Network Engineering Deel 1

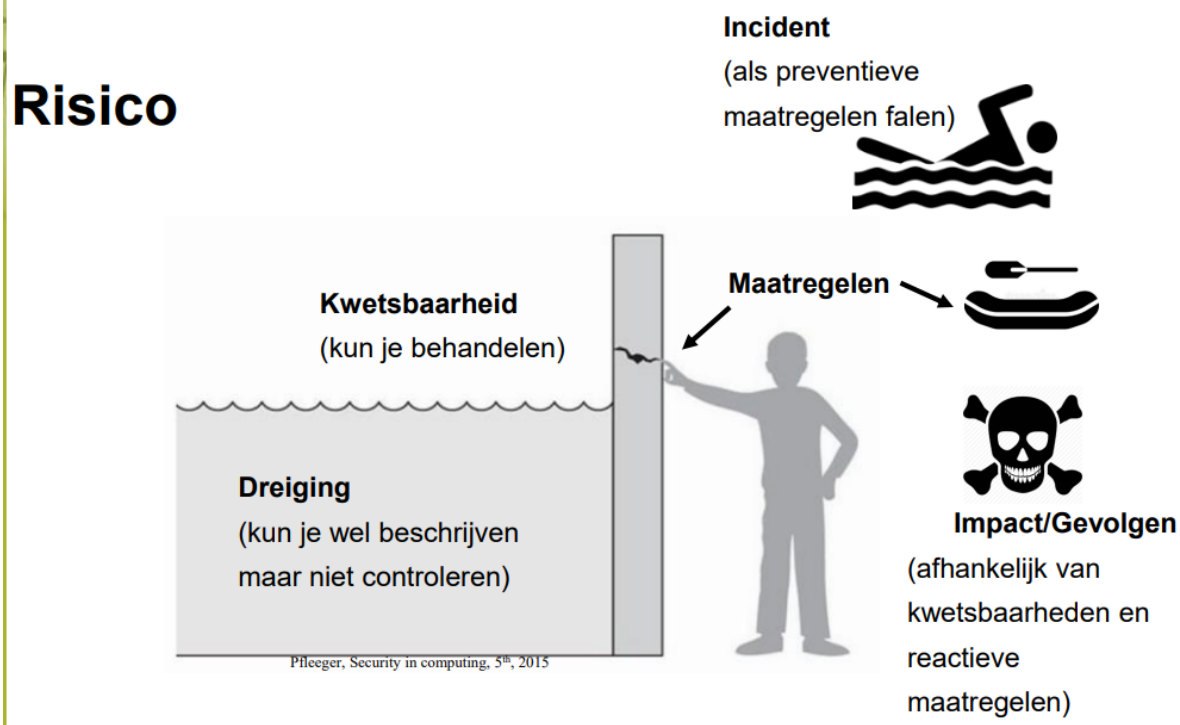
Cybersecurity

Cybersecurity (week 1)

Inleiding

In week 1 werd er een korte herhaling van Security essentials gehouden

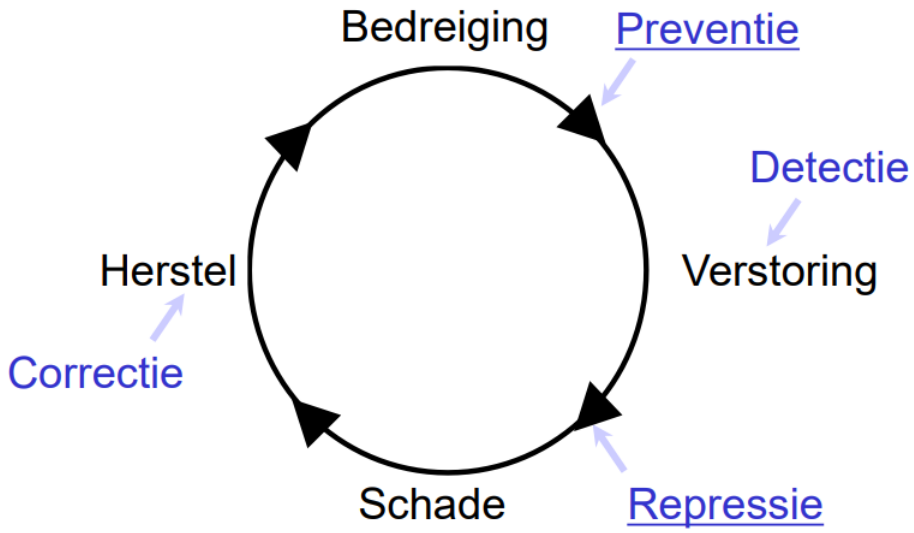
Een voorbeeld van Risico



Belangrijke begrippen

- **Incident**: Event dat tot schade gaat leiden (zonder verdere maatregelen)
  - *bijv. Host wordt overgenomen (pwnd), website down*
- **(Be)dreiging (threat)**: Oorzaak van een incident (het bestaan van deze oorzaken ligt buiten de controle van de risicopartij)
  - *bijv: malware, hacker, vijandelijke staat, APT, boze werknemer*
- **Kwetsbaarheid (vulnerability)**: escalatiefactor die de risicopartij gevoelig maakt voor een bepaalde dreiging;
  - *bijv: bug in de software, slechte configuratie, onvoorzichtige gebruiker*
- **(Beheers)maatregel (control)**: reduceert de waarschijnlijkheid van een incident en/of de impact/gevolgen van een incident.
  - *bijv: firewall, awareness-cursus*
- **Impact/Gevolgen**: (negatief) gevolg van een incident in de vorm van schade aan assets.
  – Informatiebeveiliging: impact vaak uitgedruikt in **B**eschikbaarheid, **I**ntegriteit en **V**eiligheid
  – Cybersecurity : Impact omvat ook anderssoortige gevolgen
  - *bijv: Data onbeschikbaar door onvrijwillige encryptie, Staatsgeheimen opwikileaks, Fabriek plat door een succesvolle malware-attack*

Beveiligingscyclus

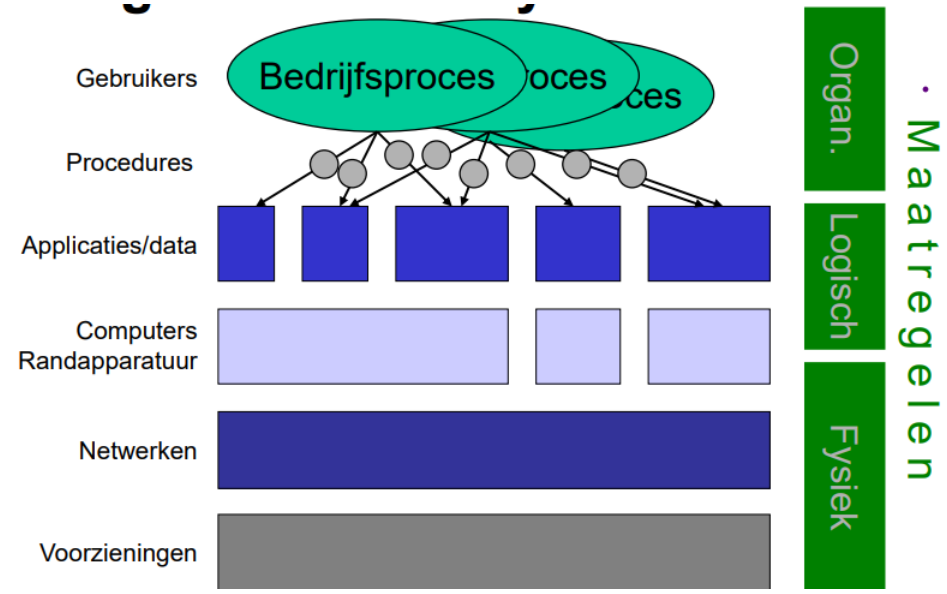


- **Preventieve maatregelen (werken voorafgaand aan het incident)**
  - *niet verwarren met proactieve maatregelen, deze neem je ook voorafgaand aan het incident. Maar deze werken pas tijdens of na het incident*
- **Reactieve maatregelen (werken tijdens of na het incident)**
  - *= detectieve + repressieve (+ correctieve maatregelen)*

Logische/Organisatorische/Fysieke Maatregelen

- Voorbeeld: beveiliging webserver:
  - **Logische maatregelen** (ook wel **Digitale maatregelen**):
    - *encryptie in de communicatie, firewall , software up-to-date, acces control voor gebruikers, AV-solution, IDS, Log-Monitoring*
  - **Organisatorische maatregelen**
    - *Beleid wie toegang heeft tot de serverruimte, IAM(Identity and access management voor users, admins, ...), SLA's (Service Level Agreements) over bijvoorbeeld storing en uitwijk, Security awareness, Scholing*
  - **Fysieke maateregelen**
    - *Server in beveiligde serverruimte met bewaking, slot op de deur, cameratoezicht*

Schematische weergave van maatregelen



Cybersecurity (week 2)

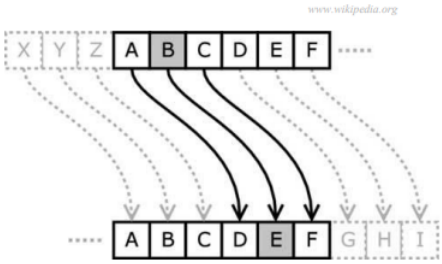
Voor meer informatie over cryptografie zie Aantekeningen Cyber 1, Aantekeningen Cyber 2

Inleiding

In week 2 hebben we het gehad over verschillende methodes voor cryptografie. De voorbeelden die besproken worden zijn:
Caesar

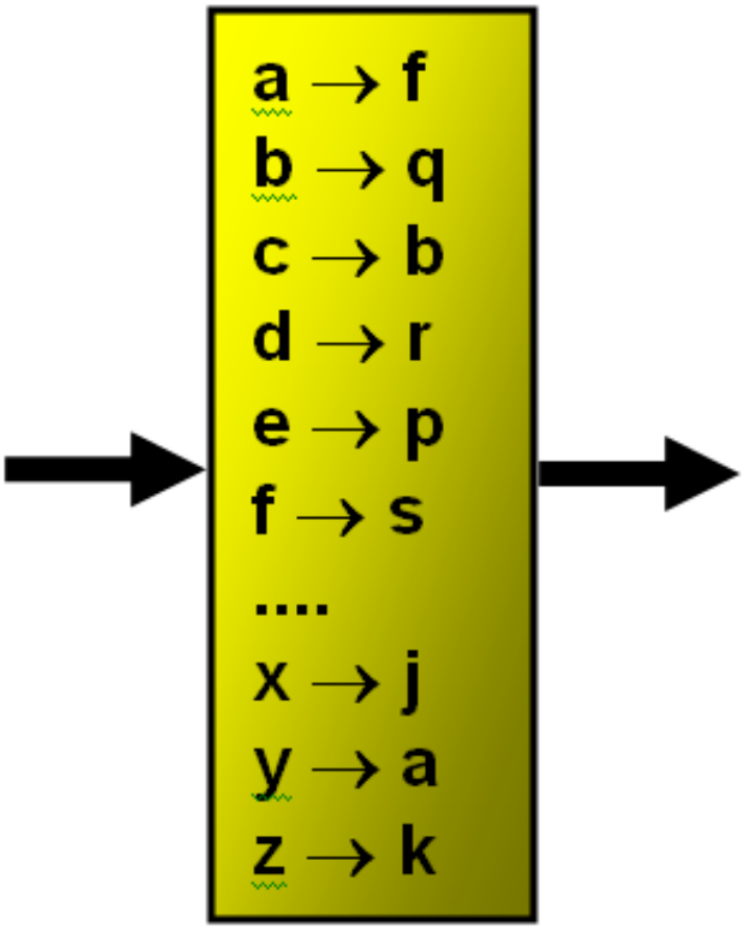
Substitutie 1 : Caesar

Meer info...
Bij Caesar encryptie word er een vaste verschuiving gebruikt zoals te zien in de afbeelding hieronder. In dit voorbeeld wordt er een verschuiving van A → D. Dit is een verschuiving van 3.
Voorbeeld



Substitutie 2: S-box

Meer info...
S-box cryptografie maakt gebruik van een lookup-table zoals hieronder.
Voorbeeld



Substitutie 3: Poly-alfabetische substitutie: Vignère

Meer info...
In plaats van een vaste verschuiving zoals bij Substitutie 1 : Caesar wordt er met meerdere verschuivigen gewerkt, vandaar

Poly-alfabetisch.

Er zijn 26^n sleutelmogelijkheden bij keylengte n

Tabel van Vignère

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y

Voorbeeld

– Stel de sleutel is **"nse"**. De letters geven drie verschillende Caesaroptellingen aan (n=13, s=18, e=4). Bij de 4^e letter van de plaintext, wordt opnieuw de eerste optelling gebruikt.

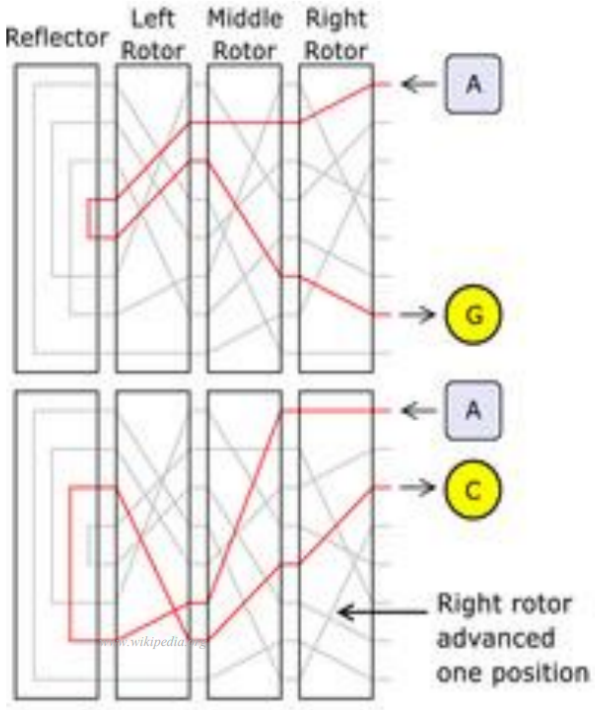
– Plain text is **"hallo"** (5 tekens) dus de 5 sleutel-rijen zijn **nsens**. Cyphertext is het snijpunt van plaintextletter en bijbehorende sleutelletter

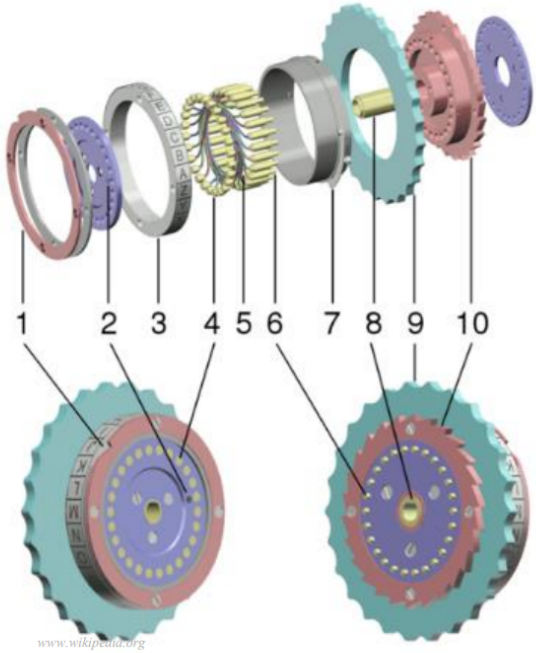
– Dus hallo ⇒ **"uspyh"**

Substitutie 4: Enigma

Meerdere rotors substitueren de letters en draaien steeds zelf verder, er is dus weer sprake van **poly-alfabetisch substitutie**
Je kunt dit alleen met de juiste beginstand van de rotors decrypten.

Schematische weergave van rotors





Vernam

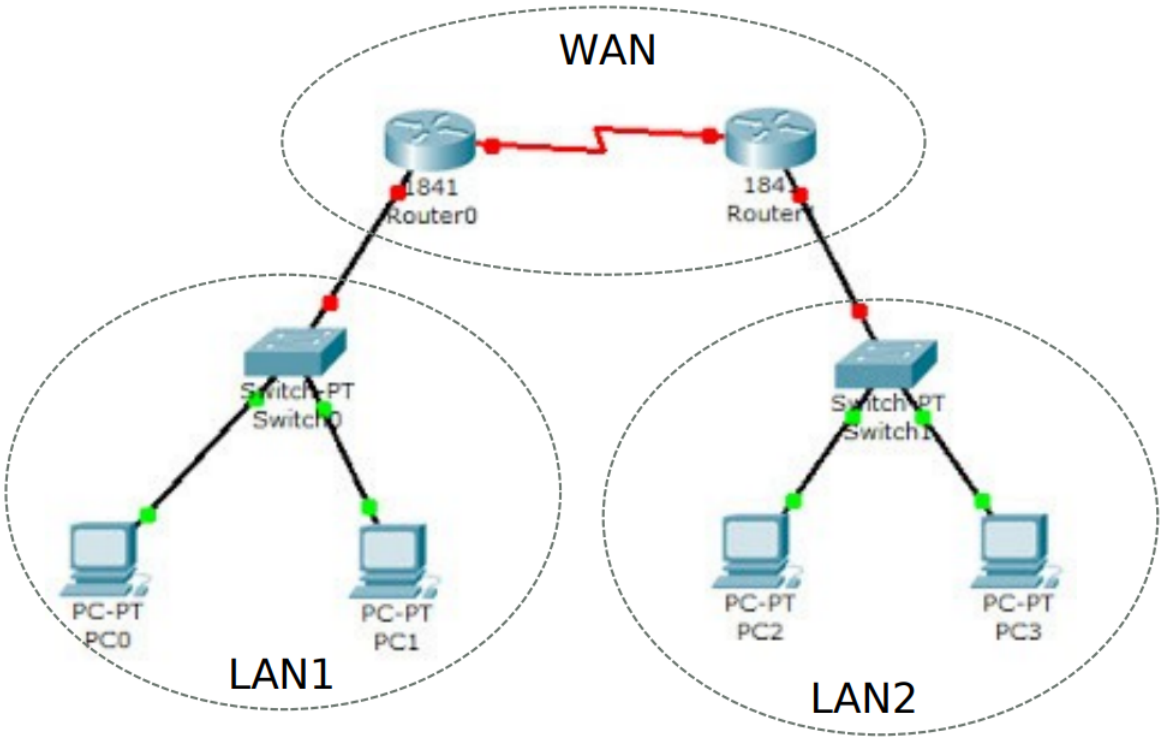
Vernam encryptie is Substitutie 3: Poly-alfabetische substitutie: Vignère waarbij legte van de key = lengte plain text

---

Routing & Switching (week 1)

LAN & WAN

- **WAN**
  - "Wide Area Network"
  - ISP (Internet Service Provider)
  - Verbindt netwerken
- **LAN**
  - "Local Area Network"
  - Thuis- of bedrijfsnetwerk
  - Verbindt clients



Mogelijke fouten in LAN

- **Collisions** Komen voor bij netwerken met een collision domain groter dan een host en bij een half-duplex verbinding
- **Late collisions** Botsing na de 512^{e} byte. Kan voorkomen als de kabel te lang (>100 meter) is, of bij duplex mismatch.
- **CRC errors** Kan ontstaan door verschillende redenen. Bv duplex-mismatch, of door botsingen of storingen (vooral bij draadloze verbindingen)
- **Runts** Een frame korten dan de minimale eis van 64 bytes. Ontstaat bij een collision. Ethernet framegroote moet altijd tussen 64-1518 bytes zitten
- **Giants** Een frame groter dan 1518 bytes
- **Discards**

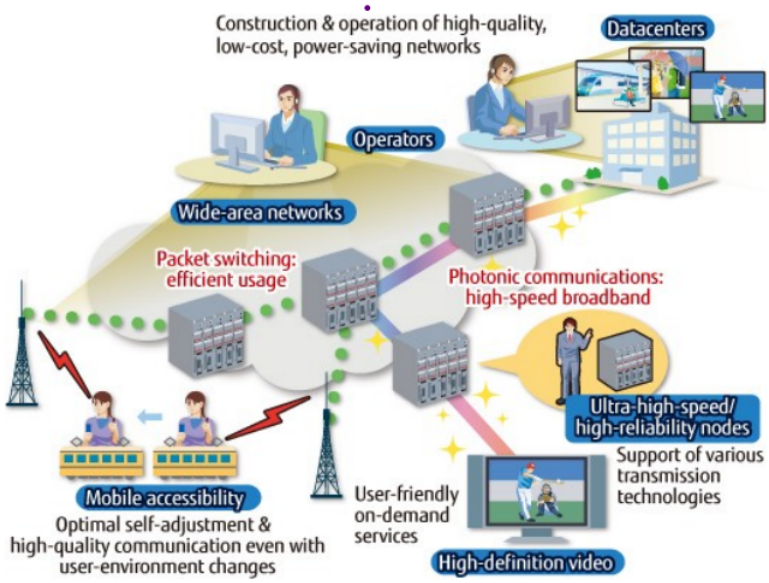
Netwerk-infrastructuur

1. **Services view**
2. **Components view**

3. **Protocols view**

1. Services View

```
De technische infrastructuur die bekeken vanuit de diensten die geleverd moet worden
```



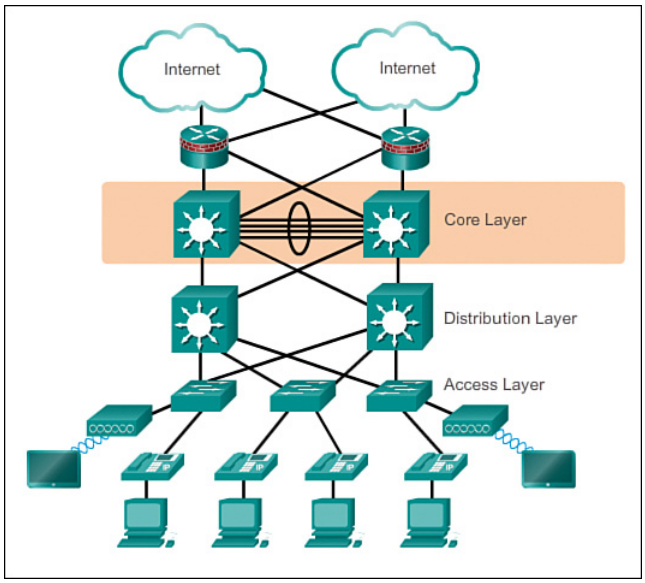
Aspecten

- Fault tolerance
  - Weerbaarheid van een netwerk tegen fouten/uitval
  - Moet blijven werken bij als een gedeelte uitvalt
- Beschikbaarheid (availability)
  - Beschikbaarheid van de services
  - Moet blijven werken bij als een gedeelte uitvalt
- Schaalbaarheid (scalability)
- Quality of service
- Beveiliging (security)
  - Vertrouwelijkheid
    - De data is niet toegankelijk voor onbevoegden
  - Integriteit
    - De data verandert niet onderweg
  - Beschikbaarheid
    - Het werkt zoals het zou moeten werken

De belangrijkste manier om Fault tolerance en beschikbaarheid te behouden is redundancy (redundantie). Hierbij heb je een backup voor als de hoofd apparatuur niet werkend is.

---

2. Components View

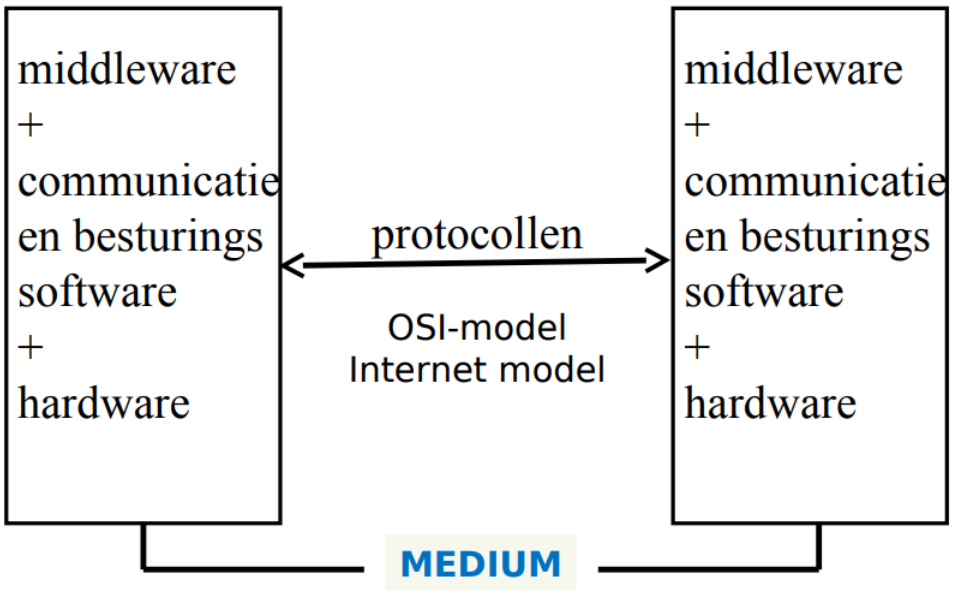


---

3. Protocols View

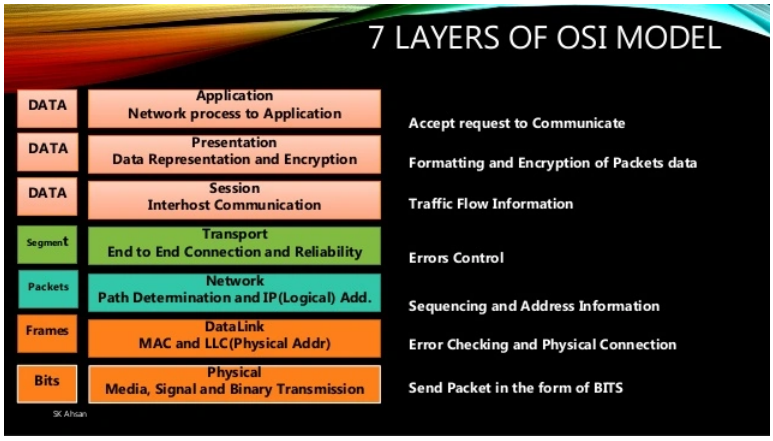
Op een computernetwerk gebruikt software databussen. Maar het daadwerkelijke transport gaat via elektromagnetische golven door bv: *fiber, kabel, ether*.
Netwerk -hardware en Software vertaalt de informatie behoefte van de applicatie naar elektrische signalen die worden verzonden via elektromagnetische golven.
Om dit te doen hebben we netwerkprotocollen nodig.

Representatie van Protocols View (Layered View)



Osi model

Lagen van het OSI model



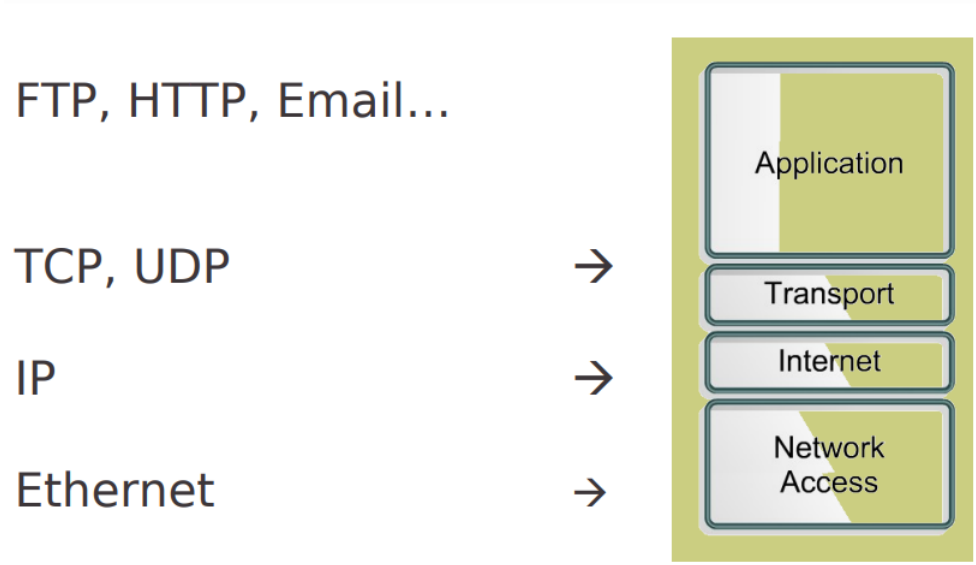
Elke laag van het OSI model levert een service aan de laag eronder

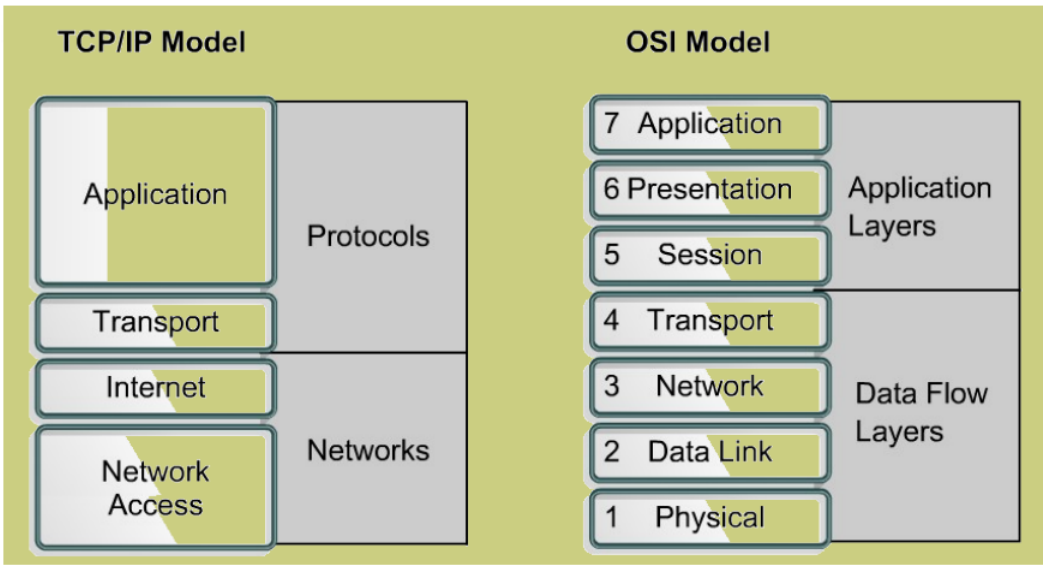
Voordelen

- Protocollen worden per laag ontwikkeld dus een verandering van een protocol hoeft geen gevolgen op de andere lagen te hebben
- Omdat er een gemeenschappelijke manier van communiceren is zorgt dit voor consistentie in de systemen

---

Internet model (TCP-IP model / DOD model)





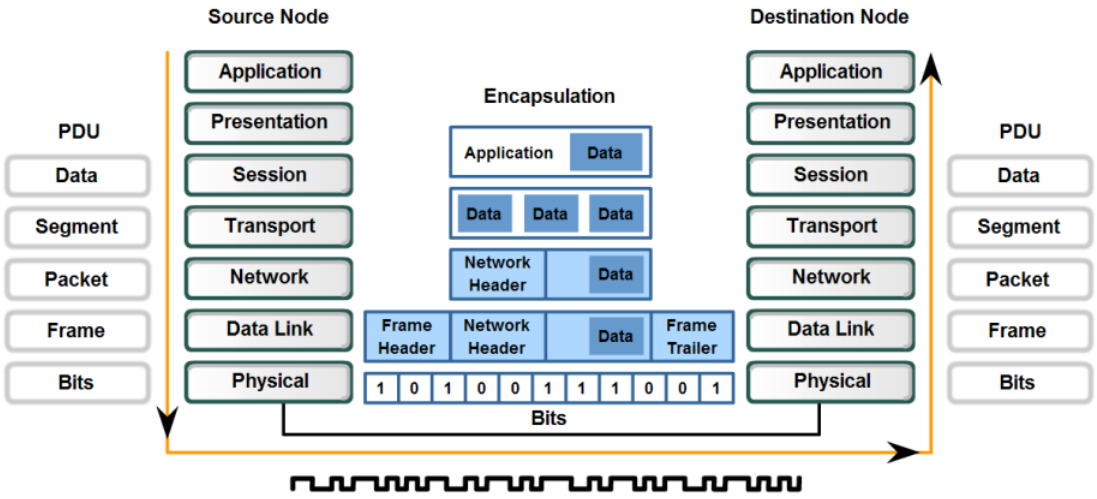
Inpakken van data (Encapsulation)

Applicatie-laag : produceert data en geeft het door aan de Transport-laag
Transport-laag:

- Deelt data op in segmenten
- Voegt aan elk segment een header toe en geeft het door aan de Netwerk-laag

Netwerk-laag: Voegt een header toe em geeft het door aan de Datalink-laag
Datalink-laag Voegt een header en een trailer toe dit wordt doorgegeven aan de Fysieke laag
Fysieke Laag Voegt bits toe voor error-correctie

In de afbeelding hieronder zie je de Encapsulation en decapsulation van de PDU's (Protocol data unit)



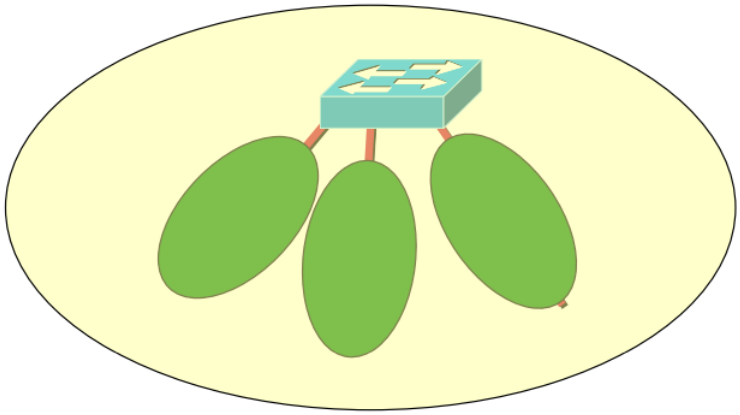
Eerder werd besproken over collisions bij

> ## LAN & WAN

Nu gaan we hier verder naar kijken

Collision vs Broadcast domains

Een switch scheidt **collision domains** en geen broadcast domains.



In dit voorbeeld zijn er 3 **collision domains** en 1 broadcast domain

Scheiden

Er zijn twee manieren om gescheiden broadcast domains te krijgen dit zijn:

- Routers
- Switch: VLAN (Virtual LAN)

Bij VLAN's wordt de switch virtueel verdeelt in kleinere switches zodat elke poort een eigen LAN heeft.

Router

Met een router word het broadcast domein verkleint, een broadcast domain is een deel van een netwerk waar alle verstuurde berichten aankomen.
Bij een router worden broadcast berichten niet doorgegeven naar het volgende netwerk en daarom wordt het broadcast domein gescheiden.

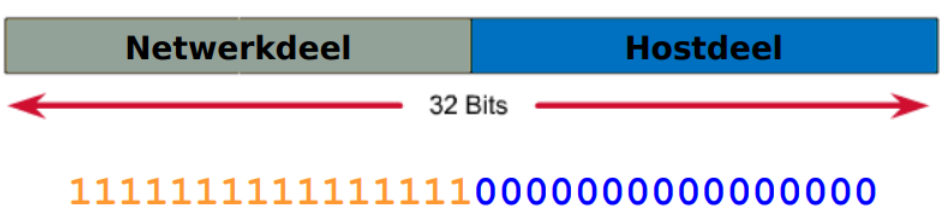
Routing & Switching (W;eek 2)

In week twee hadden we het over subnetten.

IPV4 adres

Netwerkdeel en Hostdeel

Een IP adres bestaat uit een **Netwerkdeel** en een **Hostdeel** en is in totaal 32 bits lang.
Het **netwerkmasker** bepaalt het netwerkdeel en het hostdeel
Heet net masker bestaat uit een *aaneensluitende* reeks aan enen gevold door een *aaneensluitende* reeks aan nullen. Waarbij de enen het netwerkdeel zijn en de nullen het hostdeel.



Deze enen en nullen zijn binaire getallen die als volgt worden opgeschreven.

```
11111111.11111111.0000000.000000
```

In dit voorbeeld krijg je de volgende informatie uit het binaire getal

```
Dotted decimal: 255.255.0.0
Prefix: /16
Wildcard: 0.0.255.255
```

Adressentypen

Netwerkadres (subnet) Bepaalt de range van het hostdeel. En word aangegeven met de prefix.
Hostadressen: Adressen die worden gegeven aan de eindgebruikers van een netwerk. De range hiervan is het aantal bits dat over blijft na het instellen van het netwerkadres
Broadcastadres: Wordt alleen maar gebruikt om data te versturen naar alle hosts in het netwerk.

Classful netmaskers

> | Netmask | 1^e octet | 2^e octet | 3^e octet | 4^e octet |
> |---|---|---|---|---|
> | 255.0.0.0 of /8 | Network | host | host | host |
> | 255.255.0.0 of /16 | network | network | host | host |
> | 255.255.255.0 of /24 | network | network | network | host |

In deze tabel is precies te zien waar het netwerkdeel eindigt en het hostdeel begint voor verschillende prefixes.

Subnet

Voor alle subnetten geld er dat het aantal hosts gelijk is aan s^n waarbij n het aantal host bits is. Stel je hebt 24 host bits dan zijn er dus $2^{24} = 17777216$ hosts. Ook geld er dat er altijd een netwerkadres is en een broadcastadres.

VLSM (Variable length subnetmask)

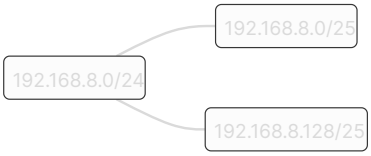
Met VLSM kan je:
Classless netwerken definiëren dus de prefix hoeft niet /8, /16 of /24 te zijn.

Supernetten

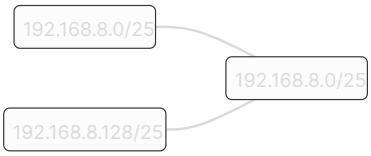
Naast subnetten heb je ook supernetten dit is wanner je netwerken combineert in een groter netwerk

Voorbeelden Sub- en supernetten

Subnetten



Supernetten

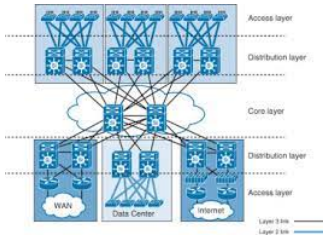


Routing & Switching (week 3)

In week 3 hebben we het over basic switching en VLAN's gehad

Netwerk Architectuur

Het in lagen verdelen van een netwerk heeft als voordeel dat elke laag zijn eigen functie heeft. Daarnaast is het makkelijker te beheren en heeft het optimale performance.

> Voorbeeld van een optimaal netwerk
> 
>

Gebasseerd op dit netwerk kan je elk netwerk maken

Lagen

Acces layer

De laag met de end devices (PC's, servers, printers, wireless acces points)

Distribution layer

- Aggregatie van/naar de acces layer
- Hier komen de meeste security en routing regels
- Verdeelt doorgaans de acces laag in VLANs

Core Layer

- High speed backbone van het netwerk Hoge availability en redundant uitgevoerd
  - Moet snel, veel data kunnen forwarden
  - Bij kleinere netwerken, collapsed model (Core and distribution samengevoegd)

High availability

- High availability minimizes $\underline{downtime}$
- Involving redundancy in:
  1. Equipment
  2. Technology - hardware and software
  3. People
  4. Processes
  5. Tools

Switches

Poorten

Poort density: Geeft het aantal poorten van de switch aan

- Forwarding rate:
  - Definieert hoeveel data de switch kan verwerken per seconde
  - lower performing switches gaan op de acces layer
  - higher performing switches gaan op de distribution en care layers
  - Als de forwarding rate te laag is, kan de switch $\underline{downtime}$

Types

Layer 2: werkt met MAC-adressen
Layer 3: werk met IP-adressen

POE

Power over ethernet:
Stroomvervoer over dezelfde ethernet kabel als het dataverkeer

Symmetrisch

- Symmetrisch
  - Alle poorten hebben dezelfde bandbreedtes
  - Voor netwerk(deel) met stabiel netwerkverkeer

Asymmetrisch switching

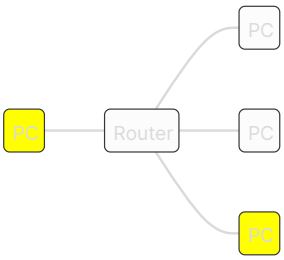
- Asymmetrisch
  - Sommige poorten hebben verschillende bandbreedtes
  - Bijv: meer bandbreedte voor een server om een bottleneck te voorkomen

---

Netwerken met VLANs

- Eeen VLAN id wordt toegekend aan een switchpoort
- Hosts die tot een gemeenschappelijk VLAN behoren, worden geconfigureerd in hetzelfde IP subnet
- Iedere VLAN beschikt over eenuniek default-gateway adres. De default-gateway is een router of multilayer switching
  De VLAN kan niet door de andere LAN's bereikt worden
  Zie #voorbeeld

#voorbeeld



Speciale VLANs

- Native VLANs
- Een van de VLANs is benoemd als native VLAN
  - Zender: voegt geen tag toe voor nativ-VLAN over de trunk
  - Ontvanger: als een frame uit een trunk komt zonder tag dan wordt deze geplaatst in de nativ-VLAN
  - Wordt gebruikt voor on-switch-protocollen
  - Default is iedere switchpoort van VLAN 1

Trunking

De frames uit verschillende VLANs kunnen over een verbinding verplaats worden naar een andere switch of router.
Dit heet trunking en word met de IEEE 802.1q standaard gedaan

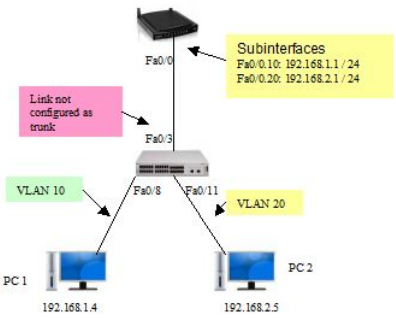
---

Routeren tussen VLANs

AKA: Inter VLAN Routing

- VLANs zijn gescheiden van elkaar
- Hosts in verschillende VLANs kunnen elkaar dus niet pingen
- Om data van een VLAN naar een host in een ander VLAN te sturen heb je dus een router nodig
- Dat kan met een "Router on a stick configuratie"

Configuratie voorbeeld router "On a stick"



Vergeet niet om de no shutdown command toe te voegen

```
$ no shutdown
```

Met dit netwerk kun je zowel pc 1 als pc 2 pingen
