Cisco CCNA

Table of Contents

[Chapter one: Personal Computer hardware 2](#_Toc264563170)

[Verschillende soorten computers: 2](#_Toc264563171)

[Binaire representatie van data 3](#_Toc264563172)

[Eenheden 3](#_Toc264563173)

[Verschil volatile-non volatile 3](#_Toc264563174)

[Chapter two: Operating Systems 4](#_Toc264563175)

[Chapter three: Connecting to a network 5](#_Toc264563176)

[OSI-model 6](#_Toc264563177)

[Application 6](#_Toc264563178)

[Presentation 6](#_Toc264563179)

[Session 6](#_Toc264563180)

[Transport 6](#_Toc264563181)

[Network (IP-Adres, packets) 7](#_Toc264563182)

[Data(MAC-Adres, Frames) 7](#_Toc264563183)

[Physical 7](#_Toc264563184)

[Chapter four: Connecting to the Internet Through an ISP 9](#_Toc264563185)

[Chapter five: Network Addressing 10](#_Toc264563186)

[Klasse netwerken 10](#_Toc264563187)

[Privé ip adressen 10](#_Toc264563188)

[Chapter six: Network services 11](#_Toc264563189)

[Poorten 11](#_Toc264563190)

[TCP-IP model 11](#_Toc264563191)

[Chapter seven: Wireless Technonlogies 12](#_Toc264563192)

[Chapter eight: Basic Security 16](#_Toc264563193)

[Network threats 16](#_Toc264563194)

[Methods of Attack 16](#_Toc264563195)

[Security procedures and applications 17](#_Toc264563196)

[Chapter nine: Troubleshooting your network 19](#_Toc264563197)

* Lab 1.3.1.1 en 1.3.2.2 🡪 P.13
* Interactive Activity: Address Blocker Game
* Interactive Activity 5-5: Who will Receive the Message-Game 🡪 netwerk id, broadcast ip etc berekenen

# Chapter one: Personal Computer hardware

**Bios** (Basic Input-Output System): Laadt de basis instructies om een functionaliteitstest uit te voeren en het OS te zoeken en te laden. De BIOS is permanent opgeslagen op een hardware chip.

**Firmware** is een reeks instructies geschreven op een hardware chip om een bepaald hardware apparaat correct te doen functioneren.

## Verschillende soorten computers:

* **Mainframe**: Grote gecentraliseerde computers, meestal in grote bedrijven en moeten aangekocht worden via gespecialiseerde verkopers
* **Server**: Zijn high-performance computers die vaak in bedrijven gebruikt worden om diensten te voorzien aan veel gebruikers of clients.
  + **Standalone**: Hoge flexibiliteit en selectie van interne componenten maar nemen veel plaats in beslag
  + **Rack-mounted**: Besparen plaats als er racks vrij zijn
  + **Blade**: Zijn voorzien van de grootste concentratie aan snelheid en kracht in de kleinste ruimte
* **Workstation**: Lijkt veel op een gewone computer maar zijn meer high-powered ontwikkeld voor gespecialiseerde high-end applicaties zoals **CAD**(Computer-Aided Design) ,...
* **Desktop**: Ook gekend als Personal Computer is een computer die als gewone consument wordt gebruikt en is uitbreidbaar en aanpasbaar voor de gebruiker
* **Laptop**: Zijn vergelijkbaar als de **Desktops** maar dan in compacte vorm en verbruiken minder stroom
* **Handheld**: Dit zijn apparaten zoals de smart-phones, PSP, PDA’s,...

Een **Daemon** is een service die draait op een server.

## Binaire representatie van data

Een digitaal signaal gebeurt met bits bestaande uit allemaal 1’en en 0’en, analoog in een elektrisch signaal.

### Eenheden

* **Snelheid over medium**: kbps (BITS!!)
* **Grootte van een bestand**: Kb (BYTES!!)
* **Resolutie van een scherm**: pixels
* **Frequentie**: Hertz

### Verschil volatile-non volatile

Volatile is een vluchtig en dus als de stroom weg valt zal het geheugen ook weg gaan, non volatile daarentagen is niet vluchtig en zal dan het geheugen bijhouden.

**NIC**: **N**etwork **I**nterface **C**ard, voor de connectie met een netwerk, zorgt voor **IP adres**, **Subnet mask** en **Default gateway**

**UPS**: **U**ninterruptible **P**ower **S**upply, heeft een interne batterij om tijdelijk stroom te voorzien als de netstroom is uitgevallen.

# Chapter two: Operating Systems

Wat is de **kernel**? De **kernel** zorgt voor de interactie van het **OS** met de Hardware, de **Kernel** vormt samen met de **Shell** het **Operating System**.

Toegang tot **OS** is verschillend, moeilijke diepgang bijvoorbeeld moeilijk mac adres veranderen in Windows, in Linux is dis makkelijker.

**DHCP**: Dynamic Host Configuration Protocol, is voorzien van een soort mechanisme voor het automatisch toewijzen van IP adres, Subnet Mask, Default Gateway en andere informatie aan hosts op het netwerk

# Chapter three: Connecting to a network

**Converged network**: Dit is een netwerk waar allerlei soorten datacommunicaties samenkomen in één netwerk structuur (computer netwerk, video netwerk, voice netwerk,... allemaal in 1 netwerk)

Een **server** kan:

* Een service aan meerdere clients tegelijk verlenen
* Meerdere types server software draaien
* Een e-mail server en web server en file sharing server zijn tegelijk

Een **client** kan meerdere types software draaien maar er moet software geïnstalleerd zijn voor iedere service vereist van de server

**Peer-to-peer netwerk:**

* **Voordelen**:
  + **Gemakkelijk** te maken
  + **Minder ingewikkeld**
  + **Goedkoper** omdat er geen netwerk apparaten nodig zijn of servers
  + Kan gebruikt worden voor **simpele taken** zoals bestanden overzetten en printers delen
* **Nadelen**:
  + Geen centrale **administratie**
  + **Niet** echt **veilig**
  + **Tragere** performance omdat alle apparaten client en server kunnen zijn

**Fysieke topologie**:

* Laat zien waar elke host zit en hoe die is verbonden met het netwerk
* Laat zien waar de kabels zijn geïnstalleerd, locatie van kabel kasten en netwerk apparaten die de hosts verbinden
* Is vaak gebasseerd op een bouwplan

**Logische topologie**:

* Groepeert de hosts op basis van hoe ze het netwerk gebruiken
* Plaats in het gebouw maakt niet uit
* Host naam, adres, groep informatie en applicaties kunnen op de logische topologie staan
* Een groep hosts kan ook weergeven worden door 1 icoon
* Details van bekabeling worden vaak weg gelaten

**CSMA/CD**: **Carrier Sense, Multiple Access with Collision Detection**, Dit betekend dat meerdere hosts luisteren naar de kabel voor een trasmissie van een andere host en als er geen gevonden is kunnen ze zelf beginnen te sturen, als twee hosts op hetzelfde moment zenden dan is er een botsing en detecteren de hosts dit en stoppen ze met zenden.  
**CSMA/CA**: **Carrier Sense, Multiple Access with Collision Avoidance**, doet het zelfde als de vorige maar stuurt eerst een reservatie signaal voor het apparaat iets gaat verzenden zodat er geen botsing kan plaatsvinden

## OSI-model

|  |
| --- |
| Zender |
| Application |
| Presentation |
| Session |
| Transport |
| Network |
| Data |
| Physical |

|  |
| --- |
| Ontvanger |
| Application |
| Presentation |
| Session |
| Transport |
| Network |
| Data |
| Physical |

Fysieke verbinding

### Application

In deze laag zijn de toepassingsprogramma’s actief waarmee computergebruikers met elkaar communiceren (browser of dergelijke). Levert geen diensten aan andere lagen, maar wel diensten aan toepassingen zoals:

* Browsers
* E-mail programma’s
* Nieuwslezers
* ...

De toepassingslaag zorgt er ook voor dat de juiste protocols worden geactiveerd voor een bepaalde verbinding. E-mail verzenden wordt dus helemaal anders behandeld dan het plaatsen van een bestand op een fileserver.

### Presentation

Niet alle computers werken met dezelfde bestandsformaten en –systemen. Daarom wordt in deze laag al de in- en uitgaande informatie getransformeerd naar een vooraf vastgesteld standaardformaat. Hier vind ook gegevenscompresse en –decompressie, encryptie en decryptie en netwerkbeveiliging plaats.

### Session

Zorgt ervoor dat een gebruiker zich bij een andere gebruiker of een server slechts één keer hoeft aan te melden voor de duur van de verbinding. De sessielaag synchroniseert ook de verbinding tussen de twee computers om te voorkomen dat de verbinding te vaak verbroken zou worden en telkens alle gegevens opnieuw verstuurd moeten worden.

### Transport

Belangrijkste taak is om de gegevens op te splitsen in kleinere eenheden, die segmenten worden genoemd, dit noemt men segmenteren of fragmenteren. Dit is tevens de eerste laag die zich bezig houdt met het datatransport tussen de twee computers.

Deze laag zorgt ook voor betrouwbaarheidsgarantie (quality of service=QOS): zorgt ervoor dat de gegevens zonder wijzigingen bij de ontvanger terecht komen. Hiervoor wordt de laag verdeeld in 5 transportklasse, terwijl de hoogste klasse de meest doorgedreven foutcontrole kent. Hoe hoger de klasse, hoe meer vertraging er kan optreden.

Om te bepalen welke transportklasse wordt gebruikt wordt de kwaliteit van de verbining bepaald volgens volgende gegevens:

* Creatietijd van de verbinding
* Foutenkans bij creatie verbinding
* Doorvoer (bytes per seconde overgebracht)
* Transittijd (tijd tussen versturen bericht en ontvangen)
* Resterende foutenfrequentie (aantal verloren of vervormde berichten)
* Kans op transfert-fouten
* Opheftijd van een verbinding
* ...

Deze QOS parameters worden door de transportgebruiker bij het aanvragen van een verbinding opgegeven(automatisch).

### Network (IP-Adres, packets)

Deze laag verpakt de informatie in pakketjes. Elk pakketje heeft de adresinformatie van het bericht, zodat er geen enkel verloren gaat. Ook regelt deze laag de doorstroming van pakketjes zodat er geen overbezadiging van de datacommunicatielijnen ontstaat. Computers worden op deze laag herkend door hun IP-adres.

IP-adres van zender en ontvanger zijn van belang voor het bepalen van de weg die het pakketje gaat afleggen, het bepalen van die weg wordt path determination genoemd en gebeurd door routers. Voor het pakketje vertrekt wordt de snelste weg bereken. Hiervoor bestaan verschillende methoden:

* Hot patatoe strategie: komt neer op het doorgeven van een binnengekomen bericht naar de uitgang met de korste wachtrij. Nadeels is dat er vaak een lange route over veel knooppunten wordt berekend, dus is zeker niet altijd snel.
* Fixed routing: vastleggen van netwerkroutes in vaste tabellen resulteert in het volgen van vaste routes. Nadeel: sommige netwerkverbindingen worden overbelast.
* Adaptive routing: In grote netwerken is het gewenst dat de wijdere omgeving van de toenemende verkeerslast op de hoogte gebracht wordt om tijdig op andere routeringsschema’s over te stappen.

### Data(MAC-Adres, Frames)

In deze laag worden de pakketjes opgedeeld in of samengevoegd tot frames. Zo’n frame kan dus meerdere pakketjes bevatten, die zelfs van verschillende zenders afkomstig zijn, maar voor een gedeelte gebruik maken van dezelfde route. Je zou kunnen zeggen dat een pakketje uit de netwerklaag een logische eenheid van te verzenden gegevens is, en een frame een fysieke eenheid.

### Physical

Deze laag vervoert de bits zonder zich ook maar iets aan te trekken van de betekenis, of de foutcontrole. Dit is de laag waartoe de netwerkbekabeling hoort. Hierin worden de verschillende componenten beschreven die belangrijk zijn voor de manier waarop de gegevens moeten doorgestuurd worden, zoals het soort bekabeling, de maximale kabellengte, de gebruikte modulatie- en codeertechniek connectoren, enz.

**Unicast**: Een client stuurt een bericht naar 1 andere host

**Multicast**: Een client stuurt een bericht naar meerdere andere hosts

**Broadcast**: Een client stuurt een bericht naar alle andere clienst

**CSMA**

* Luisteren voor je iets stuurt
* Als 2 berichten tegelijk verstuurt werden: botsing op gedeeld medium
* Botsing ontdekt 🡪 tijdelijk geen bericht

**10BASE5**: Een ethernet kabel die 10Mbit/s haalt en een max lengte van 500 meter heeft.

**Mac adres – Fysiek adres (AA : AA : AA : AA : AA : AA)**

* Is uniek en staat vast in de **Network Interface Card**
* 12 hex karakters van elk 4 bits (6 paar)
* Eerste 3 paar = staan voor de fabrikant
* Laatste 3 paar = staan voor de unieke **Network Interface Card** van de fabrikant

**PDU**: **Protocol Data Unit**, **Frame**(Data link laag), **Packet**(Netwerk laag), **Segment**(Transport laag)

**Frame**

* Max 1518 bytes – min 64 bytes
* Preamble
* Geen timing, nu start de frame
* Mac adres
* Lengte / type
* Data
* Kijken voor errors

**Collision domain**: een gebied waar botsingen van packets kunnen plaatsvinden, enkel slimme apparaten (switch, hub) kunnen een **collision domain** beperken

**Broadcast domains**: Te veel broadcasts op 1 netwerk 🡪 netwerk trager, dus meerdere **broadcast domains**. Routers stoppen **Broadcast domains**.

**ARP**: **Adress Resolution Protocol**

* Tabel is gevuld met elke frame die passeerd door de **Network Interface Card**
* Als er nog geen mapping is:
  + Een **Broadcast domain** wordt aangemaakt, in de frame is een IP pakket met destinatie adres, destinatie host zal antwoorden met zijn frame 🡪 wordt toegevoegd aan de **Adress Resolution Protocol tabel**

**IP-adres**: 192.168.1.5 🡪 192.168.1 is het netwerk portie en 5 is het host gedeelte

# Chapter four: Connecting to the Internet Through an ISP

**ISP**: **Internet Service-Provider** verschillen in:

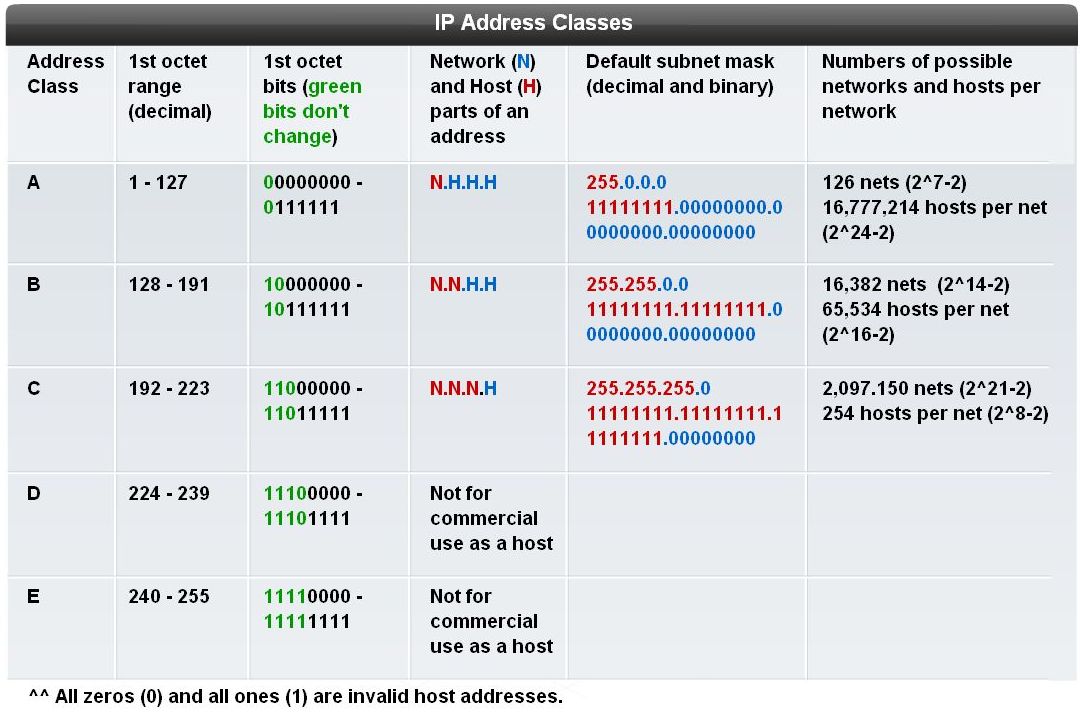
* Grootte en gebied van diensten
* De diensten die ze verlenen
* Types connectie technologieën die ze ondersteunen
* De snelheden die ze bieden

**POP**: **Point of Predence**, is het gebouw van de regio die de gebruikers toegang geeft tot het **Internet Service-Provider**’s netwerk en het internet

**Crosstalk**: Samengebundelde kabels op lange afstand kunnen het soms aan de hand hebben dat het signaal van de ene kabel overspringt naar een andere kabel.

# Chapter five: Network Addressing

## Klasse netwerken



## Privé ip adressen

|  |  |  |
| --- | --- | --- |
| Adres klasse | Nummer netwerk cijfers gereserveerd | Netwerk adres |
| A | 1 | 10.0.0.0 |
| B | 16 | 172.16.0.0 – 172.31.0.0 |
| C | 256 | 192.168.0.0 – 192.168.255.0 |

**Loopback adres:** **127**.0.0.0 – 127.255.255.255

**APIPA (geen dhcp)**: **169.254**.0.1 – 169.254.255.254

**NAT: Network Adress Translation**, zorgt voor het converteren van privé ip adressen naar Internet adressen

# Chapter six: Network services

## Poorten

|  |  |
| --- | --- |
| Poort | Protocol |
| 20 | FTP Data |
| 21 | FTP |
| 22/23 | Telnet/SSH |
| 25 | Simple Mail Transfer Protocol (SMTP) |
| 53 | Domain Name System (DNS) |
| 67 | DHCP |
| 80 | HyperText Transfer Protocol (HTTP) |
| 443 | HTTPS |

## TCP-IP model

|  |  |  |
| --- | --- | --- |
| TCP-IP model | Layer | Description |
| Application | 4 | Hier werken hoge level protocollen zoals SMTP en FTP |
| Transport | 3 | Waar flow-control en connectie protocols bestaan |
| Internet | 2 | Waar ip-adressen en routing plaatsvind |
| Network Access | 1 | Waar MAC adressing en fysieke netwerkcomponenten bestaan |

**SOCKET**: is het ip en de poort in 1 adres, dit zorgt ervoor dat er slechts 1 ‘adres’ is en die zegt naar welk ip adres het pakket moet gaan en welk programma  
vb: 192.168.0.1:80 , het pakket gaat naar computer met IP 192.168.0.1 en naar poort 80, dus HTTP 🡪 dus de browser

# Chapter seven: Wireless Technonlogies

**Voordelen draadloos:**

* Mobiliteit
* Gemakkelijk uit te breiden
* Flixibel, kan overal verbinden
* Goedkope uitrusting
* Kortere installatie tijd

**Nadelen draadloos:**

* Interference van andere apparaten
* Beveiliging is niet geweldig
* Technologie is nog aan het evolueren

**Infrarood:**

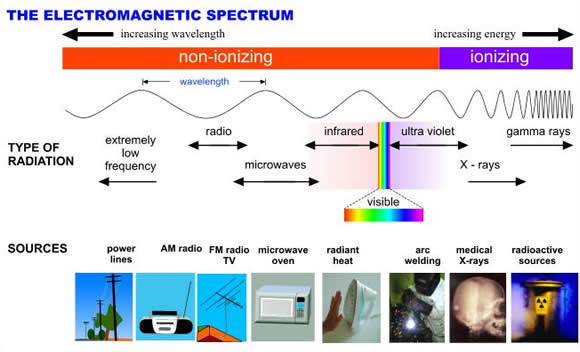
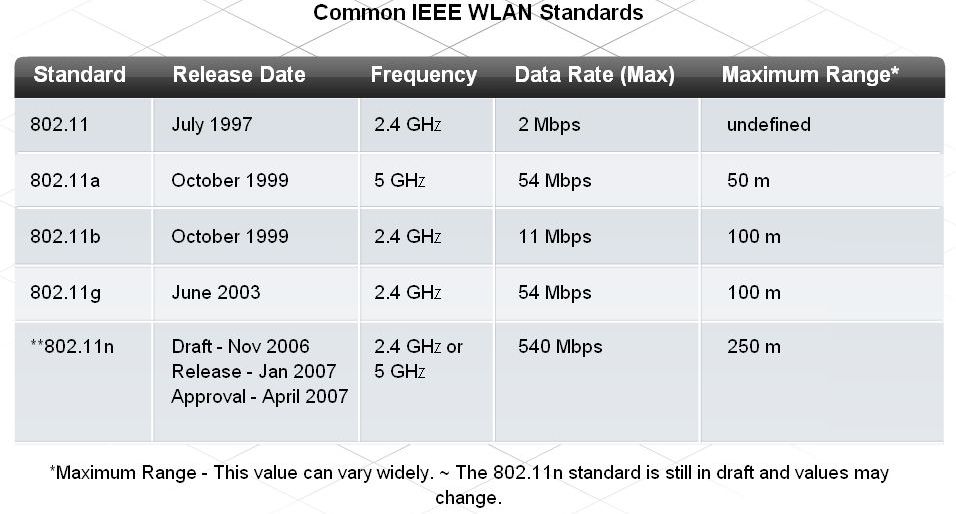
* Lage energie
* Korte afstand
* Geen penetratie van objecten
* One to one

**Radio frequencie:**

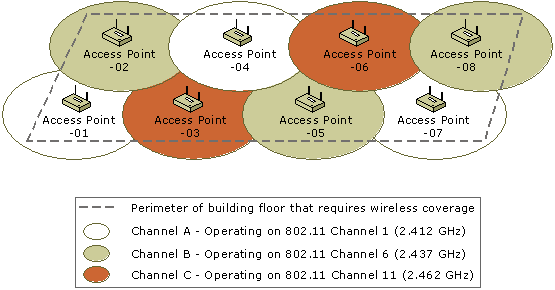
* Hoge energie
* Penetratie
* 2.4 en 5 GHz 🡪 WLAN (**IEEE802.11**)

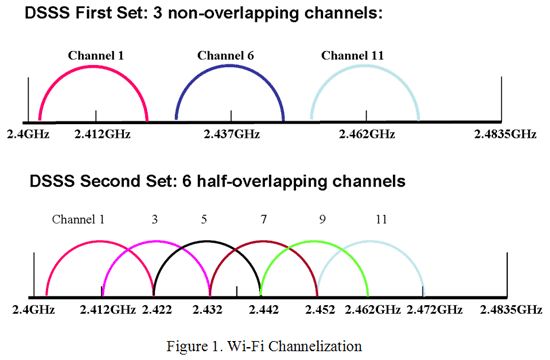
**Bluetooth:**

* Lage snelheid
* Korte afstand
* One to many communicatie



**Wireless client**: gebruiker  
**Access Point**: verbindt draadloos netwerk met het gewone netwerk, multi-functionele apparaten kunnen ook frams vertalan ven de 802.11 standaard naar 802.3 en omgekeerd  
**Wireless bridge**: Lange afstand verbinding tussen wireless connecties  
**Antennas:**  output signaal versterken  
**Omnidirectioneel:** in alle richtingen  
**Directioneel**: In slechts 1 richting (sterker signaal, het is gebundeld naar 1 richting)  
**SSID**: Service Set Identifier, het **ID** van een netwerk  
**Ad hoc**: Draadloos peer to peer netwerk





**Beveiliging draadloos netwerk**:

* SSID verbergen
* Paswoord gebruiken
* Default settings veranderen
* Encryptie gebruiken

**Open authenticatie**: Geen autheticatie nodig, iedereen kan gebruik maken van de AP  
**Pre-shared key**: Client en AP delen geheime sleutel, wanneer een client verbindt met de AP:

* AP stuurt **challenge string**
* Client encrypteert **challenge** met sleutel
* AP controlleert de encrypted challenge

**Extensible Authentication Protocol (EAP)**: 2 way authentication en user authentication. Client communiceert met back-end-authentication server. Gebruikt **Open Authentication** om eerst met de AP te communiceren.

**WEP**: **Wired Equivalency Protocol**: Gebruik een statisch wachtwoord tussen alle apparaten, heeft een serieus wiskundig probleem 🡪 makkelijk te kraken  
**WPA**: **WiFi Protected Access**: Gelijk **Wired Equivalency Protocol** maar genereerd nieuwe dynamische sleutels iedere keer als een client connectie maakt met de AP, kan gebruik maken van **Extensible Authetication Protocol**.

Om een **Access Point** zijn firmware te updaten of instellingen te wijzigen, altijd een directe **kabelverbinding** gebruiken!

# Chapter eight: Basic Security

**Information theft**: Vertrouwelijke informatie stelen  
**Identity theft**: Informatie stelen om een identiteit te stelen om legale toegang to krijgen tot documenten, credit kaarten, ...  
**Data loss/manipulation**: virus  
**Disruption of service**: deny services, DoS

## Network threats

* **External**: van buiten de organisatie uit, geen machtiging
* **Internal**: door gebruik van user accounts of fysieke toegang tot een netwerk
* **Social engineering**: Human is weakest link in security, gebruiker misleiden om zo informatie te bemachtigen
* **Pretexting**: Uitgevonden scenario om de gebruiker te overtuigen van de geloofwaardigheid, zoals social security number, gebeurt meestal via de telefoon
* **Phishing**: Zich voordoen als legitiem buiten de organisatie, zoals een bank. Gebruikt een website die heel erg lijkt op de echte website, gebeurd meestal via e-mail: “Klik op de linkom financiele data records na te kijken”
* **Vishing**: Phone vishing. Use **Voice over IP**. Voice message voor het controleren van bank records over telefoon (bankrek., pin,...)

## Methods of Attack

* **Virus**: Voert en breidt zichzelf uit door het aanpassen van andere programmas of bestanden, moet geactiveerd worden, vermenigvuldigd en verspreid zich na activatie
* **Worm**: Gelijk een virus, maar moet zich niet hechten aan een programma en heeft geen activatie nodig. Gebruik netwerk en software zwakheden. Vermenigvuldigd en verspreid zich om de omgeving te infecteren
* **Trojan horse**: Vermenigd zichzelf niet, lijkt op een legitiem programma maar doet onverwachte dingen zoals achterdeurtjes maken.
* **DoS (Denial-of-Service)**:
  + Een systeem overvloeden of netwerk
    - geen netwerk communicatie mogelijk
    - SYN-flood
  + Verbinding verbreken tussen client en server om toegang te voorkomen
    - ping of death
* **DDoS (Distributed Denial of Service)**:
  + Meer ingewikkeld, beschadigend
  + Grotere schaal
  + Master en veel slaves
* **Brute-Force Attack**
  + Een paswoord proberen te kraken, code, door alle mogelijkheden af te gaan
  + Genereert veel netwerk verkeer en zet user accounts vast
* **Spyware**: Verzameld informatie zonder toestemming (account informatie, paswoorden,...), moeilijk te verwijderen
  + Tracking cookies:
    - Soort spyware, niet altijd slecht
    - Houdt het internet gebruik in de gaten (interactieve sites)
  + Adware:
    - Soort van spyware voor gerichte advertenties
  + Pop-ups, Pop-unders:
    - Extra advertentie vensters

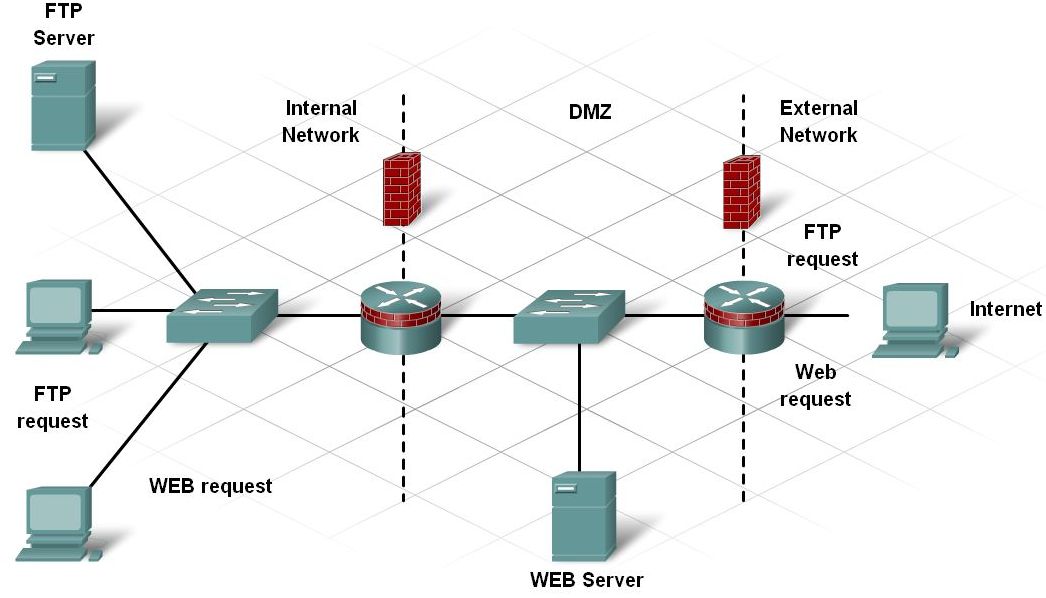
## Security procedures and applications

* **Patch**: Klein stukje code die bugs herstelt of software kwetsbaarheid
* **Update**: Bevat extra functionaliteit
* **Anti-virus software**
  + **Preventative and reactive tool**
  + **Features**: e-mail checking, geregeld scannen, automatische updates
  + Doet beroep op kennis van het virus om het te verwijderen
* **Spam prevention**
* **Spam mill**: Host geïnfecteerd met virus of trojan, en stuurt spam mails zonder het te weten
* **Most common typ of spam forwarded = virus warnings**: normaal hoax (kettingbrief)
* **Anti-spyware**
* **Firewall:**
  + Controlleert verkeer naar en van een netwerk
  + Meest effectief om het netwerk gebruikers te beschermen van externe gevaren
  + Technieken:
    - Packet filtering: IP-MAC address gebasseerd
    - Applicatie/website filtering: gebasseerd op URL
    - Stateful Packet Inspection (SPI):
      * Binnenkomende pakketten moeten een legitieme respons zijn
  + Gebruiken meestal ook **Network Adress Translation**

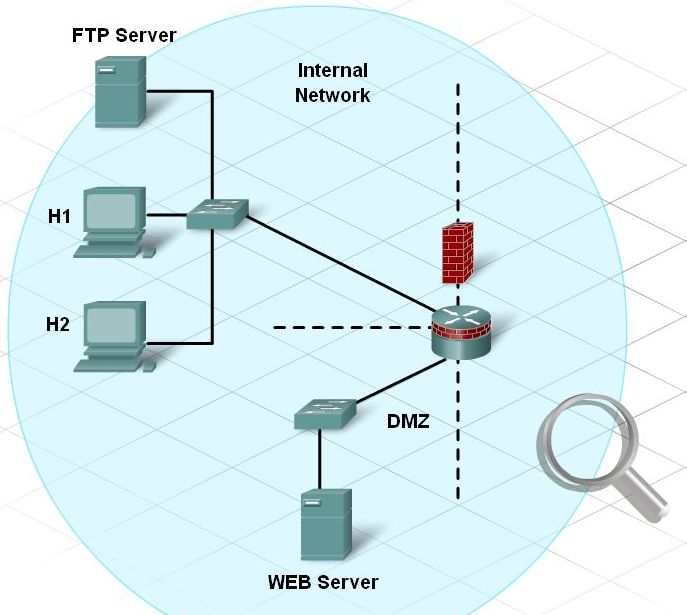
Vier soorten **firewalls**:

1. **Appliance-based firewall**: Beste firewall oplossing om netwerk te beveiligen, heel snel en duur
2. **Server-based firewall**: Firewall draaiende op server, draait op **NOS**(**Network Operating System**) minder beveiligddoor algemene beveiliging zwakheden
3. **Integrated firewall**: Geïmplementeerd door router
4. **Personal firewall**: Gebruikt op computers, meer dan 1 kan voor conflicten zorgen 🡪 zone alarm

**Demilitarized Zone (DMZ)**: Gebied dat toegankelijk is voor interne en externe gebruikers. Meer beveiligd dan extern netwerk, minder dan intern. Single of Double firewall configurations om de DMZ, het intern en extern netwerk te scheiden.



Two-firewall DMZ



One-firewall DMZ

# Chapter nine: Troubleshooting your network

Gegevens verzamelen: alle stappen neerschrijven, of in een ergens opslaan, tijdens het troubleshooten, ook de mislukte pogingen.

**Top-down**: Start met laag 7 (**OSI-model, applicatie**) en naar beneden werken, goed als bepaalde netwerk applicaties niet werken en andere wel

**Bottom-up**: Start met laag 1 (**OSI-model, fysiek**) en naar boven werken, goed voor complexe problemen, heel goede methode om mee te starten

**Divide-and-conquer**: Begin waar je denkt dat het probleem zit, test en werk zo naar boven of beneden. Goed als het probleem specifieke kenmerken heeft en de troubleshooter er hervaring mee heeft

**Trial-and-error**: De troubleshooter neemt een doordachte gok om een oplossing te zoekenn en probeerd deze toe te passen, werkt deze niet, gebruikt hij deze informatie om verder te gaan

**Substitution**: Het probleem wordt verondersteld te liggen bij hardware en deze wordt vervangen en gekeken of dit werkt.

In een netwerk waar draadloos internet is en gewoon internet is het best om **Divide and conduer** te vinden of het probleem op het draad of draadloos netwerk zit.

p209 in uwe boek