

Basis Netwerken

Luca Ruggiero

Ontstaan van het internet

1969 - ARPNET grondslag van het internet (Amerikaans ministerie van Defensie)

- Packet switching als basis voor computernetwerken

1983 - Introductie van TCP/IP in ARPNET als netwerkprotocol

- Eerste protocollen

- E-mail
- FTP
- Telnet

1991 - ontstaan van world wide web protocollen zoals http en html

1993 - internet voor overheid en universiteiten werd internet voor iedereen

Het internet van vandaag

- Wereldwijde verbinding van netwerken door glasvezel die op de bodem van de zee liggen WAN Wide Area Network.
- Een computernetwerk (of netwerk) is een verbinding tussen computers
- Fysieke verbindingen:
 - Koper kabels (UTP/COAX/HUB)
 - Glasvezel kabels
 - Draadloze verbindingen (WiFi – Satelliet)

=> Laag 1 van het OSI (Open System Interconnection Model) model

Het internet van vandaag (vervolg)

Wereldwijde verbinding van netwerken door glasvezel die op de bodem van de zee liggen.

- RFC - Request for Comments
- Zoals RFC1918 - voor private netwerken uit elke klasse is er een deel gereserveerd hiervoor:
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16
- LAN netwerken
- Meest gebruikte protocollen:
 - IP
 - UDP
 - TCP

LAN netwerk

- RFC1918 - voor private netwerken of LAN Network
 - 10.0.0.0/8 (uit klasse A)
 - 172.16.0.0/12 (uit klasse B)
 - 192.168.0.0/16 (uit klasse C)
- Noodzakelijk omdat IPv4 adressen gelimiteerd is 4.294.967.296 ip addresses (2^{32})
- Kunnen verder onderverdeeld worden in kleinere subnets:
 - VLSM: Variable Length Subnet Mask

Communicatie tussen twee computers

- Om een communicatie op te zetten tussen 2 computers zijn er verschillende handelingen nodig om menselijk begrijpbare taal of beelden over te brengen tussen twee of meerdere computers.
- De communicatie wordt bewerkt door 7 lagen dit noemen we het OSI model:
- Open System Interconnection Model:
 - Applicatie - 7
 - Presentatie - 6
 - Sessie - 5
 - Transport - 4
 - Netwerk - 3
 - Data - 2
 - Fysieke - 1
- Enkel laag is een verzameling van protocollen

Applicatie laag 7

- Heeft niets te maken met computer programma's of applicaties maar wel de protocollen die de gekende applicatie werkbaar maken zoals Safari, Chrome, IE, Firefox, Outlook etc.
- Deze applicaties noemen we ook Netwerk Applicaties dus ze maken gebruik van het applicatie laag van het OSI model



Websurfen

E-mail

Voice and video protocol

E-mail

Protocollen: HTTP(s), FTP, NFS, SMTP, NTP, SNMP, SSH, RDP, ...

Beschrijving van de verschillende protocollen kunnen gevonden worden bij IANA voor de registratie en IETF voor de beschrijving:

<https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?&page=1>

<https://www.ietf.org>

UW OPLEIDING, ONZE ZAAK



Presentatie – laag 6

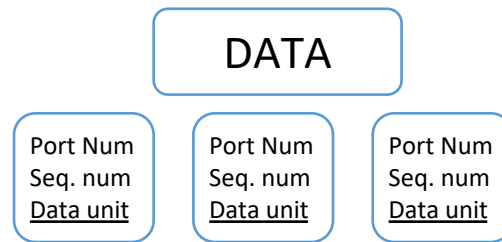
- Data wordt van de Applicatie laag vertaald naar de Presentatie laag, waar de menselijke taal omgezet wordt naar computer taal of 1 en 0
- Om de data over te brengen wordt deze ook gecomprimeerd in kleinere delen zodat de overdracht sneller gaat
- Indien nodig kan deze ook versleuteld worden (encrypted) zodat de data niet gewijzigd en gelezen kan worden:
 - SSL/TLS wordt hiervoor gebruikt!
 - SSL: Secure Socket Layer -> wordt niet meer gebruikt om veiligheidsredenen!
 - TLS: Transport Layer Security is de nieuwe standaard versie 1.2

Sessie – laag 5

- Deze laag is er om de communicatie tussen computers te regelen, hiermee bedoelen we het volgende:
 - Opbouwen van een connectie
 - Onderhouden van een connectie
 - Afbreken of stoppen van een connectie op een propere manier
- Om dit te kunnen verwezelijken zijn er verschillende helper of protocollen zoals
 - API – Application Programming Interface
 - NetBIOS – oud protocol wordt niet meer of amper nog gebruikt
 - RPC – Remote procedure Protocol
 - SMB – Server Message Block
- Services op de Data Pakketen op de juiste wijze en vorm over brengen van server naar bijvoorbeeld uw browser zijn de volgende:
 - Authenticatie
 - Autorizatie
 - Sessie management

Transport – laag 4

- Transport laag is betrokken in volgende events:
 - Segmentatie: opsplitsen van grote data pakketten in kleinere segmenten



- Port nummer om te weten voor welke applicatie het bestemd is
 - Sequence nummer om de volgorde terug te kunnen opbouwen
- Flow control: zorgen dat de juiste snelheden afgesproken worden tussen devices (10Mb/s – 100Mb/s - 1Gb/s)
- Error control: zorgen dat alle verzonden pakketten toekomen op de destination
 - Elk data unit of segment heeft een checksum zodat nagegaan kan worden of de data niet corrupt is geraakt tijdens transport

Transport – laag 4 – UDP Protocol

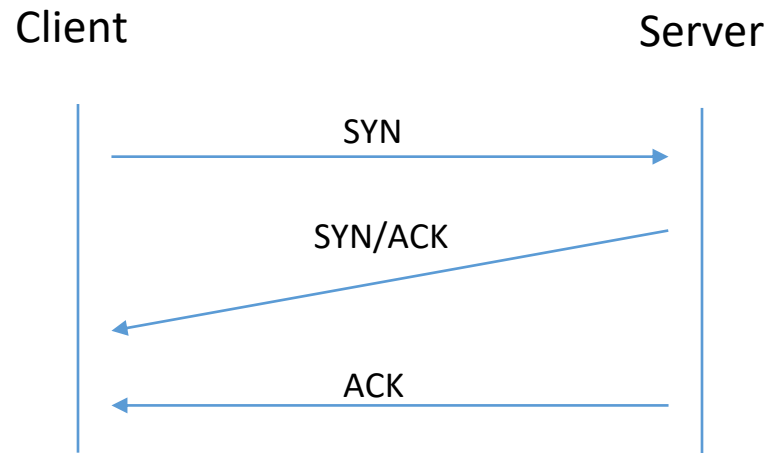
- UDP: user datagram protocol (connectieloze overdracht) wilt zeggen dat het niet controleert of het packet effectief toekomt op de bestemming

Belangrijkste protocollen en poort nummers:

- DNS: 53 domain name system
- TFTP: 69 Trivial File Transfer Protocol
- NTP: 123 Network time protocol
- NetBIOS: 137 NetBIOS Name Service
- SNMP: 161 Simple Network Management Protocol
- OpenVPN: 1194 OpenVPN

Transport – laag 4 – TCP Protocol

- TCP: Transmission Control Protocol
- Connectie georiënteerde overdracht, om na te gaan of de verzonden pakketten effectief toekomen op de bestemming en eventueel een retransmit te starten
- Connectie wordt opgestart via het three way hand shake protocol welke bestaat uit SYN - SYN/ACK - ACK pakketten



UW OPLEIDING, ONZE ZAAK



Transport – laag 4 - TCP Protocol

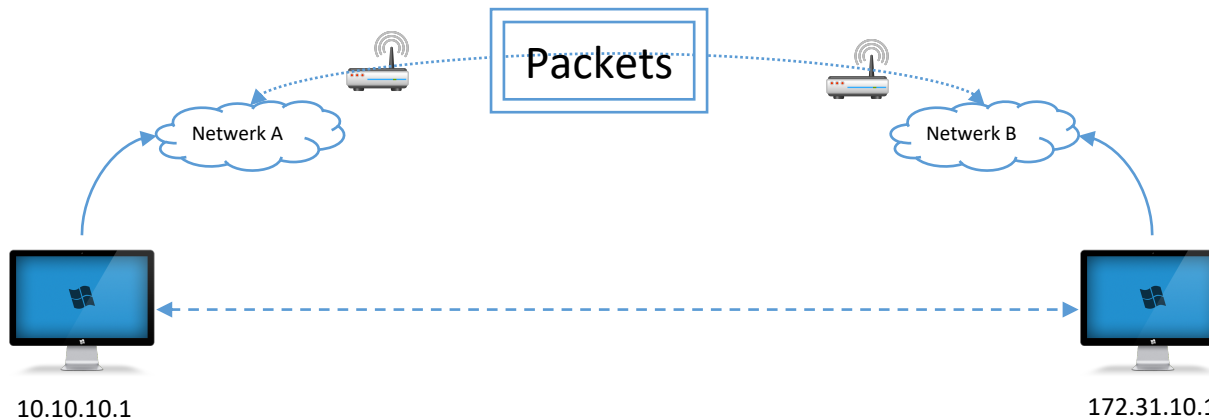
- Belangrijkste protocollen en poort nummers:
 - FTP:21/20/high port - file transfer protocol
 - Telnet: 23 - beheer van machine op afstand (onveilig protocol)
 - SSH: 22 - Secure shell beheer van machine op afstand (veilig protocol)
 - SMTP: 25 - simple mail transfer protocol
 - HTTP: 80 - HyperText Transfer Protocol
 - HTTPS: 443 - HyperText Transfer Protocol over ssl/tls
 - RDP: 3389 - remote desktop protocol

Transport – laag 4 – andere protocollen

- ESP – Encapsulating Security Payload over IP of IPSEC
- AH – Authenticating Header over IP of IPSEC
- FCP – Fibre Channel Protocol
- iSCSI – Internet Small Computer System Interface

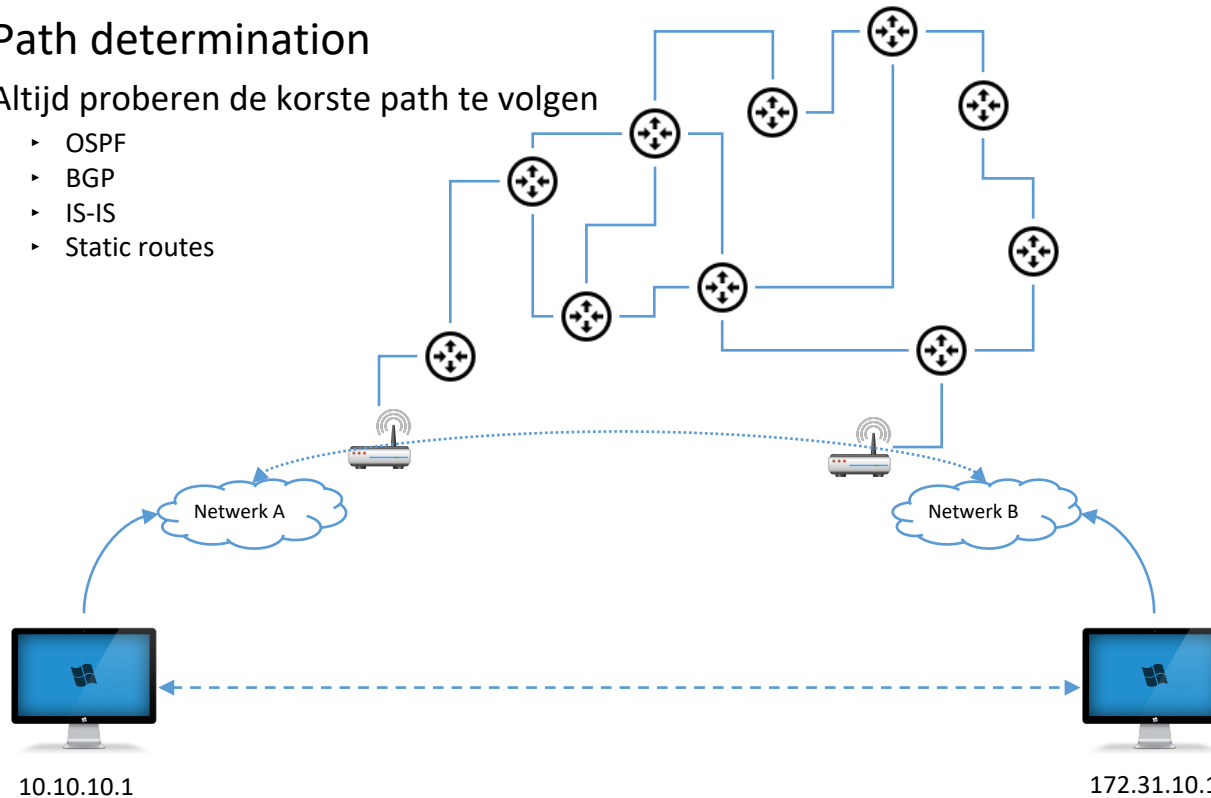
Netwerk – laag 3

- Communicatie tussen verschillende computers en netwerken wordt hier geregeld!
- Afhankelijk van de **logische adressering** spreekt van een netwerk
 - IPv4 en IPv6 + MASK (IPv6 bespreken we in de volgende module)
- Routing tussen verschillende netwerken via default gateway



Netwerk – laag 3

- Path determination
- Altijd proberen de kortste path te volgen
 - OSPF
 - BGP
 - IS-IS
 - Static routes



IPv4

Internet protocol versie 4

- 32 bits
- 4 bytes
- 2 tot de 32 macht
- 4.294.967.296 ip addresses
- 5 klasse van netwerken
 - A klasse: 0.0.0.0 - 127.255.255.255 (grote netwerken)
 - B klasse: 128.0.0.0 - 192.255.255.255 (middelgrote netwerken)
 - C klasse: 192.0.0.0 - 223.255.255.255 (kleinere netwerken)
 - D klasse: 224.0.0.0 - 239.255.255.255
 - E klasse: 240.0.0.0 - 255.255.255.255
- De subnets die standaard toegekend zijn aan netwerken uit de verschillende klasse zijn:
 - Klasse A: 255.0.0.0
 - Klasse B: 255.255.0.0
 - Klasse C: 255.255.255.0

IPv4 (vervolg)

- Uit de eerste 3 klasse hebben we een stuk gereserveerd om RFC1918 op te bouwen (zie slide 2)
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16
- Klasse D is gebruikt voor multicast
- Klasse E voor experimenteel gebruik
- 127.0.0.0/8 is gebruikt voor loopback maar zit dus in klasse A

Opbouw van een IP adres

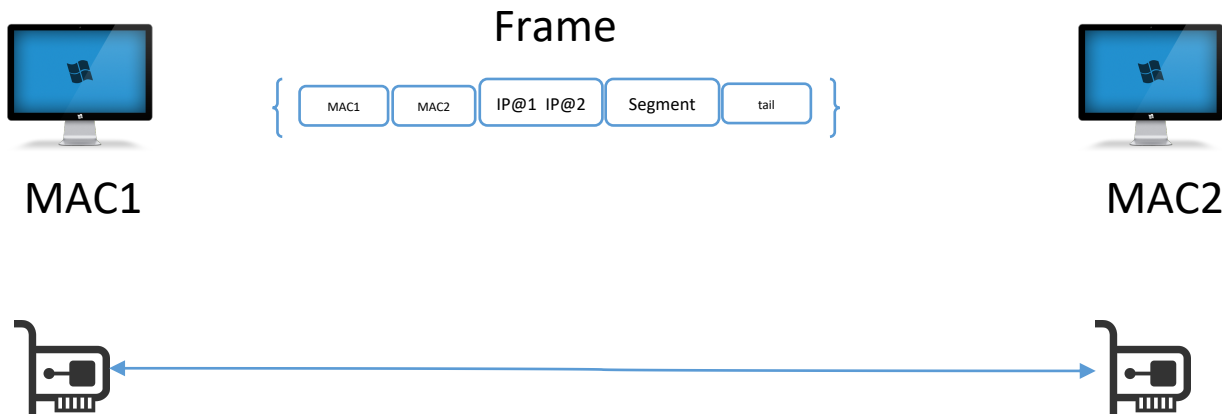
4 bytes bestaande uit volgende een combinatie van bits

192.168.22.99/17

	2 ⁷	2 ⁶							2 ⁵							2 ⁴							2 ³							2 ²							2 ¹							2 ⁰																				
	128								64								32								16								8								4								2								1							
IP	192								168								22								99																																							
	128+64								128+32+8								16+4+2								64+32+2+1																																							
IP Binair notatie	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	1	0	1	1	0	0	1	1	0	0	0	0	0	0	0																														
Subnetmask binair	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0																															
Netwerk adres binair	1	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0																															
Netwerk adres	192								168								0								0																																							
Broadcast binair	1	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1																															
Broadcast adres	192								192								127								255																																							

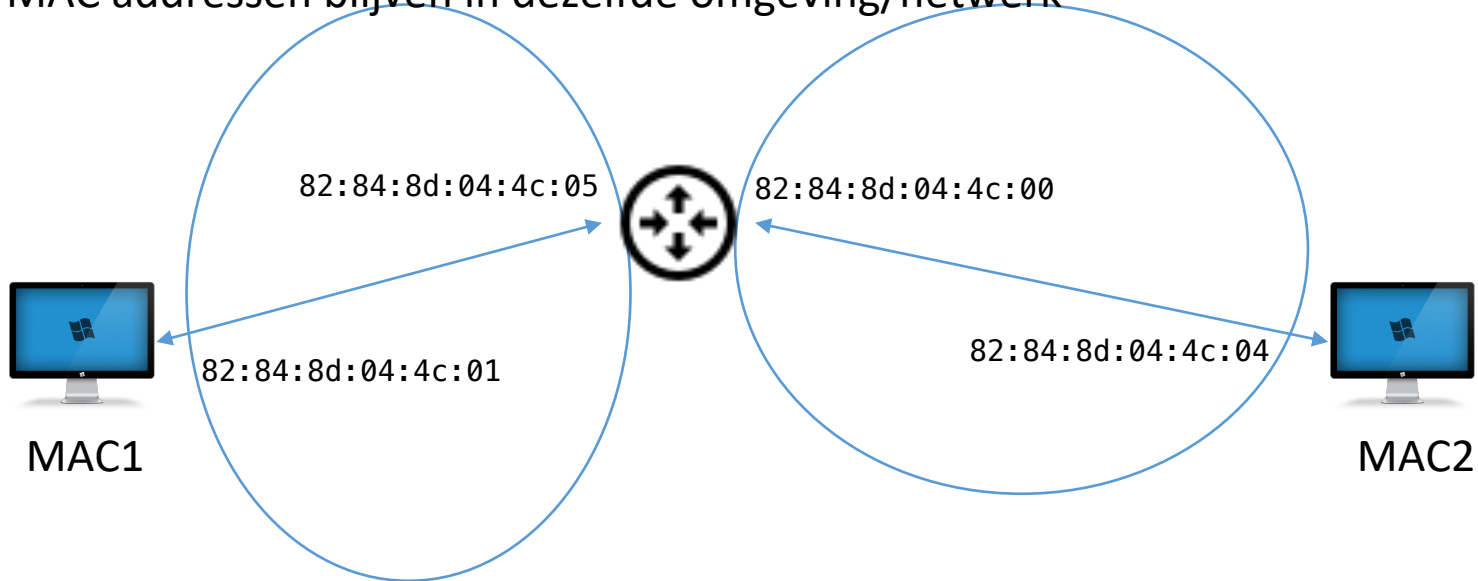
Data Link Layer – laag 2

- Logische adressen – op netwerk niveau (IP adressen)
- Fysieke adressen - op data link layer
 - Unieke MAC adressen (media access control)
 - Op network interfaces
 - Switch



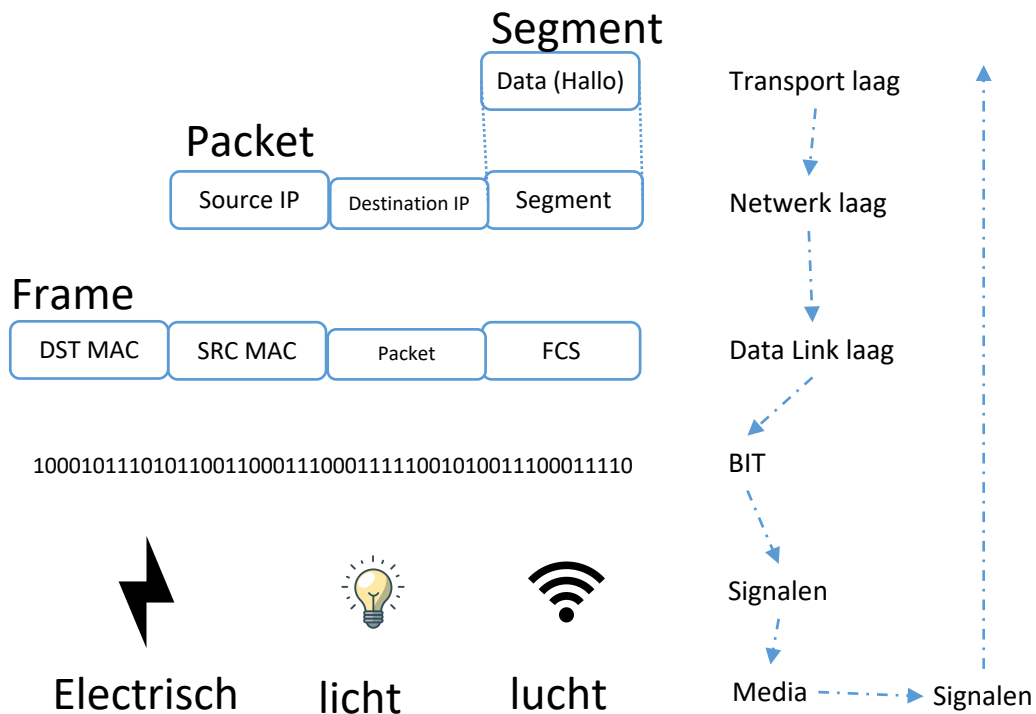
Data Link Layer – laag 2 (vervolg)

- MAC adressen blijven in dezelfde omgeving/netwerk



Fysieke – laag 1

- Communicatie verloopt over een fysieke transport
 - Koper (UTP kabel) - HUB
 - Licht (glasvezel)
 - Lucht (wireless – WiFi)

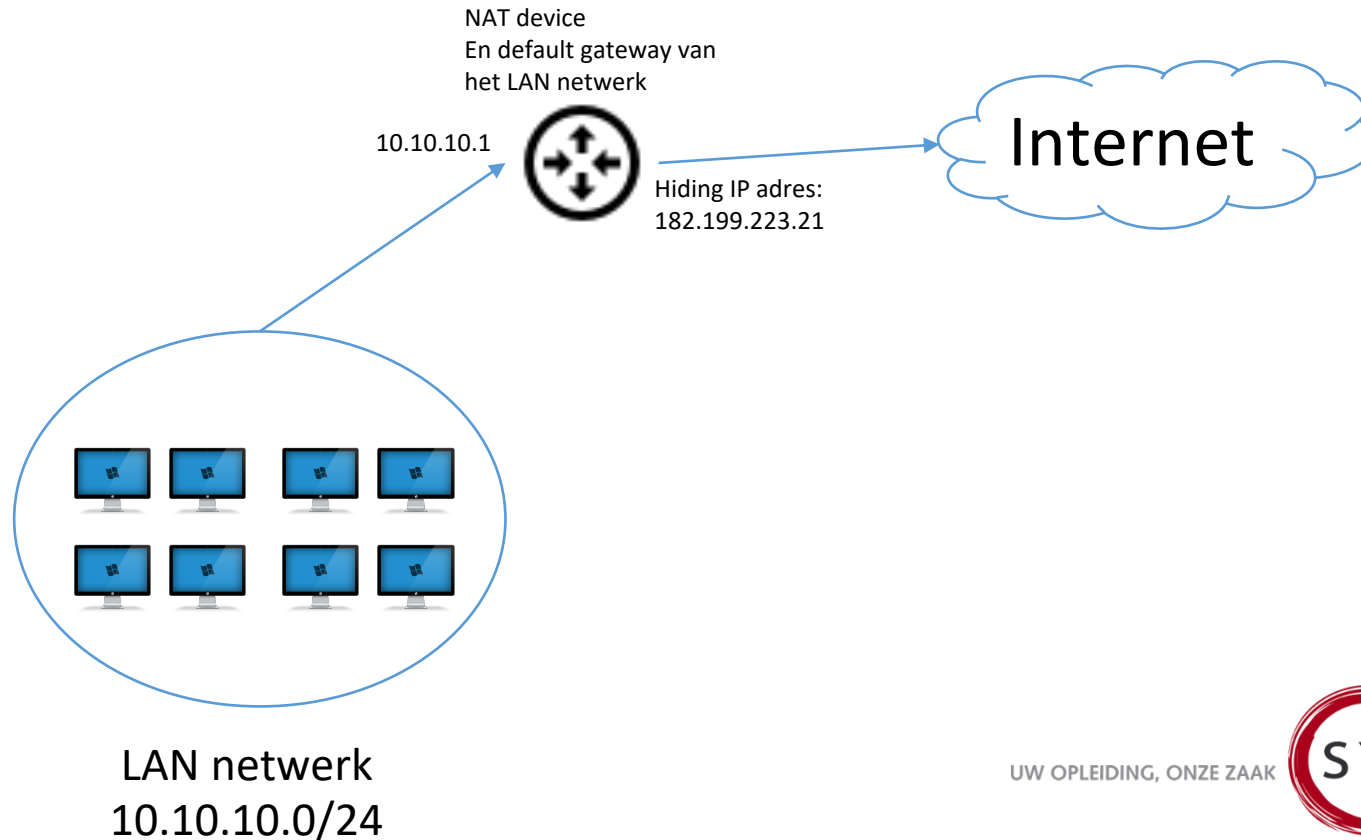


Natting

- Door het beperkte aantal IP adressen zijn er afspraken gemaakt om niet elk toestel te voorzien van een publiek IP adres (=IP adres dat op het internet voorkomt). Private IP adressen (RFC1918) (=IP adressen die gebruikt worden in LAN) worden gemaskeerd achter een publiek IP adres als ze het internet op moeten.
- Er zijn 3 verschillende soorten NAT methodes
 - Hide Nat
 - Port Forwarding
 - Static NAT

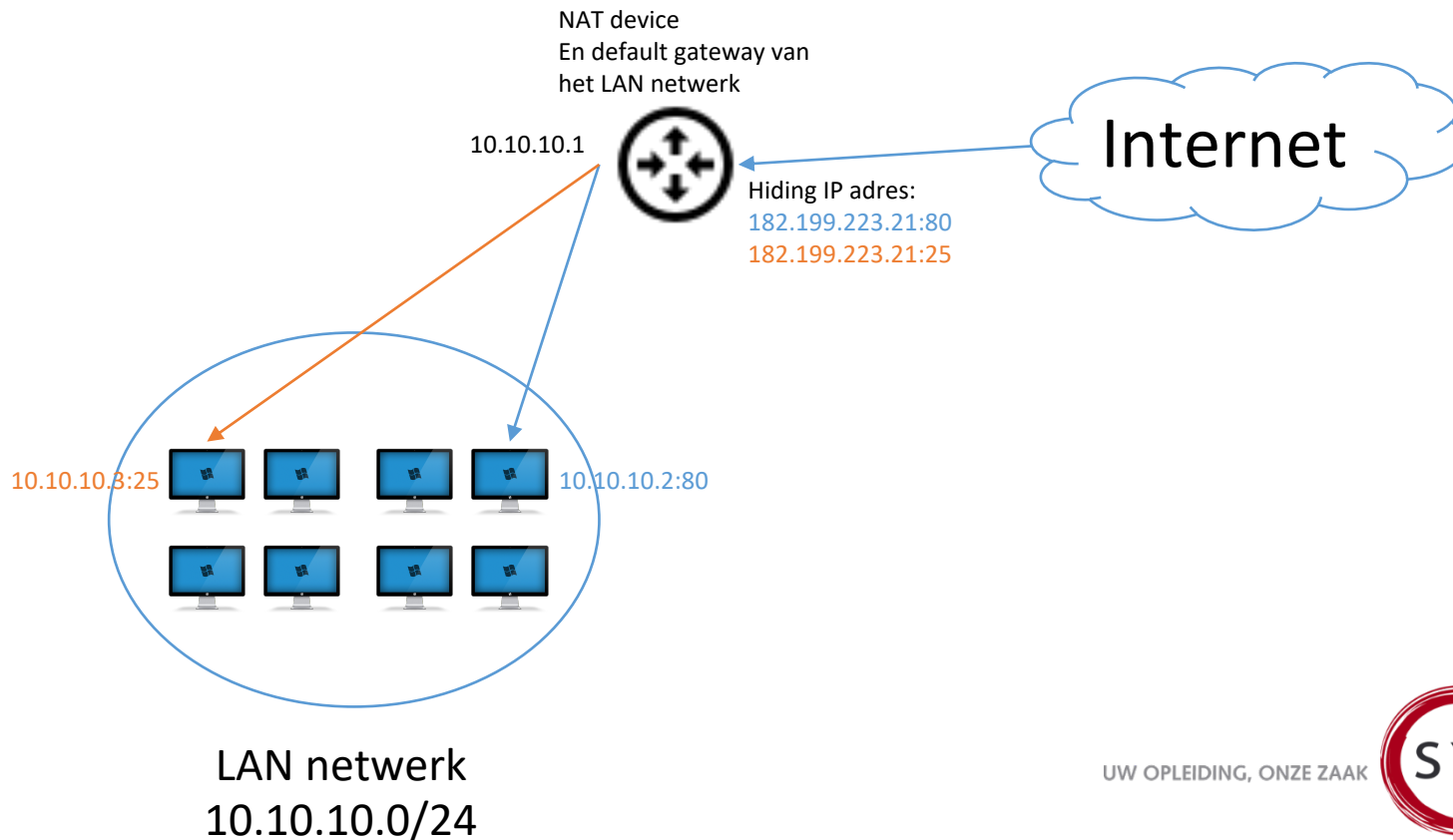
Hide NAT

- Hide NAT zorgt ervoor dat een volledig LAN netwerk vertaald wordt achter 1 of meerdere IP adressen wanneer deze het internet willen bereiken.



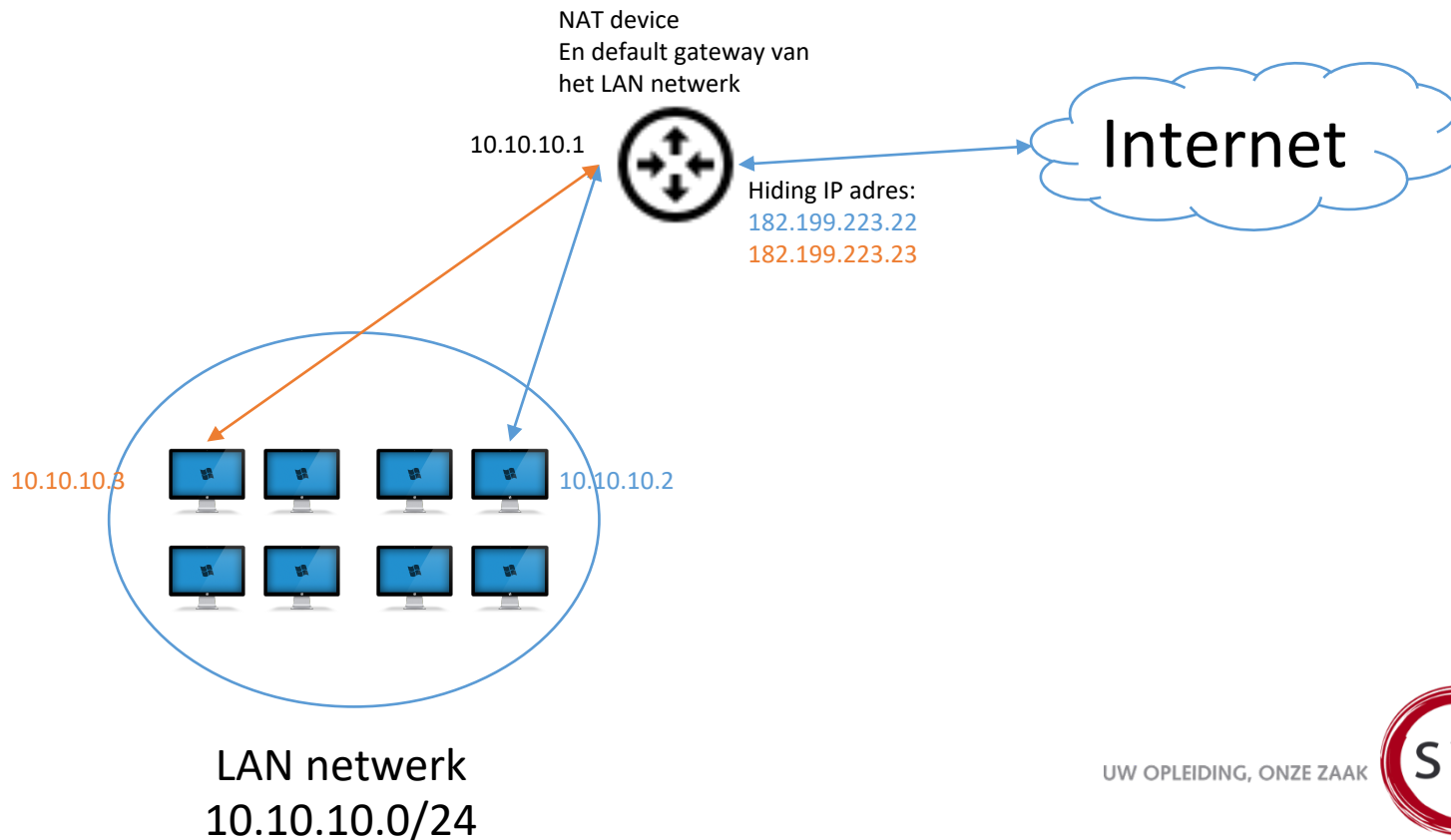
Port Forwarding

- Bij een port forward gaan we services bereikbaar maken vanuit het internet die in ons LAN netwerk zitten, we gebruiken 1 Publiek IP adres voor verschillende interne servers.



Static NAT of BINAT

- Voor elke interne server die we bereikbaar willen maken voor het internet gebruiken 1 publiek IP adres per service. Automatisch wordt dit adres gebruikt als hiding adres voor de server.

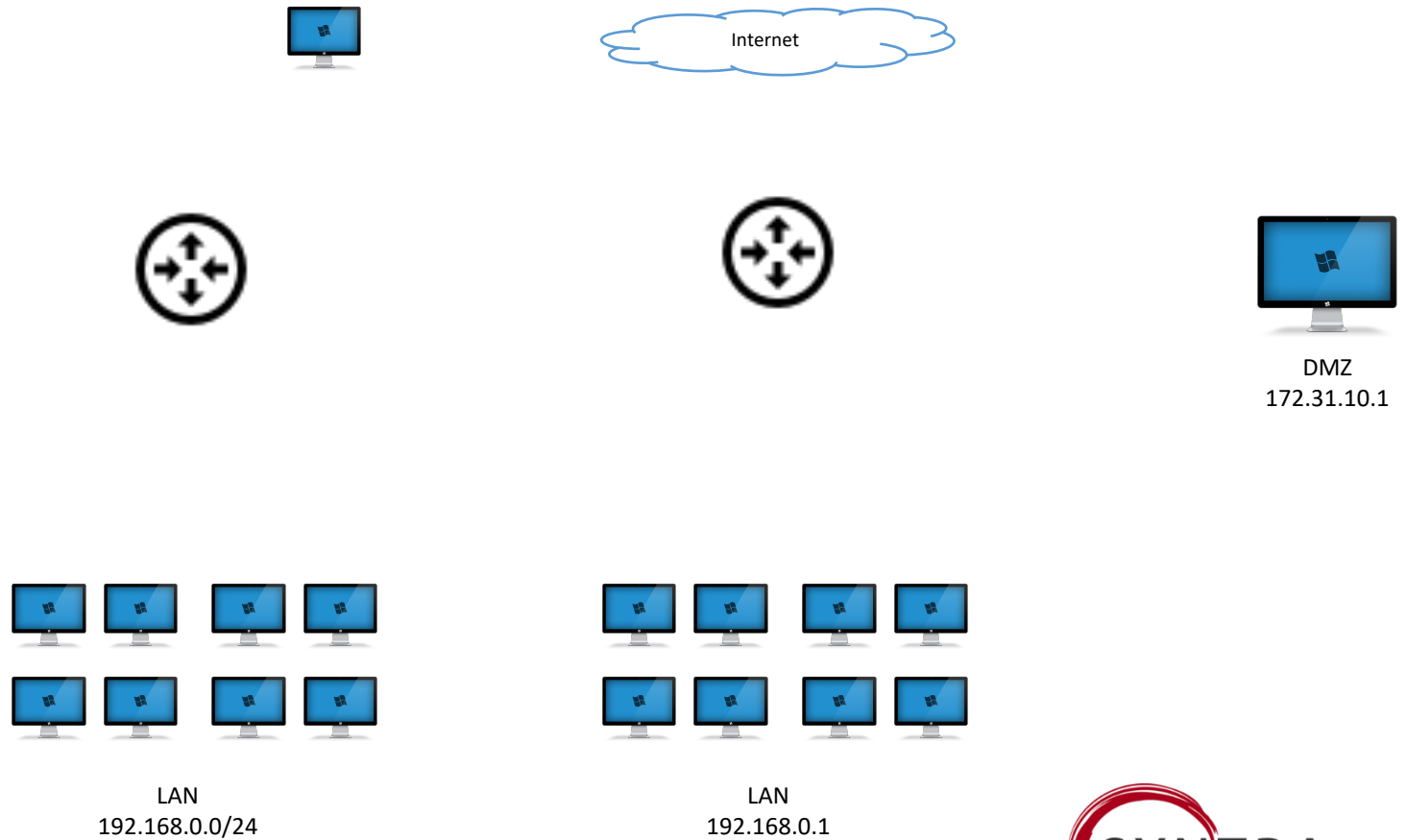


Netwerk architectuur

Concepten:

- LAN
- WAN
- DMZ
- VPN
 - Client
 - site2site
- LL
- Cloud
 - Hybrid cloud
 - Private cloud
 - Public cloud

Network on premise



VLAN Virtual Local Area Network

- Open Standaard 802.1Q
- Segmentatie = verschillende logische netwerken definiëren in één fysiek netwerk
- Beveiliging door poorten op de switch toe te kennen aan één vlan kan men nog beter segmenteren
- Kosten verlaging door fysiek minder switchen nodig te hebben om meerdere logische netwerken te maken
- Broadcast wordt beperkt per VLAN
- VLANs kunnen over verschillende switchen heel geconfigureerd worden
- TAG

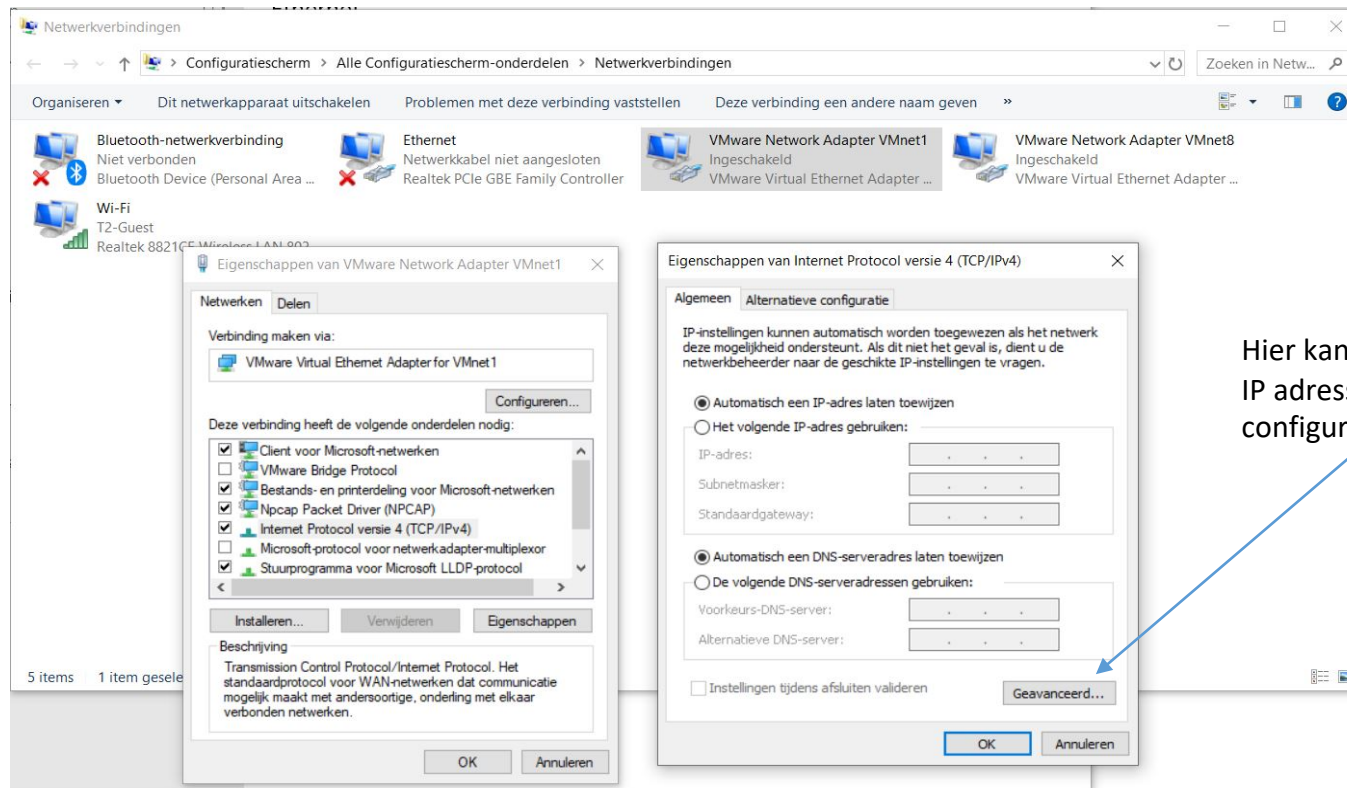


- Extra veld in de ethernet frames

- Bestaat uit 4 bytes en de belangrijkste byte is de VID of VLAN identifier of VLAN-ID
 - VID bestaat uit 12 bites dus 2^{12} of 4096
 - 0 en 4095 mogen niet gebruikt worden!!!

IP aliases als alternatief voor VLAN

- Op één fysieke interface meerdere IP adressen configureren
 - Kan zowel voor Linux/Windows/Apple/...
 - `ifconfig <interfacenaam>:1 IP adres`
 - `Ifconfig <interfacenaam> alias IP`



Hier kan je meerdere
IP adressen
configureren

Network commando's

- Windows via de command prompt (cmd)
 - ipconfig
 - Basis IP configuratie opvragen van de interfaces
 - Opties: die je kunt meegeven:
 - /all - geeft alle informatie over de interfaces zoals DNS servers, MAC adressen
 - /release – verwijderd het IP adres dat bekomen is van de DHCP server en vergeet ook alle informatie over die bepaalde DHCP server
 - /renew – vernieuwd het IP adres dat hij gekregen heeft van de DHCP server
 - |more – kan je gebruiken om een pagina per pagina print te krijgen van de output op het scherm van bovenstaande commando's
 - route print of netstat -rn
 - Print de huidige/active route table
 - route add
 - Met dit commando kan je manueel routes toevoegen
 - netstat -an
 - Hier zie je informatie over network connecties

Network commando's (vervolg)

- Linux via de terminal
 - ifconfig
 - Basis IP configuratie opvragen van de active interfaces
 - Opties: die je kunt meegeven:
 - -a - geeft informatie over alle interfaces ook de niet active interfaces
 - dhclient – vernieuwd het IP adres dat hij gekregen heeft van de DHCP server
 - route of netstat –rn - Print de huidige/active route table
 - -n optie gaat geen resolving proberen te doen van het IP adres
 - |more – kan je gebruiken om een pagina per pagina print te krijgen van de output op het scherm van bovenstaande commando's
 - route add
 - Met dit commando kan je manueel routes toevoegen
 - netstat –an
 - Hier zie je informatie over network connecties