

# **LAN-WAN verbindingen**

# Router/firewall

## ■ Router

- ◆ LAN-LAN LAN-WAN
- ◆ Verschil Cisco, ADSL, PC router
  - Aantal gebruikers
  - Hardware instructies
  - Fail-proof
  - Verbruik

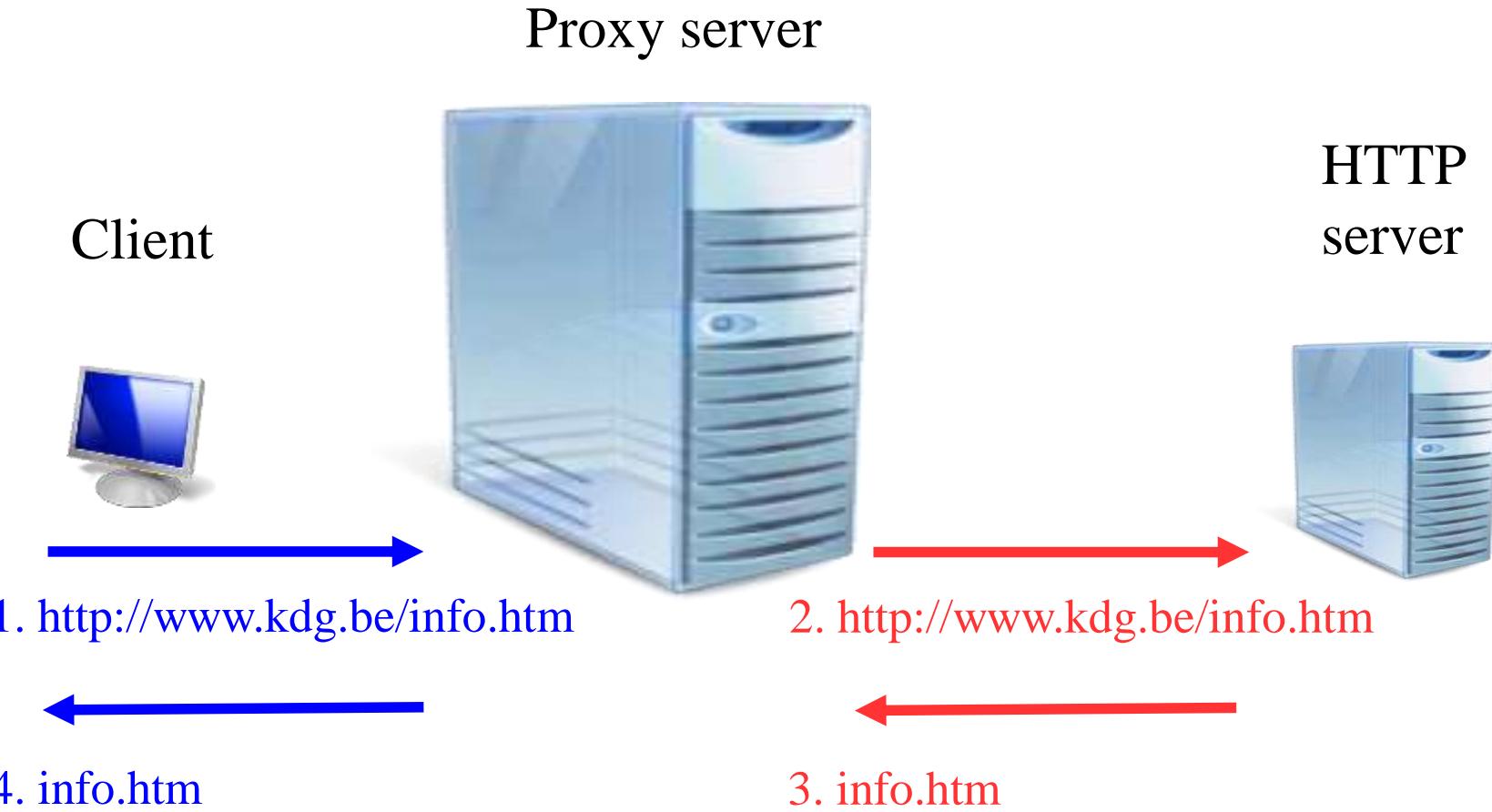
## ■ Firewall

- ◆ Blokkeren/toelaten poorten ip adressen
- ◆ Firewall box - PC firewall

## Traditionele proxy

- Voert diensten uit voor interne LAN gebruikers en beperkte diensten extern (HTTP accelerator)
- Firewallfunctie door gescheiden LAN en WAN verkeer
- Eigenschappen
  - ◆ Proxydienst voor http, ftp,...
  - ◆ Browser instellen voor gebruik proxy op poort 8080
  - ◆ DNS moet niet intern draaien, ook niet op proxy
  - ◆ Default gateway moet niet geconfigureerd zijn

# Traditionele proxy

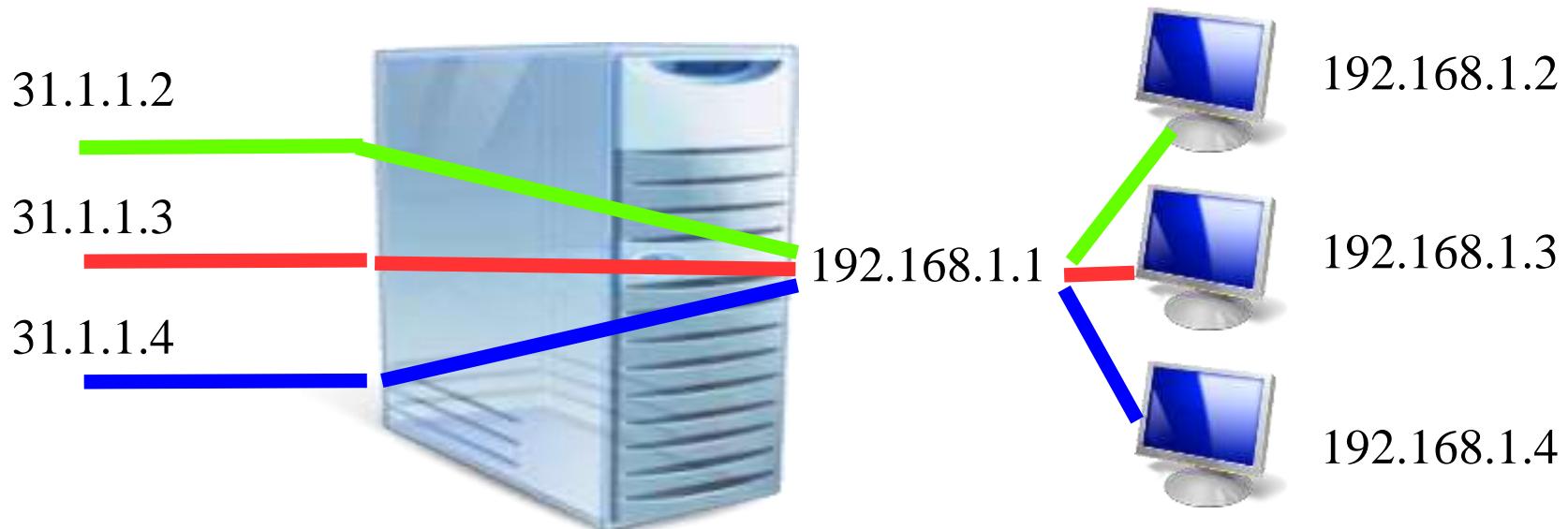


# Transparante proxy

- **Onzichtbare proxy. Clients denken dat ze gewoon via een router werken. Eigenlijk is je machine router én proxy. Je router geeft alles door aan de proxy.**
- **Eigenschappen**
  - ◆ Aanvragen op poort 80 geef je intern door aan poort 8080 (je eigen proxy)
  - ◆ Browser moet direct (niet via proxy) ingesteld worden
  - ◆ Er draait op de proxy een DNS server voor je clients
  - ◆ Je moet een default gateway instellen

# NAT

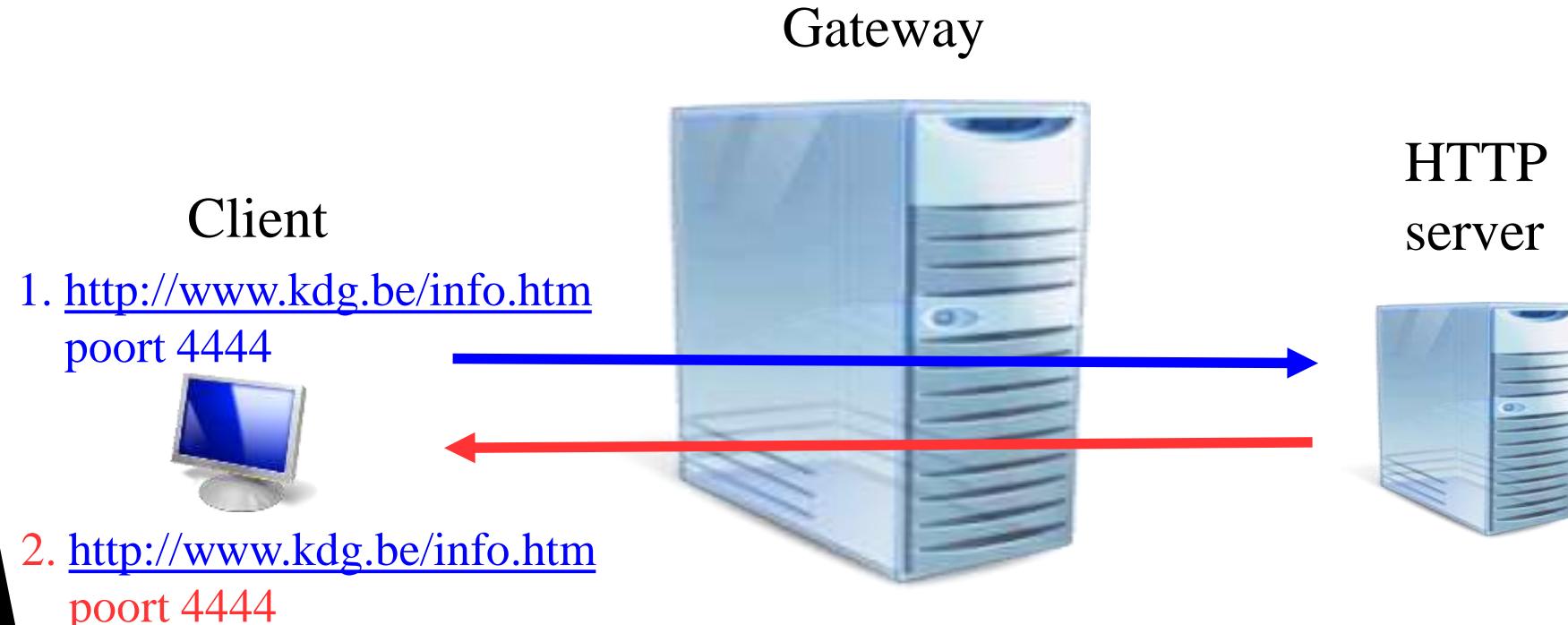
- Network Address Translation
- Externe IP's doormappen naar interne IP's
- Elke PC krijgt een uniek adres



# NAPT of masquerading

- **Network Address Port Translation**
- **Herschrijven van pakketten, wanneer deze door de firewall komen. (Niet nieuwe verbinding openen zoals bij proxy)**
- **Eigenschappen**
  - ◆ Browsers moeten direct verbinden (niet via proxy)
  - ◆ Verschillende modules doen dit voor ftp, real-audio,...
  - ◆ DNS moet intern werken en de firewall moet als default gateway ingesteld staan

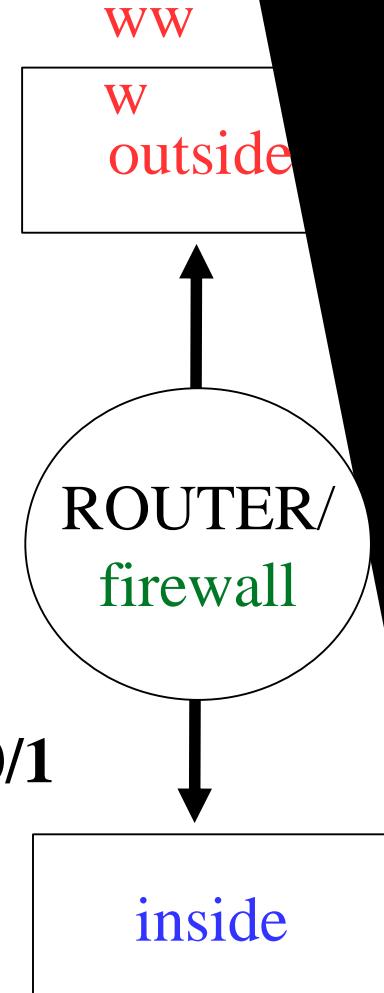
# NAPT



Onderscheid tussen verbindingen door poortnummers te onthouden

# Cisco router met NAT

- interface FastEthernet0/1
- ip address 202.17.164.50 255.255.252.0
- ip nat outside
- interface FastEthernet0/0
- ip address 192.168.1.254 255.255.255.0
- ip nat inside
- ip nat inside source list 1 interface FastEthernet0/1
- ip route 0.0.0.0 0.0.0.0 FastEthernet0/1
- access-list 1 permit 192.168.1.0 0.0.0.255
- access-list 102 permit tcp any any eq www
- access-list 102 permit icmp any any



## De andere richting: Port forwarding

Port forwarding

Interne HTTP server

2. <http://192.168.1.1/info.htm:80>



Client



1. <http://www.kdg.be/info.htm>

4. <http://www.kdg.be/info.htm>

3. <http://192.168.1.1/info.htm:80>

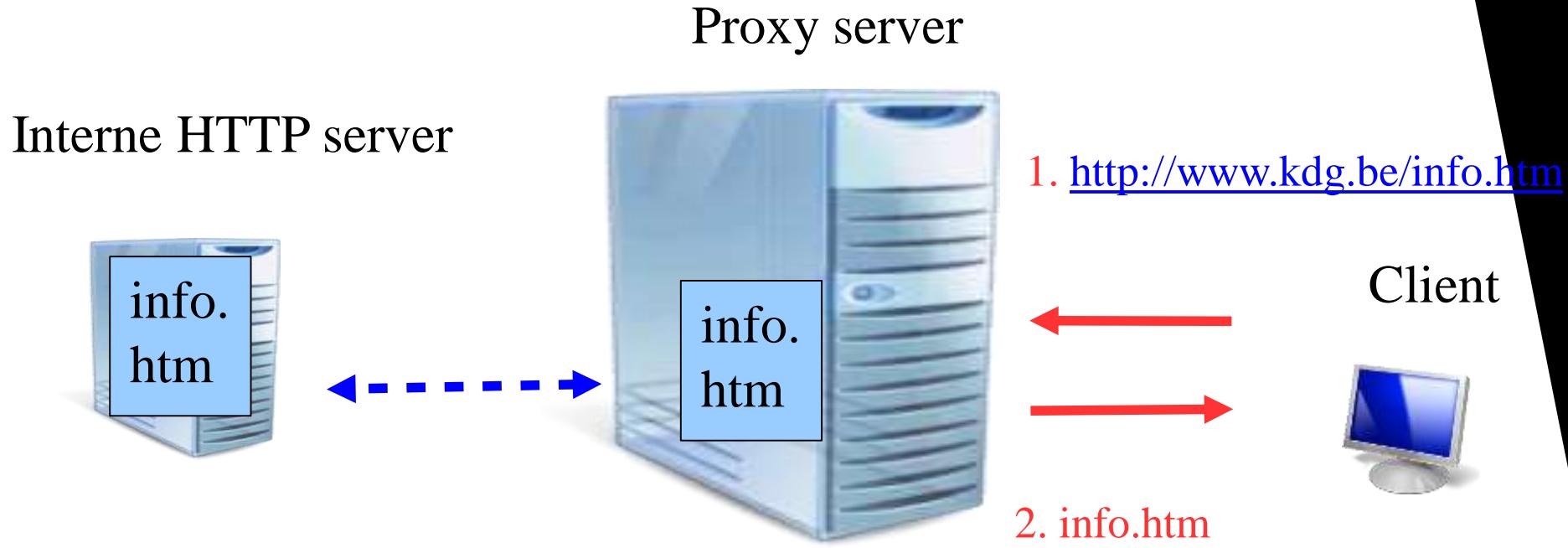


Externe ip/poort doorsturen naar interne server/poort

## De andere richting: HTTP accelerator

- **De proxy doet dienst als een front-end voor webservers op het lokale netwerk. Door een HTTP accelerator te gebruiken kunnen we het verkeer op een lokaal netwerk ontlasten.**
  - ◆ Statische pagina's worden vanuit de cache gegeven (geen interne netwerkconnectie)
  - ◆ Dynamische pagina's worden opgehaald (wel een netwerkconnectie nodig)

# De andere richting Reverse Proxy/HTTP accelerator



Voordeel: Kan meer dan 1 interne server zijn  
Proxy kan ook verkeer filteren

# TCP/IP inleiding

# OSI applicatielaag

- TELNET poort 23
- FTP File Transfer poort 21 controle/poort 20  
data
- TFTP Trivial FTP met UDP
- SMTP Simple Mail Transfer
- SNMP Simple Network Management
- HTTP Hypertext Transfer
- DHCP Dynamic Host Configuration

# OSI presentatie

- **Tekst / Prentjes / Geluid / Film weergeven**
  - ◆ TXT/DOCX/ODF/XML/JPG/GIF/Flash/Quicktime
- **Encryptie / Decryptie**

# OSI sessielag

- **Controle dialoog tussen computers**
- **Opzetten van verschillende sessies tegelijk**
- **Starten/stoppen van een sessie**
  - ◆ NFS Network File System (file share Unix)
  - ◆ RPC Remote procedure Call (file share MS Windows)
  - ◆ SQL Structured Query Language (sessies naar DB)

# OSI transportlaag

- **foutafhandeling**
- **TCP betrouwbaar (Transmission Control)**
  - ◆ Opzetten verbinding (SYN)
  - ◆ Ontvangsbevestiging (ACK)
  - ◆ FTP, telnet, HTTP
- **UDP onbetrouwbaar (User Datagram)**
  - ◆ TFTP, SNMP, DNS, RIP

# OSI netwerklaag

- Juiste pad tussen systemen
- Uniek IP adres

# OSI datalinklaag

- MAC adres
- frames in juiste volgorde

# OSI fysische laag

- Elektrische specificaties (spanning, wat is 1 en wat is 0)
- Frequenties/golven

# Overzicht lagen

- Applicatielaag, Presentatielaag, Sessielaag: **DATA**
- Transportlaag: De data wordt in **SEGMENTEN** gekapt en krijgt een TCP header met poortnummer
- Netwerklaag: De segmenten krijgen een IP header met twee IP-nummers van de bron en doelcomputer. Hier spreekt men van een **PAKKET**
- Datalinklaag: Hier worden pakketten in een **FRAME** gebracht. Een frame werkt met 48bit MAC adressen
- Fysische laag: Hier stromen de frames door met nullen en enen, die worden weergegeven door bepaalde spanningen over de draad te sturen

- **Applicatielaag, Presentatielaag, Sessielaag**

- **Data**

- .....

# Transportlaag

## ■ Segmenten

.... .... .... .... .... ....

- TCP header BronPoort, Doelpoort,
- Volgnr, ACKnr, Windowsize, Controlesom
- T.... T.... T.... T.... T.... T....

# Transportlaag

## ■ Poortnummers

Client

----->

Server

IP 172.17.167.150

172.17.164.31

mask 255.255.0.0

255.255.0.0

poort **2145**

**80**

(**>1024**)

# Netwerklaag of IP laag

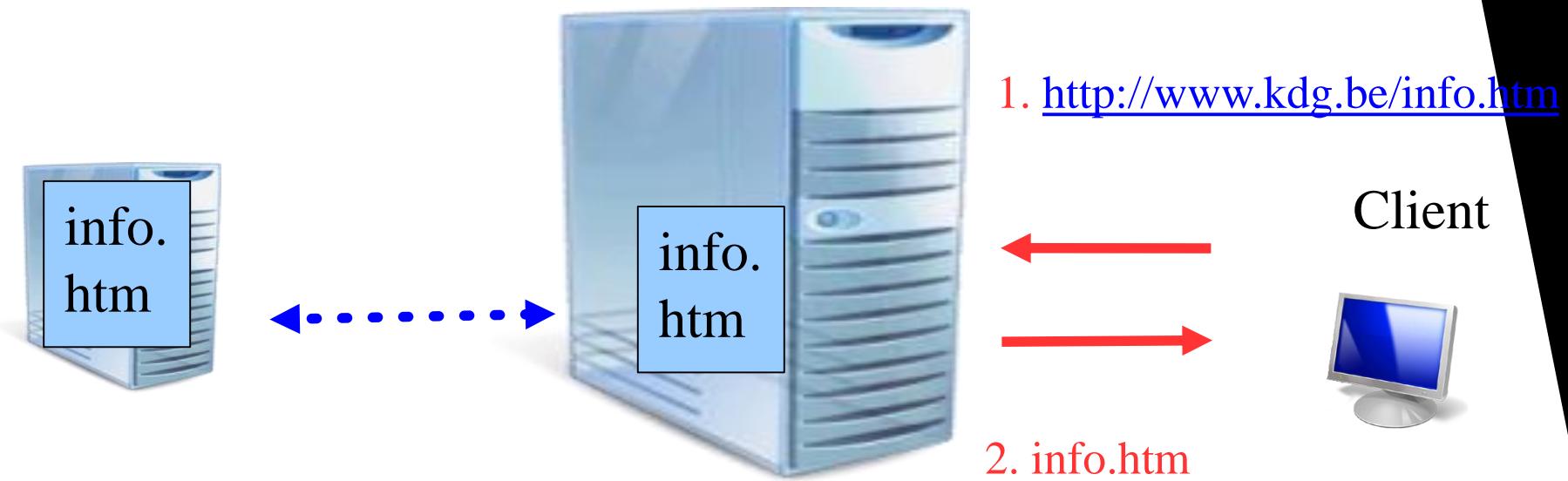
- Pakket
- Header met BronIP, Doel IP  
IT.... IT.... IT.... IT.... IT.... IT....

# Datalinklaag

- Ethernet Frames
- Header met 48bit uniek MAC adres voor bron en voor doel
- Controlesom
- EIT....C   EIT....C   EIT....C   EIT....C   EIT....C   EIT....C

# Nodig voor een pakket

- **1. Poortnummer van de client: > 1024**
- **2. IP adres van de client: Fixed of DHCP**
- **3. MAC adres van de client:**
  - ◆ Uitgelezen uit de netwerkkaart (kan je zelf met ipconfig /all)
- **4. Poortnummer van de server**
  - ◆ Well-known poortnummer HTTP 80
- **5. IP adres van de server:**
  - ◆ DNS vertaalt naam een IP adres.
- **6. MAC adres van de server:**
  - ◆ ARP, router



Vyos

**Vyatta**

**Vyos**

**DANOS**

# Wat is Vyos?

- **Open source routing software**
- **Draait op een debian based systeem**
- **CLI gebaseerd op Juniper OS (JunOS)**
- **Ondersteunt onder andere:**
  - ◆ Routing: RIPv2, OSPF, BGP
  - ◆ Frame Relay, PPP encapsulatie
  - ◆ NAT, DHCP en DHCP relay
  - ◆ Redundancy (VRRP)
  - ◆ Statefull firewall, tcpdump



# Vyos geschiedenis

## ■ Tot in 2014 Vyatta

- ◆ Hardware boxes
- ◆ Open source Community



## ■ Opgekocht door Brocade

- ◆ Geen ondersteuning open source
- ◆ Gebruiken vyatta niet
- ◆ Nieuwe Open source variant VyOS
- ◆ Ubiquity networks verkoopt EdgeOS boxes

**BROCADE®**



## ■ In 2018 opgekocht door AT&T

- ◆ Terug open source project "DANOS"  
<https://www.danosproject.org/>



# Download

## ■ Rolling release

- ◆ <https://downloads.vyos.io/?dir=rolling/current/amd64>



# Installatie

- **Boot van de iso**
  - ◆ Schijf min. 4GB, kies Debian 64bit, minimum 2G RAM
- **Inloggen met vyos/vyos (opgepast qwerty!)**
- **Start het programma: install image**
- **Reboot**
- **Start op met de KVM console**
- **Inloggen met user vyos en paswoord gekozen tijdens install**

# Vyos CLI

## ■ Operational mode

- ◆ Status opvragen (vooral show commando)
- ◆ vyos@vyos:~\$

## ■ Configuration mode

- ◆ vyos@vyos:~\$ **configure**
- vyos@vyos:~# **exit**
- ◆ vyos@vyos:~\$

## ■ Voor exit doe je

- ◆ "discard" om geen wijzigingen door te voeren
- ◆ "commit" om wel wijzigingen door te voeren

# Configuratie interfaces

## ■ DHCP

- ◆ configure
- ◆ **set** interfaces ethernet eth0 address dhcp
- ◆ commit
- ◆ save

## ■ Fixed IP

- ◆ configure
- ◆ **set** interfaces ethernet eth1 address 192.168.56.192/24
- ◆ commit
- ◆ save

# Aanrader: configureer SSH

- **Het keyboard via een ssh client geeft het juiste keyboard**
  - ◆ configure
  - ◆ set interfaces ethernet eth1 address 192.168.56.192/24
  - ◆ set service ssh
  - ◆ commit
- **Connecteren met client (kan bv met putty)**
  - ◆ ssh vyos@192.168.56.192
  - ◆ Welcome to vyos
  - ◆ vyos@192.168.56.192's password:
  - ◆ ...
  - ◆ vyos@vyos:~\$ uname -a

# Verwijderen configuratielijnen

- Cisco -> **no ervoor**
- Juniper -> **delete** in plaats van set
- Voorbeeld:
  - ◆ configure
  - ◆ **delete** interfaces ethernet eth0 address DHCP
  - ◆ commit
  - ◆ save

# Bewaren/ophalen configuratie

- Het **save** commando bewaart de config default in:
  - **/opt/vyos/etc/config/config.boot**
- Bewaren op een ftp server:
  - ◆ save ftp://kdguntu:supersecret@192.168.56.1/config.txt
- Inladen vanuit ftpserver:
  - ◆ load ftp://kdguntu:supersecret@192.168.56.1/config.txt
- Overpompen naar usb
  - ◆ mount /dev/sdb1 /mnt -t vfat # mounten usb stick
  - ◆ cp /config/config.boot /mnt # copieren config
  - ◆ umount /mnt # unmount

# Enkele show commando's

- Sommige van deze commando's werken zowel in configuratie als operator modus en geven daar verschillende resultaten:
  - ◆ show configuration
  - ◆ show interfaces
  - ◆ show ip route
  - ◆ show nat
  - ◆ show firewall

# Routering

## ■ Statisch

- ◆ set protocols static route 0.0.0.0/0 next-hop 192.168.56.1 distance '1'

## ■ Met RIP

- ◆ set interfaces loopback lo address 1.1.1.1/32
- ◆ set protocols rip network 192.168.0.0/24
- ◆ set protocols rip redistribute connected

# Firewall out

- **HTTP server mag**
- **set firewall name INSIDE-OUT default-action drop**
- **set firewall name INSIDE-OUT rule 10 action accept**
- **set firewall name INSIDE-OUT rule 10 protocol tcp**
- **set firewall name INSIDE-OUT rule 10 destination port 80**
  
- **set interfaces ethernet eth1 firewall out name INSIDE-OUT**

# Firewall in

- Terugkerend verkeer mag
- **set firewall name OUTSIDE-IN default-action drop**
- **set firewall name OUTSIDE-IN rule 100 action accept**
- **set firewall name OUTSIDE-IN rule 100 state established enable**
  
- **set interfaces ethernet eth1 firewall in name OUTSIDE-IN**

# Hints

- **Gebruik <TAB> om je commando's met autocomplete aan te vullen!**
- **Wanneer je een configuratie copieert naar een nieuwe machine gooi je bij de interfaces de lijnen met hw-id weg**
  - ◆ Het nieuwe mac adres wordt vanzelf ingevuld (anders maakt vyos extra interfaces)
- **Linux commando's (cat en | en >) werken alleen maar in de Operator modus (met \$ prompt) en niet in de configuration modus (met # prompt)**
- **Operator modus commando's vanuit configuratie modus doe je met run ervoor. Bijvoorbeeld:**

# Andere commando's

## ■ Niet bewaren wijzigingen

- ◆ exit discard

## ■ Instellen nieuw paswoord voor vyos

- ◆ configure
- ◆ set system login user *vyos* authentication plaintext-password *supersecret007*
- commit

## ■ Bewaren alle configuratie commando's in een bestand

- ◆ show configuration commands > /tmp/configcmds.txt

# Versiebeheer in Vyos: compare

- **Vergelijken versies met compare**
- vyos@vyos# set system host-name vyos1
- [edit]
- vyos@vyos# set system domain-name kdg.be
- vyos@vyos# compare
- [edit system]
- + domain-name kdg.be
- >host-name vyos1

# Versiebeheer Vyos: rollback

- vyos@vyos# compare 1
- [edit system]
- >host-name vyos1
- [edit]
- vyos@vyos# rollback 1
- Proceed with reboot? [confirm][y]
- Broadcast message from root@vyos1 (pts/0) (Tue Feb 29 23:07:45 2019):

■ The system is going down for reboot NOW!

■ [edit]

Ko<sup>y</sup>os @vyos#

# Hints slitaz

- **Virtueel 3 NICs:**
- **eth0 host-only vboxnet0, eth1 internal, eth2 NAT**
  - ◆ ifconfig eth0 down
  - ◆ ifconfig eth1 192.168.56.2/24
  - ◆ ifconfig eth2 down
  - ◆ route add default gw 192.168.56.1
- **root worden, default paswoord is root**
- **Vergeet de grub bootloader niet te installeren!**

# Referenties

## ■ DANOS

- ◆ <https://www.danosproject.org>

## ■ Vyos Wiki

- ◆ [https://wiki.vyos.net/wiki/User\\_Guide](https://wiki.vyos.net/wiki/User_Guide)

## ■ How Brocade totally missed the boat with vyatta

- ◆ <http://dotbalm.org/brocade-missed-the-boat-with-vyatta/>

# VyOS

## IPv6 configuratie

# Interface configuratie IPv6

## ■ Stateless Autoconfiguration (DHCPv6)

- ◆ set interfaces ethernet eth1 ipv6 address autoconf

## ■ Global address

- ◆ set interfaces ethernet eth1 address  
'2001:1111:1111:4567::1/64'

## ■ EUI address (MAC ingevuld)

- ◆ set interfaces ethernet eth1 ipv6 address eui  
'fc00:1111:1111::/64'

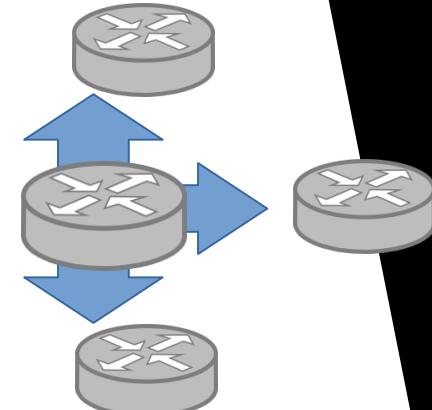
# DHCPv6

- **Opgelet! Dit is GEEN Router Advertisement**
- **DHCPv6 range**
  - set subnet 2001:1111:1111:4567::/64 start 2001:1111:1111:4567::100 stop 2001:1111:1111:4567::200
- **Domain search**
  - set subnet 2001:1111:1111:4567::/64 domain-search kdg.be
- **DNS (google)**
  - set subnet 2001:1111:1111:4567::/64 name-server 2001:4860:4860::8844

# Router Sollicitation /Advertisement

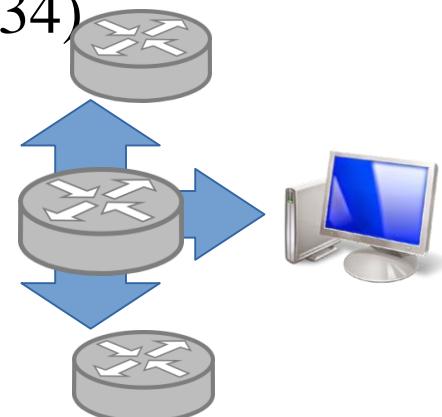
## ■ 1. Router Sollicitation (RS)

- ICMPv6 router sollicitatie bericht (type 133)
- bron is FE80:: met mac adres achteraan
- doel is **All routers multicast address FF02::2**



## ■ 2. Router Advertisement (RA)

- ICMPv6 router ICMPv6 advertisement (type 134)
- bevat IP add, Lifetime
- doel is **All nodes multicast address FF02::1**



# Router Advertisements Flags

- **A-bit – Autonomous Address Autoconfiguration Flag**
  - node moet stateless address assignment doen (RFC 4862)
- **L-bit – On-Link Flag**
  - prefix in de RA is het lokale IPv6 adres
- **M-bit – Managed Address Config Flag**
  - host moet stateful DHCPv6 (RFC 3315) gebruiken
- **O-bit – Other Config Flag**
  - host krijgt nog andere informatie zoals DNS via DHCPv6 (RFC 3736)

# Router Advertisement: Cur Hop Limit

## ■ Vyos: cur-hop-limit

- ◆ 0-255 (8bit)
- ◆ Maximaal aantal routers (hops) dat een pakket mag tegenkomen eer het mag weggegooid worden
- ◆ 0 is ongedefinieerd

# Router Advertisement: "Managed address configuration" flag

- Vyos: managed-flag
  - ◆ true/false
  - ◆ managed betekent dat alle informatie via DHCPv6 verkregen wordt

# Router Advertisement: "Other configuration" flag

## ■ Vyos: other-config-flag

- ◆ true/false
- ◆ True telt niet mee wanneer managed op true staat
- ◆ Extra informatie zoals DNS informatie wordt vanuit DHCPv6 gehaald

# Router Advertisement: Router Lifetime

## ■ Vyos: default-lifetime

- ◆ 0-65535 (16 bit)
- ◆ Aantal seconden dat een router de default router blijft
- ◆ 0 router is geen default router

# Router Advertisement: Reachable Time

## ■ Vyos: reachable-time

- ◆ 32 bit
- ◆ Aantal milliseconden dat verondersteld wordt dat een Neighbour bereikbaar blijft na een bevestiging van bereikbaarheid.
- ◆ 0 is ongedefinieerd

# Router Advertisement: Retrans Timer

## ■ Vyos: retrans-timer

- ◆ 32 bit
- ◆ Tijd tussen heruitzending van Neighbour sollicitations
- ◆ 0 is ongedefinieerd

# Router Advertisement: MTU

## ■ Vyos: link-mtu

- ◆ 32 bit
- ◆ Maximum Transfer Unit geeft het aantal octets aan dat op een link kan worden doorgestuurd (1280 minimum)
- ◆ 0 is ongedefinieerd

# Router Advertisement Prefix: Prefix

## ■ Prefix Length

- ◆ Meestal krijg je van een provider een /48 en geef je aan je clients een /64
- ◆ bv set router-advert prefix 2001:1111:1111:4567::/64

# Router Advertisement Prefix: on-link flag (de L-bit)

## ■ Vyos: on-link-flag

- ◆ true/false
- ◆ De meegegeven adressen zijn beschikbaar op deze link
- ◆ Bij false mag er NIET van uit gegaan worden dat de adressen NIET op de link beschikbaar zijn

# Router Advertisement Prefix: autonomous address-configuration flag

## ■ Vyos: autonomous-flag

- ◆ true/false
- ◆ true: prefix kan gebruikt worden voor stateless autoconfiguration

# Router Advertisement Prefix: Valid Lifetime

## ■ Vyos: valid-lifetime

- ◆ 32 bit
- ◆ Tijd in seconden dat een prefix geldig blijft op een link

# Router Advertisement Prefix: Preferred Lifetime

## ■ Vyos: preferred-lifetime

- ◆ 32 bit
- ◆ Tijd dat een prefix geldig blijft op een link
- ◆ Het verschil met de valid-lifetime is de tijd die kan gebruikt worden om een nieuw adres aan te vragen

# Router Advertisement: Extra Vyos opties

## ■ Vyos: default-preference

- ◆ low, medium of high
- ◆ Voorrang voor de router
- ◆ set interfaces ethernet eth0 ipv6 router-advert default-preference high

# Router Advertisement: Extra Vyos opties

## ■ Vyos: name-server

- ◆ set interfaces ethernet eth0 ipv6 router-advert  
2001:1111:1111:4567::/64 name-server  
2001:4860:4860::8888

# Router Advertisements ontvangen

Als root op vyos volgende kernel-parameter instellen:  
`sysctl -w net.ipv6.conf.eth0.accept_ra=2`

# Referenties

- <https://wiki.vyos.net/wiki/IPv6>
- [https://wiki.vyos.net/wiki/IPv6\\_Router\\_Advertisements](https://wiki.vyos.net/wiki/IPv6_Router_Advertisements)
- <https://tools.ietf.org/html/rfc4861#section-4.2>

# **Netwerken 3**

## **Firewalls**

## Firewalls



# Standaard TCP/IP pakket

## ■ Bron\_IP

- ◆ DHCP/Fixed

## ■ Bron\_Poort

- ◆ "random"
- ◆ gt 1023

## ■ Bron\_Mac

- ◆ Ingebakken in kaart

## ■ Doel\_IP

- ◆ DNS

## ■ Doel\_Poort

- ◆ Well-known: 80, 21,..
- ◆ lt 1023

## ■ Doel\_Mac

- ◆ binnen LAN: ARP
- ◆ buiten LAN: Mac gateway

# Standaard TCP conversatie opstarten

## ■ Client

- ◆ verbinding aanvragen
- ◆ SYN --->
- ◆ ACK --->

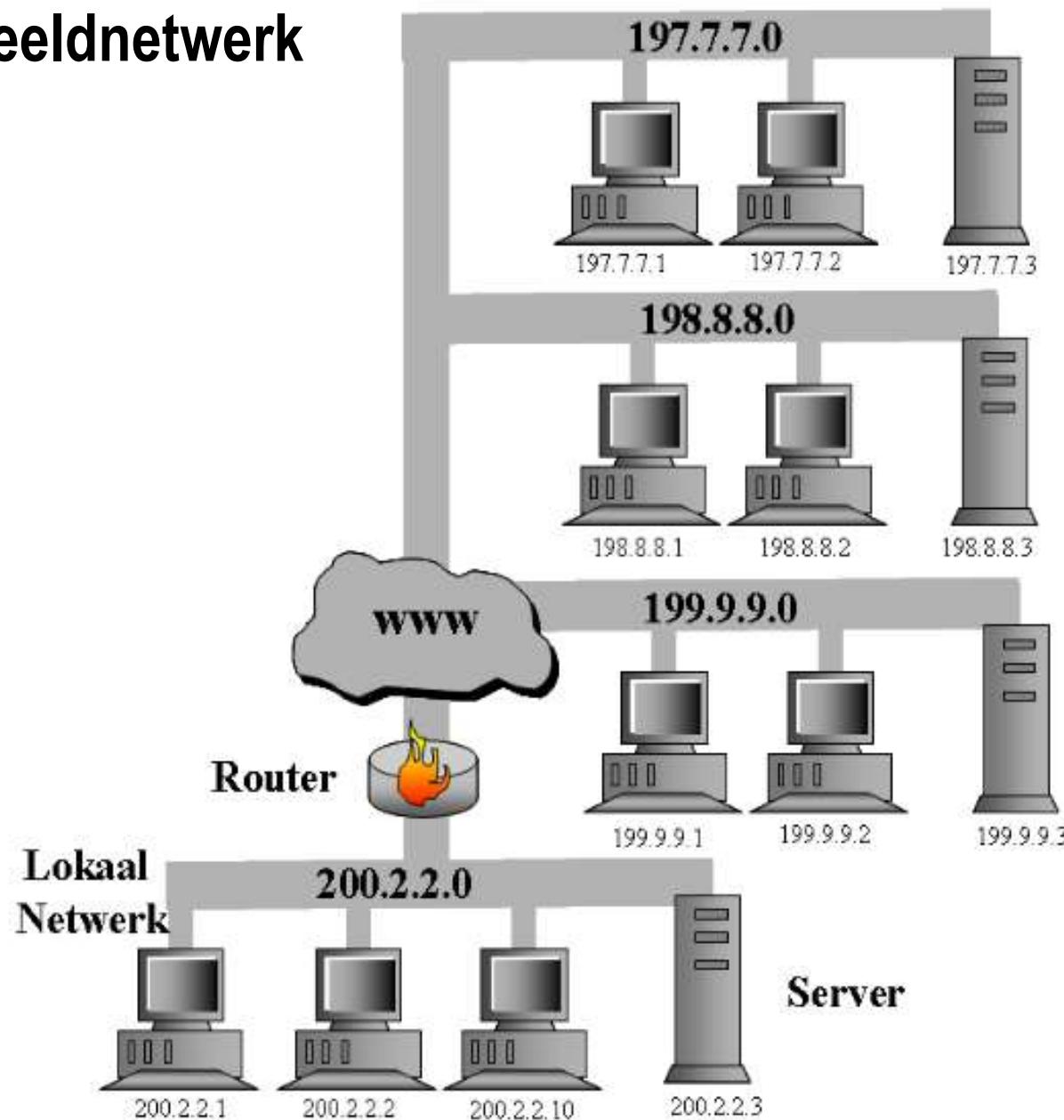
## ■ Server

- ◆ verbinding toestaan
- ◆ <----- SYN-ACK
- ◆ data sturen

# Verbinding Stoppen

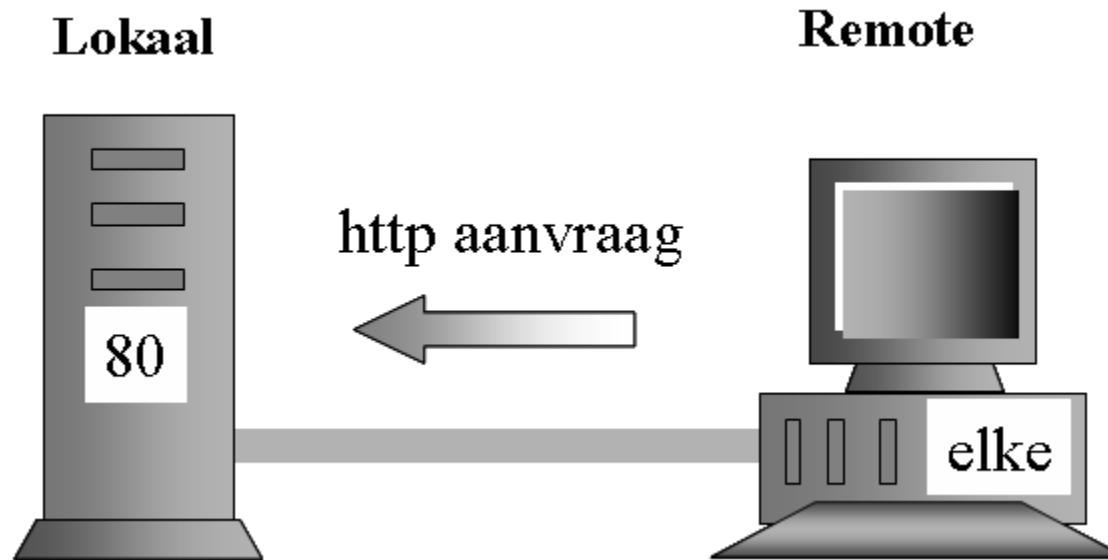
- FIN of RST
- Wat als iemand dat in jouw plaats stuurt?
  - ◆ Met vals (gespoofed) serveradres
  - ◆ Iedereen kan alle verbindingen stoppen
    - ook vanuit interne clients
  - ◆ Verhinderen door **stateful** te werken
    - status bijhouden van elke verbinding
    - ook sequence numbers bijhouden
    - timeout in milliseconden voor elke verbinding

# Voorbeeldnetwerk



# HTTP aanvraag naar jouw webserver

- TCP SYN, IN gt 1023 80 any 200.2.2.2/32

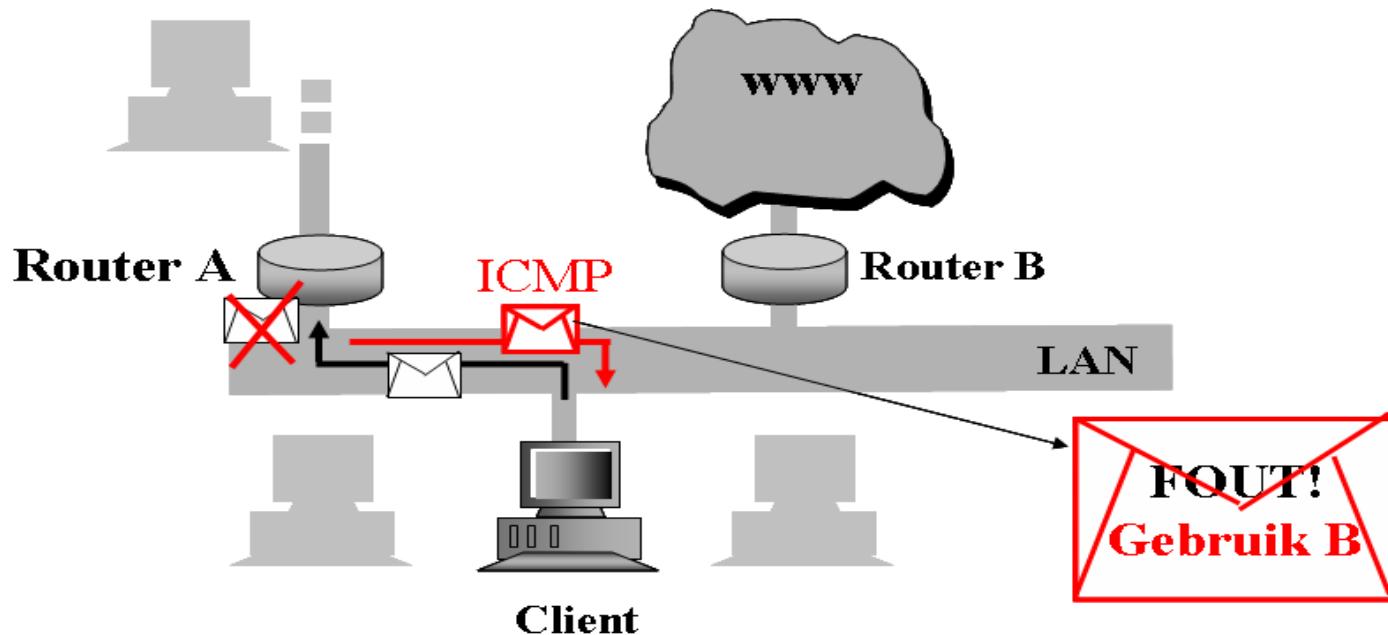


# Standaard: Anti spoofing

- **Niemand kan vanuit internet hetzelfde adres hebben als een intern adres**
- **!any IN elke poort elke poort 200.2.2.0/24 200.2.2.0/24**

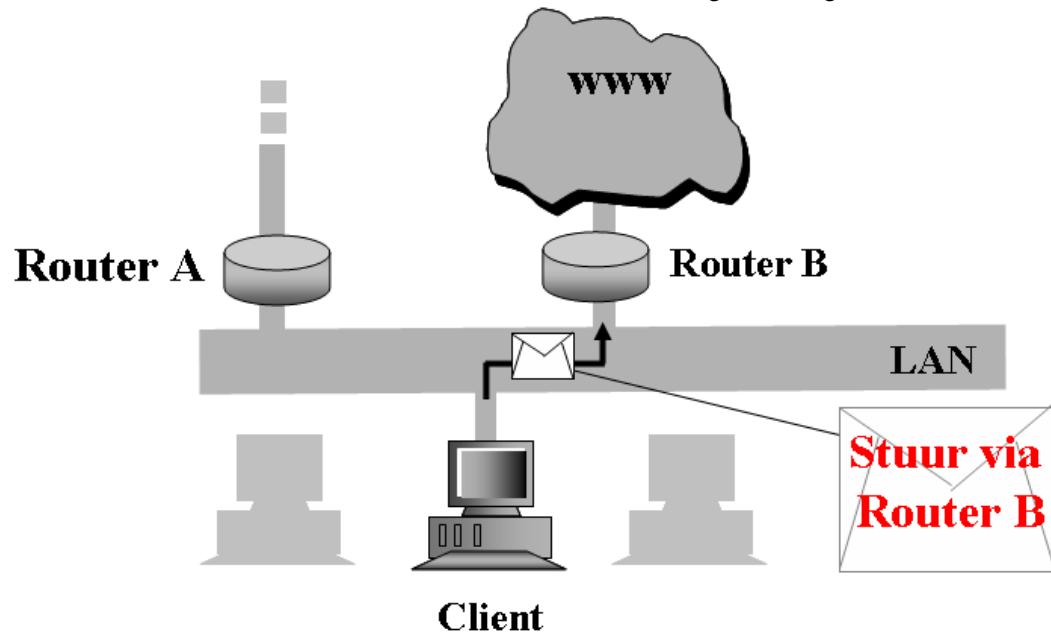
# ICMP redirect

- Foutbericht dat zegt dat je langs een andere route moet gaan
  - ◆ Misbruik: Zelf ICMP redirect sturen
    - Alle communicatie langs jou laten lopen



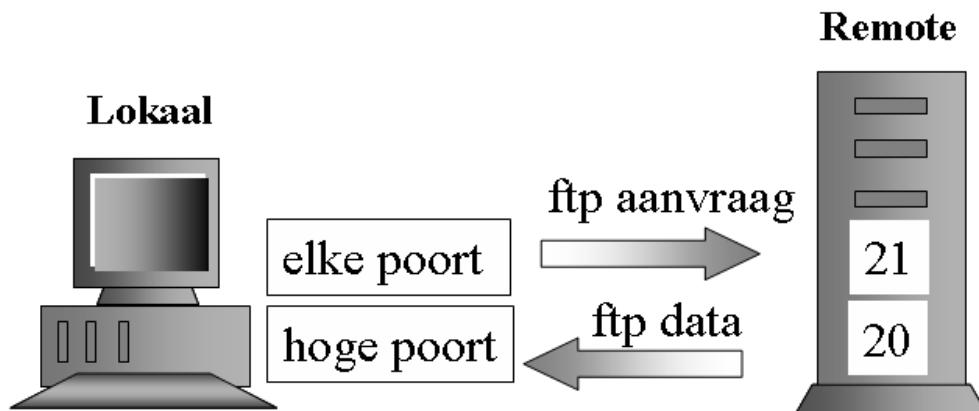
# Source Routing

- Route van een pakket aangeven binnen een pakket
- Handig bij regelen verkeer/bandbreedte
  - ◆ Soort GPS die de ideale route aangeeft
- !ip IN,OUT sourceroute – any any



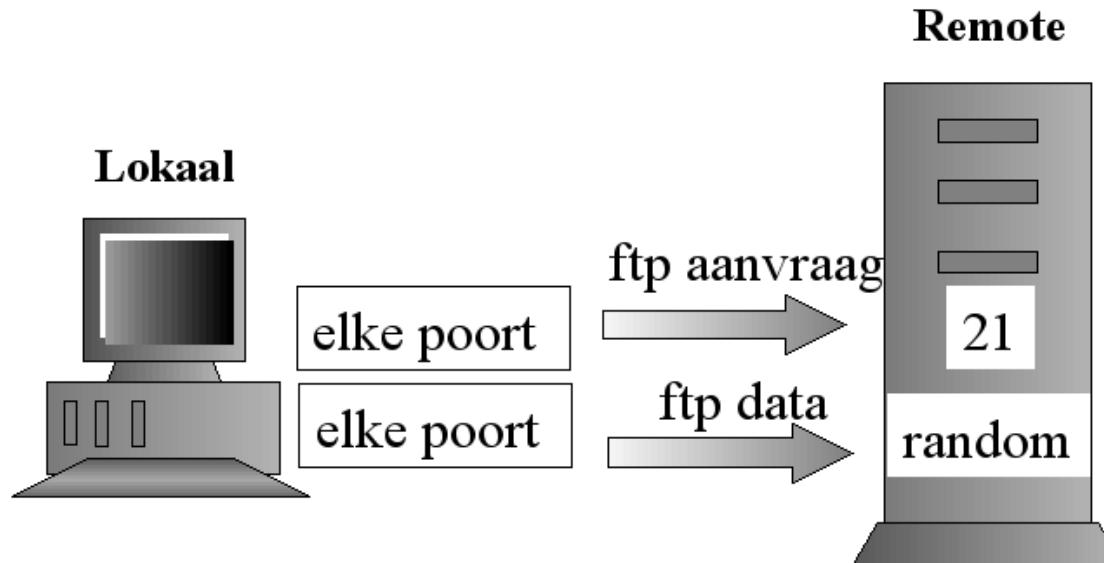
# Actieve FTP

- Aanvraag naar FTP server op poort 21
- Data vanuit FTP server vanuit poort 20
  - ◆ Alles vanuit poort 20 mag binnen naar alle hogere poorten!



# Passieve FTP

- Aanvraag naar FTP server op poort 21
- Server stuurt voor data random poort waarop client moet connecteren



# DNS

## ■ UDP poort 53

- ◆ Gewone client aanvragen aan DNS server
- ◆ Externe DNS server
  - Beperken welke externe DNS servers toegelaten zijn
    - Anders alle UDP vanuit poort 53 toegelaten
  - UDP OUT gt 1023 53 any 8.8.8.8
- ◆ Interne DNS servers
  - Beperken welke externe DNS servers parents zijn van jouw DNS server
  - TCP SYN,IN any 53 8.8.8.8 200.2.2.2/32

## ■ TCP poort 53

- ◆ Enkel voor zone transfers (doorgeven naam-ip tabellen tussen DNS servers onderling)

# Statustabel (vereenvoudigd)

## ■ Verstuurd

- ◆ TCP **SYN\_SENT**  
src=192.168.1.34 dst=172.16.2.23 sport=1054 dport=21  
**[UNREPLIED]**

## ■ Terug Verwacht:

- ◆ src=172.16.2.23 dst=192.168.1.34 sport=21 dport=1054  
use=1

## ■ Goedgekeurd (SYN is bevestigd)

- ◆ TCP **ESTABLISHED** src=192.168.1.34 dst=172.16.2.23  
sport=1054 dport=21
- ◆ src=172.16.2.23 dst=192.168.1.34 sport=21 dport=1054  
**[ASSURED]** use=1

# Cisco reflexive (stateful) access list

```
interface FastEthernet 0/0
ip access-group INKOMEND in
ip access-group UITGAAND out

ip access-list extended UITGAAND
permit tcp any any reflect TCPVERKEER

ip access-list extended INKOMEND
permit icmp any any
deny udp any any
evaluate TCPVERKEER
```

# Stateful met iptables TCP

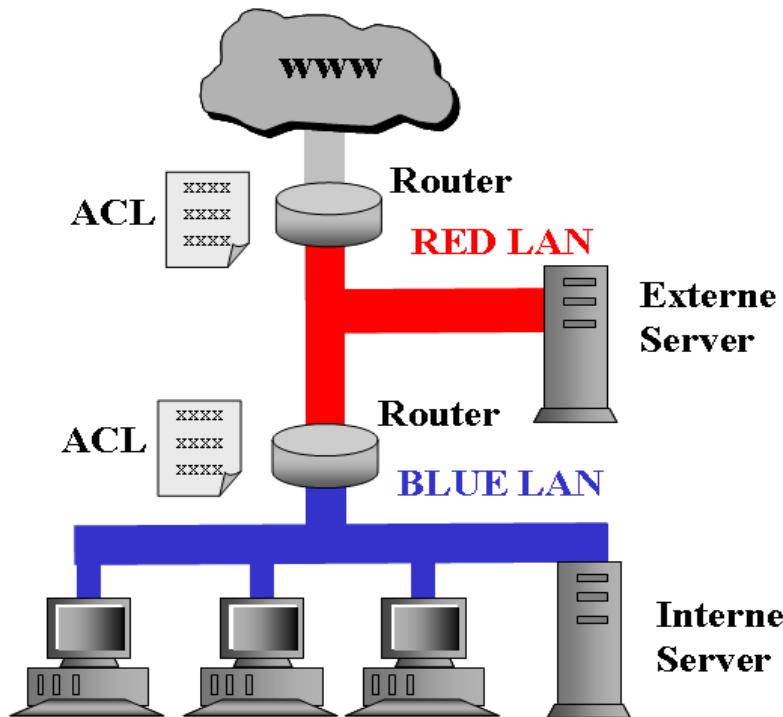
- **SYN=NEW**
- **iptables -A OUTPUT -p tcp **-m state --state NEW,ESTABLISHED -j ACCEPT****
- **Speciale optie RELATED**
  - ◆ Laat ook foutberichten (ICMP) door in verband met de verbinding
    - bv website opvragen maar poort werd geblokkeerd

# Stateful met iptables UDP

- UDP kan nooit stateful zijn
- UDP is bij iptables pseudo stateful
  - ◆ bv DNS aanvraag poort 53 waar is [www.kdg.be](http://www.kdg.be)?
  - ◆ iptables verwacht binnen x tijd een antwoord op die vraag

# Red LAN/ Blue LAN

- Red LAN DMZ (traag)
- Blue LAN intern (snel)



# If God is dead, who will save the Queen?

## ■ Logging



# **High Speed Modems**

BEGRIPPEN

xDSL

KABEL

FTTH

POWERLINE

# Asynchroon/Synchroon

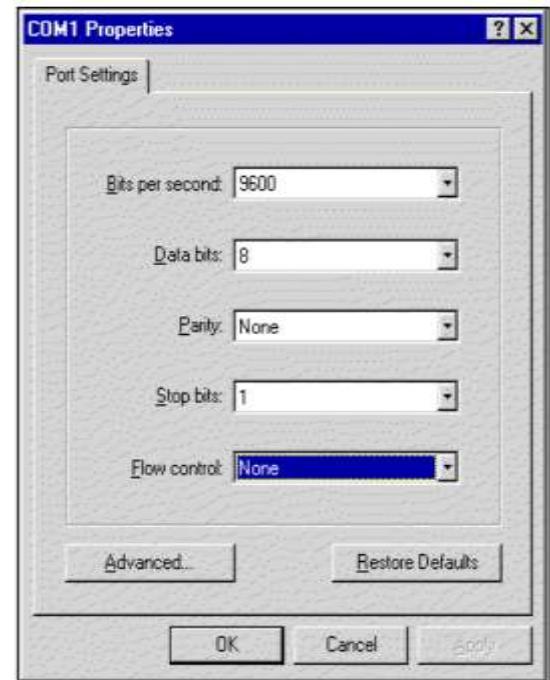
## ■ Startbit/Stopbit/Pariteit

- ◆ vaste klok zender/ontvanger



Startbit

Pariteitbit  
Stopbit(s)



# Synchroon

- Synchronisatie door reeks synchronisatiebits
- Ook gestuurd bij leeg kanaal



xDSL                    01111110 01111110

KABEL

FTTH

POWERLINE

# Multiplexing FDM

- Frequency Division Multiplexing
- Bandbreedte opdelen in frequentiegebieden
  - ◆ guardband nodig, anders overlapping
- Bv bij kabel: Bandbreedte 500MHz, per tv kanaal 6 Mhz



xDSL

KABEL

FTTH

POWERLINE



# Multiplexing TDM

- Time Division Multiplexing
- Elke deelnemer krijgt om de beurt het volledige kanaal
  - ◆ Verspilling van bandbreedte bij grote bandbreedte
  - ◆ Gebruikt per FDM kanaal



xDSL

KABEL

FTTH

POWERLINE

# Multiplexing: Statistical TDM

- Ongebruikt kanaal niet gebruiken



xDSL

KABEL

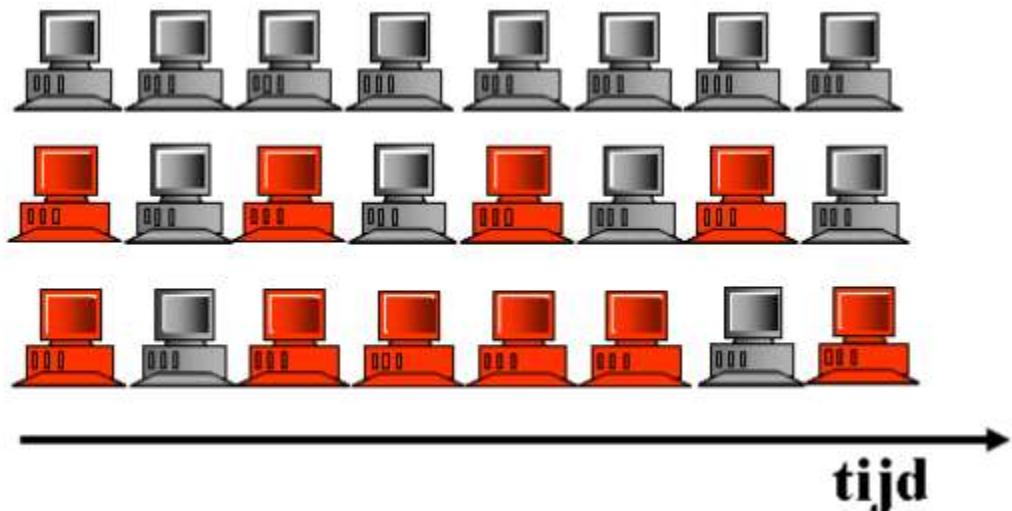
FTTH

POWERLINE

Geen Multiplexing

TDM

STDM



# Wavelength Division Multiplexing

- Bij glasvezel: Onderscheid maken tussen kanalen aan de hand van verschillende golflengten
  - ◆ bv rood licht en groen licht
  - ◆ kan ook in 2 richtingen door dezelfde glasvezel
    - upstream golflengte en downstream golflengte
- Coarse WDM: max acht kanalen tegelijk
- Dense WDM: 16 kanalen (160 Gbit/s)



xDSL

KABEL

FTTH

POWERLINE

# Verbindingen

## ■ Simplex

- ◆ 1 richting zoals radio uitzending

## ■ Half Duplex

- ◆ 2 richtingen maar nooit tegelijk zoals walkietalkie

## ■ Full Duplex

- ◆ Beide richtingen tegelijk, door elkaar

## ■ Onafhankelijk van synchroon/asynchroon



xDSL

KABEL

FTTH

POWERLINE

# Baudrate en bitrate

- Twee dataniveaus => baudrate=bitrate
  - ◆ bv -5V =0 +5V=1
- Grotere bitrate bij meerdere niveaus
  - ◆ bv 1 Volt= 1 2Volt=2 3 Volt=3



xDSL

KABEL

FTTH

POWERLINE

# Scrambling/Unscrambling

- Scrambling is het vervangen van een bitpatroon door een ander bitpatroon
  - ◆ Vervangen van grote reeks nullen door onmogelijke code



DECRYPTEN

xDSL

KABEL

FTTH

POWERLINE

# Bandbreedte

- Verschil tussen hoogste en laagste frequentie
- In Hertz (Hz)

- 
- ◆ Telefoon (spraak) 4kHz
  - ◆ CD-stereo audio 44 kHz
  - ◆ Broadcast video 4.2 MHz
  - ◆ HDTV 90 MHz

xDSL

KABEL

FTTH

POWERLINE

# Datacompressie

- **Lossless: Zonder verlies (gif,zip)**
- **Lossy: Met verlies (jpg/mp4/mp3)**
- **Run Length Encoding**
  - ◆ Een aantal identieke codes wordt vervangen door een vlag, een karakter of een aantal.
  - ◆ Bv Pieter Janssen 102
  - ◆ wordt vervangen door: Pieter# 6Janssen# 6102



xDSL

KABEL

FTTH

POWERLINE

# Datacompressie

## ■ Huffman Encoding

- ◆ De lengte van een karaktercode is gebaseerd op de statistische frequentie van het voorkomen in de tekst. We gebruiken dus een korte code voor vaak voorkomende karakters.
- ◆ Bv e wordt binair voorgesteld als 01011000  
e komt vaak voor, dus spreken we af dat we e voorstellen als 1111

## ■ Lempel-Ziv Encoding

- ◆ buffer bij zender en ontvanger van datastream
- ◆ algoritme maakt boomstructuur met strings
- ◆ reeds geziene string => pointer doorgestuurd



xDSL

KABEL

FTTH

POWERLINE

# Modulator

- De techniek om de informatie in een draaggolf onder te brengen, wordt aangeduid als modulatie
- **Modulator in combinatie met demodulator is een modem**



xDSL

KABEL

FTTH

POWERLINE

# AM FM PM

- **Amplitude Modulation: LUID stil LUID stil**
- **Frequency Modulation: Hoog Laag Hoog Laag**
- **Phase Modulation: Aanpassing fase**
  - ◆ bv normale golf op het water valt ineens terug naar laagste punt op de top
  - ◆ Veel energie nodig en veel hoogfrequente storing



xDSL

KABEL

FTTH

POWERLINE

# AM hoge golf / lage golf



xDSL

KABEL

FTTH

POWERLINE



# FM korte golf / lange golf



xDSL

KABEL

FTTH

POWERLINE



# PM top golf wordt plots laagste punt



xDSL

KABEL

FTTH

POWERLINE



Surfers houden dus vooral van phase modulation !

# QAM Quadrature Amplitude Modulation

## ■ Combinatie van Amplitude en Fase

- ◆ bv QAM met 16 levels:

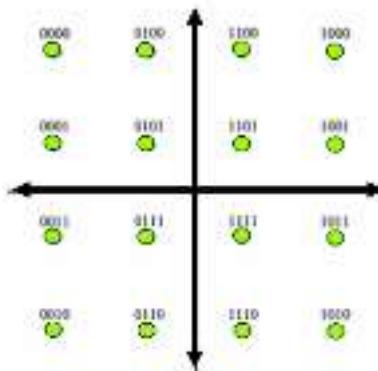


xDSL

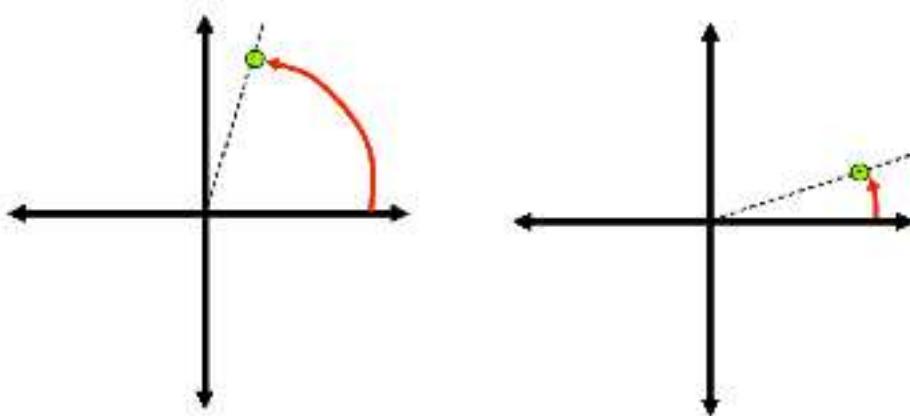
KABEL

FTTH

POWERLINE



# QAM Amplitude en Fase



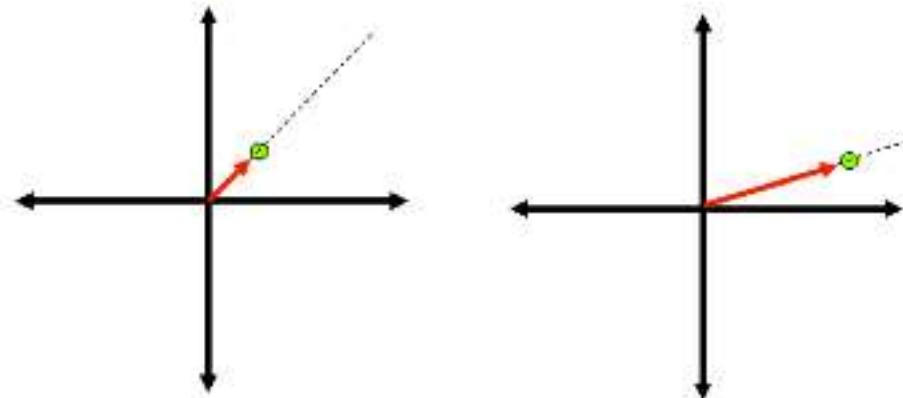
xDSL

KABEL

FTTH

POWERLINE

Figuur: Twee verschillende fases



Figuur: Twee verschillende amplitudes

# V90/V92

- **Oude Telefoonmodem standaard**
- **bandbreedte van een telefoonkanaal (voor spraak) is 4kHz**
- **Asymmetrische verdeling bandbreedte**
  - ◆ **56 kbps downstream/33.6 kbps upstream**
  - ◆ **Uit de oude doos, een dialup modem geluid:**



xDSL

KABEL

FTTH

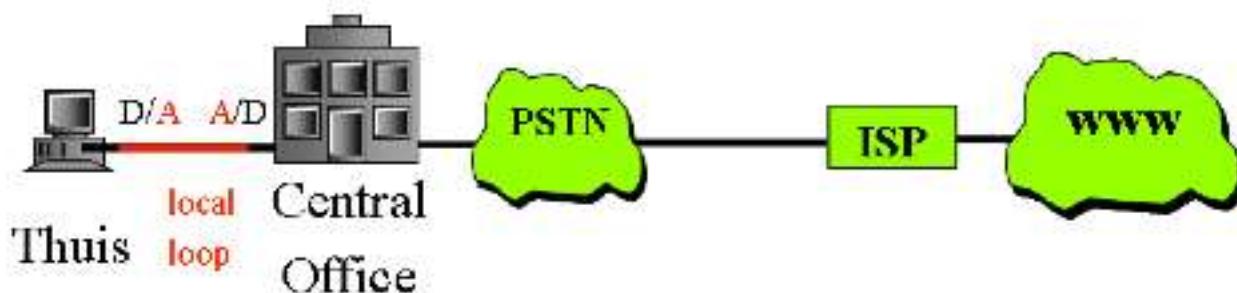
POWERLINE

# V90 verbetering communicatie

- Elke Digitaal analoog omzetting is een verlies



Figuur: Communicatie vroeger PSTN naar ISP was analoog



xDSL

KABEL

FTTH

POWERLINE

# ADSL

- **Asymmetric Digital Subscriber Line**
  - ◆ Asymmetrisch: meer download dan upload
- **Volledige bandbreedte Twisted Pair gebruikt**
- **Bandbreedte tot 1MHz**
  - ◆ Hoge frequenties geven meer storing
- **Afstand beperkt door**
  - ◆ dikte kabel
  - ◆ externe ruis



BEGRIPPEN

ADSL

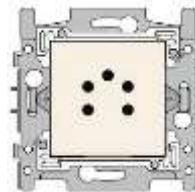
KABEL

FTTH

POWERLINE

# Oorzaken van ruis

- Niet beëindigde stukken koperdraad
- Overspraak (cross-talk)



- ◆ twisted pair draden beïnvloeden elkaar

- Gebruik telefoon

- ◆ Bellen en nummer kiezen genereert even hogere frequenties

- Huishoudapparaten, bliksem

- ◆ Korte, tijdelijke storing

- Radiogolven

- ◆ Vaste frequenties, constante storing



BEGRIPPEN

XDSL

KABEL

FTTH

POWERLINE

# ADSL en FDM

## ■ ADSL gebruikt FDM

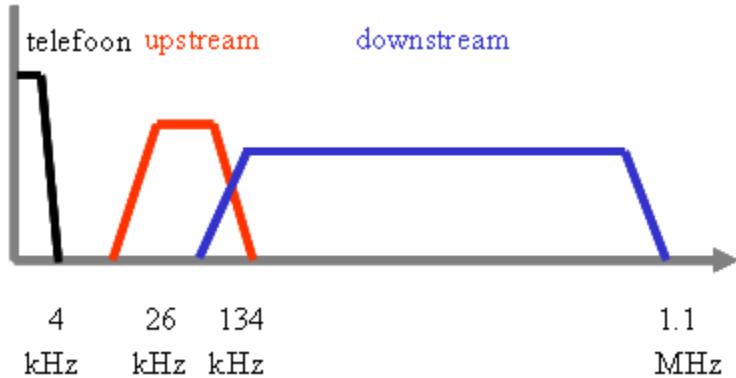
- ◆ 0-4 kHz      telefoon
- ◆ 26-134 kHz      upstream
- ◆ 134 tot 1MHz      downstream

BEGRIPPEN  
ADSL

KABEL

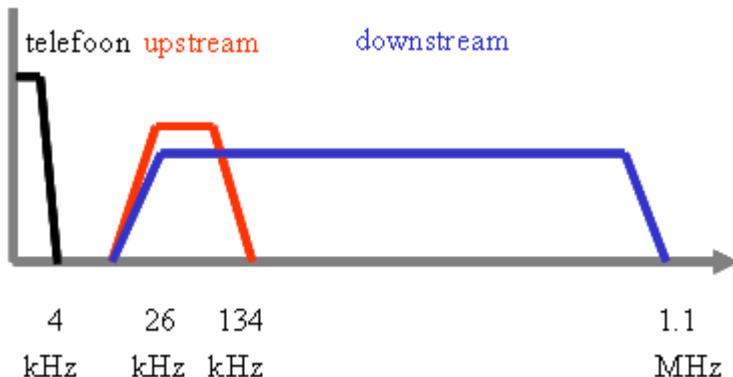
FTTH

POWERLINE



# Echo cancellation

- Upstream en downstream gebruiken overlappende frequenties



BEGRIPPEN

XDSL

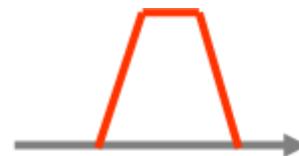
KABEL

FTTH

POWERLINE

# Echo cancellation

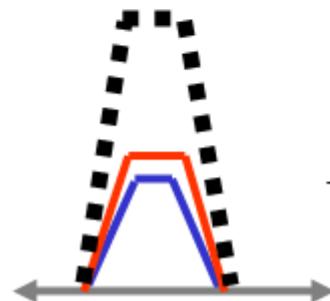
- Je kent je upload signaal, dus:



UPSTREAM signaal



DOWNSTREAM signaal



UPSTREAM + DOWNSTREAM  
- UPSTREAM

---

DOWNSTREAM



BEGRIPPEN  
XDSL

KABEL

FTTH

POWERLINE

# DMT modulatie

- Discrete Multi Tone
- 1MHz Opdelen in 256 kanalen van 4 kHz
  - ◆ Vóór het opstarten van de verbinding nakijken welke kanalen optimaal zijn
  - ◆ Per subkanaal QAM gebruiken



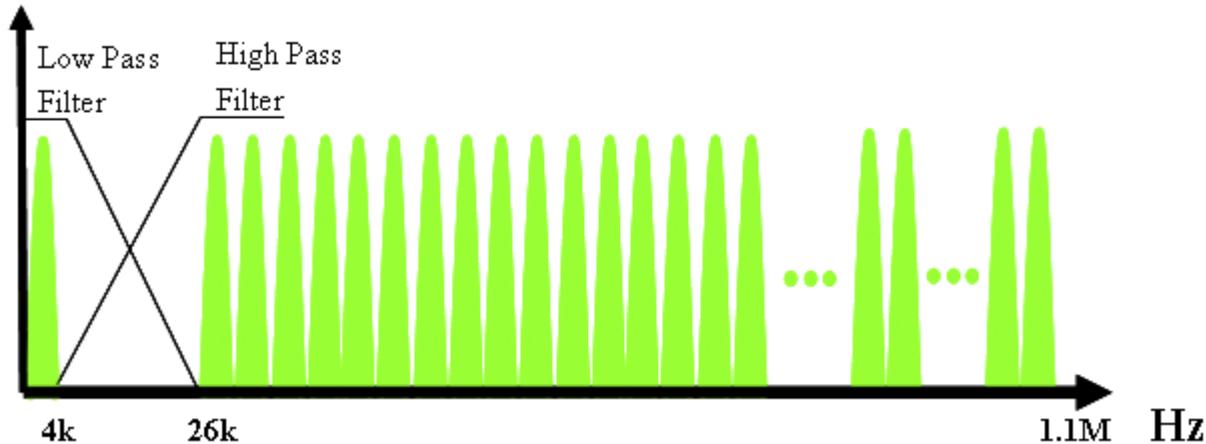
BEGRIPPEN

DSL

KABEL

FTTH

POWERLINE



# ADSL 2

- Hogere snelheid door kortere afstand tot aan  
DSLAM Digital Subscriber Line Access Multiplexer

BEGRIPPEN



KABEL

FTTH

POWERLINE



# ADSL 2+

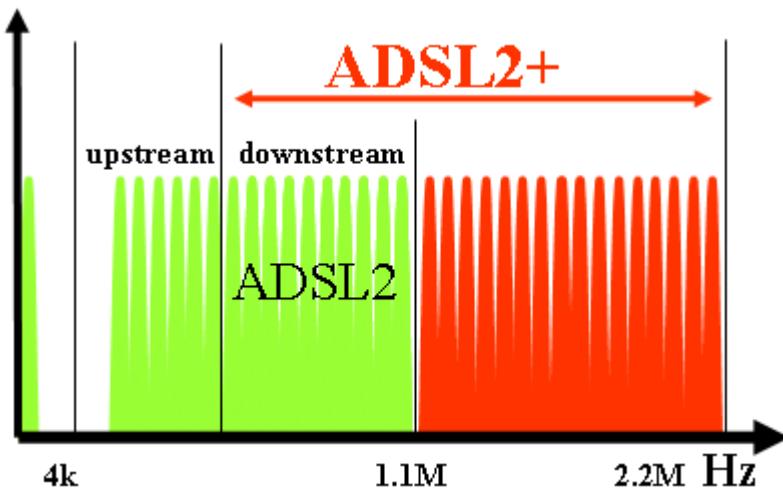
- Korte afstand tot aan DSLAM
- Uitbreiding Frequentiespectrum tot 2.2MHz
- Low Power Modus (ADSL kanalen altijd actief)

BEGRIPPEN  
→  
ADSL

KABEL

FTTH

POWERLINE



# ADSL 2+

## ■ Realtime meting Signaal/Ruisverhouding (ADSL enkel bij opstart)

- ◆ Ontvanger en zender schakelen tegelijk over naar de beste kanalen

## ■ Cross-talk vermijden

- ◆ Kan enkel 1.1MHz tot 2.2MHz gebruiken
  - op hogere frequenties is er geen cross-talk



BEGRIPPEN

ADSL

KABEL

FTTH

POWERLINE

# VDSL

- Very High Speed door beperking van de afstand tot de DSLAM tot 1 km
- Zowel symmetrisch als assymetrisch mogelijk



BEGRIPPEN

XDSL

KABEL

FTTH

POWERLINE

# Andere DSL

## ■ HDSL (High bit rate)

- ◆ 2 paar telefoonkabels

## ■ SDSL

- ◆ Symmetric
- ◆ Voor servers op internet

## ■ Naked DSL

- ◆ Zonder telefoon en dus zonder splitser



BEGRIPPEN

XDSL

KABEL

FTTH

POWERLINE

# Kabelmodems

## ■ Vroeger unidirectioneel (tv uitzending)

## ■ Aanpassingen

- ◆ Meer glasvezel want

- meer upstream verkeer
  - grotere bandbreedte nodig (meer tv kanalen en internet)

- ◆ Boomstructuur werd sterstructuur naar residentiële gebieden

- ◆ Bidirectionele versterkers (ook upstream)

BEGRIPPEN

xDSL



FTTH

POWERLINE

# Kabelmodem frequentiespectrum

- Verdeling frequentiespectrum kabel

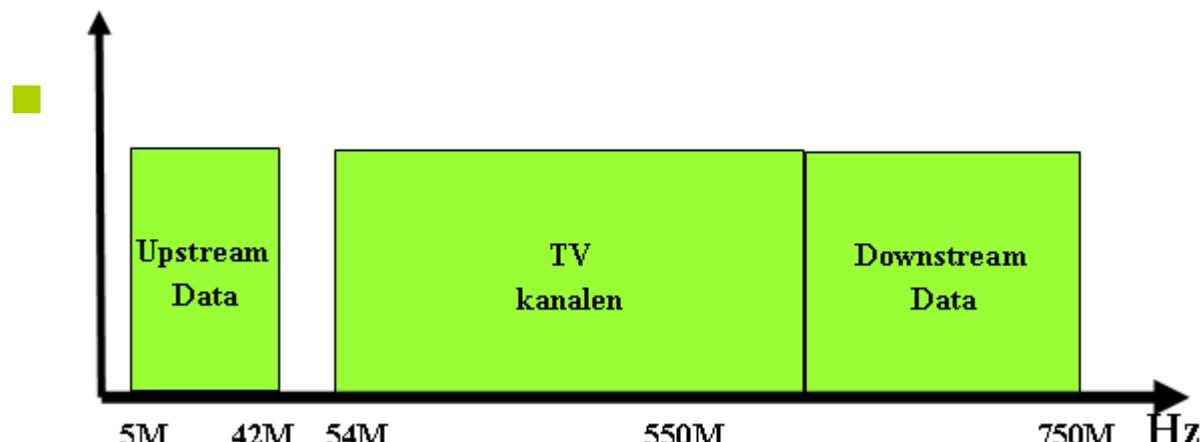
BEGRIPPEN

xDSL



FTTH

POWERLINE



- 64 or 256 QAM downstream/ 16 QAM upstream

# Kabelmodem CMTS

## ■ Cable Modem Termination System

- ◆ Opdeling verkeer van gebruikers
- ◆ Koppeling van kabelnetwerk aan DHCP, internet,..

## ■ Gebruikt DOCSIS protocol

- ◆ Data Over Cable Service Interface Specification
- ◆ Laag 1 en 2 OSI
- ◆ v1.1 QoS (opdeling Video/Game/Telefoon/...)
- ◆ v2.0 ook symmetrisch, betere ruisbescherming
- ◆ v3.0 ook IPv6
- ◆ v3.1 full-duplex en 4096 QAM

BEGRIPPEN

xDSL



FTTH

POWERLINE

# Hybrid Fibre Coax (HFC)

- Glasvezel tot aan de straat, coax tot in huis
- Telenet noemt de grijze straatkast een node
  - ◆ Een node bedient gemiddeld 290 gezinnen



## BEGRIPPEN

xDSL



FTTH

POWERLINE

- In België kan je tot 3 grijze kasten naast elkaar hebben (Telenet, Belgacom en Elektriciteit)

# Fiber To The Home

- **Vraag naar bandbreedte blijft stijgen**
- **Point to point**
  - ◆ Rechtstreeks van provider naar gebruiker
- **Passive Optical Network**
  - ◆ Fiber splitst voor 16 tot 32 gebruikers
- **Hoogste kost is graven**
  - ◆ Pilootproject universiteit Gent, fiber binnenbrengen via waterleiding
    - Lukt bij industrie waar er een bredere leiding is

BEGRIPPEN

xDSL

KABEL



POWERLINE

# Verbeteringen Fiber

## ■ Solitonen

- ◆ Tegen dispersie (verbreding golf over afstand)

## ■ All optical

- ◆ Enkel klok blijft elektrisch
- ◆ Geen storing!

BEGRIPPEN

xDSL

KABEL



POWERLINE

# Verbeteringen Fiber

## ■ Probabilistic Constellation Shaping (PCS)

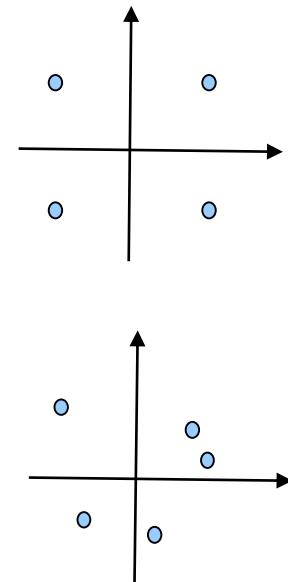
- ◆ Verbetering vaste punten QAM

- vaste amplitude
- vaste fase
- vaste punten

- ◆ Variabele punten PCS

- zo klein mogelijke amplitude
- zo weinig mogelijke storing
- realtime aanpassing
- tot 1 Terabit per seconde

QA  
M  
PC  
S



BEGRIPPEN

xDSL

KABEL



POWERLINE

# Powerline

■ **Data versturen met als modulatiegolf een lage voltslijn (220V)**

- ◆ Internet via het stopcontact

■ **Alternatief en eerder gebruik**

- ◆ Aansturen straatverlichting
- ◆ Doorsturen elektriciteitsmetingen aan leverancier
- ◆ Binnenhuisnetwerk

BEGRIPPEN

xDSL

KABEL

FTTH



# Powerline voor en nadelen

## ■ Voordelen

- ◆ Lage installatiekost
- ◆ Verbindingen bestaan al
- ◆ Mogelijkheden: Al je elektrische apparaten zijn sowieso verbonden met internet
  - koelkast, koffiezetter, broodmachine,...

## ■ Nadelen

- ◆ Interferentie met elektrische apparaten,
- ◆ Kabels onbeschermd tegen externe ruis
- ◆ Enkel last-mile (geraakt niet door transformator)

BEGRIPPEN

xDSL

KABEL

FTTH

POWERLINE

meshs3d

# Wireless

## WiFi



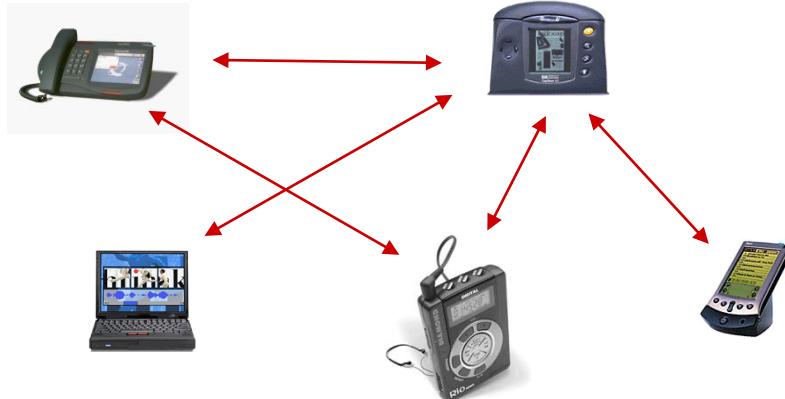
# WLAN modes en topologiën

■ Draadloze netwerken kunnen in twee modi opereren

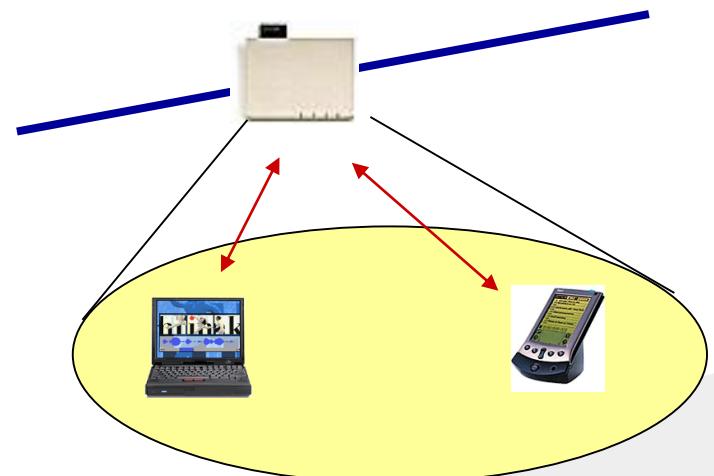
- ◆ Ad-hoc
- ◆ Infrastructure

■ Meestal worden WLANs in infrastructure mode gebruikt

Ad-  
Hoc



Infrastructure

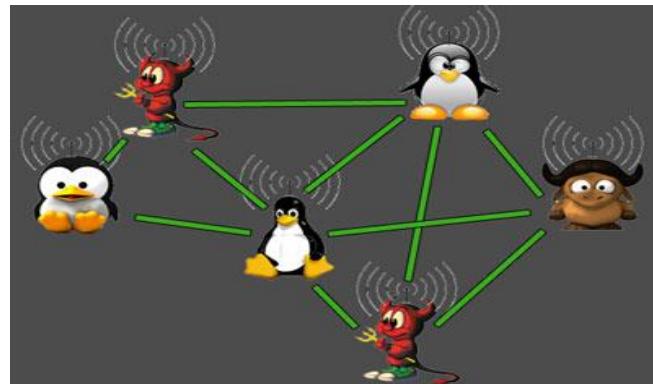


# Ad-hoc (roaming) Mode

- Apparaten kunnen direct met elkaar communiceren
- Apparaten kunnen zich verplaatsen en verbinden met eender welk ander apparaat
  - ◆ Geen basis stations
  - ◆ Nodes kunnen enkel communiceren naar nodes binnen bereik
  - ◆ Nodes organiseren zich zelf tot een “netwerk”
  - ◆ Routeren tussen elkaar

# Mobile Ad-hoc Network (MANET)

- Een mobiel mesh netwerk, ook wel MANET genoemd, is een zelf configurerend netwerk van mobiele apparaten die draadloos zijn verbonden
- Elk apparaat moet verkeer dat niet voor zichzelf bestemd is doorsturen, en is daarom een router
- De uitdaging bij een MANET is het constant updaten van informatie in het netwerk zodat de juiste route kan gekozen wordens



# Ad Hoc protocol B.A.T.M.A.N



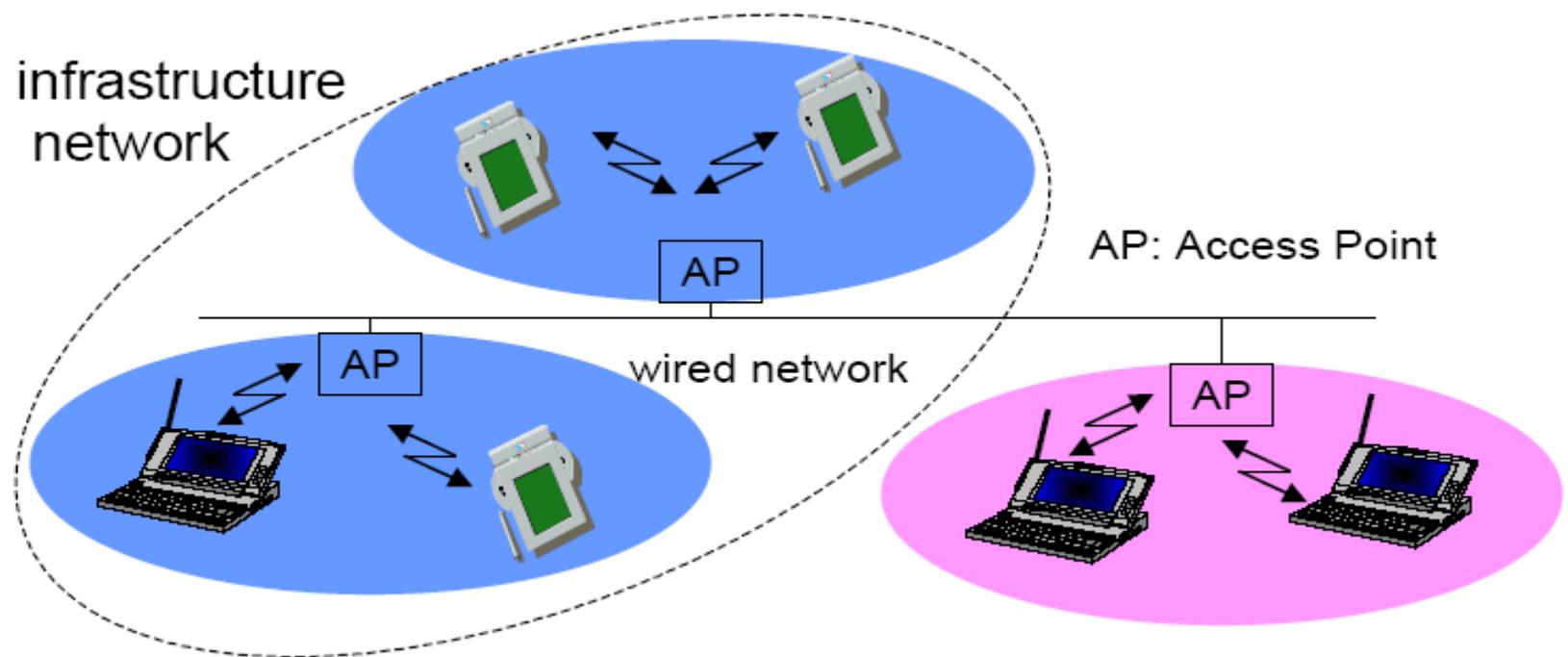
- **Better Approach To Mobile Adhoc Network**
- **Kennis over het netwerk is gedecentraliseerd**
- **Elk pakket krijgt een dynamisch geleerde route**
  - ◆ Batman-adv kernel module
  - ◆ Virtuele netwerkinterface die voor transport zorgt
  - ◆ Regelmatische broadcast van een batman node naar zijn buren
    - Luistert en onthoudt broadcasts van andere buren
  - ◆ Onthoudt langs welke node pakketten moeten gestuurd worden (niet de hele route), kan ook melden dat hij dezelfde kan bereiken
- **Werkt ook samen met wired!**

# The Serval Project

- Open source project <http://servalproject.org>
- Communicatie tussen mobiele telefoons (Android)
- Onafhankelijk van GSM netwerk
  - ◆ Serval Mesh App

# Infrastructure Mode Wireless Networks

- In een infrastructure WLAN blijven de draadloze apparaten meestal in een relatief vast gebied



# WLAN Roaming

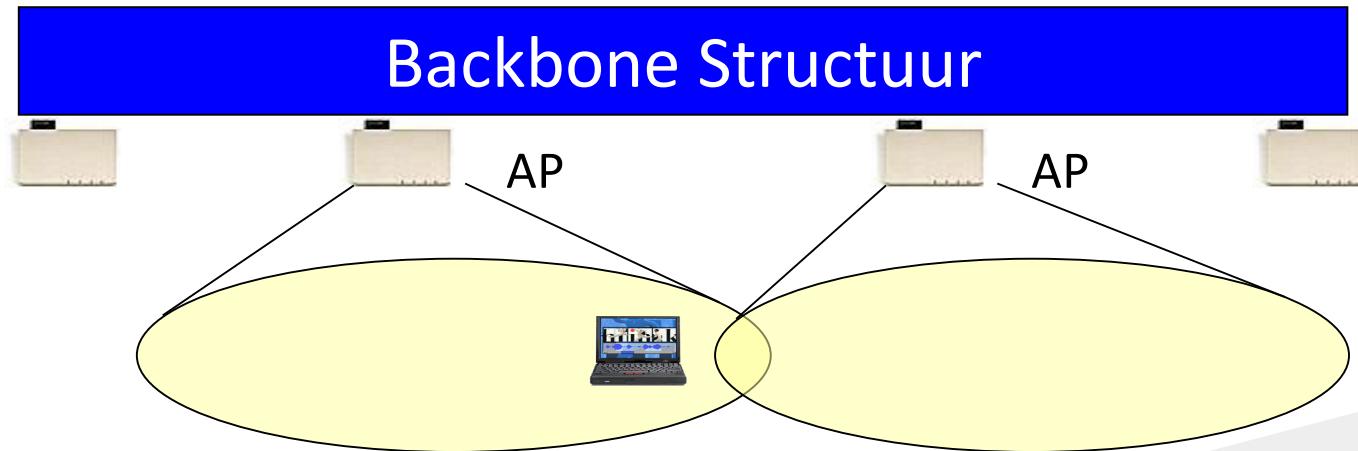
- In een multi-cel WLAN netwerk met een aantal APs kunnen gebruikers zich vrij verplaatsen eens ze geauthenticeerd en geassocieerd zijn.
  - ◆ Gebruikers kunnen dan overschakelen op de AP met het sterkste signaal
- Twee soorten WLAN roaming:
  - ◆ Seamless roaming
    - Gebruikt bij GSM
  - ◆ Nomadic roaming
    - Gebruikt bij WLAN apparaten

# 802.11 Roaming

- **Roaming gebruikt een ‘break before make’ volgorde**
  - ◆ Een bestaande connectie met een AP wordt verbroken en daarna wordt een nieuwe verbinding opgebouwd met een nieuwe AP
- **WLAN roaming gebeurt in 4 stappen**
  - ◆ Disassociatie
  - ◆ Zoeken
  - ◆ Her-associatie
  - ◆ Authenticatie
- **WLAN roaming gebeurt op laag 2**
  - ◆ WLAN apparaten kunnen dus hun IP adres behouden

# Extended Service Set

- Meerdere AP's vormen een ESS
- AP's zenden regelmatig beacons uit
- Draadloze apparaten scannen en ontdekken
- Authenticatie en associatie met een AP
- Aanliggende AP's gebruiken verschillende 'radio kanalen'



# Hot Spots

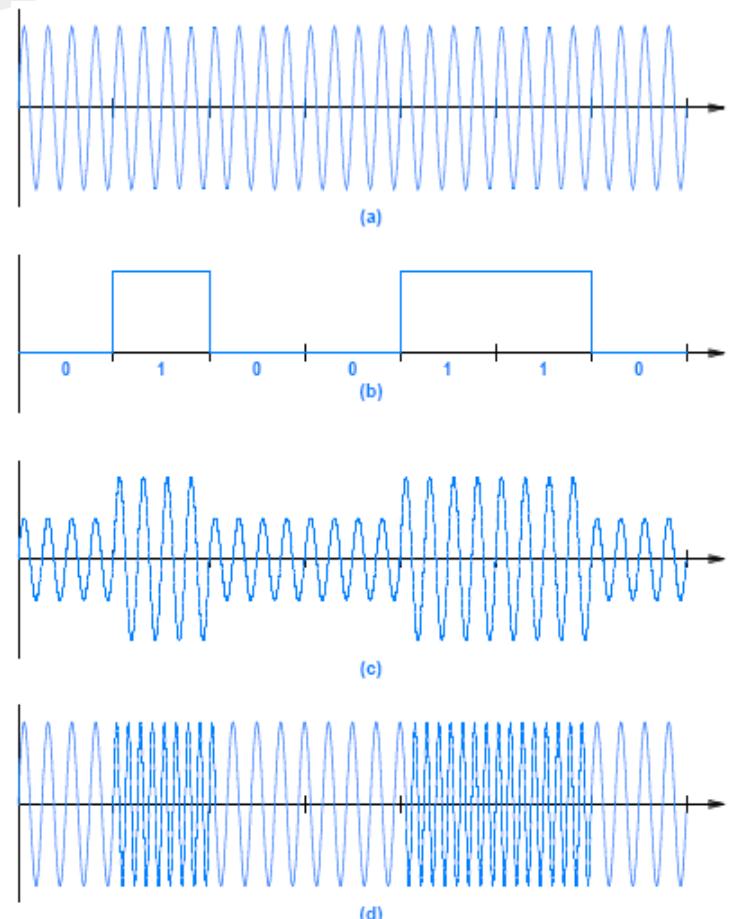
- **Een hotspot is een locatie waar internet wordt aangeboden over een gedeelde verbinding via een enkele router**
  - ◆ restaurant, treinstation, benzinestation,....

# WLAN Radio Onderdelen

- IEEE 802.11 gebruikt een aantal functies om radio communicatie te doen
  - ◆ Verschillende modulatie technieken
  - ◆ Frequency Hopping Spread Spectrum
  - ◆ OFDM (Orthogonal Frequency Division Multiplexing)

# Digitale modulatie

- (a) een draaggolf
- (b) digitaal input signaal
- (c) amplitude shift keying
- (d) frequency shift keying



# 802.11n of WiFi-4

## ■ IEEE Standaard op 11 sept 2009

- ◆ Draft-N standaarden waren gelukkig compatibel

## ■ Dual band

- ◆ Werkt op 2,4 GHz en 5,2 GHz

## ■ MIMO

- ◆ Multiple Input Multiple Output
- ◆ Tot 4 kanalen parallel
- ◆ Meerdere antennes nodig

## ■ Channelbonding

- ◆ Bundelen van 2 kanalen (20MHz + 20 MHz) op de 5,2 GHz band

# 802.11 ac of Wi-Fi 5

- Standaard goedgekeurd eind 2013
- 256 QAM modulatie
- Bandbreedte voor apparaten: 80 MHz tot 160 MHz
- Enkel 5 GHz band
- MIMO tot 8 kanalen
- Gigabit snelheden
- Antennes
  - ◆ APs hebben tot 8 antennes
  - ◆ Apparaten tot 2 antennes

# 802.11 ax of Wi-Fi 6 – Wi-Fi 6E

- Standaard goedgekeurd eind 2019
- OFDM (zie GSM technologie)
  - Netwerkverbetering 300% door minder botsingen
- Zowel 2,4 als 5 GHz band
  - WiFi 6E heeft extra 6G band
- Snelheid tot 10 Gbps (37% beter dan 802.11 ac)
  
- MiMo (multiple input, multiple output)
  - Concurrente verbindingen van/naar AP

# WLAN Apparaten

- **Netwerkkaarten**
- **Access points (AP)**
- **Repeaters**
- **Bridges**
- **Switches**
- **Routers en ‘gateways’**
- **Antennes**

# Draadloze Netwerkkaarten

## ■ Verschillende opties bij netwerkkaarten (NICs)

- ◆ Soort interface (intern, USB, PCI, PCMCIA)
- ◆ Draadloze standaard (802.11a/b/g/n, Bluetooth, ...)
- ◆ Soort antenne (los, vast)
- ◆ Power output (30 mW, 40 mW, 50 mW, 200 mW)
- ◆ Power modes (PSP, CAM)

# Power output

- Verschillende "power" beheer
  - ◆ Constant Awake Mode (CAM)
  - ◆ Power Saving
- NIC wordt in een slaapmodus gezet na een bepaalde tijd van inactiviteit
  - ◆ Periodisch wordt de NIC terug aangeschakeld om mogelijk netwerkverkeer te verwerken

# Thin AP of Fat AP?

## ■ FAT

- ◆ Voorziet alle functies voor WLAN functionaliteit:
  - RF-naar-RF verbindingen
  - RF-naar-draad conversie
  - Authenticatie
  - Encryptie
  - Beheer

## ■ Thin

- ◆ RF-naar-RF verbindingen
- ◆ RF-naar-draad conversie

# Multi-Radio AP

■ **Multi-radio APs ondersteunen verschillende standaarden tegelijk op het draadloos netwerk**

- ◆ 802.11a
- ◆ 802.11b
- ◆ 802.11g
- ◆ 802.11n



# Bridges

- Een netwerk bridge verbindt meerdere netwerksegmenten op laag 2 (data link laag) van het OSI model
- Bridges zijn vergelijkbaar met repeaters omdat ze ook segmenten met elkaar verbinden  
**MAAR bridges doen niet gewoon een broadcast op het andere segment**

# Soorten Bridges

- **Transparent (learning) bridging**
- **Source route bridging**

# Transparent Bridging

- **Gebruikt een forward tabel om frames door te sturen naar andere netwerk segmenten**
- **De forwardtabel is eerst leeg**
  - ◆ Rijen in de tabel worden aangemaakt wanneer de bridge frames ontvangt
- **Wanneer een adres niet in de forward tabel staat, wordt de frame gebroadcast naar alle poorten van de bridge**
  - ◆ forwarding naar overal behalve naar de source port

# Source route Bridging

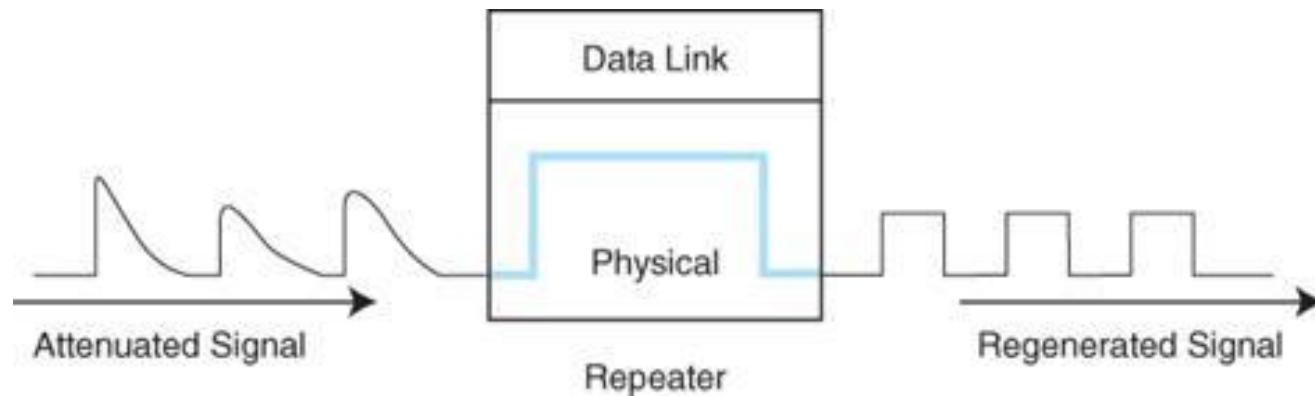
- **Twee soorten frames om het juiste doelnetwerk te vinden**
  - ◆ All-Route (AR) frames dienen om routes te leren.
    - Route onbekend dus gebroadcast
  - ◆ Single-Route (SR) frames hebben vastgelegd doeladres
    - Route is gekend
- **Elke frame heeft een maximum hop count**
  - ◆ frame wordt verwijderd wanneer hop count op nul staat
- **De eerste AR frame die bij het doel geraakt, wordt de beste SR route**
  - ◆ Andere AR frames worden genegeerd

# Stealth AP

- AP dat de service set identifier (SSID) NIET broadcast
  - ◆ Verhindert automatische herkenning van het netwerk
- Stealth mode is niet gedefinieerd in de 802.11x standaard en noemt soms:
  - ◆ Closed mode
  - ◆ Private network

# Wireless Repeaters

- Een repeater wordt gebruikt om een signaal uit te breiden
  - ◆ Uitbreiden in kwaliteit, sterkte of range
- De oorspronkelijke sterkte wordt hersteld en een gedeelte van de ruis wordt verwijderd



# LAN switching

- **Verkeer wordt enkel gestuurd naar de poort die nodig is**
  - ◆ met snelle hardware-gebaseerde methodes.
- **Gebruikt het MAC adres van de NIC om te bepalen waar het verkeer naartoe moet**

# Soorten Switching

## ■ Cut-through

- ◆ Doorsturen vanaf dat source/destination adres herkend zijn

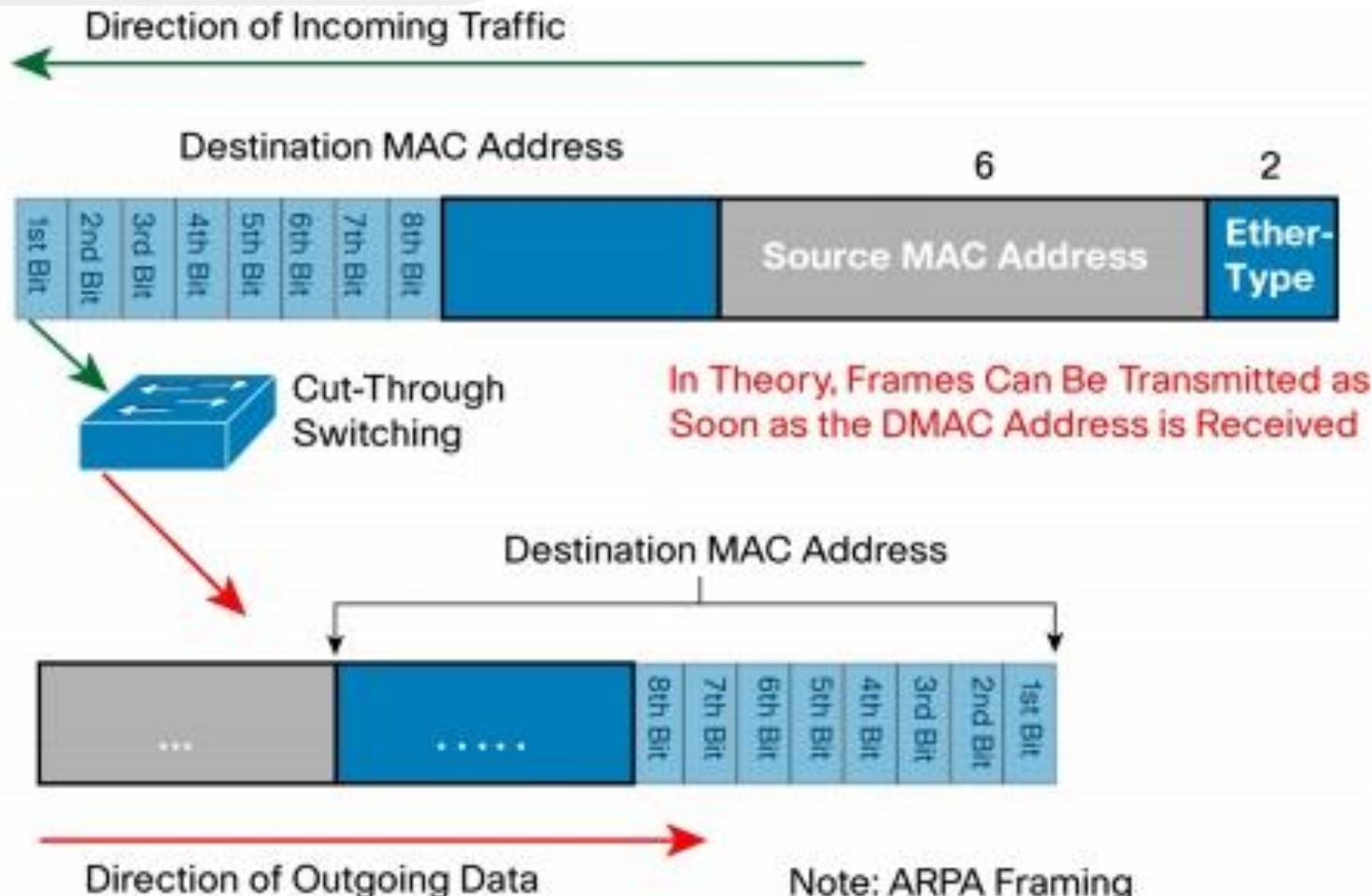
## ■ Fast-forward

- ◆ Doorsturen wanneer destination MAC adres herkend is

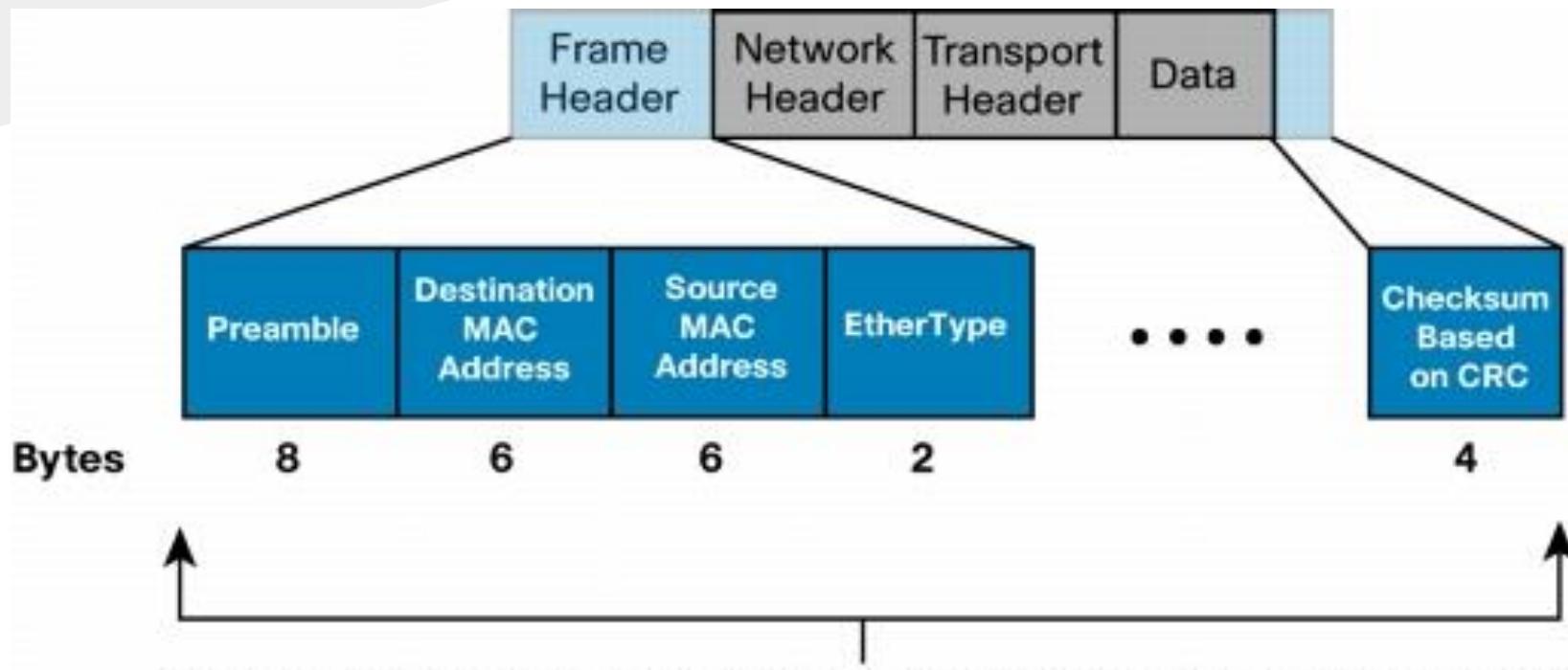
## ■ Store-forward

- ◆ Inlezen (buffer) in tijdelijke opslag en dan doorsturen frame
- ◆ Verhindert runts (onvolledige berichten) en giants (te grote datapakketten)

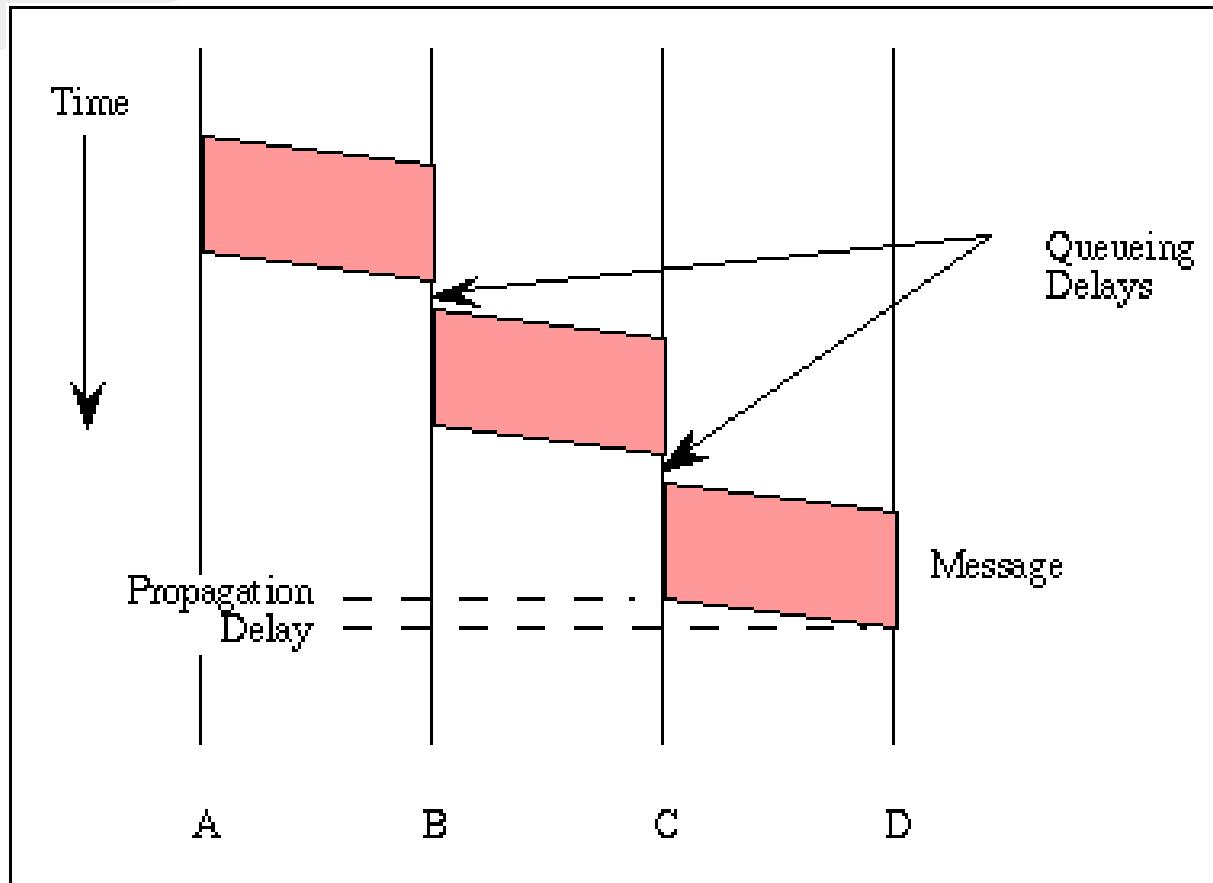
# Cut-Through Switch



# Store-Forward Switch



# Berichtvertraging bij store-forward



# WLAN Router Features

■ **Een WLAN router heeft, vergeleken met andere routers, volgende eigenschappen:**

- ◆ Is een AP
- ◆ Gebruikt Network Address Translation (NAT)
- ◆ Toegangscontrole (firewall)
  - IP-gebaseerd (beide richtingen, bron/doel)
  - Bepaalde inhoud/applicatie
  - Poort gebaseerd

# WLAN Antennes

- Intern/Extern
- Verwijderbaar of vast
- Directioneel/Alle richtingen
- Polarizatie (vertikaal/horizontaal)
- Breedte van de straal  
(beamwidth) en bandbreedte



# Antenne Concepten

## ■ Directionaliteit

- ◆ Alle richtingen (360°)
- ◆ Directioneel (beperkte zone dekking)



## ■ Gain

- ◆ Gemeten in dBi en dBd
- ◆ Meer gain betekent algemeen gezien meer dekking

## ■ Polarizatie

- ◆ Antennes staan meestal verticaal opgesteld

# Decibel (dB)

- Decibels zijn gemaakt om nummers weer te geven die in logaritmische grootte verschillen
  - ◆ bv 20 ten opzichte van 5,000,000,000,000
- Zelfs bij wetenschappelijke notatie is het verschil voor mensen niet heel duidelijk te zien
  - ◆  $2 \times 10$  en  $5 \times 10$  tot de 12de
- We nemen de verhouding tussen de twee nummers en gebruiken een logaritmische schaal

# Decibel berekeningen en metingen

- Het verschil van 2 niveaus wordt in decibels als volgt berekend

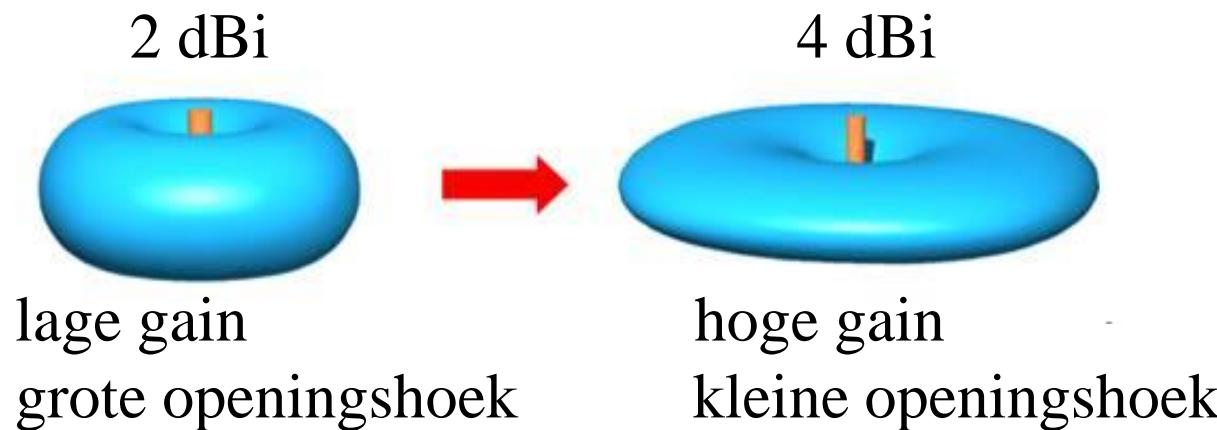
$$dB = 10 \log_{10} \left[ \frac{P_2}{P_1} \right]$$

- Negatieve dB = verzwakt signaal
- Positieve dB = versterkt signaal

- Bij verschillende sequentiele metingen over een volledig systeem, kan de totale db opgeteld worden

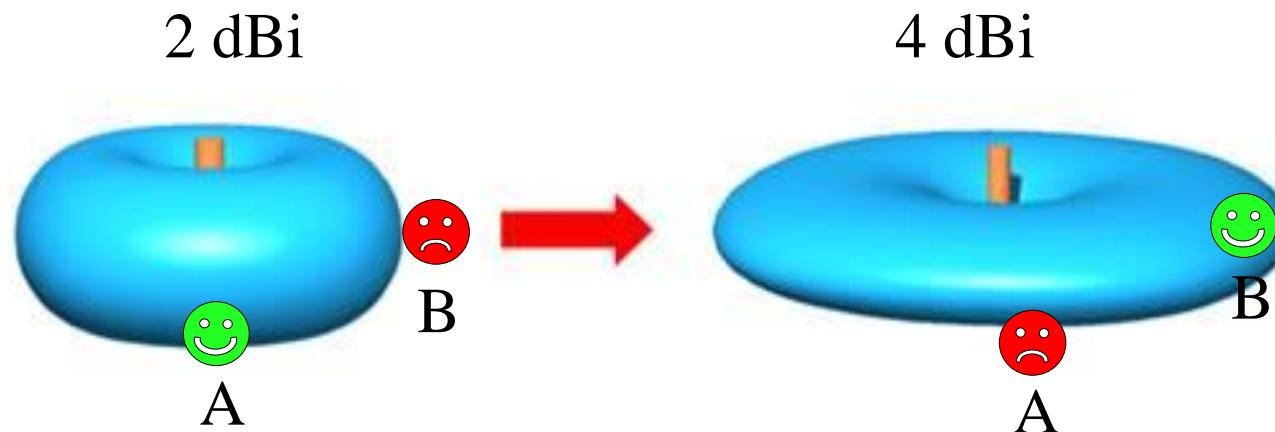
# Signaalwinst van een antenne (Gain)

- Wanneer de signaalwinst (**gain**) stijgt, vermindert de openingshoek (**angle**)
- De openingshoek wordt gemeten in graden
  - ◆ Ook wel “angle” of “beamwidth” genoemd
- Kan horizontaal en verticaal gemeten worden

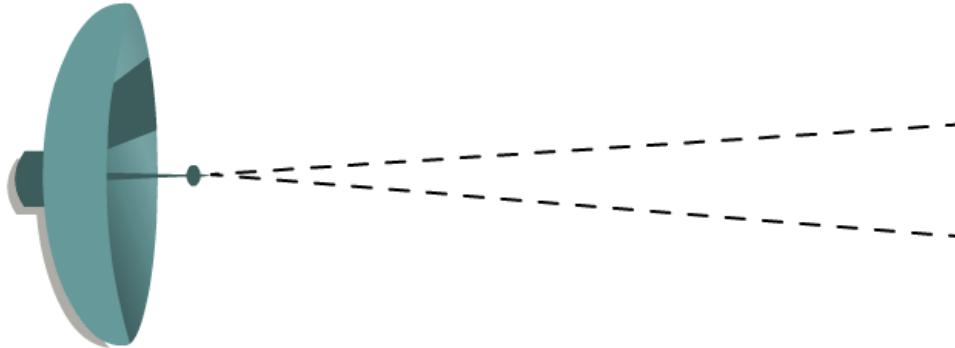


# Een hogere gain is niet altijd een betere dekking!

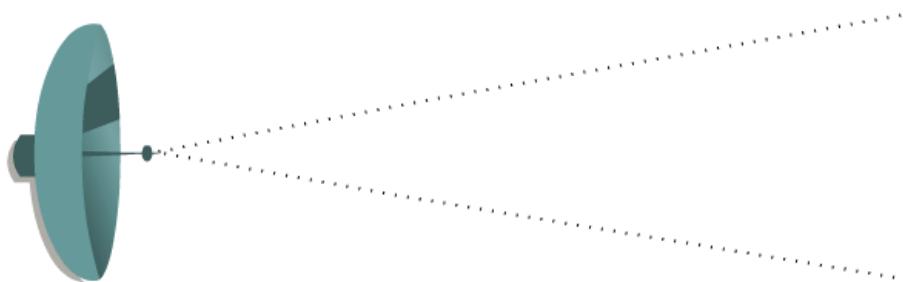
- Persoon B krijgt misschien een betere connectie door het verhogen van de gain, maar persoon A kan hierdoor een slechtere connectie krijgen
  - ◆ Dat komt omdat de openingshoek kleiner wordt



# Antenne beamwidth



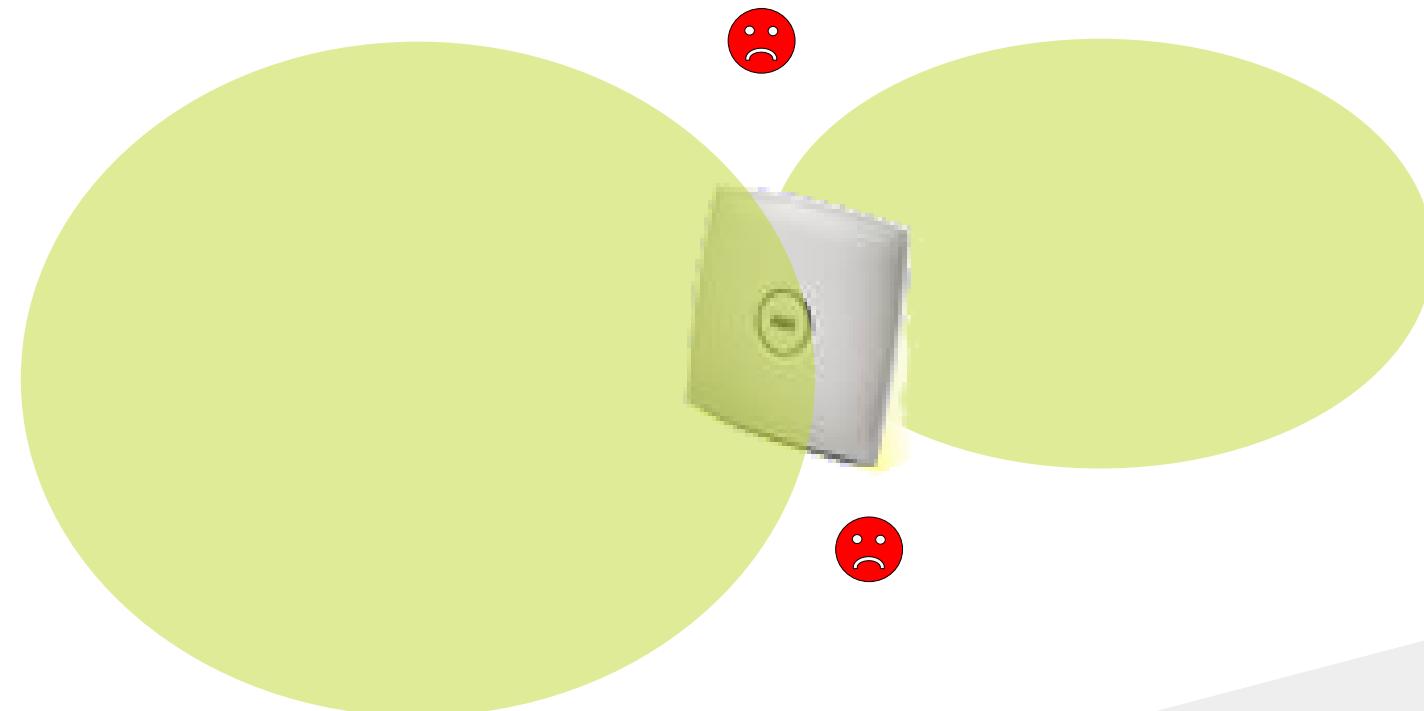
High gain antenne met kleine hoek en minder kans op interferentie



Lower gain antenne met groter hoek en meer kans op interferentie

# Omni-Directionele Antenne

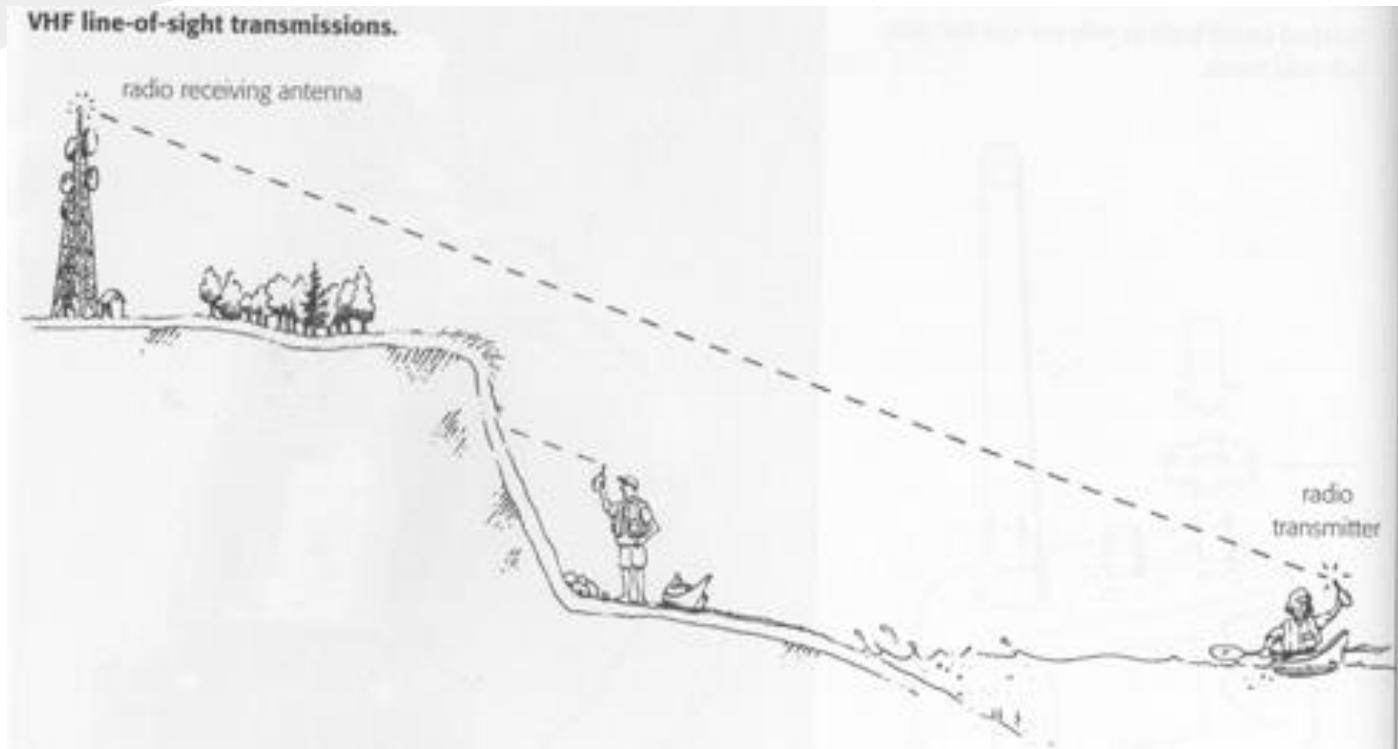
- **Groter dekkingsgebied**
- **Energieniveau dwars op de antenne is slecht**



# Antenne voorbeelden

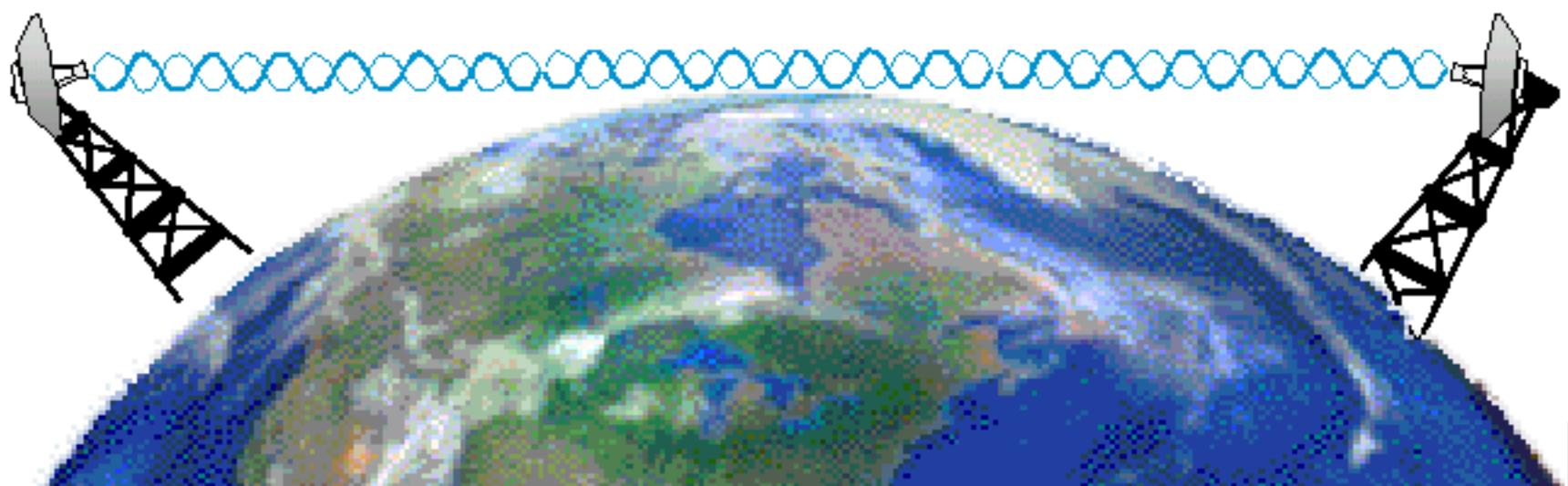


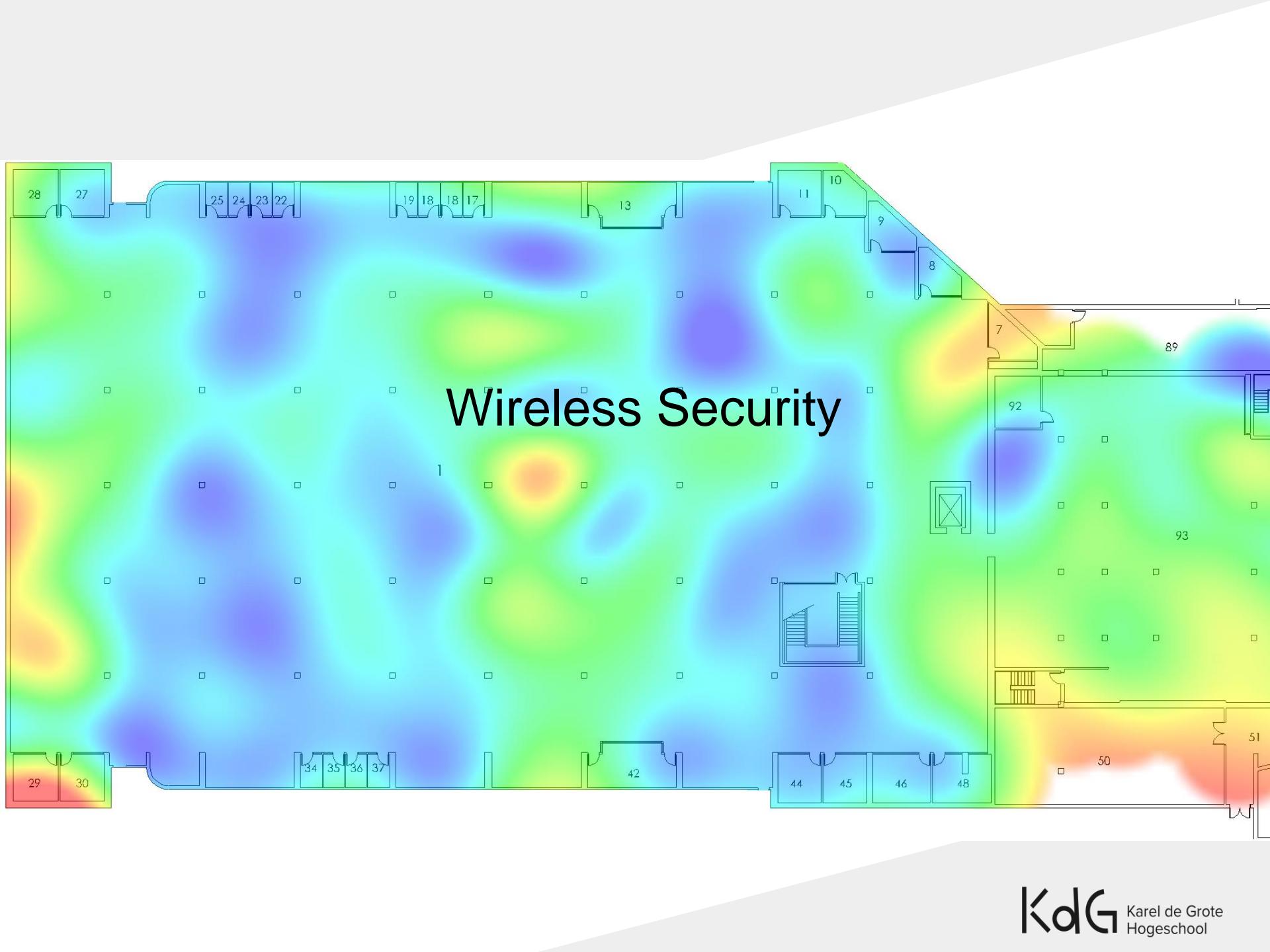
# Gezichtsveld



# Lange afstanden en gezichtsveld

Het gezichtsveld verdwijnt doordat de aarde rond is

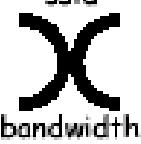




# Wireless Security

# Overzicht

- Evolutie WLAN Security
- Wireless Security in IEEE 802.11
- Verbeterde Security
- Vergelijk standaarden

let's warchalk..!	
KEY	SYMBOL
OPEN NODE	ssid  bandwidth
CLOSED NODE	ssid 
WEP NODE	ssid access contact  bandwidth

[blackbeltjones.com/warchalking](http://blackbeltjones.com/warchalking)

# Evolutie wireless

- **1997 Originele 802.11 standaard**
  - enkel SSID, MAC filter, WEP (Wired Equivalent Privacy)
- **2001 Fluhrer, Mantin en Shamir ontdekken zwakheden WEP**
  - IEEE richt "Task Group i" op
- **2003 Wi-Fi (industriegroep)**
  - Introducing Wi-Fi Protected Access (WPA)
    - Tussenoplossing voor WEP
- **2004 WPA2**
  - Gebaseerd op IEEE 802.11i standaard

# (E)SSID

- **(Extended) Service Set Identity**
  - **De "naam" van het draadloos netwerk**
- **Twee varianten van SSID**
  - **Ad-hoc draadloos netwerk**
    - **Clients zonder Access Point gebruiken SSID**
  - **Infrastructure netwerk**
    - **Clients gebruiken AP en een ESSID**
    - **Zendt beacon-frames: SSID wordt gebroadcast**
    - **Zwakheid: Sniffing mogelijk van SSID**
      - **Vraag maar aan Google**
      - **Noem je netwerk nomap\_**

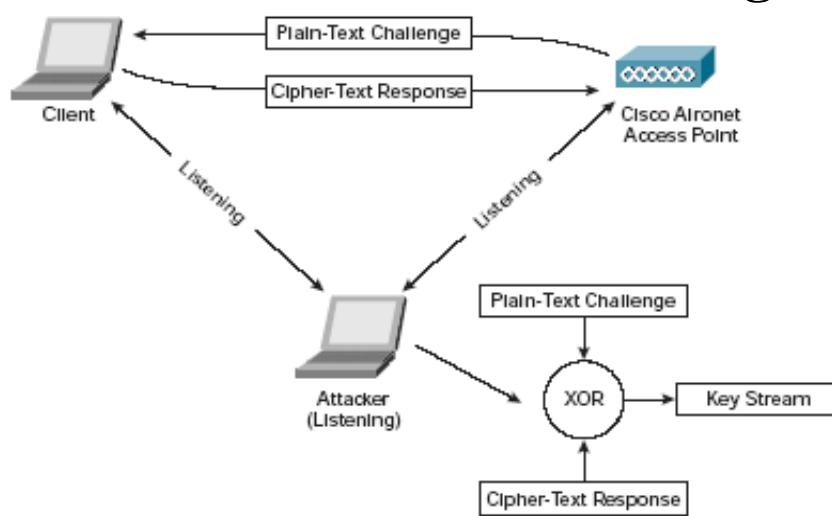
# MAC adres filter

- Elke client heeft een "werelduniek" MAC adres
- Access Point heeft een lijst met toegelaten MAC adressen
- **Zwakheid**
  - Toegelaten adressen worden gemakkelijk gesnift
    - Cleartext MAC adressen
  - Aanpassen MAC-Adres is eenvoudig

# Authenticatie WEP

- 802.11 heeft 2 authenticatie diensten:

- Open System authenticatie
  - Eender wie zich aanmeldt, wordt geauthenticeerd
- Shared-Key authenticatie
  - Client moet de gedeelde sleutel kennen om te verbinden
  - Zwakheid: sniffen van gedeelde sleutel processen



# Nadelen WEP

- **CRC is te eenvoudig om data integriteit te verzekeren**
  - WPA gebruikt hiervoor MIC

# Wi-Fi Protected Access (WPA)

- Tijdelijke oplossing voor WEP zwakheden
  - Werkt op bestaande hardware (enkel firmware update nodig)
- Onderdeel van 802.11i en dus forward compatible
- Doel
  - Verbeterde versleuteling
  - User authenticatie met 2 modi
    - WPA Personal : TKIP/MIC en Pre Shared Key (PSK)
    - WPA Enterprise : TKIP/MIC en 802.1X/EAP

# WPA Personal

- Encryptie TKIP
- Authenticatie met PSK (Pre-Shared Key)
  - Modus zonder authenticatieservers
  - Paswoordzin op alle clients en op de AP  
(Master sleutel wordt berekend)
  - Gebaseerd op four-way-key handshake (zie verder)
- Paswoordconfiguratie gelijkaardig aan WEP

# TKIP

## ■ **Temporal Key Integrity Protocol**

## ■ **Encryptiemethode**

- **Wrapper rond WEP**
  - **Gebruikt dezelfde RC4-Engine van WEP**
- **Gebruikt een MIC (Michael genoemd) op het einde van elk plaintext bericht (uitgebreide CRC)**
- **Verzekert dat berichten niet gespoofed worden**

# WPA Enterprise

## ■ **Authenticatie IEEE 802.1X/EAP**

- **Centraal beheer van gebruikersaccounts**
- **AAA server is nodig (Authenticatie, Authorizatie, Accounting)**
- **RADIUS protocollen voor AAA en sleuteldistributie**
- **Meerdere authenticatiemethodes**
  - **Met paswoorden, digitale certificaten**
    - **vb TLS met certificaten**
    - **vb PEAP, LEAP met paswoorden**

# Nadelen WPA

- Bij een zwakke paswoordzin kan het paswoord brute force gekraakt worden (best Random PSK key)
- Voor de top 1000 SSID / meest gebruikte paswoorden bestaan vooraf gegenereerde rainbowtables
  - Zwakheid in TKIP waardoor je valse ARP pakketten kan sturen  
Nov 2008 Beck Tews attack  
(De inhoud van ARP pakketten is bijna helemaal bekend dus deze zijn een gemakkelijk doelwit om er de MIC en de sleutel uit te halen)
  - Verkeer naar de client kan gedecrypteerd worden  
Feb 2010 Martin Beck
    - Verbetering is overschakelen naar AES (WPA2)

# WPA2

- AES gebruikt als encryptie (Dit is het grootste verschil met WPA)
  - Meestal in hardware (software is te traag)
- Twee modi zoals WPA
  - Personal Mode
    - Authenticatie PSK (Pre Shared Key)
    - Encryptie AES-CCMP
  - Enterprise Mode
    - Authenticatie 802.1X/EAP
    - Encryptie AES-CCMP

# WPA en WPA2: 4 way handshake

## ■ Gedeelde sleutel uitwisselen:

- Personal versie: sleutel ingegeven door paswoord
- Enterprise versie: sleutel tijdens authenticatie uitgewisseld

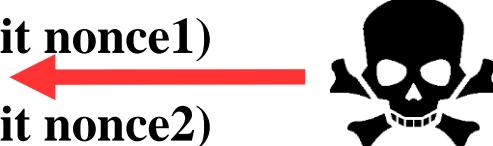
## ■ Sessie sleutel maken

- **Msg 1 client <- AP nonce1**
- **Msg 2 client -> AP nonce2**
- **Msg 3 client <- AP sessiekey1 (berekend uit nonce1)**
- **Msg 4 client -> AP sessiekey2 (berekend uit nonce2)**

# Key Reinstallation Attack

## ■ Probleem implementatie 4 way handshake

- Msg 1 client <- AP nonce1
- Msg 2 client -> AP nonce2
- Msg 3 client <- AP sessiekey1 (berekend uit nonce1)
- Msg 4 client -> AP sessiekey2 (berekend uit nonce2)



## ■ Attack

- 1. Blokkeren Msg4 (want deze rond de handshake af)
- 2. Doorlaten hertransmissie Msg3, hierdoor wordt nonce1 **gereset**
- 3. Hierna valse replays (bv commando's naar clients) of mogelijke decryptie of bij WPA valse pakketten.

## ■ Nodig

- Valse (MITM AP) tussen AP (met zelfde MAC als echte AP)

# Bij WPA2 extra Group Key

- Bij gebruik van broadcast en multicast is er, buiten de sessiesleutel, een extra Group Key die gebruikt wordt
- Deze wordt doorgestuurd na de normale 4 way handshake
- Werkt volgens hetzelfde als de 4 way handshake, maar dan met nonces van alle clients

# WPA3

- **Standaard 2018**
- **Sterkere encryptie. Minimum AES-128**
- **Doel:**
  - **Offline brute force verhinderen**
  - **Betere security bij zwakke paswoorden**
- **Maar: Downgrade attack mogelijk (dragonblood)**

# EAP -LEAP

## ■ Extensible Authentication Protocol

- Standaard 802.11 beveiliging van wireless

## ■ LEAP (Lightweight Extensible Authentication Protocol)

- Cisco manier om EAP te beveiligen. Bleek iets té lightweight te zijn en werd vrij snel gekraakt
- Gebruikte een op MS CHAP v1 protocol gebaseerde encryptie
  - Bij MSCHAPv1 is de zwakke LAN Manager Hash snel gekraakt

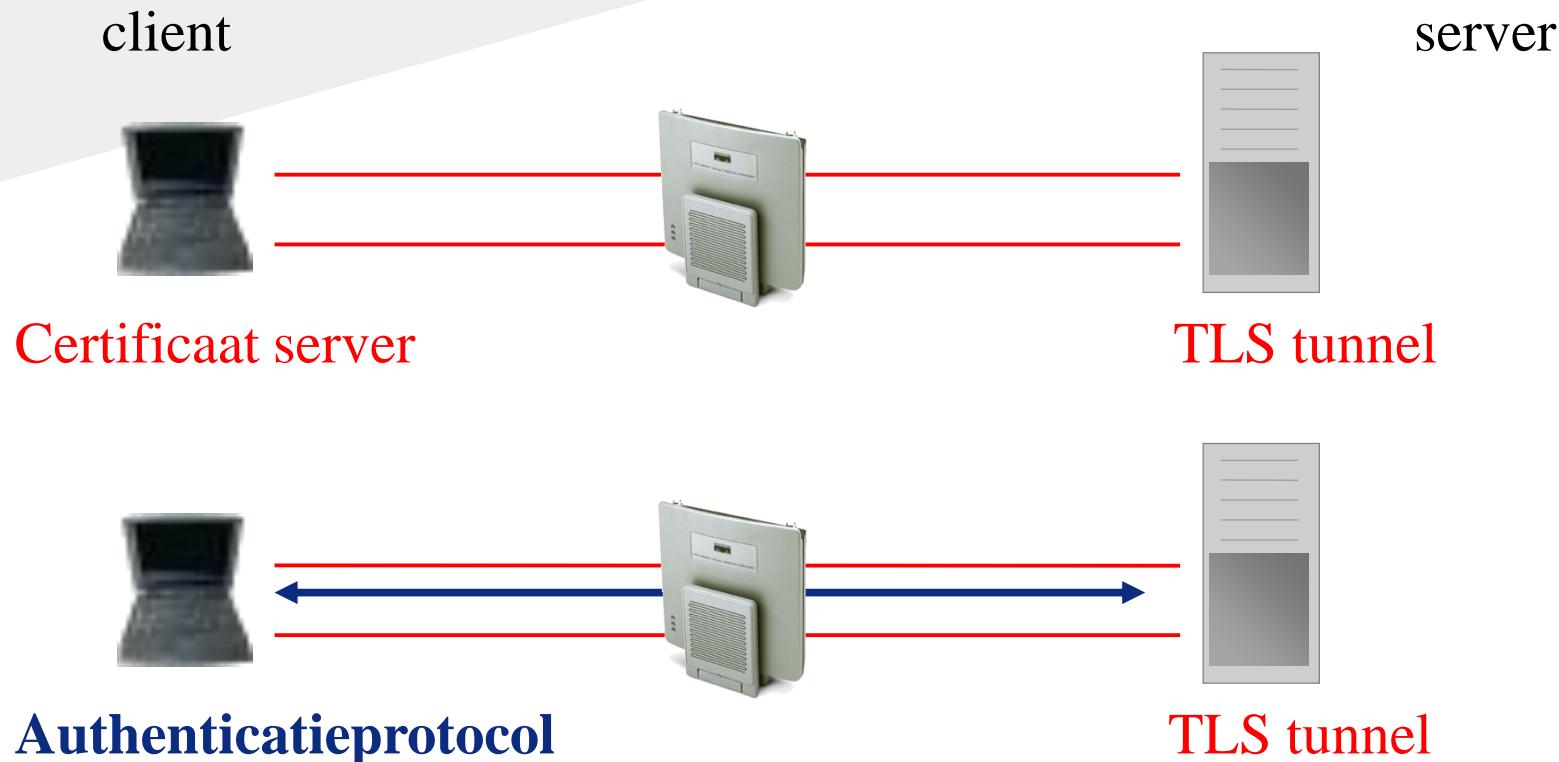
# PEAP

## ■ PEAP (Protected EAP)

- Minstens een server-side PKI certificaat
  - Hiermee wordt een beveiligde TLS tunnel gemaakt waarbinnen de authenticatie van de gebruiker loopt
- Sleutels voor de encryptie worden getransporteerd met de public key van de authenticatie server
- De uitwisseling van authenticatieinformatie met de client gebeurt nu in een geencrypteerde tunnel



# PEAP werking

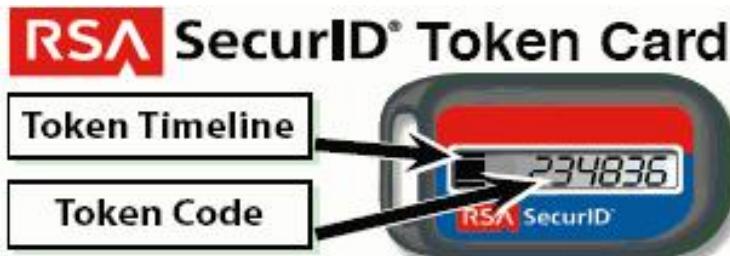


# EAP LEAP PEAP



## ■ PEAP

- Alle PEAPs gebruiken een beveiligde TLS tunnel,
- waarin ze een authenticatieproces uitvoeren
- PEAPv0 /EAP MSCHAPv2
  - Microsoft EAP (Microsoft ondersteunt enkel PEAPv0)
- PEAPv1/ EAP-GTC (Generic Token Card)
  - Gebruiker heeft een Token voor tijdelijk paswoord



Token Passcode = PIN + Token Code Number

# PEAP-EAP-TLS

## ■ EAP-TTLS (Tunneled Transport Layer Security)

- **Gelijkwaardig aan PEAPv0 (MSCHAPv2)**
  - Server certificaat maakt secure TLS tunnel
  - Ook een client certificaat
  - Binnen de tunnel volgt authenticatie met username/pass
- **Maar niet door MS verdeeld/ondersteund, dus niet zo veel gebruikt**



# Wireless KdG

- WPA2
  - AES encryptie
- PEAP v0
  - MSCHAPv2
- Servercertificaat
- Aanmelding via Radius server



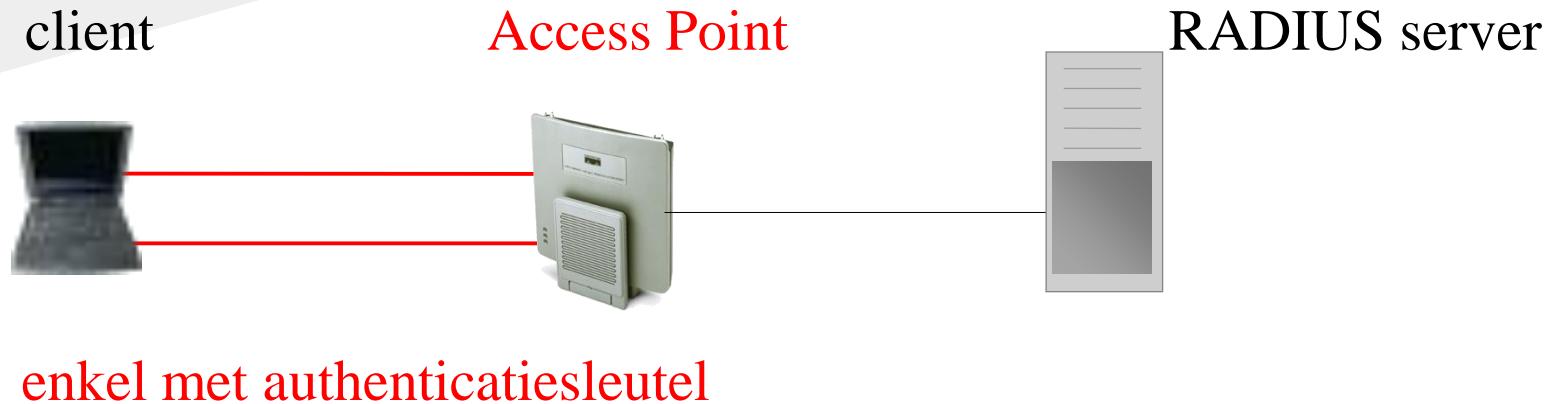
# Waarom een server certificaat?

- Valideren van het server certificaat maakt dat je zeker weet dat de server de echte server is
  - ... en geen valse Access Point waarachter een valse server staat
    - die MS-CHAPv2 handshakes kan verzamelen en binnen enkele seconden paswoorden kan kraken
- Maakt een geencrypteerde TLS tunnel waarover de authenticatie loopt.

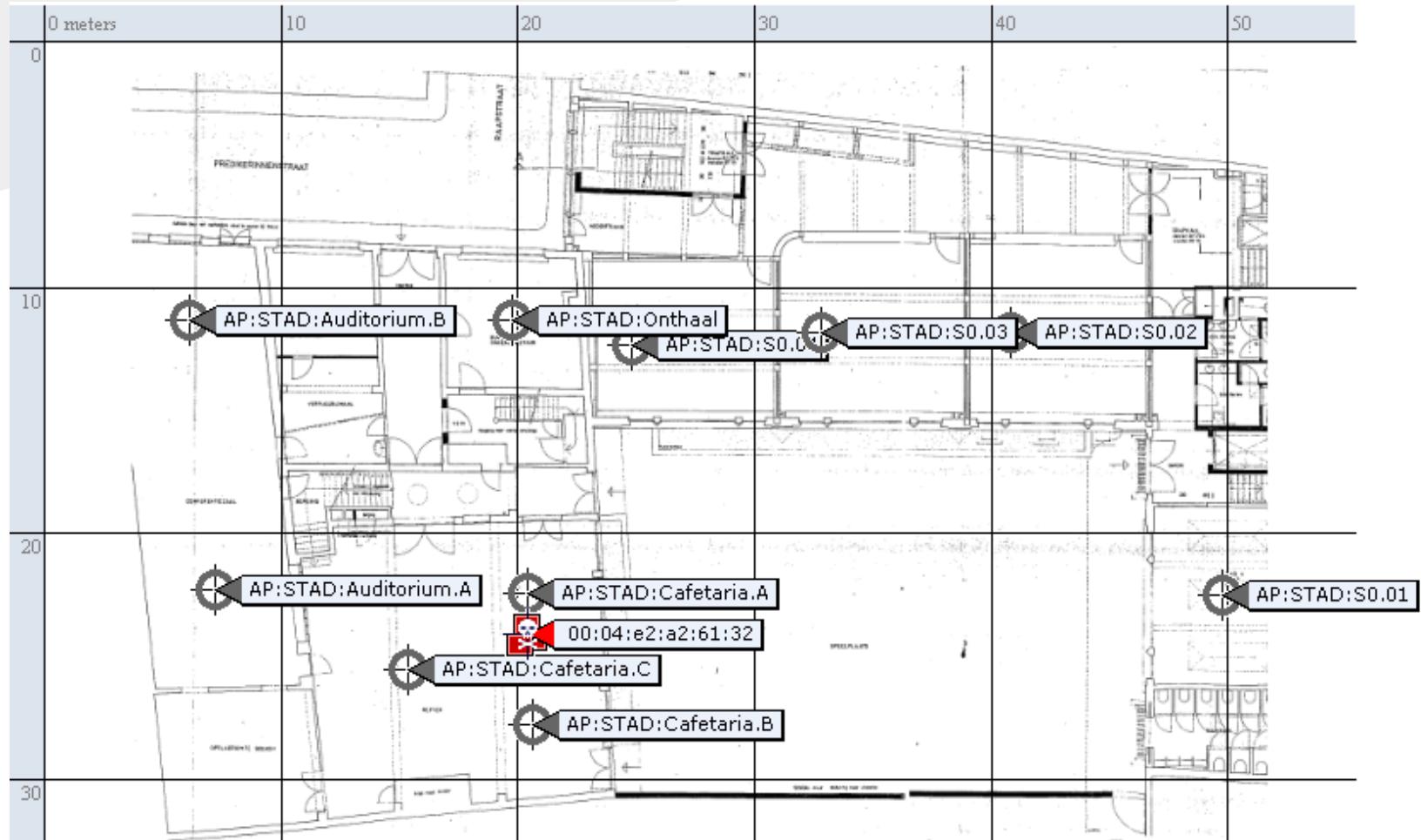
# RADIUS

- **Remote Authentication Dial-in User Service (RADIUS)**
- **Met een RADIUS server kunnen clients geen data verzenden over de AP's zonder een geldige authenticatiesleutel**
  - Client binnen range => AP stuurt challenge
  - Client authenticeert bij AP -> stuurt door naar RADIUS
  - Client stuurt credentials naar RADIUS
  - RADIUS server stuurt een geëncrypteerde authenticatiesleutel naar AP
  - De AP gebruikt deze authenticatiesleutel om beveiligde verbindingen op te zetten met de clients
    - Microsoft RADIUS server heet IAS

# RADIUS werking



# Stoorzenders detecteren (Stadswaag)



# Vergelijking security standaarden

		WEP	WPA
	WPA2		
■ Encryptiealgoritme	RC4		RC4
	AES		
■ Sleutelgrootte(bits)	40/128		128 per pakket
	128/256		
■ Key Life		24bit IV	48bit IV
	48bit IV		
■ Packet Key nodig		Concatenatie	TwoPhaseMix
■ Data Integriteit	CRC32	Security Niveau	Michael MIC
	CCM		
■ Sleutelbeheer	Geen		802.1X/EAP/PSK
	802.1X/EAP/PSK		



# Referenties

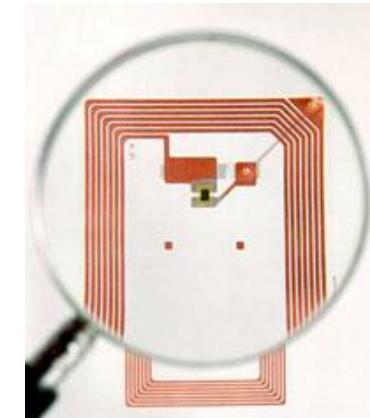
- **Unmanaged Internet Architecture (UIA)**
- **<http://pdos.csail.mit.edu/uia/>**
- **Key Reinstallation Attack Paper**  
**<https://papers.mathyvanhoef.com/ccs2017.pdf>**



# Wireless RFID

# Radio Frequency Identification (RFID)

- RFID is een op radiofrequentie gebaseerd systeem dat de mogelijkheid heeft om informatie op te slaan in apparaten
  - ◆ RFID tags genoemd
- RFID tags zijn intelligente barcodes die kunnen verbinden met een netwerk
- RFID tags kunnen in volgende categoriën worden opgedeeld
  - ◆ Actief
  - ◆ Semi-passief
  - ◆ Passief
- Een RFID systeem bestaat uit
  - ◆ Een transponder (in een tag, knop of label)
  - ◆ Een lees/schrijf unit



# RFID tags

## ■ Passief

- ◆ ID kan enkel gescand worden
- ◆ De meeste warenhuis/winkel tags zijn in principe niet RFID aangezien ze geen unieke ID hebben (wel bij Decathlon)

## ■ Actief

- ◆ Met batterij
- ◆ Kunnen signaal uitzenden (meestal met interval)
- ◆ Reikwijdte 100m tot enkele km

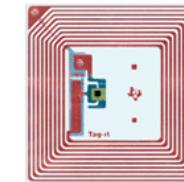
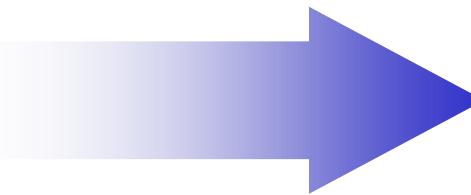
## ■ Semi Actief

- ◆ Met batterij
- ◆ Antwoorden enkel wanneer iets gevraagd wordt

# Barcode

vs

# RFID



- **Identificatie artikel type**
  - **Per stuk ("één voor één") lezen**
  - **Korte leesafstand**
    - ◆ enkele centimeters
  - **Directe zichtbaarheid noodzakelijk**
  - **Eenmalig aanmaken**
  - **Lezen extra handeling**
  - **Lage productie kosten**
  - **Eenvoudig aan te brengen**
- 
- **Identificatie artikel exemplaar**
  - **Tegelijk ("bulk") lezen**
  - **Op afstand leesbaar**
    - ◆ enkele meters
  - **Directe zichtbaarheid niet nodig**
  - **Herprogrammeerbaar (sommige)**
  - **Lezen als deel van de handeling**
  - **Duur in vergelijking met barcode**
  - **Aanbrengen kost aandacht**

# RFID frequenties

## ■ Mogen niet storen met bestaande systemen

- ◆ Identificatie mens/dier (1 EUR -80 EUR)
  - 125 kHz -134,2 KHz (Low Frequency, LF) 0,05-0,10 meter
- ◆ Bibliotheek (0,2 EUR - 1 EUR)
  - 13,56 MHz (High Frequency, HF) 0,3 meter
- ◆ Supply chain/ luchtvaartbagage/Decathlon (0,05-0,5 EUR)
  - 868 tot 955 MHz (Ultra High Frequency, UHF) 3-6 meter
- ◆ Tolpoorten/ fleet management (20 – 70 EUR)
  - Actieve tags
  - 2,45 GHz (Microwave, MW) 10 meter -1000 meter
  - 5,8 GHz

# Nadelen RFID

- **Passieve tags werken niet met vloeistof/metaal in de nabijheid**
  - ◆ 125 KHz tags worden niet gestoord
- **Tags die te dicht tegen elkaar liggen storen elkaar**
  - ◆ Bv 13,45 MHz tags moeten op 60 cm liggen
- **Beveiliging van RFID is er niet (gewoon een binaire datastream met nummer)**
  - ◆ Dus niet om prijzen in op te slaan

# Voorbeeld RFID

- Aiko heeft een passieve RFID tag
- Deze kan uitgelezen worden met een frequentie van 134,2 KHz
  - ◆ Maximum afstand 5 cm

hier



# Voorbeeld passieve RFID De Lijn / NMBS

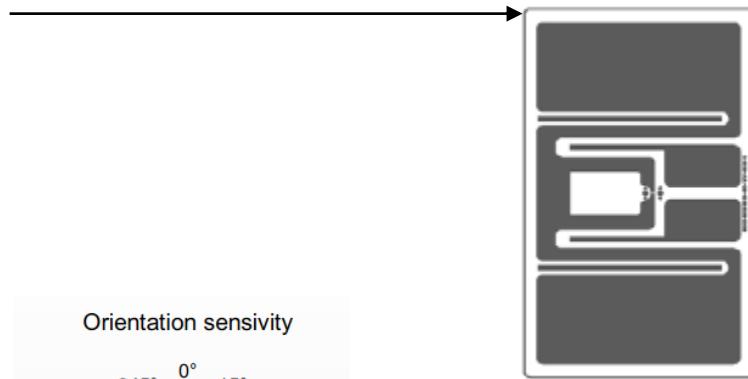


# UHF Tag Decathlon

- **200.000 unieke tags**
- **kassa 15% sneller**
- **beveiligingspoort: niet gescand item is niet betaald**

# Tageos EOS-300

- Frequency: 865-868 MHz
- Antenne = rechthoek 5x3 cm
- Prijs: 45 euro per 1000 stuks
- Uitleeshoek is belangrijk:



# RFID jammer



# Wireless

Infrarood communicatie

# Infrarood (IR)

- Al in de eerste 802.11 standaard
- Niet zo populair voor WLANs
- Zeer beperkte reikwijdte
- Gebruikt voor WPANs (Wireless Personal Area Network)
- Korte reikwijdte en lage snelheid

# IR Operaties



## ■ Belangrijkste IR onderdelen:

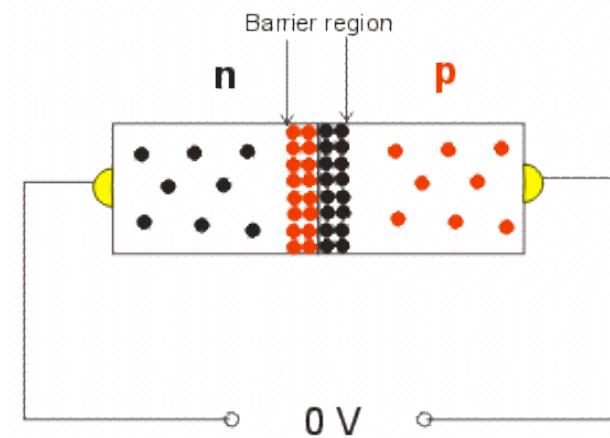
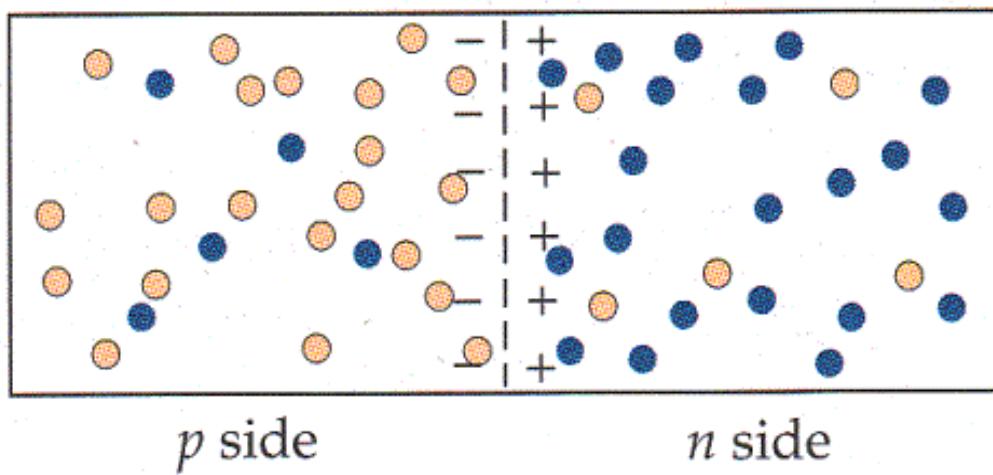
- Light-emitting diode (LED)
  - Elektronisch apparaat dat licht uitstuurt om data te coderen
- Ontvanger
  - Ontvangen lichtstraal en decoderen data

## ■ IR MOET binnen het gezichtveld, en gericht, binnen hetzelfde vlak

# Wat is een diode?

- Een diode bestaat uit twee elektrodes met wat bufferruimte ertussen

- electrons
- + holes



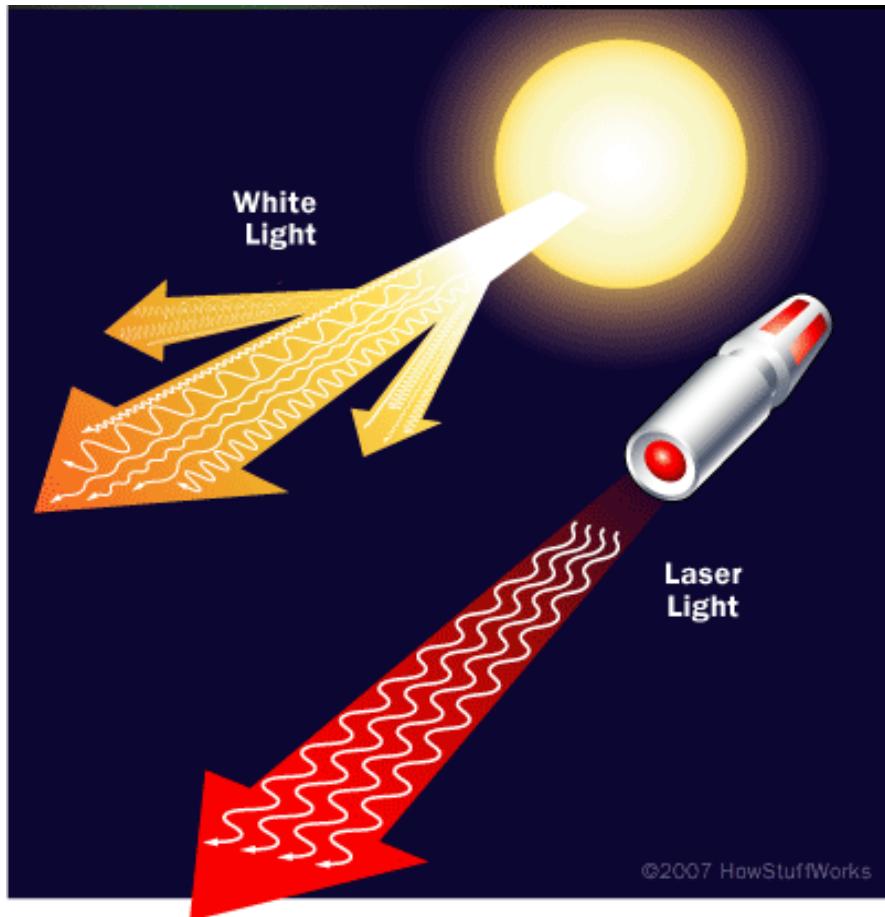
# Werking diode

- De 2 elektrodes bestaan uit materiaal dat bestaat uit atomen
  - Positief geladen (P-type)
    - Hebben ruimte (holes) voor extra elektronen
    - Extra elektronen kunnen aangetrokken worden uit een negatief geladen atoom
  - Negatief geladen (N-type)
    - Hebben extra (vrije) elektronen
    - Deze kunnen weggetrokken worden door een positief geladen atoom

# En toen was er licht

- Bij de interactie van elektronen en holes van N-type en P-type materiaal komen er deeltjes vrij: de *Photonen*
- Afhankelijk van het materiaal geven photonen
  - Zichtbaar licht (hoge frequentie)
  - Onzichtbaar licht (lage frequentie)
    - Het aantal, de frequentie, de energie en de kleur van het licht hangen af van het materiaal
- Meeste IR licht in netwerkapplicaties gebeurt met laser diodes
  - Een hele kleine chip genereert een constant licht

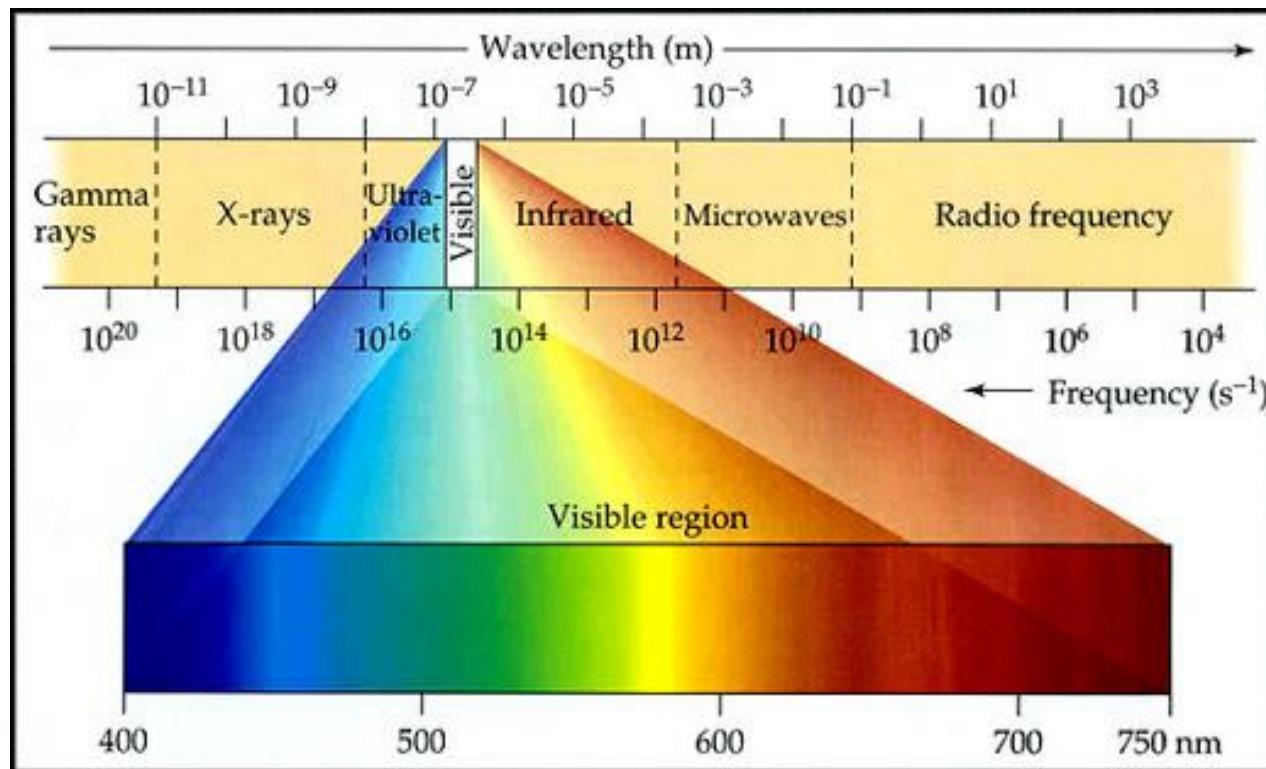
# Lasers



# IR Netwerken

## ■ IR technologie voor netwerken

- Near IR (NIR)
- Bijna dezelfde eigenschappen als echt licht



# Infrared Data Association (IrDA)

- IrDA is een onafhankelijke organisatie
- Schrijft en publiceert standaarden zodat IR van verschillende fabrikanten kan communiceren
- IrDA heeft verschillende versies

IrDA Versie	Data snelheid	Power opties
1.0	115.2 Kbps	Standaard
1.1	4 Mbps	Standaard
1.2	115.2 Kbps	Laag
1.3	115.2 Kbps en 4 Mbps	Laag/Standaard

# IrDA

- Werkt in half-duplex mode
- Storing gebeurt door
  - Omgevingslicht
    - Zon, lampen
- Het IrDA protocol zoekt verbinding door sniffing, stuurt data door en verbreekt de verbinding

# Wireless



Bluetooth



# Introductie

## ■ **Personal Area Network (PAN)**

- **Netwerken in beperkt gebied voor persoonlijk gebruik**

## ■ **Connectie van:**

- **Telefoons**
- **Computers en randapparatuur**
- **Video Games en DVD spelers**
- **TVs, beveiligingssystemen, ...**



# Bluetooth Gebruik



# Bluetooth



- Ericson 1994
- Deense koning Harald Blauwtand
  - At graag blauwbessen, waarvan hij blauwe tanden kreeg
  - Logo van Bluetooth zijn de initialen van Harald in runetekens
- RF technologie die ad-hoc PANs maakt binnen 10 meter
- Gebruikt frequency-hopping
- Bluetooth specificatie definieert het protocol
- Bluetooth profiel definieert de verschillende applicaties



# Bluetooth Protocollen



## ■ Bluetooth lagen:

- **RF communicatie met Object Exchange OBEX**
- **Verbindingsbeheer Link Manager Protocol LMP**
  - **Synchroon en Asynchroon**
- **Service discovery Protocol**



# OBject Exchange (OBEX)

- **Communicatieprotocol dat het uitwisselen van binaire objecten tussen apparaten gemakkelijker maakt**
- **Zowel bij IrDA als bij Bluetooth**
  - **OBEX heeft een gelijkaardig design als HTTP**
  - **Client verbindt via TCP naar een server en wisselt objecten uit**

# Link Manager Protocol (LMP)



- **Zet verbindingskanalen op tussen Bluetooth apparaten**
  - **Authenticatie**
  - **Encryptie (na uitwisselen sleutels en onderhandeling over de baseband pakketgrootte)**



# Synchroon en asynchroon

- **Synchroon Connection Oriented (VOICE)**
  - Reserveert Time slots
  - Geen hertransmissie van verloren frames
- **Asynchroon Connection Less (DATA)**
  - Afspraak lengte, modulatie
  - Wel hertransmissie
  - Verbinding schakelt zelf uit na bepaalde stilteperiode



# Service discovery protocol (SDP)

- **Protocol dat uitzoekt welke services er mogelijk zijn en op welke manier er mee kan verbonden worden**
  - **Bv Mobiele telefoon verbindt met headset**
- **Elke service heeft een Universally Unique Identifier (UUID)**



# Bluetooth Transmitters

- Bluetooth gebruikt FHSS (**Frequency Hopping Spread Spectrum**)
  - pseudorandom wisselen tussen verschillende frequenties
    - minder storing van specifieke frequenties
    - moeilijker af te luisteren
- Bandbreedte 2.402 – 2.480 GHz
- Bluetooth definieert 3 klassen
  - Class 1 (tot 100 m & 100 mW)
  - Class 2 (tot 10 m & 2.5 mW)
  - Class 3 (tot 10 cm & 1 mW)
    - effectieve reikwijdte hangt af van omgeving(storing)



# Bluetooth Netwerk

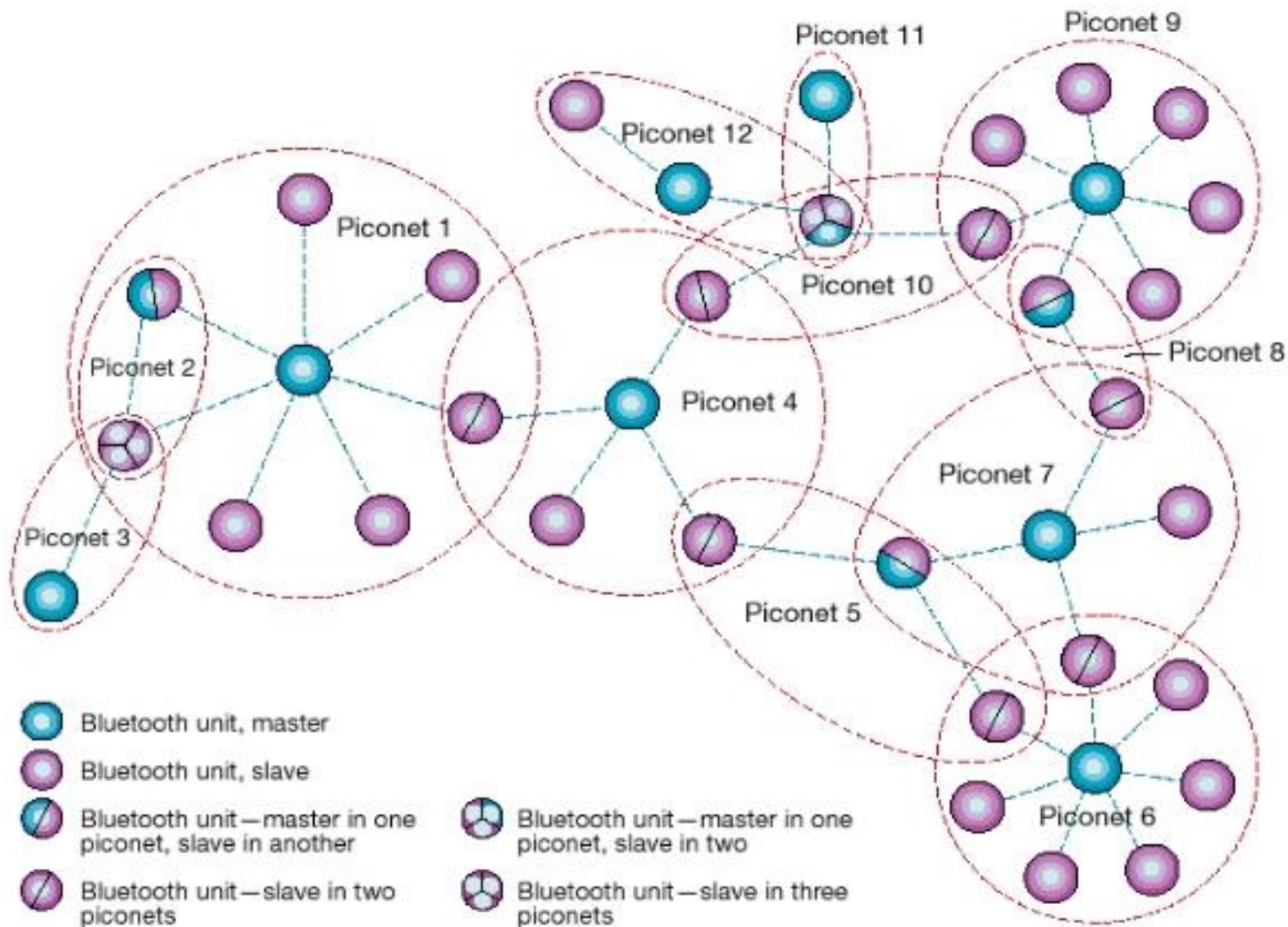
- Het Bluetooth netwerk wordt aangemaakt op een ad-hoc manier door de link manager (discovery van alle diensten)
- Een ad-hoc Bluetooth netwerk heet een ‘**piconet**’
  - Piconet bevat max 8 apparaten
  - Meer dan 8 apparaten => extra piconet
- Een aantal piconets samen wordt een ‘**scatternet**’ genoemd
  - Toestellen sturen elkaar communicatie door
  - Bij elke verbinding is één apparaat de master en een ander de slave

# Piconets



- **Master kan verbinden met max 7 actieve slaves**
  - **Tot 255 (3 bit MAC adres) slaves kunnen passief klaarstaan "geparkeerd" tot dat de master hen actief maakt**

# Scatternet





# Verbinden van Bluetooth apparaten

- Meeste Bluetooth devices vragen aan de gebruiker om “discovery” op te zetten
  - Met PIN codes:
    - Verhinderen dat eender wie verbinding maakt
    - PIN (personal identification number) verhindert dat eender welk apparaat een verbinding maakt

## Bluetooth Mobile Phone Set Up

### Pairing with the mobile phone

Your mobile phone will ask you to enter a passkey. Check your mobile phone to see if it is ready to accept a passkey. When your mobile phone is ready please enter in the following passkey:

**472754**

Once you have entered the passkey on your mobile phone the pairing process will be completed.

# Bluetooth Profielen



- Streamen van audio (naar headphone of autoradio)
- Op afstand aansturen TV/radio/stereoketen
- Doorsturen foto's voor camera/printer/GSM
- Afdrukken documenten/email (zonder printer driver)
- Extra info over device doorsturen (fabrikant/versie)
- Muis, keyboard, joystick, WII, Playstation, ..
- Hoofdtelefoon GSM (bellen, opnemen, volume)



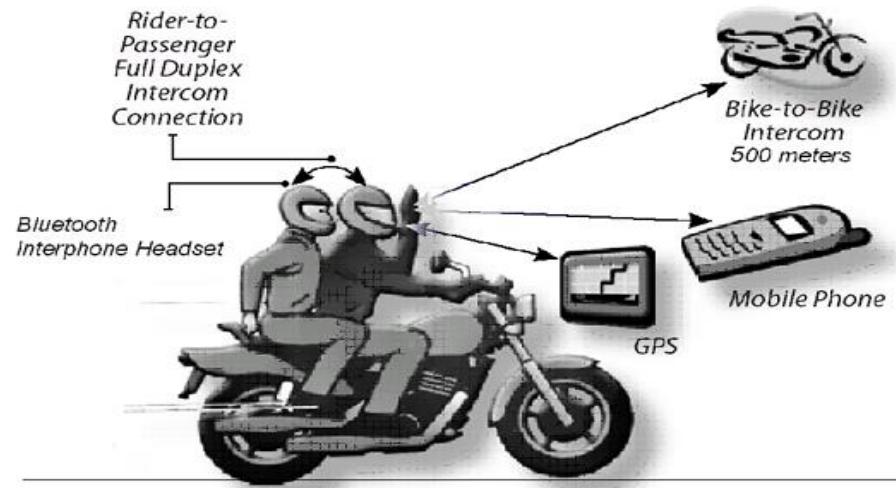
# Hands free zonder Bluetooth





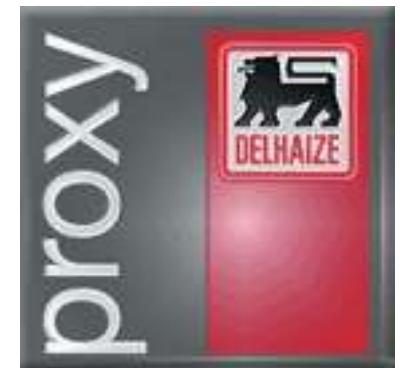
# Bluetooth Profielen

- Intercom Profiel (tussen 2 bluetooth devices)
- Personal Area Networking Profiel
- Ingebouwde telefoons in wagens gebruiken de SIM kaart van de aanwezige telefoon
- Telefoonboek toegang



Proxy servers

# Proxy servers



# Proxy

- Een proxy server is een hulpje dat verschillende diensten voor jou kan uitvoeren op internet, zoals

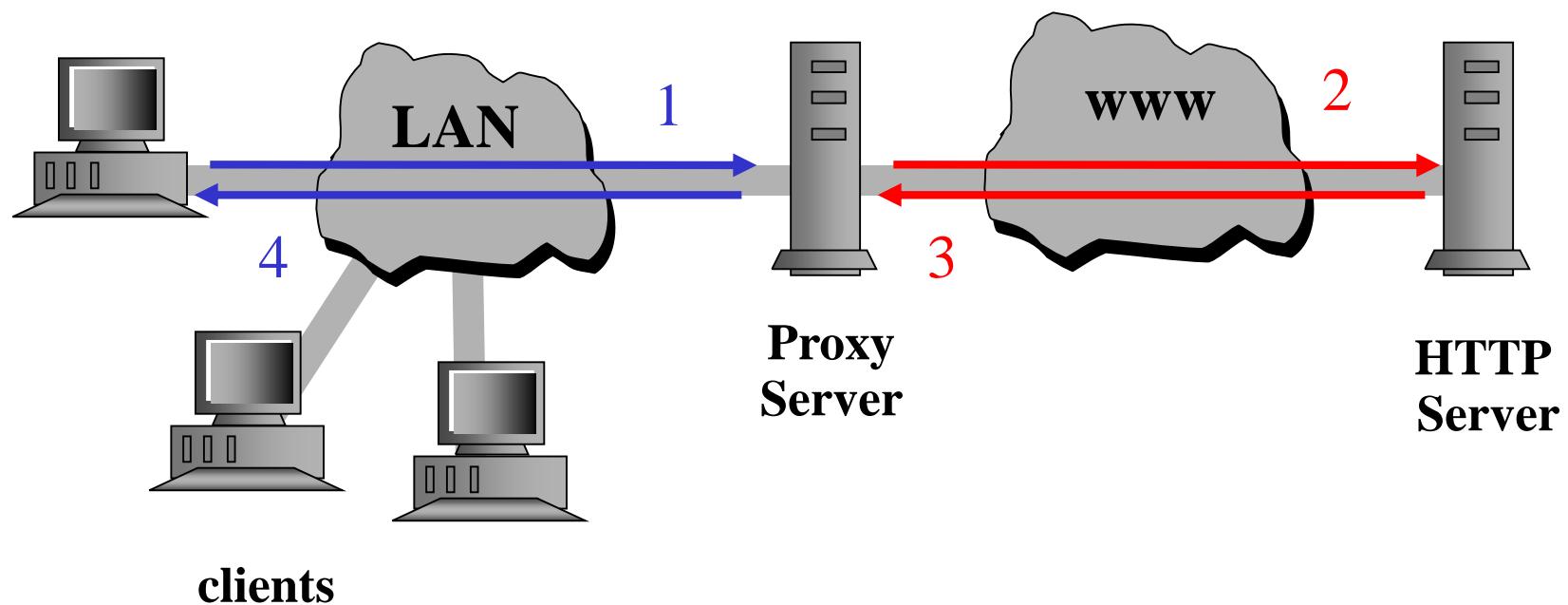
- ◆ HTTP
- ◆ FTP
- ◆ Telnet
- ◆ Real Audio
- ◆ DNS
- ◆ SOCKS



# Werking

- 1) De gebruiker stuurt een aanvraag naar het adres en de poort van de proxy**
  - 2) De proxy gaat namens de gebruiker het internet op**
  - 3) De computer op internet stuurt een antwoord terug naar de proxy**
  - 4) De proxy maakt een nieuw antwoordpakket aan en stuurt dat door naar de gebruiker**
- 
- **De computer op internet communiceert enkel via de proxy met de gebruiker.**
  - **Tijdens dit proces heeft de proxy de mogelijkheid om in toegangsregels of ACL's (Access Control Lists) na te gaan of een bepaalde actie geoorloofd is of niet.**

# Werking in schema



## Disk cache

- Dit is ruimte op de harde schijf van de proxyserver waar tijdelijk bestanden en HTTP documenten worden weggeschreven.
- Hiervoor moet een bepaalde grootte in MB opgegeven worden. Wanneer de disk cache vol zit, worden de oudste bestanden vervangen door nieuwe bestanden. Een FIFO (First In First Out) systeem dus.

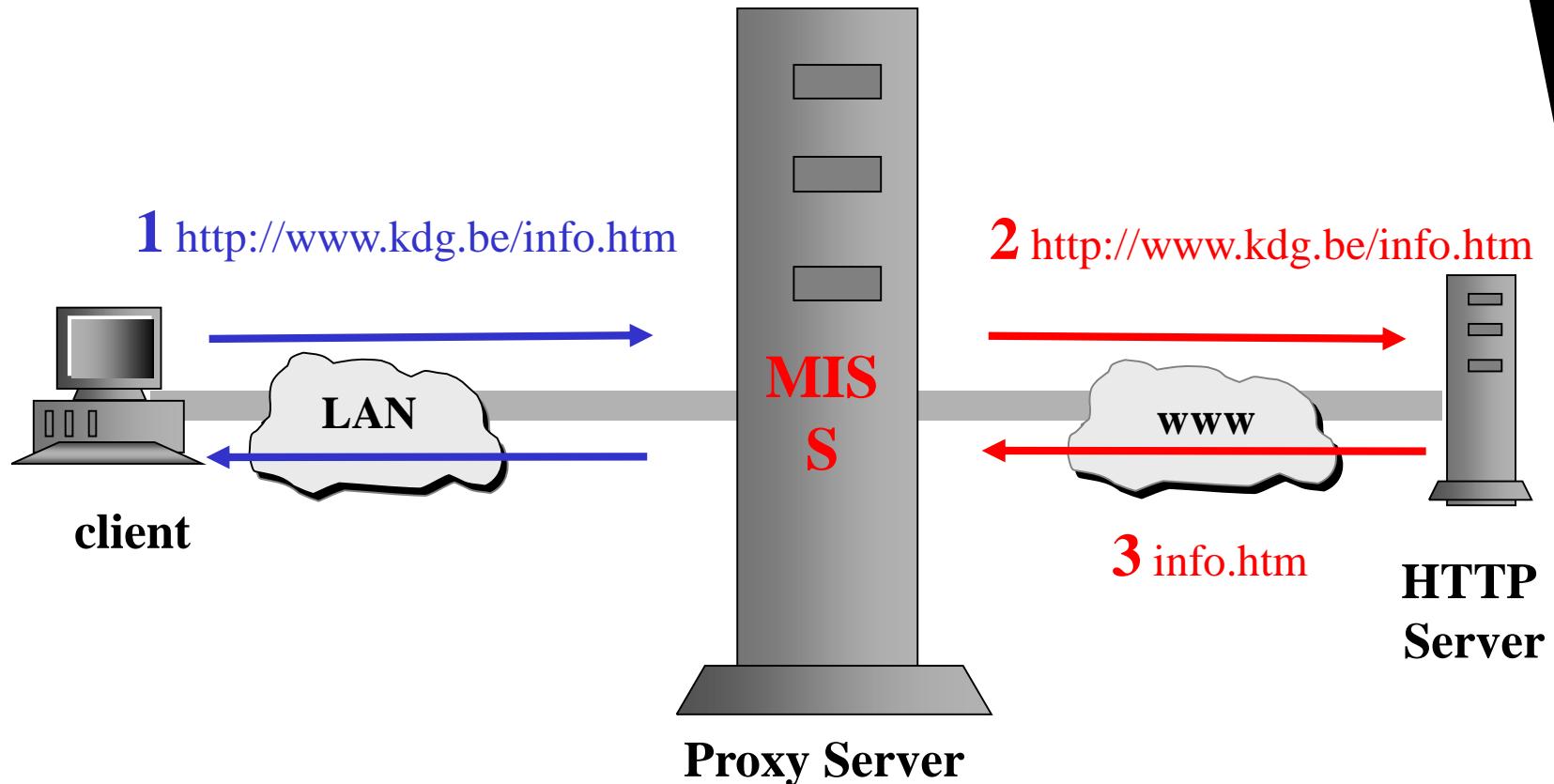
## Disk cache 2

- Doordat de gegevens in de disk cache staan, moeten ze niet opnieuw afgehaald worden van een andere server op het netwerk, maar kunnen ze rechtstreeks van de schijf van de proxy server gehaald worden. Wanneer een tweede gebruiker dus hetzelfde document ophaalt, hoeven we dus niet meer de computer op internet te raadplegen.
- Wanneer de proxy server een pagina terug vindt in zijn disk cache, dan spreken we van een **HIT**. Is dit niet zo, dan spreken we van een **MISS**.

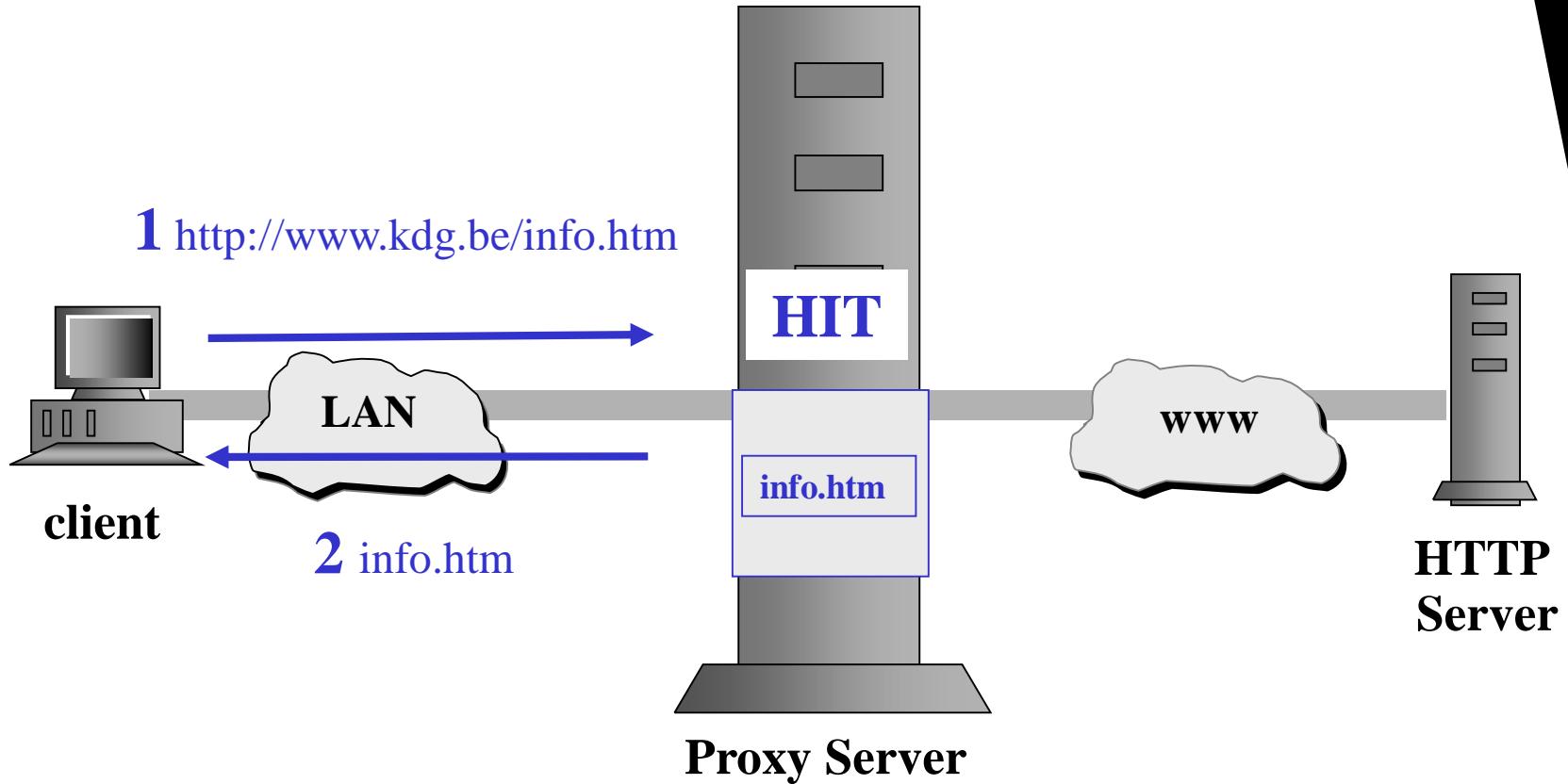
## Disk cache <> cache

- Voor de duidelijkheid: Disk cache heeft niets te maken met de hardware cache van een systeem. (Hardware cache is enkele honderden kiloBytes bv 256kB of 512kB, disk cache is enkele honderden MegaBytes tot Gigabytes).

# Disk cache MISS



# Disk cache HIT



## Functie: Client accelerator

### ■ De client accelerator of standard proxy cache

- ◆ Maakt gebruik van een disk cache om reeds opgehaalde gegevens geen tweede keer te gaan ophalen.



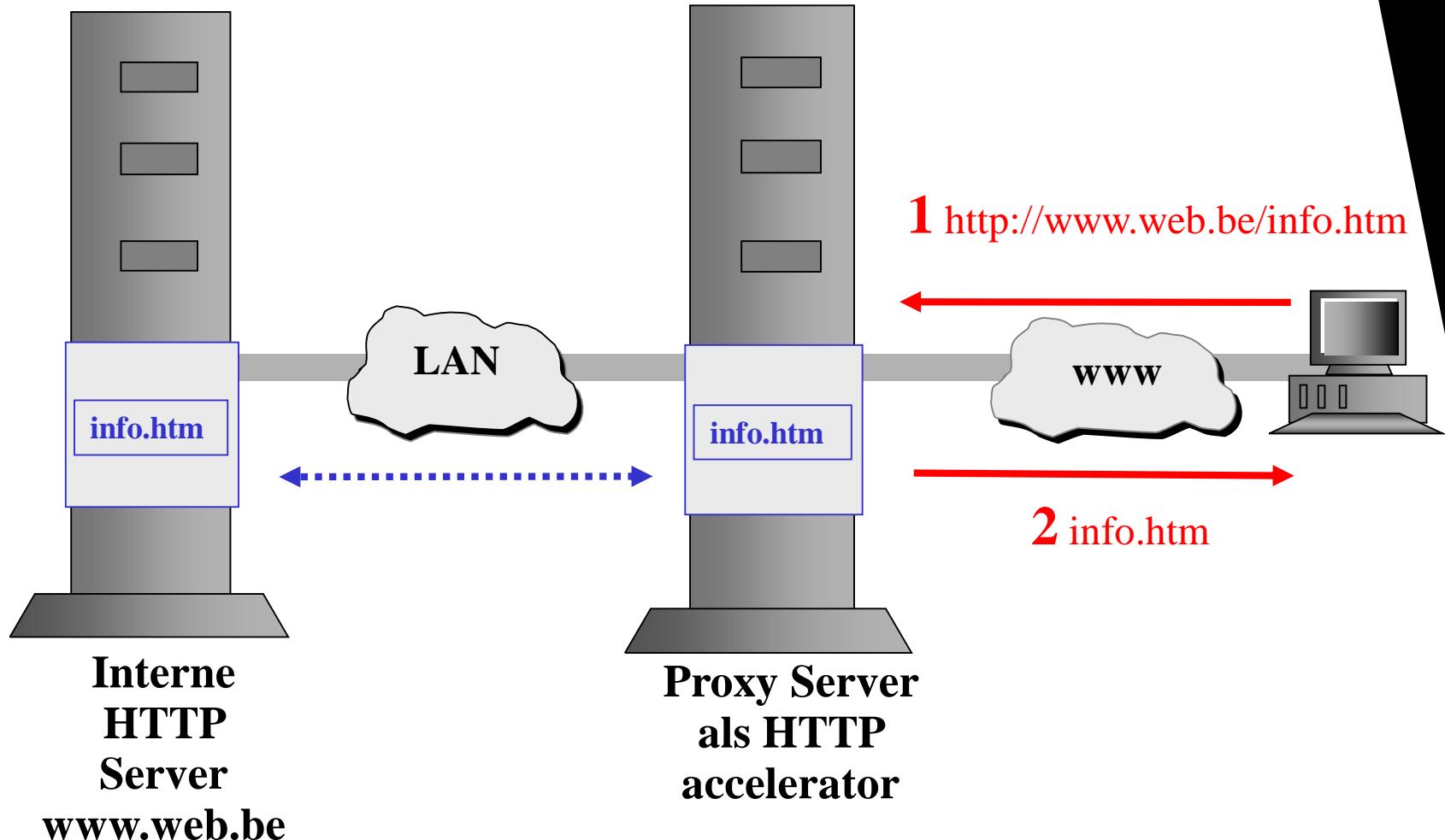
## Functie: HTTP accelerator

- **De proxy doet dienst als een front-end voor webservers op het lokale netwerk.**
- **Door een HTTP accelerator te gebruiken kunnen we het verkeer op een lokaal netwerk onlasten.**
  - De gebruiker die vanuit internet de gegevens van onze lokale webserver wil raadplegen, start geen verbinding op met de eigenlijke webserver maar wel met de HTTP accelerator.

## Functie: HTTP accelerator 2

- Gegevens die statisch zijn zoals gewone webpagina's worden vanuit de proxy cache gegeven.
- Dynamische gegevens, zoals gegevens die uit databanken worden gehaald, worden rechtstreeks van de webserver gehaald.
- De HTTP accelerator heeft ook een firewall functie. Gebruikers van het internet kunnen niet rechtstreeks binnen in het privé netwerk.

# HTTP accelerator bij statische pagina



Interne  
HTTP  
Server  
**www.web.be**

Proxy Server  
als HTTP  
accelerator

# Functie: Hierarchische proxy cache

- Deze komt voor in grotere netwerken.
- Doel is het zo snel mogelijk ter beschikking stellen van gegevens. De gebruiker vraagt gegevens aan zijn standaard proxy. Wanneer deze de gegevens niet heeft vraagt hij ze aan een volgende proxy, die op zijn beurt weer contact maakt met de volgende proxy, enzovoort.
- MISS
  - hiërarchisch hoogste proxy vraagt gegevens op.
- Proxies geven gegevens aan elkaar door tot aan de proxy die het dichtst bij de gebruiker staat.

## Voordelen

- **Snelheid:** Reeds opgehaalde documenten moeten niet een 2de keer opgehaald worden, ze staan nog in de disk cache van de proxy server
- **Beveiliging:** Vanuit internet ziet men enkel een proxy server staan. Je eigen netwerk blijft verborgen achter de proxy server.
- **Beveiliging:** Een proxy kan gebruik maken van ACL's om verkeer toe te laten of te weigeren.

# Cache principe

- **Het cache principe van de proxy wordt ook lokaal bij de client toegepast.**
  - ◆ Browsers gebruiken standaard een cache op je schijf (Tempory Internet Files) om bezochte websteks in op te slaan. Wanneer je op een reeds bezochte pagina komt haalt hij deze niet op vanuit Internet maar lokaal vanuit de cache.

## HTTP en FTP cache

- Voor de cache van HTTP documenten kan je minimum en maximum grootte bepalen van de bestanden. Je kan ook instellen of je een bestand blijft downloaden, ook al heeft de user op de STOP knop gedrukt.
- De cache voor FTP bestanden is gelijkaardig.
- Sommige documenten kunnen expliciet als *non-cacheble* gedefinieerd zijn voor een browser. Wanneer je Refresh of Reload kiest, zal de browser het bericht automatisch als non-cacheble definiëren.

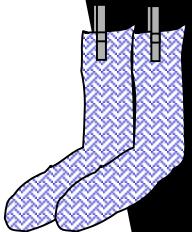
# Validatie van berichten

- **Is een bericht veranderd sedert het in de cache is gekomen? Twee methoden:**
  - ◆ 1. Aanvraag aan de webserver of de pagina intussen veranderd is.
  - ◆ 2. Proxy server kijkt zelf naar de datum en tijdstip van het document
    - De 2de methode is de snelste maar geeft mogelijk een verouderd document. Wanneer de gebruiker Reload kiest wordt toch het nieuwste document van de webserver gehaald.
    - Voor de 2de methode kan je een TTL waarde definiëren (Time To Live)
      - bv www adressen: 2 uur
      - gif files: 7 dagen
      - cgi-bin 30 minuten.

# Mail

- Lokale mailadressen gaan niet via internet maar worden door de lokale server (niet de proxy server) afgeleverd.
- SMTP server opgeven: De proxy moet weten waar hij de mail server voor uitgaande post kan vinden.
- POP3 server opgeven: De proxy moet weten van welke server hij post kan binnenhalen.

# SOCKS



- SOCKS laat toe dat hosts aan de ene kant van de proxy volledige toegang krijgen tot hosts aan de andere kant van de proxy. De SOCKS server voorziet gebruikersnaam en paswoord, en stuurt data door. SOCKS wordt algemeen gebruikt als een netwerk firewall die interne hosts volledige toegang verleent tot het Internet en de toegang tot de interne hosts afschermt voor het Internet.
  - ◆ Programma's zoals putty.exe en telnet kunnen gebruik maken van socks

# SOCKS versies

## ■ SOCKS versie 4

- ◆ Geen UDP proxy, geen authentificatie, geen DNS resolving (zoekt geen IP bij een onbekende hostnaam)

## ■ SOCKS versie 5

- ◆ Browsers ondersteunen SOCKS aan de client kant.
- ◆ Ondersteuning anonymous FTP (met e-mail adres=paswoord= nobody@)
- ◆ username+password in *cleartext*!
- ◆ Automatisch een verbinding leggen naar een ISP

# Socks version 6 -snelheidsverbeteringen

- **Ondersteuning TCP Fast Open (RFC7413)**
  - ◆ TCP SYN bevat al data, eerste ACK bevat al een antwoord
- **0-RTT ondersteuning (Zero Round Trip Time)**
  - ◆ Bij een Pre Shared Key wordt deze sleutel gebruikt om al tijdens de TLS handshake geencryptede data te versturen
    - Dat noemt men **early data**
- **Socks wacht niet op de authenticatie van de client maar opent alvast een socket**

# ICP Internet Cache Protocol

- **Proxy servers zijn opgebouwd in een watervalstructuur (een boomstructuur eigenlijk).**
  - Jou proxy kijkt of een naburige of hoger gelegen proxy server reeds bepaalde documenten heeft.
  - Men spreekt van cascading proxies of hierarchische proxy's.
- **De communicatie tussen proxy servers gebeurt met het ICP of Internet Cache Protocol.**

## Voordelen ICP

- Een aanvraag gebeurt via verschillende proxies (verdelen het werk)
- De snelste proxy geeft antwoord
- Slecht ingestelde of niet werkende proxies worden gedetecteerd.
- Squid (de meest gebruikte proxy server op Unix/Linux systemen) ondersteunt ICP

# Begrippen bij ICP

- **Neighbour:** proxy server die samenwerkt met je proxy server
- **Parent:** proxy server op een hoger niveau
- De proxy server kan aan een nabijgelegen proxyserver vragen of hij bijvoorbeeld al een bepaalde pagina opgevraagd heeft. Is dit zo dan spreken we van een HIT. Is dit niet zo, dan spreken we van een MISS.

# ICP: communicatie met de parent

- **De parent heeft een cache waarin geraadpleegde pagina's en bestanden worden bijgehouden. Mogelijke opties:**
  - authenticatie: kiezen of de parent ook authenticatie doet (dus username en paswoord moet bijhouden)
  - HTTPS (secure HTTP): kiezen of dit door jou of door de parent proxy wordt opgevangen
  - Ondersteuning van GET en POST opdrachten. Een POST stuurt de data die je invult bij een CGI, perl, PHP of ASP script achteraf onzichtbaar voor de gebruiker op.  
Een GET stuurt alle gebruikersdata mee met de URL (als optie). bv. <http://mail.yahoo.com/mail.asp?user:jan?pass:ok>
  - Ondersteuning FTP

# Interfaces naar proxyserver

- **Secure:** De interfaces van het lokale netwerk waarvoor je de proxy diensten voorziet
- **Insecure:** Normaal gezien uw modem connectie of netwerk connectie naar Internet

# Logs

- Security logs
- Error logs met verkeerde paswoorden
- Onveilige ip-nummers
- Standaard wordt elke opgevraagde pagina gelogd.

# ACL's (toegangsregels)

## ■ Blokkeren of toelaten:

- ◆ van bepaalde IP-nummers of ranges
- ◆ van bepaalde interfaces (netwerkkaart/modem)
- ◆ van het verkeer op bepaalde tijdstippen
- ◆ van bepaalde URL's
- ◆ van bepaalde types bestanden (zip, gif, mpg, html,...)
- ◆ van services (icp, http, https, ftp, telnet, socks, real audio)

# Referenties

## ■ TCP Fast Open

- ◆ <https://tools.ietf.org/html/rfc7413>

## ■ SOCKS Protocol Version 6;

- ◆ <https://tools.ietf.org/html/draft-olteanu-intarea-socks-6-02>

## ■ Squid Configuration

- ◆ <http://www.squid-cache.org/Doc/config/>

## ■ 0-RTT Handshake

- ◆ <https://ldapwiki.com/wiki/0-RTT%20Handshakes>

# ATM inleiding

## Asynchronous Transfer Mode WAN Protocol

# ATM

- **Ontstaan midden jaren 80 bij ontwikkeling van (Broadband) B-ISDN**
  - ◆ Spraak
  - ◆ Data
  - ◆ Video

# ATM Technologie

INTERNATIONALE STANDAARD

LAN en WAN TECHNOLOGIE

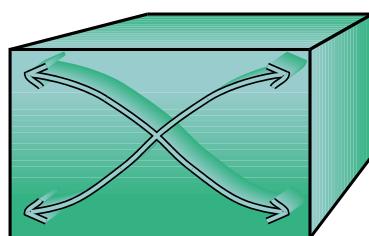


# ATM concepten



## ■ Connection oriented.

- ◆ End-to-end virtual circuits
- ◆ Kwaliteitsgarantie (QoS)



## ■ Circuit switched.

- ◆ Capaciteit ligt vast



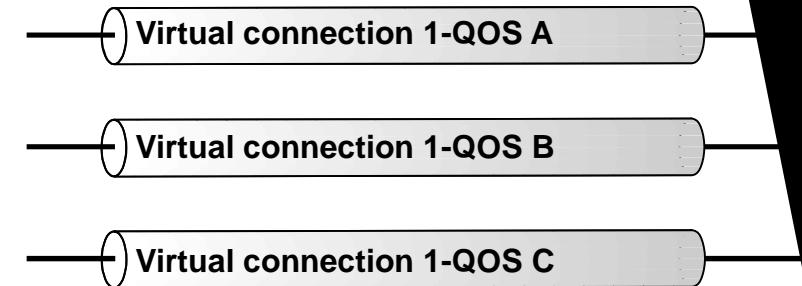
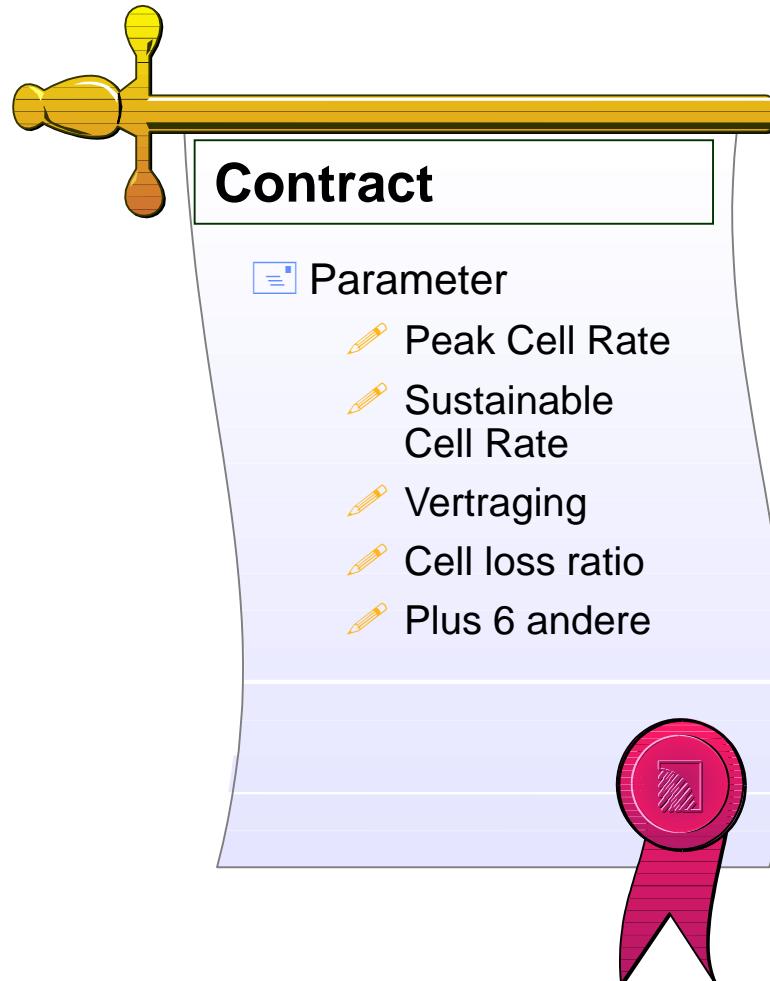
## ■ ATM-cel als basis

- ◆ Klein maar heeft vaste lengte

# Negotiated Service Connection

- **Vóór een verbinding moet er een traffic contract vastgelegd worden met volgende parameters :**
  - ◆ Peak Cell Rate
    - Maximum snelheid voor piekverkeer
  - ◆ Average Cell Rate
    - Gemiddelde snelheid
  - ◆ QoS (Quality of Service)
    - Vertraging en verlies van cellen

# Quality Of Service



# QoS ondersteuning

- Voor een verbinding kan er een **Quality of Service** vastgelegd worden.
- Voorbeeld parameters:
  - ◆ cell loss ratio
  - ◆ cell delay
  - ◆ cell delay variation
- Bij het aanmaken van een verbinding controleert elke ATM switch met de CAC (*Connection Admission Control*) functie of aan de QoS kan voldaan worden. Lukt dit, dan kan de verbinding gemaakt worden.

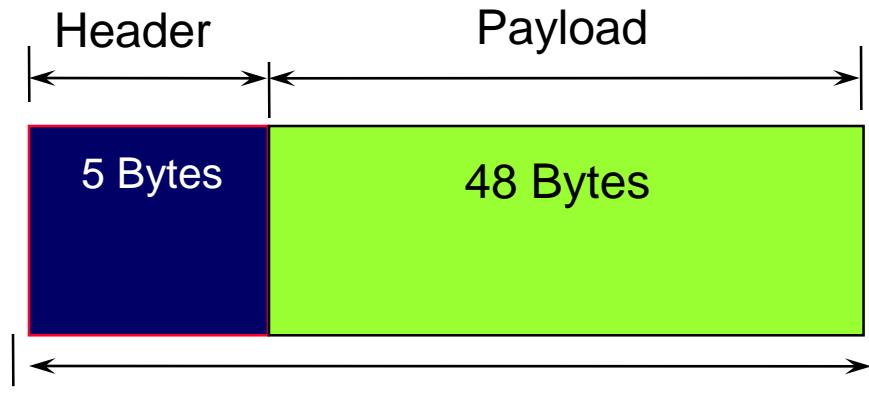
# ATM concepten: Switch gebaseerd

- ATM werkt niet shared (zoals een hub)
- ATM werkt geschakeld:
  - ◆ Verschillende toegangssnelheden
  - ◆ Toegekende bandbreedte en capaciteit

# ATM concepten: Cel gebaseerd

- **Zoeken naar de ideale lengte van een pakket (cel)**
  - ◆ Een lange cel kan meer informatie bevatten dan een kleinere maar heeft relatief veel vertraging bij het vullen van de cel.
  - ◆ Een kleine cel is sneller gevuld maar heeft weer relatief veel overhead informatie ten opzichte van de user data.
- **Europa wou 32 Bytes, Amerika 64 Bytes**
  - ◆ ...dus werd het 48 Bytes data
- **ATM cel 53 Bytes:**
  - ◆ 5Bytes header + 48 Bytes data

# Een ATM cel



- **Kleine afmetingen:**
  - ◆ Header is 5 bytes
  - ◆ Payload is 48 bytes
- **Header bevat info over virtual circuit**
- **Payload kan spraak, video of data zijn**

# Virtuele circuits: PVC en SVC

## PVC

- ◆ Een Permanent Virtueel Circuit is een vast gealloceerde verbinding tussen twee eindgebruikers
  - Van te voren vastgestelde piek (PCR)
  - Gemiddelde bandbreedte (SCR).
    - Deze toepassing wordt gebruikt voor data (zoals een huurlijn)

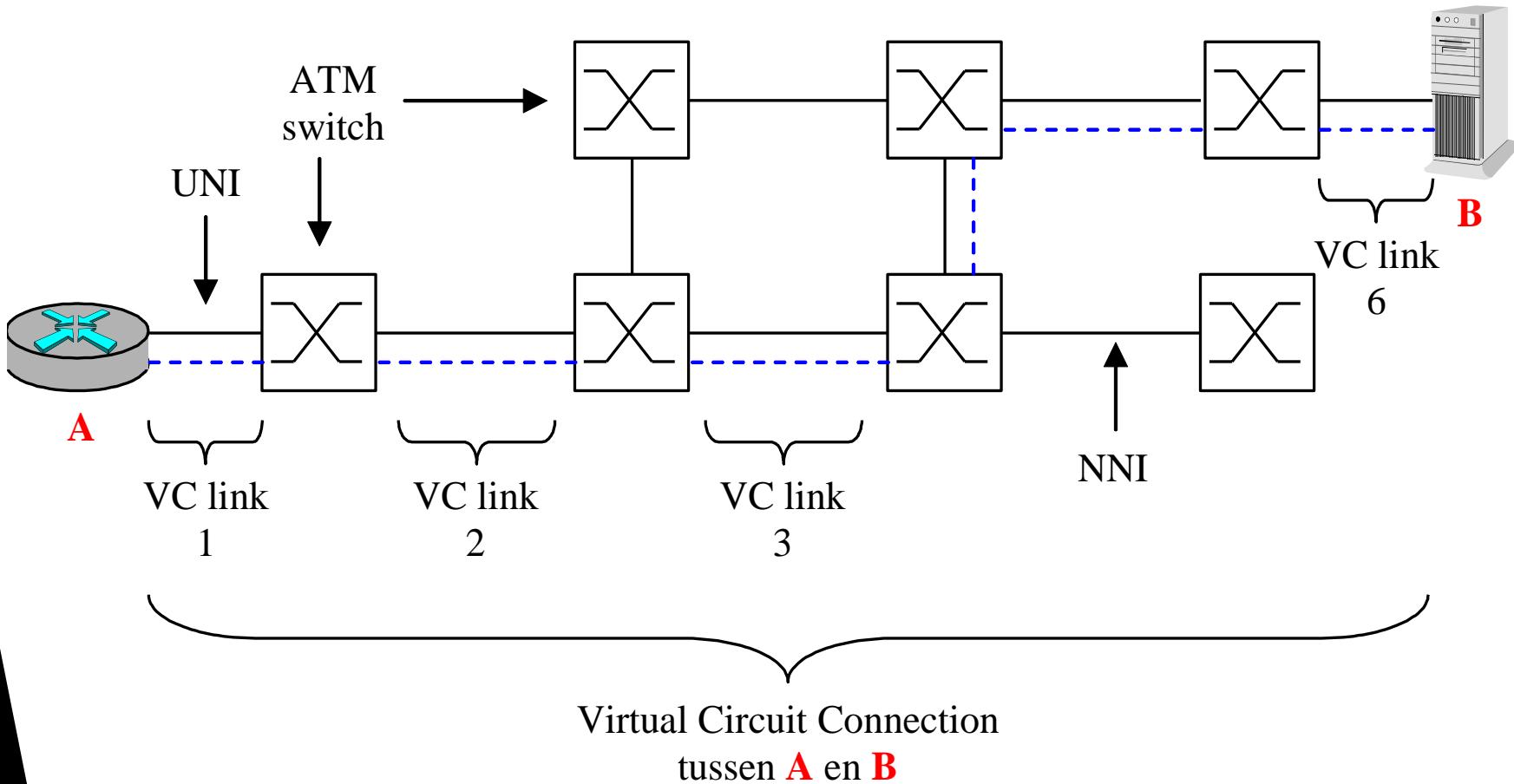
## SVC

- ◆ Switched Virtual Circuits zijn gestandaardiseerde netwerk verbindingen tussen eindgebruikers
  - Slechts opgezet wanneer en zolang als nodig (zoals een gewone telefoonlijn)

# ATM interface

- Twee soorten UNI en NNI
- **UNI: User-Network Interface**
  - ◆ Rand netwerk : Meer bits voor toepassingen
- **NNI: Network-Network Interface**
  - ◆ Binnen netwerk : Meer bits voor routes

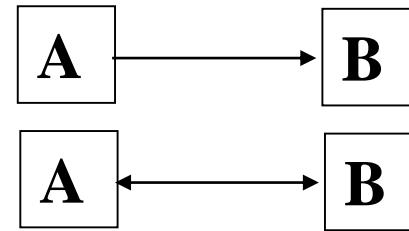
# ATM Netwerk



# Soorten verbindingen

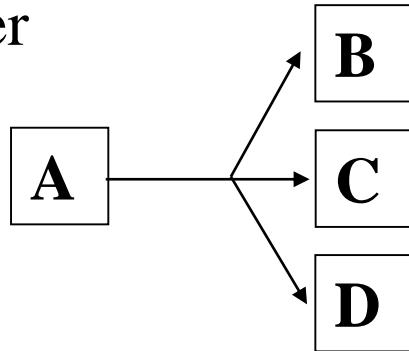
## ■ Point -to- Point

- ◆ Eénrichtingsverkeer
- ◆ Tweerichtingsverkeer

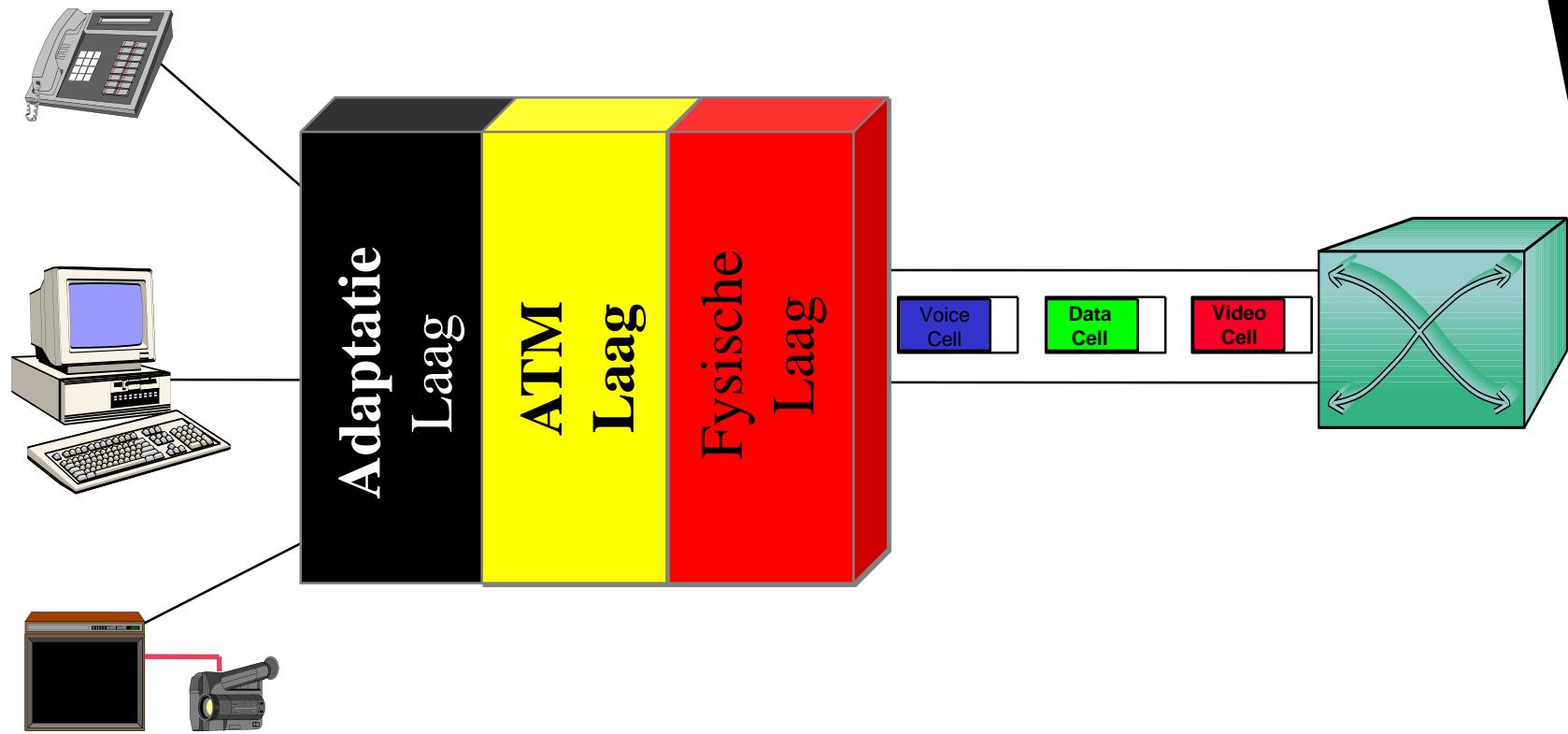


## ■ Point -to- Multipoint

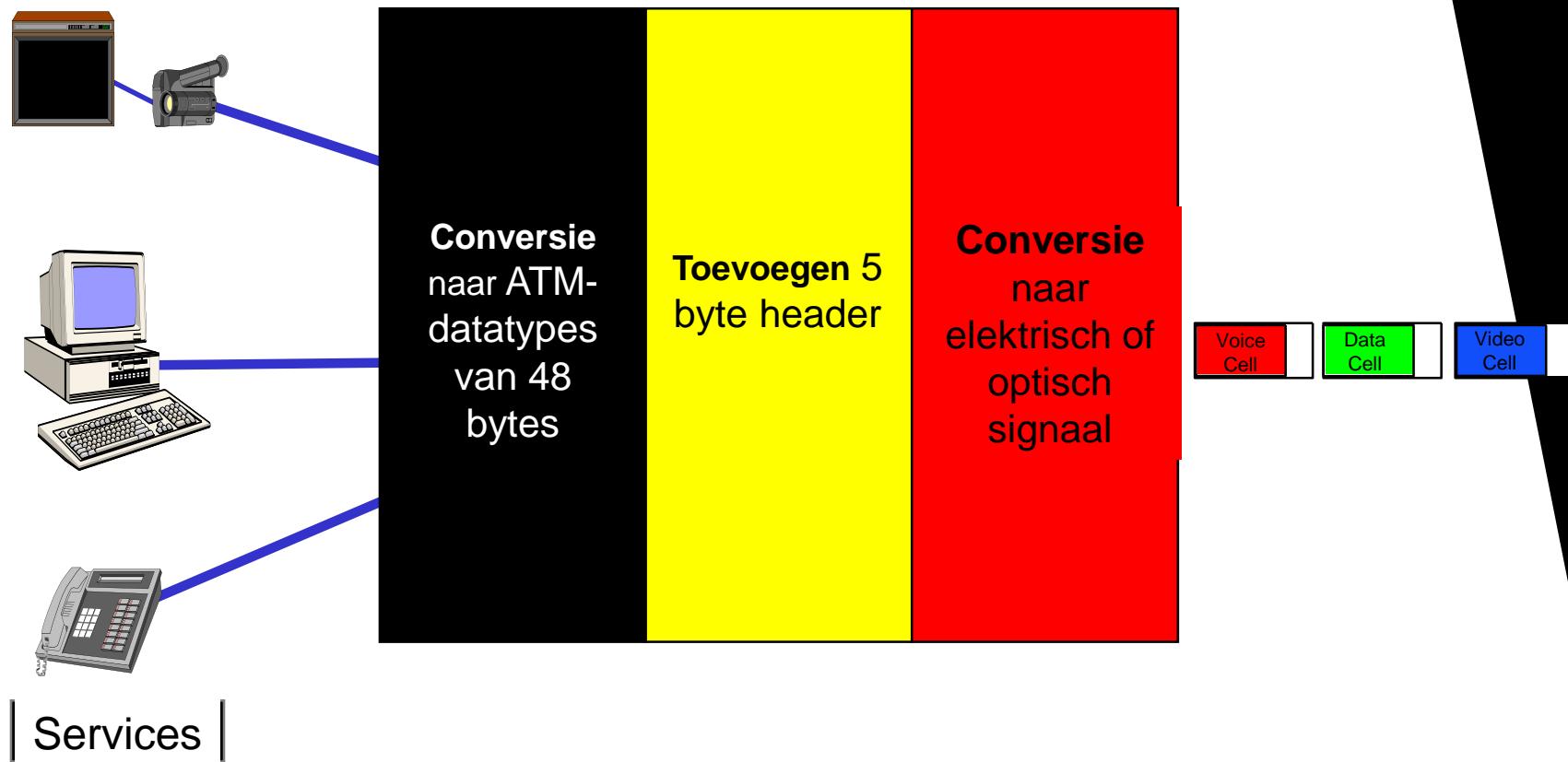
- ◆ Enkel eenrichtingsverkeer



# ATM architectuur: lagen

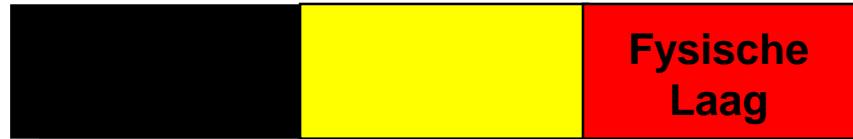


# ATM architectuur



# Fysische Laag

- **Medium: STP, UTP, Coax, Multimode -en Single Mode Fiber, Draadloos**
- **Backbones waarop ATM draait:**
  - ◆ ADSL (Asymmetric Digital Subscriber Line)
  - ◆ VHDL (Very High-Speed Digital Subscriber Line)
- **Cell Rate Decoupling**
  - ◆ Lege cellen worden opgevuld met bepaald patroon om aan te geven dat ze leeg zijn.



# ATM laag

## ■ Functies:

- ◆ Header toevoegen en verwijderen
- ◆ Beheer van virtuele circuits en paden
- ◆ Routeren via ATM switches

# Header ATM cel

## ■ Volgende onderdelen in de header:

- ◆ Algemene flow control (niet gebruikt)
- ◆ VC identifier/VP identifier
- ◆ Payload Type Identifier
- ◆ Cell Loss Priority
- ◆ Header Error Check



# Header ATM Cel

## ■ Payload Type Identifier

- ◆ Aangeven of het **data** verkeer of **controle** verkeer is
- ◆ Bit om een fileprobleem te melden

## ■ Cell Loss Priority (CLP)

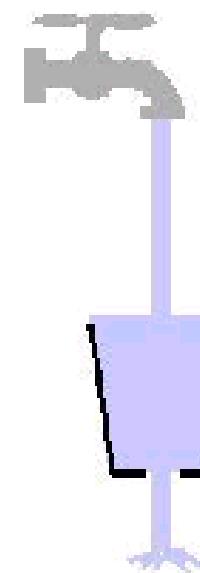
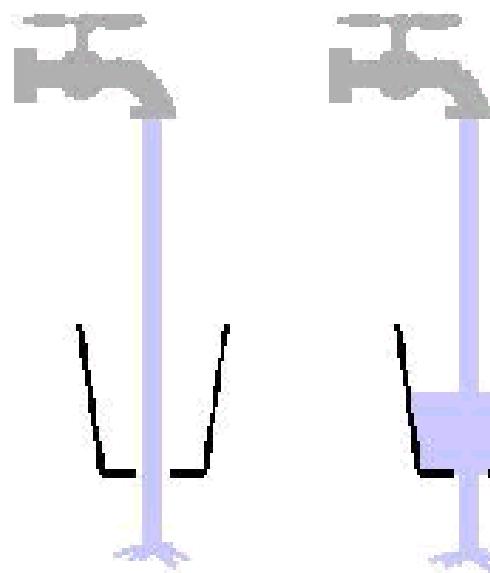
- ◆ Cellen die vloeken tegen het verkeerscontract (met QoS) krijgen CLP=1. Deze mogen eerst weggegooid worden, wanneer ATM switchen het moeilijk krijgen
- ◆ Hiervoor wordt het algoritme van de leaky bucket gebruikt

## ■ Header Error Check

- ◆ Fout detecterend en corrigerend



# Leaky bucket

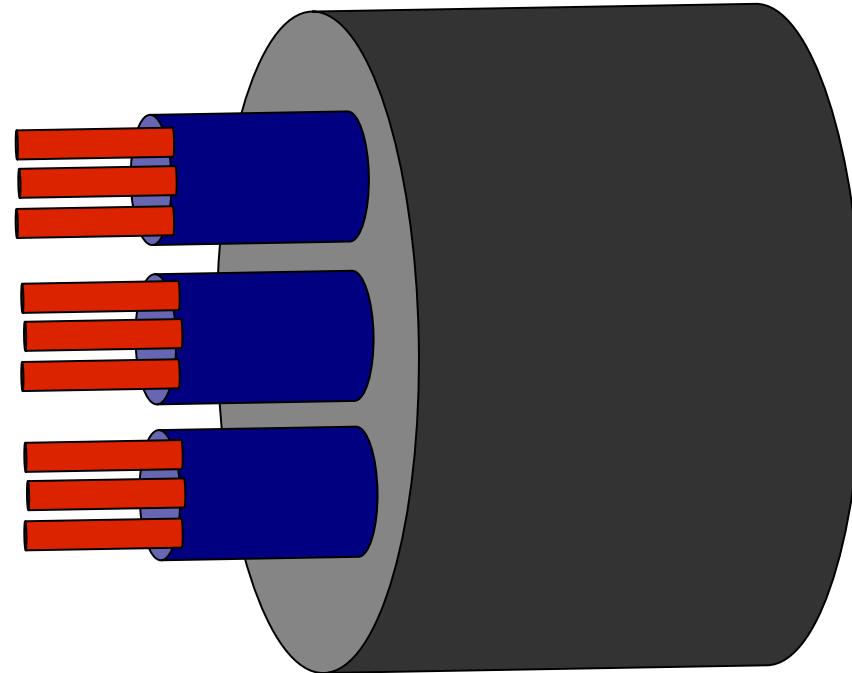


CLP=1



# Virtueel Pad en Virtueel Circuit

Virtuele  
Circuits



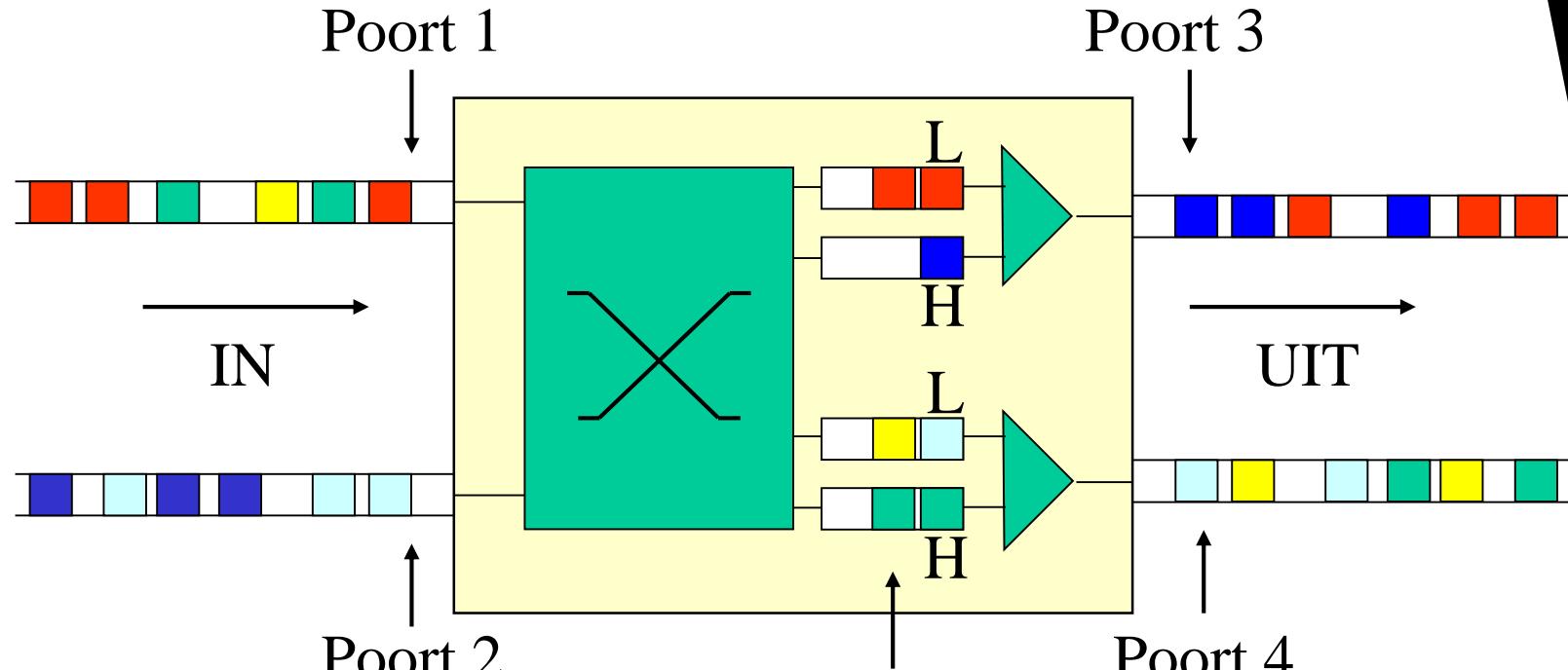
Virtuele  
Paden

Totale  
Bandbreedte

# ATM laag VPI/VCI

- ATM werkt met virtuele paden.
  - ◆ Per pad een **VPI** (Virtual Path Identifier) nummer
- Langs een pad kunnen verschillende toepassingen draaien. Deze noemen we **virtuele kanalen**
  - ◆ Per toepassing een **VCI** (Virtual Channel Identifier)
- **VPI/VCI waarden zijn enkel uniek per interface**
  - ◆ Hebben enkel lokaal een betekenis
- **Aan de rand van het netwerk (UNI) worden er 8 bits voorzien voor VPI.**
- **Binnen het netwerk (NNI) worden er meer paden voorzien (12 bits voor VPI)**

# ATM switch



VPI/VCI

	4/3
	34/11

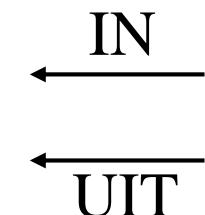
	8/12
	5/12

	8/9
	5/9

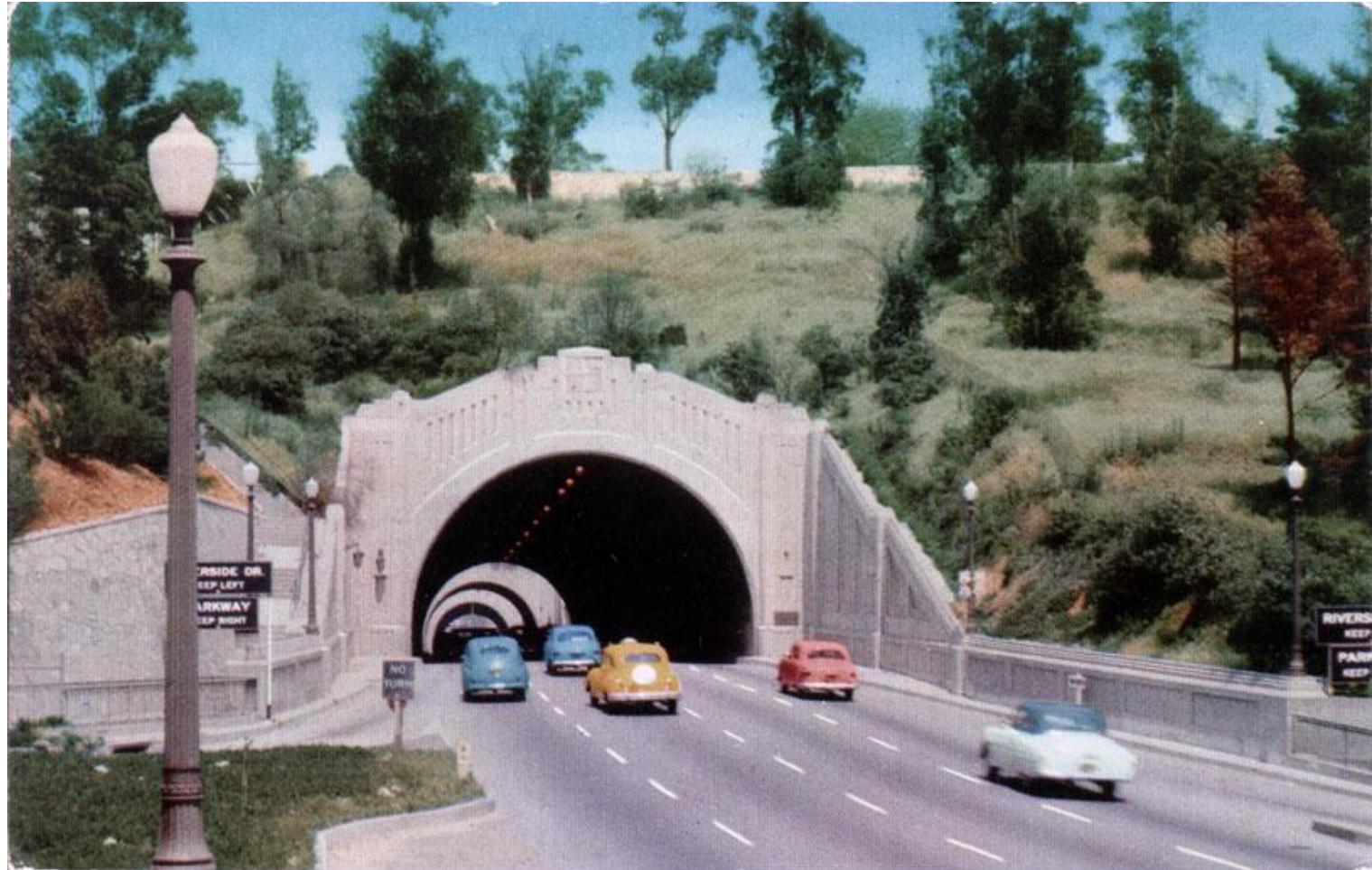
	8/42
	2/11

	61/7
	9/33

Queues



VCI= auto VPI=tunnel



# Opzetten ATM verbinding

## ■ *Network provisioning*

- ◆ Bij het vastleggen van een virtueel pad wordt telkens een verbinding gemaakt tussen een poort en een VPI aan de ene kant en een paar aan de andere kant. Dit op voorhand mappen van een verbinding heten we **network provisioning**.
  - Network provisioning gebeurt door controlecellen die tussen de ATM knooppunten worden doorgestuurd



# ATM Adaptatie Laag AAL

- AAL 1: Circuit Emulation
- AAL 2: Video / Audio
- AAL 3/4: Data Transfer
- AAL 5: LAN verkeer

## ATM AAL5 LAN

- Vereenvoudigde versie van AAL3/4 voor LAN verkeer: minder overhead bij data
- SEAL Simple and Efficient Adaptation Layer
- In praktijk wordt ATM niet voor LAN gebruikt



# ATM en OSI

- ATM past niet in het OSI model
- ATM is een *overlay*-network
- Netwerklaag:
  - ◆ ATM heeft een eigen adressering
  - ◆ ATM routeert
  - ◆ ATM gebruikt een hiërarchische adressering met autoconfiguratie (Plug n Play)

## ATM nadelen

- Wanneer een ATM verbinding is opgezet, kunnen (bv.firewalls) de informatie niet meer interpreteren of verwerken.
- PRIJS! De implementatie van ATM is zeer duur.
- Bij gebruik van ATM voor een LAN is er een verlies aan bandbreedte. ATM moet hierbij een overgang voorzien naar de TCP/IP protocollen (dit zorgt voor veel overhead).

# Routing Protocols

## Border Gateway Protocol

# Wat is BGP?

- BGP is een routing protocol waarmee Internet Providers met elkaar verbinden en waarmee eindgebruikers zich kunnen verbinden met verschillende ISP's
- BGP is een routing protocol tussen Autonome Systemen (AS) en werkt met een distance vector (dus plakt op elke verbinding een waarde en heeft niet echt een idee over de netwerktopologie)

# Autonomoos Systeem (AS)

- **Een AS is een verzameling IP netwerken en routers die beheerd worden door dezelfde administrator(s)**
- **Elk AS krijgt een unieke nummer**
  - ◆ Privaat: Mag je zelf kiezen tussen 64512 en 65535
  - ◆ Publiek: Uniek toegekend in de wereld (ASN)
    - Dit nummer was 16 bit en sinds 2007 ook uitgebreid tot 32 bit
    - De IANA — Internet Assigned Numbers Authority deelt, buiten IP adressen, via 5 organisaties ook AS nummers uit
      - AfriNIC (afrika), APNIC (azië/pacific), ARIN (amerika), LACNIC (latijns amerika/caraïben) en RIPE-NCC (europa, middenoosten/centraal azië)

# Hoe werkt BGP en “het Internet”

- Geen centrale “*core*”
- Individuele netwerken (met een AS nummer) verbinden en melden hun IP adressen
- Sturen announcements naar elkaar met
  - ◆ IP, prefix, AS PATH, ...
- AS PATH is lijst met wie de announcements doorstuurd
  - ◆ om loops te vermijden

# Interne/Externe routering

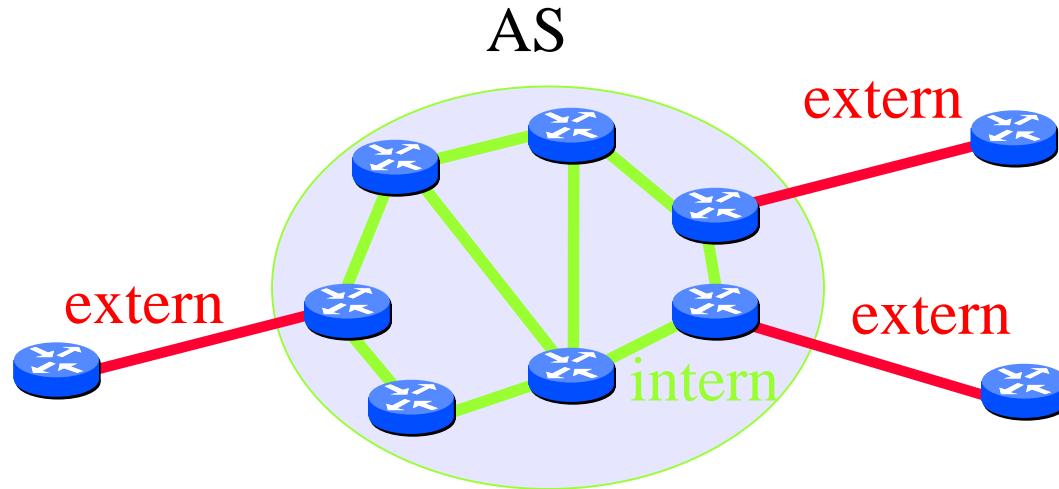
## ■ Interne routering

- ◆ Routering binnen een autonoom systeem

## ■ Externe routering

- ◆ Routering buiten een autonoom systeem

## ■ Intern = IBGP, Extern = EBGP



# CIDR

- ClassLess Inter Domain Routing
- Ip adressen werken niet meer met standaard klasse A/B/C, maar worden met een IP prefix doorgegeven
  - ◆ /24 voor klasse C
  - ◆ /16 voor klasse B
  - ◆ /8 voor klasse A
- In classfull routing wordt bijvoorbeeld adres 20.0.0.0 direct als klasse A (/8) bestempeld. Classless kan men hiermee de prefix kiezen.
- Routing protocollen, buiten BGP, die IP prefixen kunnen doorgeven zijn bv. RIPv2, OSPF en EIGRP

# BGP sessie

- **Een BGP sessie maakt verbinding over TCP poort 179**
- **Alle actieve routes worden uitgewisseld**
- **Alle incrementele updates worden uitgevoerd**
  - ◆ Update = IP prefix + attributen
    - Voorbeelden van attributen zijn:
      - AS\_PATH (aantal Autonome Systemen die je tegenkomt cfr hops)
      - MULTI\_EXIT\_DISC (een 32bit waarde die je zelf kan instellen voor je verbindingen. Deze geldt enkel tussen jij en je buren. Hoe lager, hoe sneller je deze verbinding gebruikt)
  - ◆ Opmerking: Updates met de langste prefix geven het meeste informatie en krijgen dus voorrang ten opzichte van adressen met een korte prefix.
    - bv 10.10.10.0/24 heeft voorrang tov 10.0.0.0/8

# BGP: kiezen van het beste pad

- Externe EBGP geleerde routes krijgen voorrang op intern gekende IBGP routes
- Kortste AS\_PATH
- Kleinstе MULTI\_EXIT\_DISC waarde
  - ◆ Meerdere verbindingen tussen dezelfde AS  
=> zeggen welke voorrang krijgt
- BGP ID
  - ◆ De route voorgesteld door de router met het laagste IP adres krijgt voorrang





## The Youtube hijack 25/02/2008

- **Youtube stuurt via BGP de range 208.65.152.0/22 (208.65.152.0 - 208.65.155.255) door**
- **De Pakistaanse regering blokkeert Youtube**
  - ◆ De route 208.65.153.0/24 wordt naar null0 gerouteerd
- **Toevallig werd met BGP deze routing update doorgestuurd naar de rest van de wereld**
- **Youtube surfers komen terecht bij een provider in Pakistan**
- **Youtube stuurt als reactie via BGP updates met zijn /24 en enkele /25 adressen met gedeeltelijk succes**
- **De internet lijnen naar Pakistan worden even verbroken en BGP herstelt zich.**

# Youtube Hijack BGP

Youtube



Pakistan



# De “China Telecom Hijack” 8 april 2010

- China Telecom zorgt er “per ongeluk” voor dat ALLE verkeer naar us.gov en us.mil via China wordt gestuurd
  - ◆ China claimt 15% van alle internet adressen
    - China telecom kan 15% van alle internet verkeer verwerken!
  - ◆ Na 18 minuten wordt de “fout” rechtgezet



# traceroute Londen - USA tijdens attack

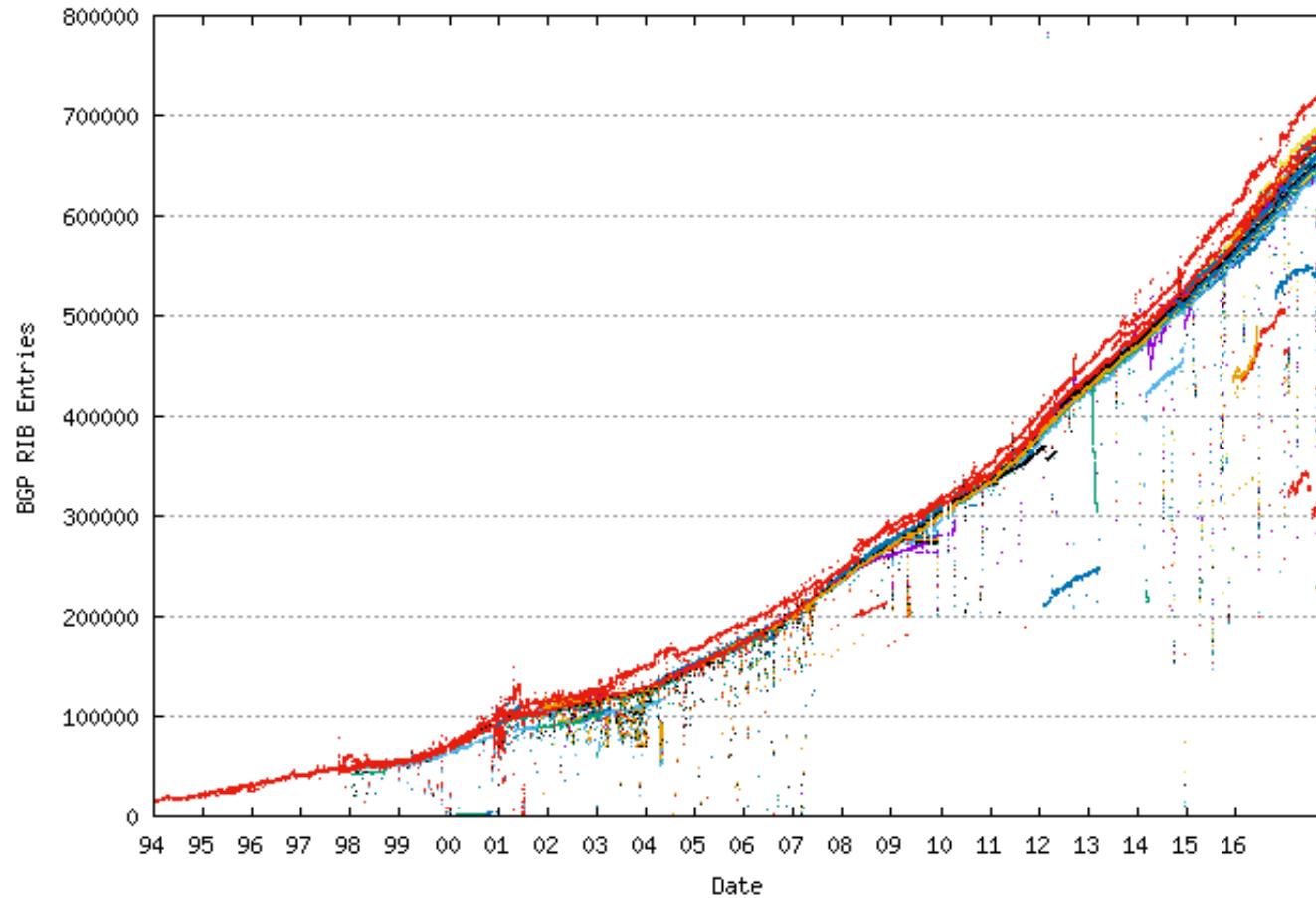
1. <our host>	0.785ms	# London
2. 195.66.248.229	1.752ms	# London
3. 195.66.225.54	1.371ms	# London
4. 202.97.52.101	399.707ms	# China Telecom
5. 202.97.60.6	408.006ms	# China Telecom
6. 202.97.53.121	432.204ms	# China Telecom
7. 4.71.114.101	323.690ms	# Level3
8. 4.68.18.254	357.566ms	# Level3
9. 4.69.134.221	481.273ms	# Level3
10. 4.69.132.14	506.159ms	# Level3
11. 4.69.132.78	463.024ms	# Level3
12. 4.71.170.78	449.416ms	# Level3
13. 66.174.98.66	456.970ms	# Verizon
14. 66.174.105.24	459.652ms	# Verizon
...		
19. 69.83.32.3	508.757ms	# Verizon
20. <last hop>	516.006ms	# Verizon

## Gevolg

- **De grootste zekerheid voor een AS geeft het doorsturen van al je adressen als een /24**
  - ◆ Deze kunnen dan niet meer overschreven worden
- **Maar dat maakt routing tabellen heel groot**
- **Het BGP routing domein is heel internet !!!**

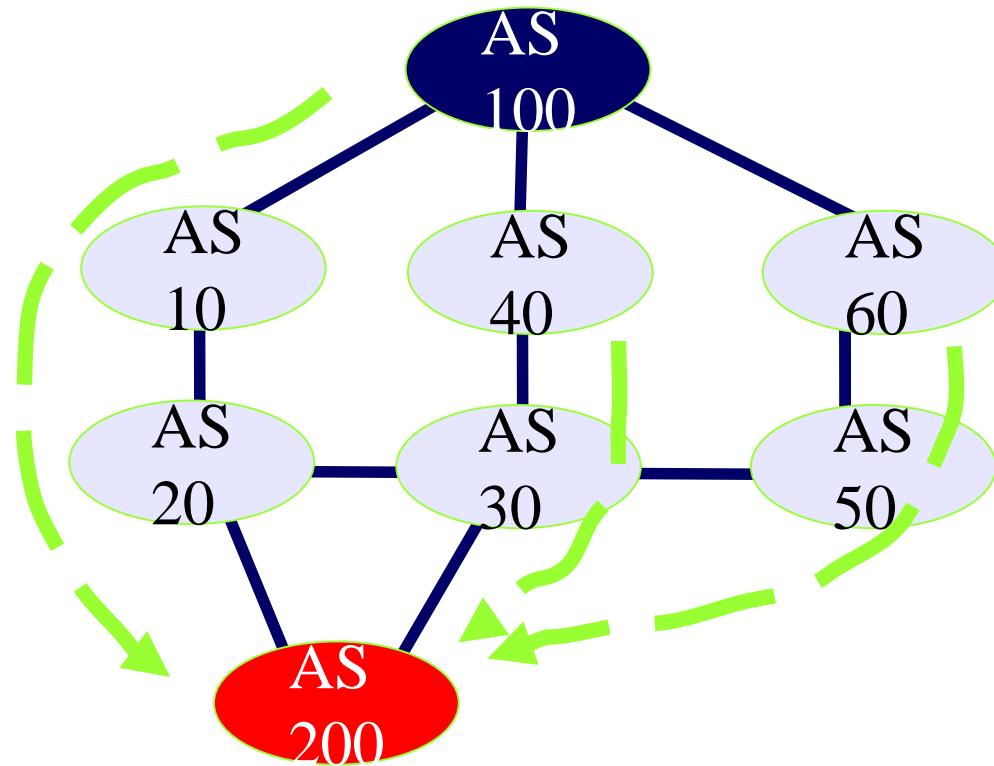


# Grootte BGP routing tabel



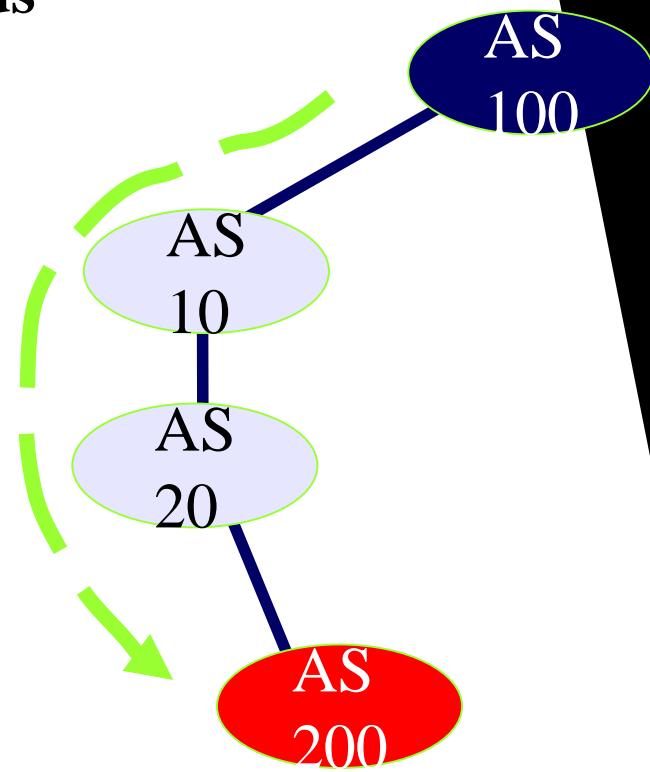
# Youtube hijacken en verder

## ■ Beginsituatie



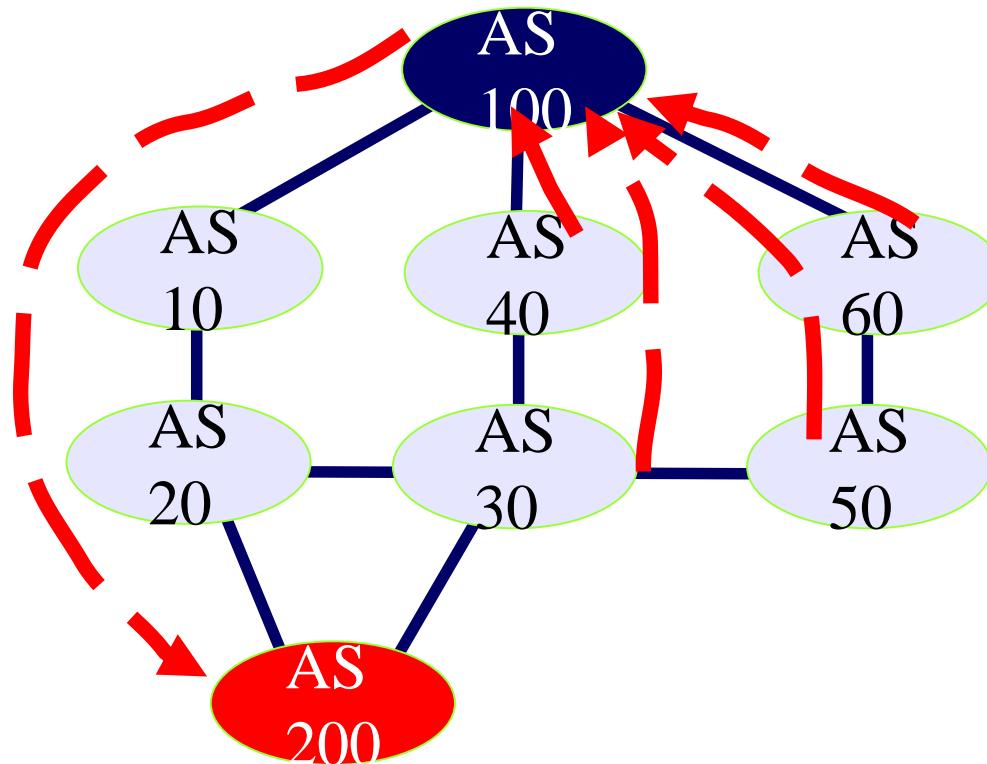
# Youtube hijacken en verder

- Als je zelf een AS nummer hebt, kan je de routing tabellen van internet dus ook manipuleren
  - ◆ Geef zelf met een /24 een betere route door van een bestaande range. De route gaat beter langs jou
- Bij BGP geef je een “beter” pad met AS een op.
  - ◆ Bij ons geven we een beter AS\_PATH 10 20 200 op
    - router map gahierlangs permit 10 match ip address prefix list onzlijst set as-path prepend 10 20 200



# Het verkeer kiest jou als ideale weg

- Je ziet dus alle verkeer én je kan aanpassen wat je wilt
- Wat je minstens aanpast is de TTL waarde, omdat anders een traceroute nogal opvalt. Dat kan met iptables



Cisco.com vergeet zichzelf door te geven via BGP  
cisco



08/04/2009 cisco.com 90 minuten unavailable

# Referenties

- A Border Gateway Protocol 4

<http://www.ietf.org/rfc/rfc4271.txt> (RFC 1771 = oud)

- Stealing the internet, Defcon 16, Anton Kapela & Alex Pilosov: <http://www.defcon.org>

- BGP, Border Gateway Protocol

<http://www.bgp4.as/>

- CIDR Address Strategy

<http://www.ietf.org/rfc/rfc4632.txt>

# **Frame Relay inleiding**

## **WAN Protocol**

## Point to point

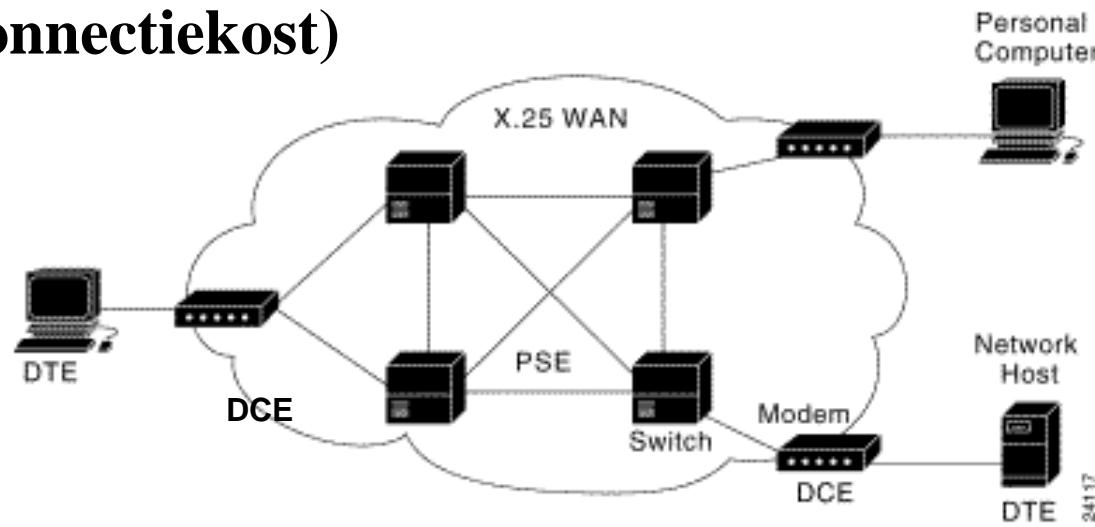
- Wat je "ziet" als een verbinding van 1 node naar andere node
  - ◆ Bv Leased Line
- Meestal gesimuleerd door een Packet Switched of een Circuit switched Netwerk

## X.25

- 1970s
- Werkt vooral op analoge en ISDN lijnen
- Data Terminal Equipment (DTE)
- Data Circuit-terminating Equipment (DCE)
  - ◆ DCE (provider) voorziet kloksnelheid
- Packet Switched netwerkdienst
  - dit ken je van Cisco!
- PAD
  - ◆ Packet Assembler/Disassembler
  - ◆ Omvormer naar X.25 pakketten

## X.25 netwerk

- Verbinden met een X.25 netwerk gebeurt via een domme terminal (DTE).
- Deze belt een X.25 service provider op, die doorverbint met de rest van de wereld (=> lokale connectiekost)



**Data Terminal Equipment (DTE)**

**Data Circuit-terminating Equipment (DCE)**

**Packet Switching Exchange (PSE)**

# X25 lagen

## ■ OSI laag 1 tot 3

- ◆ X25 past niet helemaal in het OSI model, het werd vóór het OSI model ontworpen

## ■ LAAG 3 (netwerk)

- ◆ PLP (Packet Layer Protocol)
- ◆ Adressering (Virtuele Circuits)

PLP pakket

## ■ LAAG 2 (Datalink)

- ◆ LAP-B (Link Access Procedure, Balanced)
- ◆ Voorziet UITGEBREIDE error correctie

LAP-B frame

PLP pakket

## ■ X.21 bis Fysische Laag

X.21 BITSTROOM

# Frame Relay

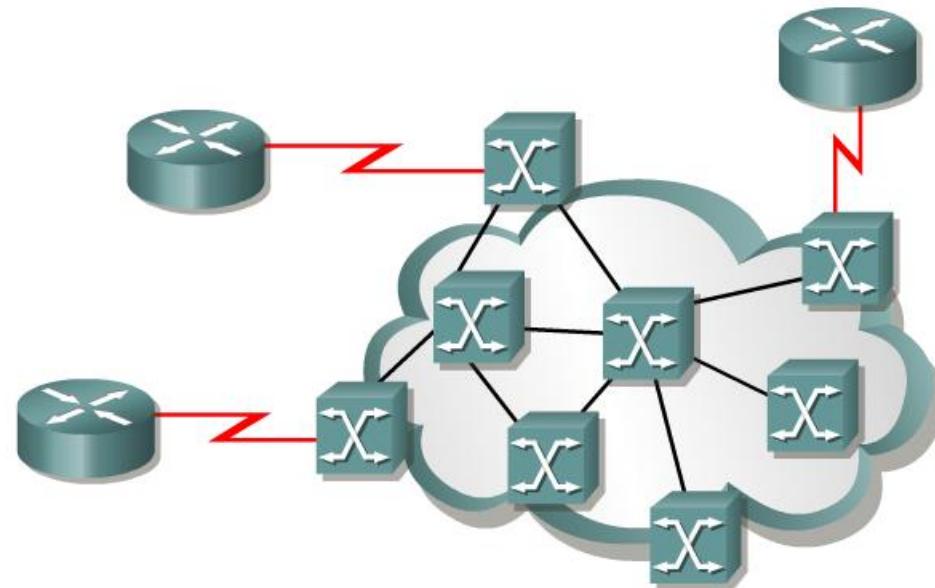
- X.25 "lite" versie
- Zonder extensieve foutcontrole
- Verschil met X.25
  - ◆ Niet zo robuust
  - ◆ Gaat uit van een betrouwbare verbindingssmedium
  - ◆ Geen hertransmissie van verloren data
  - ◆ Geen sliding windows
  - ◆ Foutafhandeling moet door hogere lagen
  - ◆ Hogere performantie

# Gebruik Frame Relay

- **Frame Relay is een gestandaardiseerde verbinding-dienst voor WAN's**
- **Het wordt vaak gebruikt om verschillende LAN's met elkaar te verbinden.**
- **Je kan deze dienst bij Belgacom aanvragen**
- **Frame Relay werkt op laag 2 van het OSI model (data link laag)**

## Voorbeeld FR netwerk

- Het eigenlijke Frame Relay netwerk (meestal bij Belgacom) bestaat uit FR switches die doorverbinden
- De verschillende LAN's connecteren met hun DTE naar het netwerk (bellen dus binnen bij hun Frame Relay provider)



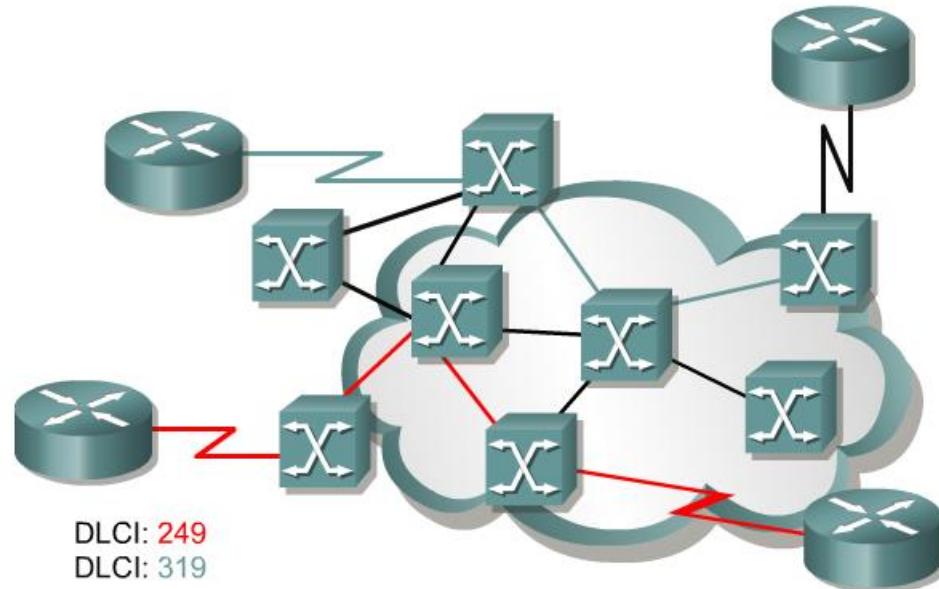
# Virtueel Circuit

- Wanneer 2 DTE 's via het FR netwerk met elkaar verbonden worden spreekt men van een Virtual Circuit.
- Hiervan bestaan er 2 soorten:
  - ◆ SVC: Switched Virtual Circuit (cfr telefoongesprek)
  - ◆ PVC: Permanent Virtual Circuit (cfr Leased Line)



# DLCI

- Op één fysieke verbinding kunnen er verschillende virtuele circuits staan.
- De verschillende VC's worden onderscheiden door een unieke DLCI of Data Link Channel Identifier



## Frame Relay laag 2

- Frame Relay krijgt IP pakketten (laag 3) aan
- Frame Relay steekt deze pakketten in zijn eigen frames (Frame Relay frames) (laag 2)
  - ◆ Het protocol dat FR hiervoor gebruikt heet Link Access Procedure for Frame Relay (LAPF)
- Daarna worden deze doorgegeven aan laag 1 en over een draad verstuurd.

## LAPF frame

### ■ In de Link Access Procedure for Frame Relay zijn volgende bits voorzien:

- ◆ Eén die aangeeft dat je sneller (of meer) frames stuurt dan afgesproken met Belgacom. Deze geven aan dat bij congestie de frame mag weggegooid worden  
cfr Cell Loss Priority bij ATM
- ◆ Eén die aangeeft dat er een fileprobleem is bij een FR switch. DTE's die dit merken, sturen minder frames op (dit wordt doorgegeven aan hogere lagen)
- ◆ Deze laatste melding gebeurt ook in de andere richting.

# Frame Relay LMI

- Frame Relay "extensie"
- Uitgevonden door "the gang of four"
- Geeft aan DTE's informatie over de toestand van het netwerk (was vergeten in oorspronkelijke FR protocol)
- Types van LMI (die niet *compatible* zijn):
  - ◆ Cisco (volgens cisco standaard)
  - ◆ Ansi (volgens American National Standard Institute)
  - ◆ Q933a (volgens International Telecommunication Union)

# LMI

- **Globale adressering**
  - ◆ DLCIs gelden niet meer enkel lokaal
- **Status berichten van Virtual Circuits**
- **Multicasting**
- **Flow Control**

# CIR Committed Information Rate

- De CIR is de afspraak die je met Belgacom maakt over de snelheid die je wil gebruiken over het FR netwerk
  - ◆ Afgesproken Burst
  - ◆ Afgesproken Tijd
  - ◆ Afgesproken Maximum Rate
- Het is mogelijk dat deze snelheid gehaald wordt, door meerdere telefoonlijnen te gebruiken.

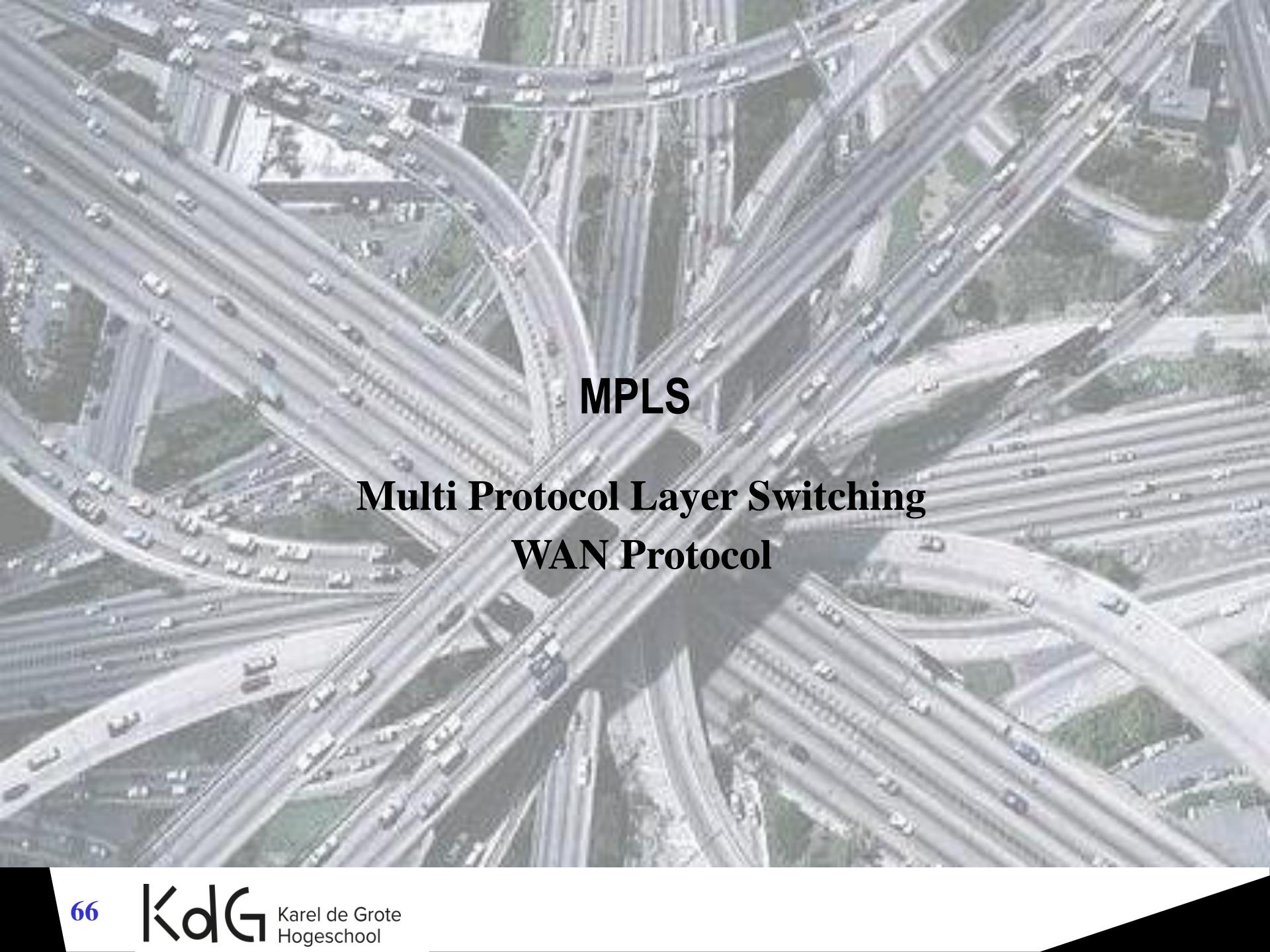


# Frame Relay

- Variabele pakketgrootte
- Geen QoS standaard
- Meer ondersteund bij Providers
- Goedkoper
- 64 Kbps tot 40 Mbps
- Voldoet NU aan de snelheden voor bedrijven
- Rand van netwerken

# vs ATM

- Vaste, kleine pakketten
- QoS en prioriteiten
- Zeer goed schaalbaar
- Duur / Moeilijk omschakelen
- Complex door QoS
- 1,5 Mbps tot 622 Mbps en meer
- Toekomst meer in gebruik door hogere snelheden
- Core van netwerken



**MPLS**

**Multi Protocol Layer Switching  
WAN Protocol**

# Definitie MPLS

- Multi Protocol Layer Switching is een oplossing voor bandbreedte- en dienstenbeheer in IP gebaseerde backbone netwerken
- MPLS is een framework dat schaalbaarheid en routering van de *traffic flow* voorziet in bestaande ATM en Frame Relay netwerken
  
- Traditionele routering (laag 3) gebeurt nog teveel op basis van het kortste pad en houdt te weinig rekening met vertraging en congestie

# Noodzaak

- Nood aan meer bandbreedte voor data, spraak en multimedia toepassingen over het Internet
- Nood aan verschillende dienstenklassen en kwaliteitsverzekering (QoS). Dit voor véél meer gebruikers dan vroeger!
- ATM kan dit maar ...
  - ◆ Duur
  - ◆ Complex
  - ◆ Niet overal beschikbaar



# Functies van MPLS

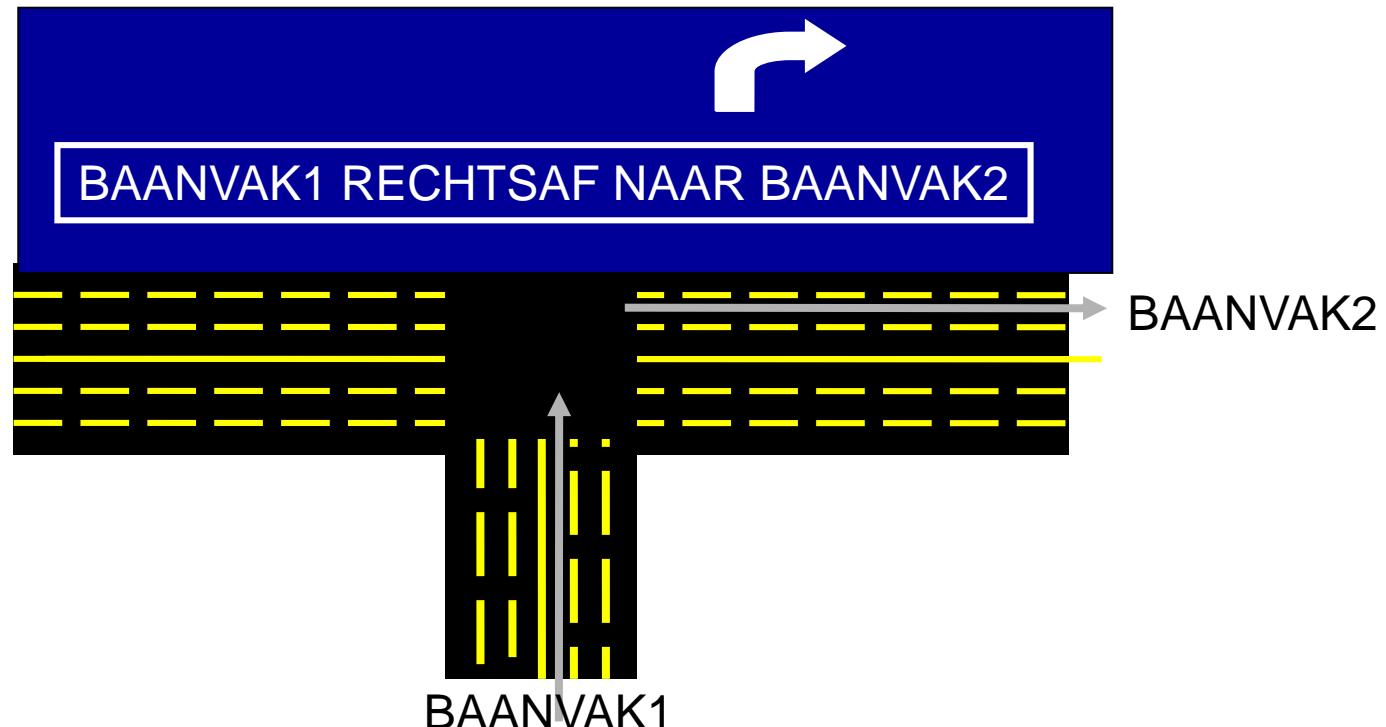
- Specifieert de manier waarop verkeersstromen tussen verschillende niveaus kunnen vloeien
  - ◆ tussen verschillende hardware, machines of verschillende applicaties
- Onafhankelijk van Laag 2 en Laag 3 protocollen
- Mapped IP adressen naar eenvoudige "labels"  
(met een vaste lengte)
- Voorziet een interface naar bestaande routing protocollen zoals Open Shortest Path First (OSPF)
- Ondersteunt IP en Laag 2 van Frame Relay en ATM

# Wat is de kortste weg naar Antwerpen?

- **BROADCAST:** Ga overal langs en stop wanneer je een plakkaat met Antwerpen ziet.  
"Zoek maar"
- **HOP BY HOP ROUTING:** Vraag in elk dorp dat je tegenkomt welk buurdorp het dichtst tegen Antwerpen ligt. Ga naar dat dorp en vraag het opnieuw.  
"Ga je naar Antwerpen? Ga langs X, het ligt op de weg! "
- **SOURCE ROUTING:** Vraag een routebeschrijving van alle dorpen waar je langs moet om in Antwerpen te geraken.  
"Ga je naar Antwerpen? Rij 5 straten rechtdoor, dan links, dan 6 straten rechtdoor en aan de lichten links."

# Label Substitution

- Je gaat met de wagen naar Antwerpen. In elke straat is er een rijvak gereserveerd en bij elk kruispunt staat er een grote pijl naar waar jij moet rijden



# Een *Label* bestaat al

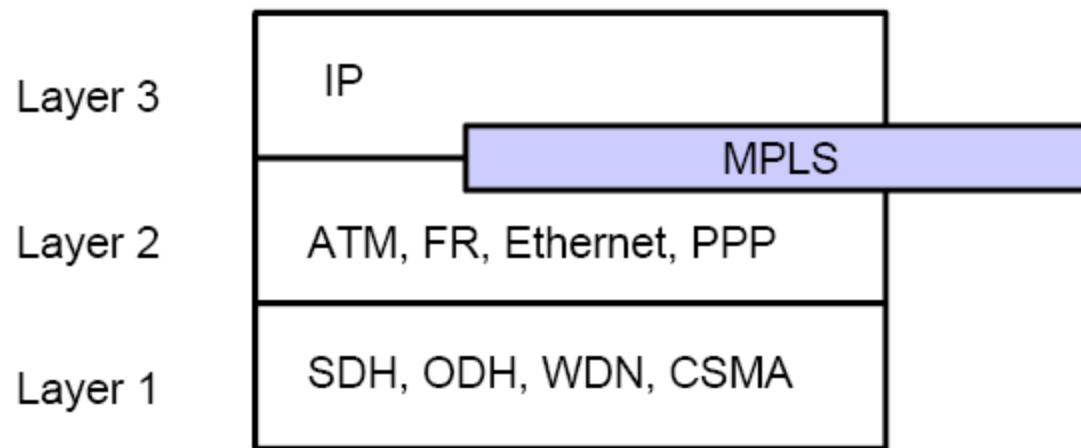
What's in a name, that which we call a *label*, by any other name,  
would smell as sweet?

- ATM - een label heet VPI/VCI
- Frame Relay - een label is een DLCI
- TDM - een label is een timeslot (zoals een baanvak)
- X25 - een label heet een LCN



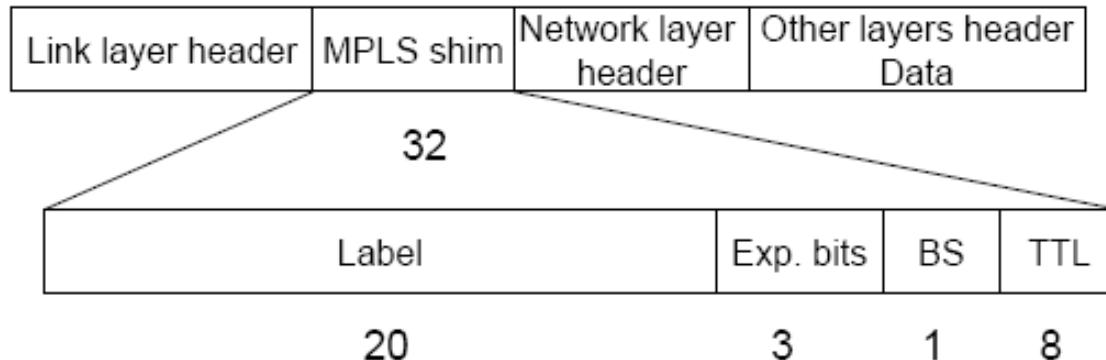
# Lagen MPLS

- Multi Protocol Label Switching gebeurt tussen Laag 2 en Laag 3



# MPLS label

## ■ Algemene vorm van een Label



**Exp.bits:**

Geven een verkeersklasse aan

**BS:**

Soort STOP bit. Er volgt geen label meer

**TTL:**

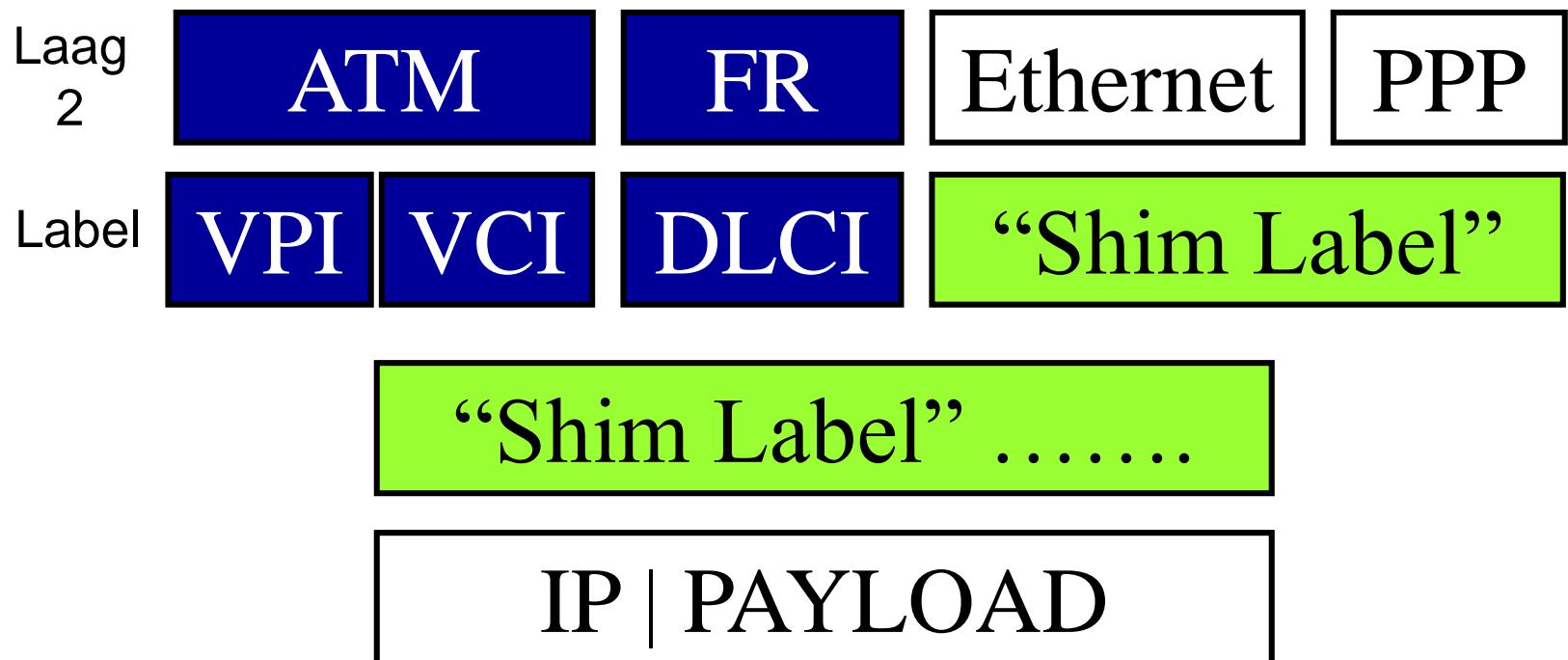
TimeToLive zoals bij IP

# Doorsturen van Labels

- MPLS zegt niet hoe de labels moeten verspreid worden
- BGP is uitgebreid met *piggybacking* om de label mee te nemen
- IETF heeft ook een nieuw protocol gedefinieerd enkel voor het doorsturen en beheer van labels:  
**Label Distribution Protocol (LDP)**
  - Extensies van LDP ondersteunen ook routing met QoS parameters

## Bestaande Labels

- Bestaande Labels worden overgenomen. Waar er geen label bestaat, wordt er een nieuwe "**Shim label**" voorzien.





**One protocol  
to rule them all**

# LER en LSR

## ■ Label Edge Router

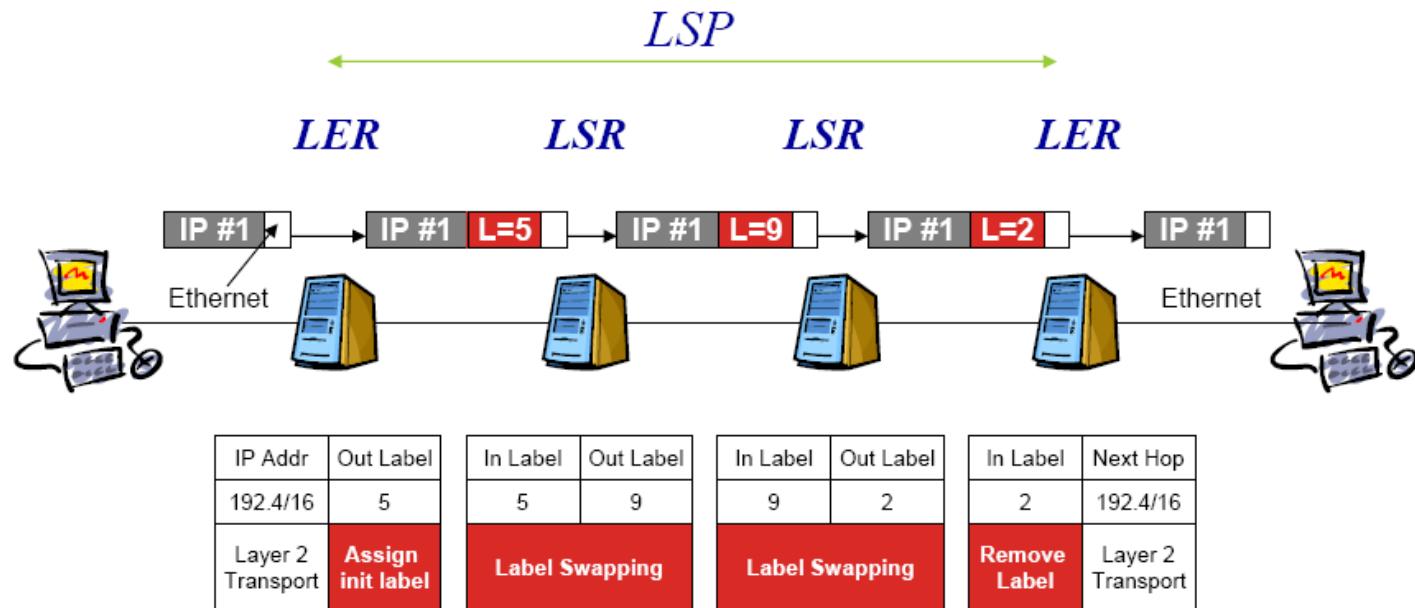
- ◆ Zit aan de rand van een MPLS netwerk en voorziet/verwijdt labels bij pakketten.
- ◆ Ondersteunt meerdere poorten naar verschillende netwerken (zoals Frame Relay, ATM, en Ethernet).

## ■ Label Switch Router

- ◆ Is een hoge-snelheidsrouter in het hart van een MPLS netwerk.
- ◆ ATM switches kunnen als LSR dienen zonder hardware veranderingen. Label switching = VP/VC switching.

# Label Switched Path (LSP)

- Het LSP wordt vastgelegd VOOR de transmissie start  
Dit is dus **network provisioning**.



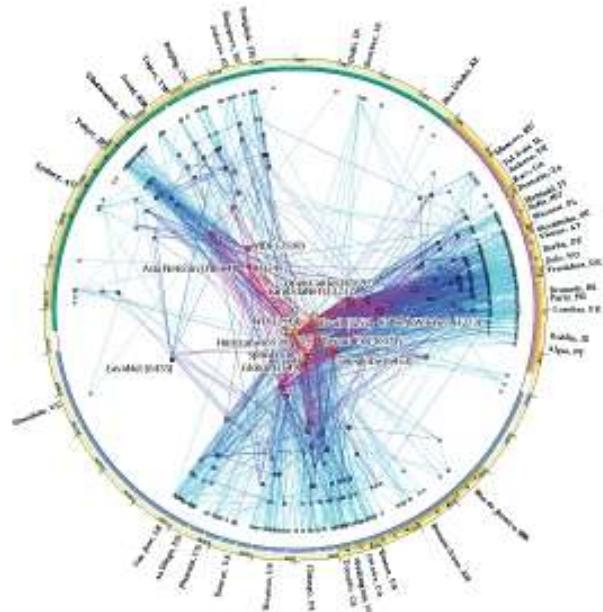
“ROUTE AT EDGE, SWITCH IN CORE”

## Opzetten van een LSP

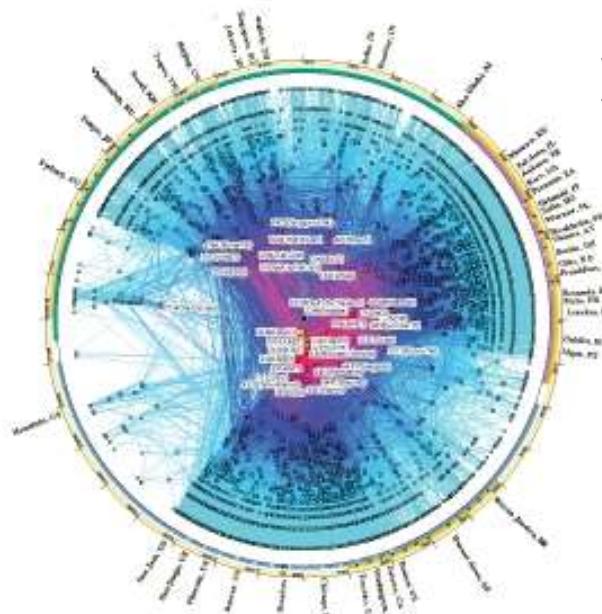
- MPLS voorziet 2 mogelijkheden om een Label Switched Path op te zetten:
  - ◆ hop-by-hop routing

**Elke LSR kiest zelf de volgende hop. LSR gebruikt eender welk routing protocol (OSPF, ATM ...).**
  - ◆ explicit routing

**Is hetzelfde als source routing. De LSR heeft een lijst met nodes waarlangs het pakket moet gaan.**
- Het opzetten van een LSP is unidirectioneel. Het terugkerende verkeer krijgt een nieuwe LSP!



# IPv6



# Introductie

# Overzicht IPv6

- Verschil IPv4/IPv6
- Addressering
- IPv6 Header
- Grootte van een pakket
- Autoconfiguratie
- Flow Labels en Verkeersklasse
- Hogere Lagen
- ICMPv6
- Veiligheid



# IPv4

- **32 bit adressen zijn op**
- **Routing tabellen zijn te groot**
  - ◆ niet hiërachisch, 400k rijen
- **IPv4 heeft geen pakketbeveiliging**
  - ◆ optie IPsec, maar niet ingebouwd
- **Realtime ondersteuning beperkt**
  - ◆ Type of Service veld bij IPv6 voor QoS wordt geëncrypteerd en dus onleesbaar



Jura F50, eerste koffiezetterapparaat waar hackers remote de sterkte van de koffie konden aanpassen

# Verschil v4 v6

- **32bit -> 128 bit adressen**
  - ◆ meer hiërarchisch
  - ◆ multicast en anycast adressen (group servers)
- **Header met optionele velden**
  - ◆ niet leeg zoals in IPv4
- **Uitbreidbare header**
  - ◆ snel doorsturen pakket
- **Labelen Stroom**
  - ◆ QoS
  - ◆ Realtime
- **Authenticatie en Privacy ingebouwd**



# IPv6 adressering

## ■ Unicast :

- ◆ 1 per interface

## ■ Anycast:

- ◆ Groep interfaces,
- ◆ 1 van de interfaces is ok (bv de NTP servers)

## ■ Multicast:

- ◆ Afleveren bij alle interfaces
- ◆ Is ook broadcast

# Voorstellen van adressen

## ■ Voorkeur

- ◆ 2001:0:0:0:0:0:200C:417A
- ◆ 2001::200C:417A

## ■ Mask is altijd met prefix

- ◆ RIPE NCC 2001:0600:: /23
- ◆ BELNET 2001:06A8:: /32
- ◆ KDG.BE 2001:06A8:0540:: /48
- ◆ STUDENT.KDG.BE 2001:06A8:0540:0101 /64

# Soorten adressen

## ■ Link-Local/Organisational-Local

- ◆ **FE80**::/10, Dit zijn de huidige private adressen
- ◆ Geldt enkel binnen een link/organisatie, bevat MAC adres

## ■ Unique Local

- ◆ **FC00**::/7
- ◆ Bevat pseudo random 40 bit nummer

## ■ Multicast

- ◆ **FF**xx (begint met FF)
- ◆ bv FF05::43 Alle NTP servers binnen deze site

## ■ Loopback

- ◆ ::1

# Zones

- Je hebt verschillende netwerkkaarten met adressen **FE80::1/64** en **FE80::2/64**.
  - ◆ Hoe kan ik verbinden met een server met adres FE80::3/64?
- **Oplossing:**
  - ◆ In de routetabel wordt een zone toegevoegd
    - Windows FE80::3%**1**
    - Linux FE80::3**eth0**
  - ◆ Deze zones zijn niet altijd zichtbaar bij het opvragen van de routetabel (ROUTE PRINT / ip -6 route)

# IPv6 Header

IPv6

Ver.	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

IPv4

Ver.	Hdr Len	Type of Service	Total Length		
Identification		Flg	Fragment Offset		
Time to Live	Protocol	Header Checksum			
Source Address					
Destination Address					
Options...					

Verdwenen: Header Length, Identification Flags, Fragment Offset, Header Checksum

Veranderd: TTL > Hop Limit  
Options > Extension Headers  
Type of Service > Traffic Class

# Uitbreidingsheader (Next Header)

## ■ Hop-by-Hop Options Header

- ◆ Opties voor tussenliggende nodes

## ■ Routing Header

- ◆ Source routing (pad weergeven)

## ■ Fragment Header

- ◆ Pakket met grotere MTU (max transfer unit) fragmenteren
- ◆ Enkel tussen bron en doel, niet onderweg zoals IPv4

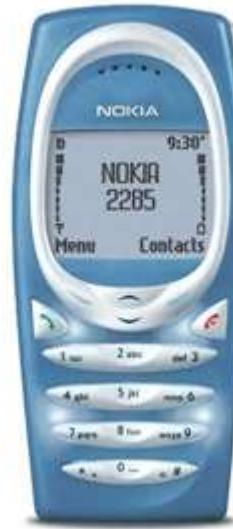
## ■ Destination Options Header

- ◆ Meestal voor veiligheidsopties

## ■ Authenticatie/Encryptie Headers

# Pakketgrootte

- Minimum 1280 octets
- Aangeraden 1500 octets
- ICMPv6 Packet Too Big pakket naar bron
- Afspraak tussen bron en doel
  - ◆ NIET onderweg zoals bij IPv4



5 nov 2003,  
1ste dual  
stack

# Stateless Autoconfiguratie

- **1. ICMPv6 router sollicitatie bericht (type 133)**
  - ◆ bron is FE80:: met mac adres achteraan
  - ◆ doel is All routers adres FF02::2
- **2. Antwoord door router ICMPv6 advertisement (type 134)**
  - ◆ bevat IP add, Lifetime
- **3. ICMPv6 Neighbour Sollicitation bericht (type 135)**
  - ◆ Heb ik wel uniek MAC adres?
- **4. ICMPv6 Neighbour Advertisement bericht (type 136)**
  - ◆ Als een host hetzelfde MAC adres heeft

# Statefull Autoconfiguration

## ■ Aanvraag UDP poort 547

- ◆ bron: link local FE80::MAC, UDP poort 546
- ◆ doel: All DHCP servers FF02::1:2 poort 547

## ■ DHCP zendt adres terug

- ◆ 128 bit adres en Lifetime

# Mobiele autoconfiguratie

- **GSM krijgt vast IPv6 adres op thuisbasis**
  - ◆ Noemt men de *Home Agent*
- **GSM krijgt tijdelijk adres op verplaatsing**
  - ◆ Stuurt naar *Home Agent* een *binding* door
    - Koppeling tijdelijk adres met vast adres
    - Tijdelijk adres kan tijdens gesprek/verplaatsing veranderen
    - Home agent fungeert als soort router

# Flow Labels en Verkeersklasse

## ■ Flow Labels

- ◆ Doel is
  - QoS
  - Realtime diensten
- ◆ Voorlopig nog experimenteel

## ■ Verkeersklasse

- ◆ Doel is
  - prioriteiten tussen verschillende pakketten
  - enkel aanpassingen mogelijk door nodes van dezelfde klasse

# Hogere Lagen

- IPv6 neemt controlesom van volledige pakket
  - ◆ ook voor UDP
- Time to Live
  - ◆ Wordt Hop Limit
- IPv6 tunnel door IPv4 is 1 Hop

# ICMP v6

## ■ Type 1

- ◆ 0: No route to destination (geen netwerk of geen gateway)
- ◆ 1: Communication prohibited (firewall)
- ◆ 3: Address unreachable (doel antwoordt niet)
- ◆ 4: Port unreachable (poort of service draait niet)

# ICMPv6 informatie

## ■ Ping

- ◆ type 128 code 0 Echo Request
- ◆ type 129 code 0 Echo Reply

# ICMPv6 configuratie

- **Type 130/131/132**
  - ◆ Group membership (voor anycast)
- **Type 133/134**
  - ◆ Router Sollicitation / Advertisement
- **Type 135/136**
  - ◆ Neighbor Sollicitation / Advertisement

# Authenticatie Header

- **Verzekering van de herkomst van het verkeer, integriteit, replay attack, tampering**
- **Security Parameter Index**
  - ◆ Afgesproken 32 bit nummers tussen zender/ontvanger
  - ◆ Weigeren onbekende nummers
- **Volgnummer**
  - ◆ Verzekeren integriteit
  - ◆ 32 bit nummer
- **Integrity Check Value**
  - ◆ Hash berekend met gedeeld geheim tussen zender/ontvanger

# Encryptie Header

- **Verzekering Confidentialiteit**
- **Sleutels uitgewisseld over UDP poort 500**
- **Encapsulation Security Payload header**
  - ◆ Encryptieprotocol
  - ◆ Volgnummer
  - ◆ Checksum
  - ◆ Enkel op de Payload (echte Data)

# **Suricata**

# Wat is suricata ?

- Intrusion Detection Systeem
- Intrusion Prevention Systeem



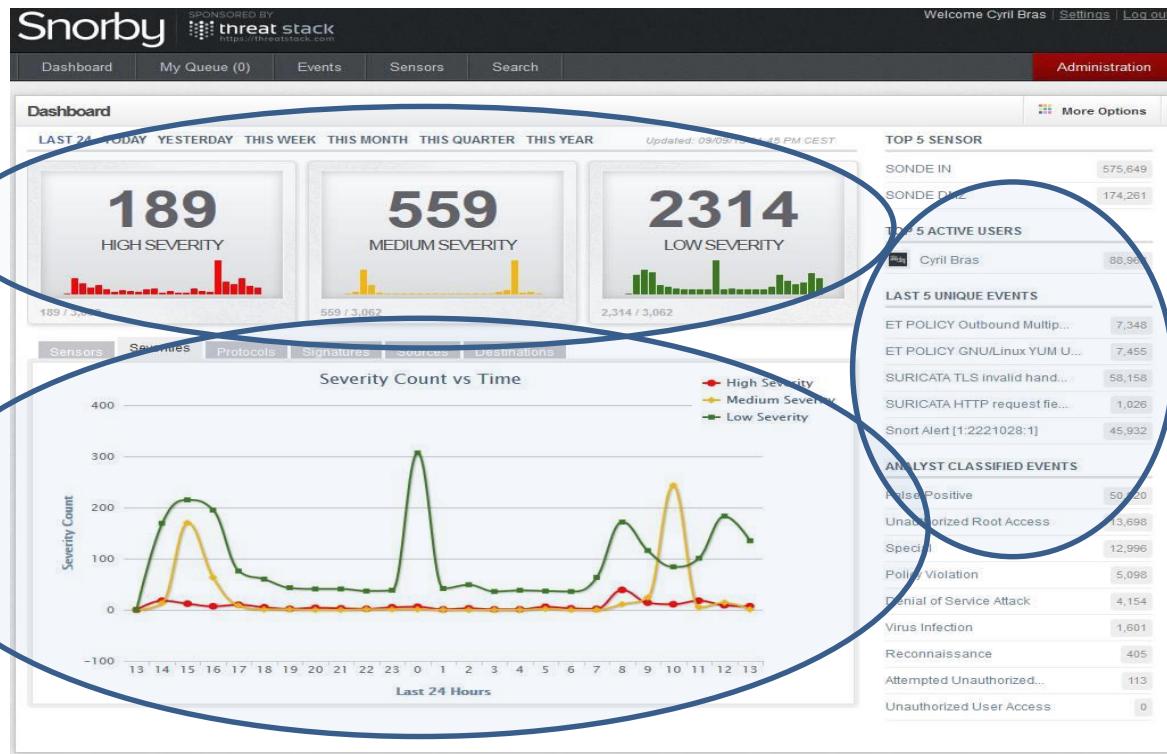
# Suricata regels

- **alert tcp \$DMZ1\_NET any -> any 80 (msg:"Tentative connexion DMZ1 http"; flow:established,to\_server; content:'|20|yum|2F|'; classtype:web-application-activity; sid:9201503; rev:2;)**
- **Syntax :**
  - ◆ Actie : alert, log, pass, drop ...
  - ◆ Beperkingen : protocol source port direction destination port
  - ◆ Meta-settings : rules naam : parameters

# Meer dan snort

- (Her)samenstellen pakketten
- Cleartext paswoorden of gecodeerd in base 64
- Gebruik clouds (Dropbox, Onedrive...)
- Gebruik P2P
- Malware, Trojan, Virus
- Informatie verzamelen
- Brute Force

# Threat detectie



# Suricata bestanden

## ■ /etc/suricata/suracata.yaml

- ◆ instellen netwerken
- ◆ instellen regels

## ■ /etc/suricata/rules

- ◆ updates door suricata/oinkmaster

## ■ systemctl start/stop/status suricata

# Chinese Firewall

## ■ Baidu ipv Google (Maps, Search)



## ■ QQ/WeChat ipv Messenger/Discord



- Blokkeren woorden/images

## ■ Youku ipv Youtube



## ■ Alibaba/Banggood/Aliexpress

- Populair omdat de rest verboden is

# Cisco en the Chinese Firewall

**The Golden Shield Project:  
Public Network Information Security Monitor System**

Cisco.com

- Stop the network-related crimes
- Guarantee the security and services of public network
- Combat “Falun Gong” evil religion and other hostiles

[Note: Statement of Government goals from speech government official Li Runsen]