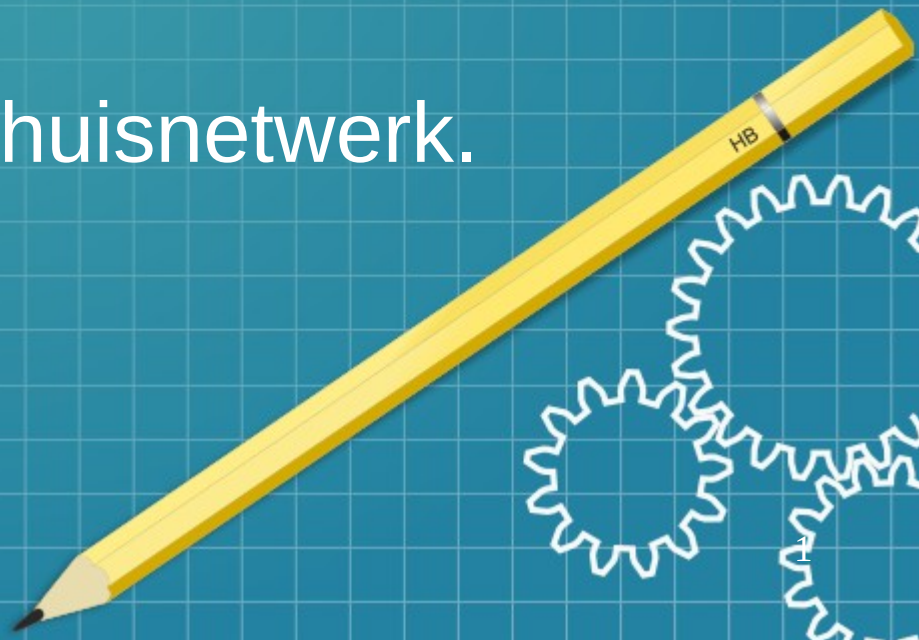
THUISNETWERK

Een uitleg over een thuisnetwerk.



Onderwerpen

- ISP / WAN / LAN
- ROUTER / SWITCH
- IP adres / NAT
- DHCP / DNS
- Netwerk classes A/B/C
- GATEWAY / SUBNETMASK
- Broadcast address
- TPC / UDP / ICMP
- Port forwarding / DMZ

Netwerken

We hebben voor ons thuisnetwerk de beschikking over IP adressen uit de privéklassen netwerken A,B of C

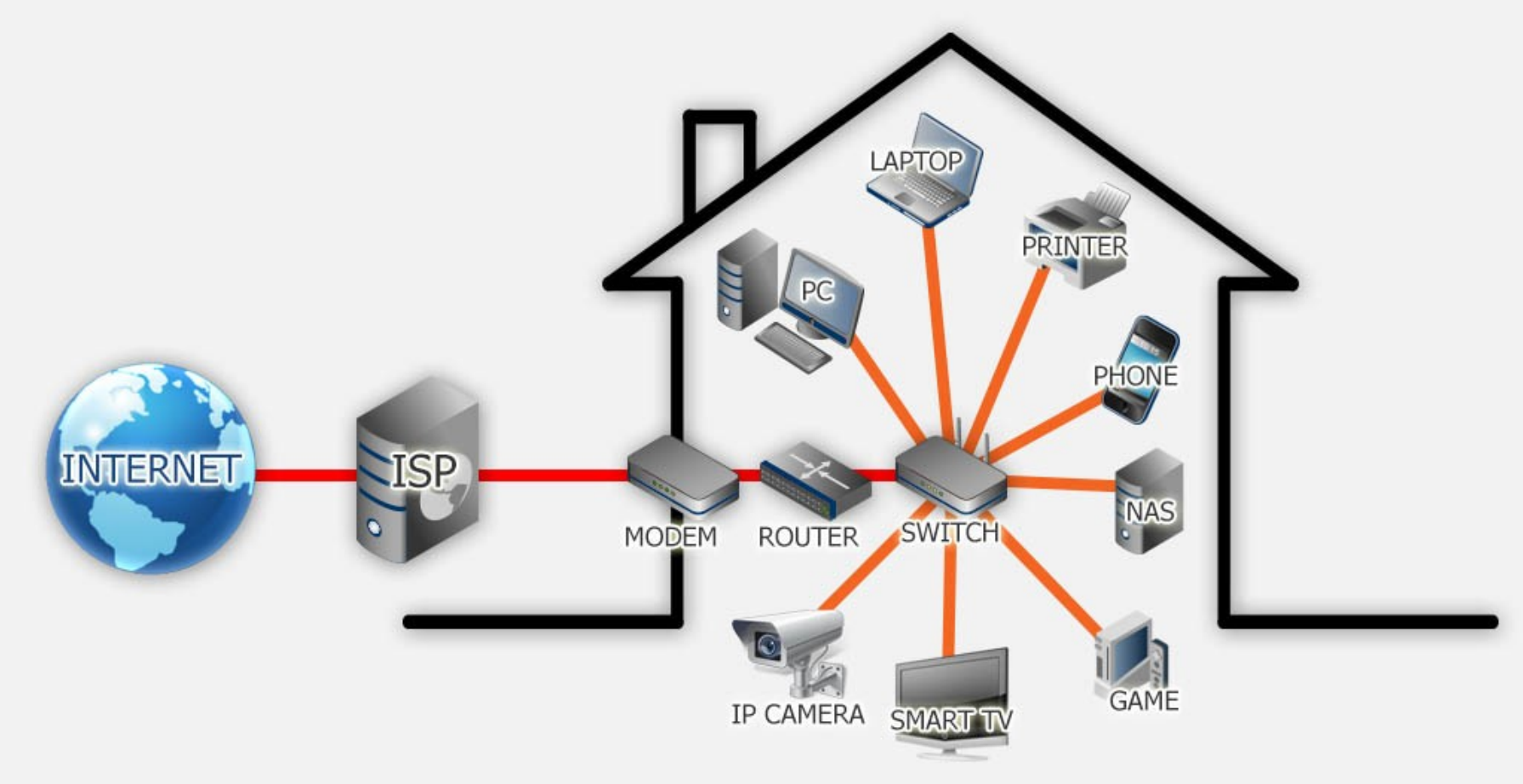
Class	Starting IP Address	Ending IP Address	Aantal apparaten
A	10.0.0.0	10.255.255.255	16.777.216
B	172.16.0.0	172.31.255.255	1.048.576
C	192.168.0.0	192.168.255.255	65.536

De meeste zullen bekend met het C netwerk zijn.
Dit zijn de adressen die beginnen met 192.168.xx.xx

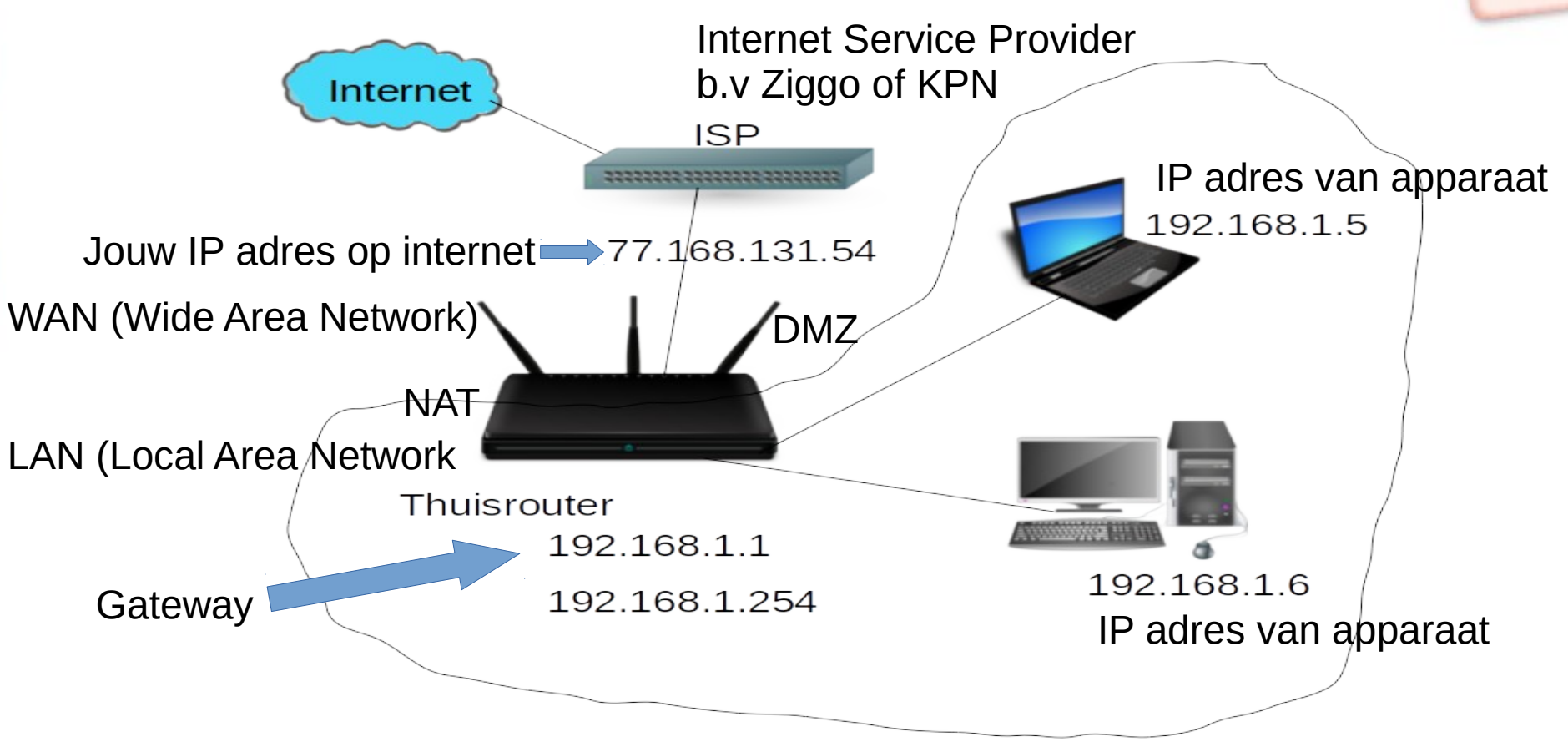
Deze adressen zijn NIET routeerbaar over internet.
Je kan ze dus alleen in een lokaal netwerk gebruiken!

Veel apparaten in huis

Opbouw


LAPTOP
PRINTER
PC
PHONE
INTERNET
ISP
MODEM
ROUTER
SWITCH
NAS
IP CAMERA
SMART TV
GAME

Wat betekenen al die kreten?



Netmask 255.255.255.0
Broadcast address 192.168.1.255
DNS1 8.8.8.8
DNS2 8.8.4.4

Netmask

Het netmask is ervoor om aan te geven welk gedeelte van het IP adres het nummer van het apparaat is die je wilt bereiken. Als we nu kijken naar het adres 192.168.1.44 zien we dat het opgedeeld is in 4 stukjes. Die noemen we octets. Computers doen alles binair dus met het 2 tallig stelsel. Daar hebben we een 1 of een 0.
Als we een netmask hebben van 255.255.255.0 dan dit binair
11111111.11111111.11111111.00000000

Netmask

11111111.11111111.11111111.00000000

Nu gaan we even rekenen:
128 64 32 16 8 4 2 1

Dit zijn de waardes van de bits, dus de meest linkse is 128 waard in ons 10-tallig stelsel.
tel nu alle 1 bits op in 1 octet. Dan krijgen we
128+64+32+16+4+2+1= 255
De router die het ip adres 192.168.1.44 binnenkrijgt “legt” hier overheen het netmask

Netmask

11111111. 11111111. 11111111.00000000

11000000.10101000.00000001.00101100

De router rekent het subnet uit dmv een binaire AND uit te voeren met het netmask. Dwz er komt alleen een 1 uit als beide 1 zijn. Dit geeft dus:

11000000.10101000.00000001.00000000

Omgerekend is dit 192.168.1.0 en dit is het subnet
De host is het nummer in het laatste octet dus 00101100 en dat is 44. De router weet nu dat hij de host met nummer 44 op het subnet 192.168.1.0 moet adresseren

Netwerkadres

- Het subnetwerkadres is dus 192.168.1.0
- Het broadcast adres is 192.168.1.255

We zien dat er op ons netwerk dus 256 adressen beschikbaar zijn van 0..255
Adres 0 kan je niet gebruiken want dit is het netwerkadres. Het allerhoogste adres is altijd het broadcoast adres (255) Dus het aantal apparaten wat je op dit subnetwerk kan adresseren is n-2 of te wel 256 – 2 = 254 verschillende apparaten.

Broadcastadres

Het broadcastadres is een IP-adres waarvan alle hostbits de waarde 1 hebben. Het broadcastadres wordt gebruikt als een IP-pakket moet worden gestuurd aan alle apparaten die zich binnen hetzelfde subnet bevinden als de afzender van het bericht. Dit kan bijvoorbeeld nodig zijn bij berichten die informatie geven over een configuratieverandering in het netwerk, bijvoorbeeld DHCP.

Gateway

Een gateway is een netwerkpunt dat dienstdoet als "toegang" tot een ander netwerk. De gateway is dan een netwerkconfiguratie-eigenschap die aangeeft welk netwerkadres de computer mag gebruiken als hij naar een bestemming moet die niet op het lokale netwerk gelegen is. Een gateway wordt daarom vaak geassocieerd met een router omdat hij wijst naar de router die uiteindelijk verbonden is met buiten. Per fysieke netwerkkaart zijn er één of meer gatewayadressen in te stellen.

DNS

Het Domain Name System (DNS) is het systeem en netwerkprotocol dat op het Internet gebruikt wordt om namen van computers naar numerieke adressen (IP-adressen) te vertalen en omgekeerd. Hoewel dit "vertalen" genoemd wordt gaat het gewoon om opzoeken in tabellen, waarin namen aan nummers gekoppeld zijn.

Unieke IP-adressen thuis?

Hoe kan het nu dat we maar 1 uniek IP-adres hebben van onze ISP en toch heel veel apparaten kunnen aansluiten in ons thuisnetwerk die allemaal een uniek IP-adres hebben?

Deze slimme truc heet NAT of te wel

Network Adress Translation

NAT

Network address translation (NAT, ook wel network masquerading of IP masquerading) is een verzamelnaam voor technieken die gebruikt worden in computernetwerken waarbij de adresinformatie in de datapakketjes veranderd wordt. Zodoende kunnen verschillende netwerken aan elkaar worden verbonden. De techniek wordt hoofdzakelijk in routers ingezet

Technisch worden IP-adressen veranderd in de header van een IP-bericht dat een router passeert. Vaak wordt ook het TCP/UDP-poortnummer veranderd, opdat men kan bijhouden welke veranderingen hebben plaatsgevonden. Een veel voorkomende toepassing is het toelaten van meerdere gebruikers van een thuisnetwerk tot het internet via één IP-adres.

Protocollen

We hebben verschillende protocollen waarmee we over het netwerk kunnen communiceren.

- DHCP Dynamic Host Configuration Protocol
- TCP Transmission Control Protocol
- UDP User Datagram Protocol
- ICMP Internet Control Message Protocol

DHCP

Dynamic Host Configuration Protocol

Bij DHCP is het principe dat toestellen in een IP-netwerk geen vast geconfigureerd IP-adres hebben, maar hun IP-adres dynamisch verkrijgen van een centraal beheerde DHCP-server. De server, die zelf een vast IP-adres heeft, beheert hiertoe een "pool" van beschikbare IP-adressen, veelal in de private address space volgens RFC 1918. Na opstarten van de DHCP-server zijn die adressen vrij en kunnen ze aangevraagd worden door de toestellen op het netwerk. Door de aanvragen worden de IP-adressen toebedeeld, uiteraard in aantal beperkt tot de grootte van de pool.

Toestellen die op het netwerk komen, kunnen via een aanvraagsequentie een IP-adres verkrijgen dat beperkt geldig is, voor de ingestelde geldigheidsduur, de "lease time". Toestellen die het netwerk verlaten, dienen hun adres vrij te geven. Dit gebeurt uiteraard niet in alle gevallen. Het adres komt echter uiteindelijk toch weer vrij door het verlopen van de geldigheidsduur.

DHCP-servers kunnen voor bepaalde toestellen een vast uit te reiken IP-adres geconfigureerd hebben. Zo kan het bv. zijn dat binnen een bedrijf alle netwerkprinters een vast IP-adres krijgen, dit terwijl andere toestellen een willekeurig adres uit de pool toebedeeld krijgen.

TCP

Het Transmission Control Protocol (TCP) is een verbindingsgeoriënteerd protocol dat veel gebruikt wordt voor gegevensoverdracht over netwerkverbindingen op het internet en op computernetwerken zoals local area networks en thuisnetwerken.

TCP/IP is een IP-netwerkprotocol voor stabiele, betrouwbare netwerkverbindingen en geen verbindingsloos protocol zoals UDP en GRE. TCP heeft als kenmerken dat het gegevens in een datastroom kan versturen, waarbij de garantie wordt geleverd dat de gegevens aankomen zoals ze verstuurd werden, en eventuele communicatiefouten, zowel in de gegevens zelf als in de volgorde van de gegevens kunnen worden opgevangen. Hierdoor hoeft een clientapplicatie die TCP als transmissieprotocol gebruikt, geen rekening te houden met de onderliggende netwerkarchitectuur en eventuele fouten in de communicatie.

UDP

Het User Datagram Protocol (UDP) is een van de basisprotocollen van het internet. Het protocol opereert op hetzelfde niveau als TCP en wordt beschreven in RFC 768.

UDP is onbetrouwbaar: het protocol biedt geen garantie dat de gegevens daadwerkelijk aankomen, wat bij TCP wel het geval is. Een aantal protocollen dat via UDP werkt, implementeert zelf een verificatiemethode. Hiermee zorgen ze effectief voor een vervanging van de functionaliteit die TCP heeft op dit gebied.

UDP wordt veel gebruikt bij toepassingen waar het snel overdragen van de gegevens en een korte reactietijd zeer belangrijk is, en het minder erg is dat er gegevens verloren kunnen gaan, zoals bij telefonie, videoconferencing, DNS of het online spelen van actievolle spellen, zoals first person shooters.

ICMP

Het Internet Control Message Protocol (ICMP) is een onderdeel van het Internetprotocol (IP). Het wordt vooral gebruikt door besturingssystemen voor het sturen van foutmeldingen, bijvoorbeeld om te melden dat een bepaalde netwerkvoorziening niet beschikbaar is, of dat een bepaalde host of router niet bereikbaar is. Soms komt een computergebruiker ook direct met het protocol ICMP in aanraking, voornamelijk bij gebruik van de netwerkdiagnoseprogramma's ping en traceroute.

Hoewel het protocol beschreven wordt in een apart RFC-document dat losstaat van het document dat het IP zelf beschrijft, is ICMP een integraal onderdeel van IP, en wordt de implementatie ervan voor iedere IP-module voorgeschreven. ICMP wordt gedefinieerd in RFC 792.[1] Voor Internet Protocol versie 6 (IPv6) wordt ICMP gedefinieerd in RFC 1885.[2] ICMP is een verbindingsloos protocol met IP-protocolnummer 1 voor IPv4 en 58 voor IPv6.[3]

Men zou ICMP kunnen beschrijven als het protocol dat de administratie van een netwerk verzorgt; het laat gebruikers toe problemen uit te pluizen, en stelt TCP/IP-implementaties in staat om foutberichten te sturen naar communicatiepartners.

Port Forwarding

In dit voorbeeld hebben we een webserver draaien op onze PC.
De webserver is actief op poort 80. Vanaf het internet is onze webserver NIET bereikbaar omdat de router (via NAT en de firewall) alle inkomende connecties blokkeert. Nu stellen we in de router in dat aanvragen voor poort 80 vanuit het internet (77.165.122.68) moeten worden doorgestuurd naar de PC met adres 192.168.1.6:80 (poort 80)
Nu kunnen we vanuit het internet met een browser intypen: http://77.165.122.68:80 en deze aanvraag zal nu door de router worden Doorgestuurd naar 192.168.1.6:80 en dat is onze webserver! Vanaf nu zijn we bereikbaar over internet. Per router is het verschillend hoe je portforwarding moet instellen.

DMZ

Demilitarized zone:Een demilitarized zone (afgekort: DMZ) is een netwerksegment dat zich tussen het interne en externe netwerk bevindt. Het externe netwerk is meestal het internet.

Een DMZ is feitelijk een andere naam voor een extranet, een gedeelte van het netwerk dat voor de buitenwereld volledig toegankelijk is.

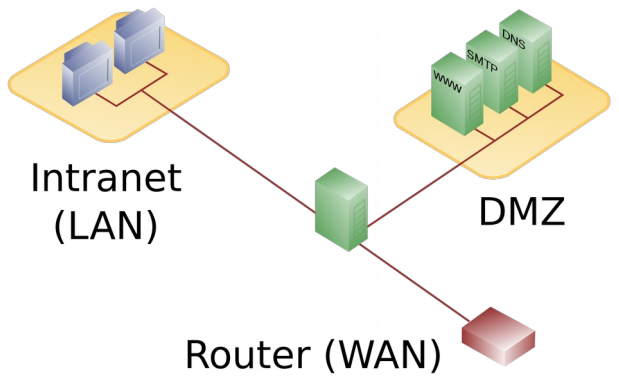
Op het netwerkdeel van de DMZ zijn meestal servers aangesloten die diensten verlenen die vanuit het interne en externe netwerk aangevraagd kunnen worden (bijvoorbeeld een webserver en/of mailserver).

De DMZ dient door een firewall beschermd te worden, maar moet wel zodanig geconfigureerd worden (gaten in de firewall) dat de diensten binnen de DMZ toegankelijk blijven.

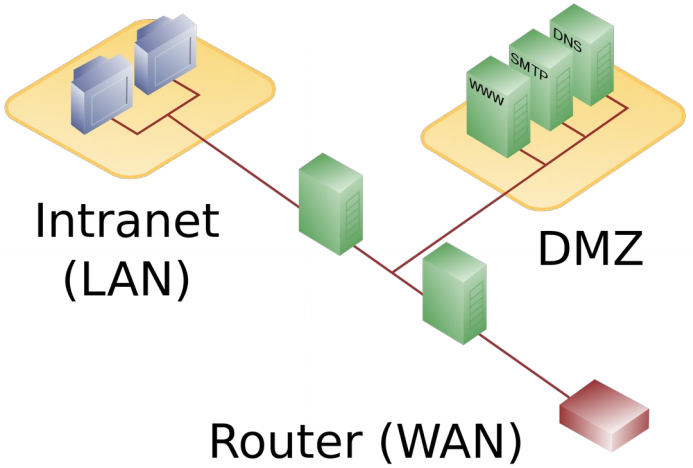
DMZ

In principe zijn er hierdoor twee architecturen voor een DMZ mogelijk.

1x 3-poorts firewall



2x 2-poorts firewalls



Dit is het einde van mijn presentatie over thuisnetwerken.
Ik heb geprobeerd om e.e.a. in “Jip en Janneke” taal uit te leggen. Het is versimpeld en niet compleet, maar ik hoop dat deze presentatie toch verhelderend werkt over hoe ons thuisnetwerk op de achtergrond een heleboel doet om ons toegang tot het grote internet te geven.