een netwerk gestuurd?

- Eerst wordt de data gemaakt in de application layer en vervolgens via een protocol verstuurd (FTP, HTTP, Telnet, ...) -> GET request, POST request, ...
- Er wordt een request doorgestuurd naar de transport layer
  - Eerste protocol dat een header gaat toevoegen aan de data
    - Hier zitten onder andere de poortnummers in
      - De *destination port* wordt gebruikt om te zien welke applicatie deze data moet ontvangen (webserver, mail server, ...)
      - De *source port* wordt gebruikt om te zien naar welke applicatie er eventueel een antwoord moet worden verstuurd (Chrome browser)
  - TCP voor betrouwbare communicatie (beveiligd)
  - UDP voor niet betrouwbare communicatie (niet beveiligd)
- Dan wordt alles doorgestuurd naar IP laag
  - Deze gaat *source* en *destination* ip adressen toevoegen
- Dan wordt alles via de LLC doorgestuurd naar de MAC sublaag
  - Deze gaat *source* en *destination* MAC adressen toevoegen
  - Op dat moment noemen we het een frame

Verschillen tussen MAC en IP? Waarom niet altijd gewoon MAC of IP?

- MAC adressen veranderen in principe niet -> *burn in address in ROM*
  - Is door de fabrikant vastgelegd in de ROM
  - Dit noemt men ook wel het fysiek adres
  - Worden op laag 2 toegevoegd (data link layer)
- IP adressen kunnen worden gewijzigd
  - Het zijn logische adressen
  - Kan worden gewijzigd door bijvoorbeeld een netwerk administrator
  - Worden op laag 3 toegevoegd (network layer)

Wat is de bedoeling van het ARP (address resolution protocol)?

- Het ARP wordt gebruikt om het *destination mac address* te achterhalen
- 2 basic functies
  - IP adres koppelen aan mac adres
  - Tabel bijhouden van mac adressen en bijhorende IP adressen
    - Als we deze tabel niet bijhouden zouden we voor elke frame opnieuw het mac adres moeten zoeken
- ARP request wordt op het netwerk verstuurd om een mac adres te achterhalen
  - Dit is een broadcast bericht met als *destination mac address* FF-FF-FF-FF-FF-FF
    - Switch zal deze *request* doorsturen naar alle poorten waar een toestel mee is verbonden
    - Het *destination* toestel zal een *ARP reply* sturen naar de source
- ARP tabel bestaat uit de mac adressen met de overeenkomende ip adressen
  - Wordt standaard 5 minuten in RAM opgeslagen
  - Deze tabel kan op twee manieren ingevuld worden
    - Door ARP request (zie hierboven)

- Monitoren van binnenkomend verkeer
  - Elke binnenkomende frame bevat de source mac adres
    - In de ARP tabel staan enkel ip adressen die in het eigen netwerk liggen
- Als een frame moet worden verstuurd buiten zijn eigen netwerk, zal als destination mac adres het adres van de default gateway worden gebruikt

Hoe kan ARP voor problemen zorgen op een netwerk?

- ARP request is een broadcast -> extra data op netwerk
  - Als tabel sneller dan 5 minuten wordt gewist, worden er broadcasts gestuurd op het netwerk wat de bandbreedte van het netwerk verlaagd
- ARP spoofing
  - Als toestel A een ARP broadcast stuurt om het mac adres van toestel B te krijgen, maar een ander toestel C antwoordt met zijn mac adres eerder dan toestel B, dan wordt alle data naar toestel C gestuurd i.p.v. toestel B. Toestel C zal dit dan doorsturen naar toestel B zonder dat toestel A dit merkt (*man in the middle*)

Voorbeeld met ping

- Soms kan de eerste ping (ICMP packet) wat langer duren omdat er nog een ARP request moet worden gedaan
- Soms kan het zijn dat bij een ping naar een ander extern netwerk de eerste packets niet aankomen omdat de default gateway (router) het mac adres van de destination nog niet heeft het de pakketje laat vallen

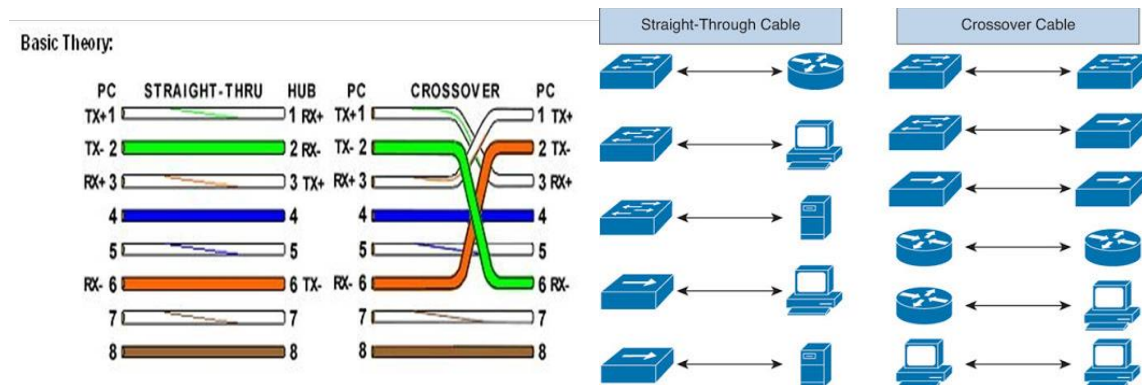
Hoe gaat een switch mac adressen gebruiken om zijn werking te optimaliseren?

- Het verschil tussen een switch en een hub:
  - Hub gaat alle frames/pakketen doorsturen naar alle poorten
    - Heeft geen intelligentie
    - Zorgt voor heel veel extra verkeer op het netwerk
    - Is ook slecht voor veiligheid
  - Een switch zal de frame enkel naar de poort waar de destination adres is sturen
- Functies van een switch?
  - Mac adressen leren
    - Zal elke binnenkomende frame bekijken en de source mac adres toevoegen aan zijn mac adres tabel
    - Als de destination mac adres nog niet is gekend door de switch, zal de switch de frame naar alle poorten moeten sturen, buiten de poort waar de frame is ontvangen -> **Flooding**
      - Dit is een unicast naar alle poorten
    - Als het mac adres wel gekend is -> **selective forwarding**
  - Aging
    - Mac adressen worden na een bepaalde tijd verwijderd uit de tabel
  - Flooding
  - Selective forwarding
  - Filtering
    - Het is mogelijk bepaalde frames niet door te sturen

Wat is het verschil tussen de ARP tabel en de mac adressen tabel?

- De arp table en mac address table zijn inderdaad verschillende tabellen. In de arp table staan ip adressen met bijbehorende mac adressen, in de mac address table staan mac adressen met bijbehorende poortnummers. Mac address tables worden gebruikt in switchen, arp tables worden gebruikt in routers en end-devices

## Soorten kabels



- In een switch zullen de TX en RX lijnen van plaats worden gewisseld (crossover)
- Op de meeste toestellen kan er automatisch worden bepaald of crossover nodig is of niet  
➔ mdix auto
- duplex settings
  - o half duplex: in een netwerk kan er maar data in één richting worden gestuurd
    - ofwel data ontvangen, ofwel data verzenden, maar niet ontvangen en verzenden gelijktijdig
    - Er zal dus de hele tijd moeten worden gewisseld tussen verzenden en ontvangen
  - o full duplex: kunnen zenden en ontvangen op hetzelfde moment

## Power over ethernet

- PoE switch kan ook stroom voorzien over de kabel
- Kan ook door een PoE injector te plaatsen

## Les 6: 24/03/2020 (video 2)

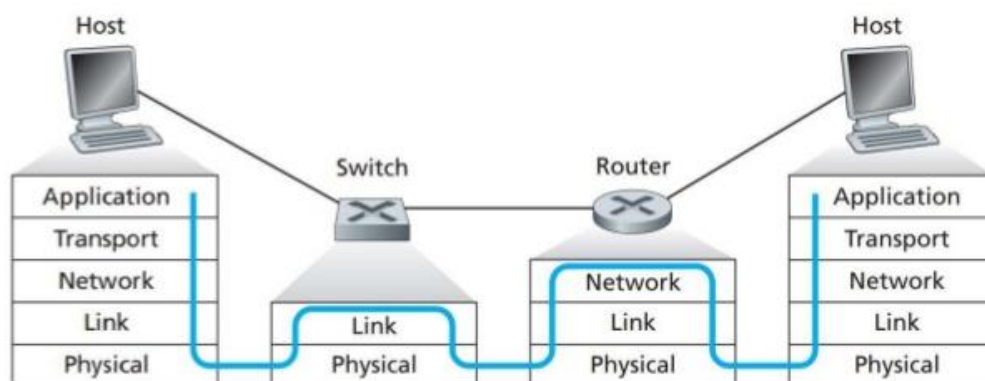
- Ip adressen worden gebruikt om de verschillende hosts op een netwerk te identificeren

## Circuit Switching Vs Packet Switching

Circuit Switching	Packet Switching
Physical path between source and destination	No physical path
All packets use same path	Packets travel independently
Reserve the entire bandwidth in advance	Does not reserve
Bandwidth Wastage	No Bandwidth wastage
No store and forward transmission	Supports store and forward transmission

3

- De netwerklaag zal de paden bij packet switching bepalen en in het oog houden
- Functies van de network layer:
  - o Zal de data van de transportlaag encapsuleren
    - Source en destination ip adressen toevoegen
    - Ook informatie over de route toevoegen
  - o Routeren van de pakketten door het netwerk
    - Source en destination zitten niet altijd op het zelfde netwerk
    - Zal dus soms door verschillende netwerken moeten reizen
    - Toestellen die dit doen: routers (ook wel een hop genoemd)
    - Switches werken met mac adressen op de data link laag <-> routers werken met ip adressen op de netwerk laag
  - o De-encapsulatie als pakketten zijn aangekomen bij de bestemming
    - Destination ip wordt bekeken
    - Als destination ip hetzelfde is als eigen ip, wordt het verder gestuurd naar de transport laag



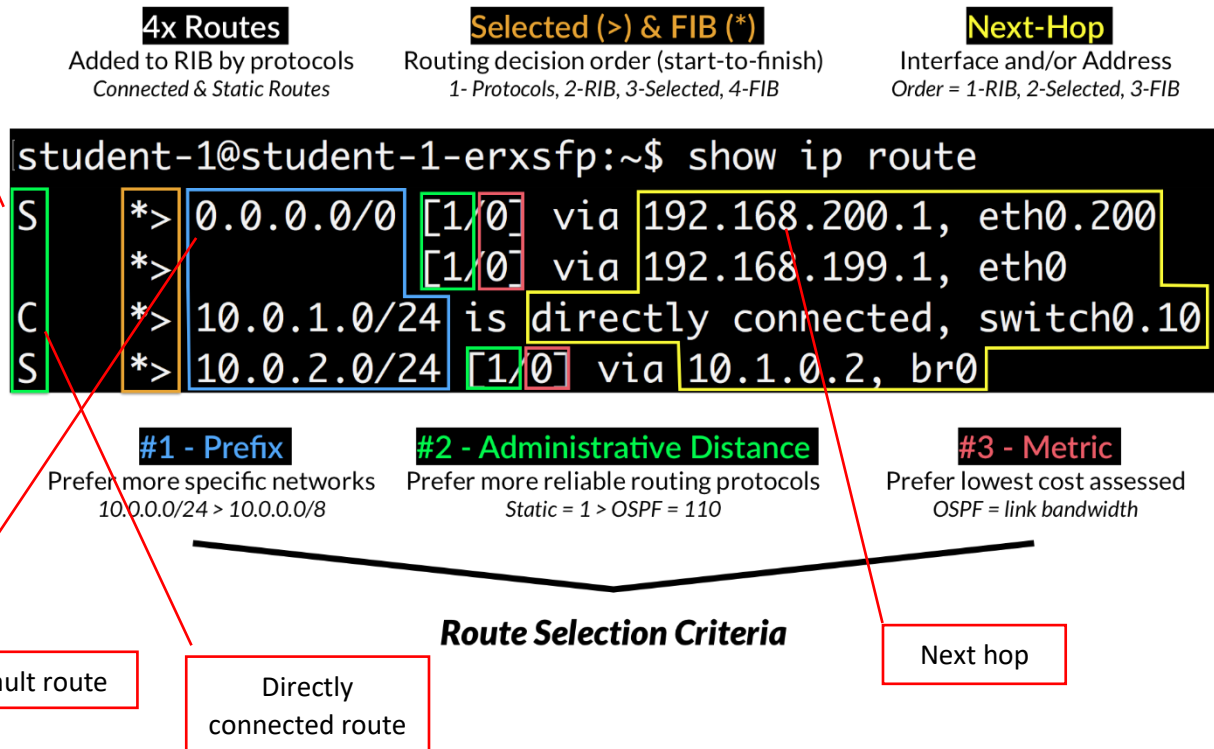
Wat is de verantwoordelijkheid van een router?

- Moet een map van een netwerk bouwen (in kaart brengen)
  - o Statische routes (manueel geconfigureerd)

- dynamische routes (aan de hand van dynamische routes protocollen)
- Routing tabel bijhouden
  - Welke netwerken bereikbaar zijn via welke next hop en via welke interface

Statische route

## Sample Router's Routing Information Base (RIB)



- Default route: als de route niet wordt gespecificeerd, zal het via de default route worden gestuurd
- Administrative distance: hoe lager, hoe meer voorkeur deze router krijgt
  - Het is mogelijk dat er meerdere redundante routers zijn op een netwerk
- Directly connected route: een netwerk dat direct is verbonden met de router zelf
  - De router heeft zelf ook een ip op dat netwerk
- Routers kennen alternatieve paden naar bepaalde netwerken
- Routers gaan het netwerk monitoren en kijken naar wijzigingen in het netwerk
  - Dynamic routing protocols
    - elke router weet welke netwerken er rechtstreeks geconnecteerd zijn
    - praat met de routers die naast hem liggen
    - **OSPF**: kan speciale pakketten versturen om andere routers op de hoogte te brengen welke netwerken er direct met de router zijn verbonden
      - De routers gaan dan ook bijhouden hoeveel hops er tussen het netwerk zitten om de snelste route te bepalen
      - Als de statische route wegvalt (met administrative distance = 1), zal de OSPF route worden genomen (administrative distance = 110) om toch het pakket bij zijn bestemming te krijgen

## IPv4 en IPv6

- Karakteristieken van IP
  - Connectionless
    - IP houdt zich niet bezig met het nakijken op de pakketten zijn aangekomen (dat is de verantwoordelijkheid van het TCP of UDP protocol)
    - IP header is klein omdat er dus geen bevestigingsdata in zit -> minder bandbreedte
  - Best effort (onbestrouwbaar)
    - Geen garantie dat pakketten aankomen
    - Efficiënt omdat het niet bezig houdt met het aankomen van de pakketten
  - Media independent
    - Het is mogelijk dat de verschillende soorten media een verschillende maximale grootte (**maximum transmission unit (MTU)**) van de frames hebben -> **fragmentation**
- Encapsulatie
  - Header toevoegen aan de pakketten die we krijgen van de bovenliggende lagen
  - Data: transport layer **PDU** (protocol data unit = data van transport laag (= data van applicatie + **segment header**))
- IPv4
  - Informatie in de header IPv4
    - Version: binair getal 4
    - Differentiated service: voorrang geven voor bepaalde pakketten
    - Time-to-Live: bijvoorbeeld 128 -> elk toestel in het netwerk zal er één van afnemen; zo kan je voorkomen dat het pakket in een loop blijft vastzitten
    - Protocol: vb UDP of TCP
    - Source IP adres (end to end)
    - Destination IP adres (end to end)
    - Identificatie en fragment offset: als een pakket in meerdere delen moet worden gesplitst, hebben ze allemaal dezelfde identificatie, maar een verschillende offset
  - IPv4 adressen
    - $4 \times 8 \text{ bits} = 4 \times 1 \text{ byte} = 4 \times 0\text{-}255 \text{ decimaal}$
    - Max  $2^{32}$  adressen = ongeveer 4,29 miljard
  - Problemen
    - Alle adressen zijn bijna gebruikt
    - Routing tabellen worden heel groot
    - Niet meer end-to-end verbinden
      - Binnen een netwerk privé adressen die niet rechtstreeks bereikbaar zijn
  - Oplossingen
    - **NAT**: network address translation
      - Router heeft één publiek adres waar meerdere privé adressen achter staan
      - Router gaat source IP adres en poort vervangen door zijn eigen IP adres en poort
      - Router houdt tabel bij van mapping tussen het lokale netwerk en het publieke netwerk



- Vb.: 192.168.1.50:45684 = 10.59.48.68:80
  - Beperking: als de poorten op zijn, ... (max is **65535**)
- Gebruik maken van IPv6
  - Hebben 128-bit adressen t.o.v. 32-bit
  - Geen NAT meer nodig, dus terug end-to-end
  - Header is iets eenvoudiger
    - Routers kunnen de pakketten makkelijker en sneller doorsturen
  - Beveiliging is standaard geïmplementeerd
- IPv4 vs IPv6
  - Header van IPv6 is groter, maar het aantal velden is kleiner
    - Versie: 6
    - Traffic class: voorrang geven van bepaalde pakketten op andere pakketten
      - = IPv4 differentiated services
    - Next header: protocol van de bovenliggende laag
      - = IPv4 protocol
    - Hop limit
      - = IPv4 end-to-life
    - Source en destination IP: 128-bits
      - IPv4 heeft 32 bits

How a host routes?

- Naar zichzelf: localhost 127.0.0.1 = "loopback interface"
- Naar een host op het lokale netwerk
  - Destination IP adres is in hetzelfde netwerk
    - Hebben zelfde netwerk adres
    - Kan via ARP pakket routeren
- Naar een remote host
  - Verschillend netwerk adres
  - Pakket versturen naar de default gateway
    - Router zal de pakketten verder doorsturen

Elke host heeft ook een routing tabel

- Dit is om er voor te zorgen dat de pakketten naar het juiste netwerk worden gestuurd
  - Er zijn verschillende interfaces -> data moet naar de juiste interface worden gestuurd
- Bevat
  - Direct connection: loopback interface
  - Local network route: toestellen op het lokale netwerk
  - Local default route: de route om naar remote addresses te gaan (=adres van de default gateway)
- 0.0.0.0 -> alle adressen die niet gekend zijn, worden naar de default gateway gestuurd
- /32 adres -> is een intern adres van de router, zoals de loopback interface bij hosts
- **EIGRP** is net zoals OSPF een protocol om de dynamische adressen te krijgen

Hardware router

- Router heeft verschillende interfaces met elk hun eigen IP adres in het eigen netwerk
- RAM – ROM – NVRAM – Flash

Memory	Volatile / Non-Volatile	Stores
RAM	Volatile	<ul style="list-style-type: none"> <li>Running IOS</li> <li>Running configuration file</li> <li>IP routing and ARP tables</li> <li>Packet buffer</li> </ul>
ROM	Non-Volatile	<ul style="list-style-type: none"> <li>Bootup instructions</li> <li>Basic diagnostic software</li> <li>Limited IOS</li> </ul>
NVRAM	Non-Volatile	<ul style="list-style-type: none"> <li>Startup configuration file</li> </ul>
Flash	Non-Volatile	<ul style="list-style-type: none"> <li>IOS</li> <li>Other system files</li> </ul>

- Aansluitingen
  - o Ethernet: fastethernet of gigabitethernet
  - o Console poort -> console kabel
  - o AUX poort, via telefoonlijn de router configureren
  - o Kan ook seriële interface hebben om routers met elkaar te gaan verbinden

#### Basisconfiguratie

- Hostname instellen
- Wachtwoorden instellen
- Interfaces op een router starten met 0/0, op een switch met 0/1
- **No shutdown** om de poort open te stellen
- Seriële interface wordt gebruikt om twee routers met elkaar te gaan verbinden

#### Layer 3 switch

- Layer 2 switchen werken enkel met mac-adressen
  - o Alle toestellen die hier om zijn aangesloten zijn lid van hetzelfde netwerk en hebben dus hetzelfde netwerkadres.
- Layer 3 switchen kunnen wel kijken naar IP adressen
  - o Hier kunnen toestellen die lid zijn van verschillende netwerken op worden aangesloten
  - o Gaat ook IP adressen associëren met poorten
  - o Hier kan ook routing plaatvinden
    - Wordt gebruikt om verschillende netwerken met elkaar te communiceren en belasting van de router weg te nemen
- Elke interface op een switch kan een IP adres krijgen
  - o Bij layer 2 kan je een IP adres plaatsen op VLAN1, waar alle poorten onderdeel van zijn
  - o Bij layer 3 kan je op een bepaalde poort een IP plaatsen (vb.: f0/1)
    - **No switchport**
      - Aangeven dat het gaan om een layer 3 switchport

Les 7: 3/04/2020 (video 3)

## IPv4 adressen

- Computers in een netwerk een adres geven + subnet mask
- Dotted decimal notation (4 decimale cijfer met punten tussen)
- Elk cijfer is een decimale weergave van 8 bits
- **Binair naar decimaal kunnen omzetten en omgekeerd**
- Subnet mask bepaald welk deel van het Ip adres het netwerk gedeelte is en welk deel het host gedeelte is
  - o Netwerk gedeelte komt overeen met alle enen van de subnet mask
    - Dit deel moet bij alle toestellen hetzelfde zijn die zijn aangesloten op één netwerk
  - o Host gedeelte komt overeen met alle nullen van de subnet mask
    - Dit moet voor alle toestellen verschillend zijn in één netwerk
- Subnet mask moet starten met enen en dan nullen
  - o Dit mag niet: 255.0.255.0
- Prefix length notation “/” (**CIDR** notation)
  - o Aantal enen in subnet mask
  - o Voorbeeld: 192.168.1.10/24 -> 255.255.255.0
- Niet alle IP adressen zijn mogelijk
  - o **Netwerk adres**
    - Alle host bits staan op nul
    - Naam van het netwerk
  - o **Broadcast adres**
    - Alle host bits op één
    - Als een host een pakket naar alle toestellen op een adres wil sturen
- Aantal hosts:  **$2^{(\text{aantal host bits})} - 2$**
- Meestal is het eerste geldige ip adres toegekend aan de default gateway (router)
  - o Zo kan iedereen makkelijk weten wat het IP adres is van de default gateway
- Drie manieren om pakketten te versturen
  - o Unicast: naar één host
  - o Broadcast: naar alle hosts
  - o Multicast: een groep van hosts
    - IP ligt tussen 224.0.0.0 en 239.255.255.255
    - Toestellen moeten zich inschrijven op een specifieke multicast
    - Switch gaat bijhouden welke MAC adressen zich hebben ingeschreven voor welke broadcasts
- Private address blocks
  - o 10.0.0.0/8 (10.0.0.0 – 10.255.255.255)
    - zeer grote netwerken
  - o 172.16.0.0/12 (172.16.0.0 – 172.31.255.255)
    - Middelmattige netwerken
  - o 192.168.0.0/16 (192.168.0.0 – 192.168.255.255)
    - thuis en kleine netwerken
  - o Deze adressen zullen worden geblokkeerd door ISP
- Speciale adressen
  - o Netwerk en broadcast adressen
  - o Loopback adres (local host address)
    - 127.0.0.0 – 127.255.255.255

- Link-local adressen
  - Gebruikt voor Windows toestellen die op een netwerk worden aangesloten waar geen dhcp server is en geen statisch IP adres wordt ingegeven
  - Nooit zelf gebruiken
- TEST-NET adressen
  - 192.0.2.0 – 192.0.2.255
- Experimentele adressen
  - 240.0.0.0 – 255.255.255.254
- Manier waarop IP adressen worden uitgedeeld is verdeeld over verschillende tiers
  - Tier 1
    - service providers geven tier 2 toegang aan zeer grote bedrijven
    - backbone van het internet
  - Tier 2
    - Maken verbinding met het internet via tier 1 bedrijven
    - Voor grote bedrijven
  - Tier 3
    - ISP
    - Kleine bedrijven en huizen
    - Gaat altijd via tier 2

Op welke manier een netwerk van IP adressen voorzien?

- Subnetting gebruiken
  - Een groot netwerk opdelen in kleinere deelnetwerken
    - De hoeveelheid pakketten die op een netwerk worden gestuurd reduceren
      - Naast het gewone verkeer is er ook veel ander verkeer (broadcasts)
        - ARP verzoeken
        - Dhcp verzoeken
      - Dit verkeer kan de overhand nemen als er teveel toestellen met het netwerk zijn verbonden
  - Extra veiligheid
    - Bepaalde servers die enkel beschikbaar zijn op een bepaald netwerk
    - Netwerk voor gasten
    - Aan de hand van firewalls en regels instellen welk verkeer naar welk netwerk mag
- Tellen hoeveel netwerken er zijn
- Tellen hoeveel hosts er zijn
- Subnet mask aanpassen naar het aantal netwerken dat we nodig hebben
- **Subnetting**
  - Lenen van bits van het host gedeelte
    - Aantal bits lenen  $2^{(\text{aantal bits})} = \text{aantal netwerken}$ 
      - Vb.:  $2^1 = 2$  netwerken
- Waar moet je op letten?
  - Het subnet met de meeste hosts moet zeker er op passen
  - Zorg dat groei in een subnet mogelijk is
  - Begin altijd met het grootste subnet
- VLSM
  - Variable lenght subnet mask
  - Soms wil je niet dat alle subnets evenveel hosts kunnen hebben

- Vb.: verbinding tussen twee routers zijn maar twee IP adressen nodig
- Een subnet onderverdelen in kleinere subnets

## Les 8: 21/04/2020 (video 4)

### IPv6

- IP protocol in de netwerk laag van het OSI model
  - Verantwoordelijkheden:
    - Het adresseren van *end devices*
    - Router van pakketten door het netwerk naar de juiste bestemming
    - Routing tabellen bijhouden welke routes er door het netwerk zijn
- IPv4
  - 1981 ontstaan voor ARPANET
  - 32-bit adres -> 4,3 miljard adressen
  - Adres blokken zijn niet ideaal verdeeld
    - Veel adressen onbruikbaar
    - Routing tabellen die momenteel nodig zijn om internetverkeer op IPv4 netwerk te routeren globaal zeer complex en zeer groot kunnen zijn
  - NAT is een tijdelijke oplossing
    - Mapping van privé IP adres naar publiek IP adres
    - Problemen
      - Elke keer dat een pakket dat vertrekt vanbinnen netwerk over die nat router gaat, zal binnen dat pakket een aantal zaken moeten worden aangepast zoals
        - destination IP adres
        - checksum in bepaalde headers moeten worden herrekend door verandering van IP
      - in ICMP zullen IP adressen moeten gewijzigd worden
      - IPsec geeft problemen omdat door het wijzigen van de IP adressen de integrity check niet zal lukken
      - Geen end-to-end mogelijk
        - Port forwarding nodig: bepaalde poorten worden geforward naar bepaalde privé IP adressen
      - NAT is NOT security
- IPv6 is de opvolger van IPv4. Waarom overstappen?
  - Opraken van IPv4 adressen
    - 128-bits =>  $2^{128}$  adressen
  - Aantal protocollen van IPv4 zijn ook verbeterd
- IPv4 en IPv6 hebben elk hun eigen netwerk

### IPv6 adressen

- 128 bits
- Hexadecimale cijfers (4 bits = 1 hexadecimal)
- Groep van 4 hexadecimale cijfers samennemen = **hextet**
- Hextets gescheiden door ':' -> 8 hextets naast elkaar
- Mogelijk dat meerdere IPv6 adressen toegekend worden aan één netwerkinterface
- Regels om adressen korten te schrijven

- *Leading zeros* weglaten
  - Vb.: 0DB8 -> DB8
  - Vb.: 0000 -> 0
- Groepen van nullen vervangen door ::
  - Kan meer één keer worden gebruikt
- Prefix (= gelijkwaardig aan het netwerkgedeelte van IPv4)
  - De lengte wordt weergegeven na de "/"
- Interface ID (= gelijkwaardig aan het hostgedeelte van IPv4)
  - Gekozen voor deze naam omdat de meeste toestellen meerdere interfaces hebben
- Typische lengte voor prefix is /64
  - 64 bit prefix
  - 64 bit Interface ID

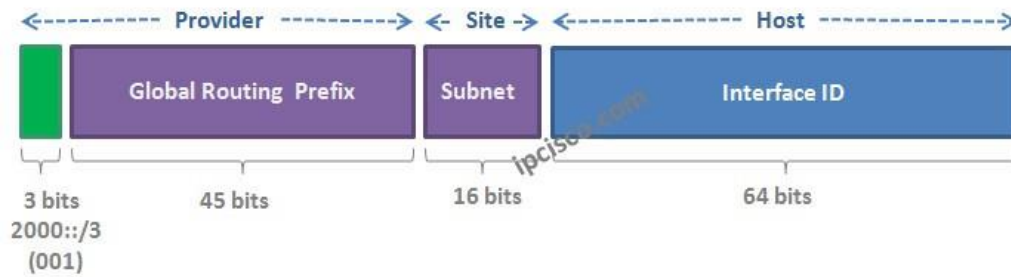
#### Verschillende soorten IPv6 adressen

- Unicast: uniek één interface identificeren
  - Één interface kan wel meerdere IPv6 adressen hebben
- Multicast: groep van interfaces
  - Verschillende interfaces kunnen luisteren naar dezelfde multicast adres
  - Dit adres kan enkel destination adres zijn en NOOIT een source adres
- Anycast
  - hetzelfde als unicast, maar verschillende interfaces hebben dezelfde unicast adres
  - pakket met dit adres zal worden gestuurd naar de route die het minste kost (lowest router cost)
- broadcast bestaat NIET meer
- Als ooit blijkt dat de distributie van de IPv6 adressen niet goed is, zijn er nog enkele kansen om het opnieuw te proberen

#### Type adressen

- Global Unicast Address (GUA)
  - Adressen die globaal op het internet routeerbaar zijn
  - gelijkaardig aan IPv4 public adressen
  - hiermee kunnen toestellen communiceren over het internet
  - elk toestel heeft een GUA, ook binnen eigen netwerk
  - geen gebruik van NAT
  - opbouw
    - start met 2000::/3
      - eerste drie bits staan vast
      - tussen 2000 en 3fff
  - kunnen we zelf niet krijgen
    - moeten we krijgen van ISP
      - geeft **global routing prefix**

## Global Unicast IPv6 Address



- Hoe worden deze uitgedeeld?
  - Regional Internet Registries (RIR)
    - Zijn verantwoordelijk voor het uitdelen van IPv6 adressen naar ISP

**2001:0DB8:4898:DAFC::/64**

**RIR** ::/12

**ISP** ::/32

**Site** ::/48

**Subnet** ::/64

- Hoe kunnen we deze configureren aan end devices?
  - Statisch toekennen
    - Voor routers, server, printers, ...
  - DHCPv6
  - Stateless Address Autoconfiguration (SLAAC)
    - Nieuwe host op netwerk stuurt **Router Solicitation** naar routers
      - Komt enkel bij de routers aan (multicast, zie verder)
    - Router antwoord met **Router Advertisement**
      - Bevat prefix, prefix lengte, default gateway en eventueel DNS
  - Optie 1: SLAAC only
    - Host heeft voldoende info gekregen uit Router Advertisement om alles in te stellen
  - Optie 2: SLAAC & DHCPv6
    - Deel op de info komt van Router en een deel van DHCPv6
    - Default gateway MOET altijd komen van de Router Advertisement
    - DHCPv6 is **stateless**
      - Heeft geeft pool met adressen
      - Geeft enkel extra opties zoals DNS server, FTP server, ...
      - Weet dus niet welk toestel welk IPv6 adres heeft gekregen
  - Optie 3: DHCPv6 Only
    - Host gaat info uit Router Advertisement niet gebruiken maar gaat zijn IP adres vragen aan een **statefull** DHCP server

- Deze heeft wel een pool van adressen
- Hoe gaat de client de Interface ID genereren?
  - Ofwel gebruikt de host zijn MAC adres hiervoor
    - MAC adres in twee splitsen en dan in het midden FF FE toevoegen om de juiste lengte te krijgen
    - Zevende bit vanaf links omzetten 1 <-> 0
  - Random ID genereren
- Link-Local Unicast Address (Unicast)
  - Worden gebruikt voor communicatie binnen eigen subnet (link)
  - Deze zijn niet routeerbaar
  - Toestellen geven zichzelf een link-local adres
    - Router doet dit niet
  - Elke interface moet een link-local adres hebben
  - GUA's zijn optioneel en enkel nodig wanneer er moet worden gecommuniceerd buiten zijn eigen netwerk
  - Opbouw
    - Start met FE80::/10
      - eerste 10 bits vast
      - van FE80 tot FEBF
- Duplicate Address Detection (DAD)
  - Als toestel Interface ID genereert, moet die in het eigen netwerk worden gecontroleerd of deze niet al bestaat
  - ICMPv6 **Neighbor Solicitation messages**
    - Geen antwoord wil zeggen dat het goed is
- Loopback adressen
  - ::1/128
- Unspecified adressen
  - ::/128
  - Kan alleen als source adres gebruikt worden
    - Vb.: wanneer een host een router aanspreekt voor het krijgen van een Ipv6 GUA
- Unique local adressen
  - Komen overeen met de privé Ipv4 adressen
  - Worden in Ipv6 zeer beperkt gebruikt omdat end devices GUA krijgen om te communiceren op het internet
- Embedded Ipv4
  - Om op een speciale manier te communiceren met Ipv4 toestellen
  - Het Ipv4 adres wordt als laatste deel ingevoerd in het Ipv6 adres
- Multicast adressen
  - Prefix FF00::/8
  - One-to-many
  - Pakketten komen enkel aan op toestellen die naar een bepaald multicast adres luisteren. Dit komt omdat multicast berichten worden gefilterd door switchen en niet bij elke host zal aankomen
  - Efficiënter dan broadcasts omdat dit kan worden gefilterd door switchen
    - Internet Group Management Protocol (IGMP) Ipv4
    - Multicast Listener Discovery (MLD) Ipv6



- Host moet MLD pakket sturen naar switch om zich aan te melden voor multicast
- Om multicast te verzenden: gebruik multicast destination adres
- Om multicast te ontvangen: gebruik MLD pakket om te registreren bij switches en routers
  - Op de interface wordt dit adres ook toegevoegd
- Aantal soorten
  - **Well known multicast adressen**
    - Permanent gereserveerd
    - Solicited-node multicast adres
      - Een deel van de unicast IPv6 adres wordt gebruikt (laatste 24 bits) om daar solicited-node multicast adres van te maken
      - Op dit adres zal elke netwerkinterface ook luisteren
      - Gebruikt voor **Neighbor Discovery (ND)** en **Duplicate Address Detection (DAD)**
        - Kijken of er een andere toestel op het netwerk zit met hetzelfde IPv6 adres
        - Maakt **neighbor solicitation** aan die wordt verstuurd naar het solicited-node multicast adres om het MAC adres van een toestel op te vragen. Toestel antwoord dan met **Neighbor Advertisement**
      - Bij ARP (IPv4) zullen er broadcast worden gestuurd die elk toestel in het netwerk ontvangt (minder efficiënt)
  - Transient multicast (**dynamic multicast**)
    - Gebruikt als tijdelijk adres door applicaties
      - Streaming

#### IPv6 header

- Header is 40 byte
  - bij IPv4 was die variabel
  - dit zorg voor snellere processing van de pakketten (door de vaste lengte)
- opmaak
  - Version: 6
  - Traffic class: Quality of Service
    - Bevat ID waarmee we quality of service kunnen doen
  - Flow Label
    - Zorgt er voor dat pakketten van dezelfde stream kunnen worden herkend zodat ze op dezelfde manier kunnen worden behandeld
  - Payload Length: lengte van de payload (hetgeen NA de header komt)
  - Next header: volgende header van een pakket
  - Hop limit: time to life
    - Verlaagt bij elke router
- Wat valt er weg van IPv4
  - IP header length (IHL) -> vaste grootte bij IPv6
  - Identification, Flags, Fragment Offset
    - Bij IPv4 konden pakketten worden opgesplitst in kleinere stukken
    - Routers zullen de pakketten niet meer fragmenteren, maar de hosts zullen dit doen

- Header checksum: zit al in de Ethernet header
- Options zitten er ook niet meer standaard in
- Extension headers
  - Opties die we willen meegeven
  - Deze headers kunnen worden toegevoegd tussen de standaard IPv6 header en de TCP/UDP header
  - In elke header zit een next header veld
  - De opties zitten nu niet meer in de standaard header, maar kunnen als nieuwe headers worden toegevoegd
  - Vb.: hop-by-hop, IPsec, ICMPv6
    - **ICMPv6** bevat: ICMP, IGMP, ARP
      - Error berichten
        - Destination unreachable
          - Als de router geen route heeft naar de bestemming
        - Packet too big
          - Als packet bij een router komt van een link die kleiner is dan de grootte van het pakket
        - Time exceeded
          - Wanneer time to life of hop limit is overschreven
        - Parameter problem
      - Query berichten
        - Echo request and reply (ping)
        - Router solicitation
        - Router advertisement
        - Neighbor solicitation
        - Neighbor advertisement
        - Multicast listener discovery

#### Overstap van IPv4 naar IPv6

- Dual-stack: zowel IPv4 als IPv6
  - Je moet hierdoor beide netwerken beveiligen
  - De routing tabellen in de routers moeten voor zowel IPv4 als IPv6
  - Tunneling
    - IPv6 pakketten versturen naar IPv4 netwerk door IPv6 pakketten te encapsuleren in IPv4 Header als data
  - Translation
    - Vertaling waarbij IPv4 wordt omgezet naar IPv6 pakketten en omgekeerd

#### [Les 9: 28/04/2020 \(video 5\)](#)

#### Transport laag

- Verantwoordelijk voor het afleveren van de data tussen verschillende applicaties
- Hier wordt gebruik gemaakt van poortnummers
- Twee protocollen waaruit je kan kiezen en die naast elkaar staan
  - TCP

- Betrouwbare communicatie
  - Kunnen zeker zijn dat pakketten aankomen
  - Acknowledgements
    - Zorgt voor meer verkeer op netwerk
    - Zal een bevestiging sturen wanneer er een aantal segmenten zijn aangekomen; je kan zelf kiezen na hoeveel segmenten er een bevestiging moet komen
- Gebruik
  - HTTP(S)
  - FTP
  - SMTP
  - Telnet
  - DNS
- Eigenschappen
  - Sessie opzetten tussen zender en ontvanger
    - Wordt afgesproken hoeveel data er verstuurt gaat worden
    - Sessie wordt daarna afgesloten
  - Same-order delivery
    - Pakketten worden in de juiste volgorde geplaatst
  - Flow control
    - Segmenten kunnen groter of kleiner worden gemaakt
- TCP voegt header toe
  - Poorten
  - Sequence number
    - Pakketten in de juiste volgorde plaatsen
  - Acknowledgement number
  - Header length
  - Control bits
  - Window
  - checksum
- UDP
  - Moet niet betrouwbaar zijn
    - We weten niet of de pakketten aankomen
  - Gebruik
    - VoIP
    - IPTV
    - SNMP
    - DHCP
    - TFTP
    - DNS
  - Eigenschappen
    - Connectionless
      - Geen verbinden tussen zender en ontvanger
    - Pakketten kunnen niet weer in de juiste volgorde worden gezet
      - Bij VoIP wordt RTP gebruikt om in de applicatielaag toch een volgorde toe te kennen
    - Geen flow control

- We kunnen niet de grootte van de pakketten aanpassen omdat we niet weten wat de kwaliteit van het netwerk is
- UDP voegt header toe
  - Is veel kleiner dan TCP header
  - Poorten
  - Length
  - checksum
- Verantwoordelijkheden
  - Tracken van data uit de verschillende applicaties
    - Data van verschillende applicaties gelijktijdig doorsturen over dezelfde netwerkverbinding
  - Segmenteren van data
    - Verschillende pakketten door elkaar laten lopen
  - Identificeren van binnenkomende pakketten en doorsturen naar de juiste applicatie

#### Poortnummers

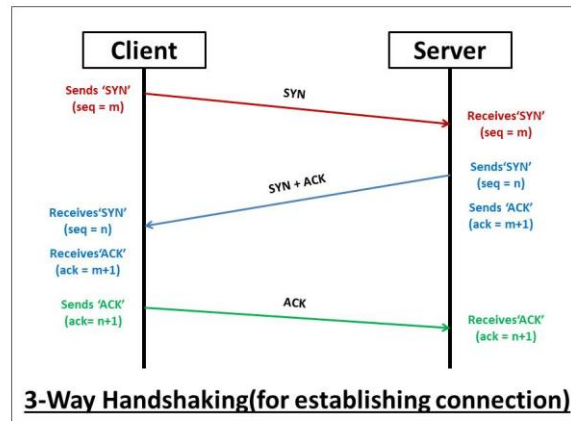
- Poortnummers worden gebruikt omdat op éénzelfde toestel meerdere applicaties draaien
  - Pakketten moeten dus naar de juiste applicatie worden gestuurd
- Combinatie van IP adres en poortnummer -> **socket**
- **Socket pair**: source en destination IP en poortnummers

#### Hoe worden deze poortnummers gegenereerd?

- **Well-known poorten**: 0 – 1023
  - Deze zijn gereserveerd voor bepaalde services en applicaties
  - TCP
    - FTP: 21
    - Telnet: 23
    - SMTP: 25
    - HTTP: 80
    - IMAP: 143
    - HTTPS: 443
  - UDP
    - TFTP: 69
- **Registered poorten**: 1024 – 49151
- **Dynamic or private poorten**: 49152 – 65535
- **Netstat**
  - Bekijken van TCP connecties

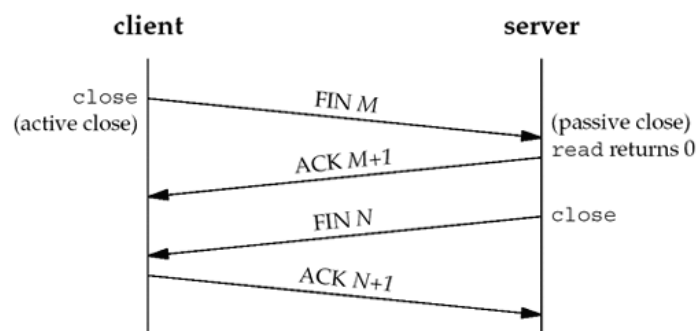
#### TCP session opzetten: **3-way handshake**

- SYN: Zender naar de ontvanger om aan te geven dat we een sessie willen opzetten
  - SEQ wordt gegenereerd door zender (meestal 0)
- SYN ACK: Ontvanger kan sessie aanvaarden
  - SEQ wordt gegenereerd door ontvanger
  - ACK wordt het ontvangen SEQ + 1
- ACK: Zender stuurt bevestiging
  - SEQ is de ontvangen ACK
  - ACK is het ontvangen SEQ + 1



- Control bits in TCP header bevatten vlaggen die op de juiste waarden moeten worden ingesteld; zo kan worden aangegeven welk soort bericht dit is

Sessie afbreken



Window size bij TCP

- Bepaalde wanneer de ontvanger een ack moet sturen
- Zonder window size moet elk bericht bevestigd worden
- Bepaald hoeveel bytes er verstuurd kunnen worden alvorens er een ack moet worden gestuurd
- Ack bestaat uit het volgend nummer dat wordt verwacht
- Met de windows size kan worden gespeeld
  - o Wanneer de window size groter is, kan de communicatie snel verlopen maar is de kans op fouten veel groter
  - o Zolang de ack's blijven aankomen, kan de window size worden vergroot

UDP

- Onbetrouwbaar
- Geen extra data (ACK, SYN, ...) -> sneller

## Les 10: 5/05/2020 (video 6)

### Application layer

- Bestaat uit drie lagen, maar worden ook vaak samengenomen als we het over netwerken hebben. Vooral de onderste 4 lagen belangrijk
  - o Session layer: laag 5
    - Hier kan een sessie worden opgezet tussen de applicaties
    - De sessie die wordt opgezet in de session layer is niet hetzelfde als de sessie die wordt opgezet door TCP
  - o Presentation layer: laag 6
    - Data in een bepaald formaat te gieten
      - GIF, JPEG, ...
  - o Application layer: laag 7
    - Verantwoordelijk voor het genereren van data
    - Hier zitten een aantal bekende protocols in
      - DNS: Domain Name System
      - HTTP: Hypertext Transfer Protocol
      - SMTP: Simple Mail Transfer Protocol
      - DHCP: Dynamic Host Configuration Protocol
      - FTP: File Transfer Protocol
      - IMAP: Internet Message Access Protocol
      - POP: Post Office Protocol
- telnet: gebruikt om commando's te sturen naar Cisco apparatuur
- DHCP: IPv4 adressen verkrijgen
- Client-server model

### DNS

- Wordt gebruikt om domeinnamen om te zetten naar IP adressen
- Mensen kunnen makkelijker namen onthouden dan IP adressen, maar computers werken met IP adressen
- Levels
  - o Top level: .org, .org, .com, ...
  - o Domain name: google, microsoft, ...
  - o Subdomain: www, be, ...
- DNS query
  - o Eerst naar primaire DNS server gestuurd
    - De server kan het antwoord hebben in cache
    - Of kan in eigen zone in A records
    - Anders moet query worden doorgestuurd naar root DNS server
  - o Root DNS server
    - Heeft alle top level domains
    - Antwoord met IP van top level domain server
  - o Top level domain server
    - Heeft alle servers waar de domeinen staan geregistreerd
    - Stuurt IP van de authoritative name server terug
  - o Name server

- Heeft IP van het domain en zal een authoritative antwoord geven
- Host records
  - A record: IPv4
  - AAAA record: IPv6
  - CNAME: alias (bijnaam) naar een andere DNS naam
  - MX: Mail exchange record
- Nslookup
  - Naam omzetten naar IP en kijken welke DNS server hiervoor gebruikt worden

#### DHCP server

- Deelt IPv4 adressen uit aan hosts op netwerk
- Heeft pool van adressen die mogen worden uigedeeld
- Kan aan opties meegeven
  - Default gateway
  - DNS server
  - NTP server (network time protocol)
- Hoe gaat DHCP server IP adressen uitdelen aan host?
  - Host gaat broadcast sturen: DHCP discovery
  - DHCP stuurt offer als broadcast omdat host nog geen IP heeft: DHCP Offer
  - Als host offer wilt aanvaarden: DHCP Request
  - Bevestiging van DHCP server: DHCP Ack
  - Nu zal de host zijn IP adres pas instellen
  - Dit is omdat er meerdere DHCP servers op een netwerk kunnen staan en kan dus meerdere offers krijgen

#### FTP


- Hier worden twee poorten gebruikt
  - Poort 20
    - Data wordt via deze poort verstuurd
  - Poort 21
    - Hier worden de commando's gestuurd om bepaalde bestanden door te sturen

[Herhaling \(video recap\)](#)

Zie video

## Vragen van anderen:

**LightFelcore** Today at 18:34  
Ik heb dus hetzelfde netwerk als de vorige keer opgesteld: pc, switch, router, switch, pc (in deze volgorde). Ik kan van de ene pc naar de andere pingen. Als ik ping van switch 0 naar switch 1 lukt dit niet. Mijn doel is om via telnet vanuit switch0 binnen te geraken in switch 1 maar dit lukt niet?-. Ook lukt het niet om via pc0 in switch 1 te geraken via telnet.



Ik kan ook pingen van pc0 naar de andere interface van de router?

**LightFelcore** Today at 19:34  
Ook is het niet mogelijk om te pingen van pc0 naar switch 1 en dus telnet werkt ook niet vanuit pc0 naar Switch1...

**joris.dieltiens** Today at 19:30  
Om een pakket te versturen buiten je eigen netwerk stuurt het device het pakket naar zijn default gateway. Op de switchen is enkel het ip adres en subnet mask ingesteld. Jammer genoeg is het voor zover ik weet op de switchen in packet tracer niet mogelijk om een default gateway in te stellen. Het loS op deze gesimuleerde switchen is beperkter dan de echte versie. Dit geldt voor eender welk pakket er vertrekt uit de host of switch, zowel request als de reply. Als je wil pingen van switch 0 naar switch 1 moet switch 1 de request naar de default gateway sturen. Die is niet ingesteld en daarom kan switch 0 het request pakket niet versturen. Als je wil pingen van PC0 naar switch 1 moet pc0 de request naar de default gateway sturen. Dat is de router en het pakket vertrekt. De router gebruikt zijn routing tabel om het pakket naar het netwerk van switch 1 door te sturen. switch 1 ontvangt de request. Maar nu moet switch 1 een reply sturen naar een host buiten zijn eigen netwerk. Maar aangezien er geen default gateway staat ingesteld op de switch kan deze de reply niet versturen. Dit geldt hetzelfde voor telnet. Als je telnet probeert van pc0 naar switch 1 zullen de pakketten wel aankomen bij switch 1 maar de switch kan geen pakketten terug sturen. Telnet is TCP. Dat wil zeggen dat er eerste een sessie moet worden opgezet met SYN, SYN ACK, ACK. De SYN ACK van switch 1 naar pc0 zal niet verstuurd kunnen worden en de sessie zal nooit kunnen worden opgezet. Tftp maakt gebruik van udp. Dat wil zeggen dat er geen sessie wordt opgezet en dat pakketten gewoon verstuurd worden. Het is dus in principe mogelijk om, moest de switch een tftp server zijn (wat niet het geval is!) deze wel van pc0 naar switch 1 te versturen. Probeer wat ik hier uitleg zeker eens na te kijken in de simulatie mode. Zet telnet en tcp aan als filter en dan zal je kunnen zien wat er gebeurt. Zeer goede oefening voor het labo examen.  
of zet icmp als filter aan en ping van pc0 naar switch 1

## Vragen:

- Network Fundamentals - 04 - IPv6
  - o Slide 19 -> IPV6 DUPLICATE ADDRESS DETECTION (DAD): hoe weet de zender van die berichten dat de berichten goed zijn aangekomen? Als er geen antwoord terug is gekomen kan dit toch twee dingen betekenen:
    - Bericht is niet aangekomen, niemand stuurt iets terug
    - Geen enkele ander toestel op het netwerk heeft dit IP adresHoe kan je nu een onderscheid maken?  
**Dat kan hij inderdaad niet. Eerst is en vooral is de kans dat een duplicaat adres voorkomt ongelooflijk klein. De kans dat net dit DAD packet wordt gedropt is nog veel kleiner. Daarnaast worden de neighbor solicitation en neighbor advertisements ook nadien nog gestuurd. De DAD zou op dat moment alsnog opgemerkt worden.**
  - o Slide 20 -> OTHER UNICAST ADDRESSES: moeten die figuren bij ::1/128 en ::/128 niet omgewisseld worden, of zit ik hier fout  
**Klopt, ik heb het aangepast**
  - o Slide 22 -> WELL KNOWN MULTICAST ADDRESSES: moeten we al die adressen uit het hoofd kennen, of zijn de eerste twee en de solicited-node voldoende?  
**FF02::1, FF02::2 en de solicited node is voldoende**
  - o Slide 25 -> NEIGHBOR DISCOVERY PROTOCOL (NDP): bij de figuur van het netwerk staan twee keer een '::' in het IPv6 adres? Dit mag toch niet?  
**Klopt, ik heb het aangepast**
  - o Slide 25 -> NEIGHBOR DISCOVERY PROTOCOL (NDP): waarom maakt men bij neighbor solicitation gebruik van het solicited-node multicast adres en stuurt men niet een unicast naar het IPv6 adres als met het adres toch kent.  
**Dat komt omdat voor het sturen naar een unicast IP adres ook het unicast MAC adres moet worden toegevoegd aan de frame. Naar dat MAC adres luistert de netwerkkaart van de ontvanger. En dat is net niet gekend. Daarom wordt het verstuurd naar een multicast wavoor een speciaal multicast MAC adres gebruikt kan worden dat door de zender zelf gegenereerd kan worden. Naast het unicast MAC adres luistert een netwerkkaart ook naar alle MAC adressen die overeen komen met de multicasts waarop deze computer is ingeschreven. Het omzetten van multicast IP naar multicast MAC hebben we niet gezien en moet je ook niet kennen.**



- Algemene vraag: bestaat een sequence uit één pakket of kan dit ook uit meerdere pakketten bestaan? Bestaat een segment uit één pakket of kan dit ook uit meerdere pakketten bestaan?  
 Data uit de applicatie laag wordt, indien nodig, gesegmenteerd in kleinere segmenten. Elk segment krijgt opeenvolgende sequence numbers (TCP). Elk segment wordt een voor een aan de netwerklaag gegeven. Indien nodig kan IP dit segment nog eens fragmenteren in kleinere fragmenten. In de IPv4 header zijn hiervoor de identification en fragment offset aanwezig, IPv6 gebruikt de fragment extension header. Een segment wordt door IP gefragmenteerd indien een van de links tussen zender en ontvanger een Maximum Transfer Unit (MTU) heeft die kleiner is dan de grootte van het segment. het IP protocol bij de ontvanger zal wachten tot alle fragmenten zijn aangekomen, dit terug samenstellen tot het originele segment en dit volledige segment doorsturen naar de transport laag. TCP zet alle segmenten terug in de juiste volgorde en geeft deze data door aan de applicatie laag bij de ontvanger. De meest voorkomende MTU is 1500 bytes. Hiermee houdt TCP ineens rekeningen en maakt segmenten die niet groter zijn dan dit (min de ip en ethernet header) zodat IP niet meer moet fragmenteren in de meeste gevallen. Dit omdat het fragmenteren extra vertraging met zich meebrengt en de load op routers en hosts verhoogt.
- Network Fundamentals - 05 - Transport Layer
  - Slide 61 -> TCP SESSION TERMINATION: waarom staat bij de eerste afbeelding ACK op 1?  
 De ack vlag staat voor alle pakketten na het eerste syn pakket aan. Het is bijvoorbeeld mogelijk dat de ontvanger na het ontvangen van het laatste segment dat laatste segment Acknowledged en in hetzelfde pakket ook de FIN vlag aan zet om meteen de sessie te beëindigen. Zo moet maar 1 in plaats van 2 pakketten verstuurd worden.
  - Algemene vraag: wordt er ook data meegestuurd met een ACK, SYN, FIN, ... vanuit de application laag  
 Met de pakketten van de 3 way handshake kunnen als data opties meegegeven worden zoals de maximum segment size, window scale, ... Met de FIN pakketten wordt geen data meer verstuurd. Maar de ACK nummer kan dus nog wel van belang zijn.

Examen: 40 meerkeuze vragen zonder giscorrectie. Soms meerdere antwoorden aanduiden.