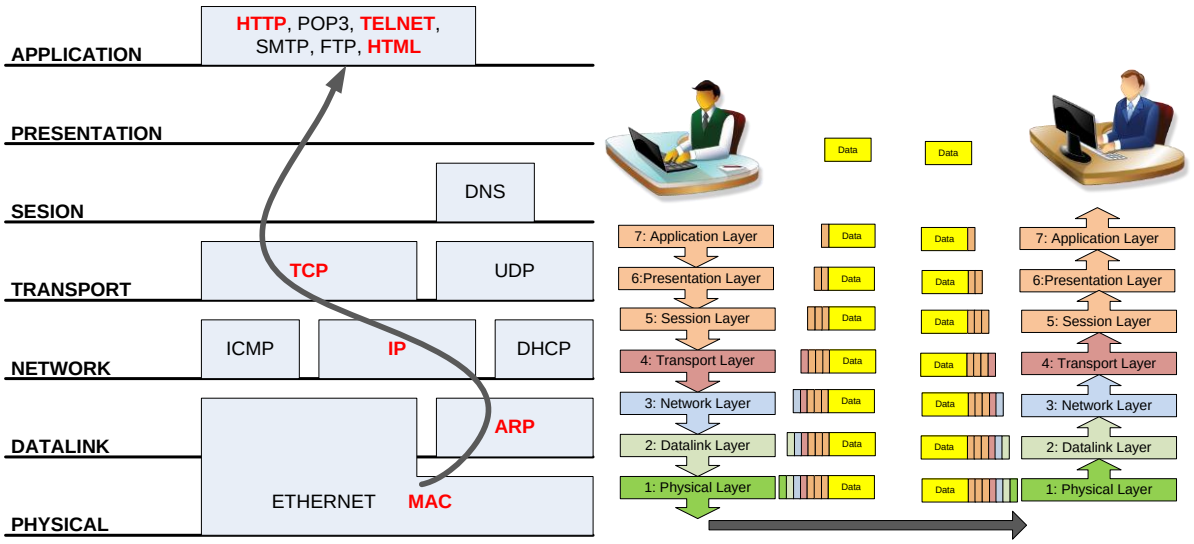
## INHOUD

## ETHERNET – INTERNET PROTOCOL

Nagenoeg iedereen gebruikt computers in een netwerk, al dan niet draadloos. Iedereen gebruikt data van 'het internet'. Deze vorm van communicatie is zo ver door-ontwikkeld dat gebruikers vandaag eigenlijk geen kennis meer moeten hebben van hoe dit alles eigenlijk werkt. We proberen in deze lessen op een eenvoudige manier uit te leggen hoe de toegepaste protocollen er voor zorgen dat al dit netwerkverkeer 'zonder' problemen blijft verlopen…

Al de toegepaste netwerk-protocollen passen allemaal in meer of mindere mate op het OSI of 7 lagen model.




Specifiek voor computernetwerken nemen de lagen volgende taken voor zich:

| | |
|---|---|
| Physical | kabels, spanningen en bitsnelheid, hubs |
| Datalink | Mac addressing, COLLISION detection, Switches |
| Network | IP adres, subnet masker, DHCP, ARP, Routers |
| Transport | TCP, UDP, Poortnummers, NAT routers, Firewall |
| Session | DNS – hoe sessie met server starten |
| Presentation | Codering berichten (meestal in Application verwerkt) |
| Application | Internet explorer, Outlook express, … |

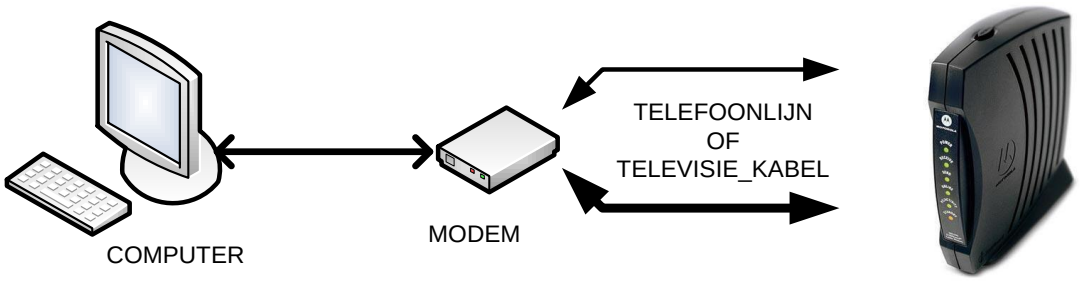
De meest voor de hand liggende manier is dat we laag voor laag zullen bespreken wat er in deze laag gebeurt. Voor heel het computernetwerk en internet gebeuren zijn de 4 onderste lagen de meest belangrijke.

## LAYER 1: PHISICAL LAYER

In de PHYSICAL LAYER worden er afspraken gemaakt over het type kabel en de wijze waarop de bitstroom over deze kabels verstuurd wordt.

### MODEM VERBINDINGEN:

Meestal is je PC verbonden met het internet via een modem. Breedband data die gemoduleerd binnen komt op de TV kabel of op de telefoonlijn wordt door de modem gedemoduleerd of omgekeerd wordt data van uw PC gemoduleerd door de modem om deze op het wereld wijde web te zetten via kabel of telefoonlijn.

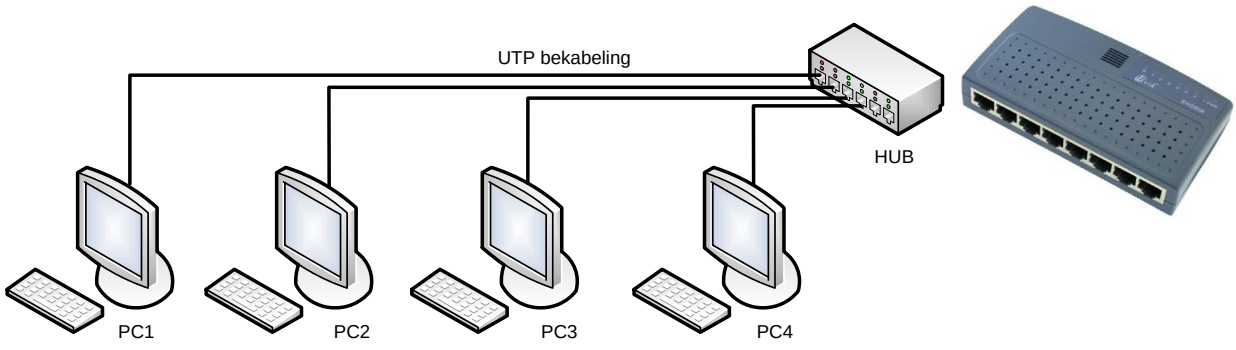



### LAN NETWERKEN

Pc's die zich allemaal op dezelfde locatie (gebouw, bedrijf, school) bevinden kunnen allen via een LAN met elkaar gekoppeld worden. LAN staat voor Local Area Network – een lokaal netwerk dus.

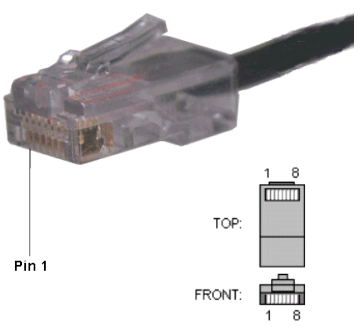
Op deze manier kunnen er bestanden en printers gedeeld worden tussen de verschillende Pc's in het netwerk. Indien één van de Pc's of de HUB ergens een connectie heeft met het internet, dan kan ook deze internetverbinding gedeeld worden.

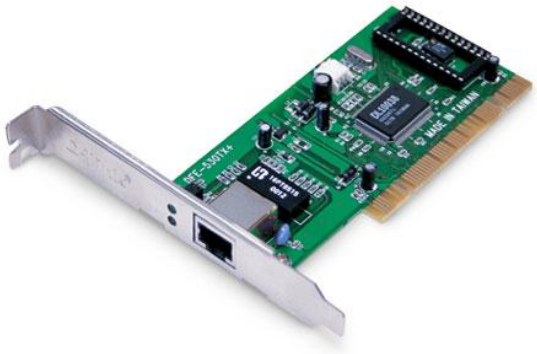
### HUB




De HUB (Engels voor NAAF of SPAAK van een wiel) verbindt alle Pc's met elkaar. Alle Pc's 'zien' dan alle data die door eender welke deelnemer op het netwerk gezet wordt. De HUB is een 'dom' LAYER 1 apparaat dat zonder de data of adressen te analyseren alle binnenkomende data verdeelt naar alle Pc's die aan deze hub hangen. Dat zorgt voor veel onnodig netwerkverkeer en dat is ook de reden dat zeker voor iets grotere netwerken hubs vervangen worden door de veel intelligentere SWITCHES. Meer over SWITCHES in LAYER 2.

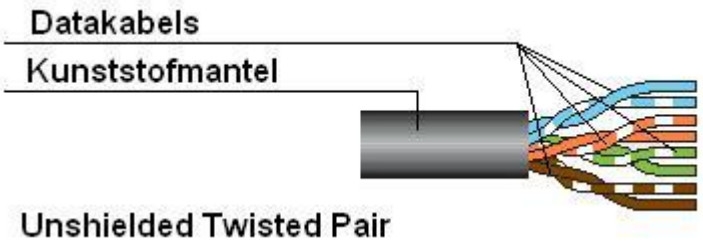
## NETWERKKAART



Elke computer moet voorzien zijn van een netwerkkaart. U ziet hier de aansluiting voor een RJ45 aansluiting van een UTP kabel.

## UTP BEKABELING




Tot voor enkele jaren kwamen er ook nog coax netwerken voor, maar vandaag zijn bijna alle netwerken uitgevoerd met UTP bekabeling. UTP staat voor Unshielded twisted pair. Er bestaat ook STP of Shielded Twisted pair kabel waar er een extra metalen afschermfolie rond de kabel, de signalen moet beschermen tegen extreme stoorpulsen. De snelheden zijn 10Mbit, 100Mbit of zelfs 1Gbit (er worden ook al snelheden tot 10Gbit gehaald over UTP kabels).

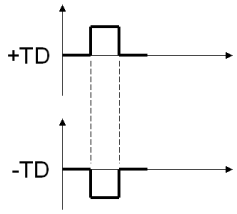
Er is een verschil in de manier waarop data tegen deze 3 snelheden over deze zelfde CAT5 UTP bekabeling wordt getransporteerd.

Standaard Ethernet CAT5 kabels hebben 8 draadjes – verdeeld over 4 paartjes. De 10BaseT (10Mbps) en de 100BaseT (100Mbps) gebruiken hiervan slechts 2 paartjes. Eén paar om te zenden (TX) en één paar om data te ontvangen (RX).

Bekabeling 10BaseT en 100BaseT

| Pin | Kleur | Functie |
|---|---|---|
| **1** | Wit-groen | +TD |
| **2** | Groen | -TD |
| **3** | Wit-oranje | +RD |
| **4** | Blauw | Niet gebruikt |
| **5** | Wit-blauw | Niet gebruikt |
| **6** | Oranje | -RD |
| **7** | Wit-bruin | Niet gebruikt |
| **8** | bruin | Niet gebruikt |

De data op deze draden wordt altijd differentieel verstuurd. Op de ene draad staat het inverse signaal van de andere draad. Mogelijke storingen kunnen zo makkelijk worden weg gefilterd.



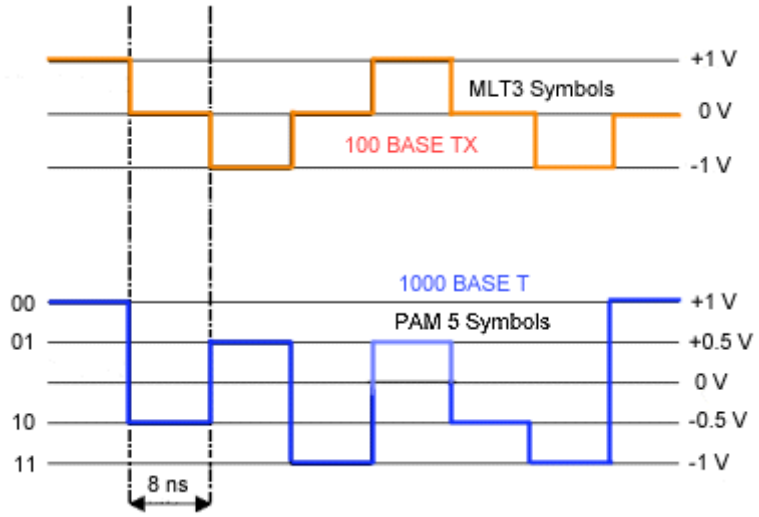

## 10BASET

Bij 10BaseT wordt er per periode 1 bit data doorgezonden. Een transmissiesnelheid van 10Mbits/sec vereist dus een kloksnelheid van 10Mhz.

## 100BASET

Bij 100BaseT netwerken wordt de data gecodeerd in een 10 bit data-woord om een bepaalde mate van error detectie bij in het bericht te steken. Om hiermee dus een snelheid van 100Mbps te halen moet de klok van een 100BaseT netwerk draaien op 125Mhz (10/8 x 100Mbps) . Cat5 kabels zijn ontworpen om signalen tot 125Mhz te kunnen transporteren.

## 1000BASET




1000BaseT of GIGABIT Ethernet past een ander soort codering / modulatie toe om binnen de bandbreedte van 125Mhz toch 1000Mbps te halen. 1000BaseT past een speciale vorm van Amplitude modulatie (4D-PAM5) toe en gebruikt hierbij verschillende amplitudes om per periode toch 2 databits door te kunnen sturen. Binnen de bandbreedte van 125Mhz wordt de transmissiesnelheid hiermee reeds verdubbeld naar 250 Mbps.

Een tweede aanpassing is dat GIGABIT alle 8 draden van de UTP kabel gebruikt i.p.v. slechts 4 draden bij 100BaseT.

Hier bovenop worden dezelfde draden gebruikt voor zenden als voor ontvangen in een soort half duplex methode, ook dit in tegenstelling met 100 en 10 BaseT waar er afzonderlijke paren waren om te zenden of te ontvangen.

Door al deze maatregelen kan GIGABIT de 1000Mbps halen zonder de maximale kloksnelheid van de UTP CAT 5 kabel te verhogen. 125Mhz x 2 bits per periode x 4 signalen per periode = 1000Mbits.

In principe kan dezelfde CAT5 kabel dus gebruikt worden voor Gigabit, maar vermits er gelijktijdig over 4 paartjes gezonden en ontvangen wordt is de kans op overspraak veel groter. Dit heeft geleid tot een CAT5e kabel waarvan de twists iets anders uitgevoerd worden om deze overspraak tegen te gaan.

De stelling dat GIGABIT draait tegen 1GHz is dus fout. GIGABIT draait tegen 125MHz.

Bekabeling GIGABIT

| Pin | Kleur | Functie |
|---|---|---|
| **1** | Wit-groen | +BI_DA |
| **2** | Groen | -BI_DA |
| **3** | Wit-oranje | +BI_DB |
| **4** | Blauw | +BI_DC |
| **5** | Wit-blauw | -BI_DC |
| **6** | Oranje | -BI_DB |
| **7** | Wit-bruin | +BI_DD |
| **8** | bruin | -BI_DD |

## LENGTE VAN UTP BEKABELING

Netwerksignalen zijn zeer zwak (+/-1Volt) wat deze signalen gevoelig maakt voor storingen en wat ook maakt dat enige verzwakking snel gevolgen kan hebben. Bij zowel 10BaseT, 100BaseT als 1000BaseT is de maximale kabellengte daarom vastgelegd op 100 meter. Om de 100 meter moet er een versterker geplaatst worden die het signaal terug krachtig genoeg maakt om zonder storing verder te kunnen.

## GLASVEZEL

Vooral voor de overbrugging van grotere afstanden wordt er dikwijls gekozen voor glasvezel. De optische signalen in glasvezelkabels kunnen veel grotere afstanden overbruggen alvorens ze moeten worden versterkt. Glasvezel wordt dan gebruikt als een zogenaamde 'BACKBONE'. De hardware die nodig is voor glasvezel is veel duurder dan die voor UTP, maar vermits er minder REPEATERS nodig zijn is glasvezel voor lange afstanden toch de beste keuze.

## UITDAGINGEN PHYSICAL LAYER

- Benoem en bespreek de functie van enkele typische LAYER 1 hardware apparaten
- Leg gedetailleerd het verschil uit tussen 10Mbit, 100Mbit en 1000Mbit netwerkcommunicatie (modulatie, spanningen, soorten kabels, functie van de draden)
- Bespreek de functie van een HUB en meteen ook het nadeel van een HUB
- Waarom word er voor kortere afstanden bij voorkeur UPT gebruikt en voor langere afstanden Glasvezel?

# LAYER 2: DATALINK LAYER

Het doel van de DATALINK LAYER is het foutloos overbrengen van een gegevenspakket van een PC naar een andere PC.

## MAC ADRES

Omdat alle Pc's via de HUB parallel met de ethernetkabel zijn gekoppeld, moet er een systeem van unieke adressering toegepast worden. Dit is nodig om ervoor te zorgen dat een bericht slechts door de PC aan de welke het bericht verstuurd wordt, wordt verwerkt. Daarom is in elke Ethernet-netwerkkaart een wereldwijd uniek adres van 6 bytes vast geprogrammeerd. Dit MAC adres wordt toegekend door de fabrikant van de netwerkkaart. Een MAC of HARDWARE adres ziet er als volgt uit:

MAC ADRES: 00:20:AC:23:56:FE

Men schrijft de waarde van elke byte in hexadecimaal. De getallen worden gescheiden door een dubbele punt. Op deze wijze verkrijgt elke PC wereldwijd een uniek MAC-adres. Er zullen dus geen twee Pc's in de wereld zijn met hetzelfde MAC adres.

## ETHERNET FRAME – DATALINK LAYER


Ethernet

Een typisch layer2 ethernet bericht begint met enkele startbytes, dan volgt het MAC adres van de bestemming van de data en het MAC adres van de bron van de data. Beide MAC adressen zijn 6 bytes lang zoals eerder besproken. Het type veld geeft het type of de lengte van de data aan. De data zelf kan bestaan uit 45 tot 1500 bytes. De CHECKSUM is een soort CRC die de ontvanger gebruikt om te controleren of de data wel correct is aangekomen.

## COLLISION DETECTION

Collision detection is eveneens een Layer 2 materie. Het mag duidelijk zijn dat als 2 Pc's op het zelfde ogenblik hun bericht op het netwerk zetten, dat de data dan corrupt wordt. Om deze botsingen of COLLISIONS te detecteren zijn er enkele afspraken die mee in LAYER 2 verwerkt zitten:

- De PC die wil zenden wacht tot het netwerk in rust is.
- Als een tweede PC op hetzelfde moment begint te zenden worden beide berichten verminkt. Beide Pc's luisteren zelf mee naar hun eigen berichten en merken dat er wat misloopt. Dit heet een COLLISION. Bij een COLLISION worden de volgende stappen doorlopen:
    - Elke PC die bij de COLLISION betrokken was start een TIMER. De tijd op deze timer is voor elke PC verschillend (random). De PC bij wie de timer als eerste afloopt start opnieuw het zenden.
    - Indien bij de tweede poging opnieuw een COLLISION plaatsvindt start deze zelfde procedure opnieuw.

## SWITCH


LAN SWITCHES zien er hetzelfde uit en hebben in principe ook dezelfde functie als HUBS, namelijk het verbinden van verschillende computers, printers e.d. via ethernetkabels in een netwerk.

Het probleem bij HUBS is dat HUBS 'domme' LAYER 1 apparaten zijn. Alle data die van 1 PC komt wordt door de HUB verdeeld naar alle Pc's in dit netwerk. De Pc's moeten zelf maar – a.d.h.v. het MAC adres van de bestemmeling in het ethernet bericht - beslissen of het bericht voor hen bestemd is. Dit is een onnodige belasting van het netwerk.

SWITCHES zijn in principe 'slimme' HUBS. SWITCHES analyseren het ethernet-bericht, filteren hier het DESTINATION MAC ADRES uit en sturen dit bericht enkel maar naar de PC met dit MAC adres. Dat maakt dat SWITCHES LAYER 2 apparaten zijn en dat HUBS LAYER 1 apparaten zijn.

Bij het aanschakelen van de switch onderzoekt de SWITCH welke Pc's met welke MAC adressen op welke poort van de SWITCH zijn aangesloten. De SWITCH houdt deze info bij in een "LOOKUP TABLE". Het gebruik van SWITCHES i.p.v. HUBS verhoogt de snelheid van grotere netwerken aanzienlijk. Vandaag (2012) worden er nog weinig HUBS gebruikt.

## UITDAGINGEN LAYER 2 - DATALINK

Waarom zijn switches layer 2 apparaten en hubs layer 1 apparaten
Teken een LAYER2 Ethernet frame en benoem de verschillende blokken en hun functie
Hoe worden er in Layer2 collisions gedetecteerd?
Wat is de procedure die doorlopen wordt indien er een collision gedetecteerd werd?
Hoe ziet een MAC adres er uit?
Hoe kan het dat alle MAC adressen wereldwijd uniek zijn?

## LAYER 3: NETWORK LAYER

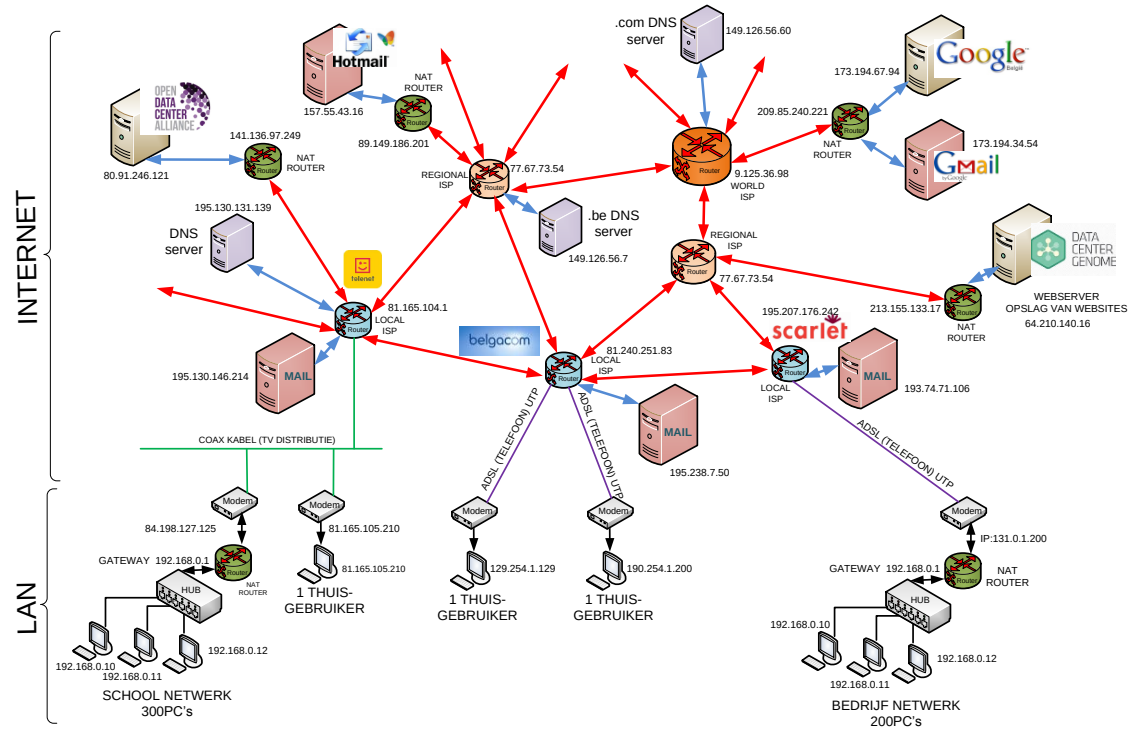
Grotere netwerken of WAN's (Wide Area Network) – zoals het internet – zijn eigenlijk een koppeling van vele LAN's.

Als we te maken krijgen met wereldwijd aan elkaar gekoppelde netwerken moet er een betere methode van adressering bestaan (beter dan MAC) om elke computer in dit wereldwijde netwerk te kunnen bereiken zonder dat alle computers in dit wereldwijde netwerk dit bericht voorbij zien komen en zelf moeten beslissen of dit al dan niet een bericht voor hen is. Dat zou een extreme overbelasting van het netwerk vormen.

Omdat computers nu niet meer via een HUB allemaal aan dezelfde kabel hangen moet er ook een manier zijn zodat een bericht weet welke ROUTE het moet volgen om de juiste bestemming te bereiken.

Zowel deze wereldwijde adressering (IP ADRES) als de ROUTING functie treffen we aan in deze LAYER 3, de NETWORKLAYER.

### ROUTER BASIS




Als je een bericht wil versturen van een PC in het SCHOOL NETWERK naar een PC in het BEDRIJFSNETWERK, dan zorgt de router er voor dat het bericht de juiste route volgt. De router 'ziet' aan het adres dat het bericht niet bedoeld is voor het LAN en zal het bericht doorsturen naar het internet waar het door een andere router zal worden binnen gepakt. Routers beslissen op basis van het DESTINATION IP ADRES welke ROUTE het bericht zal volgen, dat maakt dat ROUTERS LAYER 3 apparaten zijn.

Zo bestaan er NAT ROUTERS die specifiek ontworpen zijn om een scheiding te maken tussen INTERNET en LAN netwerken. Dit type routers werkt zelfs in LAYER 4 en wordt daar verder besproken. Het internet zelf is opgebouwd uit LEVEL 3 LOCAL, REGIONAL EN WORLD ROUTERS die al het internetverkeer regelen. De meeste van deze routers worden beheerd door ISP's – INTERNET SERVICE PROVIDERS zoals wij Telenet en Belgacom

kennen. Deze ISP's zijn op hun beurt weer klant van grotere ISP's en zo is het internet eigenlijk helemaal opgebouwd.

## IP ADRES

Het INTERNET is het grootste WAN netwerk ter wereld en om hier aan te kunnen deelnemen wordt er een specifieke adressering toegepast. De adressen worden IP ADRESSEN genoemd. IP komt van "INTERNET PROTOCOL". Voor elke internetaansluiting ter wereld is er één uniek IP ADRES nodig. U hebt zo thuis voor één PC één uniek IP ADRES nodig van uw INTERNETPROVIDER, een school met bijvoorbeeld 300 Pc's heeft ook slechts één uniek IP ADRES gekregen van zijn INTERNETPROVIDER en een bedrijf met 200 Pc's krijgt ook slechts één uniek IP ADRES toegewezen van zijn INTERNETPROVIDER. de "Internet Assigned Numbers Authority " (IANA) organisatie is verantwoordelijk voor het uitdelen (verkopen) van alle unieke IP ADRESSEN in de wereld.

Een IPV4 adres bestaat uit 32 bits. Het wordt meestal verkort geschreven als 4 decimale getallen – gescheiden door een punt. Bijvoorbeeld: 192.168.0.10. Dit zelfde getal wordt door computers echter gewoon binair verwerkt en zo zouden wij dit ook altijd moeten bekijken als we exact willen begrijpen wat er gebeurt…

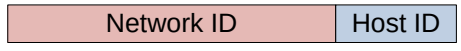
| | | | | |
|---|---|---|---|---|
| IP Adres Decimaal | 192 | .168 | .0 | .10 |
| IP Adres Binair | 11000000 | .10101000 | .00000000 | .00001010 |

## SUBNET MASKER

Het SUBNET MASKER is een snelle manier om in netwerken aan de PC's aan te geven of het bericht naar een IP ADRES binnen het huidige netwerk moet gestuurd worden of dat het een bericht is voor een ander netwerk. Op deze manier zorgt IP dus reeds voor een zekere routering.

SUBNET MASKERS zijn eveneens 32 bits lang – identiek aan IP ADRESSEN. Ook dit masker wordt meestal decimaal geschreven maar om te kunnen begrijpen hoe computers hiermee omgaan moeten we dit ook binair schrijven.

| | | | |
|---|---|---|---|
| IP ADRES: | 192.168.0.10 | Binair: | 11000000.10101000.00000000.00001010 |
| SUBNET MASK: | 255.255.254.0 | Binair: | 11111111.11111111.11111110.00000000 |




Dit SUBNET MASKER is altijd een reeks 1-tjes met daarachter een aanvulling met 0-en tot je aan 32 bits zit. Het aantal nullen is het HOST ID gedeelte en bepaalt hoeveel unieke IP ADRESSEN er in dit specifieke netwerk kunnen voorkomen. In dit geval zijn dit 9 bits – $2^9 = 512$ – dus 512 unieke IP ADRESSEN.

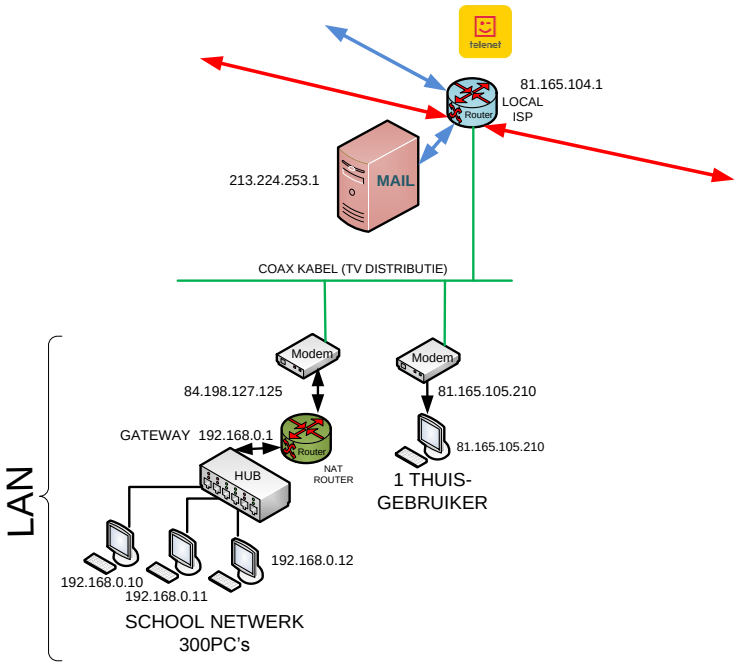
| | | | |
|---|---|---|---|
| IP ADRES TX: | 192.168.0.10 | Binair: | **11000000.10101000.0000000**0.00001010 |
| IP ADRES RX: | 192.168.0.12 | Binair: | **11000000.10101000.0000000**0.00001100 |
| SUBNET MASK: | 255.255.254.0 | Binair: | **11111111.11111111.1111111**0.00000000 |

Network ID | Host ID

Het NETWORK ID gedeelte bepaalt welke gedeelde van het IP ADRES het globale adres is van dit bepaalde LAN netwerk. Als het NETWORK ID gedeelte van het IP adres van de zender en van de ontvanger identiek is – zoals dat in bovenstaande situatie het geval is - dan weten de computers in dit netwerk dat het bericht bedoeld is voor het lokale netwerk en dat dit bericht dus niet naar het "WORLD-WIDE-WEB" moet worden gestuurd. De zender is immers PC10 in netwerk 192.168.0 en de ontvanger is PC12 in dat zelfde 192.168.0 netwerk. Geen enkele reden dus om PC's buiten dit netwerk te storen met dit bericht.

| | | | |
|---|---|---|---|
| IP ADRES TX: | 192.168.0.10 | Binair: | **11000000.10101000.0000000**0.00001010 |
| IP ADRES RX: | 80.100.1.20 | Binair: | **01010000.01100100.0000000**1.00010100 |
| SUBNET MASK: | 255.255.254.0 | Binair: | **11111111.11111111.1111111**0.00000000 |

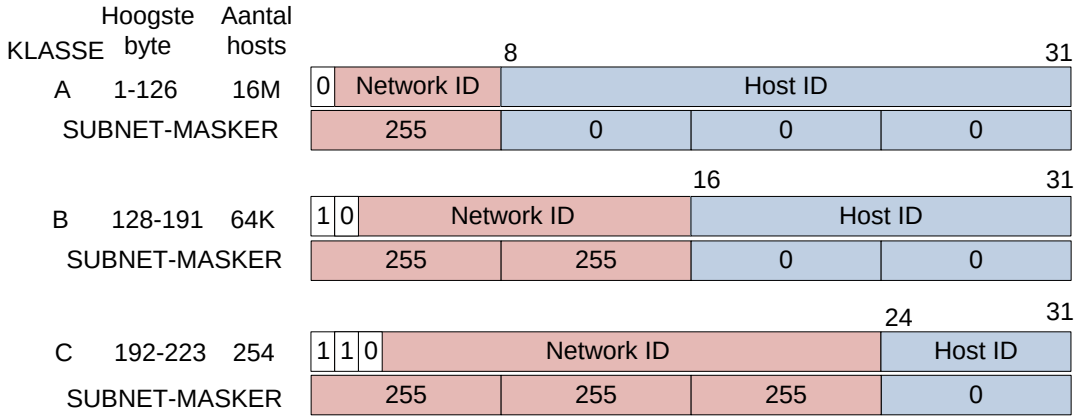
Network ID | Host ID




Bovenstaand voorbeeld illustreert een IP ADRES van de RECEIVER (RX) waarvan het NETWORK ID gedeelte niet identiek is aan dat van de TRANSMITTER (TX). Dit bericht is duidelijk niet bedoeld voor het lokale netwerk en zal meteen naar het STANDAARD GATEWAY IP adres van de ROUTER (192.168.0.1) gestuurd worden om zo via het "WWW" op z'n juiste locatie terecht te komen.

## KLASSE A, B EN C IP ADRESSEN

Hoe kleiner de NETWORK ID – hoe minder verschillende netwerken er mogelijk zijn, maar hoe meer unieke IP ADRESSEN er kunnen worden uitgedeeld. De "Internet Assigned Numbers Authority" heeft hier een zekere structuur in gebracht.




Zo zijn er klasse A, klasse B en klasse C adressen.

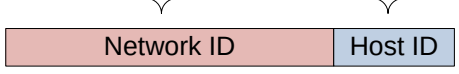
Vermits de MSB van een klasse A adres altijd een 0 moet zijn, kunnen er wereldwijd in principe slechts 128 klasse A netwerken bestaan. In een klasse A netwerk kunnen wel $2^{24}$ of meer dan 16 miljoen unieke IP ADRESSEN worden uitgedeeld. Klasse A adressen worden dus enkel uitgedeeld aan WORLD ISP's (INTERNET SERVICE PROVIDERS die op wereldschaal 'HET INTERNET' verdelen naar REGIONALE ISP's). Het SUBNET MASKER van een klasse A netwerk is steeds 255.0.0.0 of kleiner. De eerste byte van een klasse A netwerk ligt steeds tussen 1 en 126.

Er kunnen wereldwijd meer dan 64.000 klasse B netwerken bestaan die elk 64.000 unieke IP ADRESSEN kunnen uitdelen. Doordat klasse B IP ADRESSEN met 10 beginnen ligt de hoogste byte van een klasse B netwerk steeds tussen 128 en 191. Het STANDAARD SUBNET voor een klasse B netwerk is 255.255.0.0. Grote bedrijven en ISP's krijgen zo één of meerdere klasse B adressen toegewezen waaronder ze zelf dan op hun beurt ook weer 64.000 unieke IP ADRESSEN kunnen uitdelen.

Van Klasse C netwerken kunnen de meeste bestaan, maar onder klasse C netwerken kunnen er slechts 256 unieke IP ADRESSEN worden uitgedeeld. Het SUBNET van een klasse C adres is steeds 255.255.255.0.

IP ADRES: 192.168.0.10 Binair: 11000000.10101000.00000000.00001010

SUBNET MASK: 255.255.254.0 Binair: 11111111.11111111.11111110.00000000

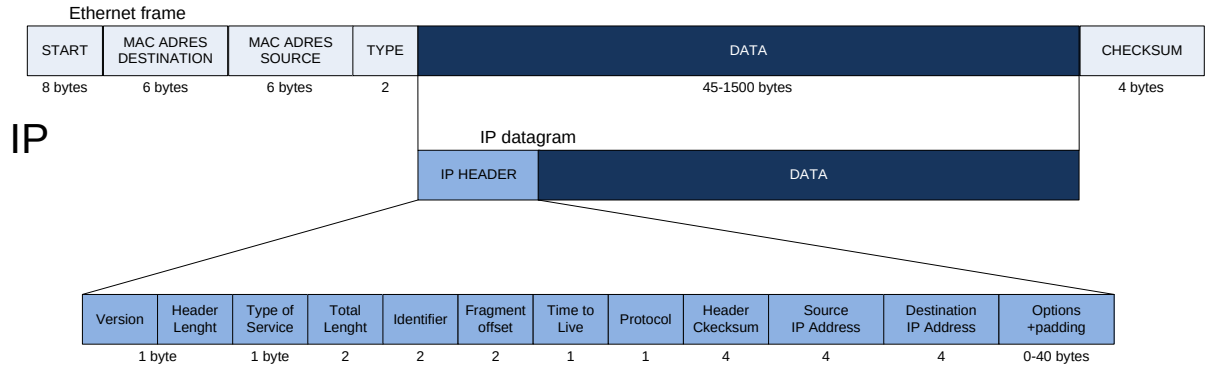



In ons voorbeeld hebben we reeds gezien dat die SUBNETS niet steeds 255 moeten zijn. Zo is het SUBNET in ons voorbeeld 255.255.254.0. Dit wordt ook al beschouwd als een klasse B netwerk (wat de theorie die hierboven verkondigt wordt meteen wat nuanceert) en hieronder kunnen zoals eerder vermeld tot 512 unieke adressen worden uitgedeeld.

Binnen de A, B en C netwerken is er telkens een range voorzien die nooit door de "Internet Assigned Numbers Authority" zullen worden uitgedeeld. Deze adressen mogen gebruikt worden om mee te testen:

| KLASSE | Begin | Einde |
|---|---|---|
| A | 10.0.0.0 | 10.255.255.255 |
| B | 172.16.0.0 | 172.31.0.0 |
| C | 192.168.0.0 | 192.168.255.255 |

## ETHERNET FRAME – NETWORK LAYER




Om het IP PROTOCOL mee in de bestaande ETHERNET berichten in te werken neemt men enkele bytes van het DATA-FRAME af en zet men hier de IP HEADER in. Er blijft echter nog ruim voldoende dataruimte over.

We bespreken kort enkele van de belangrijkste blokjes van het IP DATAGRAM

**Version** : aanduiden of het om IPV4 of IPV6 gaat

**Header Lenght** : aanduiding hoe lang deze IP header zal zijn – uitgedrukt in aantal 32 bit WORDS

**Total lenght** : aanduiding hoe lang deze IP header zal zijn – uitgedrukt in aantal bytes

**Identifier** : berichten die te groot zijn worden opgedeeld in kleinere berichten – elk van deze fragmenten krijgt een IDENTIFIER mee zodat het bericht nadien terug correct kan worden samengesteld.

**Time to live** :dit is een getal dat bij elke passage van een router met 1 verlaagt. Als het aan 0 komt wordt het complete bericht gewist. Dit is om te vermijden dat berichten die nooit hun destinatie bereiken eeuwig zouden blijven 'rondzweven' op het internet.

**Protocol** : geeft aan welk 'higher level' protocol gebruikt zal worden – voor TCP is dit het getal 06 , voor UDP de waarde 17.

**Header checksum** : een eenvoudig (niet CRC) datacontrole-getal dat wordt meegestuurd zodat routers snel kunnen nakijken of de data in de header nog correct is.

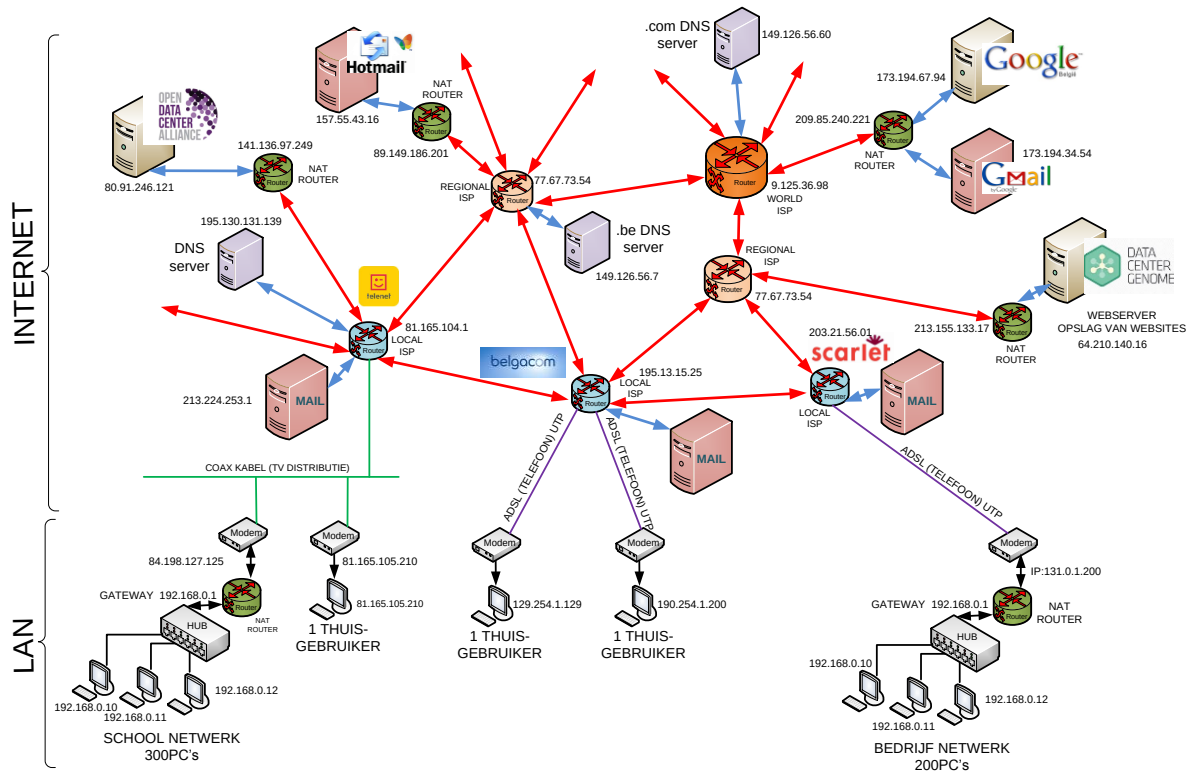
**Source IP** : dit bevat het 4 byte IP adres van de afzender

**Destination IP** : dit bevat het 4 byte IP adres van de ontvanger

**Padding** : header aanvullen met 0-en zodat het op een veelvoud van 32 bits komt.

**Data** : data

## INTERNET IP ADRESSEN TOV LAN IP ADRESSEN




Bij de thuisgebruikers dient het IP ADRES van de enige PC het IP ADRES te zijn dat hij van zijn ISP gekregen heeft. Bij netwerken van meer dan 1 PC staat er een NAT ROUTER (NETWORK ADDRESS TRANSLATION ROUTER) tussen het INTERNET en het LAN. IP ADRESSEN binnen dit LAN netwerk moeten zo niet meer wereldwijd uniek zijn, ze moeten enkel uniek zijn binnen dit LAN. Zo ziet u hier dat binnen het bedrijfsnetwerk dezelfde IP adressen gebruikt kunnen worden als binnen het schoolnetwerk. Elk bericht dat van één van de Pc's van het netwerk naar buiten gaat passeert langs de NAT ROUTER die het IP adres van eender welke lokale PC verandert in het IP adres dat de router van de ISP gekregen heeft nl: 84.198.127.125. Langs de zijde van het internet lijkt het dus alsof alle berichten die van eender welke PC in het schoolnetwerk komen, toch maar van slechts 1 PC komen met IP ADRES 84.198.127.125.

De belangrijkste reden van het bestaan van NAT ROUTERS is dat het niet meer lukt om met onze 32 bits IPV4 adressen alle netwerkapparaten in de wereld een uniek adres te geven. Met 4 bytes kunnen we ongeveer 4 miljard unieke IP ADRESSEN uitdelen en die waren begin 2011 allemaal uitgedeeld. Door gebruik te maken van NAT ROUTERS kunnen we na een NAT ROUTER terug helemaal onze eigen zin doen met IP adressen. Dit was een manier om snel een oplossing te vinden op de snel slinkende IPV4 adressen. De exacte werking van NAT ROUTERS komt aan bod in LAYER 4. Een bijkomend voordeel (of nadeel) is dat alle Pc's achter een NAT ROUTER perfect anoniem blijven. Het is zeer moeilijk om te achterhalen van welke PC achter de NAT router het bericht kwam.

De STANDAARD GATEWAY is het IP adres van de router

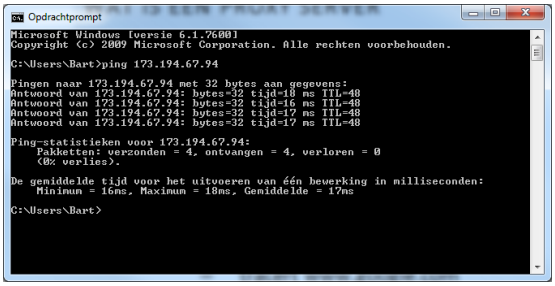
Een meer permanente oplossing is IPV6. IPV6 is de 128 bits opvolger van IPV4 en hiermee is het mogelijk om elke aardbewoner ongeveer 50 quadriljard IP adressen te geven… genoeg om even toe te komen dus…

IPV4 Address: 192.168.0.125 (32 bits of 4 bytes)

IPV6 Address: 125.235.102.056. 045.178.255.0. 0.156.0.23. 45.56.126.147 (128 bits of 16 bytes)

De overgang van IPV4 naar IPV6 is gestart in 2010 en is zeer nauwkeurig gepland om gefaseerd over vele jaren in te voeren, maar het bestaan van NAT ROUTERS maakt deze invoering wel complexer. We behandelen hier IPV4 omdat dit momenteel nog het meeste wordt toegepast.

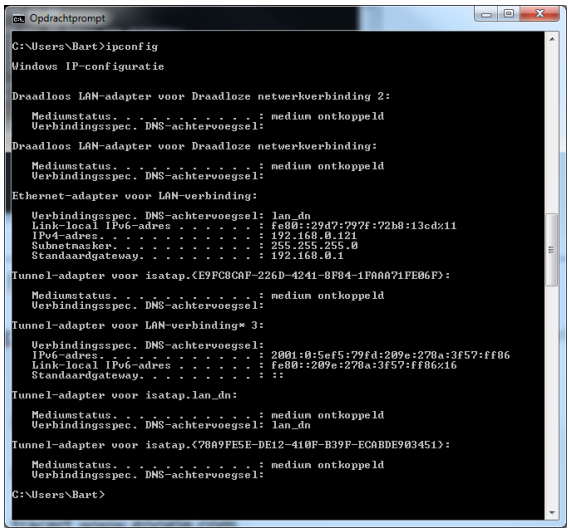
## PING




Gebruik >ping 173.194.67.94 in de opdrachtprompt om te controleren of er een verbinding kan gemaakt worden met een bepaald IP adres binnen of buiten uw LAN - dit IP adres is dat van www.Google.be. Er word dan een aantal pogingen gedaan om connectie te maken met dit IP adres en de tijd die het duurde om deze connectie op te zetten wordt telkens weergegeven.

## IPCONFIG OF IPCONFIG /ALL

Gebruik >ipconfig om te onderzoeken wat het IP adres is van uw PC, welk subnet masker, welke gateway ed is. Met >ipconfig/all kom je nog meer te weten. De STANDAARD GATEWAY is het IP adres van de router in uw netwerk. Meestal is dit het laagste IP adres in de range – bv 192.168.0.1

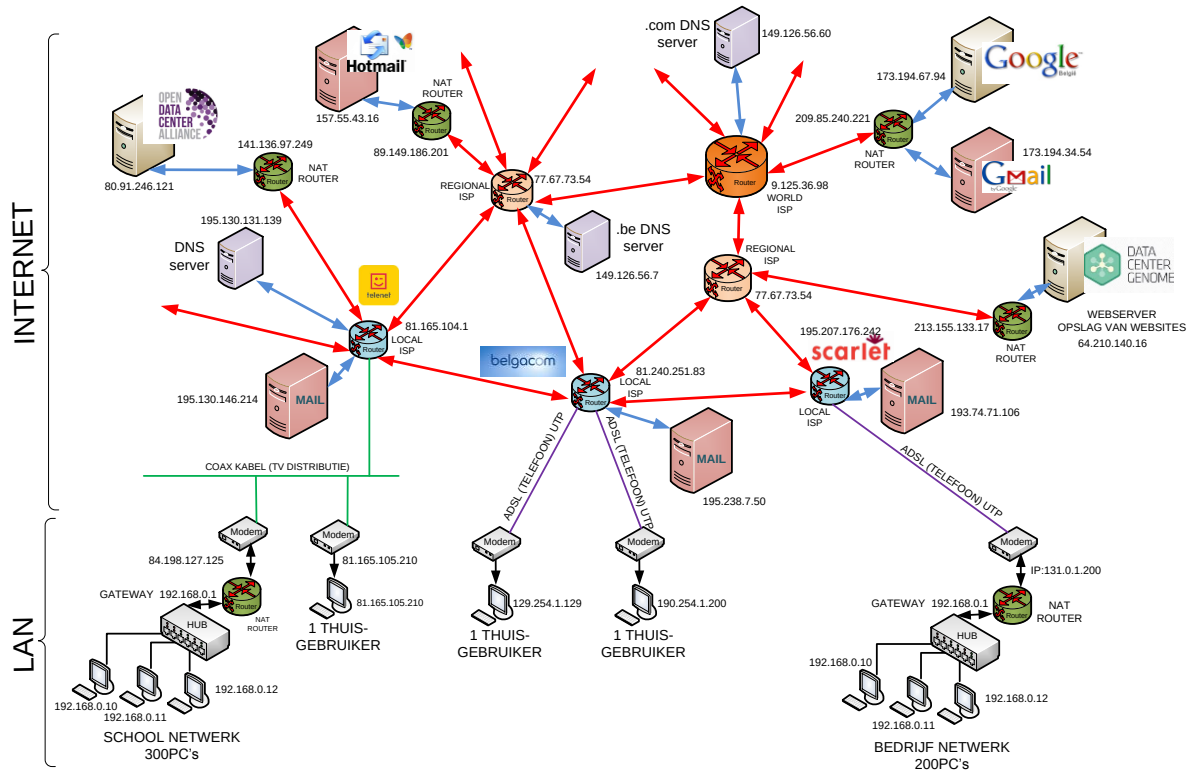



## MY IP

Om te weten te komen welk IP adres (statisch of dynamisch) je router momenteel van je ISP heeft gekregen kan je de website http://whatismyipaddress.com/ gebruiken.

## DNS

DNS: DOMAIN NAME SYSTEM




Alle info op ‘HET INTERNET’ staat ergens op één van de vele WEBSERVERS. Deze servers zijn enkel te bereiken indien je over het juiste IP adres van deze server beschikt. Het onthouden van alle IP ADRESSEN van al uw favoriete websites is onmogelijk.

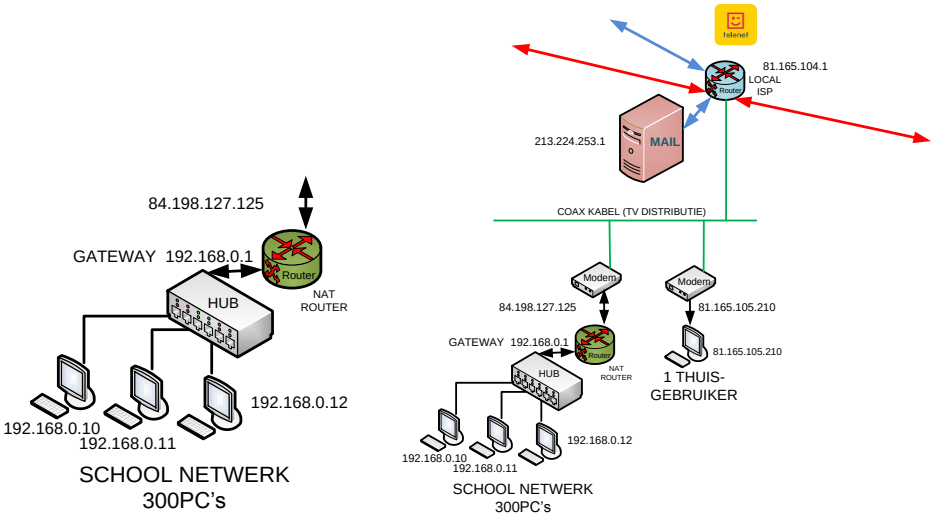
Daarom werken wij op het internet met ‘DOMAIN NAMES’ – bijvoorbeeld: “nl.wikipedia.org” . Deze website heeft als IP adres 91.198.174.232, maar onze computer kan dit onmogelijk zelf weten.

Onze computer krijgt – naast een IP adres, STANDAARD GATEWAY en SUBNET MASK ook één of meerdere DNS SERVER IP ADRESSEN mee. Indien de nl.wikipedia.org website wordt opgevraagd, dan maakt onze PC meteen contact met de DNS SERVER om te vragen welk IP ADRES bij deze website hoort. Dikwijls weet deze DNS SERVER dit IP ADRES meteen en indien niet dan geeft de DNS SERVER het IP adres van een andere DNS SERVER die het wel kan weten. Zo heb je DNS SERVERS die specialist zijn in .be of in .com domeinnamen.

DNS SERVERS zijn specialisten in het doorzoeken van ‘HET INTERNET’ . Ze slagen zo in grote tabellen op welk IP ADRES hoort bij welke domain name. Op vraag van de klant geven ze dan het IP adres dat bij de gevraagde DOMEIN NAAM hoort zodat de klant met dit IP ADRES de juiste website kan opvragen.

## DHCP

DHCP: Dynamic Host Configuration Protocol




Elke PC in een netwerk moet een IP ADRES hebben. Je kan Pc's instellen zodat ze een vast IP ADRES hebben, maar meestal stellen we de PC in op 'DHCP' en geven we zo die verantwoordelijkheid aan de router. NAT ROUTERS zullen zo aan elke PC die zich bij in het LAN netwerk zet automatisch een IP adres geven binnen de range van het netwerk. De PC krijgt dan van de ROUTER alle info over IP ADRES, SUBNET MASK, DNS SERVERS en STANDAARD GATEWAY.

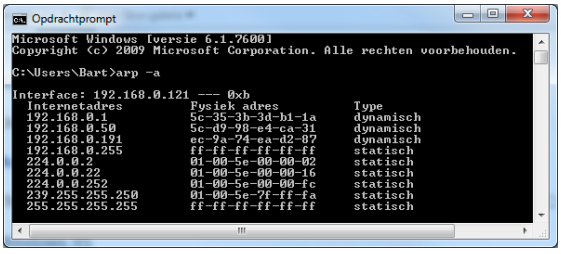
Ook ISP routers geven via DHCP dynamische of statische IP ADRESSEN aan NAT ROUTERS of rechtstreeks aan klanten die slechts 1 PC hebben.

STATISCHE IP ADRESSEN blijven altijd dezelfde. Grote bedrijven en scholen krijgen meestal STATISCHE IP ADRESSEN.

DYNAMISCHE IP ADRESSEN kunnen veranderen. Deze worden meestal uitgedeeld aan particuliere gebruikers.

## ARP

ARP staat voor ADRES RESOLUTION PROTOCOL. Zeker voor communicatie in LAN's kan de communicatie veel sneller verlopen als elke PC binnen deze LAN weet welk MAC ADRES bij welk IP ADRES hoort. Pc's komen dit van elkaar te weten via "ARP REQUESTS". Je kan in de COMMAND PROMPT met de "**arp –a**" instructie op elk moment de ARP tabel van uw PC opvragen. Deze ARP tabel is vluchtig vermits Pc's via DHCP slechts een IP adres krijgen toegewezen voor een bepaalde periode. ARP tabellen groeien naarmate er meer netwerkverkeer is en krimpen terug wanneer er een tijdje geen verkeer is.



## UITDAGINGEN LAYER 3

- Leg in eigen woorden uit wat het verschil is tussen WAN en LAN.
- Een IP adres dient wereldwijd uniek te zijn voor elke internetaansluiting, maar niet voor elke computer. Leg uit.
- Waarvoor staat ISP
- Zoek van volgende situaties uit of de destination IP adressen voor het LAN of voor het WAN bestemd zijn:

| | Decimaal | IP in Binair |
|---|---|---|
| Host IP adres | 192.168.0.45 | |
| Subnet mask | 255.255.255.0 | |
| Destination IP adres | 192.168.0.165 | |

| | Decimaal | IP in Binair |
|---|---|---|
| Host IP adres | 192.168.0.45 | |
| Subnet mask | 255.255.255.0 | |
| Destination IP adres | 192.168.1.15 | |

| | Decimaal | IP in Binair |
|---|---|---|
| Host IP adres | 192.168.0.45 | |
| Subnet mask | 255.255.254.0 | |
| Destination IP adres | 192.168.1.15 | |

| | Decimaal | IP in Binair |
|---|---|---|
| Host IP adres | 192.168.0.45 | |
| Subnet mask | 255.255.254.0 | |
| Destination IP adres | 192.168.1.250 | |

- Als het subnet masker aangeeft dat een bericht met en bepaalde destination IP niet bestemd is voor de LAN, naar welk IP adres zal dit bericht dan eerst gestuurd worden?
- Een IP adres 150.218.12.13 – is dit een Klasse A, B of C adres?
- Een IP adres 112.0.12.13 – is dit een Klasse A, B of C adres?
- Een IP adres 200.0.12.13 – is dit een Klasse A, B of C adres?
- Teken blokschematisch het volledige IP datagram in een Ethernet frame en benoem en geef kort de functie van alle blokken van de IP header.
- Als je een IP header gebruikt, wordt er dan nog steeds met MAC adressen gewerkt? Verklaar.
- Met IPV4 konden we slechts 4 miljard unieke IP adressen toewijzen. Het aantal PC's dat een uniek adres nodig had steeg te snel. Wat was de oplossing die ze snel hebben ingevoerd en welke is de meer permanente oplossing die de komende jaren zal worden ingevoerd.
- Ping eens naar 173.194.67.94 – hoeveel tijd ging er gemiddeld overheen voordat je deze server bereikt had.
- Gebruik ipconfig om je eigen IP adres, subnet mask en gateway te weten te komen
- Gebruik ipconfig/all en kijk of je meer zinvolle info krijgt.
- Gebruik de MYIP website om te weten te komen welk IP adres je router van je ISP gekregen heeft.
- Wat is het nut van DNS en hoe werkt DNS – maak een verduidelijkende tekening.
- Waarvoor staat DHCP en waarvoor dient DHCP.
- Wat is het verschil tussen statische en dynamische IP adressen
- Gebruik op een juist opgestarte PC het arp –a commando en neem een screenshot. Zorg dat er nu wat netwerkverkeer is, surf wat op het net, deel bestanden met de andere PC's in het netwerk of maak gebruik van de netwerkprinter en voor nu terug het arp –a commando uit. Vergelijk deze ARP tabel met de vorige.

## LAYER 4: TRANSPORT LAYER

Omdat er in IP geen controle is ingebouwd die een goede aflevering van het bericht garandeert is er nog een zekere mate van eindcontrole nodig. Deze eindcontrole wordt geregeld in LAYER 4 – de TRANSPORT LAYER. Er zijn 2 protocollen die kunnen worden toegepast in de TRANSPORTLAAG van het internet:

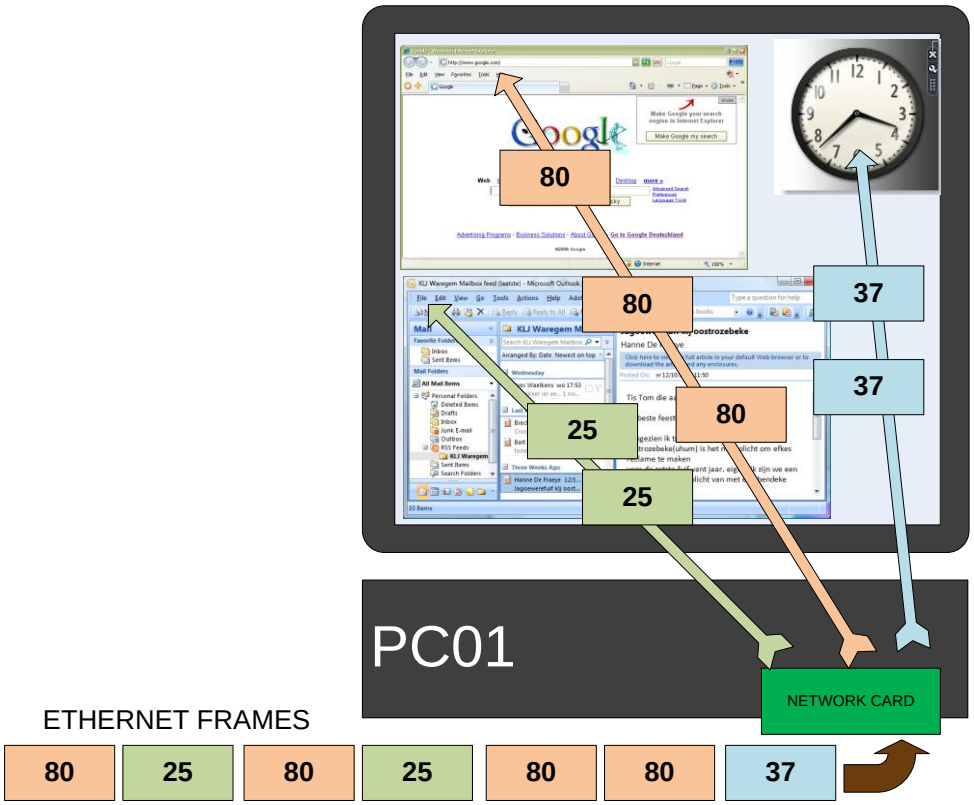
UDP : geen eindcontrole

TCP: wel eindcontrole

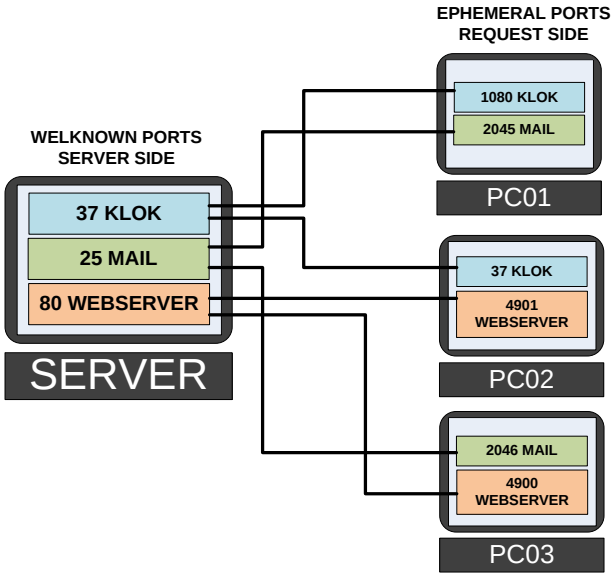
Daarnaast regelt LAYER 4 ook via POORTNUMMERS aan welke applicatie op uw PC de opgevraagde data moet worden afgeleverd. U kan immers simultaan E-mails ontvangen via outlook en internet pagina's opvragen via Internet Explorer.

### POORTNUMMERS

Op 1 node (PC, tablet, Smartphone, …) zijn er verschillende parallelle applicaties mogelijk die allemaal gebruik maken van dezelfde netwerkverbinding. Door gebruik te maken van POORTNUMMERS, die mee in het ethernetbericht worden ingewerkt, weet de node voor welke applicatie dit specifieke bericht bedoeld is. Naast INTERNET EXPLORER of OUTLOOK EXPRESS draaien er nog heel wat applicaties op de achtergrond waarvan gebruikers amper het bestaan weten (denk aan de applicatie die uw PC klok juist zet, denk aan uw virusscanner die een update vraagt, …) Ook al deze applicaties zijn gelinkt aan een specifiek POORTNUMMER.




- POORTNUMMERS zijn 16 bit getallen en kunnen dus variëren tussen 0 en 65535
- Elke applicatie 'bindt' zich aan één van deze poortnummers
- Ethernet pakketten worden zo via hun POORTNUMMER naar de juiste applicatie gestuurd




- "WELLKNOWN POORTEN" zijn poorten die gereserveerd zijn voor één bepaalde applicatie langs de zijde van de server.
  - Poort 23 TELNET
  - Poort 21-22 FTP
  - Poort 25 SMTP (Simple mail transfer protocol)
  - Poort 37 Time (om klok te synchroniseren)
  - Poort 53 DNS berichten
  - Poort 80 HTTP (Internet explorer-Mozilla-…) webbrowsers
  - Poort 110 Post office (POP3) om mails te verzenden / ontvangen
  - Poort 546 DHCP client
  - Poort 547 DHCP server
  - Poort 569 MSN
  - Poort 443 Facebook
- "EPHEMERAL" of kort levende poorten zijn poortnummers die de applicatie aan de zijde van de aanvrager van de server krijgt toegewezen voor de duur van de communicatie.
  - Windows 1024-5000
  - Andere 32768-65535
- Vrije poorten… om zelf applicaties voor te maken…
  - Windows 5001-65535
  - Andere 1024-32767
  - Samen 5001-32767

## UDP: USER DATAGRAM PROTOCOL

UDP of USER DATAGRAM PROTOCOL is een laag die bovenop IP komt, maar geen bevestiging regelt of een bericht correct de eindbestemming bereikt heeft. Het regelt wel de functie van MULTIPLEXING en DEMULTIPLEXING op basis van de POORTNUMMERS zoals hierboven beschreven. Vermits UDP geen bevestiging regelt vormt UDP minder 'OVERHEAD' en kan UDP sneller werken als TCP.

Enkele typische applicaties die UDP gebruiken zijn:

**Streaming audio en video:** Snelheid is hier belangrijk en vermits we real time werken heeft het opnieuw verzenden van eventueel foutief aangekomen pakketten geen enkel nut.

**Online gaming:** Ook hier is het real time aspect veel belangrijker dan de controle of data wel correct is aangekomen.

**DNS requests:** Tijdens de DNS REQUEST, om een IP adres te zoeken dat bij een bepaalde domeinnaam hoort, kan de huidige applicatie (INTERNET EXPLORER) even niets anders doen. Om dit sneller te laten verlopen wordt er hier UDP toegepast.

## TCP TRANSMISSION CONTROL PROTOCOL

TCP of TRANSMISSION CONTROL PROTOCOL is een system dat in tegenstelling tot UDP wel een bevestiging regelt zodat de afzender weet dat het verzonden bericht goed is aangekomen. Daarnaast neemt TCP ook nog een aantal andere taken op zich.

**Datastroom:** Applicaties maken gebruik van TCP om data via het netwerk naar andere computers te versturen. Vanuit de applicaties gezien verzendt TCP een continue stroom bytes. Dit betekent dat de applicatie niet verplicht is om de data in blokken te verdelen en zo te verzenden. Het is de taak van TCP om de data te groeperen in blokken. Men noemt deze blokken TCP segmenten. TCP geeft deze blokken ter verzending door aan IP. Het is TCP die beslist hoe en wanneer de data in segmenten wordt verdeeld en doorgegeven wordt aan de IP laag.

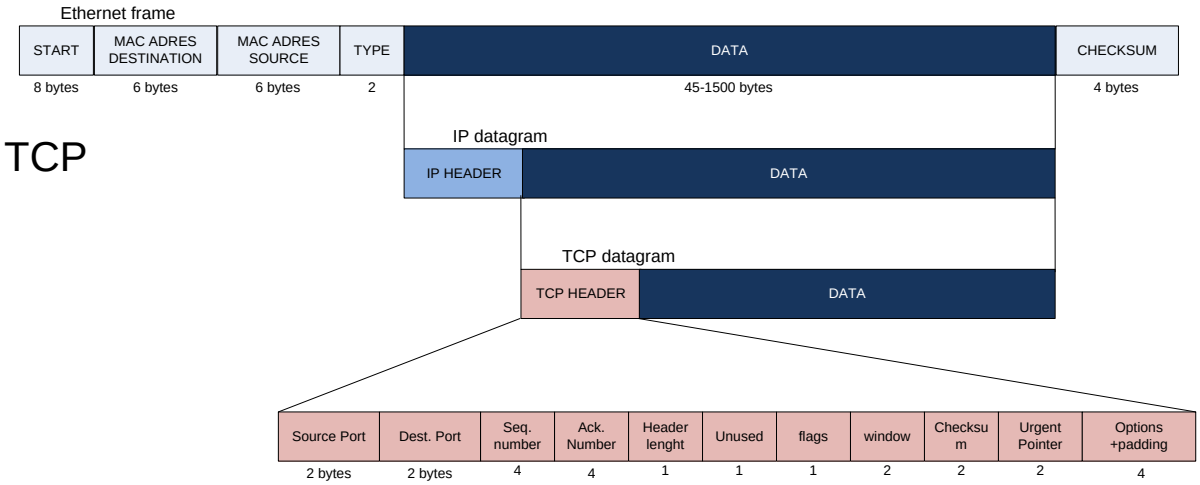
**Windowing:** De verdeling in blokken, verzending en ACK van de TCP laag gebeurt volgens een principe van windowing waarbij de volgende pakketten reeds kunnen verzonden worden voordat de ACK van de vorige pakketten is aangekomen. Naarmate de ACK berichten vlotter binnen komen betekent dit dat de lijn de huidige datastroom vlot aan kan en wordt de WINDOW van berichten die mogen verzonden worden zonder ACK bevestiging vergroot om zo de datastroom te vergroten. Als er om één of andere reden een bericht niet correct aankomt wordt de WINDOW grootte terug op 1 gezet en begint de regeling terug opnieuw.

**Betrouwbaar:** Zoals reeds eerder vermeld is TCP in staat om op een betrouwbare wijze de data bij de bestemmeling af te leveren. Het is de verantwoordelijkheid van TCP om na te gaan of er tijdens de verzending geen data is verloren gegaan. Deze controle is mogelijk door zogenaamde ACK meldingen te gebruiken. De ontvanger moet deze ACK meldingen terug sturen naar de afzender. Hiermee weet de afzender dat de data goed is aangekomen. Indien er binnen een zekere tijd geen ACK melding bij de afzender aankomt, dan gaat de afzender de data opnieuw versturen. Dit wordt allemaal geregeld binnen de TCP laag, maar dat 'kost' vanzelfsprekend wel wat bandbreedte.

**Flow control:** Wanneer de ontvanger de ACK melding terugstuurt naar de afzender, zit er in deze melding ook nog een getal dat bepaalt hoeveel data de afzender nog mag versturen. Door dit mechanisme wordt er vermeden dat de afzender meer data verstuurt dan dat de ontvanger kan ontvangen.

**Multiplexing**: Hiervoor worden de POORTNUMMERS gebruikt.

## ETHERNET FRAME TRANSPORT LAYER




Om de TCP header informatie mee in het Ethernet bericht in te werken wordt dezelfde methode gebruikt als bij het IP frame. De TCP header vervangt gewoon het eerste stukje van de data van het IP frame. We bespreken kort de belangrijkste blokken.

**Source port:** Het 16 bit poortnummer van de afzender.

**Destination port:** Het 16 bit poortnummer van de bestemmeling.

**Sequentie nummer:** is een 32 bit getal dat bij het opzetten van een nieuwe sessie willekeurig gegenereerd wordt aan de kant van de client. Dit getal wordt samen met het eerste bericht verstuurd. Bij elk volgend bericht wordt dit nummer met één verhoogd om aan te geven dat dit het volgende bericht is van de zelfde sessie.

**Ack nummer:** De Server bevestigt de goede ontvangst van het bericht van de Client door het sequentienummer met één te verhogen en dit nummer als het 32 bit acknowledge getal mee te sturen met een nieuw bericht van Server naar Client.

**Data offset** : Het aantal 32 bit woorden in de header. Hiermee wordt bepaald waar de data in het pakket terug te vinden is.

**Flags:**

| | |
|---|---|
| URG | Deze vlag geeft aan dat het Urgent Pointer veld in dit pakket ingevuld is. |
| ACK | Deze vlag geeft aan dat de ontvanger een bevestiging doet. |
| PSH | Push functie. |
| RST | Met deze vlag wordt de connectie gereset. |
| SYN | Met deze vlag worden de sequentienummers gesynchroniseerd. |
| FIN | Deze vlag geeft aan dat er geen data meer te verwachten is van de afzender. |

**Venster:** Dit 16 bit getal geeft de grootte van het venster aan. Dit veld is alleen maar geldig als de ACK bit gezet is.

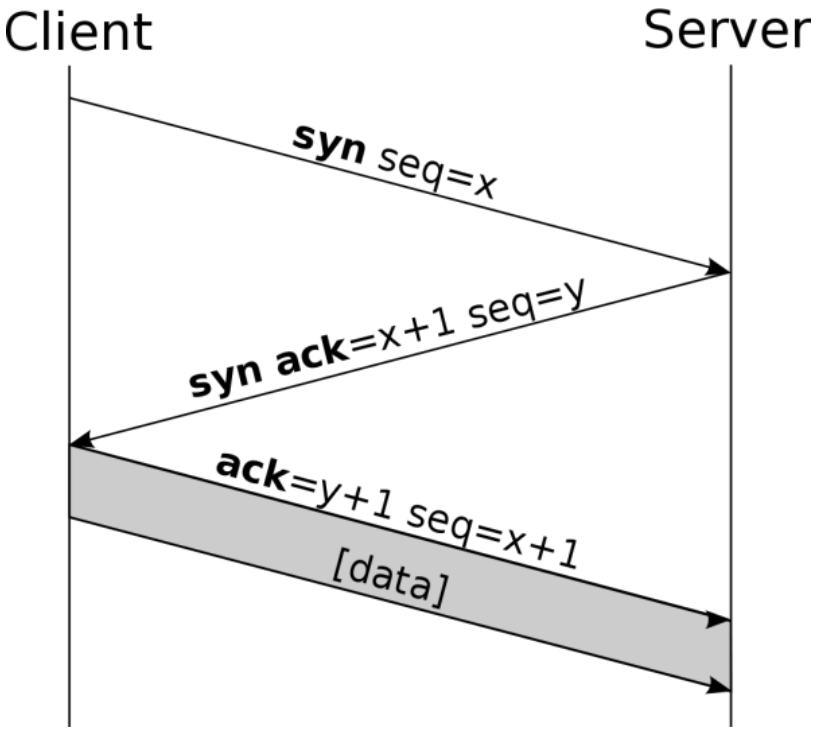
**Checksum:** Deze CHECKSUM maakt een controle op juistheid van de header mogelijk.

**Urgent Pointer:** Deze pointer wijst naar de eerste data met hoge prioriteit. Dit veld is alleen maar geldig als de URG bit gezet is.

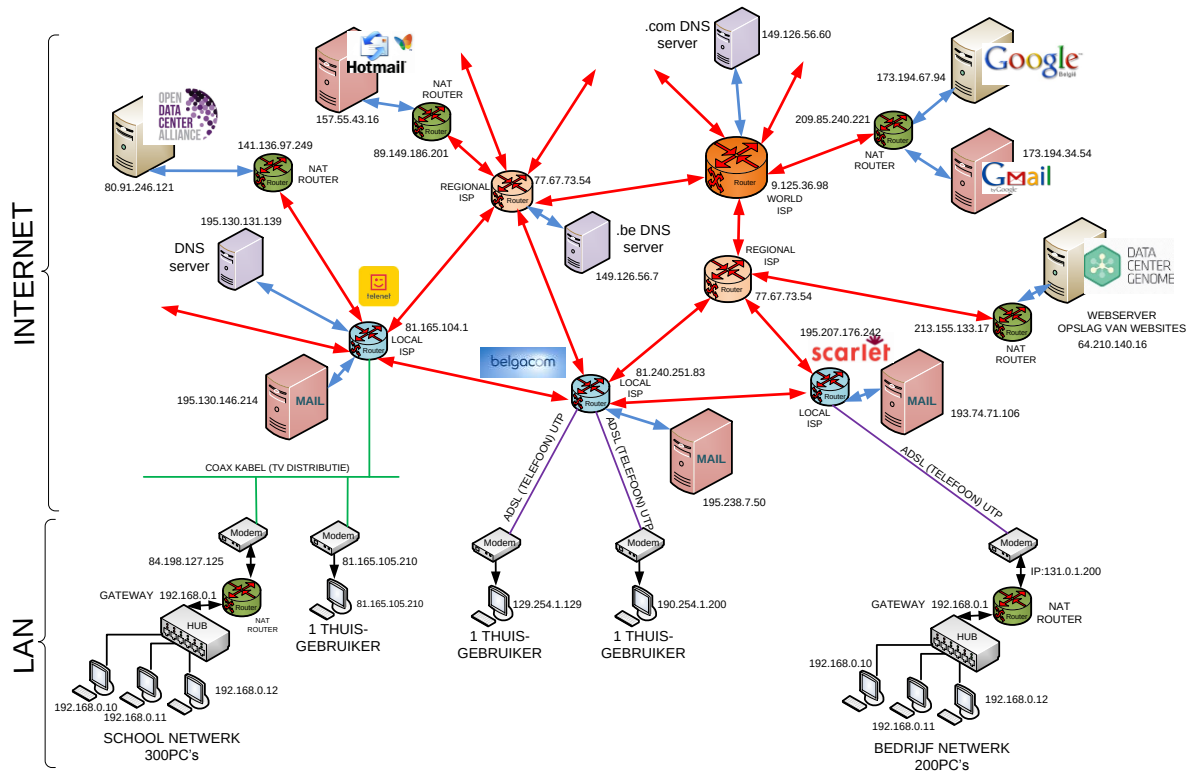
**Opties:** Er kunnen opties in de TCP header voorkomen

## WERKING SEQ EN ACK

Om een TCP-verbinding op te bouwen stuurt de CLIENT een TCP-PAKKET naar de SERVER met als SEQ NUMMER x. Als de SERVER de verbinding accepteert, wordt een pakket teruggestuurd. De ACK NUMMER wordt x+1 en de SEQUENTIENUMMER wordt y. Als de CLIENT vervolgens de SERVER accepteert, stuurt deze een pakketje terug naar de SERVER. Hierbij wordt het ACK NUMMER gelijk aan Y+1 en de SEQ NUMMER gelijk aan x + 1. Door het steeds overnemen en verhogen van de ACK en SEQ NUMMERS weten zowel de SERVER als de CLIENT dat de vorige berichten goed waren aangekomen. Hierna kunnen pakketjes met de juiste identificatienummers vrij uitgewisseld worden tussen CLIENT en SERVER. Iedere keer wordt de CHECKSUM van zo'n pakketje gecontroleerd en het pakketje wordt opnieuw opgevraagd indien er een fout in zit. Als er een heel pakket verdwijnt, is dit te merken aan het ACK-NUMMER. Zodra de verbinding gesloten wordt, stuurt de SERVER of CLIENT een pakket met de FIN-vlag, waarna de andere kant antwoordt met een ACK-vlag en dit vervolgens in de omgekeerde richting gebeurt, zodat beide partijen op de hoogte zijn dat de connectie werd opgeheven. Dit wordt allemaal geregeld door TCP in LAYER 4.



## NAT ROUTER NETWORK ADDRESS TRANSLATION ROUTER



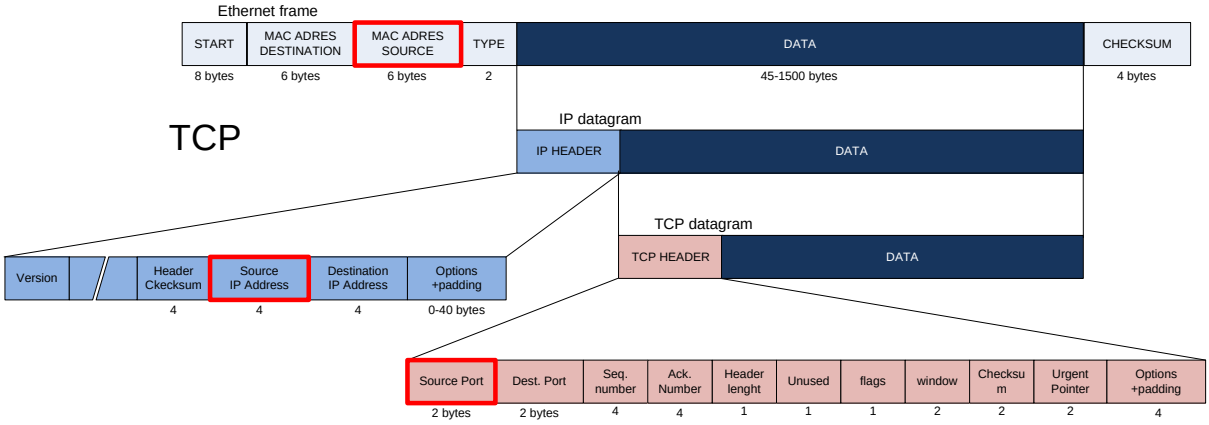

Zoals eerder (onder LAYER 3 – NETWORK LAYER) vermeld zijn NAT routers speciaal ontworpen om lokale netwerken te scheiden van het internet. De voornaamste reden hiervan was dat het aantal beschikbare IP adressen in IPV4 zeer snel verminderde en dat de ontwikkeling en invoering van IPV6 te lang op zich zou laten wachten.

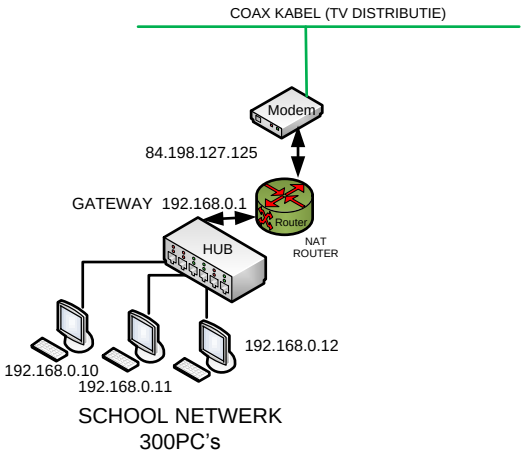
NAT of NETWORK ADRES TRANSLATION ROUTERS 'vertalen' al de IP ADRESSSEN die binnen de LAN voorkomen naar één enkel uniek IP adres om hiermee op het internet te kunnen. Vanuit het INTERNET gezien staat er in dit netwerk slechts 1 PC terwijl dit er vele honderden kunnen zijn. Dit heeft een aantal consequenties:

- Alle Pc's die in LAN netwerken voorkomen moeten geen wereldwijd uniek IP ADRES meer krijgen. Enkel de NAT ROUTER moet nog één uniek IP ADRES krijgen. IP ADRESSEN binnen één LAN kunnen zo zonder probleem identiek zijn aan IP ADRESSEN binnen een ander LAN. Het probleem met de beperking van het aantal beschikbare IPV4 adressen was hiermee even opgelost.
- De info die Pc's binnen het LAN netwerk opvragen, is in hoge mate anoniem. Men kan traceren wat het IP ADRES is van de NAT router, maar men kan niet bewijzen welke PC binnen dit netwerk de info heeft opgevraagd. Dit kan zowel een voordeel als een nadeel zijn.

## WERKING NAT ROUTER

Andere routers werken op IP basis en dus in de NETWORK LAYER (LAYER 3) , maar NAT ROUTERS werken in LAYER 4, DE TRANSPORT LAYER.




Ethernet bericht verzenden

1. PC02 met IP: 192.168.0.11 en SUBNET 255.255.255.0, met MAC 123.123.123.123.123.123 verstuurt een vraag naar een webserver op poort 80 met IP 10.0.1.5 die ergens op het internet staat.
2. Het SUBNETMASKER geeft aan dat PC met IP 10.0.1.5 niet in dit LAN staat en geeft dit bericht door aan de standaard gateway van de router (192.168.0.1).
3. De NAT router past in dit bericht volgende zaken aan, herrekent de CHECKSUM en stuurt het bericht door naar de router van de ISP:
    a. Source IP adres wordt veranderd van 192.168.0.10 naar 84.198.127.125
    b. MAC adres SOURCE wordt veranderd van 123.123.123.123.123.123 naar het MAC adres van de NAT ROUTER (het MAC adres verandert trouwens bij elke nieuwe routering in het MAC adres van de laatste router die het passeerde)
    c. De SOURCE PORT wordt door de NAT router aangepast naar een PORT nummer binnen de vrije range (5001-32767). De NAT router onthoudt dit nummer en slaat dit samen op in een tabel met het MAC, IP en PORT ADRES van het originele bericht dat van PC02 kwam. Dit is de methode die bij NAT routers wordt toegepast om berichten die van het internet naar de LAN komen terug te kunnen verdelen naar de juiste IP adressen binnen deze LAN.

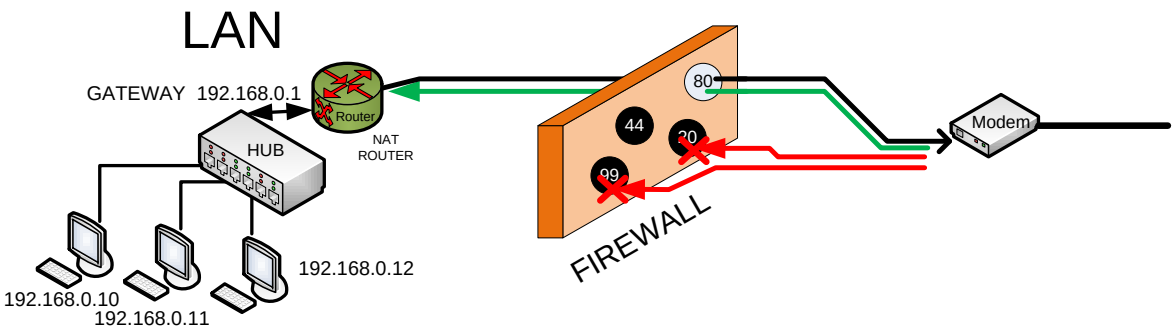
Ethernet bericht ontvangen:

- Het ethernetbericht dat als antwoord op onze eerdere vraag van het internet naar het IP adres van de router gestuurd (84.198.127.125) wordt – wordt door de router geanalyseerd:
    a. De DESTINATION PORT NUMMER in dit ontvangen bericht geeft de NAT router voldoende info om in z'n eigen tabellen op te zoeken welke PC (IP 192.168.0.10, MAC 123.123.123.123.123.123 en port nummer) dit bericht had opgevraagd.
    b. De NAT router past het DESTINATION IP adres, MAC adres en port nummer aan en herrekent de CHECKSUM.

Vermits NAT routers de port adressen manipuleren zijn dit LAYER 4 DEVICES. NAT routers moeten dus kunnen onthouden welke IP,MAC en PORT adressen bij welke veranderde PORT adressen hoorden en moeten genoeg rekenkracht hebben om snel de CHECKSUM te herrekenen.

## FIREWALL

Een firewall moet ongewenste berichten buiten houden. Firewalls zijn dikwijls ingebouwd in routers en werken eveneens op de PORT NUMBERS van LAYER 4.




Door een aanvraag te doen van binnenuit de LAN op POORT 80 bijvoorbeeld, zetten we POORT 80 van de ROUTER even open om ook een antwoord op onze vraag te kunnen ontvangen. Een antwoord op POORT 80 zal pas worden doorgelaten als er eerst een vraag is geweest. Een antwoord zonder eerst een vraag wordt weggegooid.

Een firewall zet alle poorten standaard dicht, enkel van binnen uit de LAN kunnen POORTEN kort worden open gezet, en dan enkel nog maar als reactie op een vraag van binnen dit LAN.

Een TROJAN HORSE is een stukje ongewenste software dat je via mail, mallware of virus binnen krijgt en dat van binnen uw LAN ongewild poorten open gaat zetten zodat kwaadwillige gebruikers van buiten uw LAN via die poort toegang kunnen krijgen tot uw LAN. Virusscanners scannen uw PC o.a. op deze TROJAN HORSES.

Om bijvoorbeeld van buiten uw LAN via Internet toestellen bij u thuis in of uit te kunnen schakelen moet er op uw FIREWALL een POORT worden open gezet. Je moet vanaf dan wel zelf zeer goed controleren of de berichten op deze open poort wel van legitieme gebruikers komen.

## LAYER 5: SESION LAYER

De SESION LAYER legt vast op welke manier een gebruiker een sessie kan starten met een computer van een ander netwerk.

In heel het internet protocol is het enige dat deels aan LAYER 5 zou kunnen worden toegewezen het DNS of DOMIAN NAME SERVICE SYSTEM. Om een bepaalde sessie op te zetten met een website zal de aanvrager via aan een DNS REQUEST vragen wat het IP ADRES is dat bij een bepaalde DOMEINNAAM hoort. De DNS server zal dit IP ADRES doorgeven indien deze DNS server dit weet, of zal het IP ADRES doorgeven van een andere DNS SERVER waarbij je meer kans hebt dat hij het IP ADRES weet.

## LAYER 6: PRESENTATION LAYER

In de PRESENTATION LAYER worden normaal de afspraken vastgelegd op welke wijze gegevens in de berichten worden gecodeerd. Hoe wordt een mail of hoe wordt een tekening bijvoorbeeld doorgestuurd. In het hele INTERNET PROTOCOL is deze laag gewoonlijk in de applicatie zelf voorzien en zijn de APPLICATION en PRESENTATION LAYER eigenlijk één laag geworden.

## LAYER 7: APPLICATION LAYER

De APPLICATION LAYER omvat alle applicaties die op een bepaald system draaien en gebruik maken van het netwerk.

Internet Explorer, Outlook Express, Outlook, Facebook, Mozilla, Internet-Klok, Virusscanner-Updates, …

## LAYER 8: USER LAYER

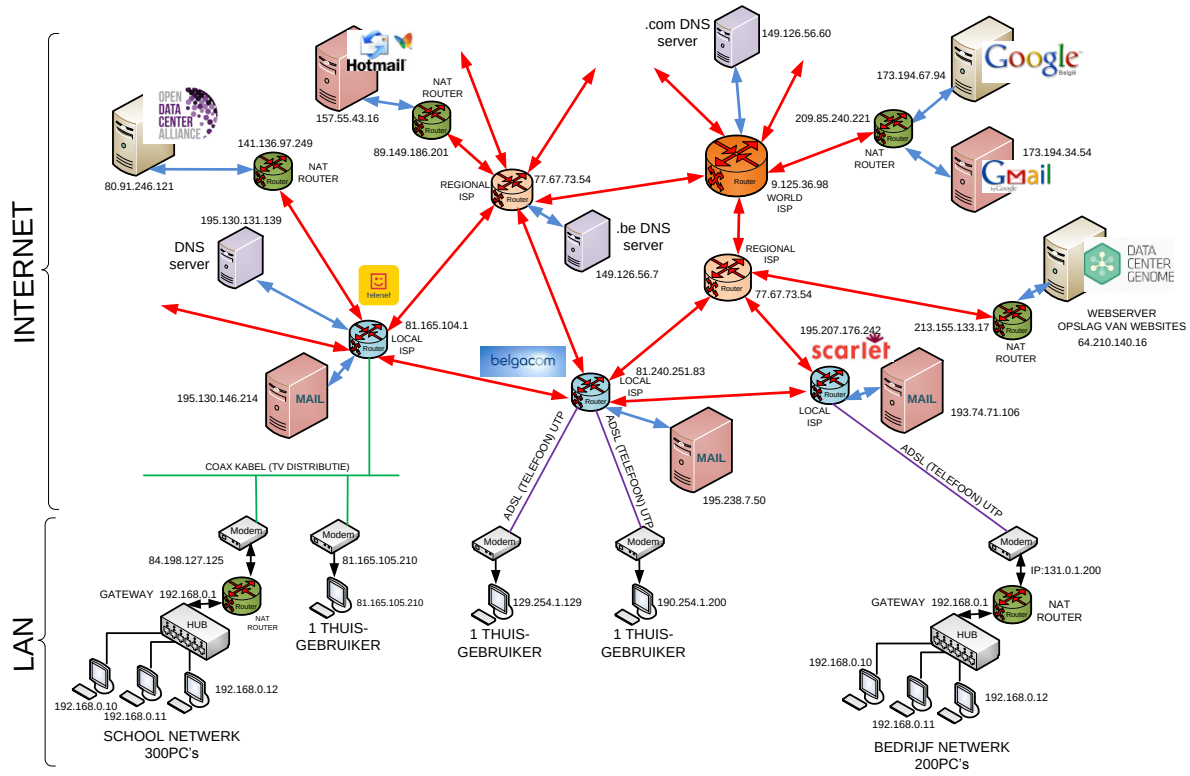
Bij HELPDESKS wordt er soms al eens gesproken over een LAYER 8 probleem. In dat geval bedoelen ze dat de gebruiker zelf een probleem heeft veroorzaakt door onkunde…

## UITDAGINGEN LAYER 4-8

- Leg in je eigen woorden het verschil uit tussen UDP en TCP
- Wat is het nut of doel van het gebruik van poortnummers? Verduidelijk met een tekening.
- Noem twee typische LAYER 4 hardware apparaten.
- Wat is het verschil tussen Wellknown en Ephemeral poortnummers.
- Waarom wordt er bij streaming audio gekozen voor UDP ipv TCP?
- Bespreek kort de 5 taken die TCP voor zich neemt.
- Teken het TCP datagram en verklaar elk blokje kort.
- Hoe groot zijn sequentie en acknowledge nummers in het TCP datagram?
- Hoe worden sequentie en acknowledge nummers gebruikt om tussen een server en een client in twee richtingen aan te geven dat de data goed ontvangen is. Geef dit ook schematisch weer.
- Hoe werkt een NAT router – en meer specifiek – hoe weet de NAT router van een inkomend TCP-IP bericht voor welke van de PC's dit bericht in het LAN netwerk bedoeld was. Leg dit stap voor stap en met een praktisch voorbeeld uit.
- Op welk principe werkt een firewall?
- Waarom spreken we bij internet toepassingen zelden over de presentation layer.
- Wat is het enige binnen het Internet protocol dat we voor een deel aan de session layer zouden kunnen toewijzen.
- Noem 5 applicaties (application layer) die gebruik maken van het netwerk.

## HOE WERKT HET INTERNET

In deze les proberen we via enkele voorbeelden aan te geven hoe het internet werkt. We maken daarom regelmatig gebruik van dit schema.

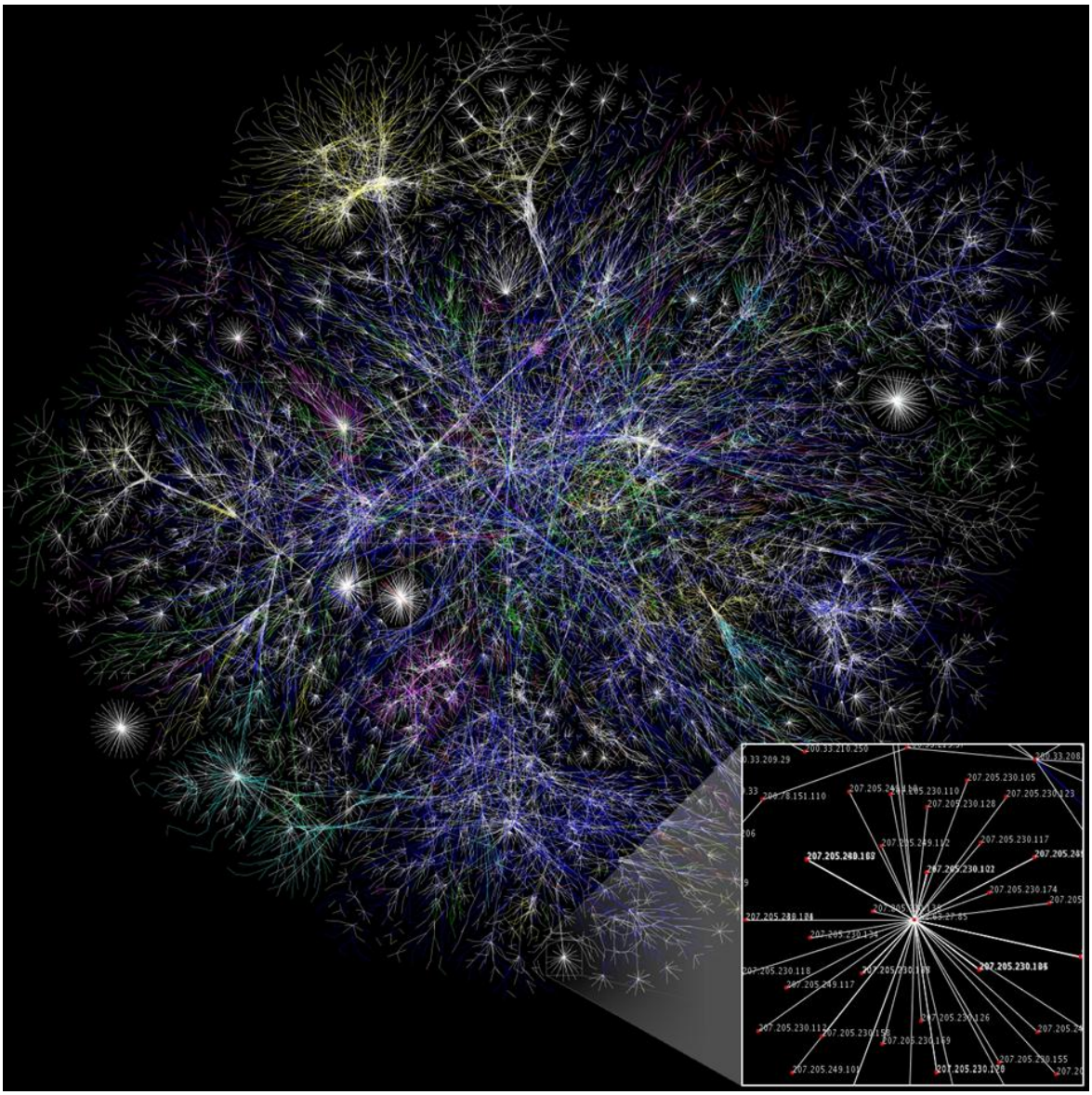



## OPBOUW INTERNET - ROUTERS

'HET INTERNET' is in de loop van de jaren gegroeid maar bestaat in feite uit niets meer dan ROUTERS. Een ROUTER zorgt er voor dat ethernet berichten in de juiste richting worden doorgestuurd. ROUTERS zijn LAYER 3 DEVICES, ze analyseren het DESTINATION IP ADRES in het ETHERNET FRAME en sturen het bericht door in de volgens de ROUTER beste richting.

U ziet in de tekening dat het internet een MAAS-STRUCTUUR heeft. Een ETHERNET PAKKET kan soms via 100-en verschillende wegen zijn bestemming bereiken. De ROUTERS beslissen welke route een pakket volgt. Zo kunnen twee opeenvolgende pakketten van dezelfde afzender naar dezelfde ontvanger toch twee totaal verschillende routes volgen. Op die manier is 'HET INTERNET' nooit volledig plat te krijgen. Als er een bepaald segment uitvalt, dan nemen de andere segmenten het over.

Dit is een ‘foto’ van ‘het internet’ anno 2010. Als we heel sterk inzoomen op één punt dan beginnen we de IP adressen te herkennen. Hierop zijn enkel de internetconnecties te zien en niet de PC’s achter de NAT routers.

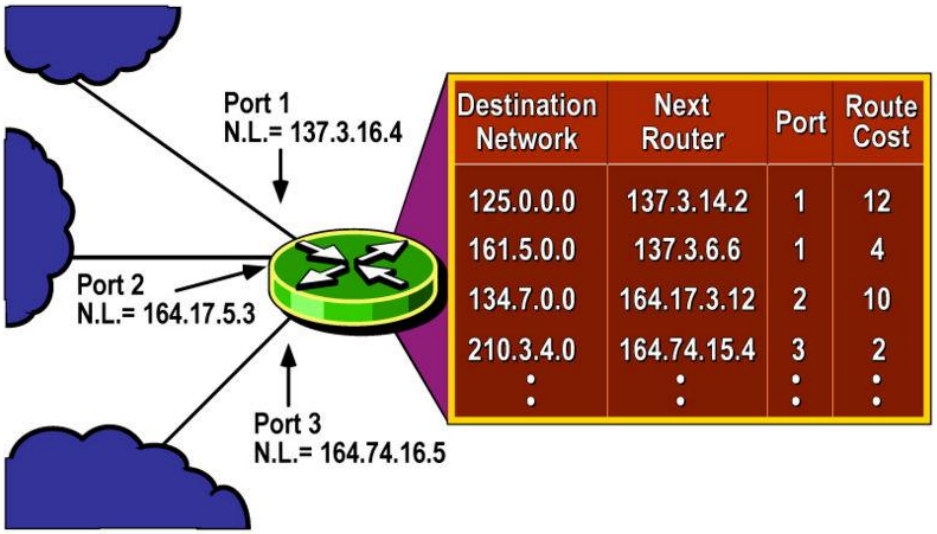



Routers zijn vrij intelligente computers die beheerd worden door ISP’s (Internet service providers) zoals wij Telenet en Belgacom kennen. Alle klanten van Telenet betalen in hun abonnement mee voor het beheer van de Telenet routers. Telenet en Belgacom zijn op hun beurt klant van (dikwijls gelijktijdig meerdere) regionale ISP’s en betalen daarvoor aan die regionale ISP’s een bijdrage afhankelijk van het dataverkeer dat ze in die richting sturen. De regionale ISP’s zijn dan weer klant bij World ISP’s die op wereldschaal het internet verdelen via routers die in hun beheer zijn. Klanten van WORLD ISP’s betalen ook per hoeveelheid data. Zo’n WORLD ROUTERS – zoals u hier op de afbeelding ziet - hebben veel weg van supercomputers.

Hoe kunnen routers weten wat de beste weg is voor een ethernet pakket met een bepaald IP adres? Het antwoord op deze vraag is dat al deze routers intelligente computers zijn die constant 'het internet' onderzoeken.

- Ze sturen zelf berichten rond om te controleren welke IP adressen waar voorkomen.
- Ze testen lijnen op snelheid en houden die bij in tabellen.
- Ze controleren pakketten die langs komen en leren hiervan.
- Ze houden resultaten bij van pakketten die ze zelf, en die anderen hebben doorgestuurd – hoe lang die er over gedaan hebben, welke route die gevolgd hebben.
- Ze geven aan elkaar door welke routes momenteel goed werken en welke routes uitgevallen zijn.
- Als een bepaalde route wat te druk wordt, dan vernemen de routers dat en kiezen ze andere routes.
- Tussen ISP's van verschillende grootte worden er onderling vergoedingen gevraagd. Routers kunnen zo de route van de laagste vergoeding kiezen.

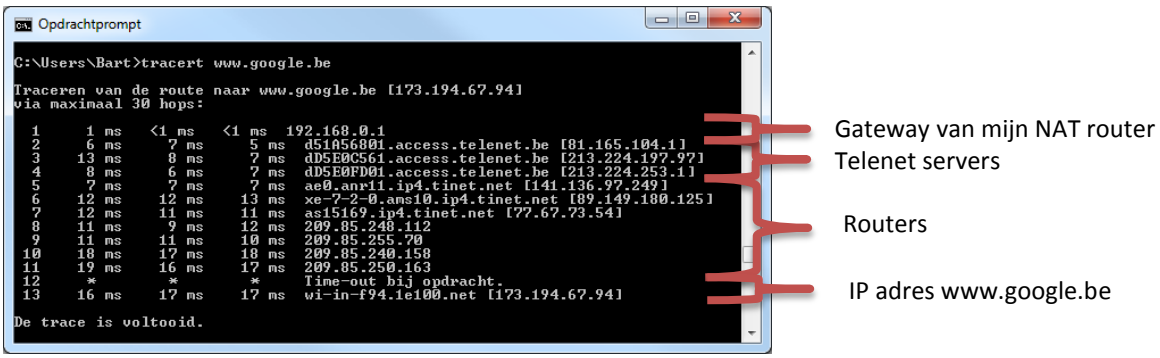
Al deze info wordt in de router bijgehouden in 'ROUTING TABLES'. Hoe krachtiger de router – hoe meer info deze kan bijhouden. Deze ROUTING TABLE is trouwens heel vluchtig en moet constant worden bijgewerkt. De toestand van het internet verandert immers constant. Echt werk voor supercomputers dus. De ROUTE COST is een soort puntensysteem waarmee een router bepaalde routes quoteert. De router zal deze gebruiken om de route van de laagste kost / hoogste snelheid te kiezen.



## TRACERT

Met de >tracert www.google.be kan je onderzoeken welke route je bericht volgt voordat het bij de google website aankomt. Je kan niet altijd zeker zijn wat er achter welk IP adres zit, maar we doen hier een poging:

ZO zie je hier als eerste het gateway adres van onze eigen router. Via enkele Telenet servers wordt het bericht dan op het internet gezet. Telenet omdat Telenet onze ISP is. Op het internet wordt ons bericht dan via enkele routers doorgegeven om zo uiteindelijk de server van google te vinden. Dit alles gebeurt op 17msec. Probeer zo maar eens eender welk domein uit. Het is verbazend hoe weinig routers er nodig zijn om op je bestemming te geraken.



## EEN MAIL STUREN

Mails worden beheerd door MAIL-SERVERS die aan het INTERNET hangen. Deze servers kunnen beheerd worden door ISP's zoals Telenet en Belgacom maar het kunnen ook losstaande servers zijn zoals dat bij G-mail en Hotmail het geval is.

CASE 1: een thuisgebruiker met e-mail adres goezot@telenet.be stuurt een mail naar nogzotter@hotmail.com

- De afzender gebruikt Outlook Express (APPLICATION LAYER) en is klant bij ISP Telenet.
- Outlook Express stuurt de e-mail door naar de Telenet MAILSERVER.
- De Telenet MAILSERVER stuurt het bericht via verschillende routers door naar de HOTMAIL mail server
- Daar wordt het bericht bewaard tot het wordt gelezen en verwijderd door de gebruiker.

CASE 2: een thuisgebruiker met e-mail adres goezot@telenet.be krijgt een mail van nogzotter@hotmail.com

- De ontvangen mail staat klaar op de MAILSERVER van Telenet.
- Wanneer de ontvanger Outlook Express opstart wordt de mail automatisch gedownload en in de meeste gevallen ook meteen verwijderd.

## EEN WEBSITE OPENEN

CASE 1: De website heeft een vast IP adres. De website is in dit geval de enige site op een server met een vast IP adres.

- Een gebruiker vraagt een website op met Internet Explorer: www.google.be
- Vermits de vragende PC het IP adres van www.google.be niet weet zal het een DNS REQUEST sturen aan de DNS SERVER van Telenet. Het IP ADRES van de DNS SERVER van Telenet is ingesteld op de Pc of is verkregen via DHCP.
- De DNS server meldt aan de PC dat het IP adres van www.google.be 173.194.67.94 is.
- De PC maakt een verbinding met 173.194.67.94 (de google.be server)
- De PC stuurt een GET http://www.google.be REQUEST naar de server (deze REQUEST wordt niet noodzakelijk gebruikt vermits de webpagina rechtstreeks achter het IP adres staat)
- www.google.be stuurt als antwoord de startpagina van www.google.be
- (typ i.p.v. www.google.be maar eens 173.194.67.94 in en test uit)

CASE 2: De website heeft geen vast IP adres. De website staat samen met vele andere websites op een server van een DATACENTER die wel een vast IP adres heeft.

- Een gebruiker vraagt een website op met Internet Explorer: www.sjs.be
- Vermits de vragende PC het IP adres van www.sjs.be niet weet zal het een DNS REQUEST sturen aan de DNS SERVER van Telenet. Het IP adres van de DNS SERVER van Telenet is ingesteld op de PC of is verkregen via DHCP.
- De DNS server meldt aan de PC dat het IP adres van de server die oa de website www.sjs.be bevat 83.169.3.164 is.
- De PC maakt een verbinding met 83.169.3.164 (de server die www.sjs.be bevat)
- De PC stuurt een GET http://www.sjs.be REQUEST naar de server om aan de server duidelijk te maken welke website we van deze server willen opvragen.
- www.sjs.be stuurt als antwoord de startpagina van www.sjs.be

- (zoek via de tracert functie het IP adres op van de server van de www.sjs.be site en surf nu rechtreeks naar dit IP adres.– je zal merken dat je nu connectie maakt met een server en niet met de sjs.be website)

## HOE WERKEN ZOEKMACHINES

Zoekmachines zoals Google en Yahoo zijn niet meer dan zalen vol computers. Dit is zo bijvoorbeeld het datacenter van Google in *Iowa in Amerika* maar elk land of elke regio heeft zo zijn eigen Google datacenter. De dichtstbijzijnde Google datacenters voor ons zijn Bergen in Wallonië en Groningen in Nederland.


Deze supercomputers doorzoeken met zeer geavanceerde algoritmes constant het internet. Ze doorzoeken websites en inventariseren woorden, zelfs tot in documenten toe, en onthouden in enorme databases waar deze woorden voorkwamen. Zo kan jij , door gebruik te maken van hun databases, enorm snel documenten terugvinden die uw zoekterm bevatten.

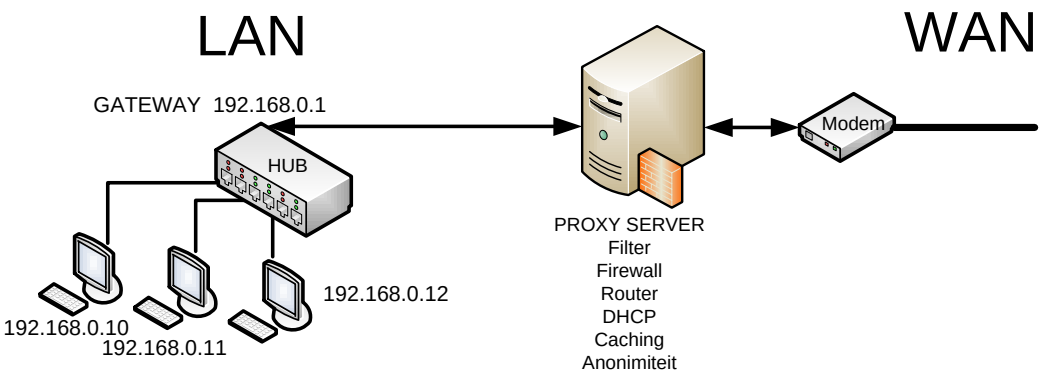
Ze onderzoeken ook hoe populair websites zijn en nemen hiervoor factoren als aantal links op andere sites naar deze webpagina e.d. voor. Hoe hoger de ranking die google geeft – hoe hoger de website staat als deze uw zoekterm zou bevatten. De exacte formule om uw ranking te bepalen bij Google is een goed bewaard geheim.

Je kan Google ook betalen om uw website een hogere ranking te geven….

Als je via Google dus een bepaalde vraag stelt, dan worden de woorden uit die vraag opgezocht in de enorme databases van Google. De webpagina's waarvan Google weet dat het deze woorden bevat worden getoond in een volgorde die Google bepaald, afhankelijk van de ranking.

## WAT IS EEN PROXY SERVER

*Een proxyserver is een server die zich bevindt tussen de computer van een gebruiker en het internet (het Engelse woord "proxy" betekent gevolmachtigd tussenpersoon). Surfen op het net gebeurt nu via een tussenstap. Het doel van deze tussenstap is afhankelijk van het type proxyserver.*




Proxyservers kunnen verschillende functies hebben:

**Filteren van informatie** : Bepaalde opgevraagde websites kunnen wel of niet worden getoond, afhankelijk van een in te stellen filter.

**Beveiliging** : De proxyserver kan de functie van de firewall voor zich nemen.

**NAT router** : De proxy kan ook de functie van de NAT router voor zich nemen. De proxy vertaalt dan alle uitgaande IP berichten naar een bericht met de IP adres van het Netwerk.

**DHCP** : De proxy kan worden ingesteld als DHCP server en kan zo de IP adressen, Subnet mask, DNS servers ed doorgeven aan alle PC's die worden ingeschakeld in dit netwerk.

**Cachen van website** : De proxy slaat een website die van binnen het netwerk wordt opgevraagd zelf ook op. Indien nog een gebruiker in dit netwerk deze website opvraagt, dan beslist de proxy om deze website uit zijn eigen cache (geheugen) te halen zodat de internetlijn voor deze aanvraag niet belast wordt. Voor websites die snel veranderen (denk aan sturen en meten via IP) is dit cachen eerder een nadeel vermits je niet zeker bent dat je de meest recente pagina ziet.

**Anonimiteit / Misbruik** : Een zeer groot deel van de spam die tegenwoordig op het internet verstuurd wordt, maakt gebruik van open proxy's. Veelal installeren spammers open proxy's op computers met behulp van virussen die voor dit doel zijn ontworpen. Je kan zo anoniem surfen via illegaal opgezette proxy servers die dikwijls aan de andere kant van de wereld staan. Mensen die misbruik maken op chat netwerken (denk aan pedofielen) maken ook vaak gebruik van open proxy's om hun identiteit te verhullen.

## WAT ZIJN COOKIES

Cookies zijn kleine stukjes data die bij het surfen op uw computer worden opgeslagen. Het zijn geen uitvoerbare bestanden en kunnen dus geen virussen bevatten.

Positief: Als u meermaals dezelfde websites bezoekt dan zorgen de cookies op uw PC er voor dat de login info reeds wordt ingevuld. Dat versnelt het surfen aanzienlijk. Het zijn ook deze cookies die er voor zorgen dat webpagina's die je al eens bezocht hebt in een andere kleur worden weergegeven.

Negatief: Door deze cookies weten de websites en zoekmachines meer over u dan u beseft. Door uw cookies te doorzoeken kennen ze uw surfgedrag, ze kennen uw interesses en websites zullen zo proberen om u producten of diensten te verkopen waar u interesse in heeft.

U kan uw webbrowser zo instellen dat cookies bij afsluiten automatisch verwijderd worden.

## WIRELESS INTERNET

Wireless internet of WIFI wordt omgeschreven in de internationale standaard IEEE 802.11. WIFI Signalen worden draadloos gecommuniceerd in de 2.4GHz en/of de 5GHz band. Het uitgezonden vermogen van deze wireless apparaten wordt bij wet beperkt tot 100mWatt wat in de praktijk het zendbereik beperkt tot minder dan 30 meter. (Op de illegale markt zijn echter routers te koop van 500mwatt of meer…)

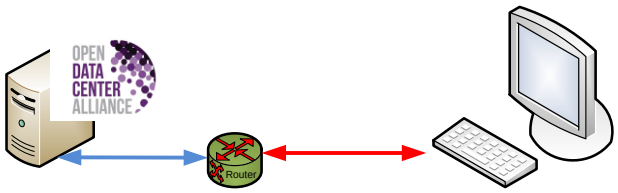
Wireless Access point : link tussen UTP en wireless transmissie

Wireless router : voorziet ook de functie van router

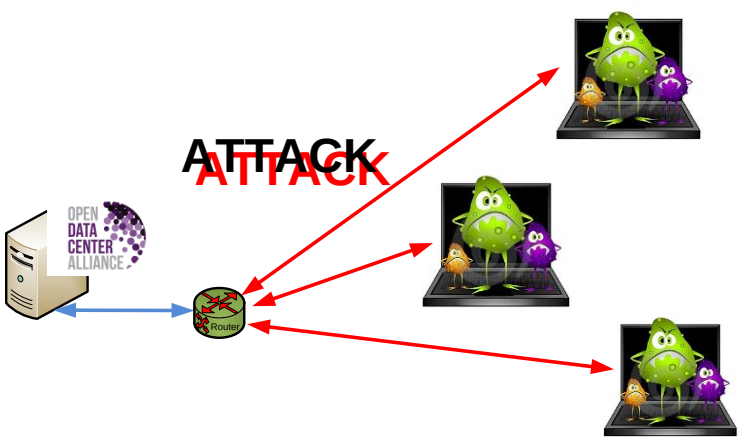
Wireless modem-router : voorziet de functie van wireless access, router en modem in één toestel.

Beveiliging: Een wireless access point dient beveiligd te worden om te vermijden dat vreemden via deze weg op uw netwerk kunnen. Dat gebeurt via een WPA of WPA2 versleuteling. De WPA2 is nagenoeg niet te kraken.

## HOE WORDEN WEBSITE PLAT GELEGD




Er wordt wel eens gesproken over een attack op een website door hackers. Praktisch gebeurt dit door een bepaalde webserver te bestoken met enorm veel en snel opeenvolgende aanvragen van webpagina's. De routers die voor deze webservers staan beveiligen de webserver hier tegen door te snel opeenvolgende requests van het zelfde IP adres te blokken.




Hackers omzeilen dit doordat ze hun aanval nauwkeurig voorbereiden:

- Hackers verspreiden eerst stukjes virussoftware via mail ed. Meestal zullen virusscanner dit detecteren en deze virussen automatisch verwijderen, maar bij nog te veel onbeveiligde PC's kan deze software toch zonder medeweten van de eigenaar geïnstalleerd worden. Soms worden zo virussen ingewerkt in games en software die als illegale download geïnstalleerd wordt door gebruikers. Op het eerste zicht blijft alles perfect werken, maar op de achtergrond draait er nu een extra programma mee, zonder dat de eigenaar hier iets van weet.
- Op het moment dat hackers dat wensen kunnen ze al deze virus-programma's gelijktijdig activeren en instellen om één bepaalde site te bestoken met info-requests. Omdat de vragen nu komen van soms duizenden verschillende IP adressen kunnen de routers deze niet blokkeren en zal de server in 'overload' gaan, maar ook hiertegen worden volop stappen ondernomen om routers en servers hiertegen te beveiligen.

## YOUTUBE FILMPJES – “HOW THE INTERNET WORKS”

| | |
|---|---|
| http://youtu.be/i5oe63pOhLI?hd=1 | How does the internet work |
| http://youtu.be/xIuBmOufbls | How IP packets travel in networks |
| http://youtu.be/zqdTW2_hDvA | How NAT routers work |
| http://youtu.be/EkNq4TrHP_U | Lange les – TCP-IP-Routing,DHCP,DNS,NAT |
| http://youtu.be/9hIQjrMHTv4?hd=1 | Animatie over ‘history of the internet – 8min’ |
| http://youtu.be/Jj6EHgSsx_U | Korte animatie over hoe internet werkt |
| http://youtu.be/Qoe8jvpOQhY | Knappe animatie over routing tabellen |

## UITDAGINGEN:

- Teken zelf een blokschema van het internet. Dit schema moet 3 routers bevatten, 2 webservers, 1 DNS server, 1 mailserver, 2 ISP routers, en 2 LAN netwerken met elk 3 PC's.
- Hoe komen routers te weten wat de beste route is voor een bepaald pakket?
- Waarin slaan routers al deze info op?
- Wie betaalt er voor al die routers en hun onderhoud?
- Gebruik "tracert" om een aantal verschillende servers te bereiken. Probeer eens om een server te zoeken waarvoor er meer dan 15 hops nodig zijn om deze te bereiken.
- Gebruik het blokschema van het internet om uit te leggen hoe een mail verstuurt wordt van een Gmail naar een Hotmail adres.
- Als ik in mijn internetbrowser intyp: http://www.technopolis.be, leg dan mbv het blokschema van het internet uit wat er juist gebeurt. Door ook nog eens gebruik te maken van de tracert functie kan je op heel wat stappen zelfs ook de exacte IP adressen plakken. – surf eens afzonderlijk naar al deze IP adressen…
- Leg in eigen woorden uit wat zoekmachines zijn. Hoe ze werken en hoe ze hun geld verdienen…
- Onderzoek op welke locaties er wereldwijd datacenters van Google staan.
- Zoek even op de naam Googleplex – dit is het hoofdkantoor van Google. Zou je hier willen werken?
- Wat zijn de verschillende mogelijke taken die een proxy server op zich kan nemen. Verklaar kort.
- Waarom kunnen cookies geen virussen bevatten?
- Waarom kunnen cookies een bedreiging zijn voor onze privacy?
- Wat is het verschil tussen een wireless access point, een Wireless router en een wireless modem router? Welk type toestel heb jij thuis staan.
- Gebruik een tekenprogramma zoals VISIO om uw netwerk tot in detail uit te tekenen. Dit kan uw schoolnetwerk, maar ook uw thuisnetwerk zijn. Teken alle PC's, router(s), switches, Wireless apparaten, proxy server, vernoem zoveel mogelijk IP adressen, kortom maak er iets knap van!
- Wireless routers kunnen officieel maximaal op 100mWatt uitzenden en dus 15 meter overbruggen. Bekijk even de website wirelessAntwerpen en laat u van het tegendeel overtuigen…
- Leg in eigen woorden uit hoe websites worden platgelegd.