Netwerkconfiguratie
Applicatie protocollen

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

UNIVERSITEIT GENT

howest

XiaK

Overzicht Cursus (1 dag)

Voormiddag

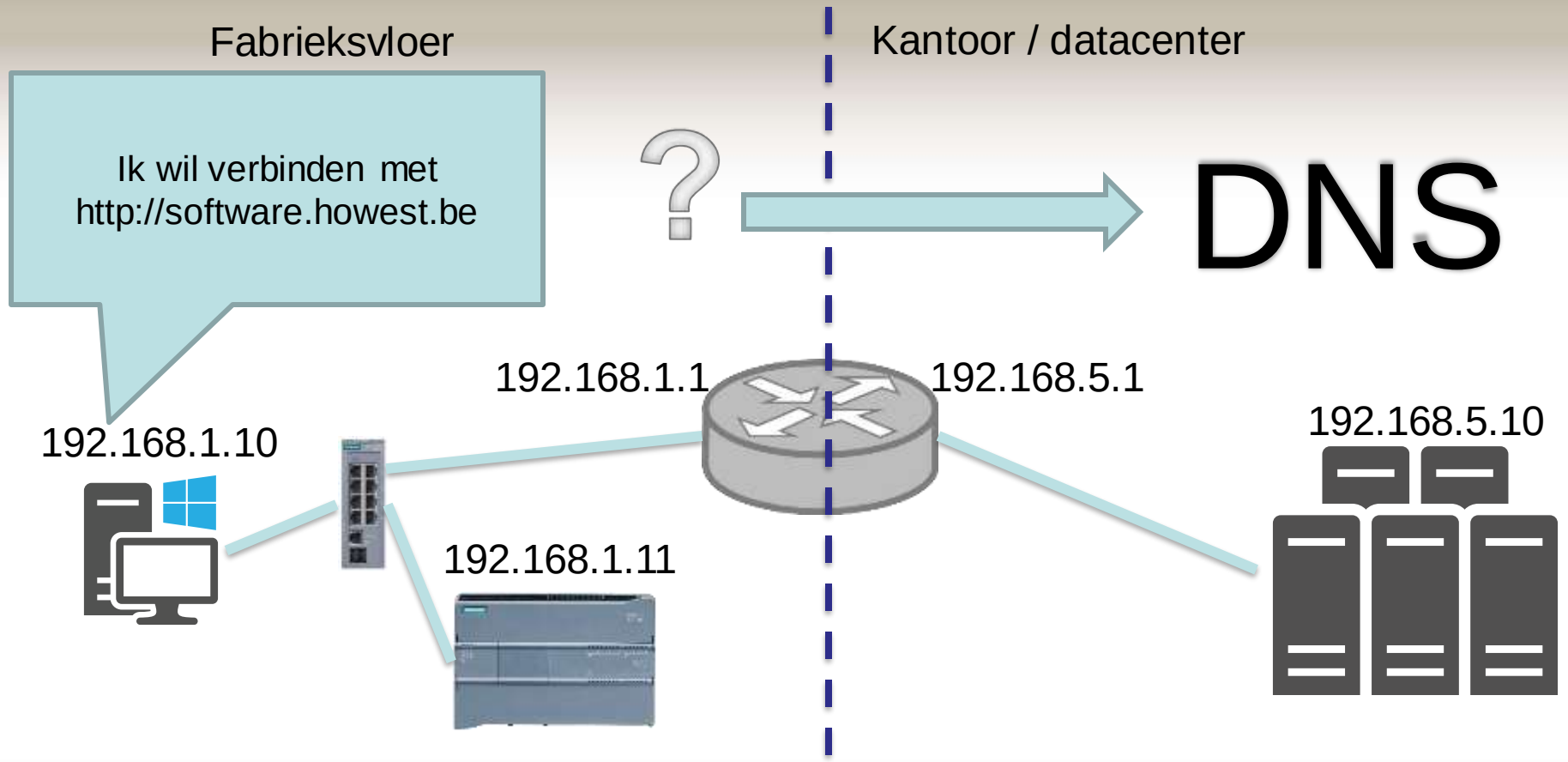
- Theorie TCP/IP
  - Hardware / bekabeling
  - TCP/IP model
  - MAC adressen
  - IP adressen
  - Netmaskers
  - Netwerken, routers (ARP)
  - TCP & UDP Poorten

Overzicht Cursus (1 dag)

Namiddag

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

Een volledig werkend netwerk

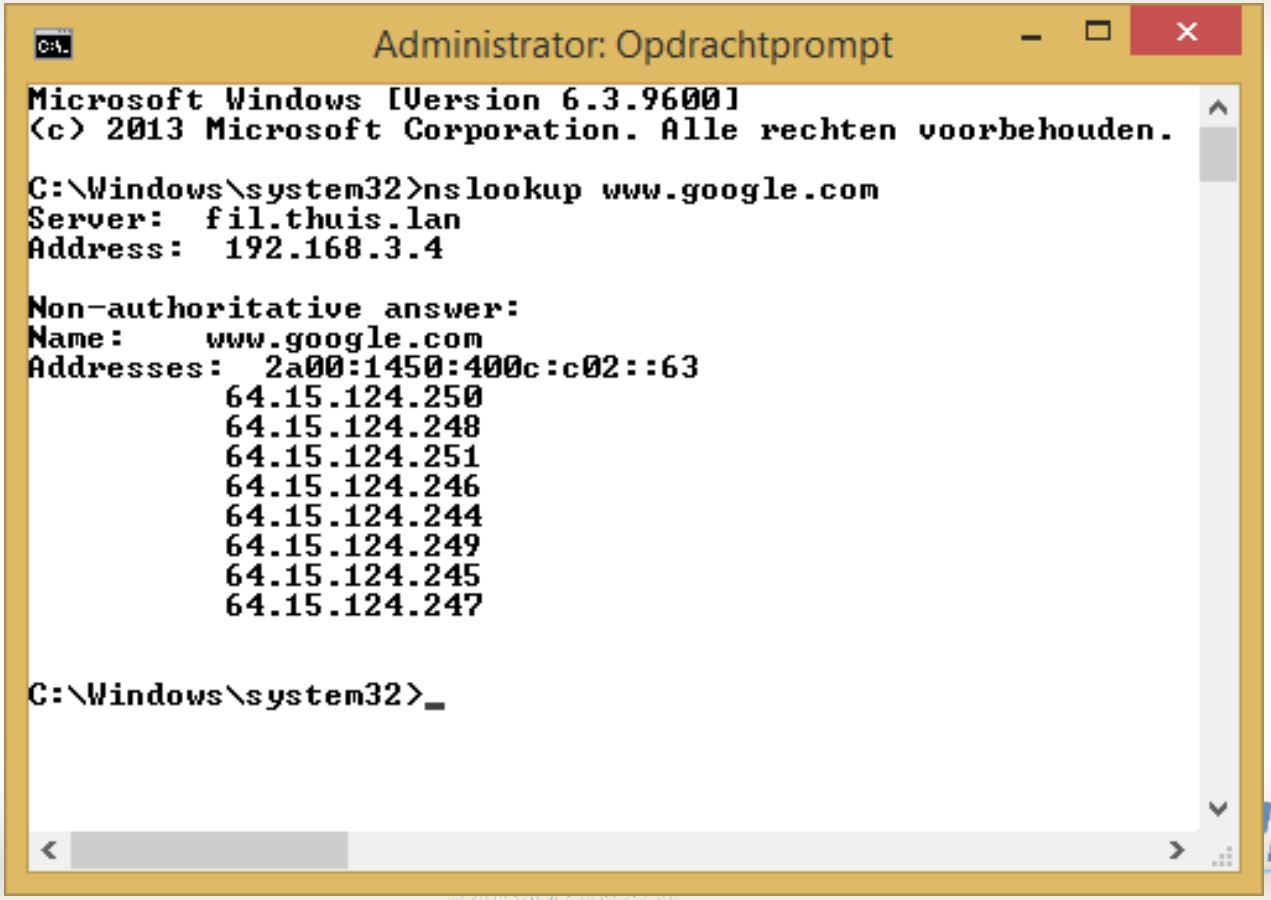


DNS / Domain Name System

- DNS is het naamgevingssysteem om op een netwerk hosts te identificeren
- DNS is ook de naam van het protocol om die namen naar IP adressen om te zetten
- Het DNS protocol (UDP!) werkt volgens het client-server systeem:
  - Een DNS client vraagt aan een DNS server (ook nameserver genoemd) naar het IP dat bij een bepaalde naam hoort: **Forward Lookup** (Naam naar IP)
  - Er bestaan nog andere soorten requests (Reverse Lookup is IP naar naam)
- **Het IP van de DNS** server(s) moet ingevuld worden samen met de IP-, Subnetmask en Gateway gegevens
- Dit omzetten heet ook wel ***resolven***

DNS Tool

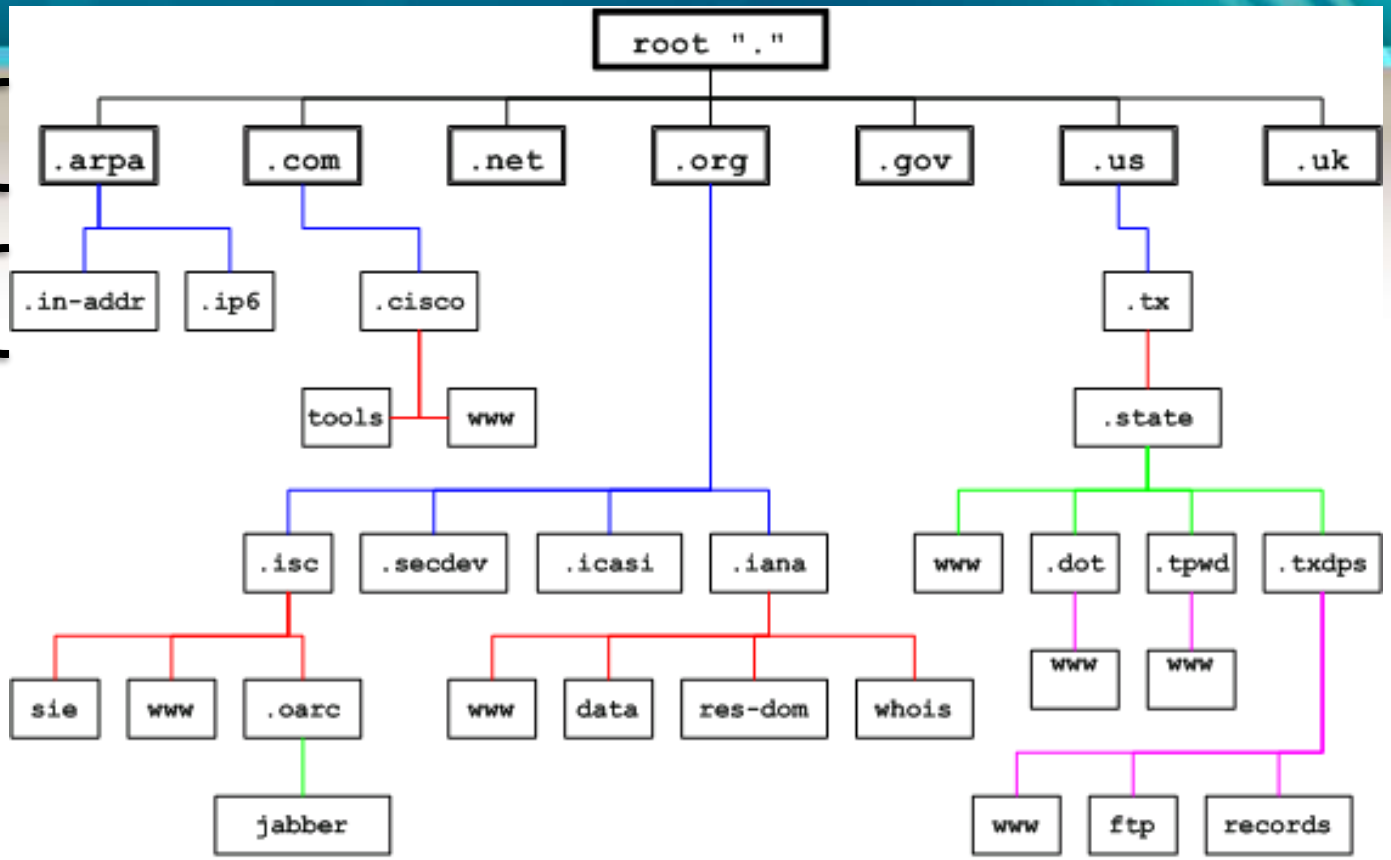
Een goede manuele DNS tool is ***nslookup*** die bestaat voor Windows, Linux en Mac OS X



DNS Namespace

Top Level Domains

Second Level Domains



.arpa: primarly used for address to host mappings

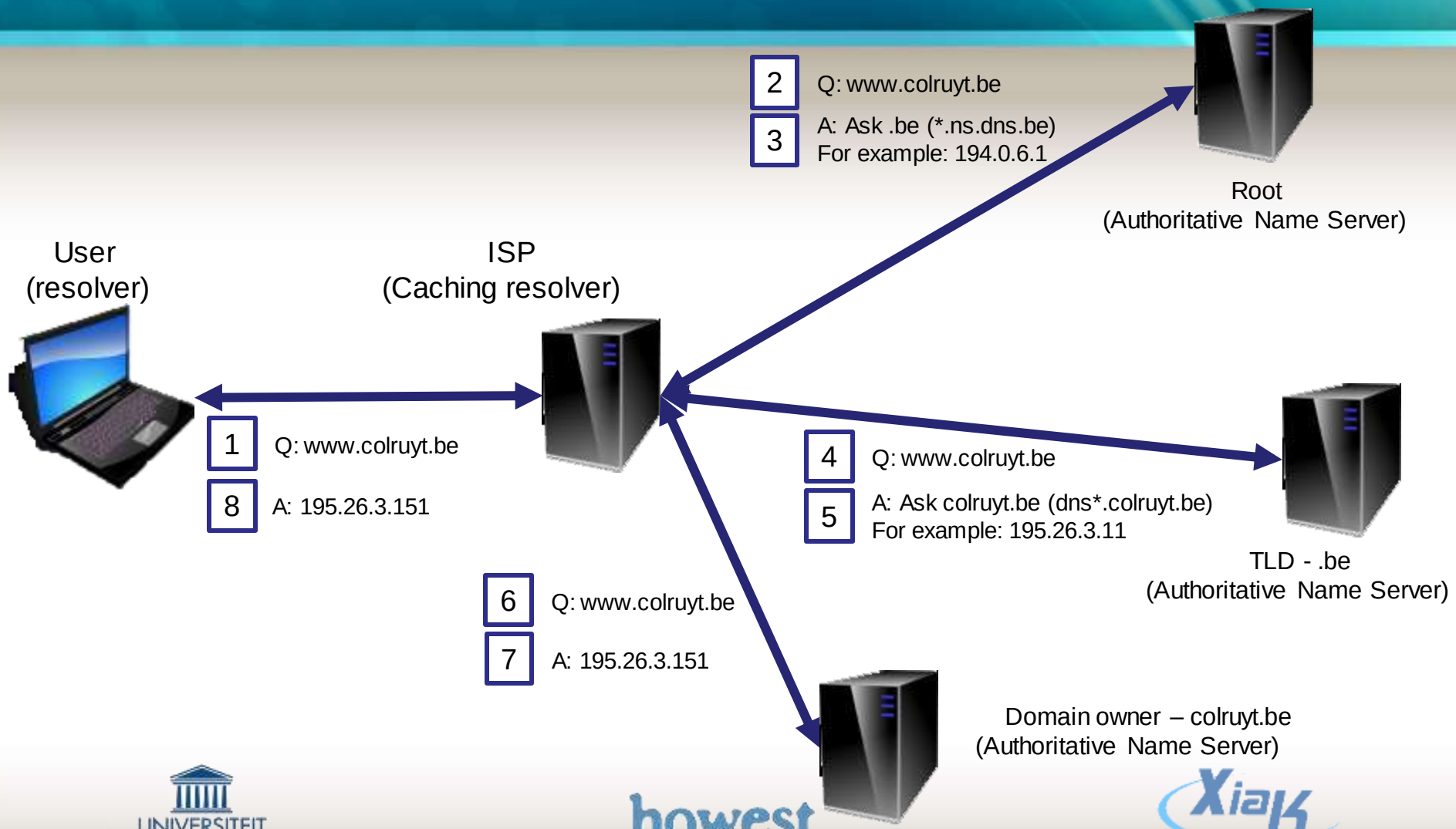
.com, **.net**, **.org**, **.org**: are generic TLDs (gTLD)

.us, **.uk**: are country code TLDs (ccTLD)

DNS Hiërarchie

- Een nameserver kent uiteraard niet alle namen + IP adressen van de hele wereld, daarom wordt een hiërarchie gebruikt
- Elke DNS server is verantwoordelijk (*authoritative)* voor een bepaalde *zone*
  - Bijv. voor de zone howest.be is dat DNS server 193.191.136.220
- Als een naam moet geresolved worden zal deze van achter naar voor, stap per stap geresolved worden, voor www.howest.be:
  - eerst de authoritative server voor .be zoeken
  - die server vertelt ons welke verantwoordelijk is voor howest.be
  - die vertelt ons het IP adres van www.howest.be

Hoe werkt DNS

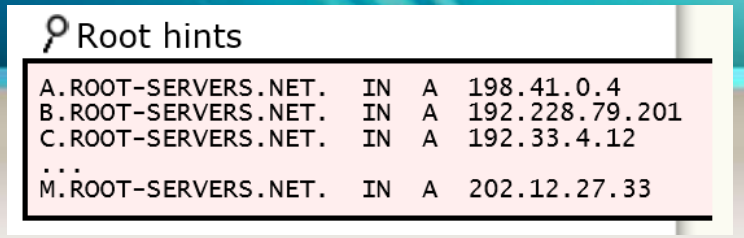


UNIVERSITEIT GENT

howest

Xiak

Het begin van alles



- … zijn dus de root servers
  - Dit zijn servers die elkaar up-to-date houden en hun IP adressen zitten “ingebakken” in Linux & Windows Server DNS services

- Deze worden miljoenen keer per dag ondervraagd, om dit vlotter te laten verlopen bestaat er **DNS Caching**
  - **DNS Caching** werkt met het TimeToLive veld in het DNS antwoord
- Élke DNS server en Windows DNS client doet aan DNS caching
  - Standaard Linux niet!

- Ter volledigheid: er bestaan ook *Forwarding DNS Servers* die niet authoritative zijn en zelfs niet caching, maar enkel requests doorsturen

DNS demo time

- Behalve de externe DNS servers is er ook een intern bestand: de hosts-file
  - Bevat de **manuele** ingaven van namen en IP adressen
    - Windows: *C:\Windows\System32\drivers\etc\hosts*
    - In Linux/Unix: */etc/hosts*
  - Wordt altijd **eerst** gecontroleerd

- ipconfig /displaydns
- ipconfig /flushdns

Een netwerk instellen

Om van een volledig en normaal functionerende configuratie te spreken zijn dus volgende dingen in te stellen:

1. IP adres
2. + subnetmasker voor eigen identificatie

3. Standaardgateway adres voor communicatie buiten het netwerk
   - Wordt genegeerd bij communicatie binnen eigen netwerk

4. Eén of meerdere DNS server adressen
   - Wordt genegeerd bij communicatie via IP adressen
   - Worden pas gebruikt indien hosts-file de omzetting niet bevat
   - Als de eerste niet antwoord zal de volgende geraadpleegd worden

Altijd manueel?

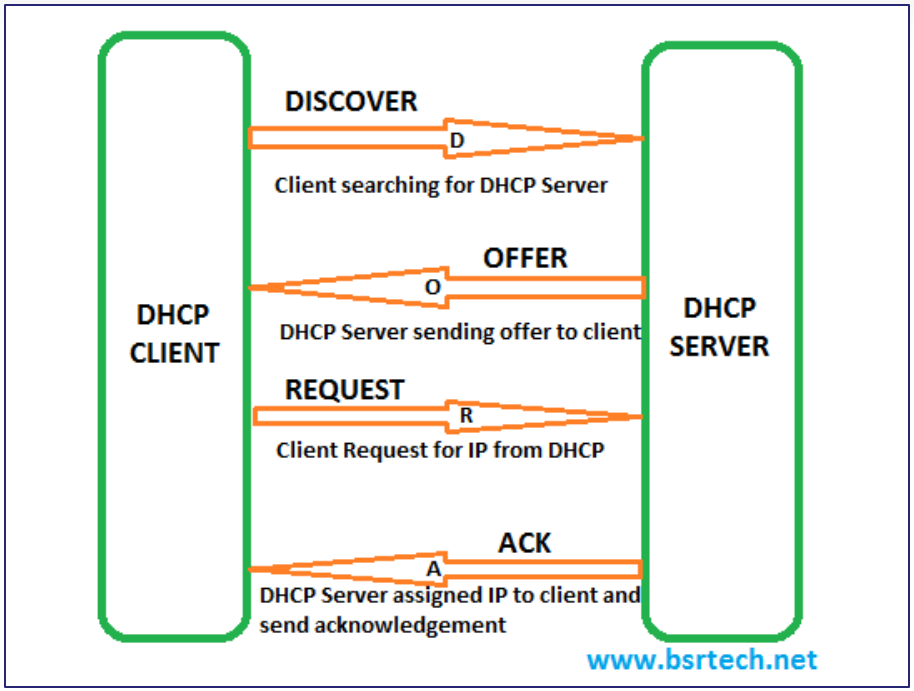
- Dit manueel instellen van de informatie zou vrij omslachtig zijn voor mobiele toestellen (smartphones, laptops, tablets …)
- Oplossing: Dynamische IP adressering oftewel

DHCP = Dynamic Host Configuration Protocol

- Ook dit protocol is een Client-Server protocol (UDP!)
  - Dus op het netwerk is een DHCP server nodig
- Bij de meeste toestellen is er dus de keuze: **DHCP** of **Statisch IP**

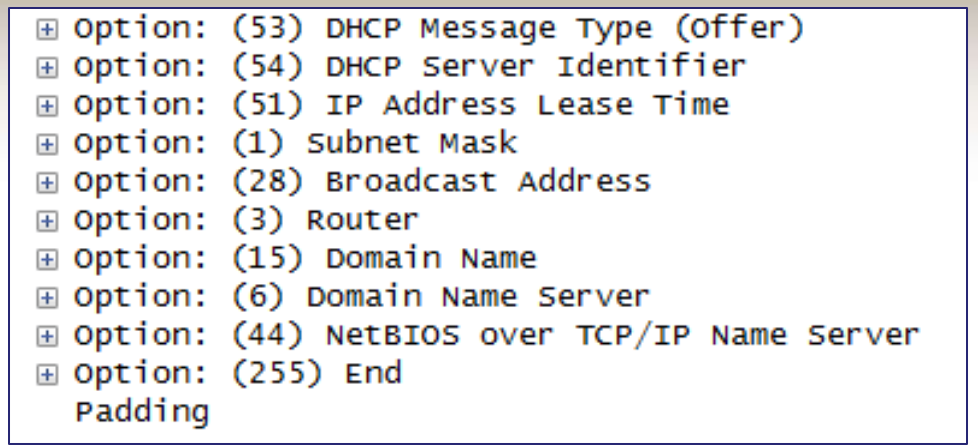
Werking DHCP

Een DHCP-client kan aan een IP-adres geraken d.m.v. vier fasen: de D.O.R.A. fasen:



Belangrijk bij DHCP

- DHCP servers delen niet **enkel** IP adressen uit, maar ook:
  - Standaardgatewayadres (router)
  - Subnetmasker
  - Domain Name Server adressen
  - De geldigheidsduur (lease time)
  - Domain Name (bv. howest.be)
  - …



- Er moet een DHCP server aanwezig zijn per netwerk;
  DHCP pakketten passeren GEEN routers (want Layer2 verkeer)

- Wat gebeurt er als er geen DHCP server reageert
  (dus als er geen Offer volgt op onze Discover)?

Windows geeft zichzelf een IP: 169.254.x.y /16 adres, ook gekend als APIPA

Software Simulatie

Het (oude) thuisnetwerk

met Packet Tracer

Demo

De Basis Firewall

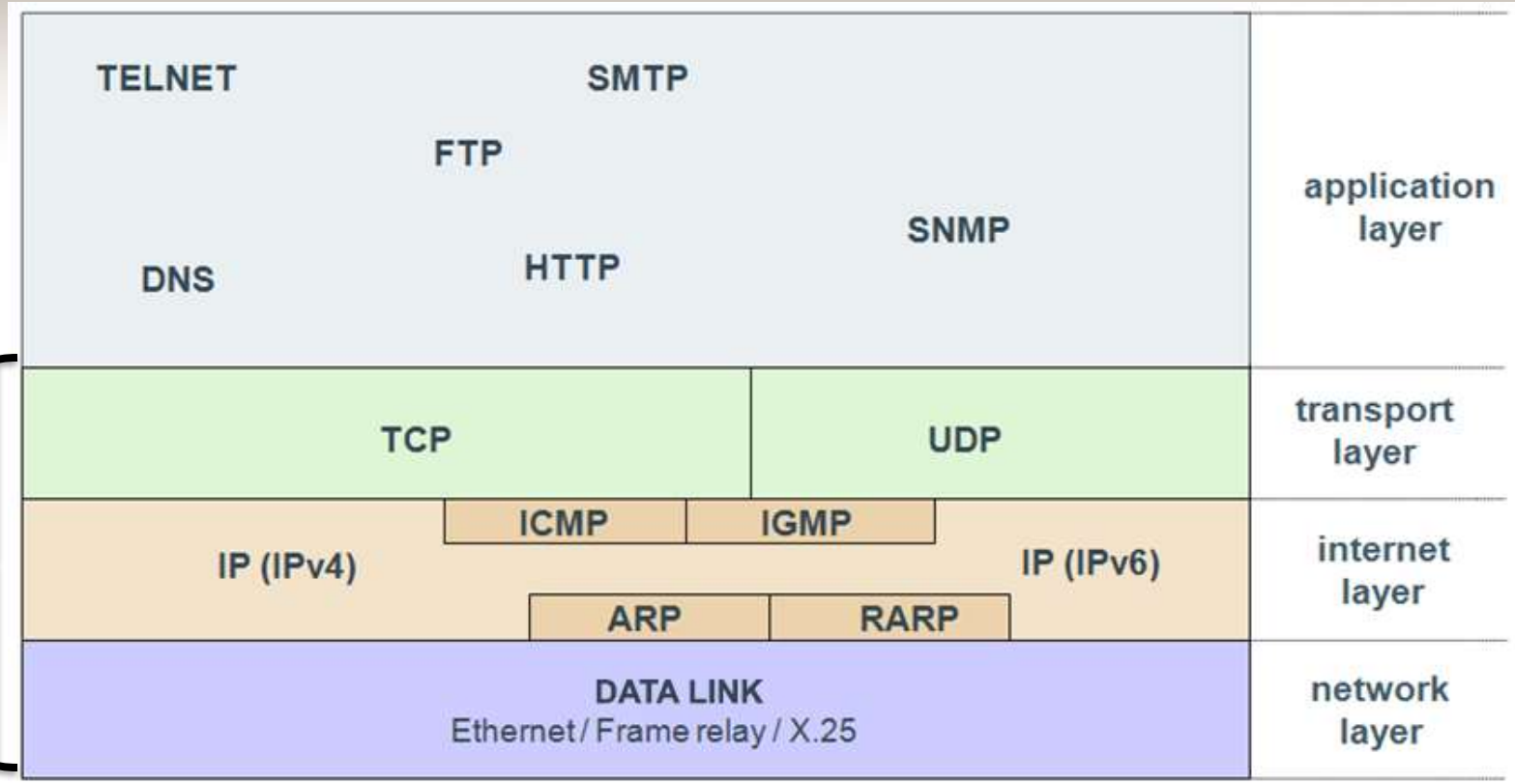
- Zeer veel routers, zowel industrieel als *SOHO* (thuis-) routers, zijn eigenlijk multifunctionals:
  - Ze bevatten een router
  - Doorgaans (bijv. thuis) ook een ingebouwde switch
  - Er zit een DHCP server in (deelt netwerk gegevens uit)
  - Er zit een DNS server in (weliswaar enkel forwarding)
  - Er zit een Web server in (om hem te beheren)
  - Ondersteund dikwijls nog protocollen als SNMP, Telnet, UPNP …
  - En meestal, zoniet altijd: een basic firewall

Firewall

- Standaard Firewalls zijn overal te vinden:
  - Bij Windows staat hij standaard aan
  - Veel Linux-distributies hebben er eentje
  - Zeer veel routers bevatten eentje (o.a. die van Telenet & Proximus)
  - Elk bedrijf heeft wel een firewall

- Deze filteren doorgaans verkeer enkel op de Data Link, Internet en Transport lagen

Basis Firewall



Basis Firewalls

Firewall Regels (rules)

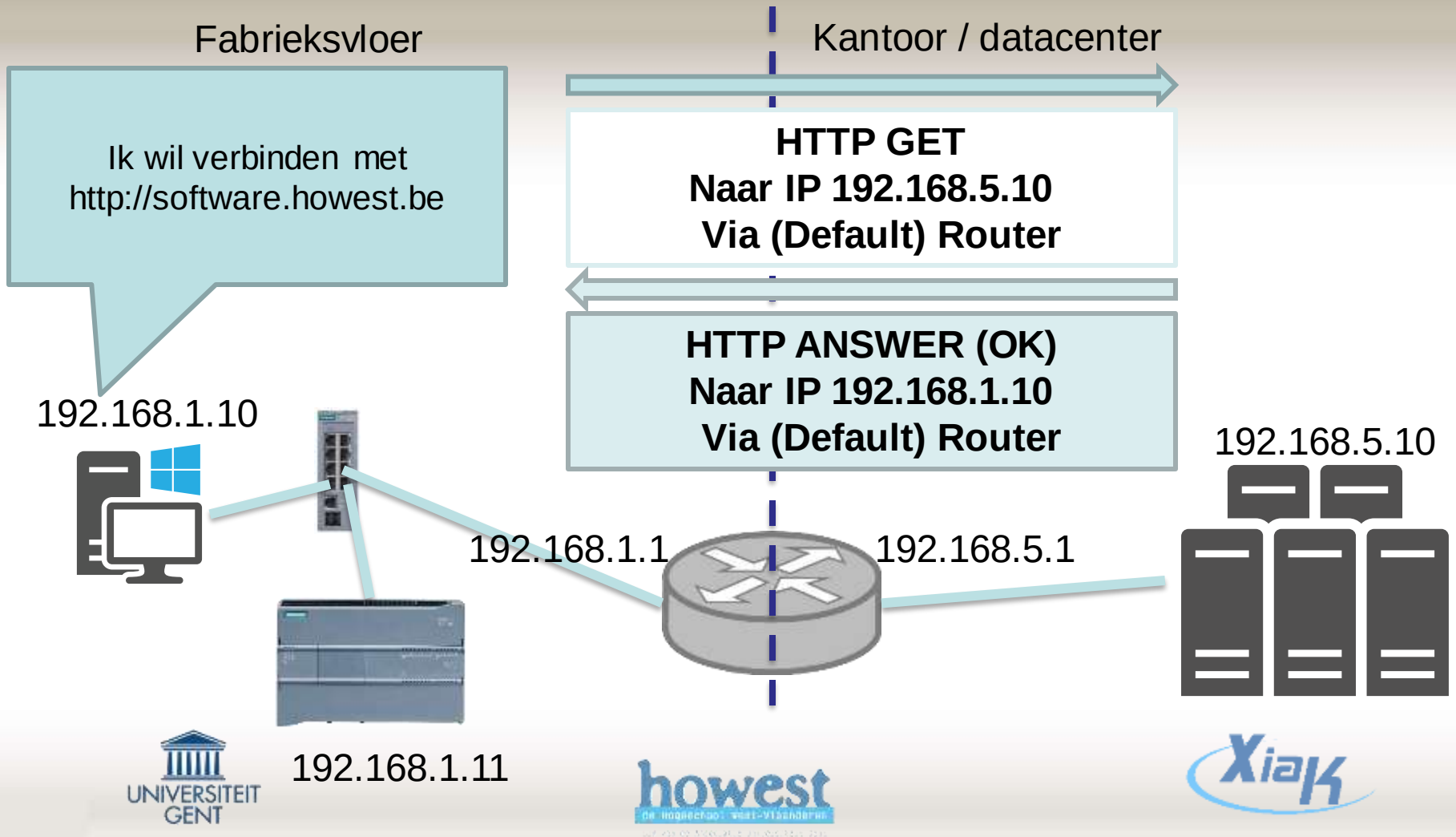
Het configureren van een firewall is regels opstellen die een antwoord geven op deze vragen:

- Welke actie geldt voor de regel: toelaten of blokkeren?
- Op welke netwerkinterface is deze regel van toepassing?
  - Bijv. de LAN interface
- Inbound/Outbound: Geldt deze regel voor inkomend of uitgaand verkeer?
  - De Windows Firewall staat bijv. standaard volledig dicht voor inbound. Sessie die uiteraard die zelf opgezet zijn, zijn wel toegelaten
- Welk bron en/of doel IP adres?
- Welke bron en /of doel poort?
- Welk protocol? (TCP/UDP/ICMP/… of allen)

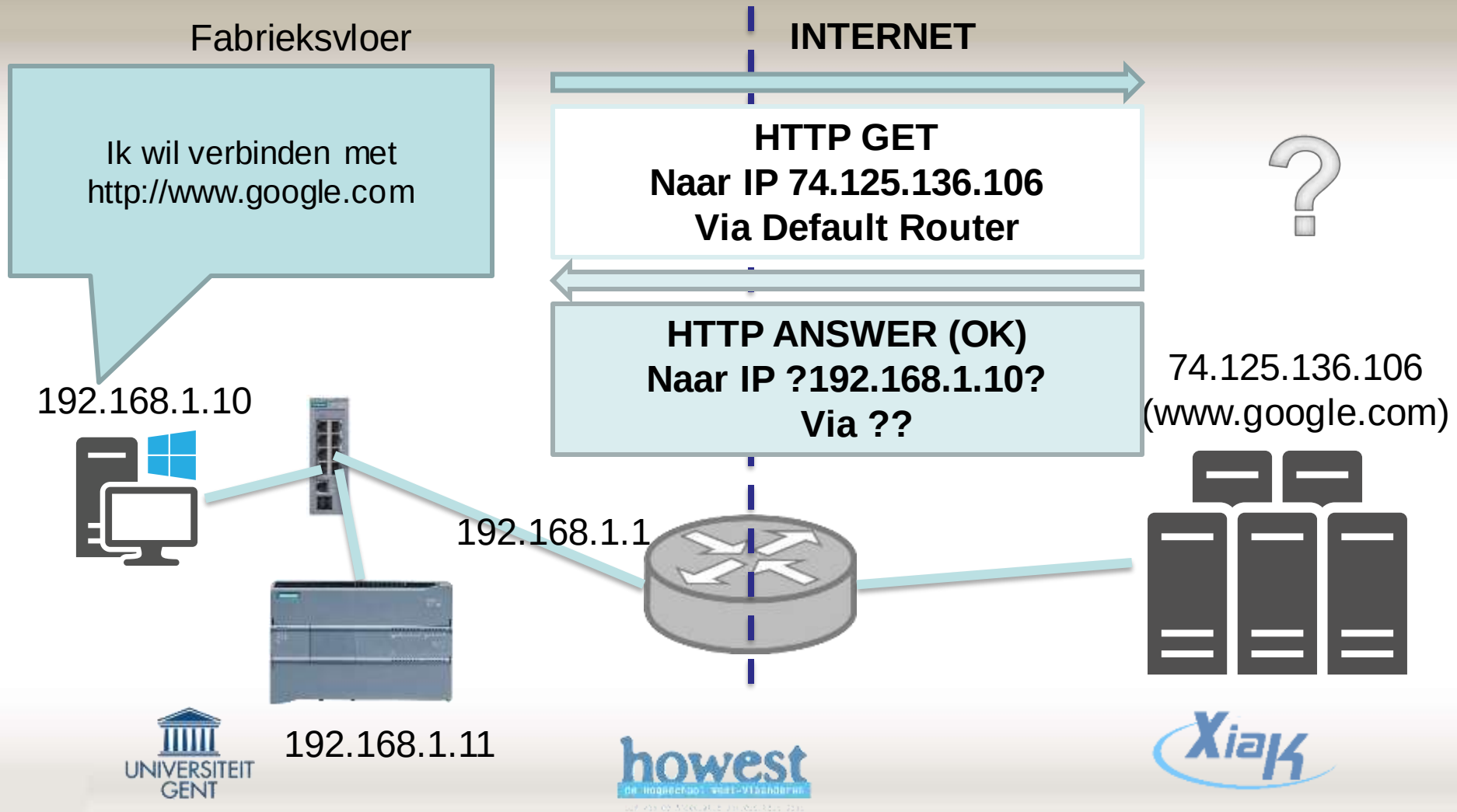
Als een pakket passeert worden de regels afgelopen en de eerste regel die past, wordt toegepast.

Firewall voorbeeld in Windows

It's all about routes



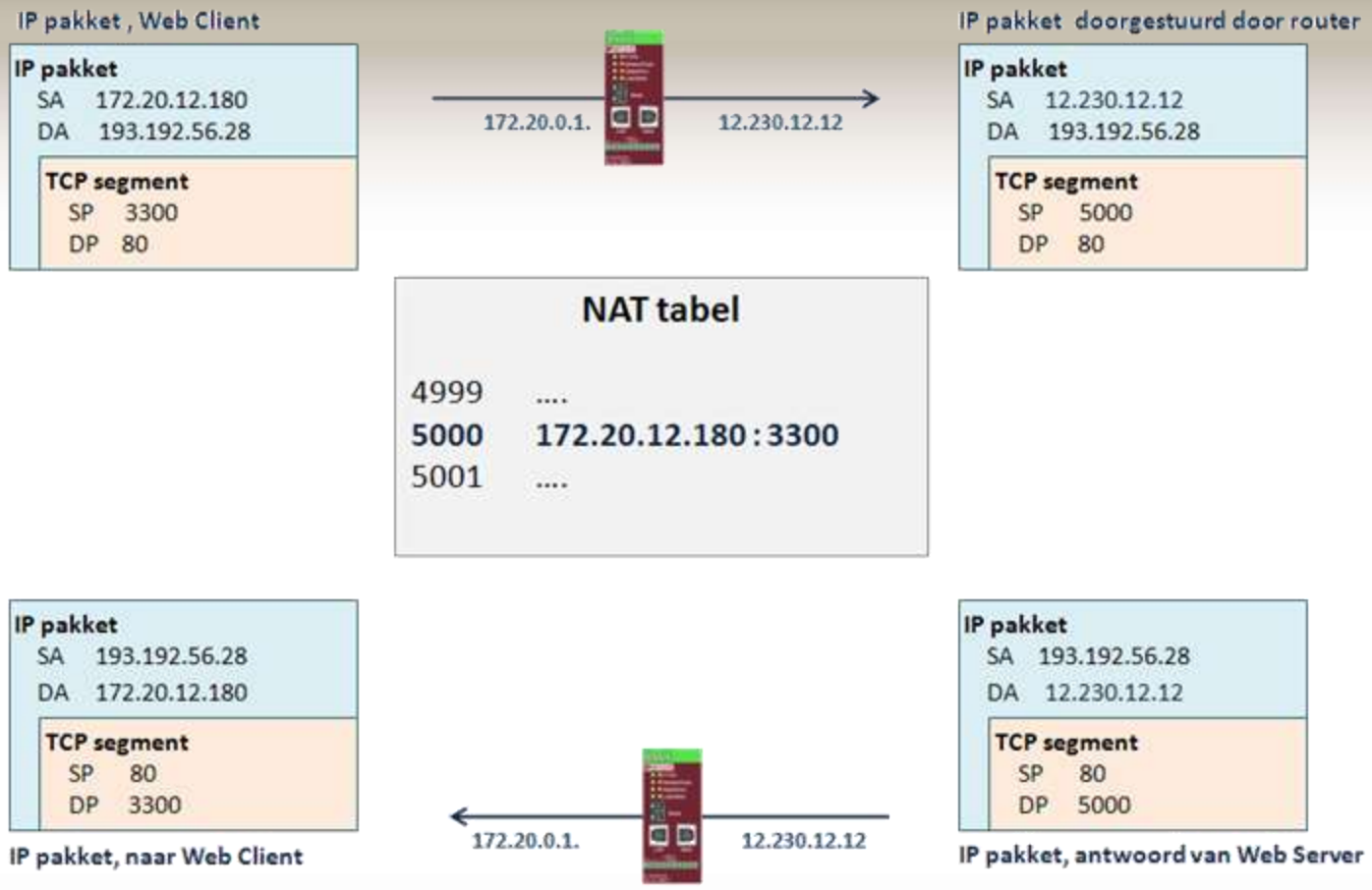
Where it fails (IPv4!)



Network Address Translation

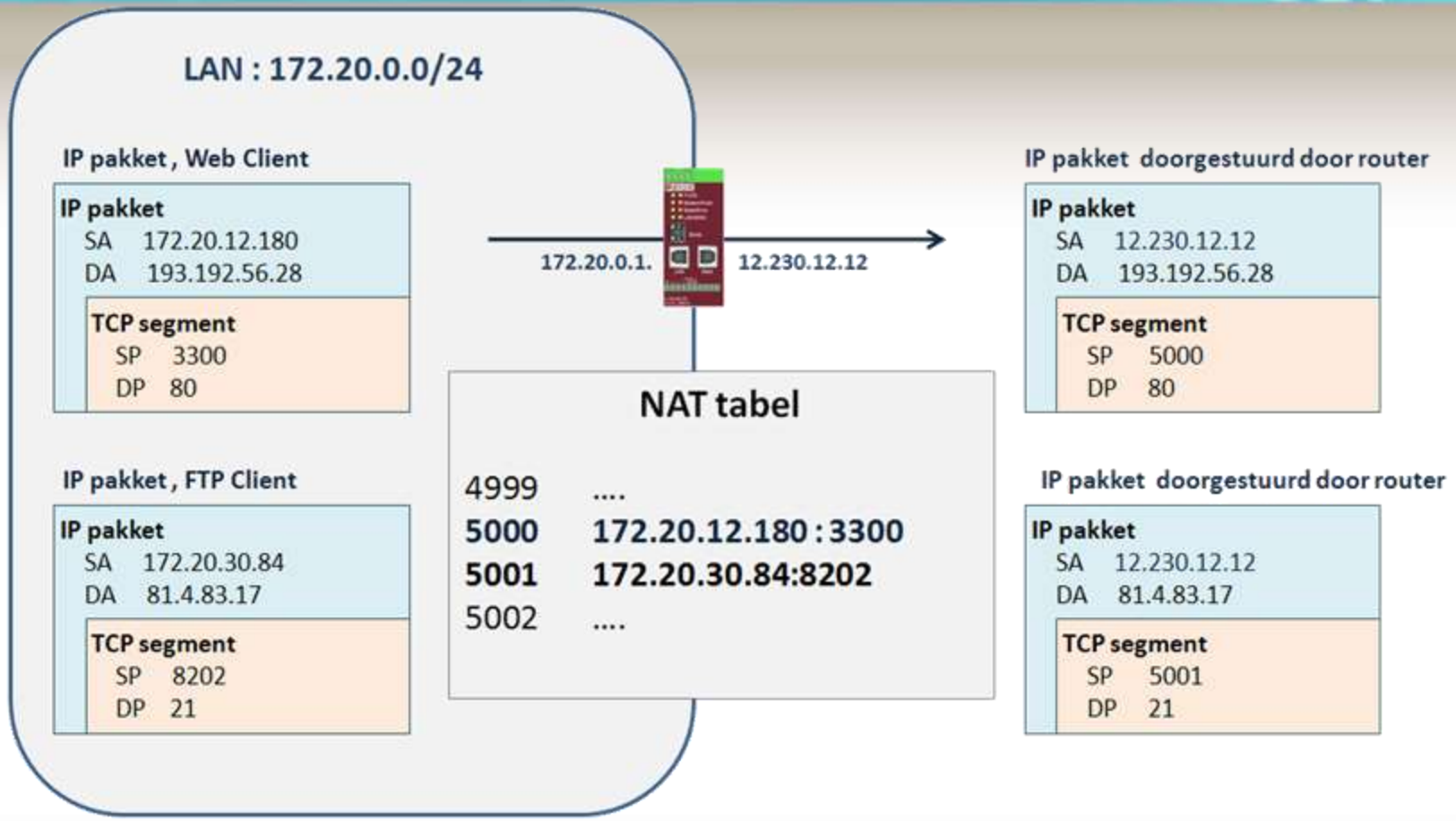
- Network Address Translation (NAT) is **altijd** een functie op **een router**
- Laat toe om een **volledig, uitgebreid, (bedrijfs-)netwerk** toegang te geven tot een ander netwerk **via één of meer eigen IP adressen**
  - In de meest simpele vorm: WAN is één IP adres, LAN is het interne netwerk
- Een NAT router heeft altijd een binnen- en buitenkant (WAN & LAN)
- Anders gezegd:
  - Switches wijzigen niks in de pakketten
  - Routers wijzigen de doel MAC adressen (o.a.)
  - NAT routers wijzigen ook **bron IP adressen en bron poorten** (bij het NAT'en)

NAT - Voorbeeld



UNIVERSITEIT GENT howest XiaK

NAT Voorbeeld



UNIVERSITEIT GENT

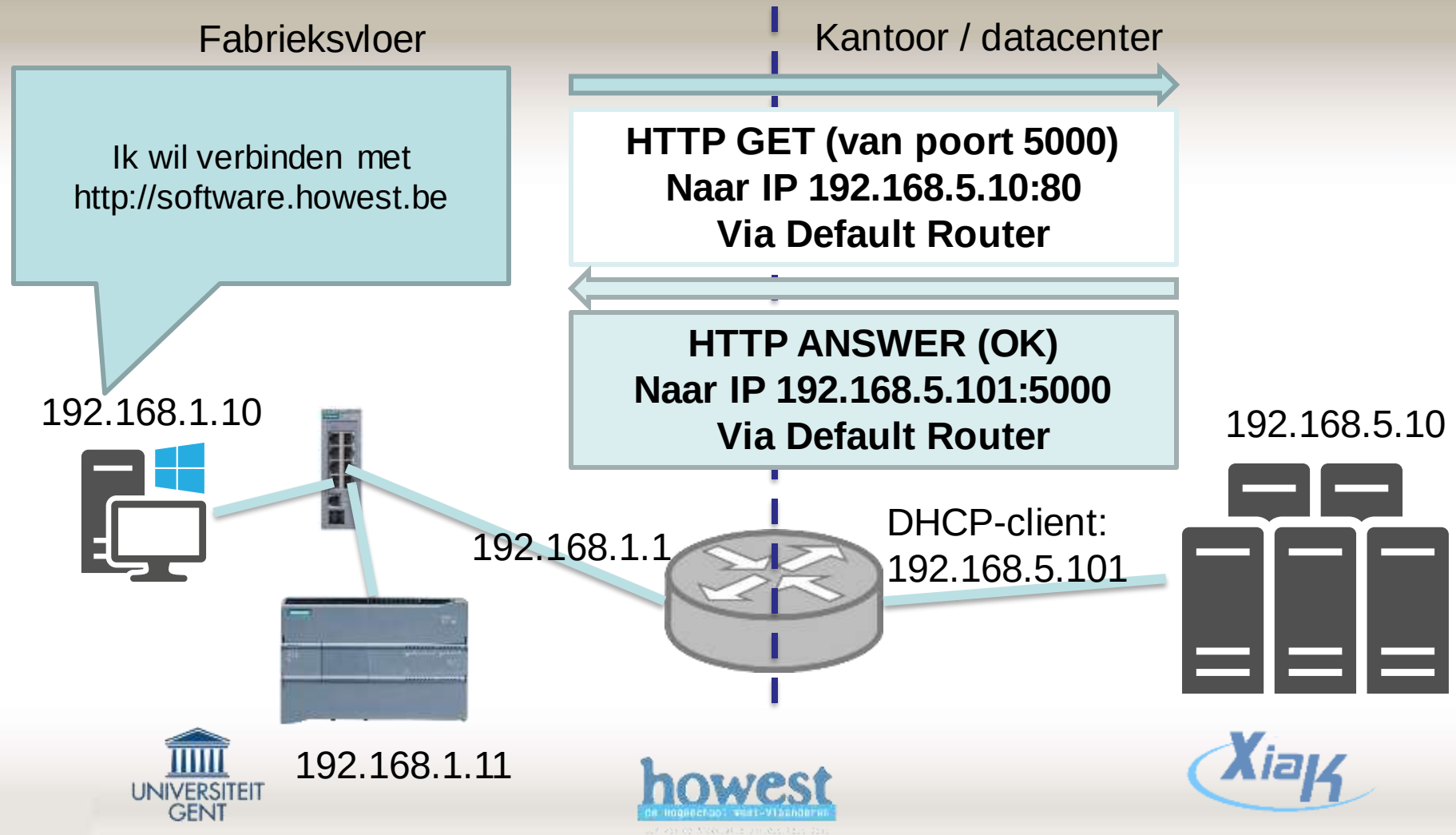
howest

XiaK

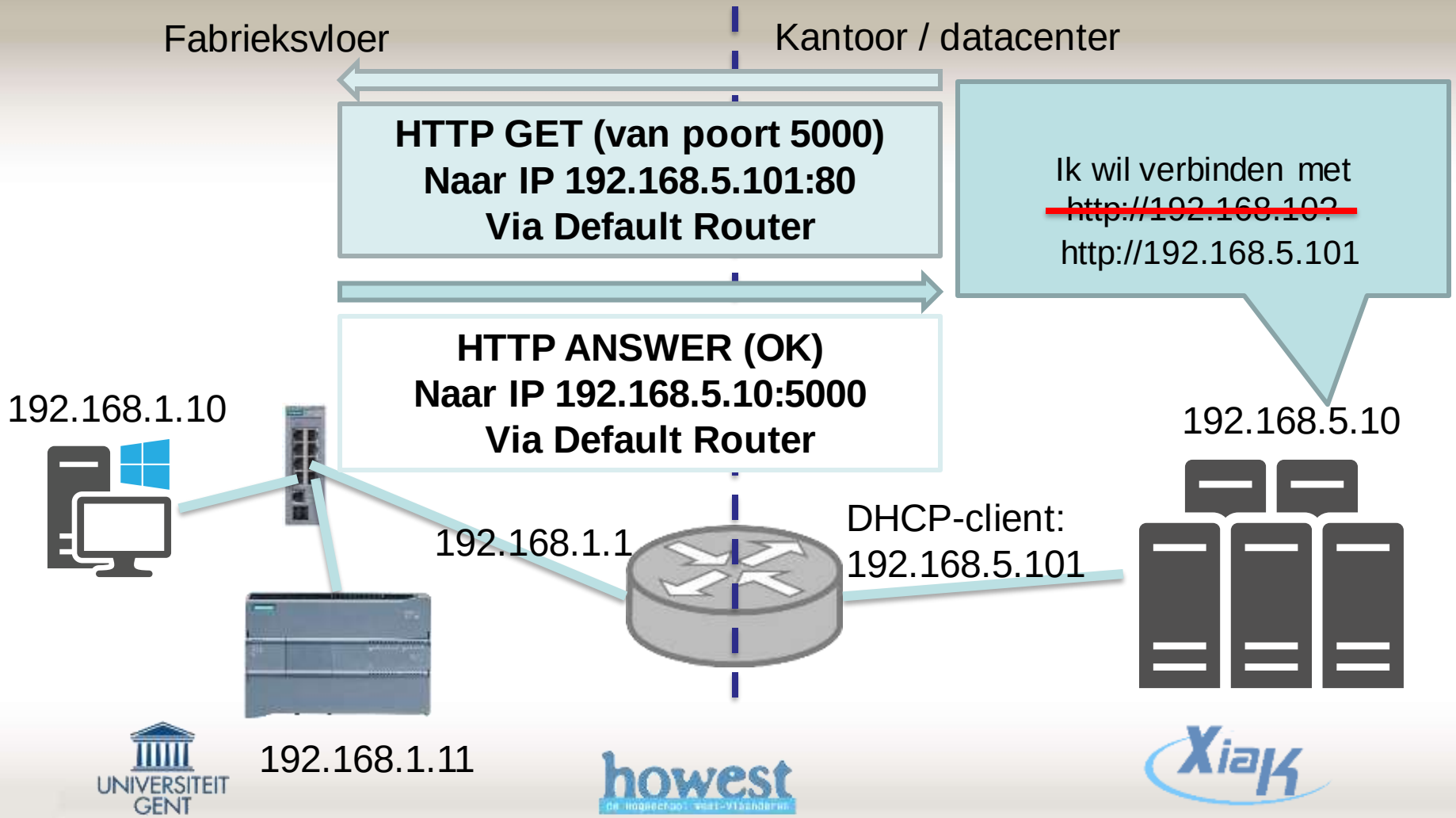
Soorten NAT?

- Single NAT: LAN 192.168.0.0/24 | WAN 12.13.14.15/32
  - Dus de NAT router gebruikt Source Ports in de NAT tabel
  - Cisco noemt dit daarom PAT, Port Address Translation
- Range NAT: LAN 192.168.0.0/24 | WAN 12.13.14.0/24
  - Dus de NAT router koppelt 1 LAN IP aan 1 WAN IP
  - Cisco noemt dit Static Address Translation
- Overload NAT: LAN 192.168.0.0/24 | WAN 12.13.14.0/26
  - Dus méér interne dan publieke adressen, als de *pool* opgebruikt is kan niemand naar buiten verbinden

NAT voorbeeld



Router Functie: Port Forwarding



NAT & Port Forwarding

Packet Tracer Demo

het thuisnetwerk

Real Life Demo's

Het configureren van toestellen,
zowel industrieel als niet-industrieel

IP instellen, DNS, DHCP, Firewall …

- Linksys WRT54GL
- PhoenixContact TC mGuard RS4000
- Siemens Scalance S623

VLAN / Virtual LANs

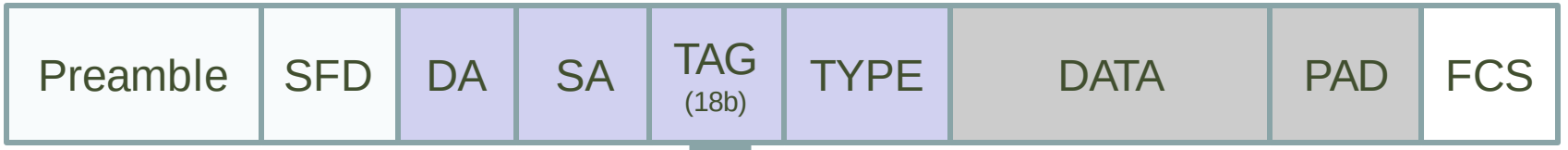
- Een VLAN is een *broadcast* domein, waarbinnen toestellen kunnen communiceren
  - Tussen VLANs is standaard geen communicatie mogelijk, tenzij via (InterVLAN) routering
  - Bekend bij IEEE als 802.1Q
- Niet fysisch maar virtueel
- **VLAN is een concept tussen SWITCHES**

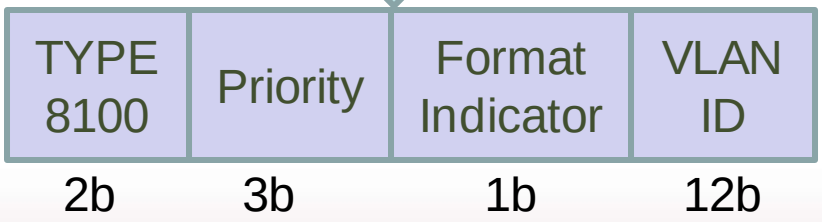
VLAN-Tagging

- VLAN is **segmentatie** op **Layer 2**

Untagged Pakket (van Switch naar toestel)

Tagged Pakket (802.1Q Tagging, van Switch naar Switch)





VLAN ID = 12 bits = 2^12 = 4096

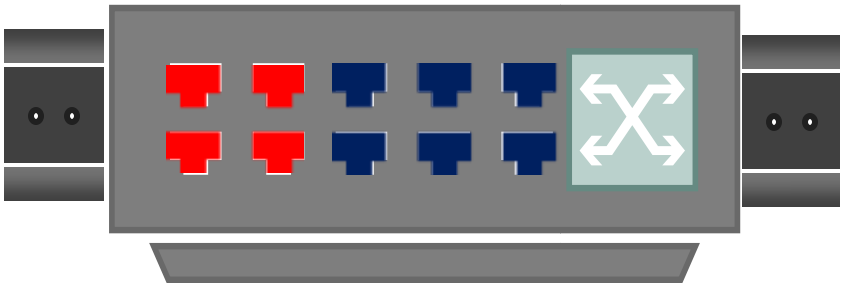
UNIVERSITEIT GENT

howest

XiaK

Tagged of Untagged?

- De VLAN regel luidt:
  - verkeer naar eind devices (PLC's, Computers, Smartphones …) zijn altijd **untagged** frames
  - verkeer tussen switches **kan** via tagged frames
- VLAN tagging wil zeggen, de frames voorzien van een VLAN ID (0-4095)
- Simpel VLAN voorbeeld, één switch:



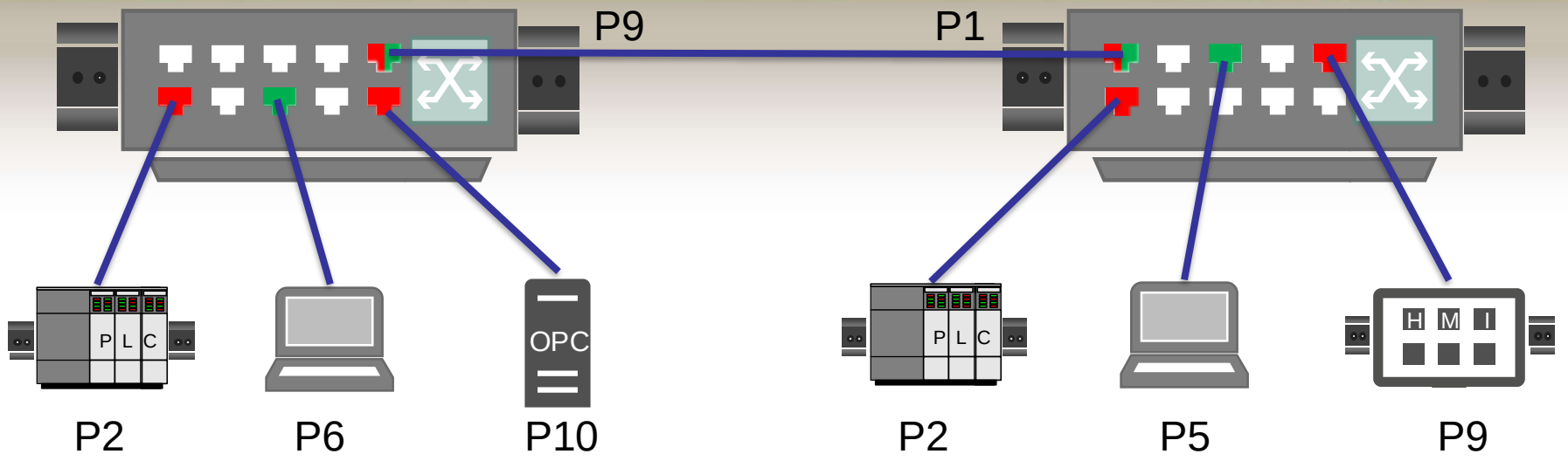
- Standaard: alle 10 poorten = VLAN ID 1
- We configureren:
  - Poorten 1 - 4 = VLAN ID 5
  - Poorten 5-10 = VLAN ID 1
  - **Allemaal untagged**

Dit is ook gekend als **Port Based VLANs**:
afhankelijk waar uw het toestel inplugt komt u op een ander netwerk terecht

UNIVERSITEIT GENT howest XiaK

VLANs over meerdere switches

Doel: Alle PLC's en HMI's in één netwerk



We configureren op Switch1:

- P2 en P10 in VLAN ID 5
- P6 in VLAN ID 10
- **P9 in VLAN ID 5 én 10**

We configureren op Switch2:

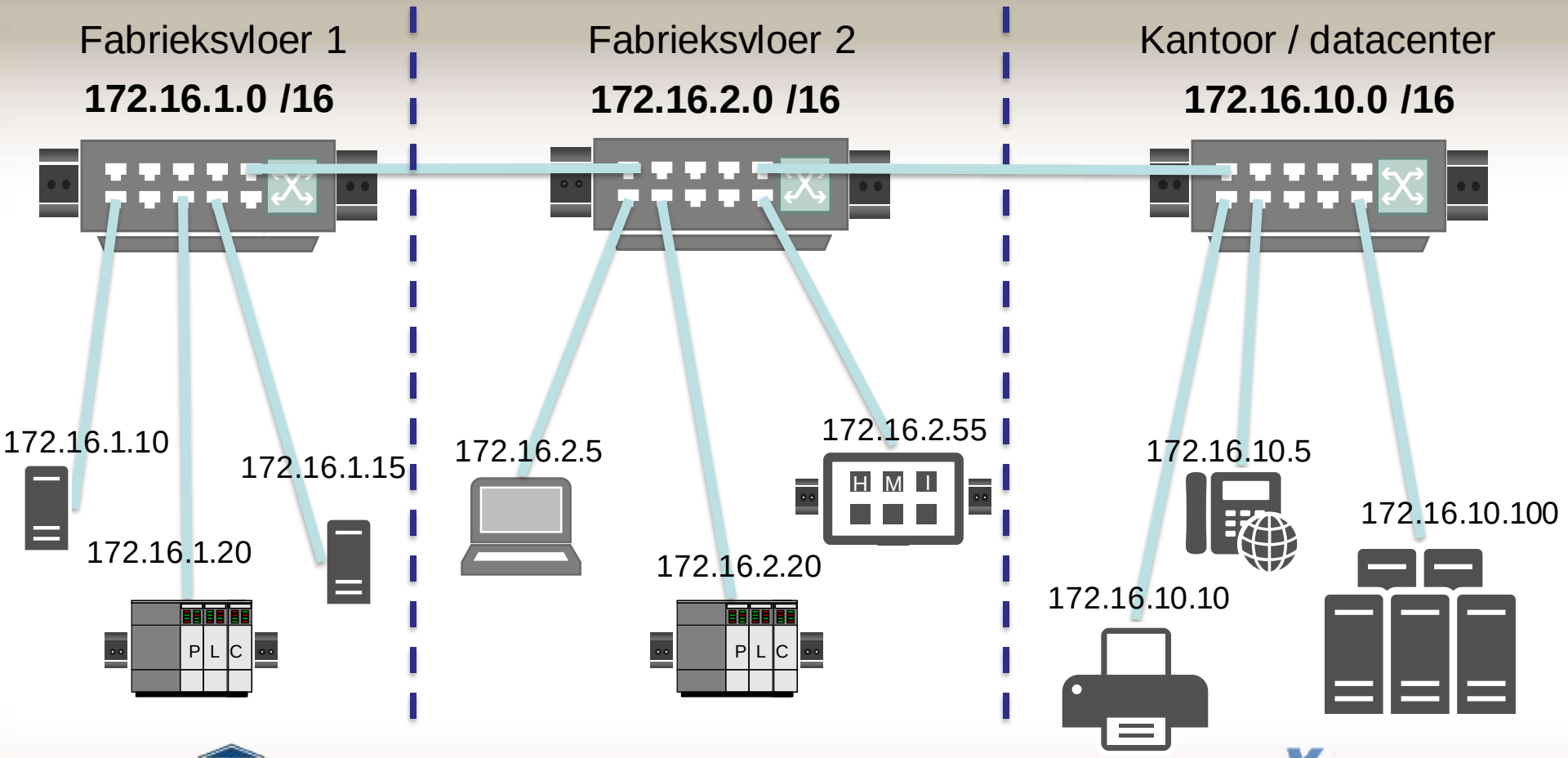
- P2 en P9 in VLAN ID 5
- P5 in VLAN ID 10
- **P1 in VLAN ID 5 én 10**

Tussen P9 en P1 bevindt zich **tagged VLAN verkeer**.
Een link met meerdere VLAN IDs is een **VLAN TRUNK**

UNIVERSITEIT GENT howest XiaK

Uitgebreid netwerk voorbeeld

172.16.0.0 /16



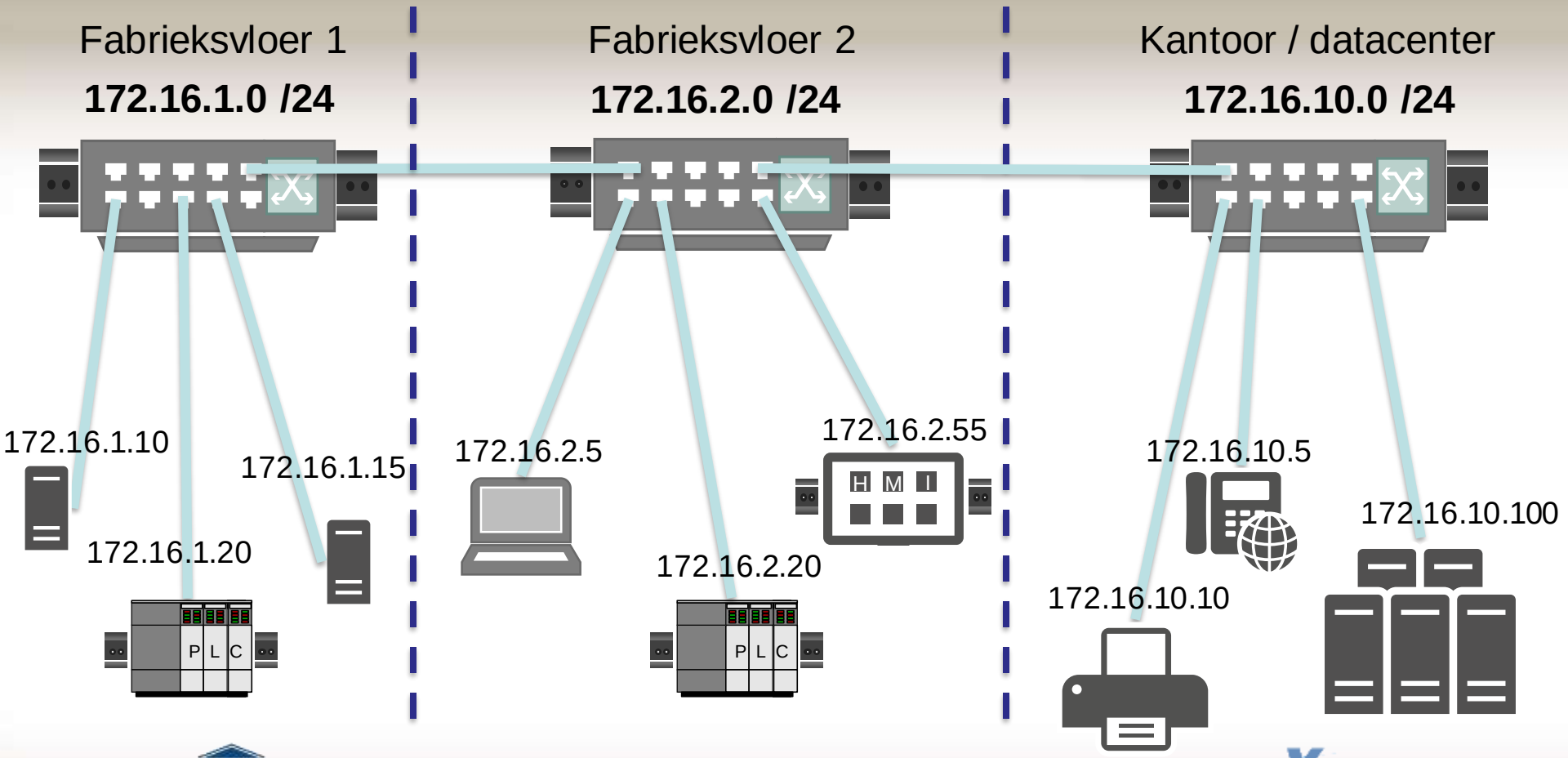
UNIVERSITEIT GENT

howest

Xiak

Uitgebreid netwerk voorbeeld

172.16.0.0 /16 maar nu mét subnets



UNIVERSITEIT GENT

howest

Xiak

Real Life Demo's

Het configureren van toestellen,
zowel industrieel als niet-industrieel

Configuratie van VLAN in een mini-netwerk

- Cisco Layer3 Switch / Router
- Siemens Scalance X308
- PhoenixContact TC mGuard RS4000