Infrastructuur

marijn verschuren

2022

Contents

[1 Het internet 2](#_Toc117257547)

[2 Lokaal Netwerk 3](#_Toc117257548)

[3 Lokale IP adressen 4](#_Toc117257549)

[4 Hardware 5](#_Toc117257550)

[5 Protocollen 6](#_Toc117257551)

[6 SSL 7](#_Toc117257552)

# 1 Het internet

Het internet is een verzameling computers die met elkaar kunnen communiceren (meestal) via kabels. Iedere computer op het internet heeft een adres dit word een IP adres genoemd, deze heb je nodig als je iets wil versturen. Als je bijvoorbeeld een site opent zoekt je computer naar het IP adres dat hoort bij de link dit doet je computer door te kijken in de DNS (Domain Name System) dit is een server en heeft een afgesproken IP-adres (bijvoorbeeld: 8.8.8.8). als je een IP-adres wil opvragen van deze DNS maak je gebruik van client server communicatie (via port 53), hierbij vraag je als client iets aan de server hierna zal de server een antwoord terug sturen.

Nu de computer (client) het IP adres van de site heeft opgezocht kan het vragen voor de web pagina aan de server. Als de server dit ontvangt zal de server de informatie nodig voor de webpagina terug sturen. De tijd die nodig is voor het laden van de web pagina veranderd naar mate de afstand tussen de client en de server veranderd omdat als je iets stuurt naar een server in New York moet deze data onder de oceaan via een onderzeese kabel (figuur 1). Om data via een onderzeese kabel te sturen heb je ook meerdere stappen nodig dit vertraagt de data nog meer. Dit verschil in laad tijd word afgebeeld in figuur 2 en 3

Diagram

Description automatically generated

Figuur 1 Onderzeese kabels (bron: https://www.submarinecablemap.com)

A screenshot of a computer

Description automatically generated with medium confidence

Figuur 2 New York Server (bron: https://www.meter.net)

A screenshot of a computer

Description automatically generated with medium confidence

Figuur 3 Amsterdam Server (bron: https://www.meter.net)

# 2 Lokaal Netwerk

Een lokaal netwerk is net als het internet een verzameling computers die met elkaar kunnen communiceren, maar in het geval van een lokaal netwerk zijn er minder computers en op een kleiner gebied of wel LAN (Local Area Network). Binnen dit netwerk krijgt elk device een lokaal IP adres dit werkt precies het zelfde als IP adres op het internet maar dan lokaal. Er is echter een device op het lokale netwerk die twee IP adressen heeft en dat is de router of default gateway deze heeft namelijk een publiek (op het internet) IP adres en een lokaal IP adres. Alle communicatie van de devices op het lokale netwerk naar het internet gaan via de router of default gateway.

Chart, box and whisker chart

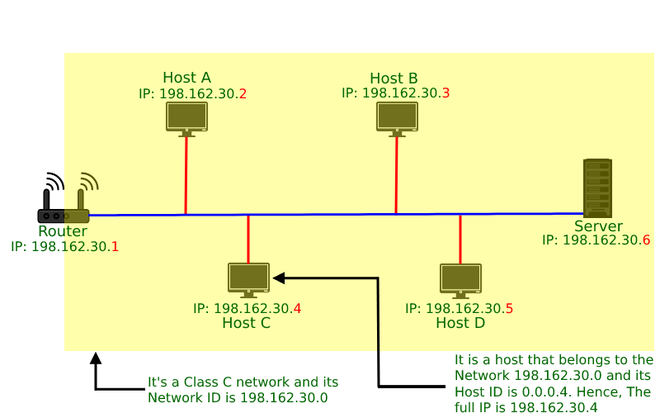
Description automatically generated

Figuur 4 Netwerk

Van af mijn router naar de servers van de apps die ik gebruik gaat de communicatie met een kabel maar van af mijn router naar mijn laptop, printer en telefoon gaan draadloos via wifi.

# 3 Lokale IP adressen

In een lokaal netwerk heb je meerdere apparaten die met elkaar kunnen praten. Ieder apparaat in dit netwerk krijgt een adres van de router (als deze geconfigureerd is als DHCP). Naast een adres heeft ieder apparaat een subnet mask deze mask geeft aan welke bits van het adres constant zijn tussen alle apparaten in het netwerk (dit subnet mask is hetzelfde bij alle apparaten in het netwerk). Alles wat niet tot het subnet mask behoort word het host-ID genoemd.



Figuur 5 host id’s binnen een netwerk (bron: https://www.geeksforgeeks.org/what-is-network-id-and-host-id-in-ip-addresses/)

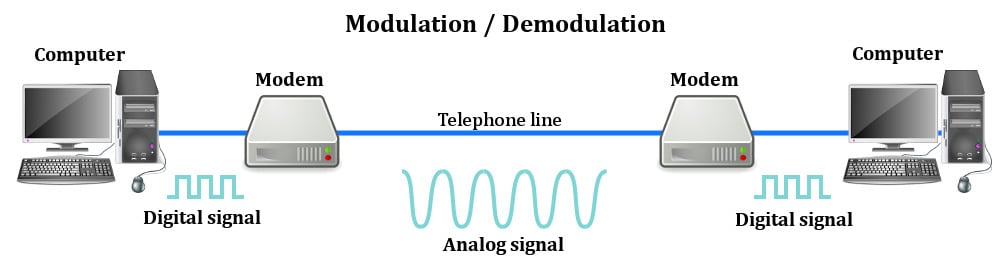
In een lokaal netwerk is de router vaak de enige weg naar buiten deze word dan ook de default gateway genoemd. De router krijgt een publiek IP toegewezen door de ISP (internet service provider) dit gebeurd op een soortgelijke manier als DHCP. Nu je router een publiek IP heeft kan je met je computer via je router het internet bezoeken omdat de externe servers die je gebruikt je terug kunnen vinden via je publieke IP.

Diagram

Description automatically generated

Figuur 6 vcenter network

# 4 Hardware

In een netwerk zitten verschillende apparaten (hardware) met verschillende taken bijvoorbeeld: de router (default gateway), Modem of een Switch. De router zorgt er voor dat communicatie met het internet mogelijk is en dat elk apparaat een lokaal IP-adres heeft (als DHCP aan staat). De modem heeft een iets andere taak, het is namelijk verantwoordelijk voor het vertalen van signalen die via een kabel bijvoorbeeld bij je huis aankomt naar een signaal dat de router snapt.De modem vertaalt ook de signalen van je router naar een signaal dat over de kabel weer weg wordt gestuurd zodat dit bij een andere modem weer afgelezen kan worden (figuur 7). De switch is speelt een iets minder cruciale rol namelijk het splitten van een internet kabel naar meerdere kabels hierdoor kunnen er meer devices op een netwerk. 

Figuur 7 modem signaal (bron: https://www.scienceabc.com/innovation/what-is-a-modem-what-does-it-do-router-working.html)

# 5 Protocollen

In een netwerk worden meestal twee protocollen gebruikt dit zijn TCP (transmission control protocol) en UDP (user datagram protocol). TCP word gebruikt voor veilige transmissie van data door de data samen met een checksum te sturen hiermee kan de ontvanger errorcorrectie toepassen als er een fout in de data is gedetecteerd. Ook moeten de client en de server een soort handshake aangaan met elkaar (figuur 8) hierdoor weten de client en de server dat de ander aanwezig is.

Arrow

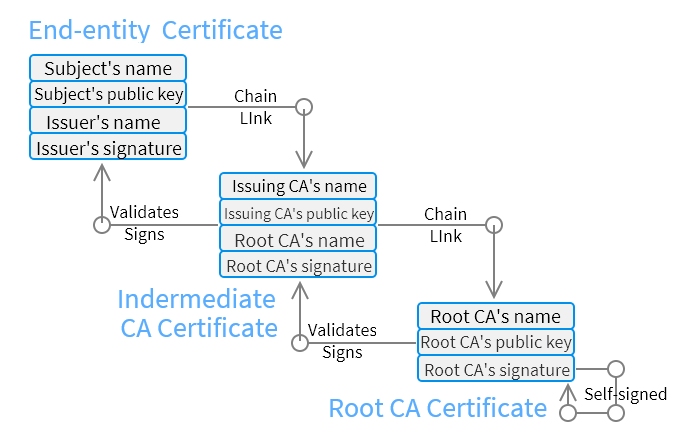
Description automatically generated with medium confidence

Figuur 8 TCP handshake (bron: https://nl.wikipedia.org/wiki/Transmission\_Control\_Protocol)

UDP is eigenlijk precies hetzelfde als TCP maar zonder fouten correctie dus deze is niet zo veilig en word daarom ook alleen gebruikt in gevallen waar het niet zo erg is als de data niet goed aankomt. De voordelen van UDP zijn dat het een stuk sneller is omdat er geen handshake nodig is. UDP heeft wel een checksum maar deze wordt alleen gebruikt om te checken of er een error aanwezig is, als dit het geval is vraagt de client voor nieuwe data.

# 6 SSL

SSL (Secure Socket Layer) is een encryptie methode die gebruikt word door https sites om er voor te zorgen dat de comunicatie tussen aparaten en de server niet afgeluisterd kan worden. SSL maakt vaak gebruik van AES (Advanced Encryption Standard). In mijn geval geeft google me alsnog een waarschuwing dat het niet veilig is omdat ik een zogeheten self signed SSL token gebruik dit is niet veilig omdat er geen derde partij is die daadwerkelijk checkt of mijn site wel veilig is (als deze derde partij mijn site veilig vind dan signen zij mijn token). Deze derde partij is gecertificeerd door de CA (Certificate Authority) en maakt deel uit van de chain of trust (figuur 9). Onder aan de chain of trust zit de Root CA certificate deze is selfsigned maar word niet als onveilig beschouwd omdat we hebben afgesproken dat we deze vertrouwen vandaar de naam chan of trust.



Figuur 9 Chain of trust (bron: https://www.keyfactor.com/blog/certificate-chain-of-trust/)

Graphical user interface, text, application

Description automatically generated

Figuur 10 site