

Basis Netwerkconfiguratie

Ing. Tijl Deneut
Lector Toegepaste Informatica/NMCT Howest
Onderzoeker XiaK, UGent



Overzicht Cursus (1 dag)

Voormiddag

- Theorie TCP/IP
 - Hardware / bekabeling
 - TCP/IP model
 - MAC adressen
 - IP adressen
 - Netmaskers
 - Netwerken, routers (ARP)
 - TCP & UDP Poorten

Overzicht Cursus (1 dag)

Namiddag

- Hands-on met Packet Tracer + demo's
 - DNS
 - DHCP
 - Basis Firewall
 - NAT & PAT
 - VLAN

Industrial Ethernet

Kantooromgeving

- Vaste basisinstallatie in het gebouw
- Variabele netwerkverbinding voor werkstations
- Kabels liggen in valse vloeren
- Wireless netwerk
- Standaard werkstations op RJ45
- Voeding van 230V AC
- Stertopologie
- 19" schakelkasten (standaardafmeting serverkasten)
- Levensduur ongeveer 5 jaar
- Toestellen met actieve koeling (ventilatoren)

Industriële omgeving

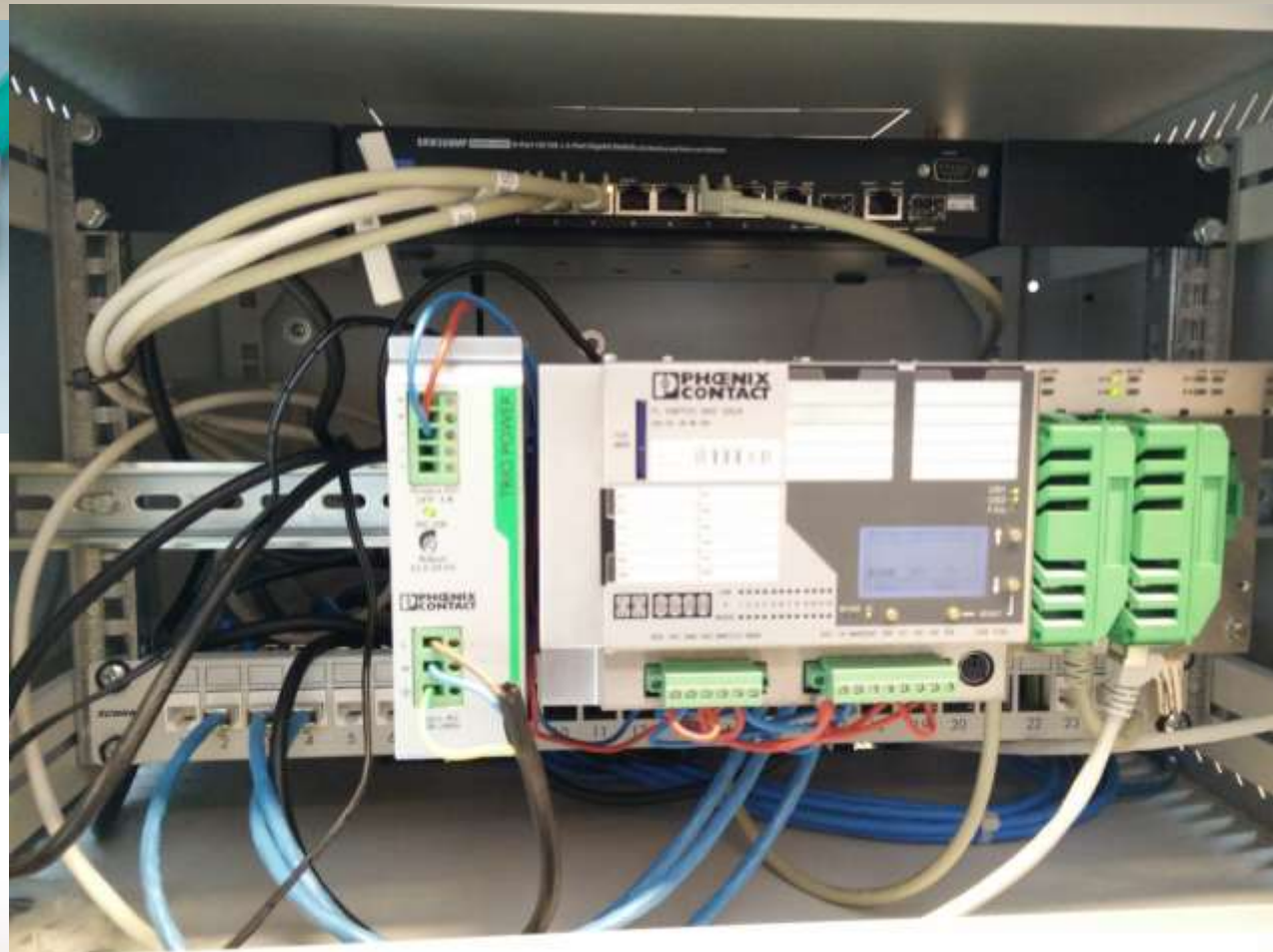
- Systeem-specifieke toepassingen
- Verbindingspunten met het netwerk worden zelden tot nooit gewijzigd
- Connectoren die op de werkvloer geassembleerd kunnen worden
- RJ45 in de kasten, M12 in het veld
- Regelmatig gebruik van fiber optics
- Bekabeling bestemd voor gebruik in beweegbare kabelgeleiders
- Zorgvuldig geïmplementeerde aardingen
- Voeding met 24V DC of Power over Ethernet
- Regelmatig gebruik van lijntopologie of ringtopologie
- Redundantie is vaak een vereiste
- Levensduur van ongeveer 10 jaar
- Terminals geschikt voor montage op een DIN rail
- Passieve koeling (geen bewegende onderdelen)
- Alarm contact voor error indicatie

Industrial Ethernet



RJ45 VS M12

19" rack =>



Industrial Ethernet

Omgevingsinvloeden

Kantooromgeving

- Gematigde temperaturen met lage fluctuaties
- Bijna geen stof
- Geen vochtigheid of water
- Bijna geen schokken of trillingen
- Laag niveau van EMC
- Lage mechanische belasting of gevaar
- Geen chemische risico's
- Geen stralingsgevaren

Industriële omgeving

- Extreme temperaturen met hoge fluctuaties
- Hoge hoeveelheden stof
- Vocht of water kan aanwezig zijn
- Vibraties of schokken mogelijk
- Hoog niveau van EMC
- Hoog mechanische belasting of gevaar
- Chemische belasting door olieachtige omgevingen of agressieve atmosferen
- Hoge blootstelling aan UV stralingen in outdoor omgevingen

Bekabeling voor Ethernet & PROFINET

Bekabelingsconcepten van de kantooromgeving kunnen niet onbeperkt in ruwe industriële omgevingen worden toegepast

Aandachtspunten:

- EMC afscherming
- Robuuste opbouw (schok en trilling bestendig)
- IP67
- Eenvoudige en betrouwbare aansluittechniek

Fysieke Bekabeling



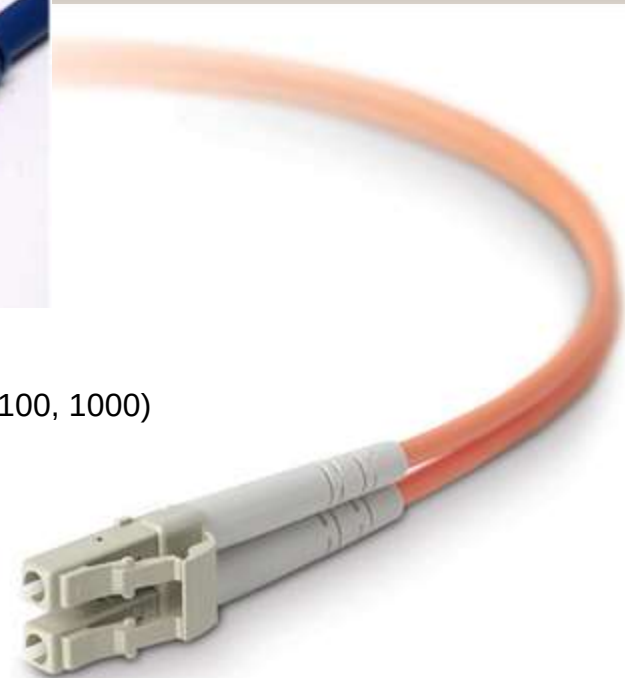
UTP, Netwerk, RJ45

Meest gebruikt voor *horizontale* bekabeling (10, 100, 1000)



Coax

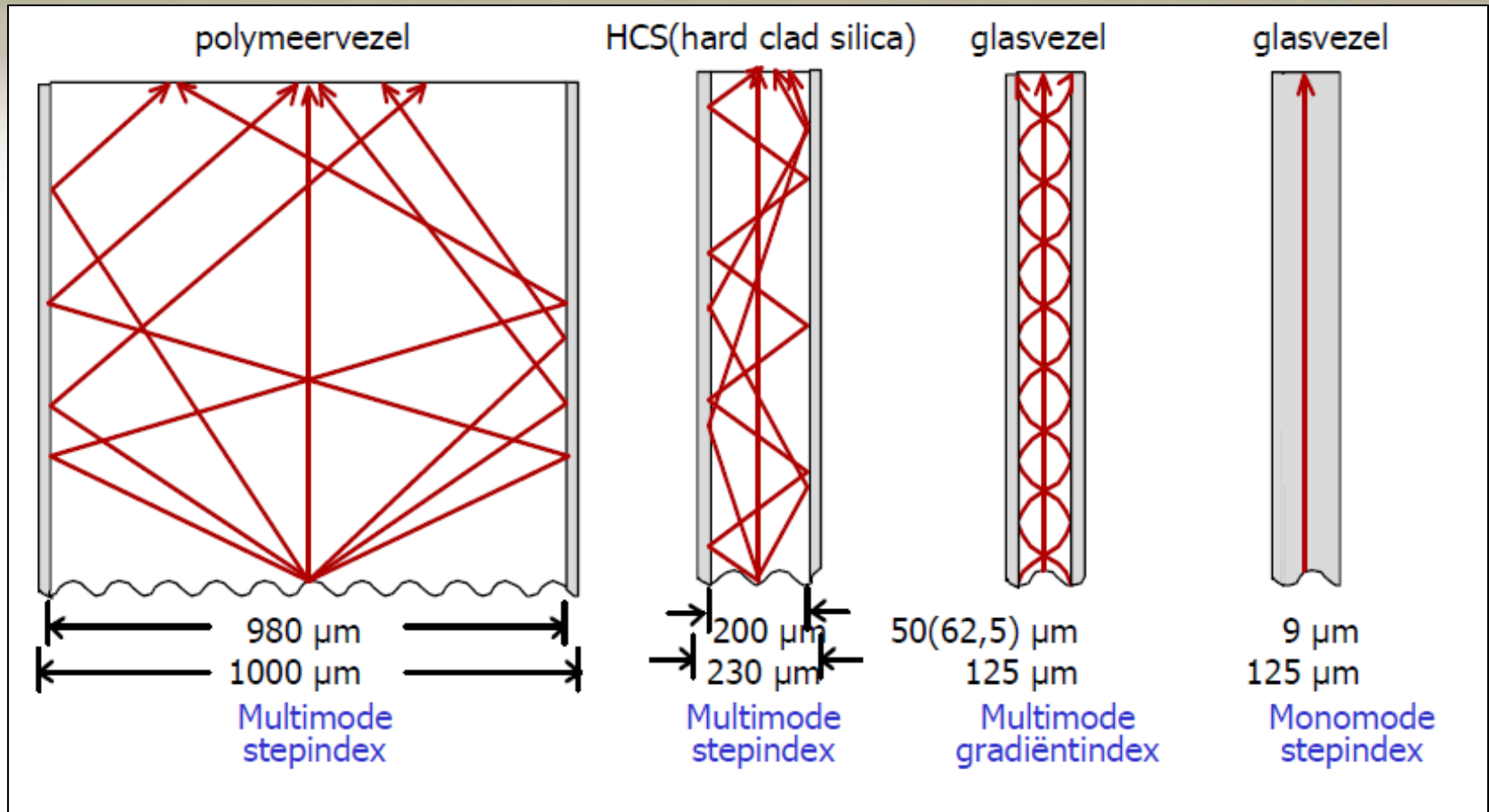
Voor netwerk in onbruik, max. 10Mbit TCP/IP



Fiber, Glasvezel

Meest gebruikt voor *verticale* bekabeling (lichtsnelheid)

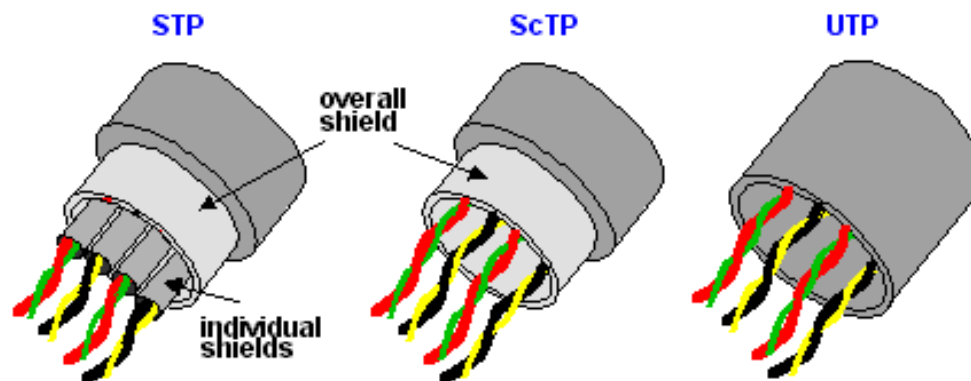
Glasvezeltypes



Netwerkkabels

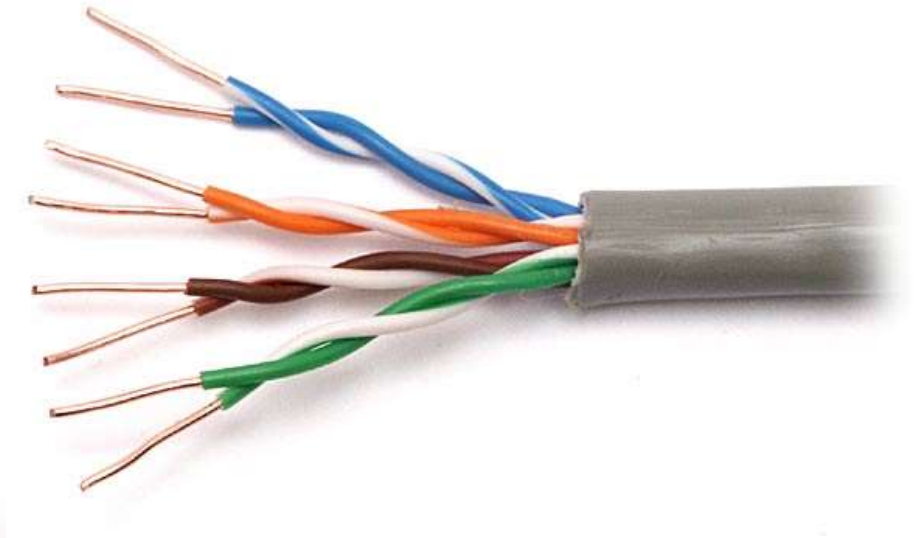
Veel verschillende soorten netwerkkabels

- UTP: Unshielded Twisted Pair
- STP: Shielded Twisted Pair (Also Screened ~)
- FTP: Foiled Twisted Pair



Twisted Pairs

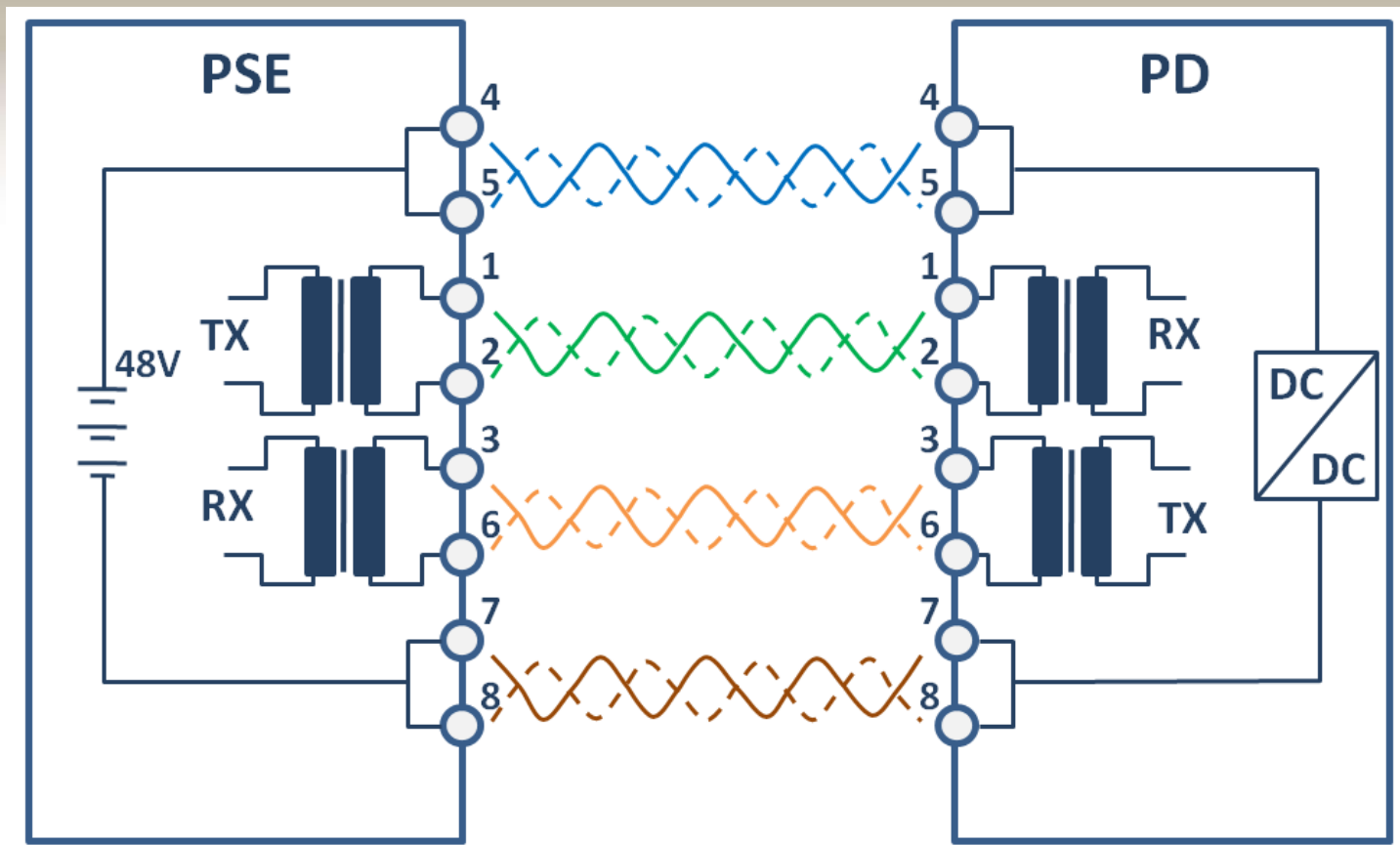
- Netwerkkabels bevatten altijd 4 paar koperen aders
 - Telkens per paar rond elkaar gedraaid, vol kleur en gestreept
 - De idee is dat externe invloeden per paar gelijk zijn
- Voor 100Mbit snelheid worden slechts 2 paar gebruikt: oranje en groen



Netwerkkabels Categorieën

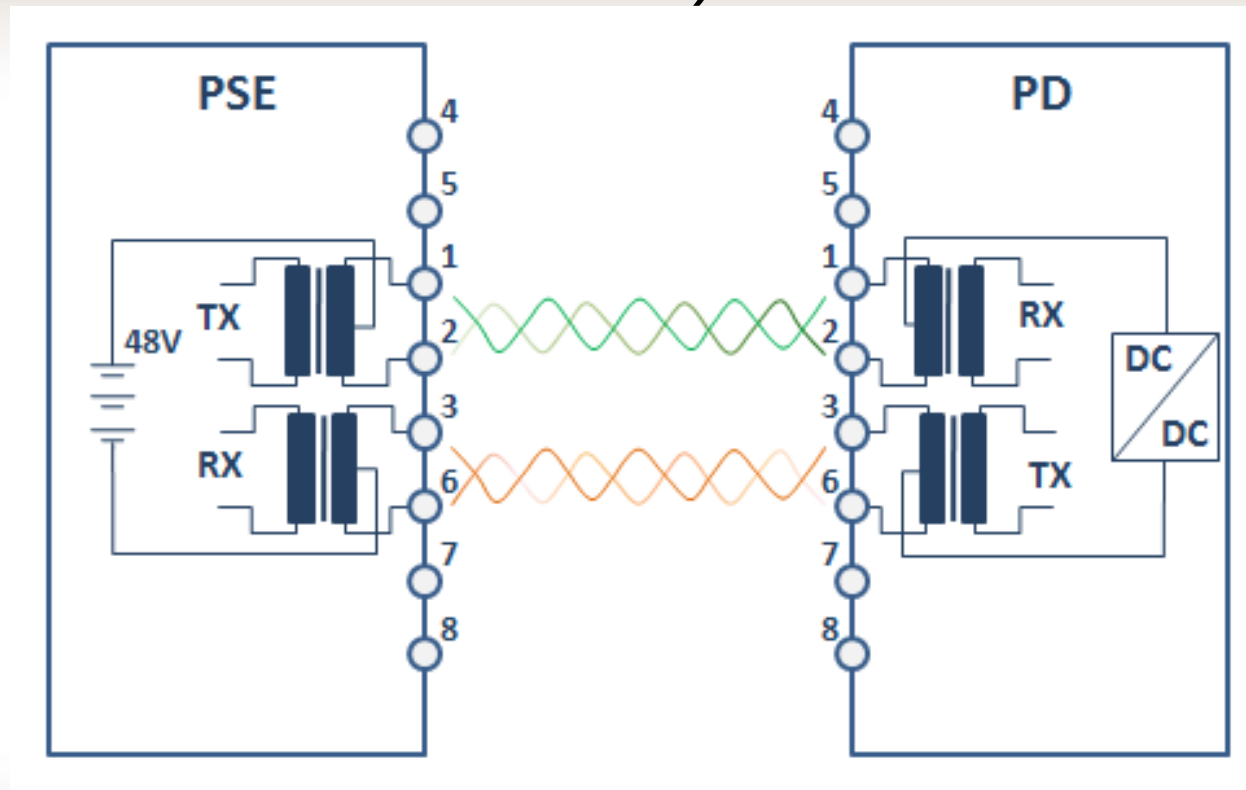
Characteristics	CAT 5e	CAT 6	CAT 7
Max bandwidth	100 Mb (Fast) 1000 Mb (Gigabit)	1000 Mb (Gigabit) 10000 Mb (10-Gigabit)	1000 Mb (Gigabit) 10000 Mb (10-Gigabit)
Min Number of Twisted Pairs	4	8	4
Max Number of Twisted Pairs	100	8	8
Max Speed	100 MHz	250 MHz 500 MHz	600 MHz / 1000 MHz
Max Length	100M	100M (Gigabit) 55M (10-Gigabit)	100M
Max Operating Temperature	60 C	60 C - 75 C	60 C
Min Operating Temperature	- 55 C	- 20 C	- 30 C
Max Operating Voltage	125 DC	300 DC	72 DC
Max Current Per Conductor	0.577 A	0.42 A	1.5 A
Shielding	Optional	Optional	Required as Standard
Primary Use	Ethernet / Data	Ethernet / Data	Telecomms / Data

PoE, Power over Ethernet



PoE, alternatieve configuratie

Met deze oplossing zijn toch 4 paren bruikbaar
(en dus 1000Mbit snelheden)



Ethernet standaarden

Alles wat met Ethernet te maken heeft en moet gestandaardiseerd worden, moet langsgaan bij de IEEE:

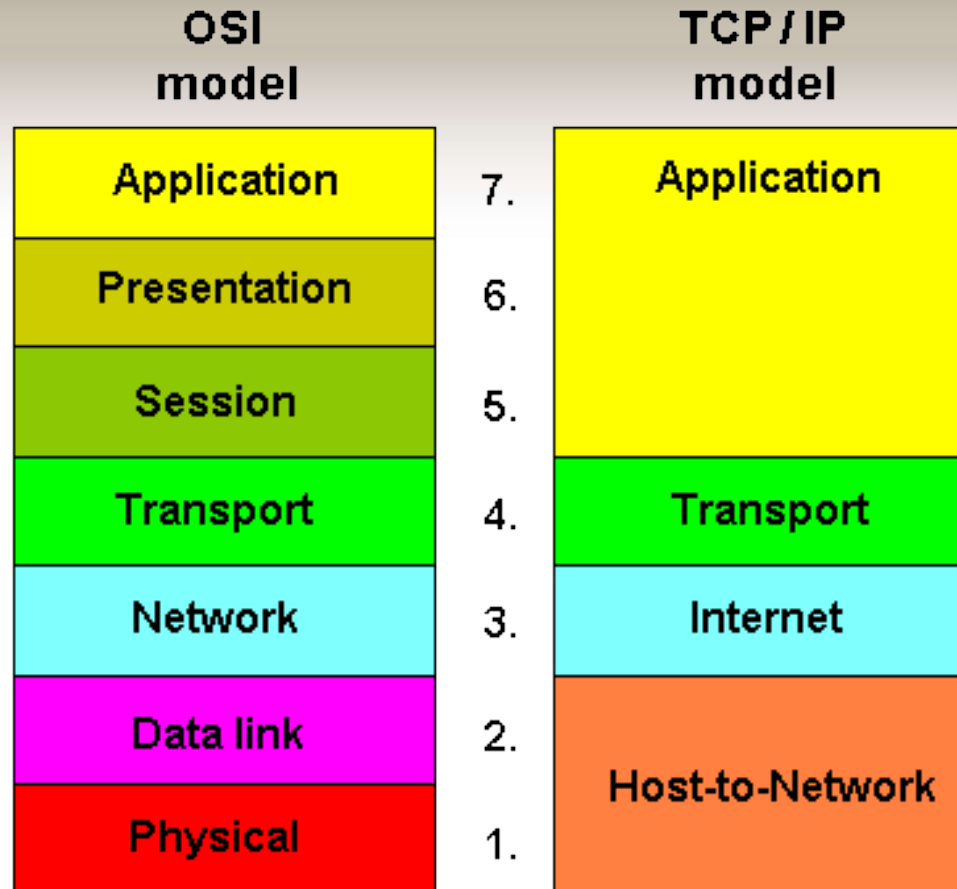
Institute of Electrical and Electronics Engineers

- PoE standaard IEEE 802.3 (bijv. 802.3af)
- WLAN standaard IEEE 802.11 (bijv. 802.11g)
- VLAN standaard IEEE 802.1Q
- LLDP standaard IEEE 802.1AB
- Link Aggregation standaard IEEE 802.AX

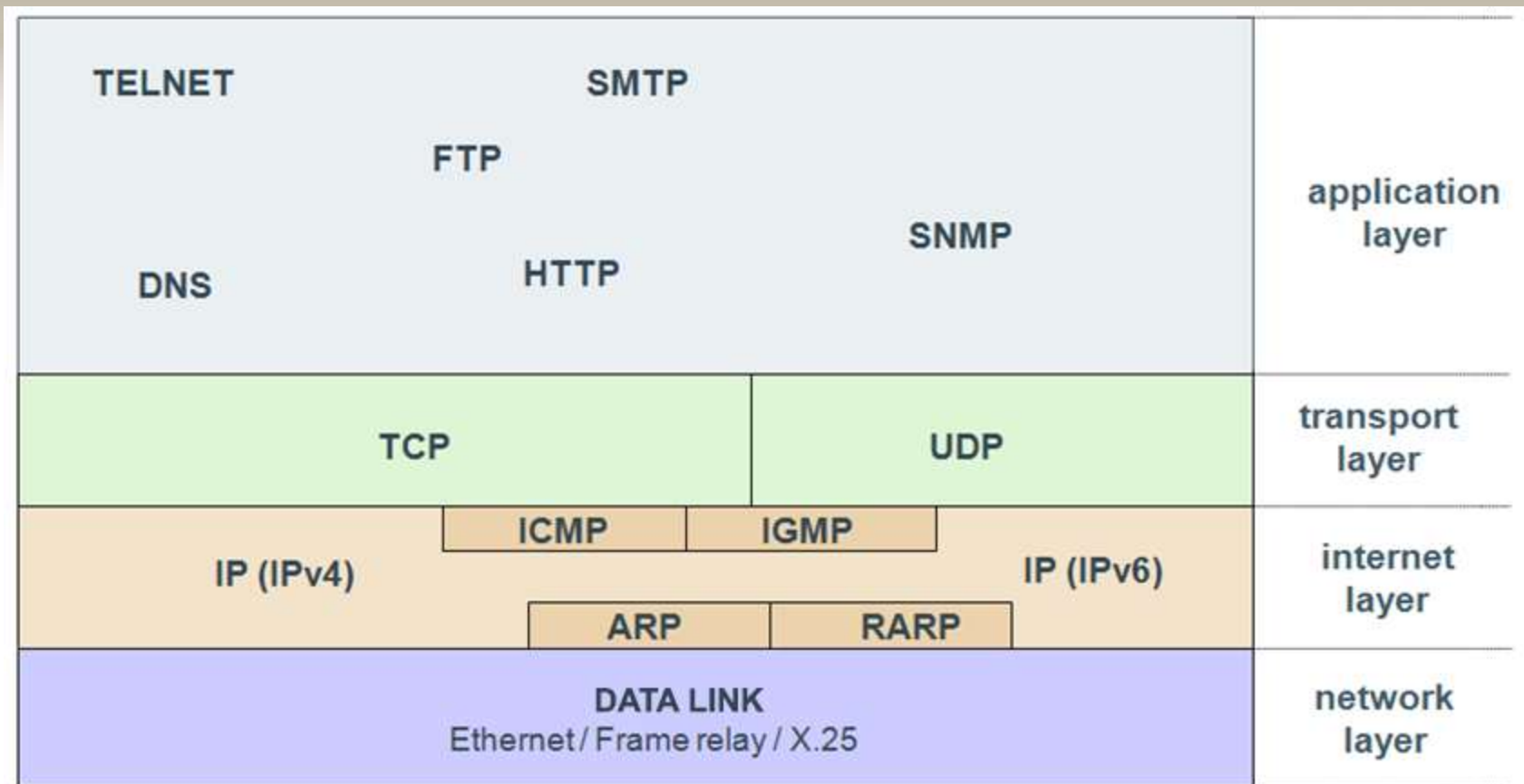
Tussenpresentatie

De Heer Thibaut Demasure

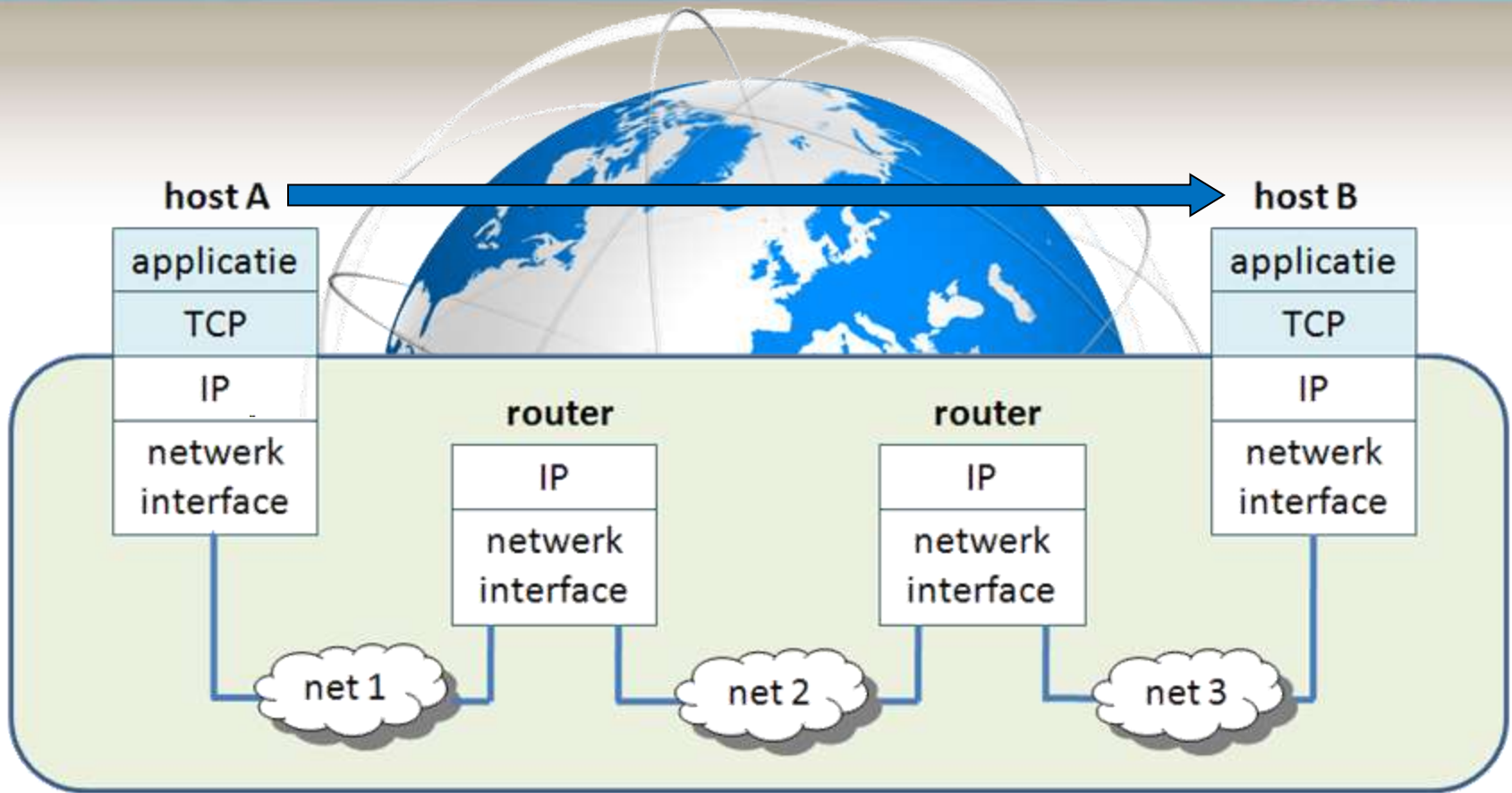
Lagen modellen



TCP/IP model



TCP/IP “stack”



Pakket opbouw, van onderen

1010 1011 1000 0100 1101 0101 1110 0101 1110

Ethernet dataframe



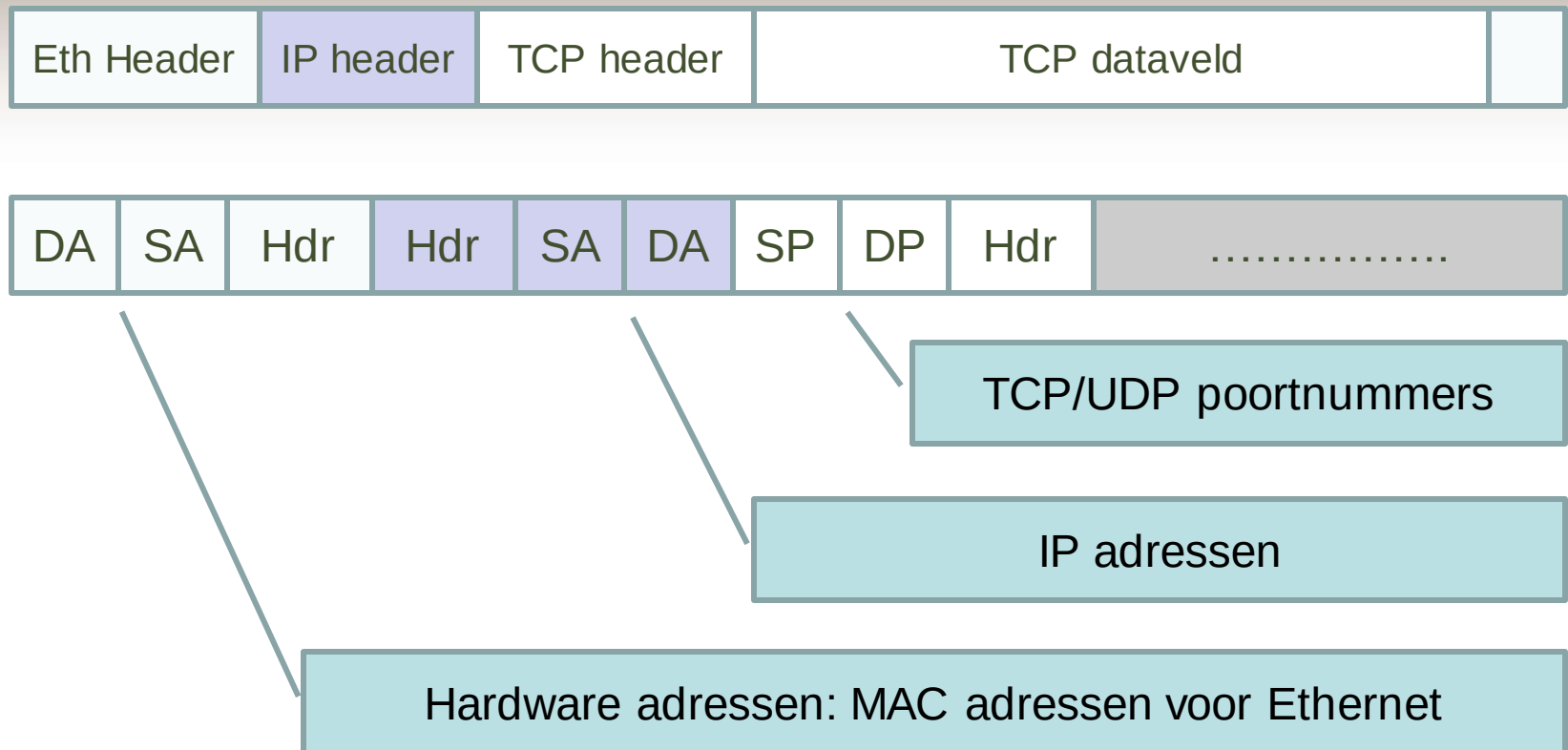
IP Pakket



TCP segment



TCP/IP Berichtopbouw

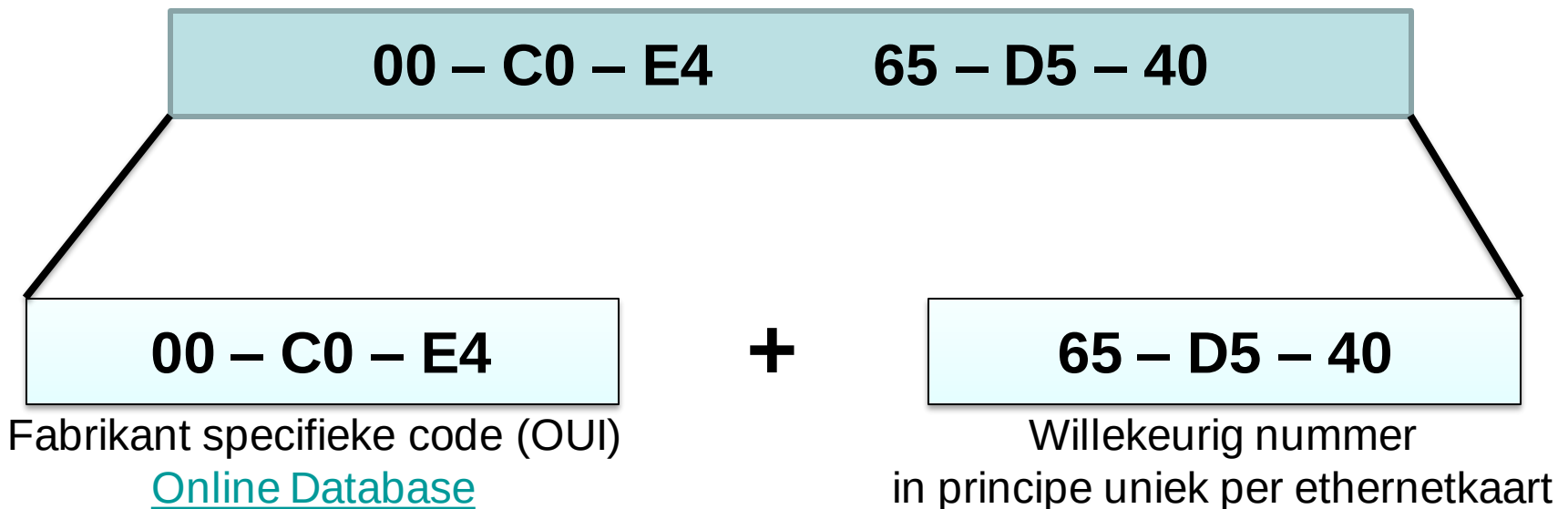


Ethernet: MAC adressen

Netwerk laag, hardware adressering

Bijv.: 20:16:D8:A0:02:DB

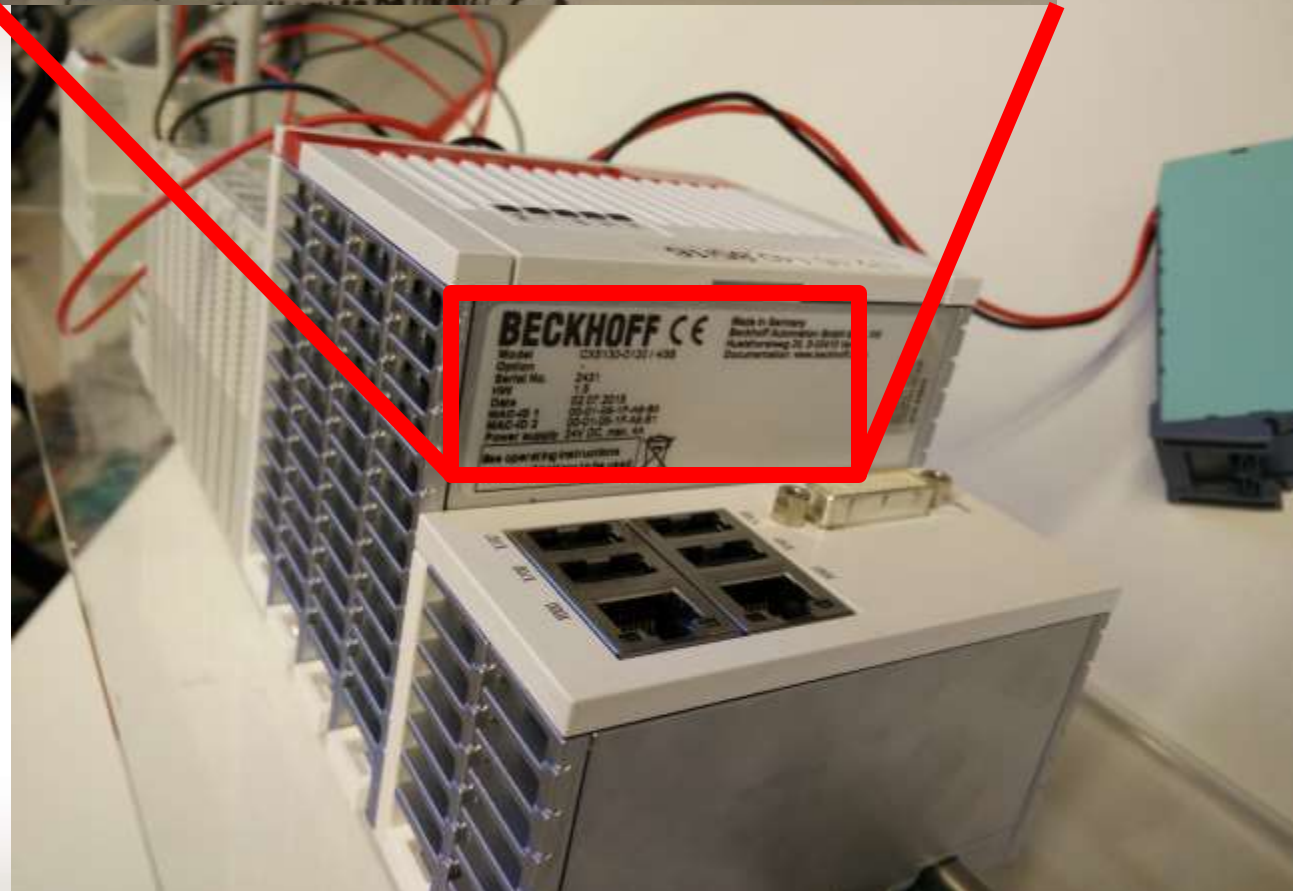
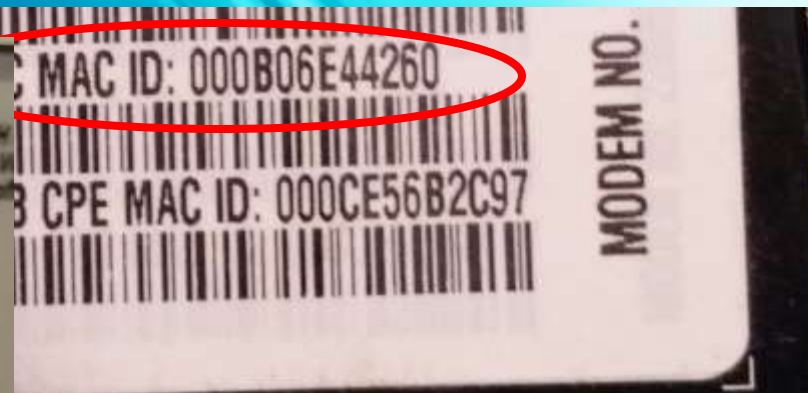
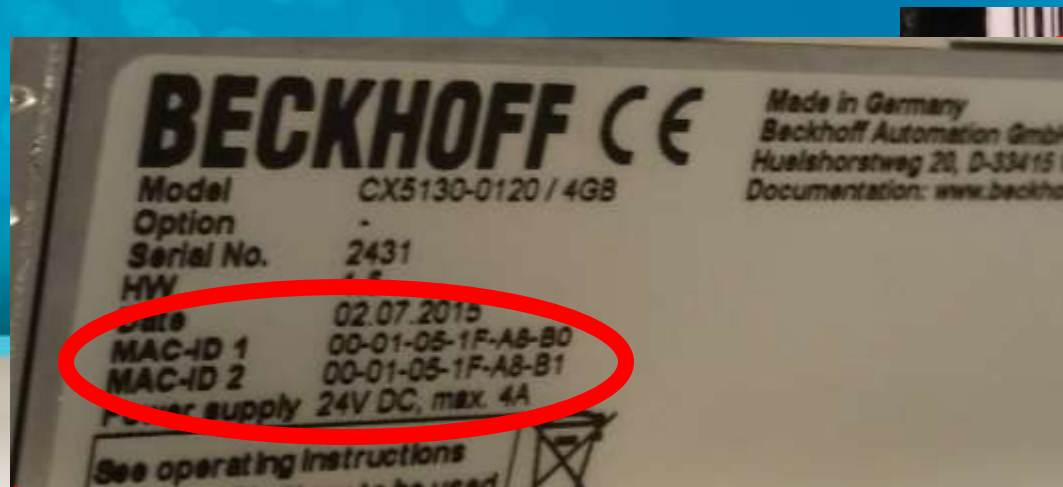
MAC adres: 48 bits, op ROM van de Ethernetkaart



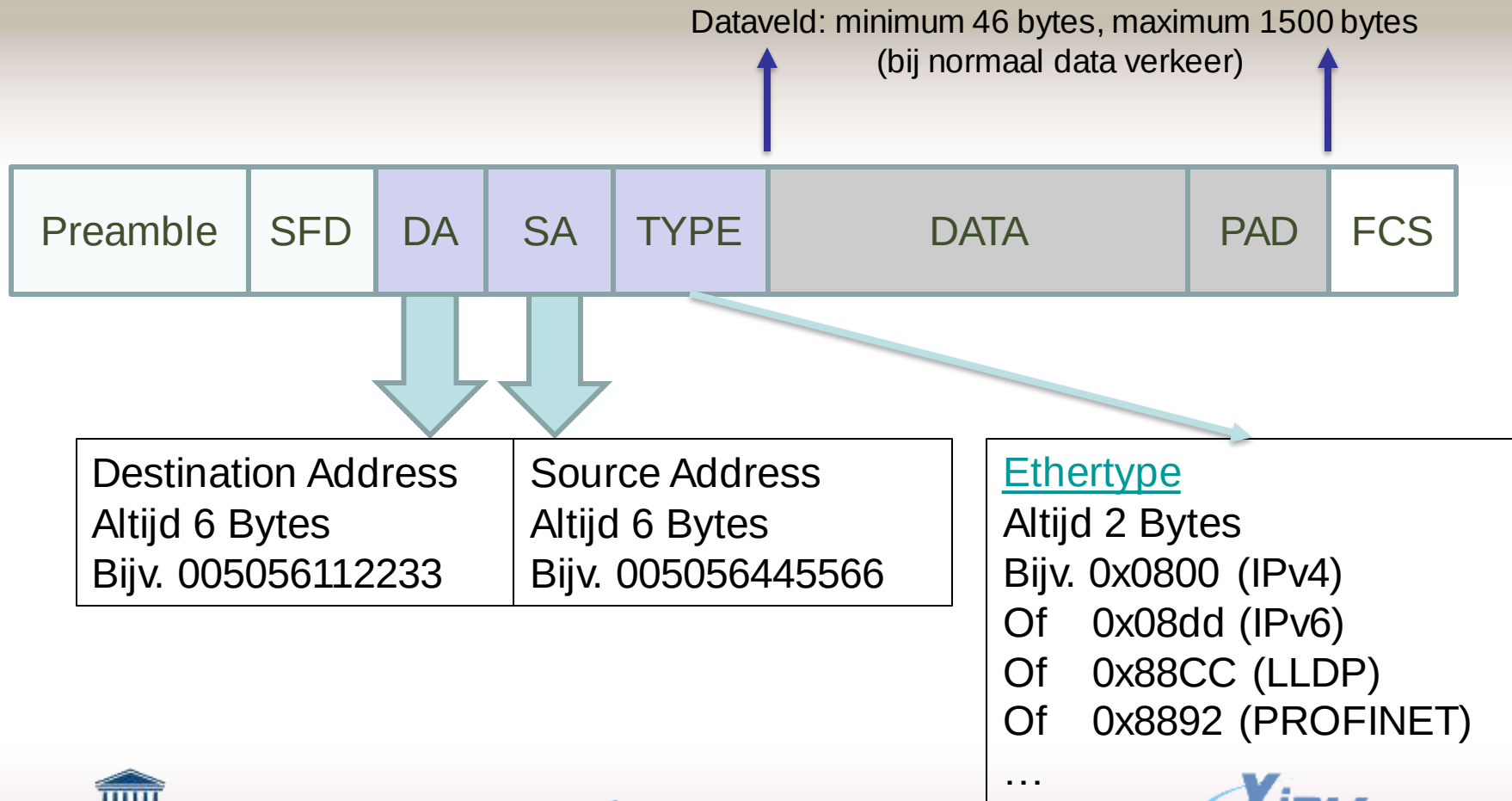
MAC a.k.a. ethernet adres

Dit is het **Hardware Adres**: uniek voor elk netwerkkapparaat (dat de IEEE standaarden volgt).

- Elke netwerkpoort **die eigen verkeer genereert** dient minimaal 1 MAC adres te hebben.
- Is meestal zichtbaar via **een sticker** op het toestel
- En uiteraard ook altijd terug te vinden via de software
- Laat communicatie toe op zeer rudimentair en laag niveau
- Speciale gevallen: multicast en broadcast adressen
 - Bijv. FF:FF:FF:FF:FF:FF is een broadcast adres, frames gaan naar **alle** toestellen
 - Of het 01:0E:CF:00:00:00 PROFINET multicast adres, frames gaan naar **alle** Profinet toestellen



Ethernet Dataframe



Voorbeeld: mini-netwerk

005056b6feb6 2863368ad256 8892

feff

05010400000300000050020500040000020702010009000053372d3
1323030000202000a0000706c632d74696a6c020300060000002a010
d020400040000020002070004000000640102000e0001ac10021efff0
000ac10021e



00:50:56:b6:fe:b6



28:63:36:8a:d2:56



De switch

- Regelt verkeer **binnen één netwerk**
- Onthoudt MAC adressen uit de berichten (SA)
- Slaat deze op in de MAC tabel (a.k.a. CAM tabel)
- Eenvoudige netwerkuitbreiding

Mac Address Table

No.	Mac Address	Port
1	00:A0:45:04:1F:12	6
2	00:50:56:B6:E0:C4	6
3	D0:67:E5:51:AA:16	6
4	00:50:56:B6:66:CB	7
5	00:0E:8C:F3:FE:71	7
6	00:50:56:B6:CE:AF	7
7	24:77:03:88:BF:00	7
8	00:0C:29:1C:DA:21	7



Managed VS Unmanaged

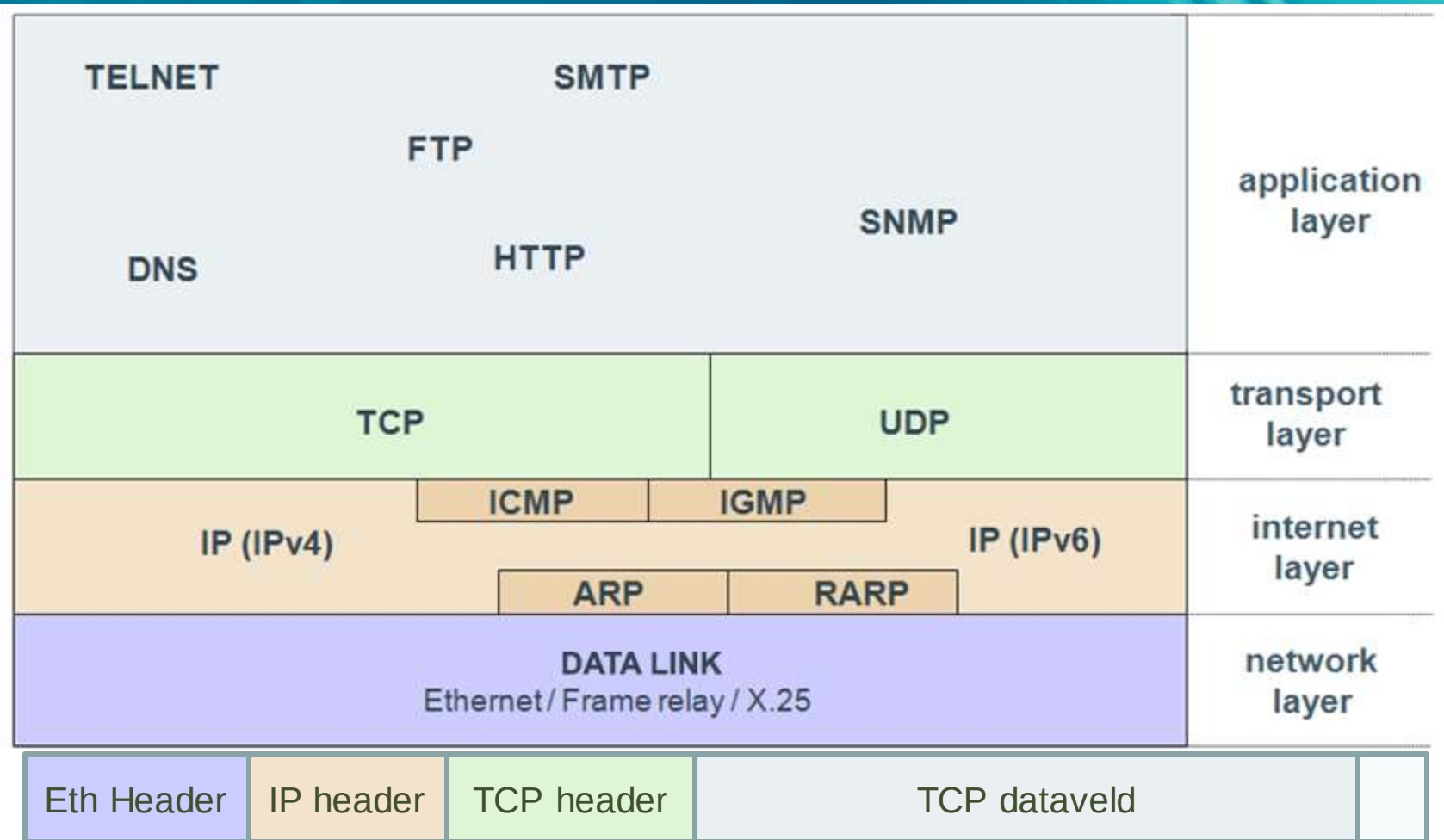
Unmanaged switches

- Plug & Play, geen bijkomende features
- Compacte industriële standaard switches
- “Goedkoop”

Managed switches

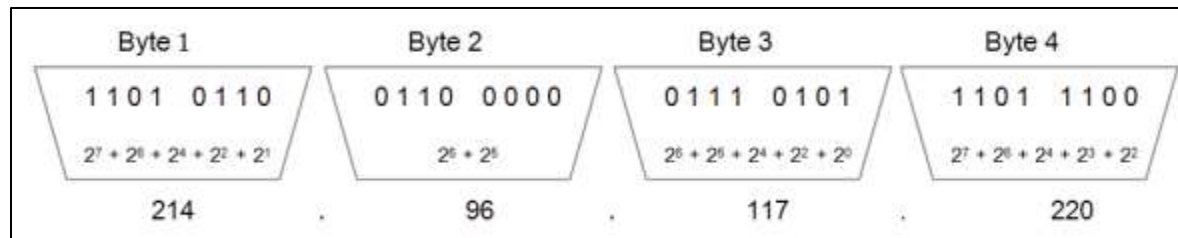
- (Webbased) configureerbaar, inclusief diagnose (monitoring)
- Ondersteuning van # features (redundantie, VLAN ...)
- Doorgaans grotere MAC tables (performanter)

Volgende Laag

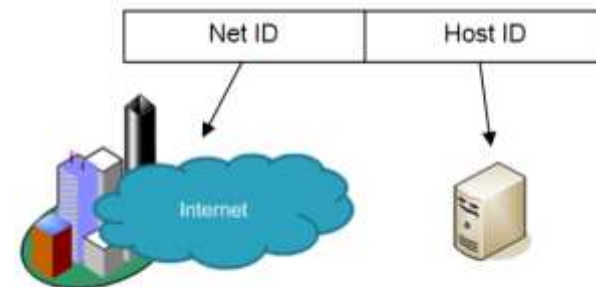


IPv4 adressen

- 32bit getal dat aan een netwerk interface wordt toegekend
 - Bijv. 11010110011000000111010111011100
- Echter meestal geschreven in *dotted-decimal* notatie
 - Bijv. 214.96.117.220



- Bestaat uit twee delen
 - Net ID bepaalt het netwerk,
elk toestel heeft dezelfde Net ID
 - Host ID is uniek
binnen het netwerk



Netwerk aanduiding: NetMask

- Hoe weet een toestel tot wat voor netwerk hij behoort?
 - D.m.v. het subnetmasker: bijv. 255.255.0.0

CIDR code	subnetmask	binair	aantal hosts
/28	255.255.255.240	11111111 11111111 11111111 11110000	16
/27	255.255.255.224	11111111 11111111 11111111 11100000	32
/26	255.255.255.192	11111111 11111111 11111111 11000000	64
/25	255.255.255.128	11111111 11111111 11111111 10000000	128
/24	255.255.255.0	11111111 11111111 11111111 00000000	256
/23	255.255.254.0	11111111 11111111 11111110 00000000	512
/22	255.255.252.0	11111111 11111111 11111100 00000000	1024
/21	255.255.248.0	11111111 11111111 11111000 00000000	2048
/20	255.255.240.0	11111111 11111111 11110000 00000000	4096
/19	255.255.224.0	11111111 11111111 11100000 00000000	8192
/18	255.255.192.0	11111111 11111111 11000000 00000000	16384
/17	255.255.128.0	11111111 11111111 10000000 00000000	32768
/16	255.255.0.0	11111111 11111111 00000000 00000000	65536
/15	255.254.0.0	11111111 11111110 00000000 00000000	131072
/14	255.252.0.0	11111111 11111100 00000000 00000000	262144
/13	255.248.0.0	11111111 11111000 00000000 00000000	524288

Gebruik subnetmasker

- Het subnetmasker wordt gebruikt om te bepalen of twee verschillende IP-adressen bij hetzelfde netwerk te horen.
- **Dit gebeurt door een AND-operatie uit te voeren op het IP-adres en het subnetmasker.**
- Op deze manier kan een host weten of hij een te versturen pakket al dan niet rechtstreeks kan afleveren aan een andere host (zelfde netwerk) of dat hij via een router moet werken (ander netwerk, zie later).
- Voorbeeld:

```
192.168.29.50/24 == 192.168.29.50 met subnetmasker 255.255.255.0

192.168.29.50 = 10000000.00000000.00000001.00110010
255.255.255.0 = 11111111.11111111.11111110.00000000
BINAIR AND -----
                10000000.00000000.00000000.00000000
== 192.168.29.0
```

Netwerk afbakening

- Elk netwerk heeft een begin en einde, wat kan berekend worden uit een willekeurig IP en zijn subnetmasker:
 - Bijv. IPv4 adres 192.168.1.3 /24 oftewel 192.168.1.3 met subnetmasker 255.255.255.0
 - Eerste mogelijke IP behorend tot dit netwerk is dan 192.168.1.1 en het laatste 192.168.1.254

Network ID			Host ID
11000000	10101000	00000001	00000011
192	.	168	. 1 . 3
32 Bits			

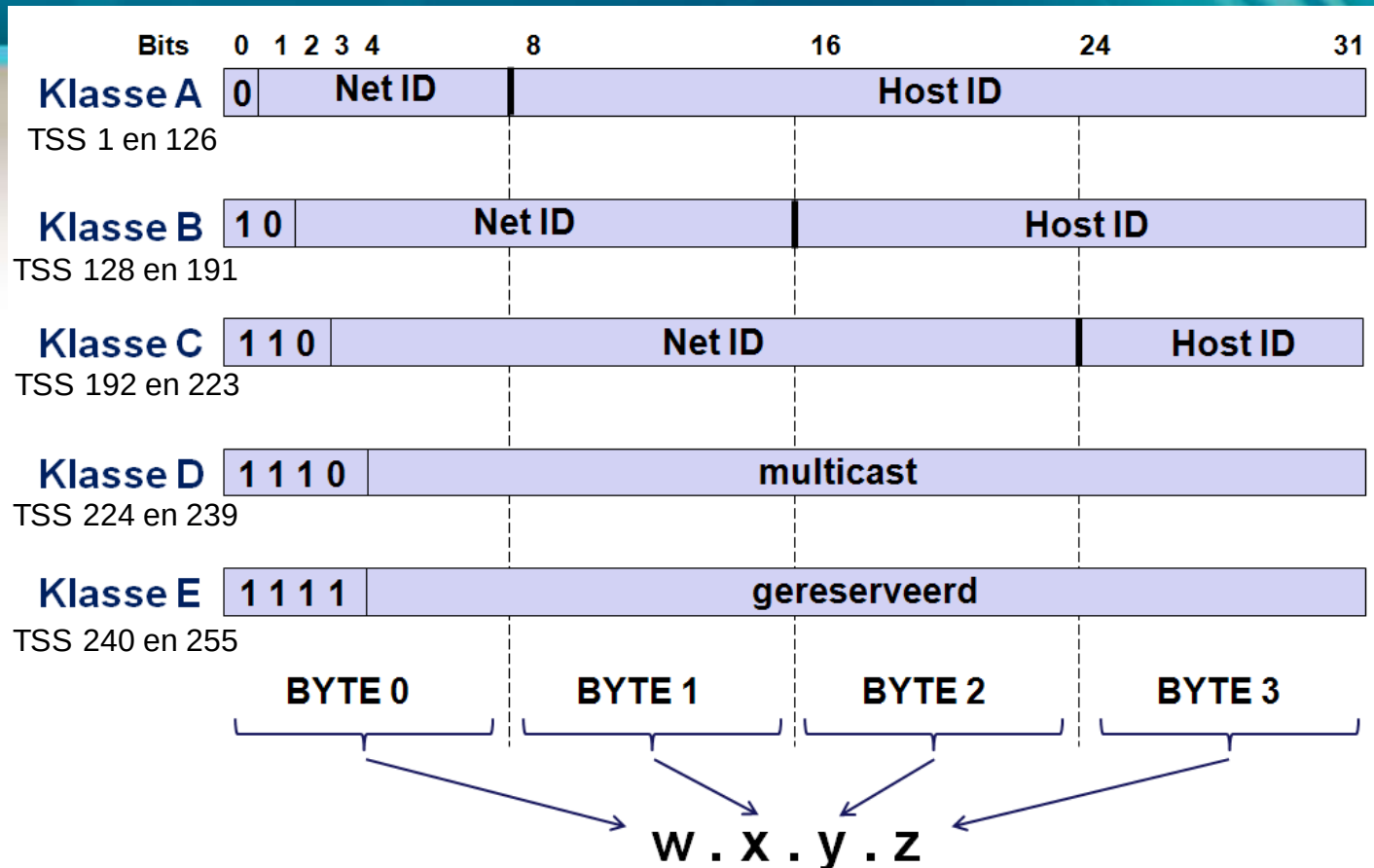
- Laagst mogelijke host ID: 0000 0001
- Hoogst mogelijke host ID: 1111 1110

Speciale adressen

- Elk netwerk heeft **twee** speciale adressen:
 - Netwerkadres: dit identificeert een volledig netwerk waarbij de Host ID allemaal nullen zijn
Bijv. 192.168.1.0 /24
 - Broadcastadres: verkeer dat naar dit adres wordt gestuurd zal aankomen bij elk toestel van dat netwerk. Dit is het adres waarbij de Host ID allemaal enen zijn.
Bijv. 192.168.1.255 /24

Net ID	Host ID	Beschrijving
allemaal nullen	allemaal nullen	IP adres van deze computer, wordt gebruikt tijdens de opstart
Net ID	allemaal nullen	Het netwerkadres, identificeert een volledig netwerk
Net ID	allemaal enen	Broadcastadres op het netwerk
127	willekeurig	IP adres voor het testen van netwerkapplicaties

IPv4 klassen



Dit is classful adressering

Publiek VS Privaat

- IPv4 heeft een aantal bereiken **gereserveerd** voor privaat gebruik d.w.z. indien zelf een netwerk wordt aangemaakt **moet** dit binnen één van deze private bereiken bevinden:
 - Klasse A privaat = 10.0.0.0 → 10.255.255.255 (Let op: 10.2.4.0 /24 kan dus ook)
 - Klasse B privaat = 172.16.0.0 → 172.31.255.255 (Let op: 172.21.0.0 /16 kan ook)
 - Klasse C privaat = 192.168.0.0 → 192.168.255.255 (192.168.3.0 /25 kan dus ook)
- Dit is classless adressering, elk subnetmasker kan gebruikt worden
- Dit wil ook zeggen: verschillende private netwerken kunnen dezelfde private adressen hebben (elk Telenet huishouden heeft hetzelfde netwerk type: 192.168.1.0/24)

Voorbeeld: mini-netwerk met IP



000c299fc292 d05099651840 0800

4500002a520540008006c2f6c0a83201 (IP Headers)

c0a83201 c0a83280 (IP SA & DA)

4574005042b83ed8da4f610350180100b9460000 (TCP Headers)

474554202f2048545450312e300d0a0d0a (TCP Data, hier HTTP GET)



192.168.50.1



192.168.50.128



Verhouding MAC <> IP adressen



- Een IP pakket bevat altijd
 - én bron en doel MAC adressen
 - én bron en doel IP adressen
- Hoe weet een toestel welk MAC adres bij welk IP hoort?
→ ARP = Address Resolution Protocol
- Dit zijn een bepaald soort rudimentaire frames die gericht zijn aan het ganse netwerk en vragen:
 - Welk MAC adres hoort bij IP W.X.Y.Z ?
 - De rechtmatige eigenaar reageert:
IP heeft W.X.Y.Z heeft als MAC 00:11:22:33:44:55

ARP Voorbeeld

Bron

192.168.1.50 /24
AB:CD:12:34:EE:50



192.168.1.0 /24

We voeren een ping uit

ICMP 192.168.0.50
Destination MAC
00:26:B8:33:44:20



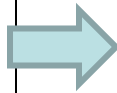
Doel

192.168.1.20



OS Berekening:

Bron IP = 192.168.1.50
Bron MAC = AB:CD:12:34:EE:50
Doel IP = 192.168.1.20
Doel MAC = ?



Zitten bron en doel IP in hetzelfde netwerk?

-> Afhankelijk van SUBNETMASKER (255.255.255.0)

Voer **BITWISE AND** operatie uit met subnetmasker en IP:

192.168.1.50 **AND** 255.255.255.0 = 192.168.1.0

192.168.1.20 **AND** 255.255.255.0 = 192.168.1.0

Direct ARP

ARP request (DA FF:FF:FF:FF:FF:FF) for destination IP:

- Who has 192.168.1.20? Tell 192.168.1.50
- 192.168.1.20 is at 00:26:B8:33:44:20

Destination MAC = 00:26:B8:33:44:20



ARP Voorbeeld 2

Bron
192.168.1.50 /24
AB:CD:12:34:EE:50



192.168.1.0 /24
We voeren een ping uit

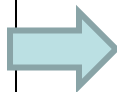


Doel
8.8.8.8



OS Berekening:

Bron IP = 192.168.1.50
Bron MAC = AB:CD:12:34:EE:50
Doel IP = 8.8.8.8
Doel MAC = ?



Zitten bron en doel IP in hetzelfde netwerk?
-> Afhankelijk van SUBNETMASKER (255.255.255.0)

Voer **BITWISE AND** operatie uit met subnetmasker en IP:
 $192.168.1.50 \text{ AND } 255.255.255.0 = 192.168.1.0$
 $8.8.8.8 \text{ AND } 255.255.255.0 = 8.8.8.0$

Router ARP (zie later)

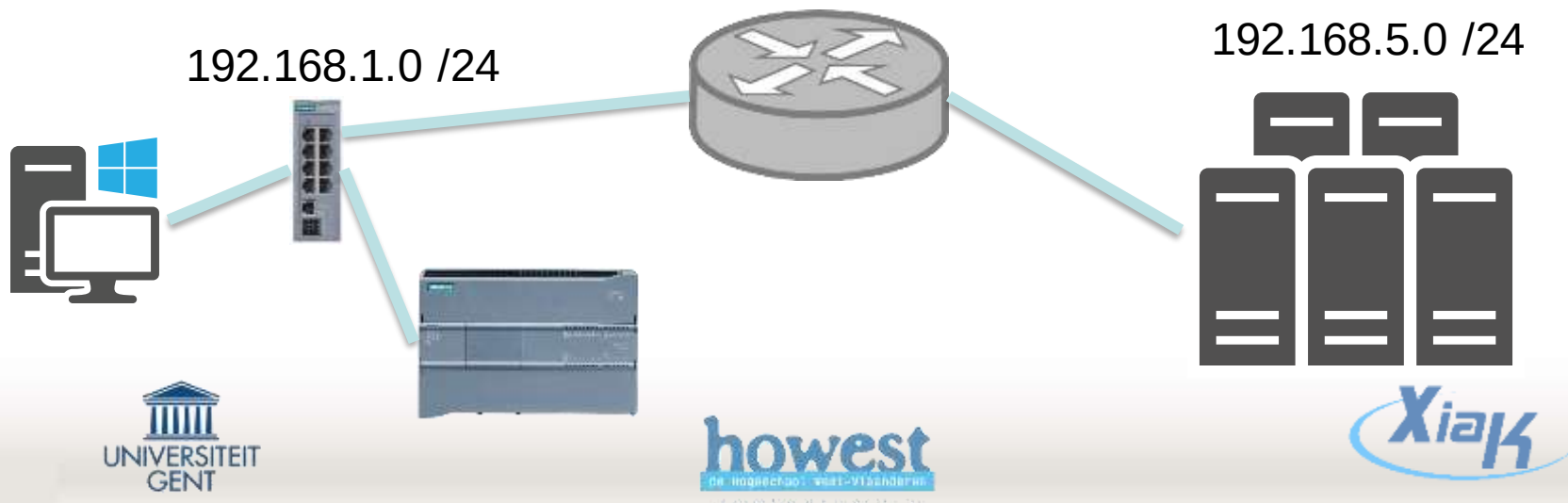
ARP request (DA FF:FF:FF:FF:FF:FF) for destination IP:

- Who has 192.168.1.1? Tell 192.168.1.50
- 192.168.1.1 is at 00:26:B8:33:44:01

Destination MAC = **00:26:B8:33:44:01**

Verschillende Netwerken

- Hoe kunnen verschillende netwerken met elkaar communiceren?
- Antwoord: via een ROUTER



Route table

```

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>route -4 print
=====
Interface List
13...00 00 1a 1a 98 bc .....Broadcom BCM5709C NetXtreme II GigE (NDIS VBD Client) #40
12...00 00 1a 1a 98 bb .....Broadcom BCM5709C NetXtreme II GigE (NDIS VBD Client) #39
14...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
27...00 50 56 c0 00 0a .....VMware Virtual Ethernet Adapter for VMnet10
1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          172.23.82.1      172.23.82.200    266
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        306
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        306
127.255.255.255            255.255.255.255  On-link          127.0.0.1        306
172.23.82.0                255.255.254.0    On-link          172.23.82.200    266
172.23.82.200              255.255.255.255  On-link          172.23.82.200    266
172.23.83.255              255.255.255.255  On-link          172.23.82.200    266
192.168.30.0               255.255.255.0    172.23.82.1      172.23.82.200    11
192.168.34.0               255.255.254.0    On-link          192.168.35.250   266
192.168.35.250             255.255.255.255  On-link          192.168.35.250   266
192.168.35.255             255.255.255.255  On-link          192.168.35.250   266
192.168.157.0              255.255.255.0    On-link          192.168.157.1    276
192.168.157.1              255.255.255.255  On-link          192.168.157.1    276
192.168.157.255            255.255.255.255  On-link          192.168.157.1    276
192.168.220.0              255.255.255.0    On-link          192.168.220.1    276
192.168.220.1              255.255.255.255  On-link          192.168.220.1    276
192.168.220.255            255.255.255.255  On-link          192.168.220.1    276
217.111.181.213            255.255.255.255  192.168.35.1      192.168.35.250   11
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link          172.23.82.200    266
224.0.0.0                  240.0.0.0        On-link          192.168.35.250   266
224.0.0.0                  240.0.0.0        On-link          192.168.220.1    276
224.0.0.0                  240.0.0.0        On-link          192.168.157.1    276
255.255.255.255            255.255.255.255  On-link          127.0.0.1        306
255.255.255.255            255.255.255.255  On-link          172.23.82.200    266
255.255.255.255            255.255.255.255  On-link          192.168.35.250   266
255.255.255.255            255.255.255.255  On-link          192.168.220.1    276
255.255.255.255            255.255.255.255  On-link          192.168.157.1    276
=====
Persistent Routes:
Network Address        Netmask          Gateway Address  Metric
192.168.30.0          255.255.255.0    172.23.82.1      1
0.0.0.0               0.0.0.0          172.23.82.1      Default
0.0.0.0               0.0.0.0          192.168.35.1      Default
=====
C:\Windows\system32>_

```

Route tabel

IPv4 Route Table

Active Routes:

Network	Destination	Netmask	Gateway
0.0.0.0	0.0.0.0	0.0.0.0	172.23.82.1
127.0.0.0	255.0.0.0		On-link
127.0.0.1	255.255.255.255		On-link
127.255.255.255	255.255.255.255		On-link
172.23.82.0	255.255.254.0		On-link
172.23.82.200	255.255.255.255		On-link
172.23.82.255	255.255.255.255		On-link
192.168.30.0	255.255.255.0		172.23.82.1
192.168.34.0	255.255.254.0		On-link
192.168.35.250	255.255.255.255		On-link
192.168.35.255	255.255.255.255		On-link
192.168.157.0	255.255.255.0		On-link
192.168.157.1	255.255.255.255		On-link
192.168.157.255	255.255.255.255		On-link
192.168.220.0	255.255.255.0		On-link
192.168.220.1	255.255.255.255		On-link
192.168.220.255	255.255.255.255		On-link
217.111.181.213	255.255.255.255		192.168.35.1
224.0.0.0	240.0.0.0		On-link
224.0.0.0	240.0.0.0		On-link
224.0.0.0	240.0.0.0		On-link
224.0.0.0	240.0.0.0		On-link
224.0.0.0	240.0.0.0		On-link
255.255.255.255	255.255.255.255		On-link
255.255.255.255	255.255.255.255		On-link
255.255.255.255	255.255.255.255		On-link
255.255.255.255	255.255.255.255		On-link

Indien doel-adres
niet in tabel (0.0.0.0 /0)
"Stuur naar **Default**
Gateway 172.23.82.1"

On-link = DIRECT ARP

Indien doel-adres
192.168.30.0 /24
"Stuur naar Gateway
172.23.82.1"

Voorbeeld van 1 IP:
217.111.181.213 /32

Route voorbeeld

IPv4 Route Table

Active Routes:

Network	Destination	Netmask	Gateway
	0.0.0.0	0.0.0.0	172.23.82.1
	127.0.0.0	255.0.0.0	On-link
	127.0.0.1	255.255.255.255	On-link
	127.255.255.255	255.255.255.255	On-link
	172.23.82.0	255.255.254.0	On-link
	172.23.82.200	255.255.255.255	On-link
	172.23.83.255	255.255.255.255	On-link
	192.168.30.0	255.255.255.0	172.23.82.1
	192.168.34.0	255.255.254.0	On-link
	192.168.35.250	255.255.255.255	On-link
	192.168.35.255	255.255.255.255	On-link
	192.168.157.0	255.255.255.0	On-link
	192.168.157.1	255.255.255.255	On-link
	192.168.157.255	255.255.255.255	On-link
	192.168.220.0	255.255.255.0	On-link
	192.168.220.1	255.255.255.255	On-link
	192.168.220.255	255.255.255.255	On-link
	217.111.181.213	255.255.255.255	192.168.35.1
	224.0.0.0	240.0.0.0	On-link
	224.0.0.0	240.0.0.0	On-link
	224.0.0.0	240.0.0.0	On-link
	224.0.0.0	240.0.0.0	On-link
	224.0.0.0	240.0.0.0	On-link
	255.255.255.255	255.255.255.255	On-link
	255.255.255.255	255.255.255.255	On-link
	255.255.255.255	255.255.255.255	On-link
	255.255.255.255	255.255.255.255	On-link
	255.255.255.255	255.255.255.255	On-link

Welke route (ARP)
voor het IP

192.168.35.123

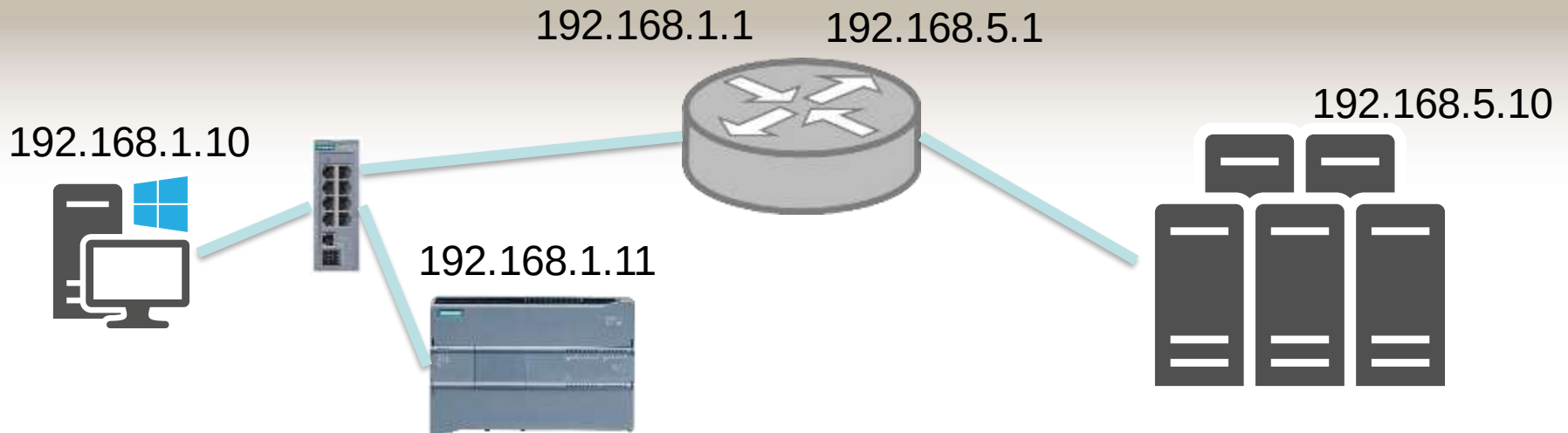
Direct ARP

192.168.35.123 is deel
van 192.168.34.0 /23

Default Gateway

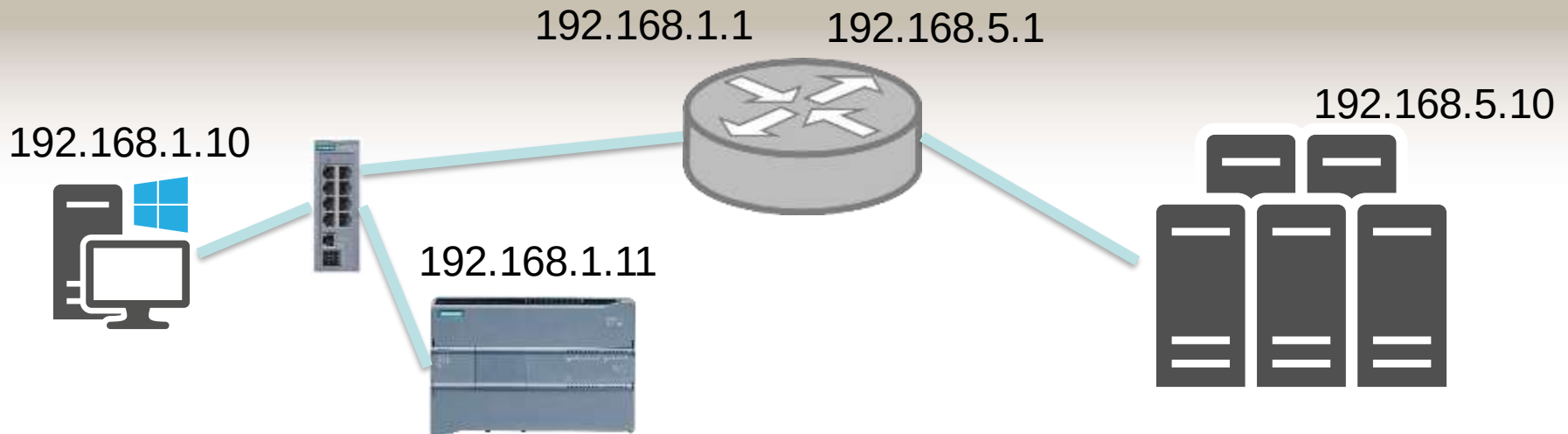
- Een host kan pakketten versturen naar:
 - Zichzelf → IPv4-adres = 127.0.0.1 = loopback adres
 - Een local host = host binnen hetzelfde netwerk
 - Een remote host = host in een ander netwerk
- Als een pakket naar een remote host moet gestuurd worden, zal het pakket in eerste instantie naar de **default gateway** gestuurd worden = de router die met het zelfde lokale netwerksegment geconnecteerd is → **een host met een IP-adresconfiguratie waarbij het IP-adres v/d default gateway niet ingevuld is, kan nooit communiceren met remote hosts!**
- Ook de routers hebben route tabellen

Voorbeeld scenario



1. Siemens S7-1200 wil een bericht sturen naar de OPC server met IP 192.168.5.10
2. Via de BITWISE AND detecteert de PLC dat het doel IP niet in zijn eigen netwerk hoort
3. Dus kijkt hij in zijn route tabel welke regel overeenkomt met het doel IP:
meestal de **default gateway 192.168.1.1** die werd ingesteld samen met zijn IP
4. D.m.v. een ARP-pakket ontdekt de PLC het MAC adres dat bij IP 192.168.1.1 hoort
5. Het pakket vertrekt met **doel IP 192.168.5.10** en het **doel MAC adres van de ROUTER**

Voorbeeld scenario (vervolg)



- M.a.w. een router heeft **altijd minstens twee IPs**: eentje in elk netwerk
- De router zal bij elk pakket hetzelfde proces doorlopen als daarnet:
BITWISE AND voor al zijn eigen netwerken, eventueel gevolgd door raadplegen route tabel,
gevolgd door een ARP en het opnieuw verzenden van het pakket
- De router zal dus **altijd** pakketten **wijzigen** (in tegenstelling tot een switch):
Het doel MAC adres wordt gewijzigd naar dat van de eindbestemming **of** dat van de gateway

De router ...

- Creëert broadcast domeinen: **Layer2 Verkeer** kan geen router passeren
- Bevat een route tabel met o.a. al zijn lokale IP adressen
- Bevat ARP cache
- Bevat een MAC tabel
(vooral handig indien de router ook een switch is/bevat)
- Zorgt ook voor het terugkerend verkeer
 - M.a.w. de andere kant van het netwerk moet ook de weg terug kennen, zoniet geen communicatie
 - Er wordt bij routers typisch van een interne (LAN) en externe (WAN) kant gesproken
- Is meestal niet alleen: een pakket over het internet passeert typisch tientallen netwerken en dus routers

Een netwerkpad: traceroute

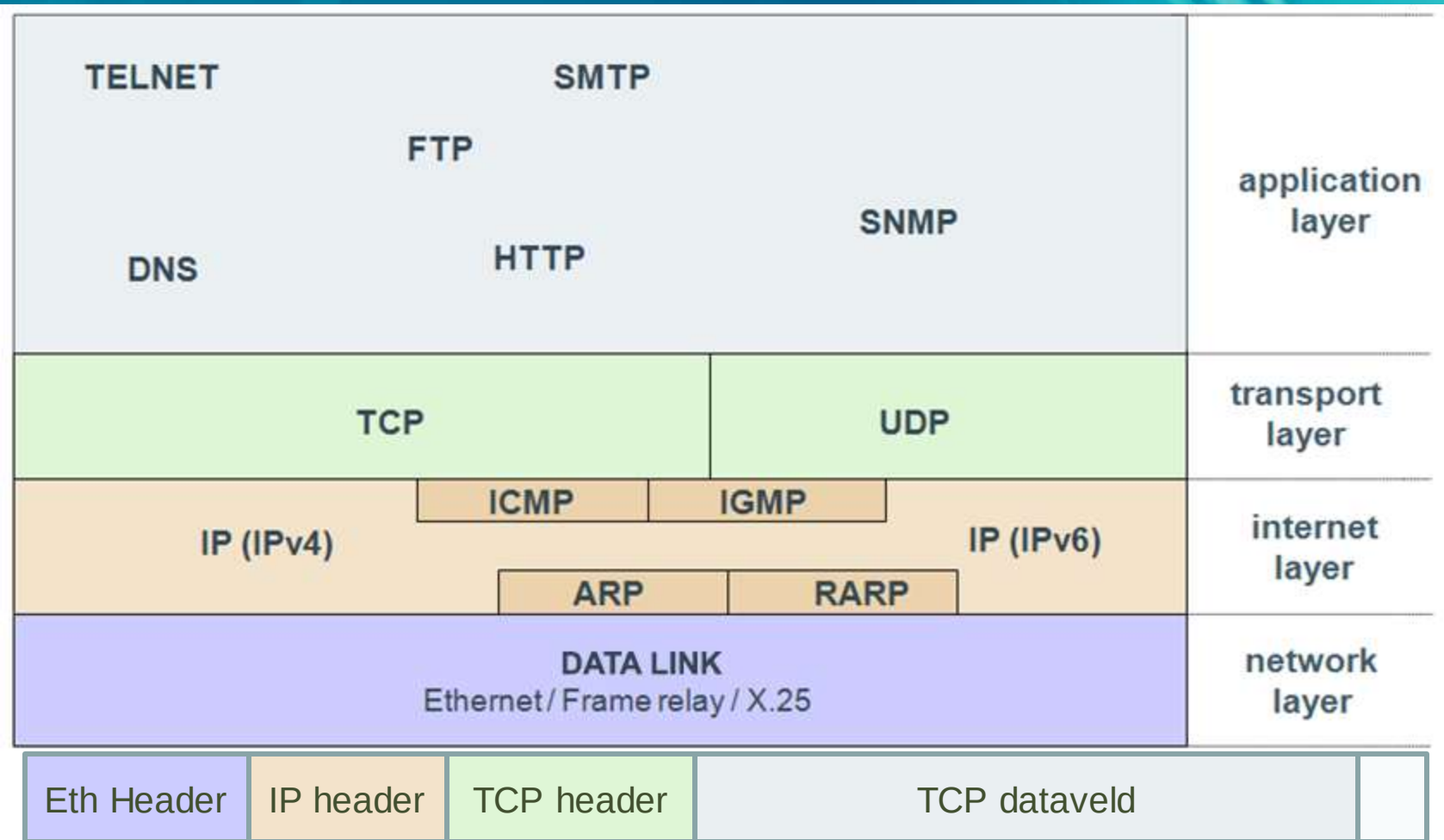
- Een pakket passeert typisch meerdere netwerken en dus routers vooraleer het aankomt.

```
em32>tracert 8.8.8.8
```

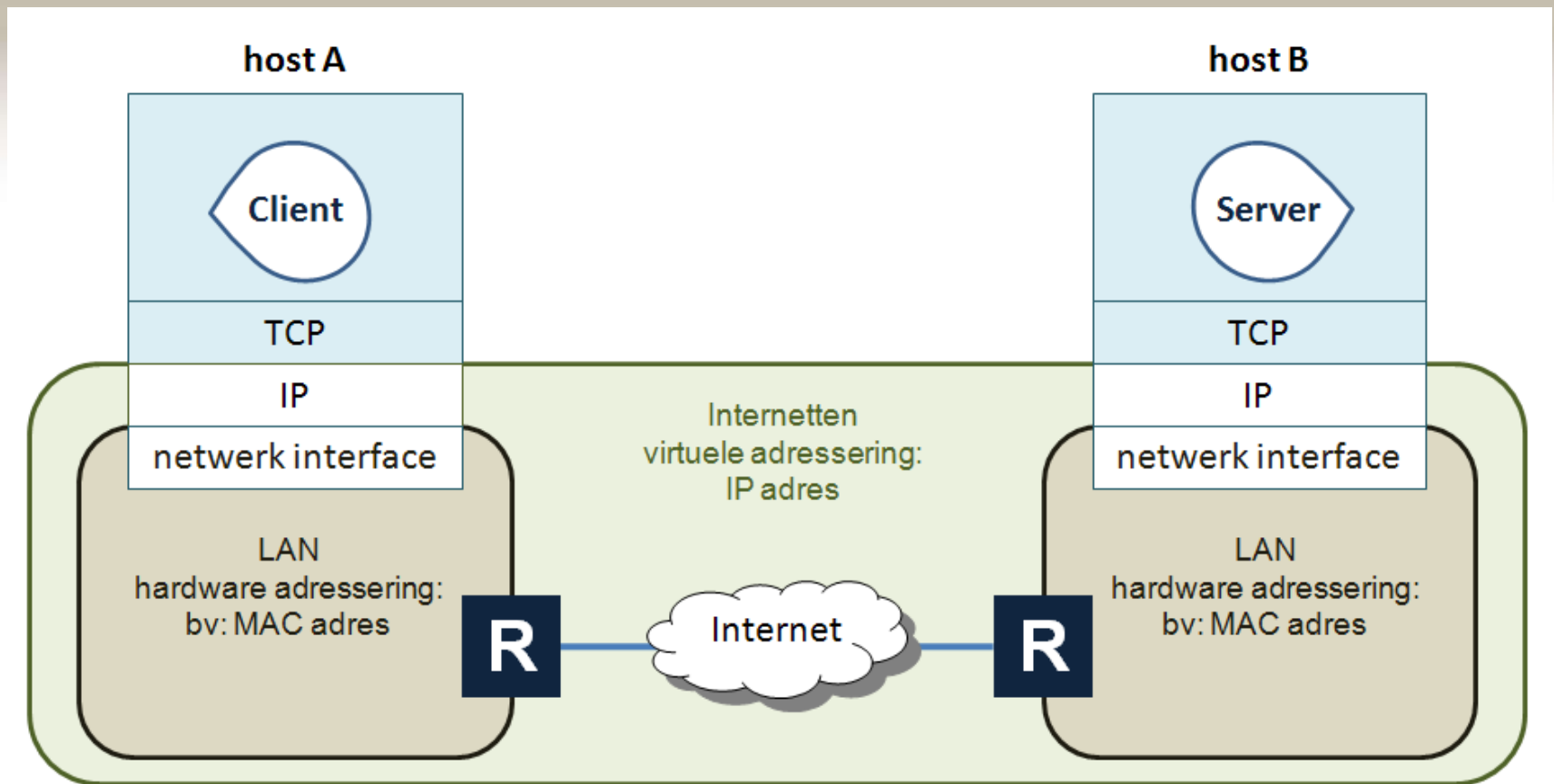
```
o google-public-dns-a.google.com [8.8.8.8]  
of 30 hops:
```

```
 7 ms      7 ms      dd576c001.access.telenet.be [213.118.192.1]  
11 ms     10 ms     dd5e0ca11.access.telenet.be [213.224.202.17]  
12 ms     13 ms     dd5e0fa5e.access.telenet.be [213.224.250.94]  
11 ms     13 ms     ae52.bar1.brussels1.level3.net [212.3.238.129]  
15 ms     13 ms     ae-117-3503.edge5.amsterdam1.level3.net [4.69.162.1]  
15 ms     16 ms     72.14.203.124  
23 ms     23 ms     209.85.143.167  
24 ms     25 ms     209.85.253.249  
29 ms     29 ms     216.239.56.72  
27 ms     26 ms     216.239.56.79  
*         *         Request timed out.  
35 ms     24 ms     google-public-dns-a.google.com [8.8.8.8]
```

Volgende Laag



TCP/IP

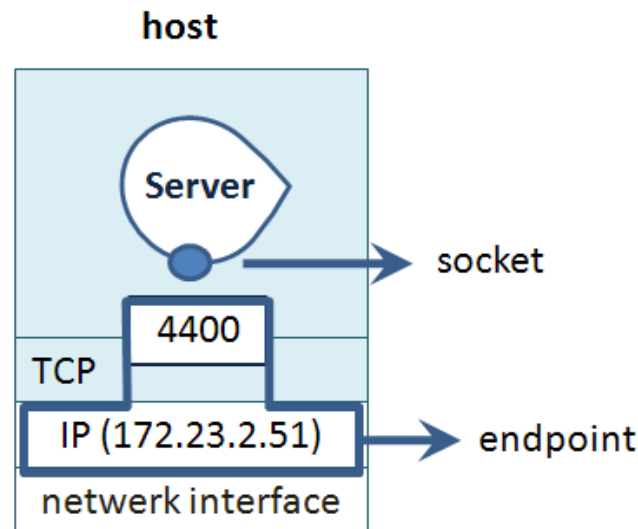


Client / Server applicatie

- Server levert één dienst en kan verschillende Clients tegelijk afhandelen
- Wordt automatisch geactiveerd wanneer een systeem opstarten en blijft actief tijdens vele sessies
- Draait eventueel op een gedeelde computer met andere server applicaties
- Wacht passief tot willekeurige Clients contact zoeken
- Vereist soms krachtige hardware en geavanceerd besturingssysteem, afhankelijk van de soort toepassing

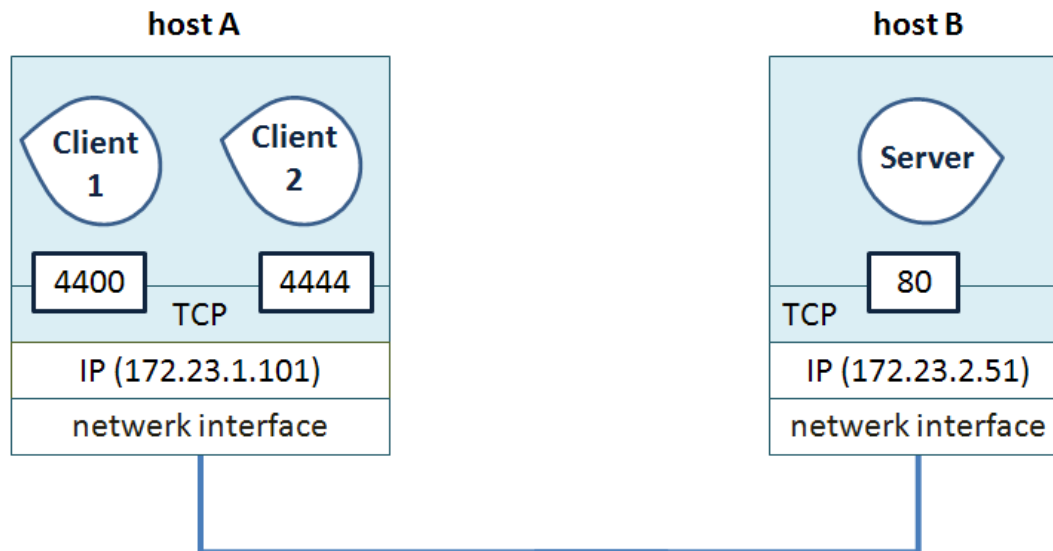
Poorten

- Een server applicatie beheert een zogenaamde *socket*: dit is een combinatie van een **IP adres** met een vast **poortnummer** (16bits)
- Clients kunnen dan met deze socket een verbinding maken, hierdoor moet de Client dus niet enkel het IP adres, maar ook het poortnummer kennen van de server applicatie



CLIENT SERVER model

- Clients verbinden met een server socket door zelf ook een socket aan te maken, dit echter door een willekeurige poort hoger dan 1023 te gebruiken per communicatie
- Eén Client sessie is dus uniek door de combinatie van volgende factoren: Client IP + Client poortnr. + Server IP + Server poortnr.



Voorbeeld Poorten

Applicatie	Poortnummer / Protocol
FTP-data (File Transfer Protocol)	20 / TCP
FTP-control (File Transfer Protocol)	21 / TCP
SSH (Secure Shell)	22 / TCP,UDP
Telnet protocol	23 / TCP
BOOTP Server	67 / UDP
DHCP Server	67 / UDP
BOOTP Client	68 / UDP
DHCP Client	68 / UDP
TFTP (Trivial File Transfer Protocol)	69 / UDP
HTTP (Hypertext Transfer Protocol)	80 / TCP
NTP (Network Time Protocol)	123 / UDP
SNMP (Simple Network Management Protocol)	161 / TCP,UDP
SNMPTRAP (Simple Network Management Protocol Trap)	162 / TCP,UDP
HTTPS (Hypertext Transfer Protocol over TLS/SSH)	443 / TCP

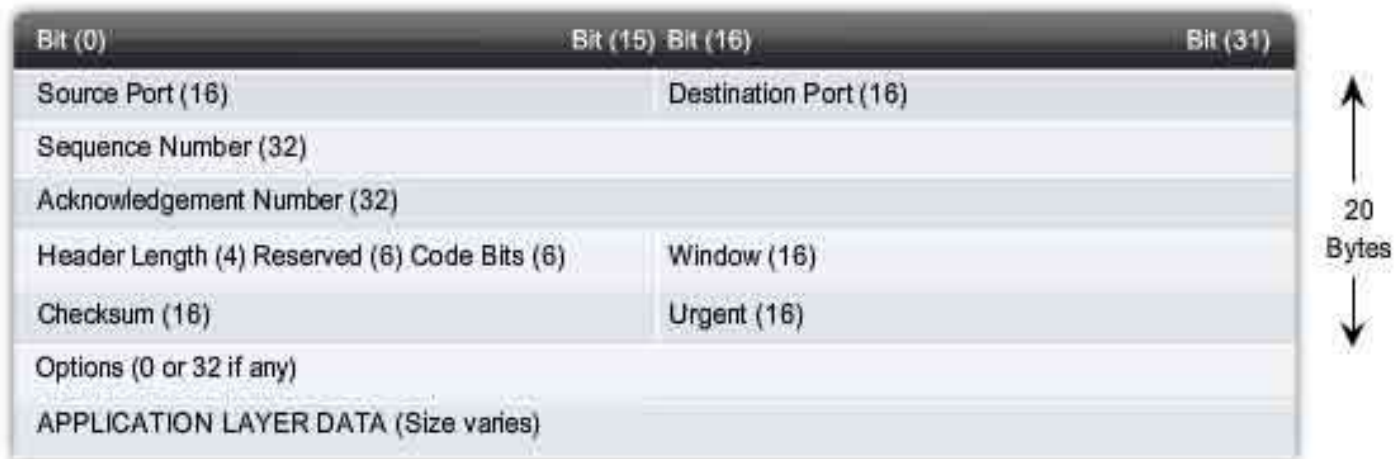
TCP VS UDP

- Meest voorkomend is TCP
- TCP (Transmission Control Protocol) werkt met sessies en is *stateful*
- UDP (User Datagram Protocol) is connectieloos en *stateless*
- TCP heeft ingebouwde ontvangstbevestiging en doet aan *flow control*, UDP doet dit niet
- UDP wordt typisch gebruikt bij de applicatieprotocollen DNS, DHCP en SNMP

TCP VS UDP Header

TCP and UDP Headers

TCP Segment



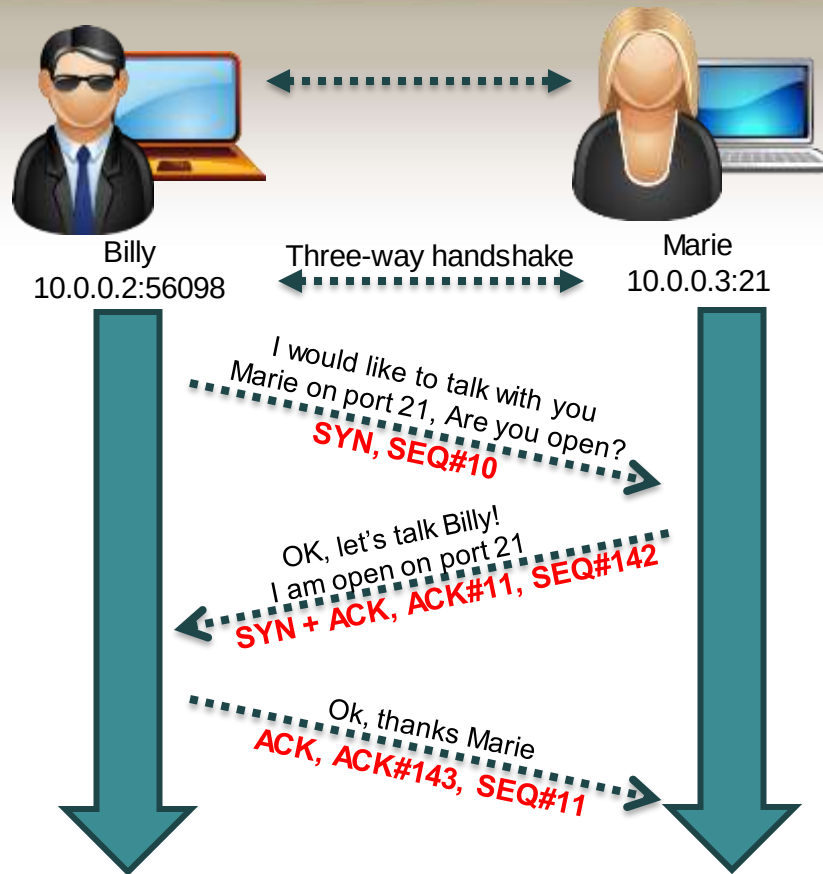
UDP Datagram



TCP: de voordelen

- Het TCP protocol houdt in dat doorgaans bij elk pakket dat verstuurd wordt er een **ontvangstbevestiging** komt, dit onder de vorm van speciale “ACK” pakketten
- Dit houdt in dat TCP zorgt voor meer en dus ook trager verkeer
- Een TCP-sessie bestaat typisch uit een zogenaamde *TCP Three-Way Handshake* om de sessie te starten en een *TCP Four-Way Close* om de sessie mee af te sluiten.

TCP Three-Way Handshake



TCP	192.168.3.200:23114	174.127.201.143:3222	ESTABLISHED
TCP	192.168.3.200:28212	132.245.228.2:443	ESTABLISHED
TCP	192.168.3.200:28213	132.245.228.2:443	ESTABLISHED
TCP	192.168.3.200:28214	132.245.228.2:443	ESTABLISHED
TCP	192.168.3.200:28215	132.245.228.2:443	ESTABLISHED
TCP	192.168.3.200:28216	132.245.228.2:443	ESTABLISHED
TCP	192.168.3.200:28218	132.245.228.2:443	TIME_WAIT
TCP	192.168.3.200:28219	132.245.228.2:443	ESTABLISHED
TCP	192.168.3.200:28224	64.15.124.245:80	ESTABLISHED
TCP	192.168.3.200:28225	64.15.124.217:443	ESTABLISHED
TCP	192.168.3.200:28228	64.15.124.247:443	ESTABLISHED
TCP	192.168.3.200:28229	64.15.124.245:443	ESTABLISHED
TCP	192.168.3.200:28233	64.15.124.247:443	ESTABLISHED
TCP	192.168.3.200:28238	132.245.228.2:443	ESTABLISHED
TCP	192.168.3.200:28239	132.245.228.2:443	ESTABLISHED
TCP	192.168.3.200:28247	191.234.5.80:80	ESTABLISHED
TCP	192.168.3.200:28248	191.234.5.80:80	ESTABLISHED
TCP	192.168.3.200:28255	64.15.124.246:443	ESTABLISHED
TCP	192.168.3.200:28256	31.13.90.2:443	ESTABLISHED
TCP	192.168.3.200:28257	31.13.90.6:443	ESTABLISHED
TCP	192.168.3.200:28258	94.31.29.40:80	ESTABLISHED
TCP	192.168.3.200:28259	64.15.124.213:443	ESTABLISHED
TCP	192.168.3.200:28260	31.13.84.4:443	ESTABLISHED
TCP	192.168.3.200:28261	74.125.136.157:443	ESTABLISHED
TCP	192.168.3.200:28269	193.191.136.205:443	ESTABLISHED
TCP	192.168.3.200:28270	193.191.136.205:443	ESTABLISHED
TCP	192.168.3.200:28271	193.191.136.205:443	ESTABLISHED
TCP	192.168.3.200:28273	193.191.136.205:443	ESTABLISHED
TCP	192.168.3.200:28274	193.191.136.205:80	ESTABLISHED
TCP	192.168.3.200:28276	193.191.136.205:80	ESTABLISHED
TCP	192.168.3.200:28278	132.245.228.2:443	ESTABLISHED
TCP	192.168.3.200:28280	132.245.228.2:443	ESTABLISHED
TCP	192.168.3.200:28281	193.190.67.98:21	ESTABLISHED
TCP	192.168.3.200:28219	132.245.228.2:443	ESTABLISHED
TCP	192.168.3.200:28224	64.15.124.245:80	ESTABLISHED
TCP	192.168.3.200:28225	64.15.124.217:443	ESTABLISHED