Computernetwerken

# Globaal verbonden (ENKEL LEZEN)

## Middelen aanbieden in een netwerk

### Netwerken van vele formaten

* **Klein thuisnetwerk,** Enkele toestellen met elkaar en met het Internet verbonden.
* **Klein kantoornetwerk,** Computers van thuis of van een extern kantoor verbinden met het bedrijfsnetwerk.
* **Middelgrote tot grote netwerken,** Vele locaties met honderden tot duizenden onderling verbonden computers.
* **Wereldwijde netwerken,** Miljoenen computers verbinden over de hele wereld (VB: Internet).

### Clients en Servers

Elke computer verbonden met een netwerk = host of eindapparaat.

* **Servers** zijn computers die informatie aanbieden aan eindgebruikerstoestellen op het netwerk. Bv: e-mail servers, web servers, …
* **Clients** zijn computers die informatie opvragen aan de servers zoals een webpagina van een web server, een e-mail van een e-mail server, …

### Peer-to-peer

Wanneer een client ook als server functioneert noemen we het netwerk een **peer-to-peer netwerk**.

**Voordelen:**

* Eenvoudig op te zetten
* Minder complex
* Goedkoper

**Nadelen:**

* Geen centrale administratie
* Niet zo veilig
* Nauwelijks tot niet schaalbaar
* Trage prestaties

## LANs, WANs, en het Internet

### Netwerkcomponenten

#### Overzicht

Een netwerkinfrastructuur omvat drie brede categorieën van netwerkcomponenten:

* **Toestellen**
* **Media**
* **Diensten**

#### Eindapparaten

Een **eindapparaat** is waar een bericht vandaan komt of waar het is ontvangen.

Gegevens zijn afkomstig van een eindapparaat, stromen door het netwerk en komen toe bij een eindapparaat.

#### Intermediaire netwerktoestellen

**Intermediair toestel** verbindt eindapparaten met elkaar in een netwerk.

Voorbeelden: switches, routers, firewalls, wireless accesspoints, …

Het beheer van de gegevens in een netwerk door Intermediaire toestellen:

* Regeneratie en opnieuw verzenden van datasignalen.
* Informatie bijhouden van de verschillende paden die bestaan in een netwerk of internetwerk (paden die de data volgen van afzender tot ontvanger).
* Andere apparaten op de hoogte brengen van fouten en communicatiestoornissen.

#### Netwerkmedia

Dit zijn de verschillende middelen die gebruikt worden om media van verzender naar ontvanger te brengen.

* **Metalen geleiders in kabels**, zoals koperkabels.
* **Glas**, zoals in glasvezelkabels.
* **Draadloze transmissie**.

#### Netwerkvoorstellingen



#### Topologiediagrammen

**Fysieke topologie:**

* Geeft de fysieke locatie weer van de apparaten.
* Identificeert de manier waarop eindegebruikerstoestellen, en netwerkapparaten zoals routers, switchen en draadloze toegangspunten verbonden zijn.

**Logische topologie:**

* Geeft de naamgeving van de poorten en netwerkadressering weer.
* Verwijst naar de manier waarop een frame wordt verstuurd van de ene node naar de andere, deze logische signaalpaden worden gedefinieerd door datalinklaag protocollen.

### LANs en WANs

#### Netwerktypes

De meest voorkomende netwerktypes zijn:

* **LAN (Local Area Network)**, omvat een klein geografisch gebied, eigendom van of beheerd door een individu of IT-afdeling.
* **WAN ( Wide Area Network)**, omvat een groot geografisch gebied, doorgaans aangeboden door een serviceprovider.

Andere netwerktypes zijn:

* **MAN (Metropolitan Area Network)**, is een netwerk dat alle stedelijke diensten met elkaar verbindt.
* **WLAN (Wireless LAN)**, een LAN maar draadloos.
* **SAN (Storage Area Network)**, netwerk voor gezamelijke opslag van gegevens.

### Het Internet, Intranets en Extranets

#### Het Internet

**Het internet** is een verzameling van onderling verbonden LANs en WANs.

* LANs worden door WANs met elkaar verbonden
* WANs worden met elkaar verbonden door glasvezelkabels, koperkabels of draadloze verbindingen.
* Het internet is geen eigendom van één bepaald individu of bepaalde groep. De volgende groepen werden opgericht om te waken over de structuur van het internet:
* IETF
* ICANN
* IAB

#### Intranets en Extranets

* **Intranet** is een private verzameling van LANs en WANs binnenin een organisatie dat enkel toegankelijk is voor de leden van de organisatie of anderen met de juiste machtigingen.
* **Extranet** wordt gebruikt om veilige toegang te verlenen tot hun netwerk aan mensen die voor een andere organisatie werken en die de gegevens en/of het netwerk moeten kunnen aanspreken.

### Internetverbindingen

#### Internetverbindingen voor thuis of klein kantoor

* **Kabel**, altijd actieve internetverbinding met hoge bandbreedte, aangeboden door kabeltelevisie operatoren.
* **DSL (broadband digital subscriber line)**, altijd actieve verbinding met hoge bandbreedte aangeboden door telefonie operator.
* **Mobiel**, gebruikt een mobiel telefoon netwerk om verbinding te maken met het internet, enkel beschikbaar op plaatsen waar er een mobiel netwerk aanwezig is.
* **Satelliet,** groot voordeel in afgelegen gebieden zonder internetproviders.
* **Inbelverbinding**, vereist een modem en is duur en heeft een lage bandbreedte.

## Het netwerk als een platform

### Convergerende netwerken

#### Traditionele gescheiden netwerken

Een voorbeeld van meerdere afzonderlijke netwerken kan een school van 30 jaar geleden zijn. Sommige leslokalen waren bekabeld voor datanetwerken en afzonderlijk voor telefonie en televisie.

* Elk van deze netwerken gebruikte een andere technologie om de signalen voor communicatie via een verschillende set van regels en standaarden te verzorgen.

#### Het convergerende netwerk

Deze kunnen meerdere types communicatie zoals data, gesprekken en video rondsturen.

* In tegenstelling tot vast toegewezen netwerken kunnen ze dit allemaal rondsturen naar verschillende types apparaten over dezelfde netwerkinfrastructuur.
* Netwerkinfrastructuur gebruikt eenzelfde set aan regels en standaarden.

### Betrouwbaar netwerk

#### Netwerkarchitectuur

Dit verwijst naar de technologieën die de infrastructuur ondersteunen bij het versturen van data doorheen het netwerk.

**Vier basiskenmerken** waaraan zo’n architectuur moet voldoen om de gebruikers tegemoet te komen:

1. Fouttolerantie
2. Schaalbaarheid
3. Quality of Service (QoS)
4. Veiligheid

**Fouttolerantie**

* Fouttolerant netwerk beperkt de impact van een storing door het aantal getroffen apparaten te beperken. Hiervoor zijn meerdere paden nodig.
* Biedt redundantie d.m.v. een pakket geschakeld netwerk, dit netwerk splitst datastromen in pakketten die over een netwerk gerouteerd worden. Theoretisch kan elk pakket een ander pad naar de bestemming nemen.
* Niet mogelijk bij circuit geschakelde netwerken waarbij het circuit van tevoren vast ligt.

**Schaalbaarheid**

* Schaalbaar netwerk kan snel en eenvoudig uitgebreid worden zonder de prestaties voor huidige gebruikers en diensten te beperken.
* Netwerkingenieurs volgen afgesproken standaarden en protocollen om een netwerk schaalbaar te maken.

**Quality of Service**

* Dit is het primaire mechanisme om ervoor te zorgen dat inhoud betrouwbaar aan alle gebruikers wordt geleverd.
* Met een QoS-beleid kan de router de stroom van gegevens en spraakverkeer eenvoudiger beheren.

**Veiligheid**

Er zijn **twee hoofdtypes** van netwerkbeveiliging die aangepakt moeten worden:

1. **Beveiliging van netwerkinfrastructuur**

* Fysieke beveiliging van netwerkapparaten
* Ongeautoriseerde toegang tot de beheersoftware op die apparaten voorkomen

1. **Informatiebeveiliging**

* Beveiliging van de informatie of data die via het netwerk worden verzonden.

Er zijn **3 doelen** van netwerkbeveiliging:

1. **Vertrouwelijkheid**, alleen bedoelde ontvangers kunnen de gegevens lezen.
2. **Integriteit**, garantie dat de gegevens tijdens de verzending niet zijn gewijzigd.
3. **Beschikbaarheid**, zekerheid van tijdige en betrouwbare toegang tot gegevens voor geautoriseerde gebruikers.

## Het netwerk in verandering

### Netwerk trends

#### Nieuwe trends

Elke trend heeft impact op organisaties en consumenten, om dit bij te benen moet de rol van het netwerk voortdurend aangepast worden.

#### Bring your own device

Gebruikers kunnen hun eigen apparaten gebruiken met meer mogelijkheden en flexibiliteit. Dit biedt hen de vrijheid om persoonlijke tools te gebruiken voor toegang tot informatie en communicatie via persoonlijke:

* Laptops
* Smartphones
* …

#### Online samenwerking

Individuen willen samenwerken met anderen via het netwerk bij gezamenlijke projecten. Samenwerkingshulpmiddelen bieden gebruikers een manier om direct te verbinden, te communiceren en hun doelen te bereiken.

Samenwerking krijgt een hogere prioriteit in bedrijven en het onderwijs.

#### Videocommunicatie

Over de hele wereld transformeren we organisaties door onze klantenervaringen te transformen.

#### Cloud computing

* Hiermee kunnen we persoonlijke bestanden kunnen opslaan of een back-up kunnen maken van onze gegevens op servers via het Internet.
* Toepassingen zoals werkverwerking en fotobewerking zijn ook toegankelijk via de Cloud.
* Cloud computing stelt bedrijven ook in staat om hun mogelijkheden op vraag uit te breiden en automatisch aan te bieden aan elk apparaat waar ook ter wereld.
* Cloud computing wordt mogelijk gemaakt door datacenters. Kleinere bedrijven die geen budget hebben voor een eigen datacenter, huren servers en opslagruimte in de Cloud.

Er zijn **4 types** cloud computing:

1. **Publieke clouds**, beschikbaar voor het grote publiek op basis van een betaalmodel volgens gebruik of gratis.
2. **Private clouds**, bedoeld voor een specifieke organisatie of entiteit zoals de overheid.
3. **Hybride clouds**, Bestaat uit twee of meer types. Elk onderdeel blijft afzonderlijk bestaan maar zijn verbonden door een gemeenschappelijke architectuur.
4. **Aangepaste clouds**

#### Powerline netwerken

Deze maken het mogelijk om toestellen te verbinden met een LAN waar datakabels of draadloze communicatie geen haalbare optie is.

Een powerline verzend de gegevens op bepaalde frequenties over de elektriciteitskabels.

#### Draadloze breedband

* Vaker te vinden in afgelegen gebieden, is een WISP (Wireless Internet Service Provider) een ISP die abonnees verbindt met toegewezen toegangspunten of hotspots.
* Andere oplossing voor huizen en kleine bedrijven.
* Maakt gebruik van dezelfde mobiele technologie als smartphones.

### Netwerkbeveiliging

#### Bedreigingen

Bedreigingen kunnen afkomstig zijn van zowel buiten als binnen het netwerk.

**Externe bedreigingen:**

* Virussen, wormen, trojaanse paarden
* Spyware en adware
* Zero-day aanvallen (zero-hour aanvallen)
* Hackeraanvallen
* Denial of Service aanvallen
* Onderscheppen en diefstal van gegevens
* Identiteitsdiefstal

**Interne bedreigingen:**

* BYOD strategieën maken bedrijfsgegevens kwetsbaarder.

#### Oplossingen

* Beveiliging in meerdere lagen implementeren m.b.v. meer dab één oplossing.
* Netwerkbeveiligingscomponenten voor thuis- of klein kantoornetwerk:
* **Antivirus en antispyware software**.
* **Firewallfiltering** om ongeautoriseerde toegang tot het netwerk te blokkeren.
* Aanvullende beveiligingsvereisten:
* **Dedicated firewalls.**
* **Access control lists (ACL),** gebruikt om toegang en doorsturen van gegevens verder te filteren.
* **Intrusion prevention systems (IPS)**, gebruikt om snel verspreidende dreigingen te identificeren (bv een zero-day aanval)
* **Virtual private networks (VPN)**, gebruikt om veilige toegang voor externe werknemers aan te bieden

# Configuratie van een Network Operating System

## IOS-bootcamp

### Besturingssysteem

* PC’s en laptops = Windows, MacOS en Linux
* Smartphones en tablets = Apple iOS en Android
* Cisco IOS voor netwerkapparatuur

Een besturingssysteem bestaat uit 3 delen :

* **OS Shell,** kan een Command-line interface (CLI) of een grafische user interface (GUI) zijn.
* **OS Kernel,** Communiceert rechtstreeks met de hardware en bepaalt hoe de hardware is gebruikt om aan de software requirements te voldoen.
* **Hardware,** het fysieke deel van een computer.

### Cisco IOS Toegang

#### Toegangsmethoden

* **Consolepoort**, dit is een aparte seriële poort voornamelijk gebruikt voor de initiële config v/h apparaat. Een Consolekabel is nodig om met deze poort te verbinden. Communicatie gebeurt buiten het datanetwerk om (out-of-band). Het netwerk hoeft hiervoor dus nog niet te werken.
* **Secure Shell (SSH)**, is een methode om vanop afstand een veilige CLI-sessie op te zetten, via het (data)netwerk. Alle data zoals wachtwoorden, commando’s, … worden geëncrypteerd over het netwerk verzonden. Minstens één netwerkinterface, al dien niet virtueel, moet hiervoor geconfigureerd zijn.
* **Telnet**, dit is zoals SSH maar wachtwoorden en commando’s worden als platte tekst over het netwerk verzonden.

**SSH boven Telnet verkiezen! Veel veiliger.**

* **AUX-poort**, dit is een oudere methode om op afstand een CLI-sessie tot stand te brengen, via een telefonische inbelverbinding met behulp van een modem.

### Navigatie in IOS

#### Primaire modes

* **User EXEC mode (>)** = “view-only”-mode, enkel toegang tot basis monitoringscommando’s. Standaard is er hier geen authenticatie vereist, aan te raden is om hier een wachtwoord op te zetten.
* **Privileged EXEC mode (#)** = “enable”-mode, hier geraak je m.b.v. het “**enable”-commando,** hier kan men configuratie- en managementcommando’s uitvoeren. Ook hier standaard geen authenticatie vereist, maar hier moet je wel degelijk een wachtwoord op zetten!

#### Configuratiemodes

De primaire config-mode is de **global config**.

* Gebruikt **« configure terminal »** **commando**.
* Wat er hier gewijzigt wordt heeft invloed op de werking v/h apparaat in zijn geheel.

Specifieke subconfiguratiemodes zijn toegankelijk vanuit de globale configuratiemode. Elke submode zorgt voor de configuratie van een bepaald onderdeel of functie van het IOS-apparaat.

Vb:

* **Interfacemode** – om één van de netwerkinterfaces te configureren.
* **Linemode** – om de console, AUX, Telnet of SSH-toegang te configureren.

#### Commando’s voor de IOS-modes

* **enable** – ga van user EXEC mode naar privileged EXEC mode.
* **configure terminal** – ga van privileged EXEC mode naar de globale configuratiemode.
* **interface** *nic* – ga van de globale configuratiemode naar de specifieke subconfiguratiemode voor het configureren van netwerkinterface *nic*, met *nic* = FastEthernet0/4, f0/4, GigabitEthernet1/2, g1/2, …
* **line [console|vty]** *number*– ga van de globale configuratiemode naar de specifieke subconfiguratiemode voor de configuratie van console, SSH, telnet of AUX.
* **exit** – keer terug naar de vorige, meer algemene mode, bvb. van de specifieke subconfiguratiemode van een interface naar de globale configuratiemode.
* **end** – keer terug van eender welke configuratiemode naar privileged EXEC mode.
* **^z (ctrl-z)** – idem als **“end”**.
* **disable** – ga terug van privileged EXEC mode naar user EXEC mode.

### Het Commandostructuur

## Basisconfiguratie IOS

### Hostnamen

#### Hostnaam

De eerste stap bij het configureren van een switch is altijd het toekennen van een unieke hostnaam. Deze naam verschijnt in CLI prompts, kan gebruikt worden in verschillende authenticatieprocessen tussen apparaten, en moet gebruikt worden op topologiediagrammen.

Zonder een hostnaam zijn netwerkapparaten moeilijk te identificeren.

Beperkingen bij het kiezen van een hostnaam:

* Max 63 tekens
* Enkel letters, cijfers en het koppelteken
* Eerste teken moet een letter zijn
* Laatste teken mag geen koppelteken zijn
* Hostnamen zijn niet hoofdlettergevoelig

#### Hostnamen configureren

* Altijd een goede, consistente **naamgevingsconventie** gebruiken binnen het bedrijf. Dit zorgt ervoor dat het veel gemakkelijker is voor de systeembeheerder om apparaten te identificeren binnen een netwerk.
* Het commando voor een hostnaam toe te wijzen is: “***hostname*** *naam*” in de globale configuratiemode.

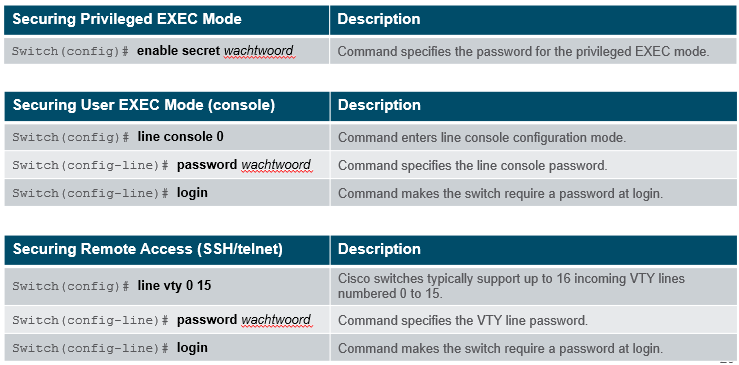
### Toegang beperken

#### Toegang tot apparatuur beperken

1. Beperk de **fysieke toegang** tot de netwerkapparaten door ze afgesloten te houden in vergrendelde rekken of zelf een vergrendelde kamer.
2. Beveilig de netwerkapparatuur met **wachtwoorden.**

* Beveilig de privileged en user EXEC modes en de toegang via SSH/telnet met een wachtwoord.
* Gebruik **veilige** wachtwoorden:
* 8+ tekens
* Combinatie van hoofdletters, kleine letters, cijfers en speciale tekens.
* Gebruik geen veelvoorkomende woorden.
* Gebruik niet voor alle apparaten hetzelfde wachtwoord.
* Encrypteer alle wachtwoorden.
* Toon juridische kennisgeving (legal notifcation) bij het inloggen.

#### Wachtwoorden instellen



#### Wachtwoorden encrypteren

De configbestanden **startup-config** en **running-config** bevatten de meeste wachtwoorden in platte tekst. Dit is onveilig aangezien iedereen in deze bestanden kan en zo de wachtwoorden kan zien.

Om dit op te lossen gebruik je **service password-encryption** (in globale configuratiemode) om op deze manier alle wachtwoorden te encrypteren. Dit is echter een zwakke encryptie maar voorkomt meelezen over de schouder (shoulder surfing).

#### Banner-boodschap

Dit zijn berichten die worden weergegeven wanneer iemand toegang probeert te krijgen tot een apparaat. Deze zijn een belangrijk onderdeel van het juridische proces in het geval dat iemand wordt vervolgd voor het inbreken in een apparaat.

Het commando hiervoor is:

**banner motd** *scheidingsteken bericht scheidingsteken*

## IP-adressen configureren

### Poorten en adressen

#### Overzicht IP-adressering

Elk eindapparaat op een netwerk vereist een IP-configuratie bestaande uit:

* IP address
* Subnet mask
* Default gateway

IPv4-adressen worden voorgesteld in een “dotted decimal format”, bestaande uit:

* 4 decimale getallen, 0 tot 255
* Gescheiden door punten (dots)

### Interfaces en poorten

* Cisco IOS laag 2 switches hebben fysieke poorten om toestellen te kunnen aansluiten. Deze poorten ondersteunen echter geen laag 3 IP-adressen.
* Om vanop afstand te kunnen verbinden met een laag 2 switch (en hem dus vanop afstand te kunnen beheren), moeten we één of meer **switch virtual interfaces (SVIs)** configureren.
* Elke switch heeft een default VLAN 1 SVI.

**Merk op**: Een laag 2 switch heeft geen IP-adres nodig om correct te werken. Het SVI IP-adres is enkel nodig als je de switch vanop afstand wilt kunnen beheren via SSH.

#### Switch Virtual Interface

Om een switch vanop afstand te kunnen beheren, moet hij een IP-adres hebben. Een switch heeft echter geen fysieke Ethernetinterface die geconfigureerd kan worden. In plaats daarvan moet u de VLAN 1 **switch virtual interface (SVI)** configureren.

De VLAN-1-SVI moet als volgt geconfigureerd worden:

* **IP-adres** – zorgt voor een unieke identificatie van de switch op het netwerk
* **Subnetmask** – identificeert het netwerk- en hostgedeelte in het IP-adres
* **interface activeren** – dit gebeurt met het commando **no shutdown**.

Switch>enable

Switch#configure terminal

Switch(config)#**interface vlan 1**

Switch(config-if)#**ip address** 192.168.1.5 255.255.255.0

Switch(config-if)#**no shutdown**

Switch(config-if)#end

Switch#**show ip interface brief**

Interface IP-Address OK? Method Status Protocol

...

Vlan1 192.168.1.5 YES manual **up** up

Switch#

# Netwerkprotocollen en -communicatie

## Communicatieregels

### De regels

#### Basisprincipes van communicatie

Alle vormen van communicatie hebben drie gemeenschappelijke elementen:

* **Zender**
* **Ontvanger**
* **Medium/kanaal**

**Regels of protocollen** regelen alle vormen van communicatie

#### Vastleggen van regels

Protocollen zijn nodig voor effectieve communicatie en omvatten:

* Een geïdentificeerde zender en ontvanger
* Gemeenschappelijke taal en grammatica
* Snelheid en timing van aflevering
* Bevestiging van ontvangst (acknowledgement)

Netwerkprotocollen definiëren:

* Message encoding (codering)
* Message format and encapsulation  
  (opmaak en inkapseling)
* Message size (grootte)
* Message timing
* Message delivery options (afleveringsopties)

#### Message encoding

* De codering moet in het juiste formaat voor het medium zijn.
* De zender converteert het bericht eerst in bits.
* Elke bit wordt gecodeerd in geluid, licht of elektrische pulsen, afhankelijk van het gebruikte kanaal/medium.
* De ontvanger ontvangt en decodeert de signalen om het bericht te interpreteren.

#### Message formatting en Encapsulation (opmaak en inkapseling)

* Een brief en een adres hebben een overeengekomen **formaat**. Dit is nodig voor een goede bezorging.
* We steken de brief in een enveloppe. Dit noemen we inkapseling (encapsulation).
* Elk computerbericht wordt geëncapsuleerd in een **frame**, voordat het wordt verzonden over het netwerk.
* Een frame is als een enveloppe met een adres en een afzender.

#### Message Size

Lange berichten worden in kleinere delen of zinnen opgesplitst.

* Elk stuk wordt in een apart frame verzonden.
* Elke frame heeft eigen adresseringsinformatie.
* Ontvangende computer zal het oorspronkelijke bericht reconstrueren uit verschillende frames.

#### Message timing

**Access Method**

Hosts op een netwerk moeten weten wanneer ze mogen starten met het verzenden van berichten en hoe ze moeten reageren op collisions (botsingen).

**Flow Control**

Zender en ontvanger gebruiken flow control om te onderhandelen over de juiste timing zodat de ontvanger niet overspoeld wordt en de berichten zeker ontvangen worden.

**Response Time-out**

Hosts op het netwerk hebben regels die bepalen hoe lang er op reacties moet worden gewacht en welke actie er moet worden ondernomen als er een time-out optreedt.

#### Message Delivery Options

**Unicast Message**

One-to-one

**Multicast Message**

One-to-many

**Broadcast Message**

One-to-all

## Netwerkprotocollen en standaarden

### Protocollen

#### Regels voor communicatie

Protocollen worden geïmplementeerd door hosts en netwerkapparaten in software, hardware of beide.

Een protocol behoort tot een layer, elke service of protocol op een hoger niveau is afhankelijk van de functionaliteit die wordt gedefinieerd in de lagere niveaus.

#### Netwerkprotocollen

Deze definiëren een gemeenschappelijk formaat voor het uitwisselen van berichten tussen apparaten.

Veel voorkomende netwerkprotocollen zijn:

* **HTTP (Hypertext transfer protocol)**
* **TCP (Transmission Control Protocol)**
* **IP (Internet Protocol)**

#### Interactie van protocollen

**HTTP,** Een applicatieprotocol dat de interactie tussen een webserver en een webcliënt regelt.

**TCP**, Transportprotocol dat de individuele gesprekken beheert.

**IP**, Encapsuleert de TCP-segmenten, wijst adressen toe en zorgt voor de aflevering.

**Ethernet,** zorgt voor de communicatie via een datalink en de fysieke overdracht van gegevens op de netwerkmedia.

### Protocol-suites

#### Protocol-suites en Industry Standards

Een **Protocol-suite** is een reeks protocollen die samenwerken om communicatie over een computernetwerk te realiseren.

**De TCP/IP-protocol-suite** is een open standaard, de protocollen zijn vrij beschikbaar en elke fabrikant kan deze protocollen op zijn hardware of in zijn software implementeren.

#### Ontwikkeling van TCP/IP

APRANET (Advanced Research Projects Agency Netwerk) was de voorloper van het huidige internet en werd gefinancierd door het Amerikaanse Ministerie van Defensie en werd gebruikt door uniefs en onderzoekslabo’s.

#### TCP/IP Communicatieproces

De encapsulatie bij **verzenden** van gegevens van webserver naar client verloopt als volgt:

1. Webserver levert HTML-pagina aan, HTTP application layer stuurt de gegevens naar de transport layer.
2. Transport layer verdeelt gegevens in segmenten en geeft deze elk een volgnummer (identificatie).
3. IP-adres van zender en ontvanger worden toegevoegd. Resultaat = IP-pakket
4. Ethernet-informatie wordt toegevoegd = Ethernet-frame of datalink-frame
5. Frame wordt afgeleverd bij dichtstbijzijnde router richting webclient. Elke router voegt nieuwe datalink-informatie toe bij het doorsturen van het pakket.

Encapsulatie bij **ontvangen** van datalink-frames van de webserver verwijdert de client de protocolheaders in omgekeerde volgorde:

1. Ethernet-header wordt verwijderd
2. Ip-header wordt verwijderd
3. Transport-layer-header wordt verwijderd
4. HTTP informatie wordt verwerkt en doorgestuurd naar webbrowser

### Standard Organizations

#### Open Standards

Deze bevorderen interoperabiliteit, concurrentie en innovatie.

Organisaties voor standaarden zijn meestal non-profit die onafhankelijk zijn van een producent. En zijn opgericht om het concept van open standaarden te ontwikkelen en te promoten.

#### Internet Standards

|  |  |
| --- | --- |
| **Internet Engineering Task Force (IETF)** | ontwikkelt, updatet en onderhoudt Internet- en TCP/IP-technologieën. |

#### Electronics and Communications Standard Organizations

|  |  |
| --- | --- |
| **Institute of Electrical and Electronics Engineers** (**IEEE**) | stimuleert technologische innovatie en creëert standaarden voor elektronica en elektriciteit, dus ook voor netwerkapparatuur. |

### Referentiemodellen

#### De voordelen van een gelaagd model

* Het helpt bij ontwerpen van protocollen omdat functies uit verschillende lagen gescheiden zijn.
* Bevordert concurrentie omdat producten van verschillende producenten kunnen samenwerken.
* Technologische veranderingen in de ene laag hebben geen invloed op de andere lagen.
* Het biedt een taal om netwerkfuncties te beschrijven.

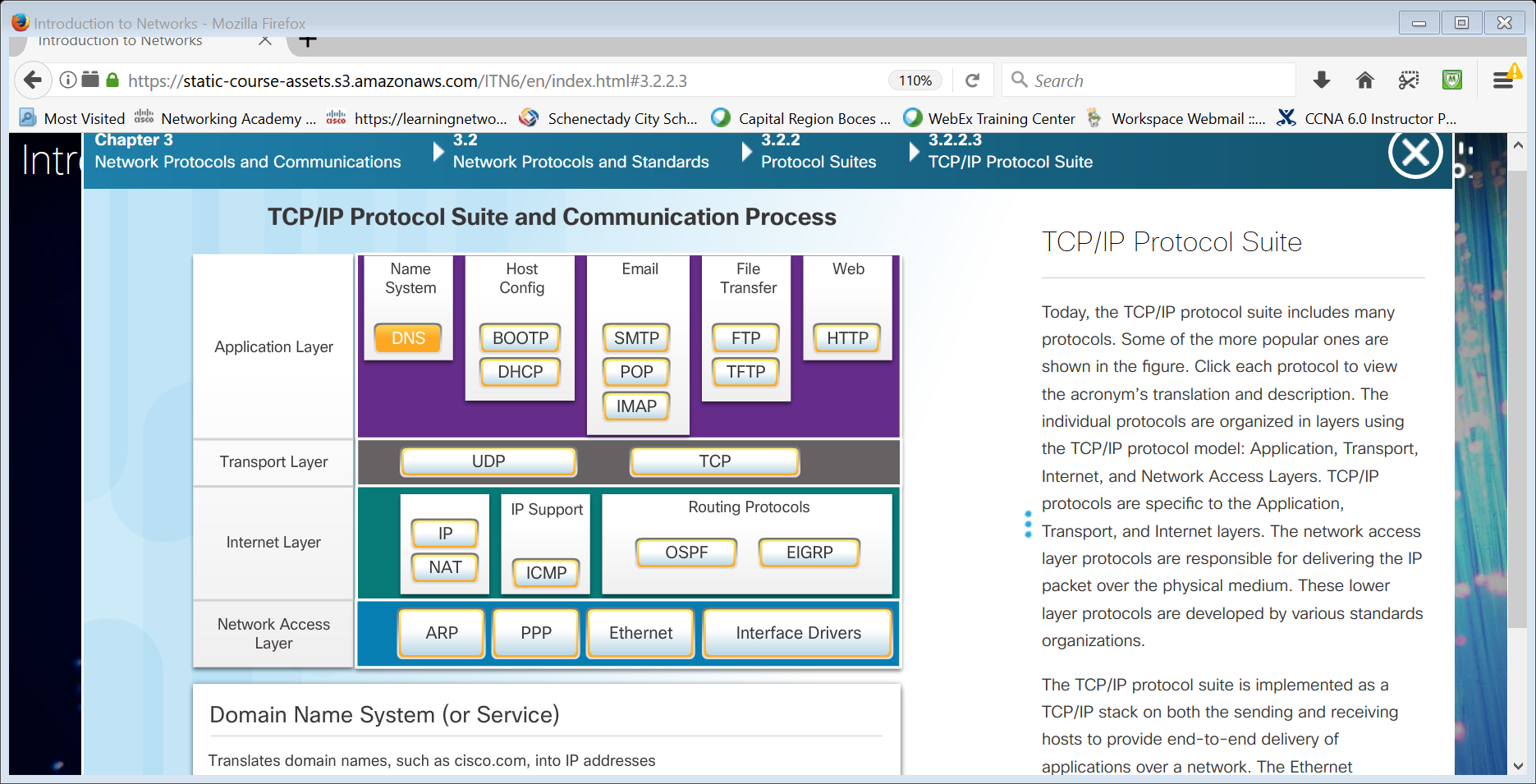
#### OSI-model

|  |  |
| --- | --- |
| **Application** | Bevat protocollen voor interproces communicatie |
| **Presentation** | Zorgt voor eenvormige representatie van data |
| **Session** | Biedt services aan aan de presentation-layer om de dialoog en de uitwisseling van data te organiseren |
| **Transport** | Definieert de services om data te segmenteren, te transfereren en te re-assembleren |
| **Network** | Biedt services aan voor uitwisseling van individuele data-pakketten tussen 2 en-devices |
| **Data Link** | Zorgt voor uitwisseling van data-frames tussen 2 devices binnen hetzelfde netwerk |
| **Physical** | Beschrijft de fysische wijze waarop bits verzonden worden over het kanaal (koper, glasvezel, radiogolven, …) |

#### TCP/IP-protocol-model

|  |  |
| --- | --- |
| **Application** | Toont de data aan de gebruiker, doet de encoding en beheerd het dialoog |
| **Transport** | Zorgt voor de communicatie tussen verschillende apparaten doorheen meerdere netwerken |
| **Internet** | Bepaald het beste pad doorheen het netwerk |
| **Network Access** | Beheerd de hardware apparaten en media dat het netwerk vormen |

##### TCP/IP Protocol-suite



**Application Layer:**

Zie tabel H10

**Transport Layer:**

* **UDP,** User Datagram Protocol
* **TCP,** Transmission Control Protocol

**Internet Layer:**

* **IP,** Internet Protocol
* **NAT,** Network Adress Translation

**IP Support**

**ICMP,**  Internet Control Message Protocol

**Routing protocols:**

**OSPF**

**EIGRP**

**Network Access Layer:**

* **ARP**, Address Resolution Protocol
* **PPP,**  Point-to-Point Protocol
* **Ethernet**
* **Interface Drivers**

#### Vergelijking OSI-model en TCP/IP-model

|  |  |
| --- | --- |
| **Application** | **Application** |
| **Presentation** |
| **Session** |
| **Transport** | **Transport** |
| **Network** | **Internet** |
| **Data Link** | **Network Access** |
| **Physical** |

## Data-transfer in het netwerk

### Data Encapsulation

#### Message Segmentation

* Grote hoeveelheden data worden opgedeeld in kleinere delen. Elk deel wordt apart gelabeld.
* Dankzij het opsplitsen in kleinere delen kunnen meerdere datastromen tegelijk over het netwerk gestuurd worden = **multiplexing.**
* Als een deel verloren gaat moet enkel dat specifiek deel opnieuw verzonden worden

#### Protocol Data Units (PDUs)

Wanneer application-data wordt doorgegeven in de protocolstack, wordt er op elk niveau info toegevoegd = **encapsulatie-proces.**

De vorm die de data aanneemt op elke laag = **Protocol Data Unit (PDU)**

|  |  |
| --- | --- |
| Data | **Application layer PDU** |
| Segment | **Transport layer PDU** |
| Packet | **Network Layer PDU** |
| Frame | **Data Link Layer PDU** |
| Bits | **Physical Layer PDU** |

#### Encapsulatie

Dit proces doorloopt de protocol-stack van boven naar onder:

1. Data wordt gesplitst en geëncapsuleerd in TCP-segmenten
2. TCP-segment wordt geëncapsuleerd in IP-pakket
3. IP-Pakket wordt geëncapsuleerd in Ethernet-frame

#### De-encapsulatie

Dit proces doorloopt de protocol-stack van onder naar boven. Dit is het verwijderen van één of meerdere protocol-headers door een ontvanger (receiving device).

Data wordt steeds verder ge-de-encapsuleerd tot het niveau van de end-user applicatie.

### Data Access

#### Network Addresses

Network-layer-source- en -destination-adres is verantwoordelijk voor het afleveren van het IP-pakket van de originele source tot de finale destination.

#### Data Link Addresses

De bedoeling hiervan is om data af te leveren van een netwerkinterface naar een andere netwerkinterface **binnen hetzelfde netwerk**.

Telkens een router een IP-pakket forward wordt het pakket geëncapsuleerd in een ander datalink-frame.

#### Hosts op hetzelfde netwerk

IP-adressen duiden de originele source en de final destination aan.

**Het netwerkgedeelte**, het meest linkse deel van het IP-adres, duidt het aan tot welk netwerk de host behoort.

**Het hostgedeelte**, de rest van het IP-adres duidt een specifieke host of device op het netwerk aan.

Het datalink-frame gebruikt MAC-adressen en kan rechtstreeks naar de ontvanger gestuurd worden.

#### Hosts op een verschillend netwerk

Source-IP en Destination-IP behoren tot een verschillend netwerk. De datalink-frame kan niet rechtstreeks naar de ontvanger gestuurd worden, het moet via de default gateway (dichtstbijzijnde router richting buitenwereld).

Router verwijdert de ontvangen layer-2 informatie en voegt nieuwe datalink-info toe om het frame dan te forwarden via de exit-interface.

# Netwerktoegang

## Protocollen van de fysieke laag

### Fysieke laag

#### Connectietypes

* Kan zowel draadloos als bekabeld
* Fysieke verbinding is nodig om communicatie mogelijk te maken

#### Netwerkkaart

NIC, verbindt een toestel met een netwerk, dit wordt gebruikt voor bedrade verbinding.

Draadloze netwerkkaarten gebruiken we voor draadloze verbindingen.

### Doel van de fysieke laag

#### De fysieke laag

* Zorgt voor omzetting van bits van een frame naar een geschikt signaal voor het medium
* Accepteert een volledige frame van datalinklaag en encodeert deze in een reeks signalen die op het medium worden geplaatst.
* Encodeert bits van een frame ontvangen door een eindgebruikerstoestel of intermediair netwerkapparaat.

### Karakteristieken van de Fysieke laag

#### Bandbreedte

Capaciteit van het medium op data te transporteren. Het meet de hoeveelheid data dat binnen opgegeven tijd verstuurd kan worden tussen 2 punten.

Ook gezien als snelheid, is het aantal bits dat per seconde verstuurd wordt.

#### Doorvoersnelheid

Meet de overdrachtsnelheid van bits over de media voor opgegeven periode in tijd.

Dit komt meestal niet overeen met de bandbreedte door enkele beperkende factoren:

* Hoeveelheid dataverkeer
* Type dataverkeer
* Vertraging door netwerkapparaten tussen bron en bestemming

## Netwerk Media

### Koperkabels

### Karakteristieken van Koperen Media

* Elektrische pulsen
* Verzwakking, hoe langer de kabel hoe zwakker het signaal
* Alle koperen media moeten strikt de limieten op vlak van afstand volgen
* EMI, elektromagnetische interferentie, of RFI, radio frequentie interferentie =>

Verstoort datasignalen = Corrupte datasignalen. Geleiders krijgen afscherming om dit tegen te gaan.

* Overspraak, verstoring van het signaal door elektrische of magnetische velden veroorzaakt door naburig gelegen geleider.

Geleiders worden rond elkaar gewikkeld om overspraak te neutraliseren.

#### Koperen Media

##### UTP, Unshielded twisted-pair

Meest gebruikte media, kleurcodes helpen om connectoren goed op kabel te plaatsen.

**Eigenschappen:**

* Bestaat uit 4 paar kleurgecodeerde geleiders rond elkaar gewikkeld om overspraak te voorkomen.
* Beperkte grootte en flexibiliteit is handig tijdens installaties.
* Annulering: Magnetisch veld van 2 naast elkaar liggende geleiders zijn het tegenovergestelde van elkaar en neutraliseren de effecten van EMI en RFI.

**Standaarden:**

Volgt de standaarden van TIA/EIA

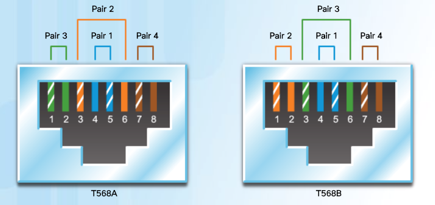
* CAT 3, wordt gebruikt voor spraak, meest gebruikt voor telefoonlijnen.
* CAT5 en 5e, gebruikt voor data overdracht, cat5 ondersteunt 100Mb/s, cat5e ondersteunt 1000Mb/s
* CAT6, gebruikt voor data overdracht ondersteund 1000Mb/s – 10 Gb/s (10 Gb/s niet aangeraden).

**Connectoren:**

* Afgesloten met RJ-45 connectoren (mannelijke kant), deze moeten kwaliteitsvol worden aangebracht op de kabel om optimale performantie en minimum aan overspraak te garanderen.
* TIA/EIA-568 standaarden beschrijven kleurcodes voor toekenning pinnen bij Ethernet kabels.
* Socket is vrouwelijke kant, te vinden op het netwerktoestel, aansluitpunt of patch paneel.

**Types:**

|  |  |  |
| --- | --- | --- |
| **Kabel type** | **Standaard** | **Applicatie** |
| Straight-through | Beide eindes T568A  Beide eindes T568B | Connecteert netwerkhost met een netwerktoestel zoals een switch of een hub. |
| Crossover | 1 uiteinde T568A, ander uiteinde T568B | * 2 netwerkhosts verbinden * Twee intermediaire netwerktoestellen verbinden (switch naar switch of router naar router) |
| Rollover | Cisco proprietary | Verbindt een workstation seriële poort met een router console poort, gebruik makend van een adapter. |



##### STP, Shielded Twised-pair

Beter beschermd tegen ruis dan UTP, iets duurder en moeilijker te installeren. Combineert verschillende technieken tegen overspraak en EMI en RFI. Gebruikt 4 paren geleiders waarbij elk paar wordt afgeschermd door folie.

##### Coax

Bestaat uit:

* Koperen geleider voor elektrisch signaal
* Flexibele kunststof isolatie rond koperen geleider
* Kunststof wordt gewikkeld in gewoven, koperen omhulsel of een metalen folie dat als 2e geleider functioneert en als afscherming voor binnenste geleider.

UTP kabels hebben coax kabels vervangen maar coax wordt nog gebruikt in:

* Draadloze installaties voor verbinding van antennes.
* Internetinstallatie bij kabelprovider.

### Glasvezel

#### Eigenschappen van glasvezel

* Heeft 4 toepassingen:

1. Bedrijfsnetwerken
2. Glasvezel naar huis (FTTH)
3. Lange-afstands netwerken
4. Onderzeese netwerken

* Kan over langere afstanden aan een hogere bandbreedte dan koperen media.
* Signalen hebben minder verzwakking en zijn immuun voor EMI en RFI.
* Bits = lichtpulsen
* Flexibel, extreem dunne transparante vezels van puur glas niet veel groter dan menselijk haar.

### Draadloze Media

#### Eigenschappen van draadloze media

* Werkt met elektromagnetische signalen die de bits van de datacommunicatie voorstellen en gebruiken radio frequenties.
* Draadloze beperkingen zijn:

1. **Dekking**, Bouwmaterialen en lokale omgeving beperken dekking.
2. **Interferentie,** verstoring door storing zoals TL-lampen, microgolfovens, en andere draadloze apparatuur.
3. **Veiligheid,** Toestellen en gebruikers die niet geauthoriseerd zijn, kunnen toch de datastroom bekijken
4. **Gedeeld medium,** slechts 1 toestel kan op een bepaald tijdstip verzenden of ontvangen en het medium wordt gedeeld door alle draadloze gebruikers.

## Datalink Protocollen

### Datalinklaag

Deze laag bereidt de netwerkdata voor voor de fysiekelaag

**L2 Header:**

Eerst de NIC van de ontvanger, dan de NIC van de afzender.

**L3 IP Packet:**

Eerst IP van de afzender, dan IP van de ontvanger.

#### Media toegangscontrole

* Pakketten worden over verschillende fysieke netwerken verstuurd tussen bron en bestemming.
* Fysieke netwerken kunnen uit verschillende types media bestaan zoals koperkabels, optische glasvezel, draadloos, satellietverbinding.

#### Toegang tot de media voorzien

Bij elke hop op zijn pad, zal een router:

* Een frame vanop het medium accepteren
* Het frame uitpakken
* Het pakket in een nieuwe frame inpakken
* Het nieuwe frame doorsturen volgens het type medium van de volgende link.

## Media Access Control

### WAN topologieën

#### Veel voorkomende WAN topologieën

##### Punt-tot-punt,

Permanente link tussen twee eindpunten.

**Fysieke topologie:**

Frames worden door de ene node op het medium geplaatst en door de andere node eraf gehaald.

**Logische topologie:**

* Eindnodes kunnen fysiek gekoppeld worden door verschillende intermediaire netwerkapparaten.
* Gebruik van fysieke toestellen in netwerk beïnvloedt logische topologie niet.
* Logische verbinding tussen noden wordt een virtueel circuit genoemd.

##### Hub and Spoke

Centraal punt verbindt de verschillende nodes via punt-tot-punt verbindingen.

##### Full mesh

Zorgt voor hoge beschikbaarheid maar vereist dat elke node verbonden is met elke andere node. Kosten en beheer kunnen aanzienlijk zijn.

### LAN topologieën

#### Fysieke LAN topologieën

|  |  |
| --- | --- |
| **Topologie** | **Beschrijving** |
| **Ster** | Toestellen worden verbonden met een centraal netwerkapparaat zoals een switch. |
| **Uitgebreide ster** | Additionele ethernet switchen verbinden zich met andere ster topologieën. |
| **Bus** | Komt voor in verouderde netwerken, alle toestellen worden in een ketting aan elkaar gehangen met een slot op de eindpunten. Switchen zijn niet vereist. Deze topologie gebruikt coax kabels omdat dit goed en eenvoudig op te zetten was. |
| **Ring** | Toestellen worden ion een kring aan elkaar verbonden. In tegenstelling tot de bus topologie, moet de ring geen afsluiting kennen op eindpunten. Deze topologie werd gebruikt in oudere glasvezelnetwerken en token ring netwerken. |

#### Half en Full Duplex

**Half-Duplex:**

* Beide apparaten kunnen op het medium verzenden en ontvangen maar niet tegelijkertijd.
* Gebruikt in oudere bus topologieën en Ethernet hubs.
* WLANs opereren in half-duplex (WiFi).

**Full-Duplex:**

* Beide apparaten kunnen tegelijkertijd verzenden en ontvangen op het medium.
* Datalinklaag gaat ervan uit dat media beschikbaar is voor data-overdracht voor beide nodes op hetzelfde tijdstip.
* Ethernet switches opereren in full-duplex, maar kan ook in half-duplex opereren indien de switch verbonden is met bijvoorbeeld een ethernet hub.

#### Media toegangscontrole

**Contentie gebaseerde toegang:**

* Nodes opereren in half-duplex.
* Concurreren voor het gebruik van het medium.
* Slechts één toestel per tijdstip kan verzenden.

**Gecontroleerde toegang:**

* Elke node krijgt tijdslot om medium te gebruiken.
* Token Ring LANs zijn voorbeeld hiervan.

#### Contentie gebaseerde toegang – CSMA/CD

Dit proces wordt gebruikt in half-duplex ethernet LANs.

* Als 2 toestellen tegelijk verzenden gebeurt er een botsing, beide toestellen detecteren de botsing, data zal corrupt zijn en moet opnieuw verzonden worden.

#### Contentie gebaseerde toegang – CSMA/CA

Gebruikt een methode om te zien of het medium vrij is, verhindert geen botsingen maar probeert die te vermijden door te wachten met verzenden.

**Note:** LANs die met switchen opgebouwd zijn gebruiken geen contentie gebaseerd systeem meer omdat switch met elke verbonden host in full-duplex kan opereren

### Datalink Frame

#### Het Frame

Bestaat uit 3 onderdelen:

* Header
* Data
* Trailer

Structuur en de velden zijn afhankelijk van een Laag 3 (L3) protocol.

#### Frame velden

FRAME IS IN DEZE EXACTE VOLGORDE OPGEBOUWD (eerste item = meest links)

* **Frame start indicatie vlag**, identificeert het begin van een frame.
* **Adressering**, identificeert de bron- en bestemmingsnodes.
* **Type,** identificeert het L3 protocol in de data.
* **Controle**, identificeert specifieke diensten zoals QoS.
* **Data**, bevat de payload.
* **Foutdetectie**, bevat een CRC checksum om na te gaan of er bitfouten zijn opgetreden in een ontvangen frame.
* **Frame stop indicatie vlag,** identificeert het einde van een frame.

# Ethernet

## Ethernet Protocol

### Ethernet Frame

#### Ethernet Frame velden

**Minimale grootte** van een **Ethernet frame** van bestemmings MAC adres tot FCS (Frame check sequence) is **64 bytes** en de **maximum grootte** is **1518 bytes**.

* Frames die kleiner zijn dan 64 bytes worden “collision fragments” of “runt frame” genoemt en worden automatisch vernietigd door ontvangende nodes
* Frames groter dan 1500 bytes worden “jumbo” of “baby giant frames” genoemd.

Ontvangende apparaten laten frame vallen indien deze kleiner is dan de minimale grootte of groter dan het maximum.

### Ethernet MAC adressen

#### MAC Adressen

MAC adres bestaat uit 48 bits, onderverdeeld in 12 hexadecimale symbolen (4 bits per symbool).

Hexadecimale symbolen worden gebruikt om ethernet MAC adressen en IPv6 adressen voor te stellen. Deze hexadecimale waarden worden in tekst vaak voorafgegaan door “0x”.

#### MAC Adressen: Ethernet identiteit

MAC adressen worden gebruikt om de bron en bestemming te identificeren, de regels van een MAC adres zijn vastgelegd door IEEE. IEEE kent de leverencier een 3-byte (24bit) code toe, Organizationally Unique Identifier (OUI) genoemd.

De leverancier moet 2 regels volgen:

* Alle MAC adressen van een NIC of ander Ethernet apparaat moeten het aan de leverancier toegekend OUI gebruiken in de eerste 3 bytes.
* Alle MAC adressen met dezelfde OUI moeten unieke waarden toegekend krijgen in de laatste 3 bytes.

#### Frame verwerking

MAC adres = ingebrand adres, het adres is permanent op de ROM chip geëncodeerd. Bij het opstarten van de computer kopieert de NIC het MAC adres van ROM naar RAM.

* Header info wordt toegevoegd aan de frame wanneer een toestel een bericht naar een Ethernet netwerk stuurt.
* Header info bevat het MAC adres van de bron en van de bestemming.

#### MAC Adres voorstellingen

**Commando ipconfig /all-in** CMD om MAC adres van Ethernet adapter op te vragen. (**ifconfig** op linux machine of Apple computer)

#### Unicast MAC adres

Dit is het uniek adres wanneer een frame wordt verzonden van het ene toestel naar één ander toestel.

Om een unicast pakket te kunnen verzenden en ontvangen moet er een IP adres in de pakket header staan en een corresponderend bestemmings MAC adres in de Ethernet frame header.

#### Broadcast Mac adres

Veel netwerkprotocollen, zoals DHCP en ARP, gebruiken broadcasts.

Een broadcast pakket heeft bestemmings IPv4 adres waarbij alle hostbits 1 zijn zodat alle hosts in een lokaal netwerk het pakket zullen ontvangen en verwerken.

Wanneer IPv4 broadcast pakket is ingepakt in een Ethernet frame => Bestemmingsadres = broadcast MAC adres = FF-FF-FF-FF-FF-FF.

#### Multicast MAC adres

Deze zorgen ervoor dat een pakket bij een groep van toestellen bezorgd wordt.

Toestellen behorend tot een multicast krijgen een groep IP adres toegekend in het gebied van 224.0.0.0 tot 239.255.255.255.

Het multicast IP adres vereist een corresponderend multicast MAC adres dat begint met 01-00-5E.

## LAN Switches

### MAC adrestabel

#### Basisprincipes van een Switch

Een L2 switch maakt beslissingen ivm het doorsturen van frames op basis van de L2 MAC adressen.

Na startup van de switch is de MAC adres tabel leeg en heeft de switch de MAC adressen van de verbonden apparaten nog niet aangeleerd.

#### MAC adressen aanleren

Switch bouwt MAC adres tabel dynamisch op.

**Proces om MAC adressen aan te leren:**

1. Switches onderzoeken inkomende frames om nieuwe MAC adres informatie aan te leren.
2. Indien het bron MAC adres ongekend is wordt deze toegevoegd aan de tabel, samen met het poortnummer.
3. Indien het bron MAC adres gekend is voert de switch een update uit door de refreshtime te vernieuwen.
4. Standaard houden switches een MAC adres bij voor 5 minuten.

**Proces om een frame door te sturen:**

1. Bij broadcast of multicast wordt het frame uit alle poorten verstuurd behalve de inkomende poort.
2. Bij unicast wordt het MAC adres opgezocht in de MAC adres tabel, daarna wordt het frame uit een specifieke poort verstuurd, indien het bestemmings MAC adres in de tabel werd gevonden.
3. Indien het MAC adres niet gevonden werd in de tabel, zal het frame uit alle poorten verstuurd worden behalve de inkomende poort (=flooding) (de pc die zijn adres herkend zal de frame binnenlaten de rest niet).

#### Frames filteren

MAC adres tabel opgevuld naarmate switch meer en meer frames ontvangt.

Wanneer de switch beschikt over het bestemmings MAC adres in de tabel, kan de switch het frame filteren en uit één specifieke poort versturen.

### Switch doorstuur methoden

#### Cut-through Switching

De switch buffert net voldoende van het frame om het bestemmings MAC adres te lezen zodat de poort waaruit de frame verstuurd moet worden, gekend is. Er wordt geen foutcontrole uitgevoerd op het frame.

Er zijn 2 varianten op deze methode van switching:

* **Fast forward switching**, dit biedt de laagste vertraging aan, meest gebruikte vorm van Cut-through switching.
* **Fragment-free switching**, haalt eerste 64 bytes op vooraleer het frame wordt doorgestuurd. Hierbij kunnen botsingsframes gedetecteerd en gedropt worden. Het is een compromis tussen store-and-forward en fast-forward switching.

#### Store-and-forward

De switch ontvangt een volledige frame en berekend de CRC (cyclic redundancy check). Als deze geldig is zoekt de switch het bestemmings MAC adres, deze bepaalt de poort waaruit de frame verstuurd wordt.

### Switch Doorstuur Methoden

#### Duplex en Snelheid instellingen

**Duplex**

Zie H4

De meeste toestellen onderhandelen automatisch over de snelheid en duplex mode die toegepast kan worden om zo performant mogelijk te kunnen werken.

Het komt regelmatig voor dat de ene kant in half-duplex werkt en de andere kant in full-duplex, dit veroorzaakt performantieproblemen op Ethernet verbindingen.

#### Auto-MDIX

Vroeger was het verplicht een bepaald type kabel te gebruiken afhankelijk van welke toestellen dat er met elkaar werden verbonden.

De meeste toestellen ondersteunen nu **Automatich medium-dependent interface crossover (auto-MDIX)**. Dit is standaard geactiveerd op switches.

Wanneer dit met het commando **mdix auto** in de interface config wordt geactiveerd kan de switch automatisch het juiste type kabel detecteren en instellen.

## Address Resolution Protocol (ARP)

### MAC en IP

#### Bestemming op hetzelfde netwerk

Een toestel krijg op een Ethernet LAN 2 primaire adressen:

* Fysiek adres (MAC adres)
* Logisch adres (IP adres)

L2 Ethernet frame bevat:

1. Destination MAC address
2. Source MAC address

L3 IP pakket bevat:

1. Source IP address
2. Destination IP address

#### Bestemming op een ander netwerk

Wanneer het Destination IP address uit een ander netwerk komt, zal het Destination MAC address deze zijn van de default gateway bij de verzendende host.

### ARP

ARP (Address Resolution Protocol) heeft twee basisfuncties:

* IPv4 adressen omzetten naar MAC adressen.
* Tabel bijhouden van koppeling

#### ARP Functies

Ethernet toestellen vertrouwen op ARP tabel (of ARP cache) in het geheugen om de koppeling tussen IPv4 en MAC adres te vinden.

Een toestel zoekt in zijn eigen ARP tabel naar het corresponderende MAC adres van het Destination IP address.

* Indien bron en bestemmings IPv4 binnen hetzelfde netwerk liggen, zoekt het toestel naar het bestemmings IPv4 in de ARP tabel.
* Indien de bron en bestemmings IPv4 in een verschillend netwerk liggen, zoekt het toestel naar het IPv4 van de def. Gateway in ARP tabel.

#### Entries uit een ARP tabel verwijderen

Elk toestel heeft een timer die ARP entries, die binnen een bepaalde periode niet werden gebruikt, verwijdert.

De timer is afhankelijk van het besturingssysteem. Je kan ook manueel alle of sommige entries uit een ARP tabel verwijderen.

#### ARP Tabel tonen

Om deze tabel te tonen:

Op cisco router: **show ip arp**

Op windows:  **arp -a**

### ARP Problemen

#### ARP Broadcasts

Een ARP broadcast frame wordt door elk toestel in het lokale netwerk ontvangen en bekeken. ARP requests kan voor een overvloed aan broadcasts zorgen indien toestellen op eenzelfde moment worden ingeschakeld en het netwerk aanspreken.

#### ARP Spoofing

Aanvallers kunnen op requests antwoorden en doen alsof ze bijvoorbeeld netwerkdiensten kunnen aanbieden.

Een type ARP Spoofing aanval is antwoorden op ARP requests voor de gateway zodanig dat pakketen die bedoelt zijn voor de gateway naar de aanvaller gestuurd worden.

Switches voor bedrijven hebben technieken om aan ARP inspectie te doen (Dynamic ARP inspection (DAI)).

# Netwerklaag

## Netwerkprotocollen

### Communicatie in de netwerklaag

#### De netwerklaag

Deze gebruikt 4 processen om het transport te voorzien “from end-to-end”:

1. Adressering van end devices
2. Inkapseling, protocol voorziet gegevenseenheden uit transportlaag van IP-header-info zoals bron en bestemmings IP adres.
3. Routering, netwerklaag biedt services om pakketten direct naar andere netwerken te kunnen sturen.
4. De-inkapseling, doelhost pakt het pakket terug uit.

#### Netwerklaagprotocollen

* IPv4
* IPv6

### Kenmerken van het IP-Protocol

#### Encapsulating IP

TCP-segment wordt ingekapseld door het toevoegen van IP-header met oog op levering aan doelhost. Deze IP-header blijft hezelfde van bron- tot doelhost.

Het proces van inkapseling van data, laag per laag, zetten diensten op verschillende lagen aan het werk zonder effect te hebben op andere lagen. **Encapsulatie isoleert de lagen dus van elkaar.**

Netwerklaag gebruikt pakketheader voor routering.

#### Kenmerken van IP

* IP is ontworpen als protocol met lage overhead- het bevat functies die zijn vereist voor het leveren van een pakket.
* Een IP-pakket wordt verzonden zonder voorafgaande vaststelling van een verbinding.
* IP is niet ontworpen voor het bijhouden en beheren van pakketten. Deze taken worden voornamelijk uitgevoerd door andere lagen, voornamelijk TCP.

#### IP – Connectionless

**IP is een connectionless-protocol:**

* Geen speciale end-to-end verbinding gemaakt voordat gegevens worden verzonden.
* Soortgelijk procedé als iemand die een brief post.
* Afzender weet niet of de bestemming geldig is.
* Functie draagt bij tot lage overhead van IP.

#### IP – Best Effort Delivery

**IP is een Best Effort Delivery-protocol:**

* IP is onbetrouwbaar omdat het niet garandeert dat alle pakketten zullen worden ontvangen.
* Onbetrouwbaar betekend dat IP niet in staat is de verloren pakketten of beschadigde pakketten te herstellen.
* Indien pakketten ontbreken of niet in juiste volgorde aankomen, moeten bovenlaag protocollen/diensten deze kwesties oplossen.

#### IP – Media Independant

**IP is een Media Independant-protocol:**

* IP opereert onafhankelijk van gebruikte media op de onderste lagen van de protocolstack, het maakt niet uit of het medium koperen kabels, glasvezel of draadloze verbinding is.
* OSI datalink layer is verantwoordelijk om IP-pakket voor te bereiden voor transmissie.
* Netwerklaag heeft maximumgrootte van PDU die kan worden uitgevoerd – genaamd MTU (Maximum transmission unit)
* Datalink layer vertelt netwerklaag wat MTU is.

### IPv4 Pakket

#### IPv4 Pakket Header

Bestaat uit binair gecodeerde velden met een totale lengte van 20 byte.

Belangrijkste velden zijn:

* **Version**, geeft aan dat het IPv4 is.
* **DS (Differentiated Services)**, wordt gebruikt om te bepalen welke prioriteit het pakket heeft
* **TTL,** Beperkt de levensduur van het pakket
* **Protocol,** Gebruikt voor het identificeren van volgende niveau protocol
* **Source IPv4 adres**
* **Destination IPv4 adres**

#### Beperkingen IPv4

Werd geüpdatet om nieuwe uitdagingen aan te pakken (nieuwe versie = IPv6).

De 3 belangrijkste issues van IPv4 zijn:

1. **IP-adresuitputting**, IPv4 heeft beperkt aantal unieke openbare adressen beschikbaar, door de exponentiële groei van nieuwe IP-enabled apparaten is de nood aan adressen toegenomen.
2. **Internet routing tabel expansie**, een routeringstabel bevat router met verschillende netwerken om het beste pad te kunnen bepalen, hoe meer apparaten op het netwerk, hoe groter de routing tabel en hoe meer routes hoe trager de router.
3. **Gebrek aan end-to-end connectivity**, Network Address Translation (NAT) is ontworpen om apparaten te voorzien van een gedeeld IPv4 adres. Een gedeeld adres zorgt echter voor problemen bij technologieën waarvoor end-to-end connectiviteit nodig is.

### IPv6 Pakket

#### Voordelen IPv6

* Grotere adresruimte, 128bits ipv 32bits.
* Verbeterde pakketafhandeling, minder velden dan IPv4.
* Elimineert noodzaak voor NAT, geen behoefte om adressen te delen.

#### Encapsulating IPv6

IPv6 header is simpeler dan IPv4 header.

**Voordelen:**

* Opmaak van vereenvoudigde koptekst voor efficiënte pakketafhandeling
* Hiërarchische netwerkarchitectuur voor routeringsefficiëntie.
* Autoconfig voor adressen.

#### IPv6 Pakket header

* **Version**, 4-bits binaire waarde ingesteld op “0110” die aanduid dat het een IPv6 pakket is.
* **Traffic class,** 8-bits veld = IPv4 DS-veld.
* **Flow Label,** 20-bit veld dat suggereert dat alle pakketten met zelfde flow label dezelfde behandeling krijgen van router.
* **Payload length,** 16-bits veld dat lengte van gegevensgedeelte of nettolading van het pakket weergeeft.
* **Next Header,** 8-bit veld = IPv4 Protocol veld. Geeft aan welk type data er in het pakket zit.
* **Hop limit,** 8-bit veld, vervangt IPv4 TTL veld. Deze waarde wordt verminderd met 1 telkens als het aan router passeert. Indien 0 wordt het pakket verwijderd.
* **Source IPv6 address,** 128-bit veld.
* **Destination IPv6 address,** 128-bit veld.

## Routing

### Hoe een Host routes

#### Host forwarding decision

Een host kan pakketten verzenden naar:

* **Zichzelf**, dit kan een host doen als test dmv de loopback interface 127.0.0.1
* **Een local host**, Dit is een host op hetzelfde lokale netwerk.
* **Remote host,** Host op een extern netwerk.

IPv4 source address en subnet mask worden vergeleken met het destination address en subnet mask om te bepalen of de host local of remote is.

#### Default Gateway

Netwerkapparaat dat verkeer naar andere netwerken kan routeren, weg van het lokaal netwerk.

Gebeurt wanneer de bestemming een remote host is. De Def. Gateway weet waarheen het pakket verzonden moet worden op basis van de routeringstabel.

Verzendende host hoeft niet te weten waar het pakket exact naartoe moet, hij zendt het gewoon naar de default gateway (of router).

#### Gebruik van de Default gateway

Host-routeringstabel bevat meestal Def. Gateway adres oftewel het IP-adres van de router voor het netwerk v/d host.

Host ontvangt IPv4 van def. Gateway via DHCP oftewel is het handmatig geconfigureerd.

Een geconfigureerde def. Gateway creëert standaardroute in routeringstabel van host, deze is de route die de computer kiest wanneer een pakket naar een remote host moet gezonden worden.

#### Host Routing Tabels

Weergeven m.b.v.:

* **Route print**
* **Netstat -r**

3 secties worden dan getoond:

* **Interface List**, lijst van het MAC-adres en het toegewezen interfacenummer van alle Netwerkinterfaces op de host.
* **IPv4 Route table**, lijst van alle bekende IPv4-routes.
* **IPv6 Route table,**  lijst van alle bekende IPv6-routes.

### Router Routing Tabels

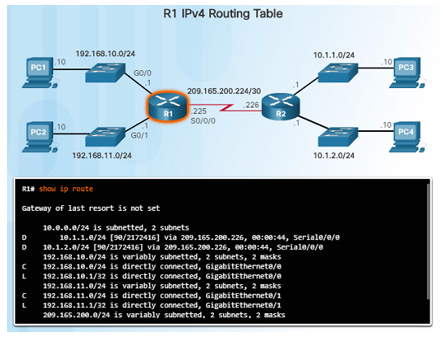
#### IPv4 Router Routing Table

Commando **show ip route** om IPv4-routeringstabel weer te geven.

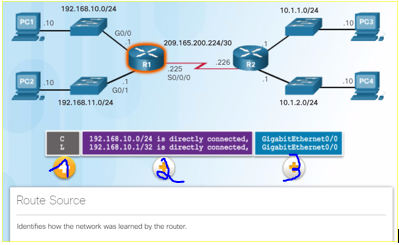
Deze tabel bevat:

* Directly connected en remote routes.
* Hoe elke route werd geleerd.
* Betrouwbaarheid en beoordeling van de route.
* Wanneer de route voor het laatst was bijgewerkt.
* Welke interface wordt gebruikt om de bestemming te bereiken.

Een router onderzoekt de header van binnenkomend pakket om doelnetwerk te bepalen. Is er een match, dan wordt het pakket doorgestuurd op basis van de opgegeven info in de routeringstabel.

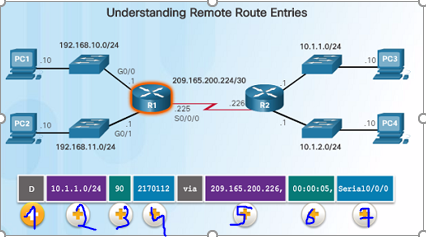


#### Directly Connected Routing Table Entries



1. **C,** duidt aan dat netwerk directly connected is en dat interface geconfigureerd is met een IP-adres en geactiveerd is.
2. **L,** identificeert dat het om een **lokale interface** gaat. IPv4 adres van de interface op de router.
3. **De gebruikte interface**

#### Understanding Remote Route Entries



1. Letter vooraan duidt Route Source aan. **D** betekend dat de route werd aangeleerd via EIGRP (Enhanced Interior Gateway Routing Protocol)
2. Identificeert doelnetwerk
3. Administratieve afstand, m.a.w. de betrouwbaarheid van de route, hoe lager hoe beter.
4. De metriek of de waarde die werd toegewezen voor het bereiken van het externe netwerk. Lagere waarden = voorkeurroutes/
5. Next-hop of IP-adres van de volgende router om het pakket door te sturen.
6. Route timestamp, tijdstip wanner router laatst van zich liet horen
7. Outgoing interface.

#### Next-Hop Address

Indien de router een pakket ontvangt dat bedoelt is voor een extern netwerk stuurt deze het pakket door naar het next-hop adres dat overeenkomt met het doelnetwerkadres in de routeringstabel. Indien er geen default gateway is ingesteld zal het pakje geschrapt worden.

## Routers

### Anatomie van een Router

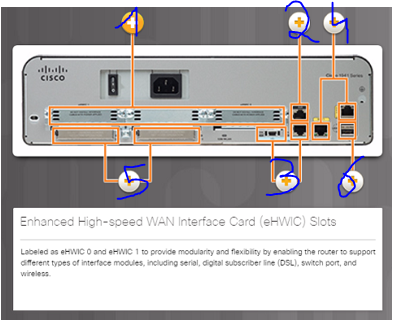
#### Router Memory

|  |  |
| --- | --- |
| **RAM** | Vluchtig geheugen gebruikt voor het opslaan van toepassingen, processen en gegevens die gebruikt worden door de CPU. |
| **ROM** | Niet-vluchtig geheugen, gebruikt voor het opslaan van cruciale werkinstructies en een beperkte IOS. Bevat de firmware, op een chip, aan de binnenkant van de router. |
| **NVRAM** | Niet-vluchtig geheugen gebruikt als permanente opslag van het configuratiebestand (startup-config). |
| **Flash** | Niet-vluchtig geheugen gebruikt als permanente opslag voor het IOS en andere systeembestanden zoals log of back-upbestanden. |

#### Binnenkant van een Router

* Voeding
* Koelventilator
* Synchronous Dynamic RAM (SDRAM)
* NVRAM
* CPU
* Hitteschilden
* Advanced Integration Module (AIM)

#### Aansluiting van een Router

1. Enhanced High-speed WAN Interface card Slots (eHWIC slots).
2. AUX, RJ-45 poort voor remote beheer.
3. Console Port, voor initiële configuratie en Command Line Interface toegang via RJ-45 of USB type B
4. Gigabit Ethernet, voor LAN access, aansluiten van switched, end-devices, of andere routers.
5. Compact Flash slots, aangeduid als CF0 en CF en gebruikt om het flash geheugen uit te breiden tot 4GB
6. USB port, gebruikt om extra opslagruimte te voorzien.

#### LAN en WAN Interfaces

* In-band router interfaces – LAN en WAN
* Management ports – Console en AUX

Meest voorkomende manieren om toegang te verkrijgen tot user EXEC mode in CLI:

* **Console** = Afzonderlijke toegang waarbij netwerkinterfaces nog niet geconfigureerd moeten zijn (out-of-band).
* **Secure Shell (SSH),** veilige manier om op afstand verbinding te maken via CLI. Dit vereist actieve netwerkservices (in-band).
* **Telnet,** is een onveilige methode om vanop afstand een CLI-sessie tot stand te brengen via een virtuele interface van een netwerk. De verbinding is niet encrypted.

### Router Boot-Up

#### Bootset Files

IOS-image en het startup-configbestand worden in het RAM geheugen geladen wanneer routers en switches zijn opgestart.

Running-config wordt gewijzigd wanneer de netwerkbeheerder wijzigingen maakt. Deze moeten worden opgeslagen naar het startup configuratiebestand in NVRAM om hen kracht bij te zetten bij volgende reboot van de router.

#### Router Bootup Process

1. POST en laden van Boostrap-programma. Na de POST wordt het bootstrap-programma gekopieerd van ROM naar RAM en is zijn job het vinden van en het inladen van de IOS is het RAM.
2. Lokaliseren en laden van de IOS. IOS is opgeslagen op het flash geheugen en wordt bij de uitvoering gekopieerd nar het RAM.
3. Lokaliseren en laden van startup configuratiebestand of toegang verschaffen tot de setup mode. Bootstrap-programma kopieert startup config file van NVRAM naar RAM en wordt de running config.

#### Show Version Output

**Show version** commando geeft weer:

* Versie van bootstrap programma
* Informatie over de hardware config
* Hoeveelheid systeemgeheugen

# IP Adressering

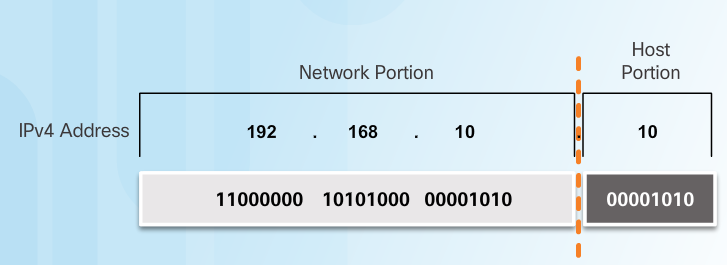
## IPv4 Netwerkadressen

### IPv4 Adresstructuur

#### Netwerk- en hostgedeelte

Een IPv4-adres is hiërarchisch opgebouwd, deze bestaat uit een **netwerk- en een hostgedeelte.**

Alle apparaten op hetzelfde netwerk moeten een identiek netwerkgedeelte hebben. De Subnet Mask helpt apparaten bij het identificeren van het netwerkgedeelte en het hostgedeelte.



#### De Subnet Mask

Bij een host moeten er 3 IPv4 adressen geconfigureerd worden:

* Dat van de host
* Subnet Mask (afhangend van de noden van de gebruiker is dit meestal 255.255.255.0)
* Default Gateway, IP adres van lokale router interface

Het IPv4 van de host wordt vergeleken met de Subnet Mask, bit per bit, van links naar rechts.  
Een 1 in de Subnet Mask geeft aan dat de overeenkomstige bit in het IPv4-Adres een bit is van het netwerkgedeelte.

#### Logische EN

* 1 van de 3 elementaire binaire operaties die worden gebruikt in digitale logica.
* Bepaalt het netwerkadres

#### Prefix lengte

* Geschreven in slash notatie, /gevolgd door het aantal netwerkbits.
* Gelijk aan het aantal bits in de Subnet mask dat op 1 ingesteld staan.

#### Netwerk, Host en Broadcast Adressen

* **Netwerkadres**, het hostgedeelte is overal 0.
* **Eerste hostadres,** het hostgedeelte is overal 0 en eindigt met 1 (NA+1).
* **Laatste hostadres,** het hostgedeelte is overal 1 en eindigt met 0 (BA-1).
* **Broadcast Adres,** hostgedeelte is overal 1.

### IPv4 Unicast, Broadcast en Multicast

#### Dynamische IPv4-adrestoewijzing aan een host

Gebeurt meestal door de DHCP, Dynamic Host Configuration Protocol, deze biedt een IPv4 adres, subnet mask, default gateway en andere configuratiegegevens aan.

Least adressen aan hosts gedurende bepaalde tijdsduur. Als de host wordt uitgeschakeld of uit het netwerk wordt gehaal wordt de lease beëindigt en kan het adres door een andere host gebruikt worden.

#### Multicast transmissie

224.0.0.0 tot 239.255.255.255 gereserveerd voor de multicast. Routeringsprotocollen gebruiken multicast-transmissie voor het uitwisselen van routegegevens.

### Typen IPv4-adressen

#### Publieke en private adressen

**Private adressen:**

* Niet routeerbeer
* Enkel gebruikt in interne netwerken
* Moet worden vertaald naar publiek IPv4 om routeerbaar te worden
* 10.0.0.0 tot 10.255.255.255, 172.16.0.0 tot 172.31.255.255, 192.168.0.0 tot 192.168.255.255

#### Speciale adressen

* **Loobback Adressen, (127.0.0.0/8 of 127.0.0.1),** gebruikt op een host om testen of de TCP/IP-config operationeel is.
* **Link-Local Adressen (169.254.0.0/16 of 169.254.0.1)**, APIPA-adressen (Autimatic Private IP Addressing). Wordt gebruikt door Windows-client om zelf te configureren als er geen DHCP-server beschikbaar is.
* **TEST-NET Adressen (192.0.2.0/24 of 192.0.2.0 tot 192.0.2.255),** gebruikt voor het onderwijs en testdoeleinden

#### Legacy Classful Addressing

**Klasse A:**

* 0.0.0.0/8 tot 127.0.0.0/8
* Ter Ondersteuning van extreem grote netwerken met 16 miljoen host adressen.

**Klasse B:**

* 128.0.0.0/16 tot 191.255.0.0/16
* Voor de behoeften van matige tot grote omvang netwerken tot ongeveer 65 000 host adressen te ondersteunen.

**Klasse C:**

* 192.0.0.0/24 tot 223.255.255.0/24
* Ter ondersteuning van kleine netwerken met maximum van 254 hosts.

#### Classless Addressing

* Classful verspilde adressen
* Classless Inter-Domain Routing (CIDR) “cider”.
* Laat serviceproviders toe om adressen toe te wijzen op elke grens tussen netwerk- en hostgedeelte in plaats van alleen door een klasse A, B of C.

## IPv6 Netwerk Adressering

### IPv4-problemen

#### Coëxistentie van IPv4 en IPv6

Migratie van IPv4 naar IPv6 technieken

|  |  |
| --- | --- |
| **Dual Stack** | Apparaten draaien op IPv4 en IPv6 protocol stacks |
| **Tunneling** | IPv6 pakket wordt ingekapseld in een IPv4 pakket |
| **Translation** | Met NAT64 (Network Address Translation 64) kunnen IPv6-apparaten communiceren met IPv4-apparaten. |

### IPv6-adressering

#### IPv6-adres weergave

* 128 bits
* Elke 4 bits = 1 hexadecimaal cijfer
* Hextet, officieuze term voor een segment van 16 bits of 4 hexadecimale waarden.

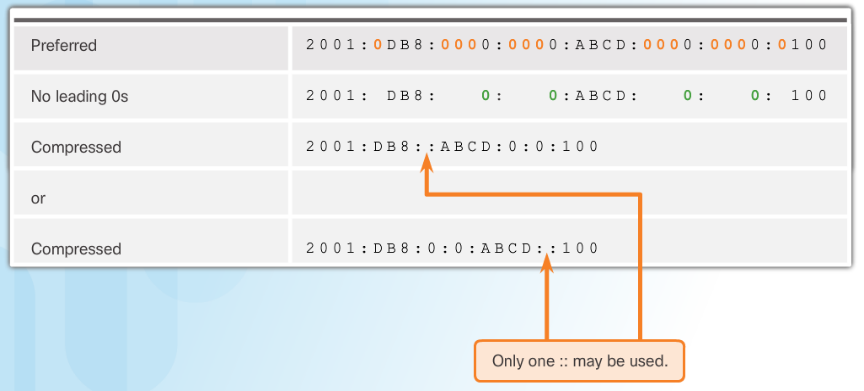
#### Regel 1, weglaten van leidende nullen

Om de lengte van een IPv6 adres te verminderen of te comprimeren gaan we de leidende nullen weghalen in een hextet.



#### Regel 2, 0 segmenten weglaten

Een dubbele dubbelpunt “::” kan elke afzonderlijke, aaneengesloten reeks van één of meer hextets vervangen, bestaande uit allemaal nullen.



### Typen IPv6-adressen

#### IPv6-adres types

3 types:

|  |  |
| --- | --- |
| **Unicast** | 1 Bron IPv6-adres |
| **Multicast** | Een IPv6-multicast-adres wordt gebruikt om één IPv6-pakket naar meerdere bestemmingen te verzenden. |
| **Anycast** | Een IPv6 anycast-adres is een Unicast-adres dat kan worden toegewezen aan meerdere apparaten. |

#### Lengte van IPv6-prefix

Wordt gebruikt om het netwerkgedeelte van een IPv6-adres aan te geven

* Kan variëren van 0 tot 128.
* Meestal /64

#### IPv6-unicast-adressen

**Global Unicast**:

* Wereldwijd unieke, Internet routeerbare adressen.

Momenteel worden alleen global unicast adressen met de eerste 3 bits van 001 of 2000::/3 toegewezen.

Bestaat uit 3 delen:

* **Global routing prefix**: netwerkgedeelte van het adres dat door de provider is toegewezen. Typisch /48.
* **Subnet ID:** Gebruikt voor subnet binnen een organisatie
* **Interface ID:** Gelijk aan het host-gedeelte van een IPv4-adres.

**Link-Local:**

* Wordt gebruikt om te communiceren met andere apparaten op dezelfde lokale link, beperkt tot één enkele link.
* Apparaat inschakelen om alleen met andere IPv6-apparaten op dezelfde koppeling te communiceren
* Zelf als er geen global unicast IPv6 adres is voor dit apparaat wordt dit adres aangemaakt
* In de FE80::/10 range.

**Unique-Local:**

* Gebruikt voor lokale adressering binnen een site of tussen een beperkt aantal sites.

### IPv6 Unicast Adressen

#### Statische configuratie van een Global Unicast Adres

Host config:

* Is gelijkaardig met het configureren van een IPv4-adres
* Default gateway-adres kan worden geconfigureerd om het link-local of global unicast-adres van de Gigabit Ethernet-interface aan te passen.

Dynamische toewijzing van IPv6 adressen:

* Stateless Address Autoconfiguration (SLAAC)
* Stateless DHCPv6
* Statefull DHCPv6

#### Dynamische configuratie SLAAC

* Apparaat kan zijn prefix, prefixlengte, default gatewayadres en andere info van IPv6 router verkrijgen
* Maakt gebruik van ICMPv6 van lokale router, Router Advertisement (RA) berichten.

ICMPv6 RA berichten worden elke 200 seconden verzonden naar alle IPv6-apparaten in het netwerk.

#### Dynamische configuratie DHCPv6

**RA optie 1: SLAAC Only:**

Ik heb alles wat je nodig hebt

**RA optie 2: SLAAC en DHCPv6:**

Gebruikt SLAAC voor IPv6 global unicast-adres en default gateway. Rest van info wordt voorzien door stateless DHCPv6-server.

**RA optie 3: DHCPv6 Only:**

Gebruikt link-local adres van routers voor default gateway. DHCPv6-server voorziet alle andere info.

### IPv6 Multicast Adressen

#### Toegewezen IPv6 Multicast adressen

Twee types IPv6 multicast:

1. **Toegewezen multicast**, gereserveerde multicastadresen voor vooraf gedefinieerde groepen apparaten.
2. **Solicited node multicast,** toegewezen aan een speciaal Ethernet-multicast-adres, staat Ethernet NIC toe om het frame te filteren op het bestemmings MAC-adres.

Twee gemeenschappelijke IPv6 toegewezen multicast groepen:

1. **FF02::1 All-nodes**, dit is een multicast-groep waaraan alle IPv6-apparaten deelnemen. Vergelijkbaar met broadcast in IPv4.
2. **FF02::2 All-routers,** dit is een multicast-groep waaraan alle IPv6-routers deelnemen.

## Connectiviteit verificatie

### ICMP

#### ICMPv4 en ICMPv6

ICMP: Internet Control Message Protocol

Dit is het Messaging Protocol. ICMP-berichten voor zowel IPv4 als IPv6 omvatten:

* Ontvangstbevestiging
* Bestemming of server onbereikbaar
* Tijd overschreden
* Route omleiding

#### ICMPv6 Router Solicitation and Router Advertisement Messages

ICMPv6 bevat 4 nieuwe protocollen als onderdeel van de Neighbor Discovery Protocol (ND of NDP).

* Router Solicitation (RS) message.
* Router Advertisement (RA) message.

RA messages worden gebruikt om adresgegevens te verstrekken aan hosts.

* Neighbor Solicitation (NS) message.
* Neighbor Advertisement (NA) message.

NS en NA messages worden gebruikt voor adresresolutie en Duplicate Address Detection (DAD).

### Testen en verifiëren

#### Traceroute – het pad testen

**Traceroute (tracert)** is een hulpprogramma dat een lijst genereert van hops (= routers) die succesvol werden bereikt langs het pad.

* Round Trip Time (RTT) – Tijd die het pakket neemt om de remote host te bereiken en voor de reactie van de host om terug te keren.
* Asterisk wordt gebruikt om een verloren pakket aan te duiden.

# Subnetting IP Netwerken

## Subnetten van een IPv4-netwerk

### Netwerksegmentatie

#### Broadcast domeinen

Apparaten gebruiken broadcasts om:

* ARP te versturen (laag 2)
* Een DHCP server te vinden

**Reactie van switches =>** Verspreiden de broadcasts via alle poorten behalve de poort waarop het werd ontvangen.

#### Problemen met grote broadcast domeinen

Problemen die ontstaan door broadcasts op grote netwerken zijn:

* Trage netwerkoperaties als gevolg van het aanzienlijke verkeer.
* Langzame apparaat operaties omdat een apparaat elk broadcastpakket moet accepteren en verwerken.

**Oplossing:**

Verminder de grootte van het netwerk om kleinere broadcast-domeinen te maken. Deze kleinere netwerkruimten noemen we **subnetten**.

#### Redenen voor subnetten

De voornaamste redenen om te subnetten zijn:

* Het vermindert het algehele netwerkverkeer en verbetert de netwerkprestaties.
* Een beheerder kan een beveiligingsbeleid implementeren, zoals welke subnetten wel of niet onderling mogen communiceren.

### Subnetting van een IPv4 Netwerk

#### Octet Boundaries

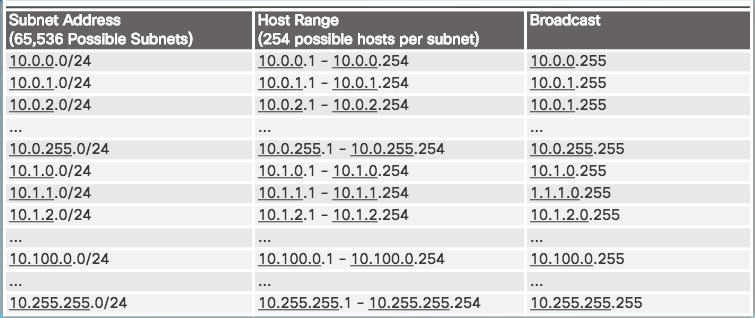
* **Netwerken zijn het gemakkelijkst te subnetten per octetgrens van /8, /16 en /24.**

Subnetten worden gemaakt door het lenen van host bits voor netwerk bits.

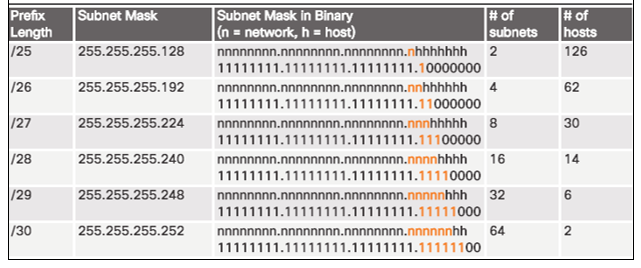
Prefix = /8, /16,… = het aantal bits voor het netwerk. Hoe groter de prefix, dus hoe meer geleende hostbits, hoe meer subnetten er mogelijk zijn.

|  |  |  |
| --- | --- | --- |
| **Klasse A** | 255.0.0.0 | 16.777.214 hosts |
| **Klasse B** | 255.255.0.0 | 65.534 hosts |
| **Klasse C** | 255.255.255.0 | 254 hosts |

#### Subnetten op de octetgrens

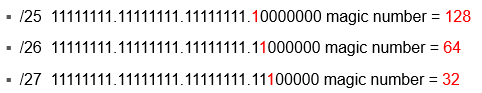


#### Classless subnetting



#### Subnetting met het Magic Number

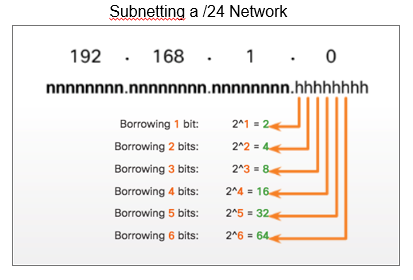
Magic number = plaatswaarde van de laatste 1 in het subnet mask.



#### Subnetting: Formule

**Formule voor het berekenen van het aantal subnetten:**

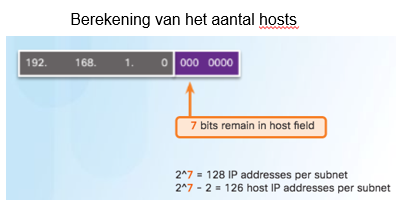
met n = het aantal geleende hostbits.



**Formule voor het berekenen van het aantal hosts:**

met n = het aantal overblijvende hostbits.

-2 => default gateway IP en Broadcast IP



### Voordelen van variabele lengte subnet masking

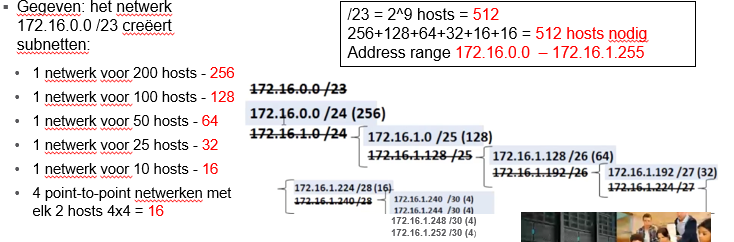
#### Traditionele subnetten verkwisten IP-adressen

Ze verkwisten een hoop IP-adressen door subnetten die veel meer hostsadressen toegewezen krijgen om te gebruiken dan dat ze eigenlijk nodig hebben.

#### VLSM, Variable Length Subnet Masks

* Subnetten hoeven niet dezelfde grootte te hebben, zolang hun adresbereiken elkaar niet overlappen
* Bij het aanmaken van subnetten is het makkelijker om te werken van groter naar kleiner.

**Voorbeeld:**



## Adresseringsschema’s

### Structured Design

#### Schema om het netwerk aan te pakken

* Elke host moet uniek adres hebben
* Goed schema en documentatie zijn een must.
* Toegangscontrole tot servers van interne en externe hosts
* Layer 3 STATIC adres van een server kan dienen als beheer van toegang tot die server.
* Controleren van beveiliging en prestaties van hosts = netwerkverkeer ondezoeken op bron-IP-adressen die buitensporige pakketten genereren of ontvangen.

#### Adressen toewijzen aan apparaten

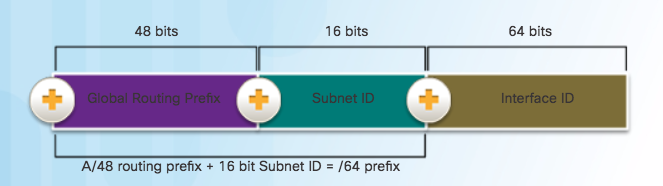
* **Eind gebruiker clients**
* **Servers**
* Statische adressen
* **Intermediary devices**
* Statische adressen voor extern beheer
* **Gateway**

## Ontwerpoverwegingen voor IPv6

### Subnetten van een IPv6-netwerk

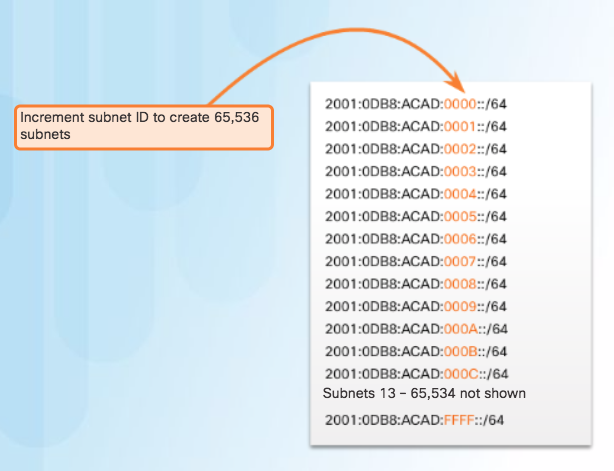
#### IPv6 Global Unicast Address

* IPv6 Subnetting is niet bezig met behoud adresruimte
* Gaat over het opbouwen van adreshiërarchie op basis van aantal nodige subnetwerken
* IPv6 link-local wordt nooit gesubnet
* IPv6 global unicast adress kan gesubnet worden en bestaat normaal uit een /48 global routing prefix, 16 bit subnet iD en 64 bit interface ID.



Subnetting gebeurd bij IPv6 adhv het Subnet ID





# Transportlaag

## Transportlaagprotocollen

### Transport van gegevens

#### Rol van de transportlaag

* Verantwoordelijk voor het opzetten van een tijdelijke communicatiesessie tussen twee toepassingen en het leveren van gegevens tussen hen.
* Koppeling tussen de applicatielaag en de lagere lagen die verantwoordelijk zijn voor de netwerkoverdracht.

#### Verantwoordelijkheden

* **Conversatie bijhouden:** Volgt elk afzonderlijk gesprek tussen bron een doeltoepassing
* **Segmentatie:** Verdeelt gegevens in segmenten die eenvoudiger te beheren en te transporteren zijn. Header wordt gebruikt voor het re-assemblen en het bijhouden.
* **Toepassing identificeren:** Zorgt dat zelfs bij meerdere toepassingen die op een apparaat worden uitgevoerd, alle toepassing de juiste gegevens ontvangen via poortnummers.

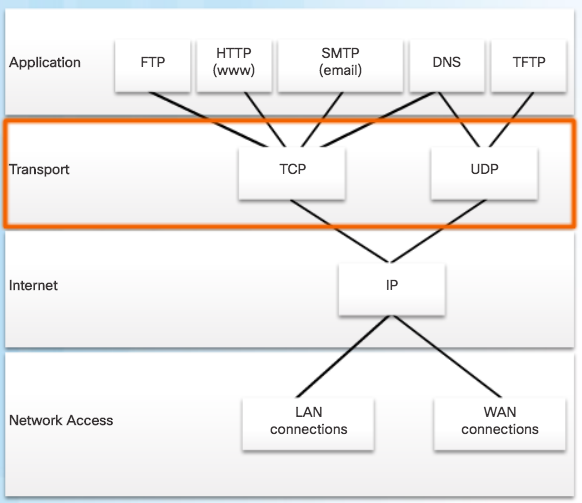
#### Conversatie multiplexing

**Voordeel segmentatie =>** Maakt het mogelijk veel verschillende communicaties te multiplexen op hezelfde netwerk.

#### Betrouwbaarheid

TCP/IP biedt 2 transportlaagprotocollen:

* TCP (Transmission Control Protocol) **Betrouwbaar**
* UDP (User Datagram Protocol) **Sneller**



#### TCP

Drie verantwoordelijkheden:

1. Gegevenssegmenten nummeren en traceren.
2. Ontvangen gegevens erkennen.
3. Opnieuw verzenden van onbevestigde gegevens na een bepaalde periode.

#### UDP

* Best-effort deliver (onbetrouwbaar)
* No acknowledgment

#### Gepaste transportlaagprotocol voor de juiste toepassing

**Voor wat gebruik maken van TCP?**

Databases, webbrowsers en e-mailclients vereisen dat alle verzonden gegevens op de bestemming in de oorspronkelijke staat terechtkomen.

**Voor wat gebruik je UDP?**

Als 1 of 2 segmenten van een live video stream niet aankomen, kan dat niet merkbaar zijn voor de gebruiker.

### TCP en UDP overzicht

#### TCP-functies

* **Sessie instellen**
* **Betrouwbare levering**
* **Same-order levering**
* **Flow control**

#### TCP Header

Inhoud van TCP Header:

* **Source port en destination port:** identificeert toepassing die info nodig heeft.
* **Sequence number :** Dient voor het opnieuw samenstellen van gegevens.
* **Acknowledgement number:** Geeft aan of het ontvangen is een klaar is voor het volgende segment.
* **Header length:** Lengte van de header.
* **Control bits:** Geeft doel en functie van TCP bits.
* **Window size:** Aantal bytes dat in 1 keer kan worden geaccepteerd.
* **Checksum:** Foutcontrole

#### UDP-functies

* Data reconstrueren in volgorde dat het is ontvangen.
* Verloren segmenten blijven verloren.
* Informeert de zenden niet bij ontvangst

#### UDP Header

#### Meerdere afzonderlijke communicaties

TCP en UDP beheren meerdere conversaties met behulp van unieke id’s = poortnummers.

#### Poortnummers

* Source Port:
  + Oorspronkelijke toepassingspoort die dynamisch wordt gegenereerd door het verzendingsapparaat.
  + Voorbeeld: elke afzonderlijke http-conversatie wordt bijgehouden op basis van de bronpoorten.
* Destination Port:
  + Vertelt de bestemming welke service wordt aangevraagd.
  + Voorbeeld: Port 80 Web Services worden aangevraagd.

#### Socket pairs

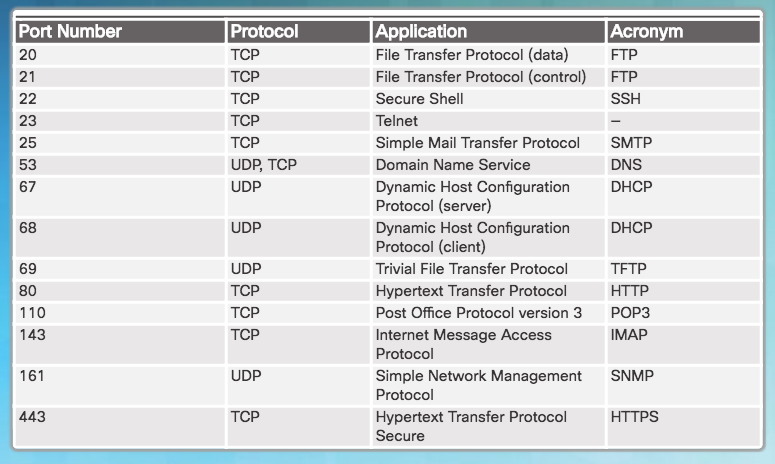
* Source & destination port in segment geplaatst.
* Segmenten ingekapseld in IP-pakket.
* IP en poortnummer = socket.
* Kunnen meerdere processen onderscheiden.
* Source port fungeert als retouradres.

#### Poortnummer groepen

**Goed gekend :** 0-1023

**Geregistreerde poorten :** 10245-49151

**Dynamisch toegewezen poorten :** 49152-65535



ALLEMAAL TE KENNEN

#### Netstat Commando

* Hulpprogramma voor verifiëren van verbindingen.
* IP-adressen proberen omzetten in domeinnamen en poortnummers naar bekende toepassingen.
* -n optie gebruikt om IPs en poorten weer te geven in numerieke vorm.

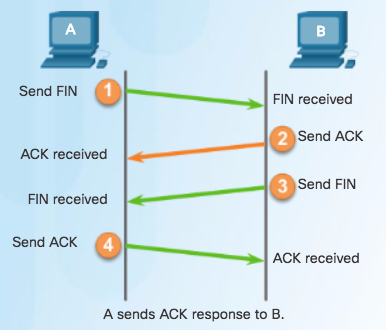
## TCP¨en UDP

### TCP Communicatieproces

#### TCP-verbinding instellen

1. Initiëren van clientverzoeken in sessies bij een server.
2. Server bevestigd en vraagt sessie met client.
3. Client bevestigd communicatiesessie met server.

#### Beëindigen van TCP-sessie



1. Vlag voor voltooien (FIN) moet worden ingesteld in de segment header.
2. Twee richtings-handshake bestaande uit een FIN-segment en een bevestigings (ACK)-segment.
3. Om een enkel TCP-ondersteund gesprek te beëindigen, zijn 4 uitwisselingen nodig om beide zittingen te beëindigen.

#### **Three-way Handshake**

* Bepaalt of doelapparaat aanwezig is op het netwerk.
* Controleert of het doelapparaat een actieve service heeft en accepteert aanvragen op het doelpoortnummer dat de client wil gebruiken.
* Informeert doelapparaat dat bron client een communicatiesessie op dat poortnummer wenst in te stellen.

6 Control bits in het veld “Control bits” van de TCP-Header = **RTS** **flag** en wordt gebruikt om verbinding te resetten wanneer een fout of time-out optreedt.

### Betrouwbaarheid en Flow Control

#### TCP Betrouwbaarheid

TCP is betrouwbaar omdat het volgnummers gebruikt en kan ontbrekende volgnummers nog een keer laten versturen. De ontvangen stuurt telkens een ontvangstbericht en een requestbericht voor het volgende pakketje.

#### Flow Control – Window Size and Acknowledgments

Venstergrootte:

* Bepaalt aantal bytes die verzonden kunnen worden vooraleer een bevestiging ontvangen is.

Acknowledgement number:

* Het te verwachten nummer van de volgende byte.

#### Flow Control – Congestion/Ophoping Avoidance

Er kan in TCP ophoping ontstaan, mogelijke oplossingen zijn:

* Verschillende timers
* Algoritmen
* …

Vb: Het aantal bytes verminderen dat wordt verzonden voordat een bevestiging wordt ontvangen.

### UDP Communicatie

#### UDP lage overhead versus betrouwbaarheid

Verschillen UDP en TCP

* UDP stelt niet eerst een verbinding op vooraleer het data verzendt, maar verstuurd direct de data en cared niet of het al dan niet toekomt. (geen retransmission, sequencing of flow control).

#### UDP Datagram Re-assembly

Hoe gaat UDP data herassembleren?

* In volgorde van ontvangst en stuurt deze zo door naar de toepassing, de toepassing moet zelf de juiste volgorde bepalen.

#### Toepassingen die gebruik maken van TCP

Zie Poortnummergroepen

#### Toepassingen die gebruik maken van UDP

* Live video en multimedia
* Eenvoudig verzoek en antwoord
* Handle reliability themselves

Zie Poortnummergroepen

# Applicatielaag

## Applicatielaag protocollen

### Applicatie, presentatie en sessie

#### Applicatielaag:

* Dichts bij de gebruiker
* Gebruikt om gegevens uit te wisselen tussen programma’s die op bron- en doelhosts worden uitgevoerd.

#### Presentatie- en Sessielaag

**Presentatielaag functies:**

* Gegevens op bronapparaat in compatibele vorm zetten voor ontvangende apparaat
* Gegevens comprimeren
* Gegevens encrypteren

**Sessielaag functies:**

* Creëren en onderhouden van gesprekken tussen bron- en bestemmingsapplicaties

#### TCP/IP Applicatielaagprotocollen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Afkorting** | **Volledige naam protocol** | **Uitleg** | **Werking** | **Poort** |
| DNS | Domain Name Server | Domeinnamen omzetten in ip-adressen | * **1)** Kijken naar eigen records om naam op te lossen * **2)** Contact opnemen met andere servers * **3)** Server slaat IP-adres tijdelijk op in geval dat dezelfde naam opnieuw wordt aangevraagd | TCP UDP 53 |
| BOOTP | Bootstrap Protocol | Wordt vervangen door DHCP |  | / |
| DHCP | Dynamic Host Configuration Protocol | Dynamische toekenning van IP-adressen aan clients | **Client => Server:** DHCPDISCOVER  **Server => Client:** DHCPOFFER  **Client => Server:** DHCPREQUEST  **Server => Client:**  DHCPACK \*\*\* | UDP client 68, server 67 |
| SMTP | Simpler Mail Transport Protocol | Clients kunnen hiermee e-mails verzenden naar e-mailserver |  | TCP 25 |
| POP | Post Office Protocol | Clients kunnen hiermee e-mail ophalen van de e-mailserver | Email wordt gedowload van server naar de client en wordt gewist van de server | TCP 110 |
| IMAP | Internet Message Access Protocol | Clients kunnen hiermee e-mail ophalen van de e-mailserver maar de originele e-mail blijft op de server | Kopieën worden van de server gedownload naar client en originele berichten worden op server bewaard | TCP 143 |
| FTP | File Transfer Protocol | Betrouwbaar, verbindingsgericht en erkend protocol voor bestandsoverdracht | 1. Client maakt eerste verbinding met server voor controleverkeer via TCP-poort 21 2. Client maakt tweede verbinding met server voor effectieve gegevensoverdracht via TCP-Poort 20 | TCP 20 en 21 |
| TFTP | Trivial File Transfer Protocol | Eenvoudig verbindingloos protocol voor bestandsoverdracht |  | UDP 69 |
| HTTP | Hyper Text Transfer Protocol | Set van regels voor het uitwisselen van tekst, afbeeldingen … op het WWW | **GET**- aanvraag voor data  **POST**- Upload bestanden naar webserver  **PUT**- Upload bronnen of inhoud naar webserver | TCP 80, 8080 |
| HTTPS | Hyper Text Transfer Protocol Secure | Gebruikt encryptie om communicatie te beveiligen |  | TCP, UDP 443 |

\*\*\*

DHCPDISCOVER: Broadcast naar DHCP-servers met vraag voor ip-adres.

DHCPOFFER: Voorstel met gegevens, IP, DNS-server, gateway, Subnetmask en lease-time

DHCPREQUEST: De gegevens dat de client wil (meestal = offer) aangevraagd aan de server die de offer heeft gestuurd

DHCPACK: Antwoord of het in orde is of niet.

### Hoe toepassingsprotocollen omgaan met eindegebruikerstoepassingen

#### Client-Server Model

* Client- en serverprocessen worden geacht zich in de applicatielaag te bevinden
* Applicatieprotocollen beschrijven het formaat van de verzoeken en antwoorden tussen clients en servers

#### Peer-to-Peer netwerken

* Gegevens worden benaderd vanaf een peerapparaat zonder gebruik van speciale server
* Elke client kan zowel als server én als client gebruikt worden.

#### Peer-to-Peer applicaties

* P2P-toepassing maakt mogelijk dat apparaat zowel als client als server kan werken binnden dezelfde communicatie
* P2P-toepassingen vereisen dat eindapparaat een GUI heeft en een achtergrondservice uitvoert.

### IP-adresseringsdiensten

#### DNS hiërarchie

#### **Nslookup** commando

* Hulpprogramma waarmee een gebruiker handmatig de naamservers kan doorzoeken om IP-adres van bepaalde host te vinden
* Kan ook gebruikt worden om problemen met naamomzetting op te lossen en om huidige status van nameservers te controleren.

### File Sharing Services

#### Server Message Block

Is een client/server protocol om bestanden te delen:

* SMB-bestandsdeling en afdrukservices zijn pijlers van Microsoft-netwerken geworden
* Clients maken langdurige verbindingen met servers en hebben toegang tot de bronnen op de server alsof die lokaal zijn voor de client.

# Bouw een klein netwerk

## Netwerkontwerp

### Apparaten in een klein netwerk

#### Netwerktopologieën van kleine netwerken

Meestal:

* 1 router
* 1 of meerdere WAPs (Wireless access point)

Beheer van klein netwerk valt te vergelijken met het beheer van een groot netwerk:

* Onderhoud en troubleshooting bestaande apparatuur.
* Beveiliging van apparaten en informatie op netwerk.

Internetverbinding komt tot stand dmv 1WAN-verbinding via DSL, kabel of ethernet.

#### Apparaat-keuze voor een klein netwerk

Factoren om op te letten bij bouwen van een netwerk:

* Prijs
* Snelheid en soorten poorten/interfaces
* Uitbreidingsmogelijkheden
* Besturingssystemen, kenmerken en diensten. (QoS, VolP, Layer 3 switching, NAT, DHCP, beveiliging)

#### IP-adressering van een klein netwerk

* Ip-adresruimte moet worden ingepland bij implementeren van klein netwerk.
* Alle hosts moeten uniek adres hebben.
* Verschillende apparaten in IP-ontwerp zoals eindapparaten, servers, hosts toegankelijk via internet en intermediaire apparaten.

#### **Redundantie** in een klein netwerk

Betrouwbaarheid = belangrijk element. => redundantie zorgt hiervoor.

4 soorten redundantie:

* Server redundantie
* Verbinding redundantie
* Switch redundantie
* Router redundantie

**Redundantie = voorzien van back-up apparaat zodanig dat het netwerk kan blijven functioneren.**

#### Verkeersmanagement

Netwerkverkeer wordt ingedeeld op prioriteit, om productiviteit omhoog te doen gaan en downtime van netwerken tot minimum te beperken.

* + Voice 🡪 hoge prioriteit
  + Video 🡪 hoge prioriteit
  + SMTP 🡪 medium prioriteit
  + Instant Messaging 🡪 normale prioriteit
  + FTP 🡪 lage prioriteit

### Applicaties en protocollen van kleine netwerken

#### Veel voorkomende toepassingen

/

#### Veel voorkomende protocollen

* DNS
* DHCP
* …

#### Stem- en videotoepassingen

Alsmaar meer gebruik IP-telefonie en streaming media om te communiceren in bedrijven.

VoIP-apparaten zetten analoge signalen om in IP-pakketten.

IP-telefonie => IP-telefoon zet zelf spraak naar IP. Voice-enabled router zijn niet vereist in netwerk met geïntegreerde IP-telefonieoplossing. IP-telefoons gebruiken speciale server.

Real-time-toepassingen, het netwerk moet toepassingen kunnen ondersteunen die vertragingsgevoelige aflevering vereist. Hiervoor zijn RTP en RTCP, Realtime transportprotocol en Real- Time Transport Control Protocol.

## Netwerkveiligheid

### Beveiligingsbedreigingen en kwetsbaarheden

#### Soorten bedreigingen

* **Informatiediefstal** (vertrouwelijke info stelen)
* **Verlies en manipulatie van gegevens** (gegevens aanpassen of verwijderen)
* **Identiteitsdiefstal** (persoonlijke informatie die gestolen wordt)
* **Verstoring van de service** (legitieme gebruikers geen toegang op diensten waar ze recht op hebben)

#### Fysieke beveiliging

4 klasse bedreigingen:

* **Hardware-bedreigingen** (fysieke schade)
* **Omgevingsdreigingen** (extreme temperaturen of extreme vochtigheidsgraden)
* **Elektrische bedreigingen** (spanningspieken, onvoldoende voedingsspanning,…)
* **Onderhoudsdreigingen** (slecht gebruik belangrijke elektrische componenten, slechte etikettering,…)

#### Soorten kwetsbaarheden

3 primaire kwetsbaarheden:

* **Technologisch** (onveilige protocollen, zwakheden in OS en netwerkapparatuur)
* **Configuratie** (onbeveiligde accounts of met makkelijk te raden wachtwoorden, verkeerd geconfigureerde netwerkapparatuur)
* **Beveiligingsbeleid** (gebrek aan schriftelijk beveiligingsbeleid, ontoereikende monitoring van het netwerk)

### Netwerkaanvallen

#### Soorten malware

Malware => of malcode = kwadaardige software of code, speciaal ontworpen om schade toe te brengen, te verstoren, te stelen van gegevens,…

* **Virussen** (uitvoerbaar bestand, maakt kopie van zichzelf en maakt deel uit van ander programma, verspreidt zich van pc tot pc)
* **Wormen** (vergelijkbaar met virus, geen host-programma nodig, stand-alone software die profiteren van systeemfuncties om te reizen via het netwerk)
* **Trojaanse paarden** (gebruikers worden misleid bij laden en uitvoeren van deze malware, ze creëren achterdeuren om een derde partij toegang tot het systeem te geven.)

#### Verkenningsaanvallen

Dit is het in kaart brengen van systemen en hun kwetsbaarheden.

Hoe werkt dit?

1. IP adressen bepalen via nslookup of whois.
2. Fping gebruiken om ip-adressen te pingen en te zien wie luistert.
3. Nmap gebruiken om te zien naar welke poorten de ip-adressen luisteren.

#### Toegangsaanvallen

Dit is de manipulatie van gegevens etc.

Verschillende soorten toegangsaanvallen zijn:

* Wachtwoordaanvallen, brute force / trojan horse / packet sniffers.
* Exploitatie van vertrouwen
* Poortomleiding, installeren van software op gehackte host om toegang te krijgen tot een doelhost op andere port.
* Map-in-the-middle, fishing mails,…

#### Denial of Service

Dit is het uitschakelen of beschadigen van netwerken.

Hoe werkt dit?

* Ping of death (heel groot misvormd ping pakket versturen)
* SYN flood: meerder SYN aanvragen sturen naar webserver zodat de server een Threeway handshake wil doen daardoor is de server niet bereikbaar voor andere SYN aanvragen
* DDoS: dmv veel tussenhosts/zombies (vaak met veel malware in) veel aanvragen naar de server te sturen
* Smurf attack: groot aantal ICMP pakketten verzenden

### Remediëringen voor netwerkaanvallen

#### Backup, Upgrade, Update en Patch

* Up-to-date blijven met nieuwste ontwikkelingen = cruciaal voor beveiliging
* Up-to-date blijven met nieuwste versies antivirussoftware
* Beveiligingsupdates van leverancier van OS downloaden en patches op alle kwetsbare systemen installeren
* Gebruik centrale-patch-server om patches automatisch te installeren.

#### Authentication, Authorization, Accounting

= AAA

* Wordt gebruikt om te bepalen wie toegang heeft tot netwerk, wat ze kunnen doen en wat ze deden ze terwijl ze toegang tot het netwerk kregen.

#### Firewalls

Dit is een beveiligingstool die gebruikers beschermt tegen externe bedreigingen.

Verschillende soorten technieken gebruikt door firewalls zijn:

* Packet filtering (authorisatie adhv IP/MAC adressen)
* Application filtering (authorisatie adhv applicatietypen op basis van poortnummers)
* URL filtering (Authorisatie adhv URL’s)
* SPI = Stateful Packet Inspection (Verkeer van buiten firewall moet van hetzelfde interne netwerk komen tenzij specifiek toegestaan)

#### Beveiliging van eindapparaten

Dit zijn de moeilijkst te beveiligen apparaten binnen een netwerk.