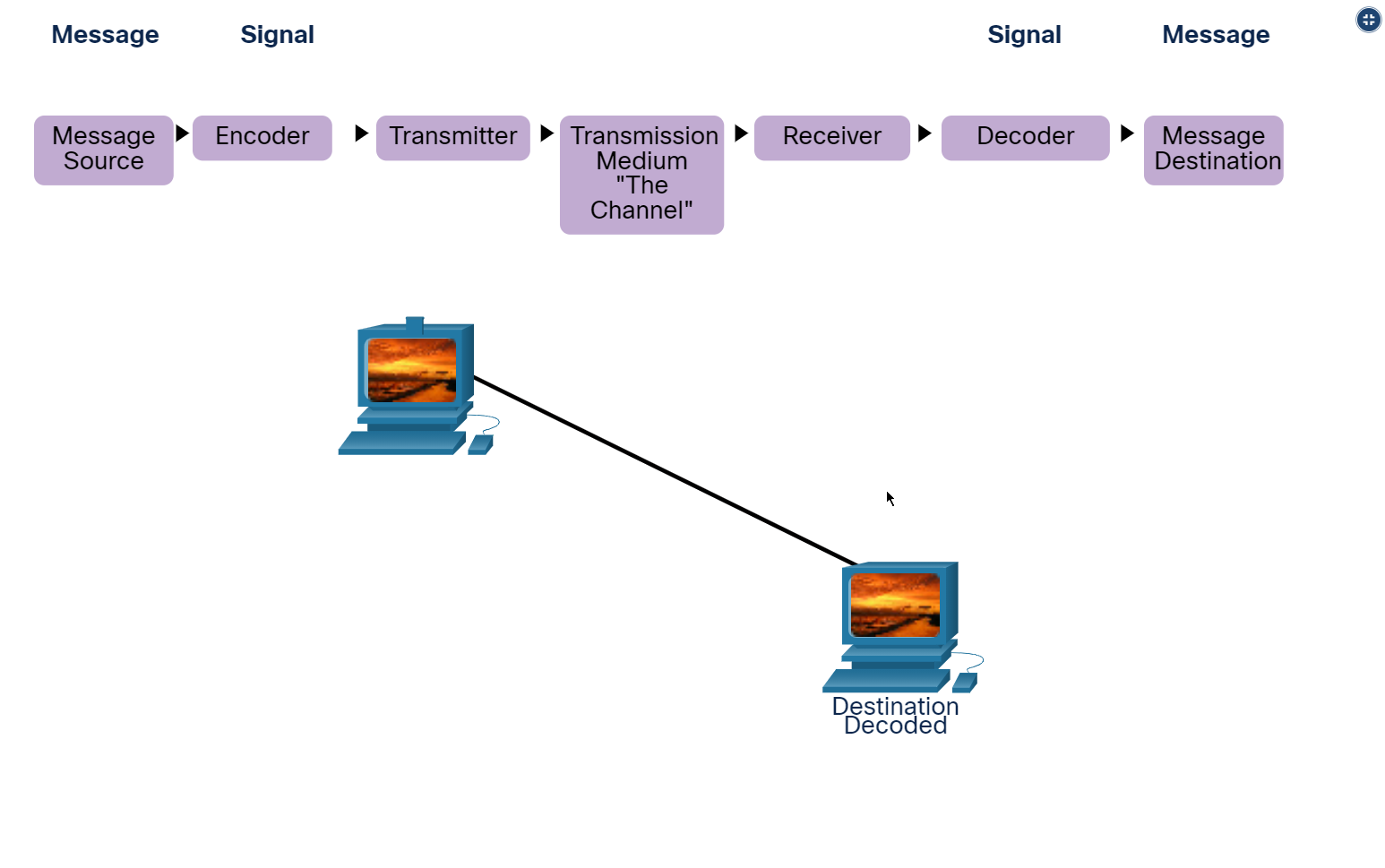
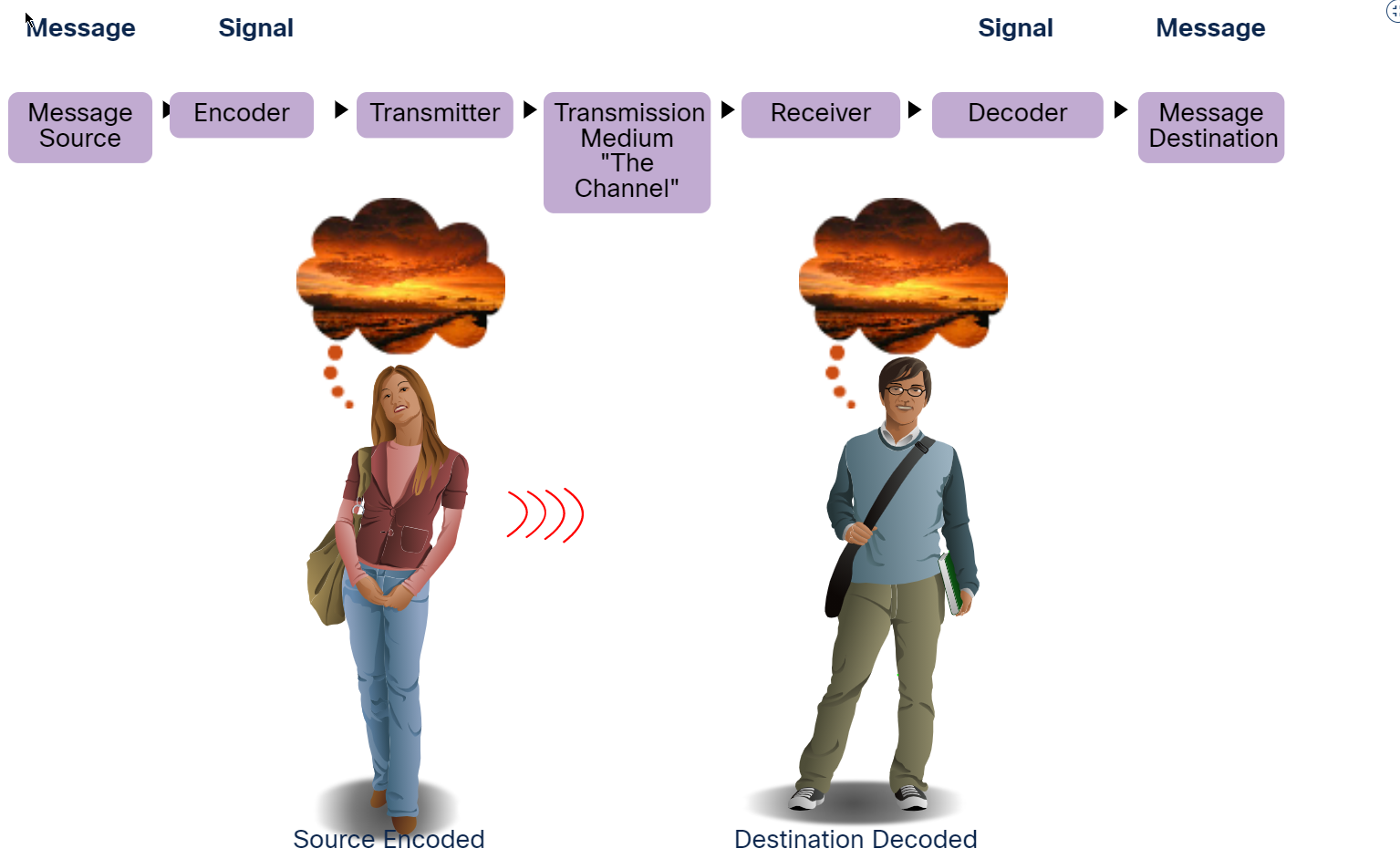
# Chapter 3: Protocols and models

Protocollen: afspraken over hoe iets gedaan moeten worden

* DHCP/ICMPv6
  + Computer moet ip-adres weten, hij kan dit krijgen van DHCP. Hij kan hieruit de ip-adres krijgen, de default gateway, dns, welke netwerk je zit.
* DNS
  + Als die dat weet, vraagt die wil je me de ip addres geven
* IP and TCP
  + Endan stuurt die request naar de ip adress om de website te krijgen.
  + Tcp zorgt ervoor dat de vraag correct verloopt.

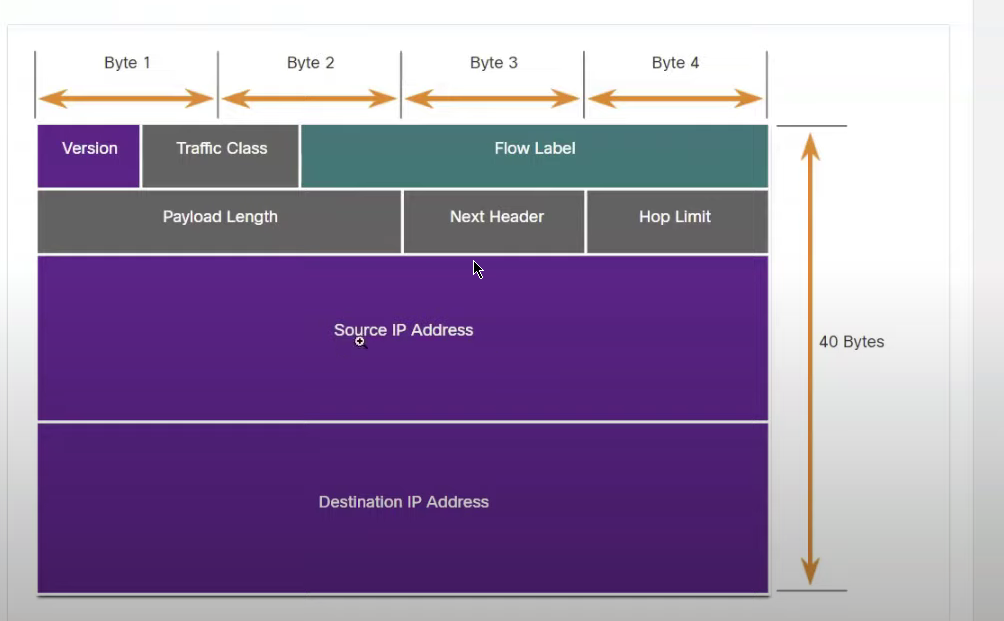
**Message encoder:**

* De vrouw denkt aan iets(de pc denkt iets of doet iets(aantal pitjes))
* Probeert dat via spraak over te brengen(hij brengt dit over via ethernet kabel of via radio waves of via lichtimpulsen)
* Endan gaat die man dat over te nemen en een beeld over te nemen. Dus zogezegd de spraak decoderen.(en hier worden die terug naar nulletjes en eentjes gezet)



**Message Formatting and Encapsulation:** We gaan onze data steken in een aparte pakketje om het zo te versturen via het netwerk. En men plaats alles in de juiste vakjes.





**Message size:** Als de boodschap te groot is kan de ontvanger het niet verwerken dus, men moet het sturen in meerdere kleine messages.

## Message Timing

**Flow control:** Hoeveel informatie er kan verstuurd worden aan welke snelheid. Voorbeeld als ge dichtbij u router zit => beter internet => sneller doorsturen en beter

**Response Timeout:** Hoelang een pc wacht als die denkt dat die niet heeft geantwoord.

Voorbeeld: Als iemand niet terug stuurt, vraagt ge of die nog beschikbaar is

**Acces Method:** met kabel of zonder kabel

## Message Delivery Options

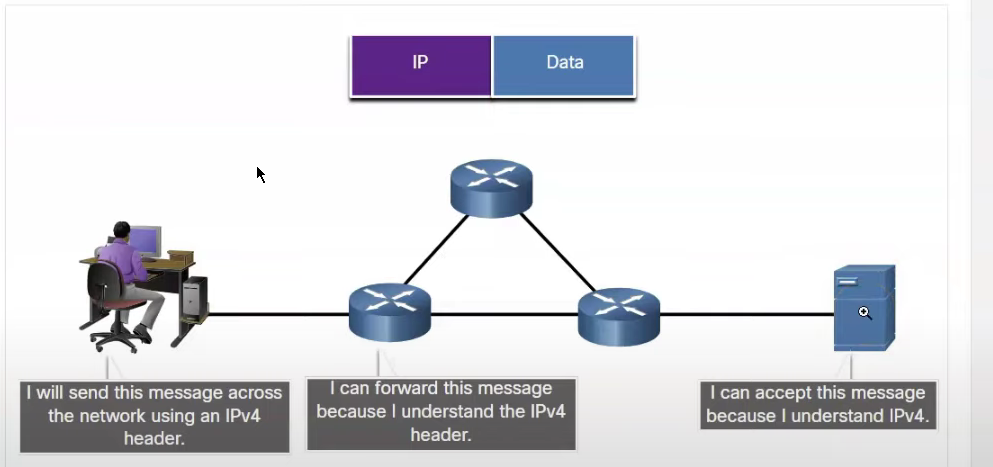
Bij ipv4

* Unicast: Dit is 1 op 1
* Multicast: naar een aantal pc’s sturen
* Broadcast: naar iedereen iets sturen

## Network Protocol Overview

* Network Communications Protocols
  + IP
    - Om andere pc te kunne begrijpe
  + TCP
    - Zeker zijn dat data goed word ontvangen
  + HTTP
    - Waar webservers mee spreken
* Network Security Protocols
  + SSH
    - hoe je via secure shell shell commands kunt uitvoeren
  + SSL
    - Dus dit dient voor HTTPS. Als je naar u bank gaat bv hoe daar alles wat je via de lijn verstuurd geencrypteerd verloopt
  + TLS
    - Opvolger van SSL
* Routing Protocols
  + Dit is meer voor de volgende Boek. Welke weg kan de pakketje het best nemen.
* Service Discovery Protocols
  + DHCP
    - Computer moet ip-adres weten, hij kan dit krijgen van DHCP. Hij kan hieruit de ip-adres krijgen, de default gateway, dns, welke netwerk je zit.
  + DNS
    - Als die dat weet, vraagt die wil je me de ip addres geven van de zogezegde website.

## Network Protocol Functions



**Addressing:** ipv6, Ethernet, ipv4

**Reliability:** zeker zijn dat alles goed verloopt en ook zeker zijn dat het echt is verlopen => TCP

**Sequincing:** 1 groot data wordt over meerdere kleinere data verstuurd. En ieder pakket kan via verschillende wegen verstuurd worden. Dit zorgt er voor dat alles op juiste volgorde wordt gezet.

**Error Detection:** Die gaat de foute mappen herkennen en gaat die opnieuw verzenden ervoor zorgen dat die toch correct verlopen.

**Application Interface:** dit zijn de applicaties op zich proces-to-proces. https en https als we het hebben over webservers.

## Protocol Interaction

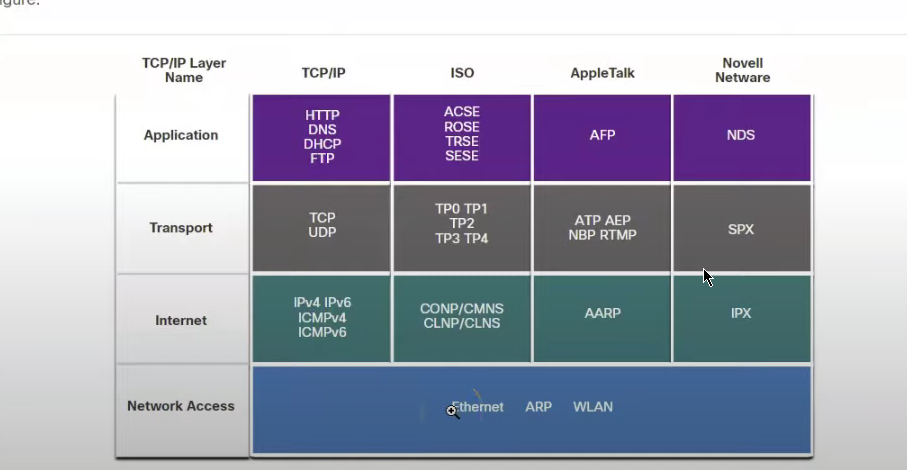
**HyperText Transfer Protocol(HTTP):** aanvraag van u default pagina. Poort 80. https => poort 443

**Transmission Control Protocol(TCP):** We willen zeker zijn dat het goed loopt.

**Internet Protocol(IP):** van ons ip naar zijn ip.

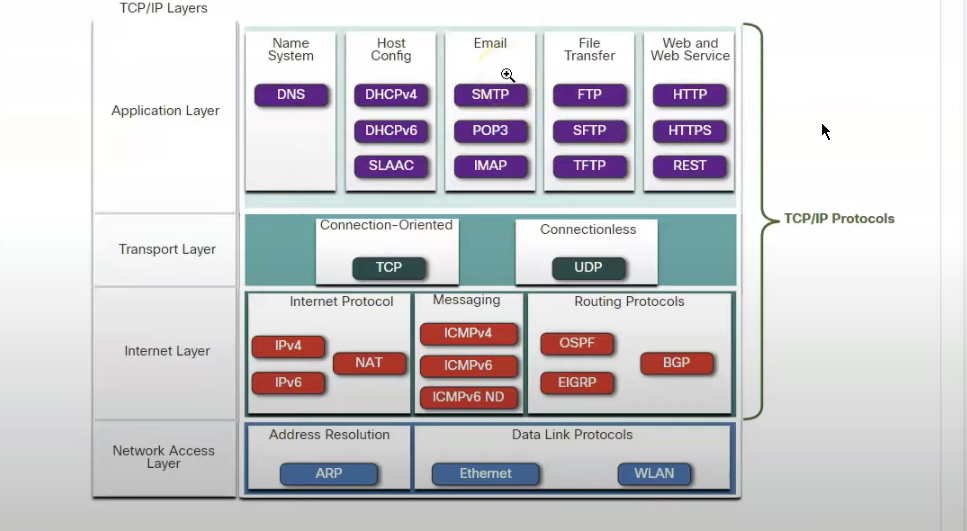
**Ethernet:** Het moet zorgen dat het eerst uit u eigen default gateway uitgaat endan communiceren ze met MAC-Adressen.

## Evolution of Protocol Suites

****

**Netwerk Access:** Hoe geraak hij op de kabel, hoe geraak ik aan de eerste device binnen mij netwerk(dus mac-adres van default gateway).

## TCP/IP Protocol Suite



**EMAIL**

* **SMTP:** Simple Mail Transfer Protocol Dit is om mails te versturen en ontvangen.
* **POP3:** om mails binnen te halen, mails afhalen en plaatsen op u lokale machine.
* **IMAP:** Synchroniseren, hiermee zit je eigenlijk te praten.

**File transfer**

* **FTP:** Dit is op files op servers te plaatsen, downladen
* **SFTP:** FTP over SSH
* **TFTP:** FTP versie protocl dat mekkelijk is om op te zetten ,maar waar je niet veel kan doen om op u hand te zette => veelgebruikt door hackers

**Web and Web Service**

* **HTTP:** Het verkeer kan gesnift worden
* **HTTPS:** hier kan je niet sniffen dus dit is geëncrypeert

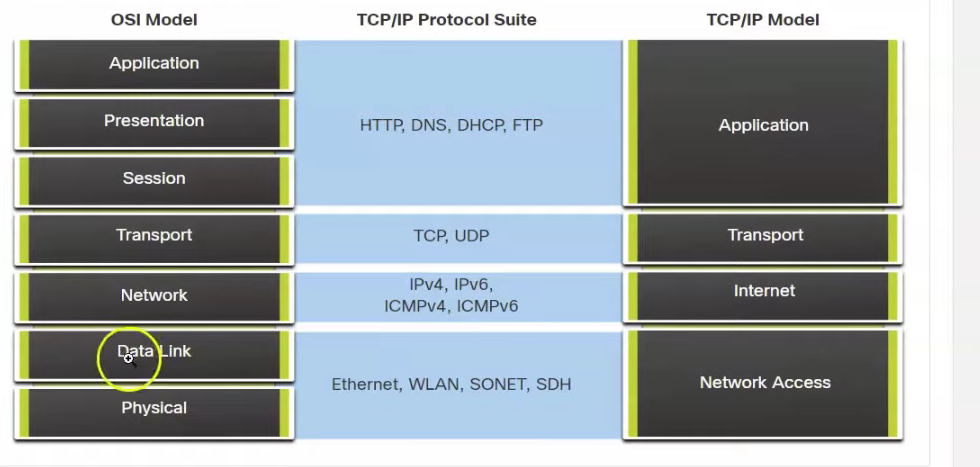
**UDP:** Connectionless als iets fout is laat die dat. Bij TCP vraagt die dat opnieuw aan hier laat die dat gewoon.

**NAT:** Dit zorgt ervoor dat je in een LAN netwerk ip addressen kan hergebruiken.

**ICMP:** ping commando: graag zou die antwoorden terug willen en krijgt die ook.

**ARP:** Eerst gebeurt het via IP addressen de communicatie zeg maar en dan wordt eerst een vraag gesteld welke mac-address ze allebei hebben want ze zitten binnen hetzelfde netwerk

## Reference Models



Alle lagen communiceren met elkaar, maar zitte los van elkaar.

**Laag1:** Hier zit u netwerkbekabeling in, welke netwerk je hebt.

**Laag2:** Hier zitte je MAC-addressen

**Laag3:** Hier werk je met IP-adressen. Het begint van u eigen addres naar zijn address

**Laag4:** Is de stroom goed aangekomen of niet. Betrouwbaarheid

**Laag5:** Encryption TLS en SSL. Als ge connectie maakt, dan moet ge een passwoord ingeven. Als ge t elang wacht krijg je een session time out

**Laag6:** Hoe moet de data hier gepresenteerd worden

**Laag7:** De applicatie zelf, DNS

## Data Encapsulation

**Segmentatie:** van 1 grote bestand meerdere kleinere bestanden maken

**Multiplexing:** bestanden in elkaar verweven(in elkaar zetten).

**Sequiencing:** nummering van de mappen en die ook op volgorde zetten.

## Protocol Data Units

Hoe een pakketje eruitziet op elke layer.

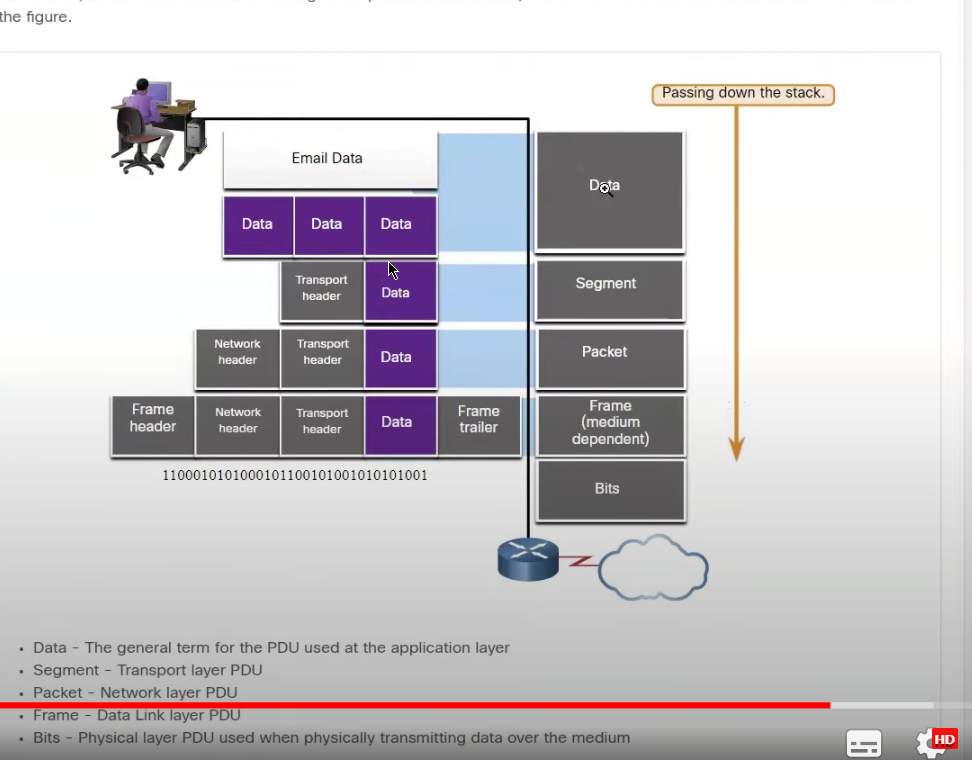
Physical layer => Bits

Data Link Layer => (Ethernet) Frame

Network Layer =>(IP) Packet

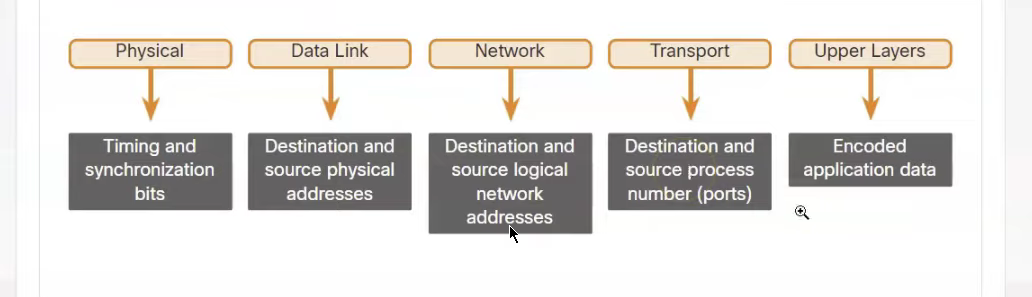
Transport Layer =>(Transport) Segment

Application layer =>(Application) Data

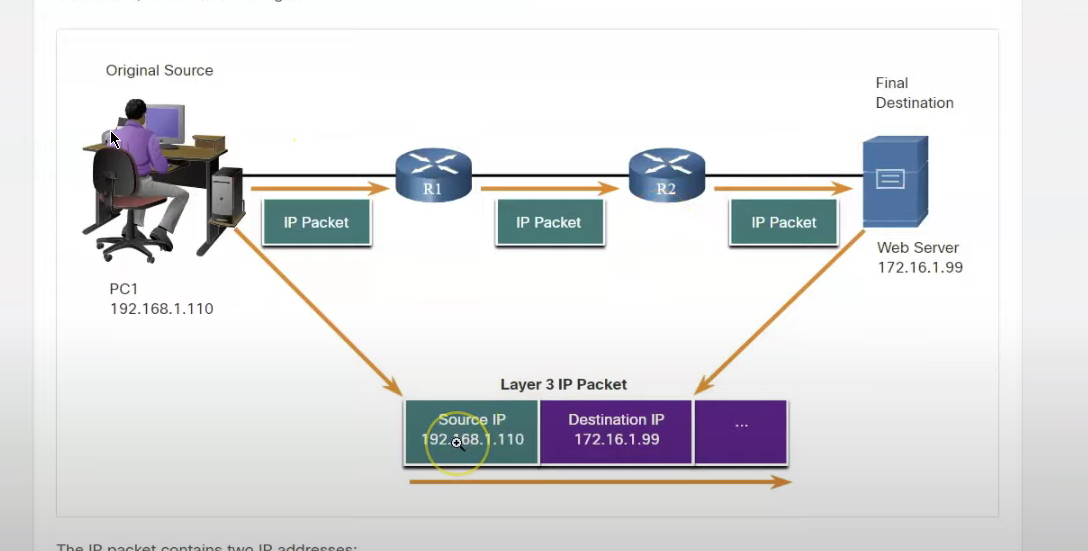


## Addresses

**Mac-addressen:** dit wordt gebruikt voor dezelfde netwerk



IP-addressen veranderen nooit, indien je gaat werken met nat.



U IP address bestaat uit een netwerk address en een host gedeelte(Dit zal je nog zien later)

# Chapter 4: Physical layer

Niet alleen voor software, maar ook hardware. Ge kunt alles fysiek zien.

## The Physical connection

Alles wat te maken heeft met hardware, alles wat te maken heeft met bekabeling en transporteren van data.

Routers kan je op verschillende manieren verbinden, via netwerkkaart. Die zit in je laptop. 2 manieren waarmee je kan verbinden is:

* Wireless verbinden
* Met kabel verbinden(internet kabel)

**De physical layer heeft 1 doel.** Transporteren van data. Dit doet hij aan de hand van frames. Frames worden niet doorgestuurd als softwareblok, maar als hardwareblok. De Data link laag gaat dus iets verplaatsen op dat medium door middel van stroom of van elektromagnetisch ding (wireless) of lichtimplusen.

Mac-adressen zitten in Ethernet frame, die zitten dan ge embed in u netwerk kaart.

## Physical layer standard

De protocol die te maken heeft met ethernet gedeelte en dat is IETF(Internet Engineering Task Force.

Encoding: Encoding is eigenlijk een manier om meer data tegelijk kunt doorsturen.

0=>1 (stijgen is 1) 1=>0 (dalen dus 0)

Hoe meer spanningsniveau hoe meer gelijktijdige bits je eraan kunt koppelen.

**Multi mode Fiber:** Meerdere signalen tegelijk

* Voordeel
  + De core wordt dikker dus die gaat meer botsen dus je kan meerdere signalen tegelijk doen omdat die niet in 1 rechte lijn lopen
* Nadeel
  + iets meer tijd nodig om signalen te sturen

**Singel mode Fiber:** 1 signaal tegelijk en ook in 1 richting op hetzelfde moment

* Voordeel
  + Geen botsing dus energie kan verder
  + Ook als ge 2 verschillende kabels gaat gebruiken(ene voor het sturen ene voor het ontvangen)

**Wireless:** er worden gewoon electromagnetische signalen van de ene kant gestuurt en andere kant opgenomen

**Bandbreedte(mogelijke capaciteit):** Hoe meer bandbreedte hoe meer data er kan gestuurd worden

****

**Througput:** Wat er effectief over de band gaat.

**Goodput(effectieve bruikbare data signalisatie enz word ervan af getrokken):** wat je er als data echt door gooit.

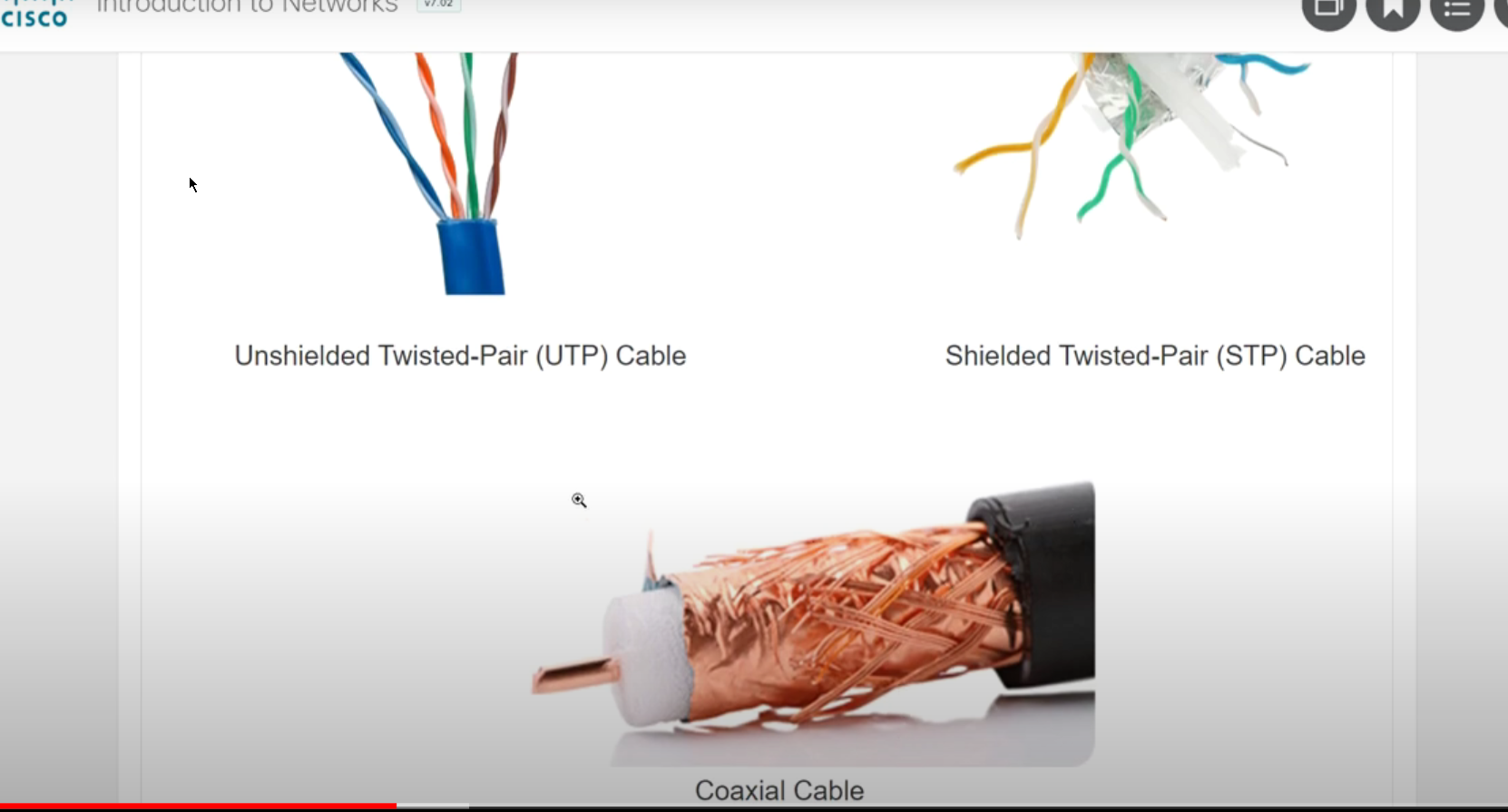
**Latency:** Is de vertraging tussen het versturen en ontvangen(hoe langer de kabel hoe meer Latency.

## Characterics of Copper Cabling

**Unshielded Twisted-Pair:** 2 soorten koper bekabeling. Die 2 kabels worden om elkaar draait omdat als er een storing is dan gaat die indetiek zijn om bijde kabels. Op de ene gaat negatieve signalen zijn en bij de ander gaat het positieve signalen zijn. Allebei optellen endan delen door 2 gaat die de foutmeldingen wegwerken.

**Shielded Twisted-Pair:** Kooi van faraday zorgt ervoor dat de stroom via de buitenkant komt wegfilteren naar de aarding

**Coaxiel Cable:** zelfde werking als Shielded Twisted-Pair

****

**Nadelen:**

* Strongen kan je krijgen => Electromagnetische Interference of Radio Frequenct Interference => Dit kan bepalen of je een kopere kabel kan gebruiken of niet.

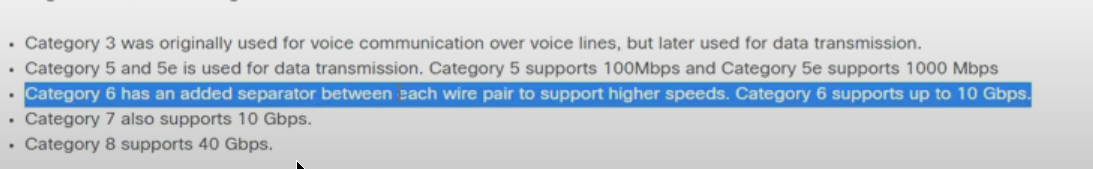
**Voordelen:**

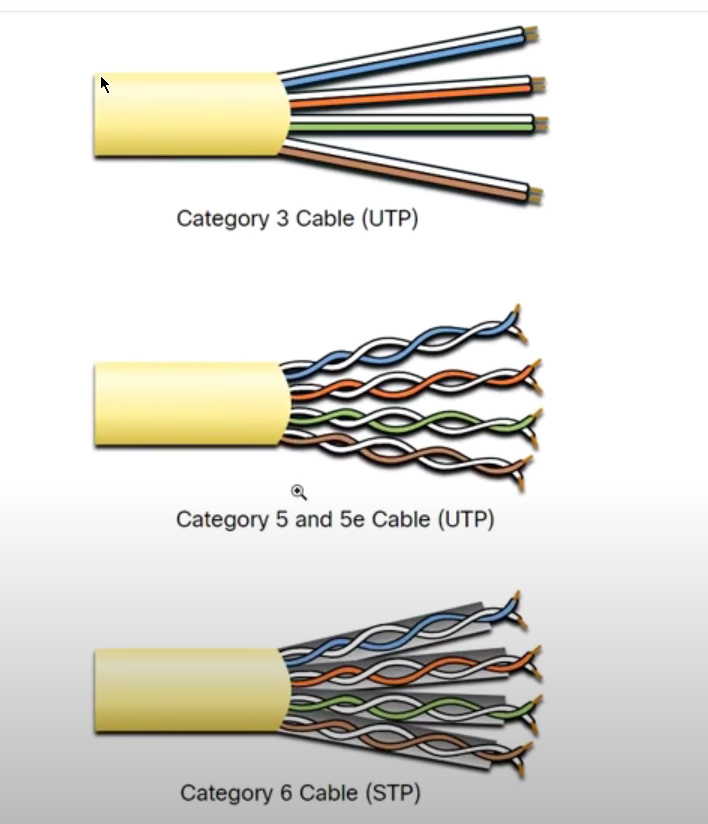
* Goedkoop 10 keer goedkoper dan fiber
* Makkelijk te plaatsen(makkelijker te draaien)

**3 Connectors**

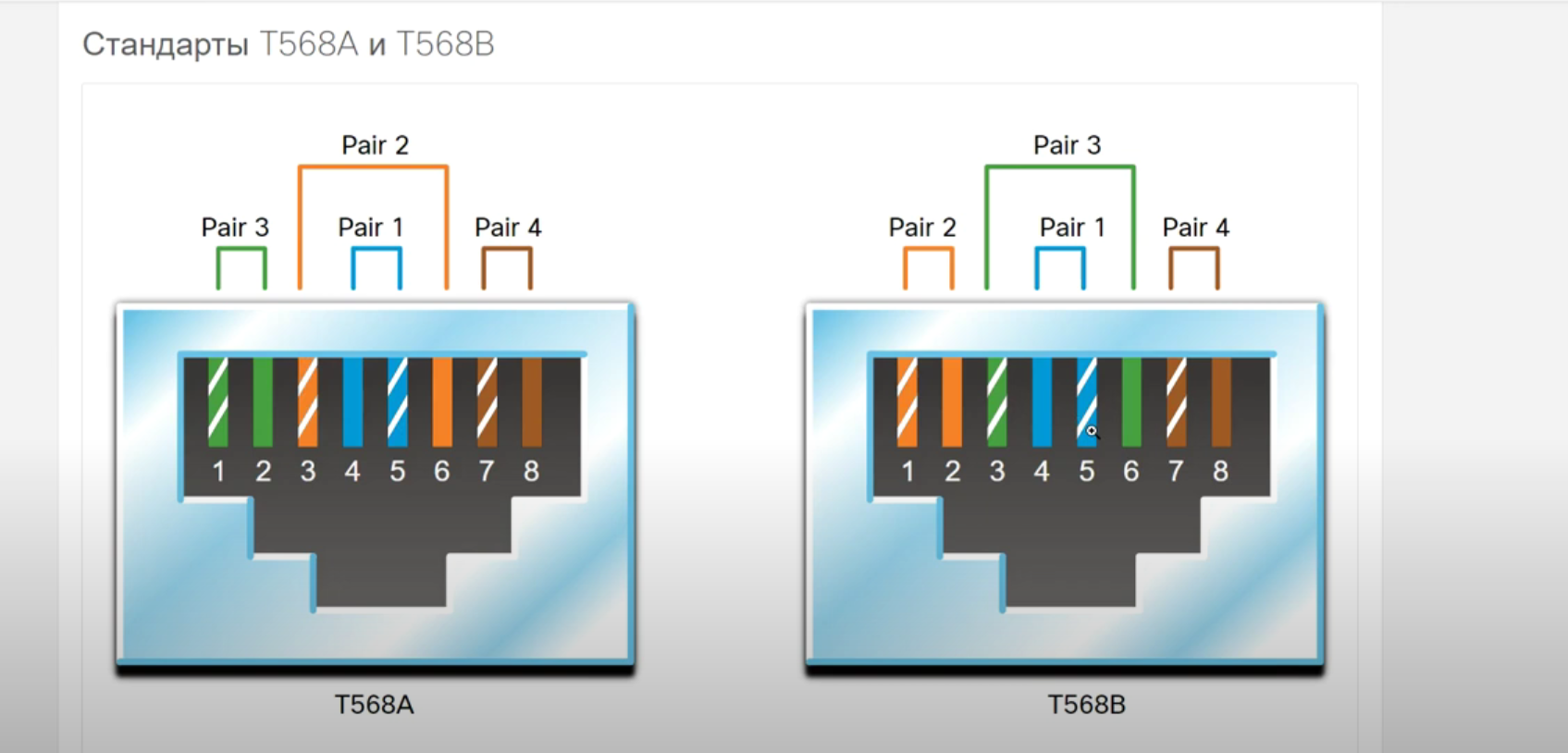
* BNC
* N Type
* F Type (verbinding te maken met versterker)

**Soorten UTP Cabeling(Hoe hoger de ranking hoe meer data je kan versturen en sneller):**





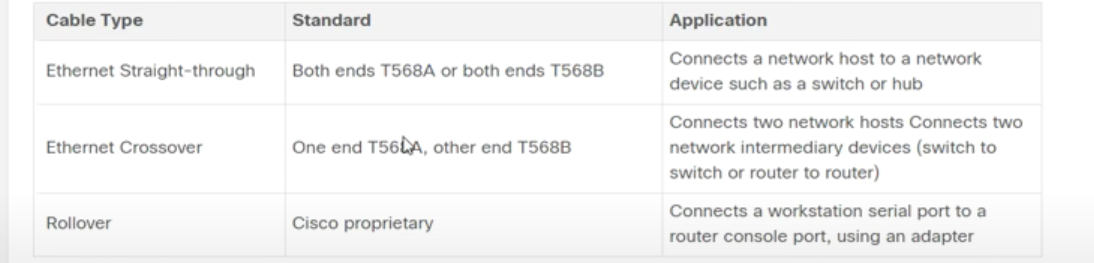
RJ-45 enkel te gebruiken voor UNShielded(plastic)



**Ethernet Straight-Through:** Dit dient voor pc’s en swithes

**Ethernet Crossover:** CrossoverCable

**Rollover(enkel voor configuratie):** kleurtjes achter elkaar geplaatst

****

## Fiber Optic Cabling

**Grote verschil tussen koper bekabeling:**

* Dit is dunner hier zit maar 1 core in en bij de kopere kabel zit er 4.
* Fiber is flexibeler

**Voordeel:**

* Geen electromagnetische inferentie
* Omdat ge met licht werkt dus langere afstand zelfde kabel gebruiken(ge kunt soms zelfs 100 km met eenzelfde kabel

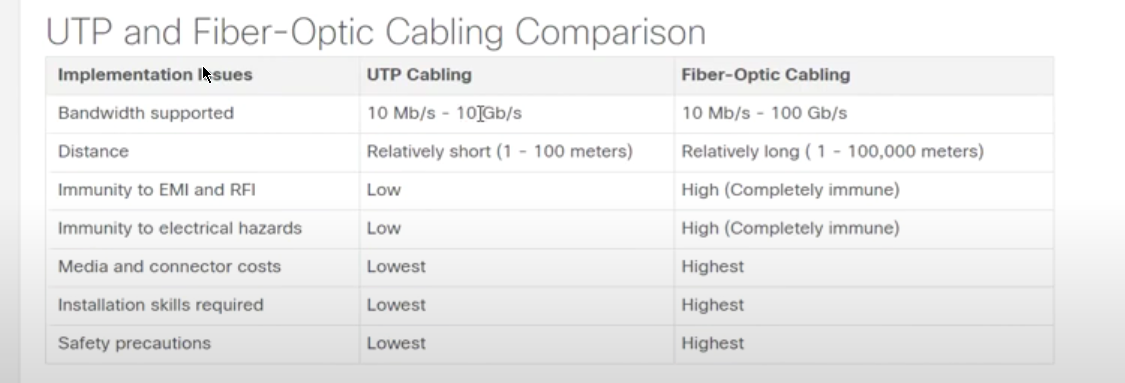
**Verplicht als je 2 gebouwen met elkaar wilt verbinden**

Fiber cable wordt gebruikt bij bedrijven die veel data wilt transporteren of waar bedrijven veel elektromagnetische stralingen kan zijn. En ook als je over het zee wilt versturen.

De kleur orange: Multimode

De kleur geel: Singel mode

**Verschil**

****

## Properties of Wireless Media

Voordeel

* Geen kabel meer nodig je kan zitten waar je wil

Nadeel

* Hoe meer personen op internet zit hoe trager het internet dus hoe lager bandbreedte

**WIFI:** Wireless LAN

**Bluetooth**: communicatie tussen toestellen

**WiMaX**: grotere dekking dan WIFI, maar vergelijkbaar, speciale netwerkkaarten

**Zigbee**: vergelijkbaar met Bluetooth lower power communicatie(IOT devices)

**Wireless acces point:** bedraadde kabel omzet naar wifi

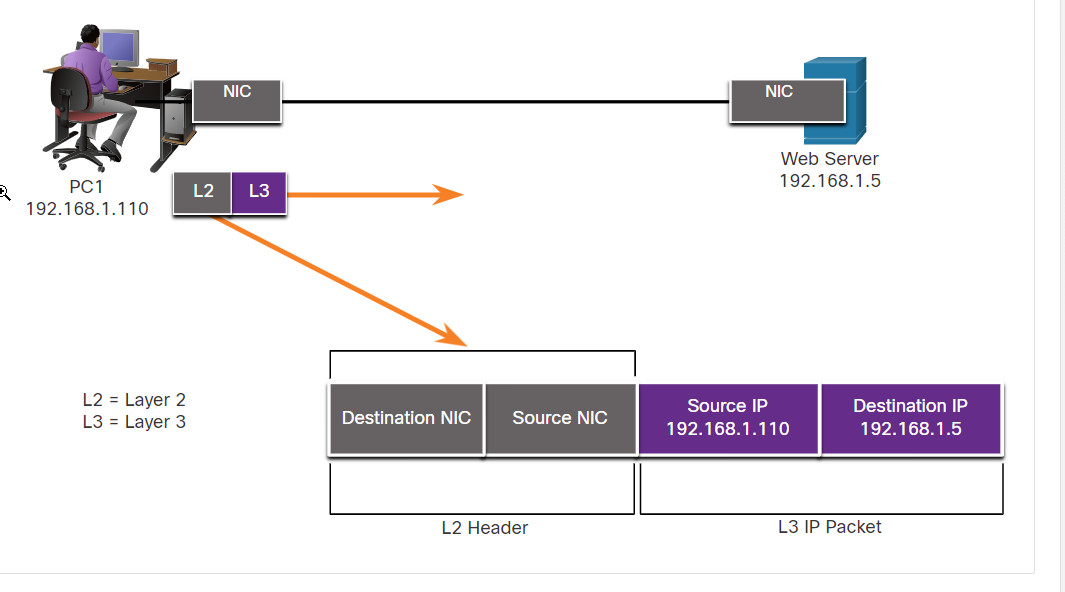
# Chapter 6: Data Link Layer

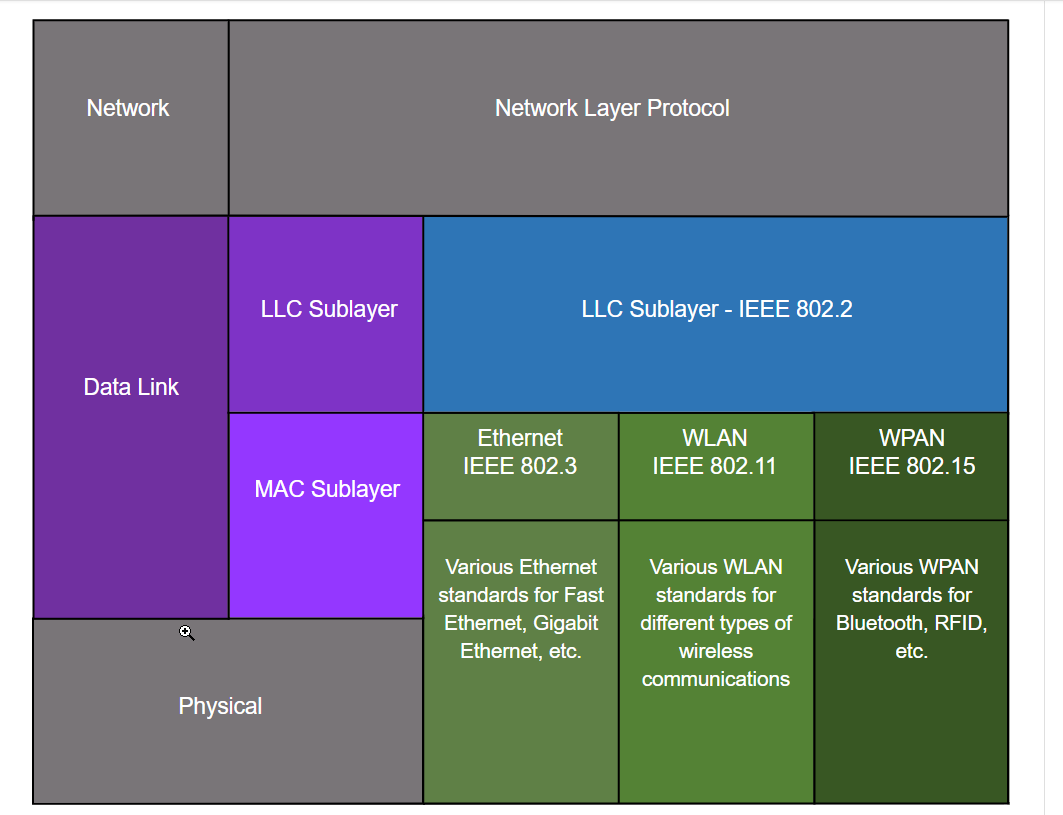
Rechtstreeks verbonden met hardware, verbindt ons met wat ons laat transporteren dus IP. Verbindingen tussen netwerk laag naar physical layer.

* Zorgt ervoor dat we data kunnen transporteren van onze IP protocol naar physical laag. Hardwarematig apparaat(netwerkkaart gecontroleerd door data link layer.
* Die accepteert pakkets die van IP protocol komen die vertaald die in een hardw arematige taal richting onze physical laag en die voegt er een adressering aan.
* Hij controleert of in de data(frames) geen fouten zitten. => error detection

Frame: bestaat uit data heeft 2 ip adressen(thuis adres en bestemmingsadres) endan gaat die een destination nic en source nic toevoegen(deze gegevens dienen voor het eerste communicatie).

De 2 NICS(mac-adressen), gaan veranderen van netwerk naar netwerk en de IP’s niet.





**MAC Sublayer** => hardware gedeelte(die zorgt voor hardwarefunctionailteite om gegevens die komen van onze connectors van physical gedeelte omzetten naar digitele bits en dit doen die voor onze LLC Sublayer). Dit zorgt er ook voor dat u mac-adres uniek is. Controleeert of er foute in zijn(error detection) => de frame wordt dan gewist. Wanneer er een frame start of stopt => frame delimiting.

**LLC Sublayer** => Software gedeelte(de driver van onze hardware gaat dan zorgen dan dat die communicatie verloopt van onze hardware richting onze ip) Zorgt ook voor de adressering destination NIC, controle of er geen foute in zitte in het data en controle of het data echt bestemd is.

Bij de data link layer gaat het de hele tijd van de ene medium naar de andere. Endan gaat de mac-adressen(source destination) de hele tijd veranderen.

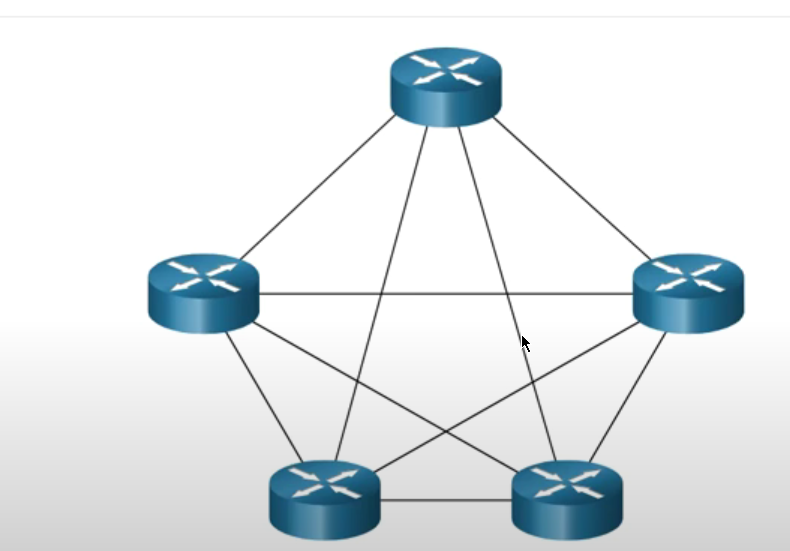
## Physical and logical Topologies

**Physical Topologies:** wanneer ge de hardware apparatuur ziet en hardwarematige bekabeling en ook de locatie. Hier kunnen ook nummering van sockets zitten.

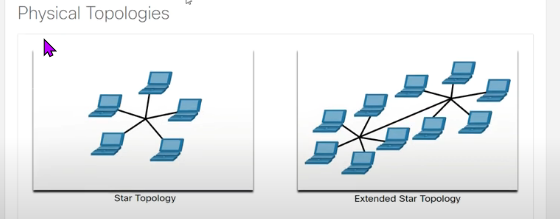
**Logical Toplogies:** Alles wat te maken heeft met software. De computers kunnen ook virtuele machines zijn, alles wat te maken heeft met services en IP adressen. Ook de configuratie wordt hier getoond

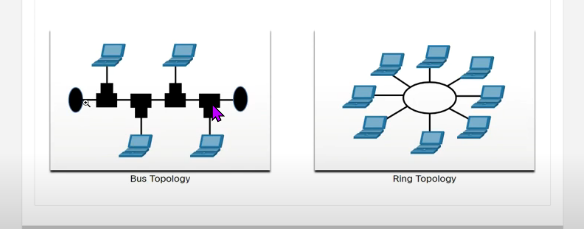
WAN topologies

* Point-to-Point(Point-to-Point protocol)
  + 1 dedicated toestel maakt verbinding met 1 andere toestel
    - Voordelen
      * Data die over die lijn gaat is dedicated(niet gedeeld wordt met andere destination) makkelijker beveiligd en makkelijker te encrypteren.
* Hub and Spoke
  + 1 centraal apparaat waar alle connecties naar toegaan
* Mesh(ookal gaat ene verbinding “kapot” kan het nog steeds naar de eindbestemming gaan via een andere weg).



Dit is bij de LAN(lokale netwerk)





**Half and full duplex Communication :** Als 2 toestellen met elkaar communiceren wordt er tussen de toestellen data getransporteerd. Bij full gelijktijdig data ontvangen en verzonden. Bij Half wordt er eerst verzonden daarna pas ontvangen.

**Acces Control Method:** Dit kijkt of hij echt kan communiceren.

Eerst ga je luisteren dus kijken of er iets op de kabel staat en kijken of je mag verzenden(en blijft luisteren als de stroom niet gaat verschillen) als die botsen gaat het stoppen **=> CSMA/CD(carrier sense Multiple access with collision** detection). Als 2 toestellen toch gelijktijdig wille verzenden (stroompulsen) als die met elkaar in contact komen(botsen), wordt die niet meer leesbaar.

Hier ga je een melding doen dat je aan het zenden bent en jullie moeten wachten tot ik melding geef dat jullie mogen zenden. Zorgen dat er geen botsingen mogelijk zijn=> **(carrier sense Multiple access with collision avoidence)**

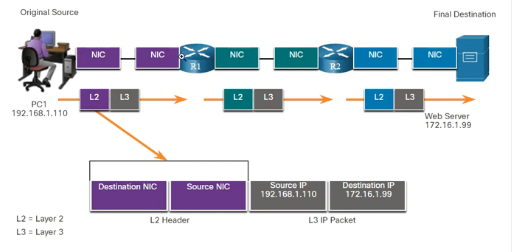
**CSMA/CD =>** bekabeld ethernet(pc stuurt een frame, kijkt of die geen botsing meemaakt)

**Een HUB:** verbindt alle kabels met elkaar(verbindt dit gwn met pc’s). Dit luistert ook of er 2 toestellen niet tegelijker tijd verzenden.

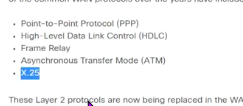
Frame

* Header
  + Begin van een frame(source, destination)
  + Controle => cyclic redundancy check(CRC)
* Data
* Trailer
  + Controle of er een fout is
  + Delimiter(dus kijken of er een limiet is dus wanneer die moet stoppen





Protocollen om van 1 fysieke kaart naar een andere fysieke kaart te gaan



Samengevat Data link layer: Zorgt voor communicatie tussen IP gedeelte in onze netwerk laag en hardware in onze physical layer. Met vele protcollen.

# Pakket Tracer

Een switch kijkt altijd naar een frame, mac-adress en vult altijd de mac-adress aan en gaat ook forwarden.

**ARP** gaat ervoor zorgen dat je via u ip adres een mac address vindt(die gaat zogezegd roepen in u netwerk en vraagt “wie heeft deze ip adres” en doet dit met behulp van het broadcast

# Commando’s

**en**  
**show mac address-table =>** ge kunt u mac-adressen enz zien en ook op welke poorten die mac-adressen zijn  
**clear mac address-table =>** leegmaken van het tabellen(en als deze gecleared is gaat die kijken naar de tabel en omdat die leeg is gaat die naar iedereen sturen.)  
**met ping “ip adress” =>** kan je de computers met elkaar late communiceren  
**arp -a =>** laat u ip adres zien en een bijhorende mac-adres  
**arp -d =>** cleared u arp table  
**clear arp cache =>** cleart gewoon de cache