# Exploring the network

## Exploring the network

### Introduction

* er zijn veel verschillende soorten netwerken.
* netwerken worden steeds belangrijker in ons leven, we hebben het nodig.

## Globally connected

### Networking today

#### Networks in our daily lives

* Netwerk is overal in ons dagelijks leven, we hebben het nodig.
* We zijn erdoor verbonden.

#### Technology then and now

* Een twintigtal jaar geleden waren de dingen die vandaag doodnormaal zijn niet te bedenken.
* De technologie blijft evolueren en stopt niet.
* IoE internet of everywhere

#### The global community

* netwerk heft mogelijk gemaakt dat men over heel de wereld met iedereen interactie kan hebben
* het moedigt wereldwijde samenwerking aan

#### Networks support the way we learn

* Netwerk heeft een grote invloed op hoe we leren.
* Het overwint geografische grenzen
* Het is enorm uitgebreid. Er kunnen naast de boeken en de lector ook verwijzingen naar het web zijn om meer informatie te krijgen.
* Je kan vragen gewoon posten en met de hele wereld erover discussiëren

#### Networks support the way we communicate

* Instant messaging(IM)/texting: communicatie in het hier en nu
* Social media: interactieve websites met door gebruiker vermelde gegevens
* Collaboration tools: laat toe samen te werken en bestanden te delen, zonder op tijd en plaats te letten. Mensen op afgelegen plaatsen kunnen net zo goed meewerken als anderen.
* Weblogs(blogs): een website die makkelijk aangepast kan worden. Ze zijn van gewone mensen en in bijna alle onderwerpen te vinden.
* Wikis: websites die door een grotere groep mensen bekeken en gewijzigd kan worden. Ze kunnen gemaakt worden door iedereen.
* Podcasting: het verspreiden van audiobestanden (muziek, audiobook, …)
* Peer-to-peer(P2P) file sharing: van gebruiker naar gebruiker verspreiden van bestanden zonder deze van een centrale te halen of erop op te slaan.

#### Networks support the way we work

* Origineel was het netwerk bedoelt om intern informatie te delen.
* Nu is het meer uitgebreid, men bel over het netwerk, mailen, ….

#### Networks support the way we play

* Netwerk laat toe meer te kunnen i.v.m. recreatie. Bv spellen, video, muziek,…. Alles wordt leuker met meer mensen. Deze kunnen overal zijn.

### Providing resources in a network

#### Networks of many sizes

* Een netwerk kan gaan van twee computers tot miljoenen apparaten
* Simple networks: een netwerk binnen huis
* Smal Office Home Office: een netwerk voor iemand die thuis werk of in kleine bedrijven
* Medium to large networks: meestal voor in bedrijven en grote organisaties.
* World wide network: internet. Het betekend netwerk van netwerken

#### Clients and servers

* Host: alle computers die verbonden zijn aan een netwerk. Ze kunnen berichten sturen en ontvangen.
* Server: host met software om informatie te verschaffen aan andere hosts
  + Een computer kan meerdere types serversoftware draaien
* Client: computer hosts met software om informatie op te vragen en te tonen
  + Een computer kan meerdere types clientsoftware draaien

#### Peer to peer

* Een netwerk waar de hosts zowel server als cliënt zijn
* Twee soorten: met twee direct aan elkaar gekoppelde computers of verschillende computers verbonden via een switch.
* Voordelen
  + Makkelijk op te zetten
  + Niet zo complex
  + Lagere kost
  + Kan voor kleine, simpele taken dienen
* Nadelen
  + De prestaties van de host kan traag worden
  + Geen centrale administratie
  + Niet zo veilig
  + Niet goed in te schatten

## LANs, WANs, and the internet

### Components of a network

#### Components of a network

* Een netwerk kan zo simpel zijn als een computer via een kabel gekoppeld aan een andere of zo complex dat het letterlijk de wereld overspant
* Er zijn drie categorieën: apparaten, media en diensten
* Apparaten en media zijn de fysieke elementen of hardware, diensten zijn de software

#### End devices

* Host
* Het is de interface tussen gebruikers en het network
* Computer, laptop, smartphone, printers, …
* Is het begin en eindpunt van een netwerk
* Het heeft een adres zodat het door het netwerk erkend wordt

#### Intermediary network devices

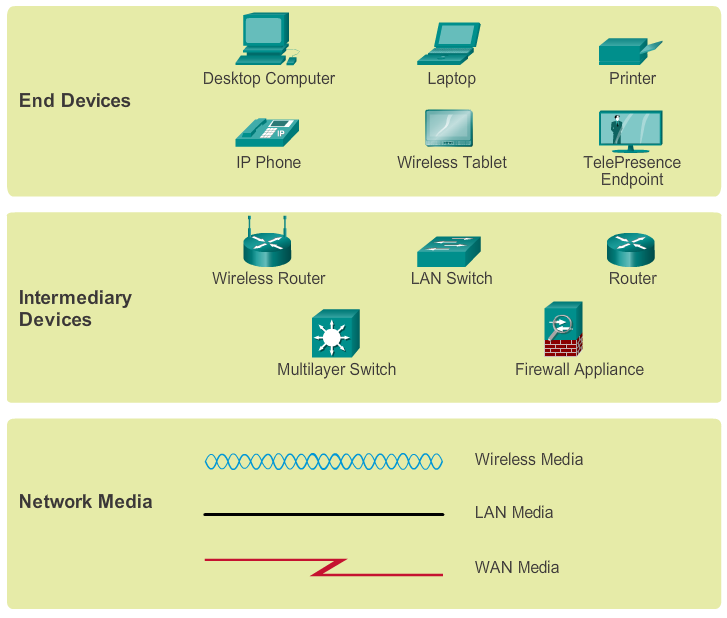
* Verbinden eind apparaten en netwerk. Het geeft verbinding en werkt achter de schermen
* Vb. netwerkverbinding, firewall, …
* Het behandeld de data als het over het netwerk vloeit

#### Network media

* Het medium waarover de communicatie gaat
* 3 soorten: koper, fiber en draadloos

#### Network representations

* Symbolen die gebruikt worden



* Network interface card (NIC): een LAN adapter: geeft de fysieke verbinding tussen het eindstation en het netwerk
* Physical port: een connector op een netwerkapparaat waar het media wordt bevestiging aan een host of ander netwerkapparaat
* Interface: speciale poorten op een internetapparaat dat individuele netwerken verbindt

#### Topology diagrams

* Geeft een visuele map van hoe het network in elkaar zit
* 2 soorten
  + Fysieke topologische diagrammen: geeft de fysieke plaats van het onderdeel weer
  + Logische topologische diagrammen: identificeert apparaten, poorten en IP-adres schema’s

### LANs and WANs

#### Types of networks

* Het type hangt af van
  + Groote van het overkoepeld gebied
  + Aantal verbonden gebuikers
  + Aantal en type van diensten
* Local area network(LAN): in een kleine geografische omgeving
* Wide area network(WAN): in een grote geografische omgeving
* Metropolitan area network(MAN): overspant een gebied dat groter is dan een LAN, maar kleiner is dan een WAN. Meestal voor steden, grote bedrijven
* Wireless LAN(WLAN): hetzelfde als de LAN alleen draadloos
* Storage area network(SAN): een network gespecialiseerd in het ondersteunen van opslagsystemen

#### Local area networks

* Omspannen een klein gebied zoals thuis, op school, op kantoor of op campus
* Meestal beheerd door een organisatie
* Controle en beveiliging gebeuren op netwerk level
* Bied een hoge snelheid aan eindapparaten en intermediaire apparaten

#### Wide area networks

* Op een groot geografisch gebied
* Beheerd door meerdere service providers(SP) of internet service providers(ISP)
* Verbind LAN over grotere geografische gebieden
* Geeft een langzamere verbinding tussen Lans

### The internet

#### The internet

* Internet is om met een bron buiten het eigen netwerk te communiceren
* Internet bestaat uit een serie gekoppelde netwerken
* Informatie wordt gedeeld via veelvoorkomende standaards
* Het is een samenwerking van verschillende netwerk management organisaties (IETF, ICANN,…)
* Internet 🡺 wereld wijde netwerk, internet 🡺 meerdere verbonden netwerken
* protocol 🡺 regels voor communicatie (snelheid, taal, …)
* standard 🡺 meest gebruikte protocol

#### Intranet and extranet

* Intranet
  + Private verzameling verbonden netwerken van een onderneming
  + Gemaakt zodat enkel leden van de organisatie erop kunnen
* Extranet
  + Voor beveiliging en veilig toegang voor individuen die bij een andere organisatie werken maar data van de onderneming nodig hebben

### Connecting to the internet

#### Internet access technologies

* Veel verschillende manieren om op het internet te komen
  + Thuisgebruikers, teleworkers, SOHO:
    - Verbinding met de ISP(Internet service provider):
      * Breedband kabel (Telenet)
      * broadband digital subscriber line (DSL) (Belgacom)
      * draadloos WAN
      * Mobile services
  + Organisaties
    - Verbinding via een SP(service provider)
      * Verbinding met Internet en andere bedrijfssites
      * Snelle connectie
      * Voor IP telefoons, video conferentie en data opslag
      * Meestal zakelijk DSL, gehuurde lijnen en metro ethernet

#### Connecting remote users to the internet

* Kabel
  + Het data signaal wordt verzonden via de kabel van de kabeltelevisie
  + Hoge bandbreedte, altijd aan, verbonden aan het internet
  + Speciale modem om het internet en andere signalen te splitsen
  + Met een ethernetkabel verbonden voor een LAN
* DSL
  + Hoge bandbreedte, altijd aan, verbonden aan het internet
  + Modem splitst het data verkeer van het telefoonverkeer
  + Met een ethernetkabel verbonden voor een LAN
  + Drie kanalen: een telefoon, een download en een upload kanaal
  + Digital Subscriber Lines
* Mobiel
  + Via het gsm netwerk
  + Gelimiteerde prestaties
  + Vooral goed voor afgelegen gebieden en mensen die zich steeds verplaatsen
* Satelliet
  + Voor mensen die geen toegang hebben tot DSL of kabel
  + De schotel vereist een zuiver zich op de satelliet
  + Vooral goed voor afgelegen gebieden
* Bel telefoon
  + Niet voor groot dataverkeer
  + Alleen als de andere opties niet kunnen
  + Goedkoop, lage snelheid
* Fiber verbinding
  + Futuristisch
  + Heel hoge snelheid

#### Connecting businesses to the internet

* Hebben hogere en zekerdere bandbreedte nodig, evenals management services
* Dedicated leased line:
  + Zekere verbinding
  + Gereserveerde lijnen die geografische gescheiden kantoren verbinden
* Metro ethernet:
  + Niet wijd verspreid
  + Over een koper of glasvezelverbinding
  + Beperkt door afstand
* DSL
  + In verschillende formaten
  + Symmetric Digital Subscriber Lines (SDSL) (dezelfde upload en downloadsnelheid)
  + Asymmetric Digital Subscriber Line (ADSL)
* Satelliet
  + Verbinding waar een bekabelde verbinding niet mogelijk is
  + Kan duur zijn
  + Trager en minder betrouwbaar

## The network as a platform

### Converged networks

#### The converging network

* Vroeger:
  + een toegewijd netwerk voor elke dienst
  + gelimiteerd in het verzenden van data tussen verbonden apparaten
  + telefoon, data en tv-signalen hebben elk een eigen kabel, een eigen toegewijd netwerk
  + elke dienst had een eigen set regels en standaarden
* nu:
  + geconvergeerd netwerken
  + de diensten worden versterkt, hechter gemaakt
  + het netwerk is in staat om verschillende diensten over hetzelfde netwerk te sturen
  + er kunnen veel verschillende eindaparaten zijn
  + er geldt maar een set regels voor heel het netwerk

#### Planning for the future

* Netwerken zijn en zullen blijven evolueren
* Niet allen hechter maken van de verschillende soorten berichten/data, ook de applicaties die de berichten genereren, versturen en beveiligen hechter maken op geïntegreerde netwerken
* Resultaat is dat het communicatieplatform hoge kwaliteit levert tegen een lage prijs
* De snelheid van de ontwikkeling van het bestaande netwerk is te wijden aan de snelle groei en uitbreiding van het internet, en het potentieel van het IoE
* De redenen die deze explosieve groei veroorzaken hebben, hebben geresulteerd in een netwerk dat kan groeien en veranderingen kunnen ondersteunen. Het internet moet zich continu aanpassen om aan de standaards te kunnen blijven voldoen.

### Reliable network

#### The supporting network architecture

* Fysieke architectuur: de kabels en apparaten
* Netwerk architectuur: de technologie die de infrastructuur en de geprogrammeerde apparaten, regels en/of protocollen
* Vier onderdelen
  + Fouttolerantie
  + schaalbaarheid
  + Quality of service (QoS)
  + veiligheid

#### Fault tolerance in circuit switched networks

* Fout tolerantie
  + Een netwerk moet altijd beschikbaar zijn
  + Een netwerk dat ontworpen is om zo min mogelijk aantal apparaten te treffen en zo min mogelijke schade/impact bij een fout te hebben
  + Zo snel mogelijk herstellen indien een fout gebeurt, ze vertrouwen op een netwerk aan verschillende paden tussen bron en doel
  + Redundancy: meerdere paden hebben om data/berichten over te verzenden
* Circuit-switched connection-oriented networks
  + Vergelijkbaar met een oud telefoonsysteem
  + Je belde, de oproep onderging een opzet proces (welke verbindingen zijn er tussen ontvanger en verzender) , een tijdelijk pad werd opgesteld. Als het pad mislukte moet er een nieuwe oproep en nieuwe route gemaakt worden
  + De prioriteit wordt gegeven aan bestaande connecties, zolang de verbinding niet verbroken wordt, wordt het pad ook niet opgebroken
  + Niet optimaal voor het internet wegens de beperkt aantal paden die gecreëerd kunnen worden

#### Fault tolerance in packet-switched networks

* Packet-switched networks
  + Data wordt in stukken opgedeeld met het begin- en eindpunt
  + Die stukjes kunnen elk over een ander pad verzonden worden, eenmaal aangekomen bij de bestemming worden ze terug aan elkaar gerijgd
  + De tussenapparaten weten niets van de inhoud enkel het bron en bestemming adres: IP-adres: in decimale met punten vorm (10.10.10.10)
  + Indien een pakket niet kan geleverd worden, wordt het via een andere weg opnieuw verzonden
  + Zo werkt het internet

#### Scalable networks

* Een netwerk dat zich kan aanpassen aan de vraag, zonder de prestaties te beïnvloeden
* Het internet is opgebouwd in een hiërarchische structuur
  + Boomstructuur (wortels en onder vertakkingen)
  + Elke vertakking is verantwoordelijk voor een deel van de hiërarchie
  + Om het hoofdnetwerk te ontzien van data die er niet hoeft te zijn
  + Het betekend ook dat het netwerk bekwaam is om nieuwe producten en applicaties te accepteren
  + Alle individuele netwerken werken samen om zo het internet staande te houden volgen dezelfde protocollen en standaards

#### Providing QoS (Quality of Service)

* Verschillende soorten verkeer met verschillende prioriteiten
* Een verhoogde vereiste
* Netwerken moeten voorspelbaar, meetbare soms gegarandeerde services bieden. Dit is niet altijd het geval. Bij packet-switched is zelfs niet zeker of alles wel aankomt
* Netwerken moeten ook over mechanisme beschikken om overbelast netwerkverkeer te beheren
* Hoeveel data kan verzonden worden binnen een seconde: Gemeten in bits per seconde (bandbreedte)
* Bij overbelasting krijgt het netwerk meer binnen dan dat ze kan verzenden
* De data pakketten komen in wachtrijen te staan, die vullen zich tot ze vol zijn. Dan pas worden er pakketten gedropt
* Door de vertraging en verlies van pakketten te beheren verkrijgt men de nodige QoS
* De pakketten worden geclassificeerd naar belang/prioriteit per groep worden de pakketten hetzelfde behandeld
* Soorten prioriteiten
  + Tijdsgevoelige data, Belangrijke bedrijfsdocumenten 🡪 hoge prioriteit
  + Niet-tijdgevoelige data, Ongewenste communicatie 🡪 lage prioriteit

#### Providing network security

* Twee netwerk beveiligingszorgen
  + infrastructurele beveiliging
    - Fysiek beveiligen van de apparatuur
    - Beveiligen tegen inbreuk op de software van deze apparatuur
  + informatiebeveiliging
    - het beveiligen van de informatie die over het netwerk lopen
    - het beveiligen van de informatie die op de op het netwerk aangesloten apparatuur staan
* beveiliging moet zorg dat
  + ongeautoriseerde toegang voorkomen
  + gegevensdiefstal voorkomen
  + ongeautoriseerde wijziging van gegevens voorkomen
  + (Denial of Service)weigering van dienst voorkomen
* drie primaire eisen om het netwerk te beveiligen
  + vertrouwelijkheid
    - alleen de bedoelde en toegestane afnemers(mensen, processen of apparaten) krijgen toegang tot de data
    - via gebruikers na te trekken, moeilijkere wachtwoorden en versleutelde gegevens
  + communicatie integriteit
    - gegevens niet gewijzigd onderweg van bron tot bestemming
    - geen beschadigde data (gemoedwillig of niet)
    - mogelijk gemaakt door validatie van de data
  + beschikbaarheid
    - zekerheid van tijdige en betrouwbare toegang tot de gegevens voor de geautoriseerde gebruikers
    - desktop antivirus, serverantivirus, netwerk firewall
  + netwerken bouwen met weinig faalpunten kunnen deze bedreigingen verminderen

## The changing network environment

### Network trends

#### New trends

* Hoe het internet wordt gebruikt is sterk verandert en zal blijven veranderen
* Video
* Cloud computing

#### BYOD

* Bring your own device
* Hoe langer hoe meer apparaten verbonden zijn via het internet en elke toepassing moeten kunnen gebruiken op ieder moment (any device, to any content, any way)
* Overal verbonden met het netwerk

#### Online collaboration

* Samenwerken met andere aan een project via het internet
* Zonder kijken naar fysieke positie

#### Video communication

* Dit blijft belangrijker worden zowel voor bedrijven als voor particulieren
* Gaat over culturele en geografische grenzen heen
* Video on demand, video conferenties, live TV,…

#### Cloud computing

* Het gebruik van computermiddelen al een dienst over het netwerk
* De lokale gebruiker moet hierdoor niet meer het zware liften doen
* Opslaan en bereiken van gegevens/data
* Web gebaseerd computeren, zonder software op de computer te moeten zetten
  + Online banking, online retail stores, online music downloading
* Soorten: publieke, private, aangepaste en hybride (bestaande uit meerdere clouds) clouds
* Mogelijke voordelen
  + Fexibel (overal toegankelijk)
  + Wendbaarheid en snelle tewerkstelling (focussen op het gereedschap om te analyseren, delen van gegevens, …)
  + Verlaagt de kost van de infrastructuur
  + Herlegt de focus op IT bronnen
  + Creëren van nieuwe bedrijfsmodellen
* IaaS: Infrastructure as a Service (connectie met viruele hardware)
* PaaS: Platform as a Service( al seen platform op de viruele hardware)
* SaaS: Software as a Service(geeft toegang tot applicaties, zonder iets te moeten instaleren)

#### Data centers

* Nodig door cloud computing
* Een plaats gebruikt om computers, servers te houden en
  + Overtollige dataverbindingen
  + Hogesnelheid virtuele servers
  + Overbodige opslagsystemen
  + Overtollige of back-up stroom voorraden
  + Milieucontroles
  + Beveiligingsapparaten
* Kan een kamer zijn, maar net zo goed een heel gebouw

### Networking technologies for the home

#### Technology trends in the home

* Intelligentie verbonden aan zowat alles in je huis. Melk op? Sms ga melk halen!, eten klaar, …

#### Powerline networking

* Gebruik maken van de bestaande stroomkabel voor het verspreiden van het netwerk

#### Wireless broadband

* Via een antenne verbinding maken met een WISP (wireless internet service provider) i.p.v. bekabeld een verbinding met de ISP
* Wireless broadband service
  + Gsm netwerken als basis voor je verbinding met de ISP

### Network security

#### Security threats

* Beveiliging zijn een essentieel deel van huidige netwerken en applicaties
* Bedreigingen
  + Virussen, wormen, en Trojaanse paarden: kwaadaardige software op de pc van de gebruiker
  + Spyware en adware: software die stiekem informatie steelt van de gebruikers
  + Zero-day attacks (zero-hour attacks): aanval die gebeurt op de eerste dag dat een zwak punt gevonden werd.
  + Hacker aanvallen: een aanval van een persoon met kennis van gebruikersapparaten of netwerkbronnen
  + Denial of service aanval: aanvallen ontworpen om applicaties te vertragen/crashen op een netwerkapparaat
  + Data interception and theft: een aanval om persoonlijke gegevens te stelen van een bedrijf
  + Identity theft: een aanval om logingegevens te stelen om toegang te krijgen op privé gegevens
* Er kunnen evengoed interne bedreigingen zijn ( mees voorkomende veiligheidsschending)
  + Gestolen apparaten, mis gebruik door werknemers, …

#### Security solutions

* Meerdere oplossingen gebruiken, geen elke kan alle bedreigingen tegengaan
* Mogelijke netwerk beveiligingsmogelijkheden
  + Antivirus, antispyware: tegen kwaadaardige software
  + Firewall filtering: blokkeert geauthentiseerde toegang tot het netwerk
  + Dedicated firewall systems: voor gevorderde firewall capaciteit
  + Access control lists(ACL): om toegang te filteren
  + Intrusion prevention systems(IPS): om snel verspreidende bedreigingen te identificeren
  + Virtual private networks(VPN): geeft beveiligde toegang aan afgelegen werknemers

### Network architectures

#### Cisco network architectures

* Netwerken zijn al enorm geëvalueerd en zullen moeten blijven evalueren
* De basis ligt bij het begrijpen van de noden en onderliggende structuur

#### CCNA

* Achieving Cisco Certified Network Associate (CCNA)

# Configuring a Network Operating System

## Configuring a Network Operating System

### Introduction

#### Introduction to cisco IOS

* Thuis netwerk
  + Verbind PCs, laptops, tablets, smartphones, smart TVs, Digital Living Network Alliance (DLNA),…
  + Alles in huis is verbonden met de thuis router(router, switch, wireless acces point, firewall)
    - Router: stuurt data door en ontvangt data van het internet
    - Switch: verbind eindapparaten via netwerkkabels
    - draadloos toegangspunt een radiozender geschikt voor het verbinden van eindapparaten
    - firewall appliance: beveiligt uitgaand verkeer en beperkt inkomend verkeer
* bedrijfsnetwerk
  + veel meer data verkeer
  + gebruik van verschillende alleenstaande toegewijde apparaten met elk hun eigen primaire functies
    - toegewijd: focus ligt op de eigen functie
    - toegewijde firewall: een apart apparaat dat enkel de firewall dienst doet
* alle apparaten hebben een operating system nodig om de hardware te laten werken
  + NOS network operating system

## IOS Boot camp

### Cisco IOS

#### Operating systems

* Pc boots
  + Operating system (OS) wordt van de harde schijf in het ram-geheugen opgeslagen
    - Deel dat communiceert met de hardware: kennel(drivers)
    - Deel dat communiceert met de software/gebruikers = shell
    - Gebruiker communiceert met de shell via
      * Command Line Interface (CLI)
      * Graphical User Interface (GUI)
* De meeste eindaparaten zijn toegankelijk via een GUI
* Switch of router internetwork operating systems biedenopties om:
  + Interfaces te converteren
  + Routing en swiching functies in te schakelen
* Alle netwerkapparaten komen standaard met een default IOS
* IOS versie is altijd upgrade baar
* Thuis routeer OS 🡪 firmware

#### Purpose of OS

* Pc OS (windows, OS X, …) gebruiken technische functies die
  + Het gebruik van een muis toelaten
  + Het resultaat weergeeft
  + Toelaat tekst in te voeren
  + Opties in een dialoogvenster toelaat te selecteren
* Switch of router IOS voorzien opties om:
  + Interfaces te configureren
  + Routing en swiching functies in te schakelen
* Alle netwerkapparaten komen standaard met een default IOS
* IOS versie is altijd upgrade baar

#### Location of the Cisco IOS

* De Cisco IOS zit in de flash
  + Non-volatile storage: niet kwijt indiende stroom wegvalt
  + Kan veranderd/overschreven worden indien nodig
  + Er kunnen meerdere versies van de IOS op opgeslagen worden
  + De IOS wordt naar het vluchtig RAM-geheugen worden gekopieerd
  + De kwaliteit van de flash en RAM geheugenbepalen de IOS die gebruikt kan worden

#### IOS functions

* De grootste functies van de routers en switchen zijn:
  + Beveiliging
  + Routing
  + QoS
  + Adressering
  + Bronnen beheren
  + Interface configuratie

### Accessing a cisco IOS device

* Meest gebruikte manier: console, Telnet of SSH en aux poort

#### Console access method

* Indien er nog geen netwerkdiensten zijn geconfigureerd
* Een speciale consolekabel
* Laat toe configuratie commando’s in te geven
* Zou geconfigureerd moeten worden met wachtwoorden tegen ongeautoriseerde toegang
* Het apparaat zou in een veilige kamer moeten staan zodat de console poort niet makkelijk toegankelijk is

#### Telnet, SSH, and AUX access methods

* telnet
  + op afstand contact maken met de CLI over een netwerk
  + er is een actieve interface en actieve netwerkdiensten nodig, beide geconfigureerd
* secure shell (SSH)
  + maak op afstand contact met de CLI net als het Telnet, elke meer beveiligd
  + sterkere wachtwoord authenticatie
  + gebruikt encryptie bij het transporteren van data
* aux port
  + out-of-band connective
  + gebruikt de telefoonlijn
  + gebruikt zoals de consolepoort

#### Terminal emulation programs

* er zijn verschillende softwaremogelijkheden om verbinding te maken met een netwerkapparaat
  + putty
  + tera term
  + …

### Navigating the IOS

#### Cisco IOS modes of Operation

* Verschillende modes van de IOS
* Dit is in hierarchische structuur
  + User executive (User EXEC) mode
  + Privileged executive (Privileged EXEC) mode
  + Global configuration mode
  + Andere specifieke configuratie modes, zoals de interface voor de configuratie mode
* Iedere mode heeft zijn taken en instellingen

#### Primary modes

* User EXEC mode
  + Gelimiteerde kapaciteiten, voor basis operaties
  + > op het einde van het commando
* Privileged EXEC Mode
  + Eerst user EXEC mode daarna pas privileged EXEC Mode
  + # op het einde van het commando

#### Global configuration mode and sub modes

* Vanaf de privileged
* Global Configuration Mode
  + Modus onder de privileged mode
* Specific Configuration Modes
  + Sub-configuratie modes die elk toelaten een deel van de IOS te configureren
    - Interface mode: om een van de interfaces te configureren
    - Line mode: een van de viruele of fysieke lijnen te configureren
* Command Prompts
  + Bij CLI, de mode die geïdentificeerd door de command line prompt is, is uniek

#### Navigating between IOS models

* Door de enable en disable commando
  + Enable: ga naar de privileged EXEC
  + Disable ga terug naar de user EXEC
* Van en naar global configuratie mode en sub modes
  + Exit: van globaal configuratie naar privileged EXEC mode
  + End: van een sub mode van de privileged EXEC naar de privileged EXEC of Ctrl + Z

### The command structure

#### IOS command structure

* Prompt command space keyword or argument
* Commandos zijn niet hoofdlettergevoelig

#### Cisco IOS command reference

* Syntax: meest gedetailleerde versie van de syntax voor een commando
* Default: hoe het apparaat standard is ingesteld
* Mode: de configuratie mode waar het commando wordt ingevoerd
* History: beschrijvingen van hoe een commando is geïmplementeerd t.o.v. het IOS
* Usage Guide Lines: richtlijnen hoe een commando moet worden ingegeven
* Examples: laten situaties zien waar de commando’s gebruikt kunnen worden

#### Context-sensitive help

* Verschillende soorten hulp mogelijk
* Commando? Geeft een lijst met alle commando die zo beginnen

#### Command syntax check

* De command line interpreteer leest het commando en geen commentaar als het commando juist is. Als het niet juist is of niet leesbaar komt er commentaar over

#### Hot keys and shortcuts

* Tab: vervolledigt de rest van het commando
* Ctrl-R: laat een lijn opnieuw zien
* Ctrl-A: verplaatst de cursor naar het begin van de lijn
* Ctrl-Z: verlaat de configuratie mode en keert terug naar de user EXEC
* Down Arrow: laat toe doorgaande door de voorgaande commando te zoeken
* Up Arrow: laat toe teruggaande door de voorgaande commando te zoeken
* Ctrl-Shift-6: laat toe een IOS proces te onderbreken
* Ctrl-C: verlaat de huidige commando en verlaat de configuratiemode

#### IOS examination commands

* Show commando

#### The show version command

* Geeft informatie over het huidig geladen IOS system, samen met de informatie van de hardware

## Getting basic

### Hostnames

#### Why the switch

* Een van de simpelste apparaten
* Focussen op
  + Een twee pc network via een switch
  + Een naam aan de switch geven
  + De toegang tot de configuratie van de switch limiteren
  + Berichten configureren
  + De configuratie opslaan

#### Device names

* Naam moet uniek zijn
* Richtlijnen
  + Naam start met een letter
  + Geen spaties in de naam
  + Eindigt met een letter of een cijfer
  + Enkel gebruik maken van letters, cijfers en streepjes
  + Korter dan 64 karakters
* Zonder naam zijn de apparaten moeilijk te configureren

#### Hostnames

* Laten toe dat apparaten geïdentificeerd kunnen worden door netwerkadministrators over een netwerk of het internet

#### Configuring hostnames

* Host name 🡪 naam van de switch verandert in naam

### Limiting access to device configurations

#### Securing device access

* Wachtwoorden
  + Enable password: limiteert de toegang tot de privileged EXEC mode
  + Enable secret: encrypteert en limiteert de toegang tot de privileged EXEC mode
  + Console password: limiteert apparaat toegang via de console connectie
  + VTY password: limiteert apparaat toegang via de Telnet verbinding

#### Securing privileged EXEC access

* Gebruik het enable secret commando, niet het oudere enable password commando
* Enable secret geeft meer veiligheid wegens dat het geëncrypteerd is

#### Securing user EXEC access

* Console poort moet beveiligt zijn
  + Dit verkleint de kans dat ongeautoriseerd personeel fysieke verbinding kan maken met het apparaat en zou gegevens krijgt
* VTY lijnen laten toegang tot een Cisco apparaat toe via Telnet
  + Het aantal lijnen dat ondersteund wordt varieert va, het type en de IOS versie af

#### Encrypting password display

* Verhindert dat wachtwoorden tevoorschijn komen als gewone tekst in de configuratie
* Dit dient om ongeautoriseerde individuelen te verhinderen om de wachtwoorden in de configuratiefile te zien
* Eens toegepast, doet het verwijderen van de encryptie dienst niet de encryptie omkeren

#### Banner messages

* Belangrijk deel van het legale proces indien er iemand op het apparaat inbreekt
* Formuleringen die impliceren dat een login welkom of uitgenodigd wordt is uit den boze
* Vaak gebruikt om juridische kennisgeving, omdat deze wordt getoond aan alle aangesloten terminals

### Saving configurations

#### Configuration files

* Switch reload
  + System configuratie was aangepast. Opslaan?
* Opstart configuratie is verwijdert met gebruik van de erase startup-config
* Op de switch is ook het probleem van verwijder vlan.dat
  + Verwijder filenaam?
  + Verwijder flash: filenaam?

#### Capturing text

* De configuratiefiles kunnen ook opgeslagen worden als tekstfiles
* Een configuratiefile kan gekopieerd worden van opslag naar een apparaat

## Address schemes

### Ports and addresses

#### IP addressing of devices

* Elk eindapparaat moet een IP-adres hebben
* De structuur van een IPv4 adres heet dotted decimal
* IP-adres wordt in decimale vorm weergegeven (4 cijfers tussen 0 en 255)
* Met een IP-adres is een subnet makser nodig
* IP-adressen kunnen toegewezen worden aan zowel een fysieke poort als een virtuele interface

#### Interfaces and ports

* Netwerkcommunicatie hangt af van eindgebruiker apparaat, netwerk interfaceapparaat, en de kabels die hun verbinden
* Enkele types van netwerkmedia zijn koperen kabels, fiber kabels, coax kabels of draadloos
* Elk soort netwerkmedia heeft zijn voor- en nadelen
* Ethernet is het meest voorkomende LAN
* Ethernet poorten zijn te vinden op eindgebruiker apparaten, switchen, en andere netwerkapparaten
* Cisco IOS switchen hebben fysieke poorten maar ook switch virtuele interfaces (SVI)
* SVI bied de mogelijkheid om een switch op afstand te beheren

### Addressing devices

#### Configuring a switch virtual interface

* IP-adres: samen met een subnet masker, uniek, identificeert eind apparaten op het internetwerk
* Subnet mask: beslist welk deel van het netwerk gebruikt wordt bij het IP-adres
* Interface VLAN1: interface configuratie modus
* IP-adres 192.168.10.2 255.255.255.0: configureert het IP-adres en het subnet masker voor de switch
* No shutdown: zet de interface administratief aan
* Switches hebben nog steeds fysieke geconfigureerde poorten en VTY lijnen nodig om op afstand de switch te beheren

#### Manual IP address configuration for end devices

* Te vinden bij de pc instellingen
* Ook DNS server en default gateway kunnen hier worden ingesteld
* DNS vertaalt IP-adressen naar webadressen

#### Automatic IP address configuration for end devices

* Dynamic Host Configuration Protocol (DHCP)
* Automatisch toekennen van de IP-adressen

#### IP address conflicts

* Er kunnen twee IP-adressen voorkomen indien een apparaat een handmatig en een ander apparaat een automatisch IP-adres heeft. Dit levert conflicten, wie is wie?

### Verifying connectivity

#### Test the loopback address on an end device

* Commando ping wordt gebruikt op een gereserveerd adres(loopback)

#### Testing the interface assignment

* Er zijn ook commando’s voor het verifiëren van de interfaces van intermediaire apparaten
* Show IP interface brief

#### Testing end-to-end connectivity

* Pc naar switch verbinding
  + Ook hier kan het commando ping gebruikt worden
* Eind naar eind verbinding
  + Ook hier kan het commando ping gebruikt worden

# Network Protocols and Communications

## Rules of Communication

### The Rules

#### What is Communication?

* Netwerken verbinden ons
  + De netwerkindustrie gebruikt registers om te bepalen hoe de communicatie verloopt
  + Registers verdelen communicatie in stukken in verschillende lagen
  + Een aantal internationale organisaties zijn verantwoordelijk voor elke laag
* Communicatie over een netwerk is gelijkaardig aan communicatie tussen mensen
  + Mensen moeten erover eens worden hoe te communiceren, Ze maken hier regels over
  + Protocol: regels om te communiceren
* Menselijke communicatie
  + Identificeer met wie je aan het spreken bent
  + Kies een overeenkomende taal en grammatica
  + Kom overeen over snelheid en timing van het bericht
  + Kom overeen over de bevestiging en aanvaarding van de regels

#### Establishing the Rules

* Pc’s gebruiken dezelfde regels/principes als mensen

#### Message Encoding

* Confereert info in een andere vorm voor transport
* Mensen beschrijven vormen, geluiden, …
* Pc’s transformeren bv een email in een elektrische signalen

#### Message Formatting and Encapsulation

* Hoe de data verzenden naar de ontvanger
  + Mensen sturen brieven volgens een bepaald register (inleiding, midden, slot)
    - Brieven steken in een envelop met de gegevens van ontvanger en zender
  + Pc’s gebruiken hetzelfde principe
    - Elk data deel moet een ontvanger en een verstuurder hebben
* Encapsulation: een formaat van het bericht in een ander formaat stoppen

#### Message Size

* Data moet een bepaalde groter hebben
  + Mensen praten in zinnen, niet te lang en niet te kort
  + Pc’s breken data in stukken, niet te lang, niet te kort
  + Indien niet in stukken gebroken kunnen er stukken niet opgevangen worden

#### Message Timing

* access method
  + Mensen: als je spreekt: als je tegelijk spreekt 🡪 botsing, misverstanden
  + Pc’s: ze moeten vereenkomen wanneer een apparaat een medium mag gebruiken, ander ontstaat een botsing
* Flow control
  + Mensen: hoe snel of langzaam moet je spreken
  + Pc’s: als de data te snel komt kan de pc een beetje data missen omdat de pc de kabel leest op een bepaalde snelheid (niet constant)
* Response time-out
  + Mensen: als er een vraag wordt gesteld en er komt geen antwoord 🡪 stel de vraag opnieuw
  + Pc’s: willen een bevestiging dat de data gearriveerd is, anders wordt de data opnieuw verzonden

#### Message Delivery Options

* Unicast: 1 op 1 communicatie
* Multicast: 1 op een groep communicatie
* Broadcast: 1 op iedereen communicatie

## Network Protocols and Standards

### Protocols

#### Protocols: Rules that Govern Communications

* Net zoals bij mensen moeten computer protocollen kunnen samenwerken voor een goede communicatie
  + Protocol suite: een groep van protocollen die samen werken
  + Het is als een stapel: de bovenste laag is afhankelijk van de onderliggende lagen
    - Lagere lagen 🡪 sturen de data over het netwerk
    - Hogere lagen 🡪 focust op de inhoud van de boodschap
* Waarom lagen
  + Deelt het complexe communicatiemodel in kleinere stukken
  + Elk deel is verantwoordelijk voor een deel van het communicatieproces

#### Network Protocols

* Ze defineren bv
  + Hoe de boodschap is geformatteerd of gestructureerd
  + Het proces waarbij netwerkende apparaten informatie delen over paden met andere netwerken
  + Hoe en wanneer fout en systeemberichten doorgegeven worden tussen apparaten
  + De opzet en beëindiging van datasessies

#### Interaction of Protocols

* Enkele voorbeelden van protocollen die geschikt zijn in netwerk communicatie  
  communicatie tussen PC en webserver: TCP/IP protocol stack
  + Application Protocol: Hypertext Transfer Protocol (HTTP)
    - Neemt data van de pc en steekt het in HTTP formaat om met de webserver te kunnen communiceren
  + Transport protocol: Transmission Control Protocol (TCP)
    - HTTP data wordt omgezet in een TCP segment, de taal voor betrouwbaar transport over een netwerk
  + Internet Protocol: Internet Protocol(IP)
    - TCP data wordt in een IP pakket gestoken, de taal om te transporteren naar een ander netwerk
  + Network Access Protocols: Data Link & Physical layers (Ethernet)
    - IP data wordt in een Ethernet frame gestoken (indien ethernet het gekozen medium is) en vertaald van bits naar elektrische signalen (de taal van communiceren over de draad)

### Protocol Suites

#### Protocol Suites and Industry Standards

* Er zijn verschillende protocol suites voor elektronische communicatie
  + Sommige zijn gepatenteerd, andere zijn dat niet
  + TCP/IP (TCP over IP) is de belangrijkste/meest gebruikte

#### Creation of the Internet and Development of TCP/IP

#### TCP/IP Protocol Suite and Communication Process

* TCP/IP is de meest belangrijke protocol suite
* Enkele veelvoorkomende protocollen in verschillende lagen
  + Applicatie laag
    - Naamsysteem:
      * DNS: vertaalt domeinnamen in een IP-adres
    - Host config:
      * BOOTP: laat een werkstation toe om zijn eigen IP-adres te ontdekken, het IP-adres van een BOOTP server te ontdekken en een bestand in het geheugen te laden om het apparaat te starten
      * DHCP: doet dynamisch IP-adressen toewijzen aan cliënt stations bij de start-up en laat toe adressen te hergebruiken wanneer deze niet meer nodig zijn
    - Email:
      * SMTP: laat een gebruiker een email sturen naar een mailserver, en laat een server een mails sturen aan een ander server
      * POP: laat toe dat een gebruiker email ontvangt van een server en download de e-mails van de server naar de pc
      * IMAP: laat toe dat gebruikers toegang hebben tot emailservers en onderhoud de e-mails op de server
    - File transfer:
      * FTP: sets van regels die toelaten dat de gebruiker om op een host toegang te krijgen en bestanden over te zetten van en naar een andere host
      * ITFTP: een simpel, connectie loos bestand verzendt protocol
    - Web:
      * HTTP: stel regels voor het verzenden van tekst, afbeeldingen, geluid, video en andere multimedia bestanden naar het Internet
  + Transport laag
    - UDP: laat toe een proces te runnen op een host om pakketten te sturen naar een proces dat op een andere host runt, geeft niet weer of de pakketten succesvol zijn ontvangen
    - TCP: laat toe een proces te runnen op een host om pakketten te sturen naar een proces dat op een andere host runt, geeft weer of de pakketten succesvol zijn ontvangen
  + internet laag
    - IP:
      * IP: ontvangt berichtsegmenten van de transprot laag, steekt berichten in pakketten en adresseert de pakketten voor end-to-end bezorging over Internet
      * NAT: (network adress translation) vertaald IP adressen van een privé netwerk naar globale unieke IP adressen
    - IP support:
      * ICMP: geeft feedback van de bestemming aan de verzender over fouten in de ontvangen pakketten
    - Routing protocols:
    - OSPF: hiërarchisch ontworpen gebaseerd op regio’s, open standaard
    - EIGRP: protocol van cisco
  + Netwerk toegang laag
    - ARP: zorgt voor een dynamische mapping van een IP adres en een hardware adres
    - PPP: geeft een manier van encapsulatie van pakketten voor transport over een seriële link
    - Ethernet: bepaalt de regels voor bedrade en signalerende standaards op de netwerk toegang laag
    - interface drivers: geeft de regels op een machine voor de controle van een specifieke interface op een netwerk
* Encapsulation
  + Het proces van een stuk data te nemen en het vertalen naar het juiste protocol
  + Het naar het onderliggende laag sturen
  + Die laag neemt het hele stuk en encapsuleert het in een stuk data volgens het protocol van die specifieke laag en stuurt het naar zijn onderliggende laag, tot het verstuurt kan worden
* PDU(Protocol data unit)
  + De naam van het stuk data in die specifieke laag
  + Ethernet frame, IP packet, TCP segment

### Standards Organizations

#### Open Standards

* Moedigen wedijveren en inovatie aan
  + Geen enkel product kan alleen aanbieder zijn op de markt
  + voorbeeld het bekijken van een webpagina: alle besturingssystemen gebruiken dezelfde lagen en principes, enkel de top laag is anders per OS
* standaard organisaties zijn de baas over volgende standaards
  + The Internet Society (ISOC)
  + The Internet Architecture Board (IAB)
  + The Internet Engineering Task Force (IETF)
  + The Institute of Electrical and Electronics Engineers (IEEE)
  + The International Organization for Standardization (ISO)

#### ISOC, IAB, and IETF

* ISOC (Internet Society)
  + Promotie van ontwikkeling, evaluatie en internet
  + De baas over IAB
* IAB (Internet Architecture Board)
  + Beheert en ontwikkeld internet standaards
  + Bij de bestuurders horen ook de IETF
* IETF (Internet Engineering Task Force)
  + Ontwikkeld, update en onderhoud TCP/IP technologieën
  + Produceert RFCs (Request For Comments)
* IRTF (internet research task force)
  + Gefocust op lange termijn onderzoeken

#### IEEE

* Institute of Electrical and Electronics Engineers
* Creëert standaards voor WAN/LAN technologieën, bedraad zowel als draadloos
* Hoofd focus ligt bij de toegankelijkheid tot het medium (fysieke en data link laag)

#### ISO

* International Organization for Standards
* Werelds grootste ontwikkelaar van standaards, met een grootte waaier aan producten en diensten, niet enkel computer/netwerk protocols
* ISO komt van isos wat gelijk betekend
* Ontwikkelaar van het OSI model

#### Other Standards Organizations

* EIA (Electronic Industries Alliance)
  + Standaard die te maken hebben met elektrische bedradingen, connectoren, …
* TIA (Telecommunications Industry Association)
  + Standard voor gsm, radio, satelliet, …
* ITU-T (The International Telecommunications Union – Telecommunications Standardization Sector)
  + Standard voor video compressive, DSL, …
* ICANN (Internet Corporation for Assigned Names and Numbers)
  + Hoog level van DNS management, poortnummers, coördinatie van IP adressen
  + Non-profit organisatie, zet de richtlijnen voor IANA
* IANA (Internet Assigned Numbers Authority)
  + Deel van ICANN dat verantwoordelijk is voor IP adressen, domein namen en poortnummers

### Reference Models

#### The Benefits of Using a Layered Model

* Assisteert in de protocol ontwerpen (men weet de verantwoordelijkheid van elke laag)
* Bevordert concurrentie tussen verkopers
* Voorkomt dat aanpassingen in een laag effect heeft op een ander laag
* Jargon: veelvoorkomende taal in netwerken
* Referentiemodel
  + OSI
  + Bespreekt elke laag en hoe ze samen werken, niet de exacte werking details
  + Technisch model
* Protocolmodel
  + Vertaald het referentiemodel in concrete protocollen op iedere lag en de werking details
  + Praktisch model

#### The OSI Reference Model

1. Fysieke laag
   * Vertaald bits in elektronische, opticale signalen. De hardware
2. Data link laag
   * Toegang tot het medium (MAC: Media Access Control) ethernet, Wi-Fi
   * Communicatie binnen een LAN frames de NIC
3. Netwerk laag
   * Transporteren van pakketten tussen LAN’s, routing IP
4. Transport laag
   * Segmentatie van data, data ophooping. Verantwoordelijk voor het transport van segmenten
5. Sessie laag
6. Presentatie laag
7. Aplicatie lag
   * De connectie met de gebruiker. De programma’s

#### The TCP/IP Protocol Model

* Vier categoriëen
  + Applicatie
  + Transport
  + Internet
  + Netwerk toegang

#### Comparing the OSI Model with the TCP/IP Model

* Applicatie categorie = laag 7, 6, 5 van het OSI model
* Transport categorie = laag 4 van het OSI model
* Internet categorie = netwerk laag van het OSI model
* Netwerk categorie = laag 2 en 1 van het OSI model

## Moving Data in the Network

### Data Encapsulation

#### Communicating the Messages

* Segmentatie
  + Verdeelt data over kleinere stukken om ze over het netwerk te sturen
  + Indien een grote file 🡪
    - overbelasting van de connectie
    - volledig opnieuw versturen indien een fout optreedt
* voordelen van segmentatie
  + veel gesprekken kunnen verweven worden op het netwerk (multiplexing)
  + de betrouwbaarheid stijgt: de pakketten hoeven niet dezelfde weg te volgen
* nadeel van segmentatie
  + voegt level toe aan de complexiteit

#### Protocol Data Units (PDUs)

* De vorm die elk stuk data aanneemt in de lagen
* Ze worden genoemd naar de protocols van het IP/TCP model

#### Encapsulation

1. Data komt van de browser
2. Data wordt in TCP segmenten geëncapsuleerd om het te kunnen sturen naar de juiste poort
3. TCP segment wordt geëncapsuleerd in IP pakketten om het naar het juiste netwerk te sturen
4. IP pakketten worden geëncapsuleerd naar een Ethernet frame om het in de volgende hop te sturen binnen een netwerk (MAC adres)
5. Vertaald bits in elektrische signalen

#### De-encapsulation

* De omgekeerde weg als de encapsulatie
* Van bits naar het originele bestand

### Accessing Local Resources

#### Network Addresses and Data Link addresses

* Data link adres (MAC)
  + Verzorgt de data link tussen een NIC en een andere NIC binnen dezelfde netwerk
  + Meest voorkomende: Ethernet en Wi-Fi frames
* Netwerk toegang (IP)
  + Bezorgt het IP pakket van de verzender naar de bestemming (mogelijk in een ander netwerk)
  + 2 delen netwerk prefix deel en host deel
    - Subnet mask werkt als een filter om te bepalen wat het netwerk ID en de host ID in dat netwerk is

#### Communicating with a Device on the Same Network

#### MAC and IP Addresses

MAC krijgt de pc door een ARP te sturen op hetzelfde netwerk

### Accessing Remote Resources

* Bij het zenden van andere host
  + Zit de host in mijn netwerk
    - Gebruik je eigen subnet mask op je eigen IP en de bestemming IP
    - Het aanbrengen van een IP adres geeft een netwerk
    - Als het IP van de bestemming gelijk is aan het netwerk van je eigen IP
      * Bestemming zit in je eigen netwerk 🡪 gebruik de ARP tabel om het MAC adres van de bestemming te krijgen
    - Als je 2 verschillende netwerken krijgt
      * De bestemming zit niet in je netwerk
      * Zendt de data naar de uitgang van je netwerk (default gateway)
      * Kijk de ARP tabel na om het MAC adres van de bestemming te krijgen
      * Het is de taak van de DG om de boodschap het juiste netwerk op te sturen
        + Wanneer data arriveert aan de DG van het bestemde netwerk, die DG zal dat IP omzetten naar het MAC adres van de bestemming
* De default gateway is de manier om uit het netwerk te raken. Het is de host van dat netwerk
* IP adres en subnet mask
  + IPv4 = 32 bits
  + Subnet mask (ook 32 bits) definieert welke host in welk netwerk is
  + Het mask toepassen op het IP adres = je doet de logische AND-operatie
* Het Subnet mask splijt het IP adres in 2
  + Als je alle 0en achter de slash steekt krijg je het netwerk ID adres
  + Als je alle 1en achter de slash steekt krijg je het broadcast IP adres van dat netwerk
* Er zijn 2 IP adressen die je niet kan gebruiken voor hosts in je netwerk:
  + Het netwerk IP
  + Broadcast IPNetwork Access

# Network Access

## Physical Layer Protocols

### Getting It Connected

#### Connecting to the Network

* Netwerk toegang laag = fysieke en data link lag
* Data link: bereid de data voor om te verzenden en controleert hoe data toegang heeft tot media
* Fysieke laag: de bits naar signalen en de eigenlijke verzending
* Connectie tot een apparaat
  + Bedraad (ethernet, …)
  + Draadloos, met een Wireless Access Point(Wi-Fi, …)
  + Combinatie van bovenstaande: Home Integrated Services Router

#### Network Interface Cards

* NIC
  + Nodig om connectie te maken met het netwerk
  + Bedraad en/of draadloos
* Prestaties
  + Bedraade NIC
    - Apparaat gebruikt de hele Ethernet kabel bandbreedte
    - Heeft versterking nodig na 100 m (max lengte)
  + Draadloze NIC
    - Meerdere apparaten delen dezelfde draadloze verbinding
    - Minder bandbreedte per apparaat
    - Afstand en omgeving hebben grote invloed op het signaal
      * (nood aan een signaalversterker)

### Purpose of the Physical Layer

#### The Physical Layer

* L1
  + Accepteert frames van de datalink (L2)
  + codeert het frame voor t-verzending over het medium
    - Elektrisch, opticaal of radiogolfsignaal

#### Physical Layer Media

* Verschillende soorten media
  + Koper kabel
  + Fiber-optic kabel
  + draadloos

#### Physical Layer Standards

* Afkomstig van de standaarden organisaties

### Fundamental Principles of Layer 1

#### Physical Layer Fundamental Principles

* Fysieke componenten
  + NIC, connectors, kabels, …
* Encoding (omzetten naar code)
  + Vertaald binaire data in voorspelbare elektrische patronen zodat de ontvanger het ook verstaat en kan vertalen
  + Ook gebruikt om begin en einde te vinden
    - Manchester encoding
      * 0 is van hoog naar laag voltage
      * 1 is van laag naar hoog voltage
    - Non-return to Zero (NRZ) encoding
      * 0 is een laag voltage, 1 een hoog voltage
      * Er is geen ‘geen voltage’, geen terugkeer naar 0
* Signaleren (hoe het op het medium zetten)
  + Asynchroon
    - Geen klok
    - Willekeurige spaties tussen datablokken
    - Heeft start en stop indicators nodig
  + Synchroon
    - Data wordt gelijk verspreid, gebruikmakend van de klok, zo weet de ontvanger wanneer het volgende data komt
  + Modulatie
    - Zet gecodeerde berichten op een draaggolf om over grotere afstanden te reizen

#### bandbreedte

* De hoeveelheid data dat van een plaats naar een ander kan stromen binnen een bepaalde tijd
* Theoretisch
* Bits per seconde

#### Throughput

* De echte hoeveelheid data dat van een plaats naar een ander kan stromen binnen een bepaalde tijd
* Praktisch
* Komt niet altijd overeen met de theoretische bandbreedte
  + Hangt af van het type verkeer, hoeveelheid verkeer, latency …
  + Latency (hoeveelheid tijd incl. Vertraging)
    - Data moet over een pad van A naar B reizen
    - Over verschillende apparaten reizen 🡪 apparaten hebben proces tijd nodig 🡪 vertraging
    - Als er een traag segment tussen A en B zit resulteert dit in een bottleneck met vertraging als gevolg

## Network Media

### Copper Cabling

#### Characteristics of Copper Media

* Waarom koper
  + Niet duur, makkelijk te instaleren, …
* Maar
  + Lage weerstand tegen elektriciteit
  + Gelimiteerd in afstand (verzwakking)
  + Gevoelig aan storing (noise)
    - Electromagnetisch storing (EMI), radio frequentie storing(RFI)
      * Gecreëerd door TL lampen, motors, metalen objecten
    - Cross talk:
      * Aangrenzende draden spreken met elkaar door elektrische en magnetische veld interactie
* Hoe fixen?
  + Verzwakking fix: zet de max lengte voor een verstrekker nodig is
  + Zet een EMI en RFI schild: kabels met een metalen schild
  + Crosstalk fix: gedraaide kabels vernietigen dit effect

#### Copper Media

* Drie soorten
  + Unshielded twisted-pair (UTP)
  + Shielded twisted-pair (STP)
  + coaxial

#### Unshielded Twisted-Pair Cable

* UTP
* Meest gebruikte netwerk media
* Heeft een RJ-45 connector
* 4 paar kleuren
  + Hoe meer draaiingen het heeft, hoe beter het beschermd tegen crosstalk
  + Gebruikt categorieën om een level aan bescherming tegen storing te definiëren

#### Shielded Twisted-Pair (STP) Cable

* STP
* Beter schild
* Duurder, moeilijker te instaleren
* Gebruikt ook de RJ-45 aansluiting
* 2 types van schild
  + Een schild rond de hele bundel om tegen storing te beschermen
  + Een schild rond heel de bundel en rond de individuele draden
* Enkel gebruikt als er heel hoge ethernet connecties nodig zijn

#### Coaxial Cable

* Grote koperen geleider
* Metaal schild
* Verschillende connectoren
* Voornamelijk gebruikt om
  + Internet kabel instalatie (telenet)
  + Draadloze installaties: verbindt een antenne aan een draadloos toestel

#### Copper Media Safety

* Pas op bij het gebruik als er elektrische spanning op de draden staat
* Nooit 2 gebouwen met een koperen kabel verbinden
  + Blikseminslag gevaar
  + Als er bliksem inslaat op een van de gebouwen kan het overslaan op het andere gebouw
  + Gebruik fiber optic kabels

### UTP Cabling

#### Properties of UTP Cabling

* Unshielded twisted pair
  + Geen schild, gelimiteerde EMI – RFI bescherming
    - Gebruik draden in geschikte omgeving zonder te veel storing
  + Bescherming tegen crosstalk
    - Cancellation
      * Gebruikt kabels als een paar, draait ze, zodat het magnetisch en elektrisch veld elkaar opheffen
      * Geeft een beetje bescherming tegen EMI/RFI
    - Variatie van het aantal draaien per paar
      * Meer draaiingen geven meer cancellation en betere bescherming tegen EMI/RFI

#### UTP Cabling Standards

* Kabels zijn in categorie verdeelt aan de hand van hun maximale bandbreedte
  + Cat 5, CAT 5e, cat6

#### UTP Connectors

* RJ-45 connector

#### Types of UTP Cable

* Ethernet straight-though
  + Geen kruising van de 8 kabels
  + Wordt gebruik als een apparaat een MDI interface heeft en een andere MDIX interface
* Ethernet cross-over
  + Kruist de kabels
  + Wordt gebruikt indien de apparaten ofwel beide de MDI ofwel de MDIX interface heeft
* Rollover
  + Kabel van Cisco

#### Testing UTP Cables

* kabeltang
* Testen met een kabeltester

### Fiber Optic Cabling

#### Properties of Fiber Optic Cabling

* Glasvezel
  + Puur glaze kern
  + Gebruikt licht signalen om data door te sturen
  + Heel snel en kan over grote afstanden reizen
  + Immuun voor EMI/RFI
  + Geliefde manier om 2 gebouwen te verbinden met draad(geen elektrische signalen)
* Glasvezel netwerken
  + Bij bedrijfsnetwerken het centrum
  + Fiber to the home (FTTH): glasvezelconnectie van thuis tot de ISP
  + Lange afstandsvluchten: verbind landen, steden, continenten, …
  + Congenitale verbindingen over de zeebodem

#### Fiber Media Cable Design

* De kern is een soort spiegel in een jasje

#### Types of Fiber Media

* 2 types van lichtsoorten
  + Laser:
    - Hoge power, lange afstand, gebruikt voor single mode fiber, een signaal
  + Light Emitting Diode (LED)
    - Minder power, niet duur, kan getuned worden voor multimode fiber, meerdere signalen

#### Network Fiber Connectors

* Veel verschillende soorten: verschillen in grootte en de methode van koppelen
  + Straight-tip (ST)
  + Subscriber connector (SC)
  + Lucent connector (LC)
* Licht kan maar een richting op reizen, dus voor volledige tweezijdige communicatie hebben we 2 fibers nodig
* Patchkabels
  + Om apparaten onderling te verbinden

#### Testing Fiber Cables

* Speciale training is nodig om het beëindigen en instaleren van fiber te doen
* Veel voorkomende fouten
  + Misalignment: twee einden zijn niet perfect uitgelijnd: onderbreking van het licht
  + End gap: 2 delen zijn niet volledig aan elkaar, er is een gat in
  + End finish: einddeel is vuil
* De kwaliteit van de link wordt nagekeken met speciaal gereedschap
  + Optical time domain reflectometer (OTDR)
    - Zend pulsen over de draad en meet de terugslag en berekend de tijd tussen de fout

#### Fiber versus Copper

### Wireless Media

#### Properties of Wireless Media

* Wi-Fi: gebruikt radio frequenties om data te versturen
* Pro’s
  + Grote mobiliteit
  + Makkelijk nieuwe apparaten aan het netwerk toe te voegen
  + Snelheid is ok, maar niet te vergelijken met bedraad internet
* Con’s
  + Grote van de bereik
    - Gelimiteerd bereik binnen gebouwen door materiaal die het signaal blokkeert
  + Interactie
    - Draadloze telefoon, microgolf oven, …
  + Veiligheid
    - Makkelijk met een netwerk te verbinden, geen fysiek toegang, kwetsbaarder voor hackers

#### Types of Wireless Media

* 3 grote draadloze standaards
  + IEEE 802.11: Wi-Fi, WLAN technologie
  + IEEE 802.15: Bluetooth, WPAN technologie
  + IEEE 802.16: WiMAX: hoge snelheid, stadsnetwerk, WMAN technologie

#### Wireless LAN

* Er is nood aan een wireless access point (AP) en draadloze NIC adapters

#### 802.11 Wi-Fi Standards

## Data Link Layer Protocols

### Purpose of the Data Link Layer

#### The Data Link Layer

* Wat is de data link lag
  + Het accepteert L3 pakketten en encapsuleert deze in frames
  + Het controleert de toegang tot het medium en doet aan fout ontdekking
  + De connectie laag tussen de hardware en software

#### Data Link Sub layers

* Data link laag is verdeeld in 2 delen
  + Logical link control (LLC)
    - Verbinding sublaag naar de software
    - Levert diensten aan netwerk laag protocollen
  + Media Access Control (MAC)
    - verbindingen sublaag naar de hardware
    - Levert adressering (MAC adres)

#### Media Access Control

* L2 protocollen defineren
  + De encapsulation van het frame
  + Wanneer en hoe toegang tot het medium
    - Verschillende media hebben verschillende technieken, verschillende protocollen nodig
    - Als een nieuw Wi-Fi protocol ontwikkeld wordt, enkel de L2 protocollen moeten gedefinieerd worden, doet dit de netwerkprotocollen niet zo veel beïnvloeden als bv IPv4

#### Providing Access to Media

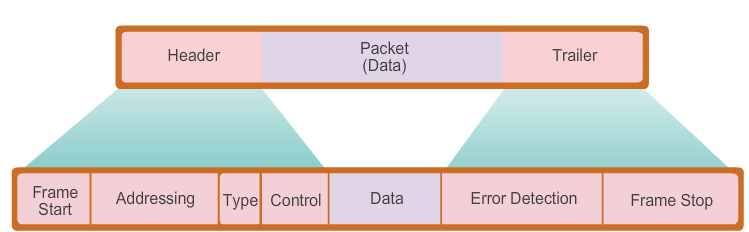
* Tijdens de reis van A naar B kunnen meerdere media voorkomen met elk hun protocollen voorkomen
* De data link laag accepteert het frame, deëncapsuleerd deze, her encapsuleert in een nieuw frame en het nu geschikte frame dan terug doorstuurt naar het medium

### Layer 2 Frame Structure

#### Formatting Data for Transmission

* Encodering op de data laag
  + Als een knooppunt een stroom bits ontvangst
    - Hoe beslissen waar het frame start en eindigt
    - Hoe controleren of alle bits juist zijn ontvangen
    - Hoe moet je weten voor welke netwerk laag protocol de data moet worden voorbereid

#### Creating a Frame



### Layer 2 Standards

#### Data Link Layer Standards

* Verschillende standaards

## Media Access Control

### Topologies

#### Controlling Access to the Media

* Wanneer data op het medium zetten?
* Hangt af van
  + Topologie: hoe de datalink laag de knooppunten ziet
  + Media delen: hoe delen de knooppunten de media?

#### Physical and Logical Topologies

* Fysieke topologie: refereert naar de fysieke connecties
* Logische topologie: refereert naar hoe een netwerk frames transporteert van een knooppunt naar een ander

### WAN Topologies

#### Common Physical WAN Topologies

* Point-to-point
  + Fysieke P2P: geen echte adressering nodig
  + Logische P2P: virtueel circuit
* Hub-and-spoke
* mesh

#### Physical Point-to-Point Topology

* Verbind 2 punten direct

#### Logical Point-to-Point Topology

* Mogelijk dat de 2 eindpunten niet direct zijn verbonden maar via een aantal tussen media
* Het fysieke gebruik van apparaten heeft geen invloed op de logische topologie

#### Half and Full Duplex

* Half duplex: enkel zenden of ontvangen van data
* Full-duplex: zowel zenden als ontvangen gaat tegelijk

### LAN Topologies

#### Physical LAN Topologies

* Ster
  + Meest gebruikte, gebruikt een centrale swith
  + Soort point-to-point van apparaat naar switch
* Uitgebreide ster
  + Ster van sterren
* Bus
  + Gebruikt in oudere Ethernet netwerken
  + Veroudert, nu met een switch wat resulteert in een ster
* Ring

#### Logical Topology for Shared Media

* Gedeelde media?
  + Wanneer het media gebruiken
  + 2 basis media toegang controle methods
    - Verbinding gebaseerde toegang
      * Alle knooppunten strijden voor het gebruik van het medium,
      * maar hebben een plan voor als er botsingen zijn
    - gecontroleerde toegang
      * elk knooppunt heeft zijn eigen tijdsslot om het medium te gebruiken

#### Contention-Based Access

* Carrier sense multiple access with collision detection (CSMA/CD)
  + Carrier sense: luistert naar het medium voor een signaal
  + Geen signaal 🡪 data verzenden
  + Maar, het is meerdere toegankelijkheid, meerder apparaten hebben toegang tot het medium 🡪 luistert voor botsingen
  + Indien er een botsing is gaan alle apparaten wachten voor een random tijd
* Carrier sense multiple access with collision avoidance (CSMA/CA)
  + Verstopt knooppunt problem met Wi-Fi
  + Zoekt de lucht af voor signalen 🡪 lucht vrij?
  + Zend ‘request to send’ aan het toegangspunt
    - Toegangspunt controleert om te zien of er botsingen gaan ontstaan of niet
    - Toegangspunt stuurt ‘clear to send’ signaal aan de host

#### Multi-Access Topology

* Elk knooppunt ziet de frames op het netwerk, maar alleen het knooppunt aan wie de frame geadresseerd is kan de inhoud verwerken

#### Controlled Access

* geschematiseerd toegang, wie het token heft mag communiceren
* Het token wordt steeds doorgegeven
* Bekendste: token ring

#### Ring Topology

### Data Link Frame

#### The Frame

* Drie delen
  + Header
  + Data
  + trailer

#### The Header

* Bevat de controle informatie die nodig is voor het transport over een specifiek medium
  + Vatbare omgeving vraagt meer controle informatie
  + Beschermde omgeving vraagt minder
* Velden
  + Start frame veld
  + Source and destination adres veld
  + Type veld

#### Layer 2 Address

* Zit in de header
* Enkel gebruikt om binnen lokale levering te zoeken

#### The Trailer

* Einde van het frame
* Om na te gaan of het frame is aangekomen zonder fouten

#### LAN and WAN Frames

#### Ethernet Frame

#### PPP Frame

* Point-to-point protocol
* Gebruikt voor leveringen tussen 2 knooppunten

#### 802.11 Wireless Frame

# Ethernet

## Ethernet Protocol

### Ethernet Operation

#### LLC and MAC Sub layers

* Ethernet
  + Een van de meest gebruikte LAN technologieën
  + Werkt in de datalink laag en de fysieke laag
  + Is familie van de netwerktechnologieën gedefinieerd in de IEEE 802.2 en IEEE 802.3 standaards
  + Ondersteunt dat bandbreedte van 10, 100, 1000, 10.000, 40.000 en 100.000 Mbps
* Ethernet standaards
  + Definieert laag 2 protocollen en laag 1 technologieën
  + Twee aparte sublagen van de data link laag om te werken
    - Logical link control (LLC) sub layer 🡪 IEEE 802.2
      * (De software interface) de drivers van de NIC
      * Behandelt communicatie tussen hogere en lagere lagen
      * Neemt de netwerk protocol data en voegt controle informatie toe om te helpen bij het afleveren van het pakket bij de bestemming
    - Media Access Control (MAC) sub layer (+L1) 🡪 IEEE 802.3
      * (de hardware interface) de NIC zelf
      * Vormt de lager sublaag van de data link laag
      * Gebruikt met hardware, typisch in de computer NICM

#### MAC Sub layer

* Twee verantwoordelijkheden
  + Data encapsulation
    - Frame delimiting (start/stop)
    - Addressing (MAC adressen)
    - Error detection (FCS – CRC code)
  + Media access control
    - Plaatsing en verwijderen van frames op en af het medium
    - Ethernet = Multi-access bus topologie
      * Alle knooppunten op het segment delen het medium
      * Contention bases 🡪 Carrier Sense Multiple Access/Collision Detection CSMA/CD!!!!
        + Ethernet in het verleden: gebruik van hubs 🡪 veel botsingen
        + Ethernet nu: gebruik van switches 🡪 bijna geen botsingen

#### Media Access Control

* Collision domain – broadcast domain
  + Als een botsing gebeurt op een segment, hoever zal dit het netwerk beïnvloeden?
    - Hub = L1 apparaat: gewoon een versterken, geen intelligentie, zal geen botsing stoppen
    - Switch = L2 apparaat: moet het MAC adres lezen, stopt botsingen
  + Hoever zal een broadcast frame in het netwerk reizen
    - Een broadcast frame heeft twee adressen
      * Broadcast MAC (FF:FF:FF:FF:FF:FF)
      * Broadcast IP(hoogste IP adres van het netwerk – niet voor een host)
    - Hub: geen intelligentie, zal de broadcast niet stoppen
    - Switch: leest het MAC, is een broadcast, dus zendt het naar alle verbonden kabels (buiten de inbound kabel)
    - Router: L3 apparaat, leest het MAC en het IP: stopt de broadcast (bescherming van het netwerk)
  + Collision domain 🡪 domein waarbinnen botsingen kunnen voorkomen
  + Broadcast domain 🡪 domein waarbinnen een broadcast kan reizen

#### MAC Address: Ethernet Identity

* 48 bits, gerepresenteerd in 12 hexadecimale karakters = 6 paren
  + Eerste 3 paren = ID van het bedrijf
  + Laatste 3 paren = ID van de NIC

#### Frame Processing

* Globaal uniek
* Enkel onthuld binnen een netwerk
* Ingebrand adres (BIA) – in het ROM 🡪 kan niet veranderd worden

### Ethernet Frame Attributes

#### Ethernet Encapsulation

* Er zijn eigenlijk 2 types van Ethernet frames:
  + IEEE 802.3 frames: oude standaard
  + Ethernet II frames: tegenwoordig gebruikt in TCP/IP netwerken
* Enige verschil:
  + Start frame delimiter
  + Type van het veld versus lengte van het veld

#### Ethernet Frame Size

* Minimum grootte: 64 bytes
  + Als het frame kleiner is, is het een runt frame ( gecreëerd door een botsing
* Maximum grootte: 1518 bytes(of 1522 bytes als de VLAN tag erbij zit
* Als het frame buiten deze groottes valt, laat het frame vallen

#### Introduction to the Ethernet Frame

### Ethernet MAC

#### MAC Addresses and Hexadecimal

* Getallen van 1 tot F
* Basis 16
* Twee hexadecimale getallen zijn makkelijker te lezen dan 4 binaire getallen

#### MAC Address Representations

* Ipconfig/all 🡪 commando om het MAC adres te identificeren

#### Unicast MAC Address

* Verschillende MAC adressen worden gebruikt voor de soorten cast communicatie
* Unicast MAC adres: uniek, gebruikt als een frame een op een wordt verzonden

#### Broadcast MAC Address

* Bestemming IP heeft allemaal enen in het host deel, wat betekend dat alle hosts op dat broadcast domain het pakket zal ontvangen

#### Multicast MAC Address

* Er wordt gebruik gemaakt van een groep IP adres die meerdere IP adressen bevat
* Heeft net als unicast en broadcast heeft een Multi cast een correspondeerde MAC adres nodig
* De range van IPv4 Multi cast adressen is 224.0.0.0 tot 239.255.255.255
* Multicast MAC adres is een speciale waarde die begint met 01-00-5E hexadecimaal

### MAC and IP

#### MAC and IP

* MAC adres is het fysiek adres (verandert niet)
* IP adres is het logische adres (kan veranderen)
* Werken samen om een apparaat te identificeren

#### End-to-End Connectivity, MAC, and IP

* IP adres wordt gebruikt om het beste pad naar de bestemming te bepalen
* IP adres bepaalt het end-to-end gedrag van een IP pakket
* MAC adres wordt gebruikt om de bron en bestemming host te identificeren op lager level

## Address Resolution Protocol

### ARP

#### Introduction to ARP

* MAC address
  + Dit adres verandert niet
  + Is zoals de naam van een person
  + Gekend als het fysieke adres omdat het fysiek aan de host NIC toegewezen
* IP adres
  + Gelijk aan de het adres van een persoon
  + Gebaseerd op waar de host zich bevindt
  + Gekend als het logische adres omdat het logische is toegekend
* Toegekend aan alle hosts door een netwerk administrator
  + Beide de fysieke MAC en de logische IP adressen zijn nodig om een computer te laten communiceren, net zoals de naam en adres van een mens nodig zijn om een brief te sturen
* Zendende node heeft het MAC en IP adres van de ontvanger nodig om te encapsuleren

#### ARP Functions

* ARP details
  + ARP mapping (MAC/IP) is gewoonlijk dynamisch gedaan, maar kan ook statisch gedaan worden
    - De mogelijkheid van statisch mapping is tegen ARP vergiftiging van de default gateway

#### ARP Operation

* Gewoonlijk is het IP adres gekend (door de DNS), maar het MAC?
  + Als de bestemming in het eigen netwerk ligt dan kun je het MAC adres van de bestemming gebruiken
  + Ten tweede: krijg het MAC adres van de bestemming
    - Zoek het op in de ARP tabel (database van MAC-IP koppelingen)
    - Als het er niet is, gebruik de ARP om het MAC adres te vinden
      * Broadcast ARP verzoek
      * Bestemming zal antwoorden met een unicast

#### ARP Role in Remote Communication

* Als de bestemming niet in het eigen netwerk ligt gebruik je het MAC adres van de default gateway
* Krijg het MAC adres van de default gateway
  + Zoek het op in de ARP tabel (database van MAC-IP koppelingen)
  + Als het er niet is, gebruik de ARP om het MAC adres te vinden
    - Broadcast ARP verzoek
    - Bestemming zal antwoorden met een unicast

#### Removing Entries from an ARP Table

* ARP ingevingen hebben een tijdstempel, vervaldatum
  + Elke keer als het apparaat een frame ontvangt kijkt het de ARP tabel na en reset de timer

#### ARP Tables on Networking Devices

* De ARP tabel nakijken
  + Show IP ARP
  + ARP –aIntroduction to ARP

### ARP Issues

#### How ARP Can Create Problems

* ARP beveiliging:
  + ARP vergiftiging 🡪 beperking: maak het mapping statisch (or ARP on/ARP Watch)
  + ARP vergiftiging: hacker zendt het doel een frame met als het bron IP het IP van de default gateway IP, maar als bron MAC zijn eigen MAC adres
  + ARP zal zijn mapping nakijken en zal het aanpassen om de DG IP te verbinden met het hacker IP 🡪 zend data naar DG en zal dan data naar de hacker zenden

#### Mitigating ARP Problems

* ARP verkeer
  + ARP creert veel broadcasts en unicast berichten
  + In een gedeeld medium zet dit veel druk op het netwerk: zelfs unicast frames worden verzonden naar en verwerkt door iedereen
  + Verzachting: gebruik segmentatie(gebruik een switch om collision domains te splitsen, nu worden de unicast berichten enkel naar het juiste segment gezonden

## LAN Switches

### Switching

#### Switch Port Fundamentals

* Layer 2 LAN switch
  + Het verbindingspunt naar het netwerk toe
  + Heeft een MAC tabel (database)
    - MAC adressenzijn verbonden met switch poorten
      * (apparaat met MAC AA is op poort fa0/1)
    - MAC tabel is gevuld met passerende frames
      * Switch kijkt naar het bron MAC op de inkomende poort, om dat MAC aan de MAC tabel toe te voegen
  + Doet aan switching en filtering gebaseerd enkel op de bestemming MAC adres
    - Switch kijkt naar het bestemming MAC adres, kijkt naar zijn MAC tabel om te zien welke uitgaande poort te gebruiken(filtering)
    - Als MAC niet in de tabel: stuurt hij het frame uit alle poorten (except inbound)
  + Layer 2 doet enkel aan switching binnen het LAN, geen routing tussen netwerken gebaseerd op IP

#### Switch MAC Address Table

* De switch ontvangt een broadcast frame van vb. PC1 op poort 1
* De switch zet het bron MAC adres en de switchpoort die het frame ontving in de adres tabel
* Omdat het doel adres een broadcast is, stuurt de switch het frame door alle poorten buiten die waar het frame door binnen kwam
* Het bestemmingsapparaat antwoord op de broadcast met een unicast frame geadresseerd aan PC1
* De switch zet het bron MAC van PC2 en de poort die het frame ontving in de adres tabel.  
  Het bestemming adres van de frame en zijn geassocieerde poort staan in de MAC adres tabel
* De switch kan nu frames doorsturen tussen bron en bestemming omdat het ingevingen in de adres tabel heeft die de geassocieerde poorten identificeert

#### Duplex Settings

* Gebruik de juiste duplex instellingen
  + Half duplex mode: enkel met ouder gereedschap zoals hubs een richtingsverkeerd per keer
  + Full duplex mode: standaard tweerichtingsverkeer
  + Auto-gegotiation duplex mode

#### Auto-MDIX

* Gebruik de juiste bekabeling
  + Switches en hubs interfaces zijn MDIX
  + Alle andere apparaten hebben MDI interfaces
    - Verbinding MDI – MDIX gebeurt met een straight through kabel
    - Verbinding MDI - MDI of MDIX – MDIX gebeurt met een cross kabel
    - Standaard tegenwoordig is dat een interface een MDIX auto sensing gebruikt om de mode van de interface te bepalen, gebaseerd op de ingestoken kabel

#### Frame Forwarding Methods on Cisco Switches

* Store and forward:
  + Default mode
  + Neemt de hele frame in de buffer
  + Kijkt de CRC na

#### Cut-Through Switching

* twee varianten:
  + Fast-forward switching
    - Laagste level van vertraging, stuurt een pakket onmiddellijk door na het lezen van de bestemmingsadres, typisch cut-through methode van switching
  + Fragment-free switching
    - Switch slaat de eerste 64 bits van het frame op voor het door te sturen, de meeste netwerk fouten en botsingen gebeuren in de eerste 64 bits

#### Memory Buffering on Switches

* 2 soorten an buffering data op switches
  + Port-bases memory buffering
    - Elke poort heeft zijn eigen buffer, als het vol is zullen frames worden gedropt
  + Shared memory buffering
    - Een grote buffer voor alle inkomende frames. Belangrijk voor switchen met asymmetrisch switching met verschillende poort snelheden

### Fixed or Modular

#### Fixed versus Modular Configuration

* Kiezen van de juiste switch
  + Doorstuursnelheid (hogere klasse switch heeft grotere verwerkingscapaciteiten)
  + Poort dichtheid en type van de poort(PoE, Fa, Gi, fiber)
  + Stapelbaar of niet stapelbaar (in rank units (RU))
* Fixed configuration:
  + WYSIWYG what you see is what you get, niet mogelijk om capaciteiten toe te voegen
* Modular switches
  + Mogelijk om capaciteiten toe te voegen wanneer nodig, flexibel, add-ons

#### Module Options for Cisco Switch Slots

### Layer 3 Switching

#### Layer 2 versus Layer 3 Switching

* Layer 2 switch
  + Default switch: kijkt naar de L2 MAC adres, kijkt naar de MAC tabel en stuurt het frame door
  + Heeft een router nodig om van een netwerk naar een ander te gaan
* Layer 3 switch
  + Niet enkel switching op lader 2, maar kan ook routing doen(L3, gebaseerd op IP adressen)
    - Geen nood voor specifieke L3 router

#### Cisco Express Forwarding

* 2 hoofdcomponenten
  + Forwarding information base (FIB)
    - Conceptioneel vergelijkbaar met een routing tabel
    - Een netwerkapparaat gebruikt deze opzoektabel om bestemming gebaseerde switching beslissingen te maken
    - Wordt geüpdatet wanner er veranderingen gebeuren in het netwerk en bevat alle routes gekend op die tijd
  + Adjacency tables
    - Onderhoud lader 2 next-hop adressen voor alle FIB ingaven
    - Gelijk een ARP tabel, maar zonder timer, dus niet cache-like gedrag, geen nood voor ARP vragen

#### Types of Layer 3 Interfaces

* Grootste types van Layer 3 interfaces
  + Switch Virtual Interface (SVI): logische interface op de switch geasosiseerd met een virtual local area network (VLAN)
  + Routed Port: fysieke poort op een Layer 3 switch geconfigureerd om zich te gedragen al een router poort. Configureert routed poorten door de interface in Layer 3 mode met geen switchpoort interface configuratie commando te steken
  + Layer 3 EtherChannel: logische interface op een Cisco apparaat geassocieerd met een bundel van geroute poorten

#### Configuring a Routed Port on a Layer 3 Switch

* Interface f0/6
* No switch port
* IP address 192.168.200.1 255.255.255.0
* No shutdown
* end

# Network Layer

## Network Layer Protocols

### Network Layer in Communication

#### The Network Layer

* OSI laag 3
* Laat toe dat eindapparaten data uitwisselen doorheen het netwerk
* Vier basis processen
  + Adressering
  + Encapsuation
  + Routing
  + Deëncapsulation

#### Network Layer Protocols

* Netwerk laag:
  + Communicatie over het netwerk
  + Logische addressing (IP)
  + Encapsulation naar pakketten
  + Routing
* Hoofdprotocollen
  + IPv4
  + IPv6
* Nalatenschap
  + IPX (Novell Internetwork Packet Exchange)
  + Appletalk (nu vervangen door Bonjour protocol)

### Characteristics of the IP protocol

#### Characteristics of IP

* Basis karakteristieken
  + Connectieloos
  + Beste moeite (onbetrouwbaar)
  + Media onafhankelijkheid

#### IP – Connectionless

* Geen idee of de ontvanger het bericht ontvangt, of de lezer het bericht kan lezen, als de ontvanger er is.
* De ontvanger weet niet wanneer het bericht gaat komen.

#### IP – Best Effort Delivery

* Als een onbetrouwbaar netwerk protocol, IP garandeert niet dat alle verzonden pakketten ontvangen zullen worden
* Andere protocollen beheren het proces van de pakketten te traceren en hun levering verzekeren

#### IP – Media Independent

* IP is niet afhankelijk van het medium, het kan draadloos, over fiber, over koper,

#### Encapsulating IP

* Een IP packet heeft een IP header en een transport lader PDU
* De IP header blijft hetzelfde van bron tot bestemming
* L2 header kan veranderen, door de verschillende media waar het over reist

### IPv4 Packet

#### IPv4 Packet Header

* 2 delen
  + IP header
  + payload
* De belangrijke delen
  + Versie
    - IPv4 = ‘0100’ = 4 decimalen
    - IPv6 = ‘0110’ = 6 decimalen
  + Differentiated Services (DS) (type van service)
    - Prioritaire velden voor QoS (Quality of Service)
  + Time to live (TTL)
    - Een ‘levende’ teller die verlaagt wordt elke keen het door een router gaat
  + Protocol
    - Welk L4 protocol zal er in het pakket zitten? TCP, UDP?
  + Bron en bestemming IP adres
    - 32 bits waarde: het belangrijkste deel

#### IPv4 Header Fields

* Minder belangrijke delen
  + Internet Header Length (IHL)
    - Definieert hoe groot de hoofding is
    - Afhankelijk van de opties en de padding
  + Totale lengte
    - Totale lengte van het pakket
  + Hoofding checksum
    - Kijkt na of de hoofding in orde is
  + Soms is fragmentatie nodig
    - Router kan verschillende netwerken verbinden met verschillende media
      * Elk medium heeft een verschillend MTU (Maximum Transmittable Unit) = maximale grote van de data
      * Router moet soms het pakket opsplitsen = fragment
    - Identificatie, vlaggen, fragment offset zijn om te assisteren bij de herbouw bij de bestemming

### IPv6 Packet

#### Limitations of IPv4

* IP adres uitputting
  + Gelimiteerd aantal IP adressen
  + Nu zijn er meer apparaten dan adressen
* Internet routing tabel uitbreiding
  + Aantal routers op het internet vergroot
  + Veel IP adressen betekenen veel routes
  + Gebruikt een hoop CPU en geheugen
* Gebrek aan eind aan eind verbinding
  + Om de uitputting tegen te gaan is NAT ingevoerd
    - Gebruikt een publiek IP adres voor meerdere private IP adressen
    - Door deze vertaling mapping is slechts een publiek adres gekend op het internet, niet wie eigenlijk het aan het gebruiken is binnen het netwerk
    - Sommige programma’s moeten weten met wie ze spreken

#### Introducing IPv6

* IPv6 is gecreëerd door IETF als oplossing voor de IPv4 beperkingen
  + Hogere adres plaats
    - 128 bits adressen (4\*32 bits van IPv6), dus enorm veel IP adressen
  + Verbeterde pakket behandeling
    - Simpelere IPv6 hoofding zorgt voor snellere routing en betere routing tabellen
  + Elimineert de nood aan NAT
    - Geen nood voor private/publieke IP adressen of hun vertaling
  + Geïntegreerde beveiliging
    - IPv4 was niet zo veilig.
    - IPv6 is gecreëerd om dat probleem op te lossen (betere integratie van IPsec)

#### Encapsulating IPv6

* Simpelere IPv6 hoofding
* Verschillende voordele ten opzichte van IPv4
  + Betere routing efficiëntie voor prestaties en doorstuur snelheid, schaalbaar
  + Geen behoeft aan processing checksums
  + Vereenvoudigde en meer effectievere verlenging van hoofding mechanismes
  + Een flow label veld om per flow te verwerken zonder de nood om de innerlijke transportpakket te openen

#### IPv6 Packet Header

* Versie: ‘0110’ (IPv6)/’0100’ (IPv4)
* Verkeersklasse: ToS in IPv4: was voor QoS om de prioriterings- en opstoppingscontrole
* Flow label: speciaal label voor real-time applicaties, om dezelfde verkeersdoorstroom te behouden, dus geen herordening nodig
* Payload length: lengte van het volledige pakket
* Next Header: verwijst naar de TCP header of addon header van IPv6
* Hop limit: TTL veld
* Bron/bestemmingsadres: 128 bits

## Routing

### How a Host Routes

* host routing tabel

#### Host Forwarding Decision

#### Default Gateway

* Verbindt het lokale netwet met het internet
* Bepaald hoe een bericht wordt doorgestuurd door te kijken in een database, de routing tabel
  + Als het bericht voor zichzelf is:
    - Zendt naar 127.0.0.1, lokaal host
    - Directe connectie
  + Als het bericht voor een host is binnen hetzelfde netwerk
    - Kijk naar de ARP tabel om het MAC adres te krijgen van de host
    - Lokaal netwerk route
  + Als het bericht voor een host is buiten hetzelfde netwerk
    - Zendt het bericht naar de default gateway, kijk in de ARP tabel voor het MAC adres van de default gateway
    - lokaal standaard route

#### IPv4 Host Routing Table

* Host routing tabel kan je bekijken door het commando ‘netstat –r’ of ‘print route’
  + Toont de netwerk bestemming, net mask, gateway, interface, metric
  + bestemming IP is AND-ed met het net mask om het netwerk ID te krijgen
    - kijk of het netwerk ID overeen komt met het netwerk doel
    - beste/langste overeenkomst wordt gekozen

#### IPv4 Host Routing Entries

* 0.0.0.0/0: default route, zal altijd overeen komen
* 127.\*.\*.\*: loopback adres, local host
* 192.168.10.\*: local network
* 224.0.0.0: multicast adres
* 255.255.255.255/32: lokaal broadcast adres om de DHCP te krijgen

#### IPv6 Host RoutingTable

* netwerk bestemming, gateway, interface, metric
* IPv6 host routing tabel
  + Een interface heeft 2 IPv6 adressen
    - Link lokaal adres
    - Global unicast adres
  + ::/0 local default route (allemaal 0en)
  + ::1/128: IPv6 loopback (zoals 127.\*)
  + 2001::/32: Global unicast adres
  + FE80::/64: Link local address
  + FF00::/8: multicast address (zoals 224.\*.\*.\*)
  + Geen broadcast in IPv6!!
  + Note: hexadecimal notatie en subnet mask in slash notatie

### Router Routing Tables

#### Router Packet Forwarding Decision

* Direct verbonden routes
  + Activeert de interface op een router (IP, mask en no shutdown) resulteert in een routing tabel
* Remote routes
  + Netwerk leert bij naburige routers
  + Via routing protocols
    - RIP(‘R’), EIGRP(‘D’), OSPF(‘O’)

#### IPv4 Router Routing Table

* Show IP route 🡪 commando om de routing tabel op te vragen
* Ongeveer hetzelfde als van een host

#### Directly Connected Routing Table Entries

* Direct verbonden routes
  + ‘C’: direct verbonden op die interface
  + ‘L’: link lokaal route (de interface zelf)
* Statische routes
  + Administrator kan manueel statische routes in de tabel toevoegen ‘S’
* Remote routes
  + RIP(‘R’),
  + Enhanced Interior Gateway Routing Protocol 🡪 EIGRP (‘D’),
  + Open Shortest Path First 🡪 OSPF(‘O’)

#### Remote Network Routing Table Entries

* Route source
  + Identificeert hoe het netwerk aan de router is geleerd
* Destination network
  + identificeert het adres op een buitenstaand (remote) adres
* Administrative distance
  + Identificeert de betrouwbaarheid van de route bron
* Metric
  + Identificeert de waarde toegekend aan hoe het buitenstaande netwerk te bereiken
  + Lagere waarden betekenen een de voorkeur route
* Next-hop
  + Identificeert het IP adres van de volgende router om het pakket door te sturen
* Route timestamp
  + Identificeert wanneer de router voor het laatst gehoord is
* Outgoing interface
  + Identificeert de uitgaande interface om een pakket door te sturen naar de eindbestemming

#### Next-Hop Address

* Verwijst naar het apparaat dat het packet als volgende zal verwerken

## Routers

### Anatomy of a Router

#### A Router is a Computer

* Het heeft
  + Operating System OS
  + RAM geheugen
  + ROM flash rn NV-ROM geheugen
  + Central Processing Unit CPU

#### Router CPU and OS

* CPU is nodig om OS instructies uit te voeren

#### Router Memory

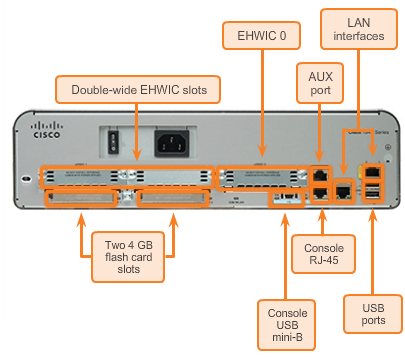
* 4 soorten
  + RAM
  + ROM
  + NVRAM
  + Flash
* RAM wordt gebruikt om applicaties en processen op te slaan
* ROM wordt gebruikt om volgende op te slaan
  + de bootup instructies
  + de basic diagnostic software 🡪 doet de power-on self-test (POST)
  + gelimiteerd stuk van de OS
* NVRAM wordt gebruikt bij Cisco om de start up configuratie file op te slaan
  + Verliest inhoud niet als de stroom eraf gaat
* Flash Memory wordt gebruikt voor de opslag van het OS

#### Inside a Router

* Ventilator
* Stroomvoorziening
* Schild voor WAN interface card WIC of high-speed WIC (HWIC)
* SDRAM
* NVRAM
* CPU
* Advanced integration Module (AIM)

#### Router Backplane

* Console USB mini-B
* Console RJ-45
  + Voor de initiële configuratie en command line interface (CLI) toegang
* USB poorten
* Double-wide EHWIC slots
* Flash card slots
* EHWIC 0
  + Twee sloten die zorgen voor modulariteit en flexibiliteit bij de router om verschillende soorten interfaces te ondersteunen
* AUX poort
  + Een RJ-45 poort om afstandig beheer toegang, gelijkaardig aan LAN toegang
* LAN interfaces
  + Twee gigabit Ethernet interfaces voor LAN toegang



#### Connecting to a Router

* Verschillende soorten poorten en interfaces, om met kabel het apparaat te verbinden
* Bij Cisco 2 categorieën
  + Management poorten (poorten voor het beheer van de router)
  + Inband router interface (WAN/LAN interfaces die het verkeer met IP adressen draagt)

#### LAN and WAN Interfaces

* Twee groepen interfaces
  + Ethernet LAN interface
    - gebruikt om LAN apparaten met kabel te verbinden
  + serieel WAN interface
    - gebruikt om routers met het externe netwerk te verbinden

### Router Boot-up

#### Cisco IOS

* Alle cisco aparaten zorgen voor
  + Addressing
  + Interfaces
  + Routing
  + Beveiliging
  + QoS
  + Bronnen management

#### Bootset Files

* IOS image File start in het flash geheugen en wordt bij opstart naar het RAM geheugen gekopieerd
* Startup configuration file start in het NVRAM geheugen en wordt bij opstart naar het RAM geheugen gekopieerd

#### Router Bootup Process

* File start in het flash geheugen en wordt bij opstart naar het RAM geheugen gekopieerd
  + ROM 🡪 voer POST uit
  + ROM 🡪 laad de bootstrap
* Locating and Loading Cisco IOS
  + Flash en TFTP server 🡪 laad internetwork OS in
* Locating and Loading the Configuration File
  + NVRAM, TFTP server, console 🡪 configuration

#### Show Version Output

* Gebruik show version om de basis hardware en enkele software componenten na te kijken (verifiëren en foutopsporing)
* Laat volgende zien
  + IOS versie
  + ROM boottrap program
  + Locatie van IOS
  + CPU en de hoeveelheid RAM
  + Interfaces
  + Hoeveelheid van NVRAM en flash

## Configuring a Cisco Router

### Configure Initial Settings

#### Router Configuration Steps

* Enable
* Configure terminal

Naam aan het apparaat geven

* Host name naamke
  + host krijgt de naam naamke

wachtwoord instellen

* Enable secret class
* Line console 0
* Password Cisco
* Login
* Exit
* Line vty 0 4
* Password Cisco
* Login
* Exit
* Service password encryption

Legale notificatie

* Banner motd #

Sla de configuratie op

* Copy running-config startup-config

Kijk de confuguratie na

* Show run

### Configure Interfaces

#### Configure LAN Interfaces

* Routers moeten bereikbaar en configureerbaar zijn
* Conf t 🡪 interface type en nummer
* Interface gigabit Ethernet 0/0
* IP address 192.168.10.1 255.255.255.0 🡪 IP en subnet mask ingeven
* Description Link to LAN-10
* No shutdown 🡪 Activeer de interface
* Exit
* Int g0/1
* IP add 192.168.11.1 255.255.255.0 🡪 Ip en subnet mask ingeven
* Des Link to LAN-11
* No shut 🡪 Activeer de interface
* exit

#### Verify Interface Configuration

* Show IP interface brief

### Configuring the Default Gateway

#### Default Gateway on a Host

* Moet in hetzelfde netwerk als het IPadres liggen

#### Default Gateway on a Switch

* Default gateway wordt gebruikt op alle apparaten die het gebruik van een router nodig hebben
* Opzetten IP adres
  + Interface vlan1
  + IP adres 192.168.10.50 255.255.255.0
  + no shut
* opzetten default gateway
  + IP default-gateway 192.168.10.1

# Transport layer

## Transport Layer Protocols

### Transportation of Data

#### Role of the Transport Layer

* Start een tijdelijke communicatie sessie tussen 2 applicaties
* Kijk niet naar: het type van het media, het pad genomen door de data, opstopping op een link, grote van het netwerk
* Primaire verantwoordelijkheden
  + Het individueel communicatie pad traceren
    - Bron / doel
  + De stromen in segmenten breken en terug in stromen zetten
    - Segment id toevoegen
  + De juiste applicatie identificeren voor elke stroom
    - Poort adres
  + Socket = IP en de poort bv 192.168.0.1:80
* 2 hoofdzakelijke transport lader protocollen
  + TCP (Transmission Control Protocol)
  + UDP (User Datagram Protocol)

#### Conversation Multiplexing

* Segmentatie van de data
  + Maakt meerdere soorten communicatie mogelijk, van verschillende gebruikers, om multiplex/van elkaar gescheiden te zijn op hetzelfde netwerk, op dezelfde tijd
    - Geen beslag leggen op de link voor slechts een data transmissie
  + Verschaft de benodigdheden aan zowel verzonden als ontvangen data wanneer er meerdere applicaties draaien
  + Zonder zou maar een applicatie per keer data kunnen ontvangen
  + Een hoofding is toegevoegd aan elk segment om het te identificeren

#### Transport Layer Reliability

* TCP/IP geeft 2 transport lader protocollen, TCP en UDP
* Verschillende applicaties vragen verschillende transport verantwoordelijkheden

#### TCP

* Transmission Control Protocol
  + Bied betrouwbare levering, verzekert data alle data arriveert op de bestemming
  + Gebruikt erkende levering en andere processen om levering te garanderen
  + Stelt grotere eisen on het netwerk –more overhead

#### UDP

* User Datagram Protocol
  + Biedt enkel de basis functies voor levering, geen betrouwbaarheid
  + Minder overhead

#### The Right Transport Layer Protocol for the Right Application

* Er is een wisselruil tussen de waarde van betrouwbaarheid en de last die het op het netwerk plaatst
* Applicatie ontwerpers kiezen het transport lader protocol op basis van de vereisten van hun applicatie

### Introducing TCP and UDP

#### Introducing TCP

* Connectie georiënteerd, bij het oprichten van sessies
  + Onderhandelt en richt verbindingen op
* Betrouwbare levering
  + Erkenning van juist ontvangen data
* Vraagt data heropbouw aan
  + Herordert data door de verschillende paden kunnen ze namelijk door elkaar staan
* Flow control
  + Als botsingen gebeuren aan de host kant (niet op de netwerk link, die is de IP zijn verantwoordelijkheid), reguleert het verkeer

#### Role of TCP

* Zodra een verbinding is gestart wordt het pakket gevolgd over de lijn
* In de hoofding staan:
  + Sequence number (32 bits)
    - Gebruikt om de data te herordenen bij de bestemming
  + Acknowledgement number (32 bits)
    - Geeft veer data de data is ontvangen
  + Header length (4 bits)
    - Data offset, geeft de grootte van de hoofding weer
  + Reserved (6 bits)
    - Gereserveerd voor in de toekomst
  + Control bits (6 bits)
    - Geven het doel en de functie van de header weer
  + Window size (16 bits)
    - Geeft het aantal segmenten dat in een keer kunnen geaccepteerd worden weer
  + Checksum (16 bits)
    - Gebruikt om foutopsporing te doen op de segment header en data
  + Urgent (16 bits)
    - Geeft weer of de data dringend is

#### Introducing UDP

* Connectieloos
  + Geen sessie opgericht, best effort
* Onbetrouwbare levering
  + Geen proces dat nagaat of herverzending nodig is
* Geen aanvraag voor data herordening
  + Geen herordening van de data
* Geen flow control
  + Als er botsingen aan de host kant zijn wordt de data gedropt

#### Role of UDP

* Handig voor applicaties die tegen data verlies kunnen

#### Separating Multiple Communications

* Poort nummers worden gebruikt door TCP en UDP om verschil te maken tussen applicaties

#### TCP and UDP Port Addressing

* Wel gekende poorten (0-1023)
  + Gerserveerd voor services en aplicaties
* Geregistreerde poorten (1024-49151)
  + Gebruikt voor user processen of applicaties, kan als dynamische poort worden gebruikt
* Dynamische poorten(49151-65535)
  + Gebruikt door cliënten om een connectie te starten
* Bestemmingspoort(naar server)
  + Gewoonlijk een wel gekende poort, onder 1024
* Bronpoort(van de cliënt)
  + Meestal een dynamische poort, kan een geregistreerde poort zijn) tussen 1024 en 65k
* Netstat
  + Gebruikt om TCP verbindingen te onderzoeken die geopend zijn en lopen op een netwerk host

#### TCP and UDP Segmentation

* Onpractisch om data in een stuk te sturen (veel te groot)

## TCP and UDP

### TCP Communication

#### TCP Reliable Delivery

* Grootste verschil tussen TCP en UDP is betrouwbaarheid
  + TCP is connectie georiënteerd
  + Creatie van een stateful connectie om de communicatiestroom te traceren
  + Erkenningen zijn de basis van betrouwbaarheid
  + Geen erkenning? 🡪 herzendt het segment 🡪 overhead (kost van betrouwbaarheid)

#### TCP Server Processes

* Poortadressen worden gebruikt om te bepalen wat de correcte deamon is

#### TCP Connection Establishment and Termination

* Three-Way Handshake (!)
  + Verzekerd dat het bestemmingsapparaat op het netwerk aanwezig is
  + Verifieerd dat het bestemmingsapparaat een actieve service heeft en aanvragen accepteert op de bestemmingspoort die de bron cliënt probeert te gebruiken
  + Informeert het bestemmingsapparaat dat de bron cliënt een verbinding probeert op te zetten op die poort
  + Elk TCP segment heeft 2 nummers: sequence number (SeqNr) en acknowledgement number (AckNr)
* 3 stappen
  + Client vraagt een TCP verbinding aan
  + Servers erkenning en vragen ook een verbinding met de cliënt
  + Client erkend de aanvraag
  + De TCP verbinding is nu tot stand gebracht

#### TCP Three-way Handshake Analysis - Step 1

* Client zendt SYN (synkroniseert de cliënt sequence getallen)
  + SeqNr\_client = randomly chosen = x, AckNr\_client = empty

#### TCP Three-way Handshake Analysis - Step 2

* Server zendt SYN en ACK: erkenning van de cliënt en zendt zelf zijn sequence getallen om te synkroniseren
  + SeqNr\_server = randomly chosen = y, AckNr\_server = x+1

#### TCP Three-way Handshake Analysis - Step 3

* Client er kent de server zijn synkronisatie aanvraag
  + SeqNr\_client = x+1, AckNr\_client = y+1
* Data kan nu verzonden worden tussen cliënt en server
* SeqNr en AckNr zijn opgeslagen in elk segment dat verzonden wordt

#### TCP Session Termination Analysis

* Om een verbinding te sluiten stuur de FIN controle vlag in de segmentheader steken
* Two-way handshake
  + Step 1: Wanneer de cliënt geen data meer heeft om te zenden in een stroom, zendt hij een segment met de FIN vlag.
  + Step 2: De server zendt een ACK flag om de ontvangst de FIN vlag om de sessie te beëindigen te erkennen
  + Step 3: De server zendt een FIN naar de cliënt om de verbinding tussen hunt e verbreken.
  + Step 4: De cliënt antwoord met een ACK vlag om de FIN vlag van de server te acepteren

### Reliability and Flow Control

#### TCP Reliability – Ordered Delivery

* Sequentie getallen worden gebruikt om de segmenten te herordenen naar de oorspronkelijke volgorde

#### TCP Reliability – Acknowledgement and Window Size

* De sequence number en acknowledgement number worden samen gebruikt om ontvangt te bevestigen
* Uitzonderlijke erkenning
  + Ack waarde x:
    - Apparaat verwacht x aantal bytes, en nu uitzonderlijke bits
* window size
  + het aantal data dat een bron kan versturen voor een bevestiging moet ontvangen moet worden

#### TCP Reliability - Data Loss and Retransmission

* Data verlies en herverzending
  + Wanneer TCP aan het bron host geen erkenning wordt ontvangen
    - Na een vooraf gekende hoeveelheid tijd zal het terug gaan naar het laatste erkenningsnummer dat ontvangen is en herzendt data vanaf dat punt vooruit

#### TCP Flow Control – Window Size and Acknowledgements

* Flow control
  + Gebruik het schermgrootte veld om de hoeveelheid data die verzonden kan worden voor een erkenning ontvangen moet worden te specifiëren
  + Past de effectieve snelheid van data versturing aan de maximale doorstroom die de bron en de bestemming ondersteunen zonder verlies aan.
  + Beheert de snelheid van verzendingen zodat alle data ontvangen zal worden en herverzendingen geminimaliseerd worden

#### TCP Flow Control - Congestion Avoidance

* Gebruik dynamische window sizes
* Verklein de window size en de zender wordt vertraagt, controleer de doorstroom

### UDP Communication

#### UDP Low Overhead versus Reliability

* UDP (User Datagram Protocol)
  + Simple protocol dat de basis transport layer function geeft
  + Gebruikt door applicaties die kleine aantal verliezen van data aan kunnen
  + Gebruikt door applicaties die geen vertraging kunnen tolereren
* Gebruikt door
  + Domain Name System (DNS)
  + Simple Network Management Protocol (SNMP)
  + Dynamic Host Configuration Protocol (DHCP)
  + Trivial File Transfer Protocol (TFTP)
  + IP telephony or Voice over IP (VoIP)
  + Online games

#### UDP Datagram Reassembly

* Grootste verschil tussen TCP en UDP:
  + UDP is connectie loos (TCP is connectie georiënteerd)
    - UDP is staatloos, geen tracering van communicatie stromen
    - Geen her verzending van verloren datagrammen
  + Poortadressen worden gebruikt om te bepalen wat de juiste deamon is

#### UDP Server Processes and Requests

* Net zoals met TCP gebruik UDP wel-known en registerend poort nummers

#### UDP Client Processes

* Selecteert random een poort uit de dynamische poorten

### TCP or UDP, that is the Question

#### Applications that use TCP

* Applicaties die niet tegen verlies van data maar wel tegen vertraging kunnen
* Enkele voorbeelden
  + Hypertext Transfer Protocol (HTTP)
  + File Transfer Protocol (FTP)
  + Simple Mail Transfer Protocol (SMTP)
  + Telnet

#### Applications that use UDP

* Drie soorten aplicaties
  + Applicaties die een beetje dataverlies kunnen tolereren, maar geen vertraging kunnen tolereren
  + Applicaties met simpele aanvragen en verzending
  + Applicaties die betrouwbaarheid niet vragen of kunnen behandelen

# IP Addressing

## IPv4 Network Addresses

### IPv4 Address Structure

#### Binary Notation!!!!Oefenen

Binair rekenen

#### Binary Number System

* Het binaire adres omzetten naar dotted decimal

#### Converting a Binary Address to Decimal

* Elk octet bestaat uit 8 bits
* Die groepen vormen een waarde van 0 tot 255

#### Converting from Decimal to Binary

Van decimaal naar binair omzetten

### IPv4 Subnet Mask

#### Network Portion and Host Portion of an IPv4 Address

* Het subnet mask zorgt dat de host weet welk deel van het IPv4 van het netwerk is en welk deel van de host is

#### Examining the Prefix Length !!!!! Examenvraag

* /24
  + Enkel de drie octetten
  + alle adressen van 1 tot en met 254
* /25
  + De 3 octetten met een extra bit
  + alle adressen van 1 tot en met 126
* /26
  + De 3 octetten met twee extra bits
  + Alle adressen van 1 tot en met 62

#### IPv4 Network, Host and Broadcast Addresses

* Broadcastadres zijn alle host bits op 1

#### First Host and Last Host Addresses

* Eerste host adres is in het host deel allemaal 0 en op het einde een 1
* Laatste host adres is in het host deel allemaal 1 en op het einde een 0

#### Bitwise AND Operation

* 1 en 1 = 1
* 0 en 1 = 0
* 0 en 0 = 0
* Netwerkadres is het host gedeelte allemaal nullen en netwerk gedeelte overschrijven

#### Importance of ANDing

* IPv4 adres optellen met het subnet mask resulteert in het netwerkadres

### IPv4 Unicast, Broadcast, and Multicast

#### Assigning a Static IPv4 Address to a Host

* Manueel een IP adres ingeven

#### Assigning a Dynamic IPv4 Address to a Host

* Krijgt automatisch een IP adres, … van de DHCP server
* Kies de optie obtain

#### Unicast Transmission

* Een op een verzenden

#### Broadcast Transmission

* Een op iedereen verzenden
* Limitid broadcast: Allemaal enen in the host gedeelte, Laat niet toe door een router weg te sturen
* directed broadcast: doeladres in het netwerkgedeelte, eerst instellen, standaard niet mogelijk

#### Multicast Transmission

* Een op groep verzenden
* Maakt gebruik van een groep IPadres

### Types of IPv4 Addresses

#### Public and Private IPv4 Addresses

* Adressen die niet op het internet kan, niet buiten het eigen netwerk zijn private adressen
  + 10.0.0.0 tot 10.255.255.255
  + 172.16.00 tot 172.31.255.255
  + 192.168.0.0 tot 192.168.255.255

#### Special Use IPv4 Addresses

* Loopbackadres: 127.0.0.1 : surfen naar jezelf

#### Legacy Classful Addressing

* /30 gebruikt tussen twee routes
* Klasse hoe hoger de klasse hoe verder de 0 wordt opgeschoven
* Klasse A netwerk
  + 1-127 range
  + 01111111
* Klasse B netwerk
  + 138-191 range
  + 10111111
* Klasse C netwerk
  + 192-223 range
  + 11011111
* Klasse D netwerk: multicast netwerk

#### Assignment of IP Addresses

* Elk bedrijf krijgt een range van netwerkadressen toegewezen.
* De bedrijven verdelen de adressen over hun klanten

## IPv6 Network Addresses

### IPv4 issues

#### The Need for IPv6

* IPv4 adressen zijn op, IPv6 heeft veel meer mogelijke adressen
* Lost de problemen van IPv4 op

#### IPv4 and IPv6 Coexistence

* Dual-stack: elke machine kan IPv4 en IPv6 spreken
* Tunnelling: IPv6 pakket wordt omgezet naar een IPv4 pakket en daar na terug omgezet naar IPv6
* Translation: router vertaalt IPv4 naar IPv6 en terug

### IPv6 Addressing

#### Hexadecimal Number System

#### IPv6 Address Representation

* 128 bits in lengte geschreven als string of hexadecimale getallen
* 16 bits of 4 hexadecimale getallen zijn een hextet

#### Rule 1 - Omitting Leading 0s

* Leesbaarheid verbeteren alle voorlopende nullen wegdoen
* 0082:0000:ABCD:1525:7524:0000:0000:1234 wordt 82:0:ABCD:1525:7524:0:0:1234

#### Rule 2 - Omitting All 0 Segments

* Alle volledige nullen samentrekken
* 0082:0000:ABCD:1525:7524:0000:0000:1234 word 82:0:ABCD:1525:7524::1234
* Hij telt zelf hoeveel nul hextet er moeten ingevuld worden

### Types of IPv6 Addresses

#### IPv6 Address Types

* Unicast
* Multicast
* anycast

#### IPv6 Prefix Length

* Gebruikt de dotted-decimal subnet mask notatie niet
* Prefix lengte (/getal) duidt het netwerkgedeelte aan
* Meeste /64

#### IPv6 Unicast Addresses

* Link local is nodig
  + Gebruikt om met andere apparaten te communiceren op hetzelfde link, subnet
  + Gaat niet door routers heen
* Global unicast
  + Gelijk het public IPv4 adres
  + Het is globaal uniek
  + Internet routeerbare adressen
  + Kan statisch of dynamisch toegekend worden
* Loopback
* Unspecified adres
  + Allemaal nullen genoteerd als ::
  + Geen herkomst terug te vinden
* Unique lokaal
  + Gelijkaardig aan het private IPv4 adres
  + Niet de bedoeling gebruikt te worden

#### IPv6 Link-Local Unicast Addresses

* Begint met FE80
* Eerste 10 bits staan vast
* Moet uniek zijn op die link of dat netwerkje

### IPv6 Unicast Addresses

#### Structure of an IPv6 Global Unicast Address

* 3 delen
  + Netwerk deel:
    - eerste 3 hextets is het global routing prefix (toegewezen door ISP)
    - 4de hextet is het subnet ID (toegewezen door het bedrijf)
  + De interface (‘host’) deel:
    - De laatste 4 hextets (afgeleid van het MAC adres van de interface

#### Static Configuration of a Global Unicast Address

* Ipv6 adres adres(tussen :: geen spaties) in de prompt
* In netwerk venster: IPv6 adres ingeven met de lengte van de prefix en de default gateway

#### Dynamic Configuration of a Global Unicast Address using SLAAC

* Methode laat toe dat een apparaat zijn prefix, prefix lengte en default gateway krijgt van een IPv6 router als RA
* Geen DHCPv6 server nodig, geen DNS informatie beschikbaar

#### Dynamic Configuration of a Global Unicast Address using DHCPv6

* Client gebruikt de informatie van de RA jiet
* Client vraagt alle gegevens aan de DHCPv6

#### EUI-64 Process or Randomly Generated

* Geeft een interface een uniek ID, en is dus makkelijk te traceren. Met privacy problemen.
* Maakt gebruik van het MAC adres van de NIC
* Willekeurig gegenereerd
* MAC(24 hoogste bits) FFFE MAC(24 laagste bits)

#### Dynamic Link-local Addresses

* FE80::/10 prefix en de interface ID
* Word automatics toegekend

#### Static Link-Local Addresses

* Zelf een link-lokaal adres instellen

#### Verifying IPv6 Address Configuration

### IPv6 Multicast Addresses

* Multicast addresses: enkel packet naar groep
  + Multicast IP adres kan enkel een bestemming IP zijn
  + Als een host wil luisteren naar een Multi cast groep 🡪 kom bij de groep
* IPv6 Multi cast adressen hebben een prefix FFxx::/8
  + Alle IPv6 adressen die een Multi cast zijn starten met FF
  + De xx definieert de scope, zoals FF02: enkel lokale segmenten
  + FF02: ‘Wat gebeurt in Vegas, blijft in Vegas’

#### Assigned IPv6 Multicast Addresses

* FF02::1: all-nodes multicast
  + Zendt naar alle knooppunten op de lokale segmenten
    - Opgepast: het is zoals een broadcast, er kunnen miljarden host zijn
* FF02::2: all-router Multi cast
  + Zendt naar alle routers op het locaal segment

#### Solicited-Node IPv6 Multicast Addresses

* Automatisch gecreert al seen global unicast of link-local address is toegewezen
* Primair gebruikt voor L2 adres resolutie (MAC adres)
  + In IPv4 werd ARP, gebruikt, maar deze gebruikt broadcast
  + Hoe het L2 adres van een host B krijgen als er geen broadcast gebruikt kan worden?
  + Je kan het FF02::1 all-nodes adres gebruiken, maar alle hosts van het segment zou het nakijken 🡪 IPv6 kan miljarden hebben!
  + Gebruik de gevraagde knooppunten Multi cast adressen van host B
    - Je weet het link-lokaal IPv6 adres van host B
    - Neem het laatste deel (24 bits) van dat adres en plak het achter FF02::1:FFxx:xxxx

## Connectivity Verification

### ICMP

#### ICMPv4 and ICMPv6 Messages

* ICMP (internet control messaging protocol) messages
  + Host bevestiging: ICMP echo vraag/antwoord
  + Doel of service onbereikbaar: ICMP bericht ‘kan host niet bereiken’
  + Time exceeded: ICMP bericht om te vertellen dat TTL=0 voor een pakket

#### ICMPv6 Router Solicitation and Router Advertisement Messages

* ICMPv6 heeft bijkomende functies
  + Neighbor discovery protocol (NDP))
    - Router Solicitation (RS) / Router Advertisement (RA)
      * RS: host heft een IPv6 nodig via SLAAC
        + RS Multi cast naar alle routers(FF02::2)
      * RA: router zendt een RA in antwoord van een RS of elke 200 s
        + RA Multi cast naar alle knooppunten(FF02::1)

#### ICMPv6 Neighbor Solicitation (NS) and Neighbor Advertisement (NA) Messages

* Gebruikt voor twee redenen
* Address resolution
  + Geen ARP functionaliteit in IPv6, dus om het MAC adres van een host te krijgen moet je het IPv6 adres kennen
    - Zendt een NS naar het doel via het solicites node IPv6 adres(FF02::1:FFxx:xxxx)
    - Het doel zal antwoorden met een NA dat het mac adres bevat
* Duplicate Address Detection (DAD)
  + Wanneer een IPv6 adres aan een host is toegekend (dynamisch of statisch
    - Kijkt na om te zien of er duplicaten zijn op het segment
    - Zendt een NS naar het eigen IPv6 adres, als er duplicaten zijn zal het antwoorden met een NA

### Testing and Verification

#### Ping - Testing the Local Stack

* Pingen naar het eigen IP adres

#### Ping - Testing Connectivity to the Local LAN

* Pinged naar de default gateway

#### Ping - Testing Connectivity to Remote

* Pinged naar een afstandige host

#### Traceroute - Testing the Path

* Genereet een lijst van hops die succesvol bereikt zijn over het pad
* Geeft de round trip time
* Gebaseerd op de TTL field inIPV4, of het IPv6 hop limit

# Subnetting IP networks

## Subnetting an IPv4 Network

### Network Segmentation

#### Reasons for Subnetting

* Grote netwerken moeten opgedeeld worden in kleinere subnetten om zo kleinere groepen toestellen en services te creëren om
  + Verkeer te controleren binnen het subnet
  + Netwerkverkeer te verminderen en de verbetering van prestaties
* Subnetting:
  + Proces van segmentatie van een netwerk in meerdere kleinere netwerk plaatsen sub netwerken of sub nets genoemd

#### Communication Between Subnets

* Een router is nodig om apparaten om verschillende netwerken en sub nets te laten communiceren
* Elke router interface moet een IPv4 host adres hebben dat toebehoort aan het netwerk of subnet waar de router aan verbonden is
* Apparaten op een netwerk en sub netwerk gebruiken de router interface verbonden aan hun LAN als hun default gateway
* Om te bepalen of verkeer voor een lokale host of afstandelijke host is gebruikt de router het subnet mask

### IP Subnetting is FUNdamental

#### The Plan

* Er zijn twee overwegingen wanneer men sub nets plant:
  + Het aantal nodige sub nets
  + Het maximaal aantal nodige host adressen
* Onthoud dat volgende IP adres ranges private zijn
  + 10.0.0.0 with a subnet mask of 255.0.0.0
  + 172.16.0.0 with a subnet mask of 255.240.0.0
  + 192.168.0.0 with a subnet mask of 255.255.0.0

#### The Plan – Address Assignment

* Creëer standaards voor de toewijzing van IP adressen
* Wat krijgt een :
  + Statisch IP adres
  + IP adres van de DHCP server

### Subnetting an IPv4 Network

#### Basic Subnetting

* Prefix en subnet mask zijn twee manieren om hetzelfde te laten zien, namelijk het netwerk deel van een adres
* Subnets worden gecreëerd door een of meer host bits te gebruiken als netwerk bits
  + Hoe meer host bits geleend, hoe meer sub nets
* De bits kunnen enkel bij het host gedeelte geleend worden, het netwerkgedeelte is vastgelegd bij de provider en onveranderbaar
* 24 bits in het netwerk gedeelte, 8 bits in het host gedeelte 🡺 subnet mask 255.255.255.0 of /24 notatie
* 25 bits in het netwerk gedeelte, 7 bits in het host gedeelte 🡺 subnet mask 255.255.255.128 of /25 notatie

#### Subnets in Use

* Eerste of laatste beschikbare IP adres wordt gebruikt voor de router interface
* Richtlijnen voor sub nets
  + Network adres: allemaal 0 in het host gedeelte
  + First host adres: allemaal 0 in het host gedeelte met een 1 op de aller rechtste bit
  + Last host adres: allemaal 1 in het host gedeelte met een 0 op de aller rechtste bit
  + Broadcast adres: allemaal 1 in het host gedeelte
* Om het eerste IP adres toe te wijzen gebruik het IP adres commando

#### Subnetting Formulas

* Formule om het aantal bruikbare host te bepalen
  + 2^n-2
  + 2^n (n= het aantal host bits die over zijn)
  + -2: subnetID en broadcast adres kunnen niet gebruikt worden
* Het aantal subnetten berekenen
  + 2^n (n=het aantal geleende bits)
  + Kijk hoeveel sub nets nodig zijn en neem het aantal dat het best past

#### Creating 4 Subnets

* 2 host bits worden geleend 2^2=4 sub nets
* Subnet mask: 255.255.255.192 laatste octet (1100 0000)
* 6 host bits blijven over 2^6=64 host per subnet
  + 2 adressen staan al vast dus nog 62 adressen om te verdelen
* Voorbeeld van de eerste twee sub nets
  + PC1 (192.168.1.2/26) gebruikt 192.168.1.1 (G0/0 interface address of R1) als zijn default gateway adres
  + PC2 (192.168.1.66/26) gebruikt 192.168.1.65 (G0/1 interface address of R1) als zijn default gateway adres
* Alle apparaten op hetzelfde subnet hebben een host adres van de range van host adressen en zullen hetzelfde subnet mask gebruiken

#### Creating 8 Subnets

* 3 host bits worden geleend 2^3=8 sub nets
* Subnet mask: 255.255.255.224 laatste octet (1110 0000)
* 5 host bits blijven over 2^5=32 host per subnet
  + 2 adressen staan al vast dus nog 30 adressen om te verdelen
* Voorbeeld van de eerste vier sub nets
  + PC1 (192.168.1.2/27) gebruikt 192.168.1.1 als zijn default gateway adres.
  + PC2 (192.168.1.34/27) gebruikt 192.168.1.33 als zijn default gateway adres.
  + PC3 (192.168.1.98/27) gebruikt 192.168.1.97 als zijn default gateway adres.
  + PC4 (192.168.1.130/27 ) gebruikt 192.168.1.129 als zijn default gateway adres.

#### Creating 100 Subnet s with a /16 prefix

* 7 host bits worden geleend 2^7=128 sub nets
  + 1 host bit blijft over 2^1=2 host per subnet
  + 2 adressen staan al vast dus nog 0 adressen om te verdelen
* Standaard mask van /16 of 255.255.0.0
  + 16 bits netwerk en 16 bits host
  + 16 host bits om te lenen
  + 7 host bits worden geleend 2^7=128 sub nets
  + 9 host bits blijven over
  + Derde octet = 1111 1110, vierde octet=0000 0000
  + Subnetting gebeurt in het derde octet

#### Calculating the Hosts

* 7 host bits worden geleend 2^7=128 subnets
* 9 host bits blijven over 2^9 = 512 hosts
* 2 adressen staan al vast dus nog 510 adressen om te verdelen
* Eerste host adres = 172.16.0.1
* Laatste host adres = 172.16.1.254

#### Calculating the Hosts

* Als zelfs meet dan 100 sub nets nodig zijn gebruik /8 of 255.0.0.0
* 10 host bits worden geleend 2^10=1024 sub nets
* 14 host bits blijven over 2^14 = 16384 hosts
* 2 adressen staan al vast dus nog 510 adressen om te verdelen
* Subnet mask = 255.255.192.0
* Eerste host adres = 10.0.0.1
* Laatste host adres = 10.0.63.254

### Determining the Subnet Mask

#### Subnetting Based on Host Requirements

* Hoeveel host zijn nodig in een subnet
* Hoeveel sub nets zijn nodig

#### Subnetting Network-Based Requirements

* Soms is het aantal sub nets belangrijker dan het aantal host in dat subnet

#### Subnetting to Meet Network Requirements

* Het is belangrijk om balans te vinden tussen het aantal benodigde sub nets en het aantal benodigde host in het grootste subnet
* Ontwerp het adresseringsschema om het maximum aantal host van elk subnet te voorzien
* Laat groei toe in elk subnet

### 9.1.5 Benefits of Variable Length Subnet Masking

#### Traditional Subnetting Wastes Addresses

* Traditioneel subnetten
  + Hetzelfde aantal adressen is voorzien voor elk subnet
* Subnets die minder adressen nodig hebben ongebruikte (verspilde) adressen
* Variable Length Subnet Mask (VLSM) of een subnet in subnet verdelen biedt efficiënter gebruik van adressen

#### Variable Length Subnet Masks (VLSM)

* VLSM laat toe om een netwerk plaats te verdelen in ongelijke delen
* Het subnet mask zal variëren afhankelijk van hoeveel bits er geleend zijn voor een bepaald subnet

#### Basic VLSM

* Een subnet wordt verdeelt in meerdere sub nets
* Subnet wordt verdeelt zodat het minimaal aan adressen verloren gaan

#### VLSM in Practice

* Het kan zijn dat sommige hosts een host adres een /27 mask hebben en andere een /30 mask hebben
* Host zullen het adres dat samengaat met de aanhangende router LAN interface als default gateway
* Configuratie van de router
  + Interface gigabitethernet 0/0
  + Ip adres 192.168.20.1.255.255.255.224
  + Exit
  + Interface serial 0/0/0
  + Ip adres 192.168.20.255.255.255.255.252

#### VLSM Chart

* Tool voor de adresserings planning
* Toont welke blokken adressen vrij zijn en welke al bezet zijn

## Addressing Schemes

### Structured Design

#### Planning to Address the Network

* De toewijzing van netwerk adressen zou gepland en gedocumenteerd worden om:
  + Duplicaten te vermijden
  + Een gecontroleerde toegang te geven
  + Veiligheid en prestatie bij te houden
* Verschillende apparaten in een netwerk:
  + eindgebruikers
  + Servers en randapparatuur
  + Hosts die vanaf het internet toegankelijk zijn
  + Tussenliggende apparaten
  + Gateway

#### Assigning Addresses to Devices

* Het kan dat een netwerk adresseringsplan verschillende range van het subnet gebruiken voor elk soort apparaat
* Adressen voor cliënten: meestal dynamisch toegewezen door gebruik te maken van de Dynamic Host Configuration Protocol (DHCP)
* Adressen voor servers en randapparatuur: statische IP adres, voorspelbare IP adressen zijn hierop nodig
* Adressen voor hosts die via het internet toegankelijk zijn: moeten statisch zijn
* Adressen voor tussenliggende apparaten: statisch, manueel ingeven
* Adressen voor de gateway (routers en firewalls): elke interface heeft een eigen IP adres. Typisch heeft de router interface de laagste of de hoogste adres van het netwerk. Dit moet consequent gebeuren

## Design Considerations for IPv6

### Subnetting an IPv6 Network

#### Subnetting Using the Subnet ID

* Subnetten met IPv6: stukke makkelijker
  + Met IPv4 moesten we de adressen schaarste beheren
  + Niet zo’n probleem bij IPv6 (daar maakt de lengte niet uit)
  + In IPv6 ontwikkelen we de subnetten om makkelijk begrepen, logisch en hiërarchisch te zijn
    - Kijk naar een IPv6 adres en je weet van waar het is
    - Vb.: 2001:0DB8:ACAD:0000::/64
* Elk subnet krijgt een nieuw subnet ID van de subnet hextet
  + Makkelijk in hex 🡪 geen vertaling naar decimalen meer nodig
  + Enkel het subnet ID hextet verhogen

#### IPv6 Subnet Allocation

* Het maakt niet uit als /64 te lang is voor een WAN link (IPv6)
* Het is makkelijker, logischer

#### Subnetting into the Interface ID

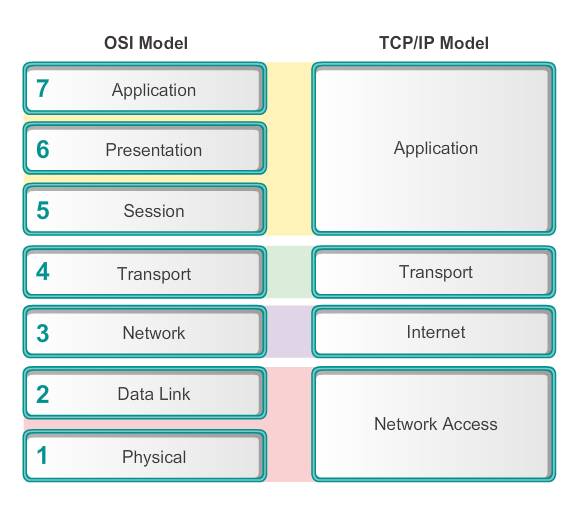
* Als je meer beveiliging wilt, gebruik minder hosts per netwerk
  + Leen een bit van het host gedeelte, zoals bij IPv4
  + Maar als je /65 gebruikt in plaats van /64 moet je het hex nummer naar binair omzetten om te zien wat het subnet is en wat het interface ID is
  + Dus altijd 4 bits (een nible) lenen, een volledig hexadecimaal nummer
    - Dan zie je wat het subnet is en wat het interface id
  + Gebruik altijd: /64, /68, /72, /76, … (nibbles)
  + Gebruik geen: /65, /66, /67, …

# Application Layer

## Application Layer Protocols

### Application, Session and Presentation

#### OSI and TCP/IP Models Revisited



#### Application Layer

* De applicatie lag voorziet de interface naar het netwerk

#### Presentation and Session Layers

* Presentatie lag heeft drie primaire functies
  + Coderen en converteren van de applicatie laag data
  + Compressie van data
  + Encryptie van data voor verzending en het decrypteren van data bij aankomst aan de bestemming
  + Motion Picture Experts Group (MPEG)
  + Graphics Interchange Format (GIF)
  + Joint Photographic Experts Group (JPEG)
  + Portable Network Graphics (PNG)
* Sessie laag
  + Creert en onderhoud dialogen tussen bron en bestemming applicaties
  + Verzorgt de uitwisseling van informatie om dialogen te beginnen, ze actief te houden en sessies te herstarten

#### TCP/IP Application Layer Protocols

* Domain Name Service Protocol (DNS) : vormt internet namen om naar IP adressen
* Telnet: een terminal wedijverend protocol die toegang op afstand bidet aan servers en netwerk apparaten
* Bootstrap Protocol (BOOTP): een voorloper van DHCP, een netwerk protocol gebruikt op de IP adres gegevens te verkrijgen bij de opstart
* Dynamic Host Control Protocol (DHCP): wijst een IP adres, subnet mark, default gateway en DNS toe aan een host
* Hypertext Transfer Protocol (HTTP): gebruikt om bestanden te verzenden die de opmaak van de webpagina’s op het www bepalen
* File Transfer Protocol (FTP): gebruikt om interactieve bestanden te verzenden tussen twee systemen
* Trivial File Transfer Protocol (TFTP): gebruik voor verbindingsloze verzending van actieve bestanden
* Simple Mail Transfer Protocol (SMTP): om mail berichten en bijlage te verzenden
* Post Office Protocol (POP): gebruikt door email cliënt om email te verkrijgen van een server op afstand
* Internet Message Access Protocol (IMAP) : een ander protocol voor email ophaling

### How Application Protocols Interact with End-User Applications

#### Peer-to-Peer Networks

* Beide apparaten worden als gelijk beschouwd in de communicatie
* De rollen van cliënt en worden op aanvraag opgesteld

#### Peer-to-Peer Applications

* Client en server zitten in dezelfde communicatie
* Beiden kunnen een communicatie beginnen en zijn beschouwd als gelijken in het communicatieproces

#### Common P2P Applications

* Met P2P applicatie, elke computer in het netwerk die loopt op de applicatie kan als cliënt of als server functioneren voor de andere computers in het netwerk die die applicatie lopen
* Veelvoorkomende P2P applicatie zijn bv:
  + eDonkey
  + eMule
  + Shareaza
  + BitTorrent
  + Bitcoin
  + LionShare
* Sommige P2P applicaties zijn gebaseerd op het Gnutella protocol die toestaat dat mensen bestanden delen op hun harde schijf met anderen

#### Client-Server Model

* Server: bronnen zijn bewaard op de server
* Client: een cliënt is een hardware/software combinatie die mensen direct gebruiken

## Well-Known Application Layer Protocols and Services

### Common Application Layer Protocols

#### Application Layer Protocols Revisited

* Drie applicatie laag protocollen die broken zijn bij dagdagelijks gebruik of spel zijn:
  + Hypertext Transfer Protocol (HTTP): surfen op het web
  + Simple Mail Transfer Protocol (SMTP): gebruikt om gebruikers email te laten zenden
  + Post Office Protocol (POP): gebruikt om gebruikers email te laten ontvangen

#### Hypertext Transfer Protocol and Hypertext Markup Language

* uniform resource locator (URL)
* Voorbeeld: URL: <http://www.cisco.com/index.html>
* Eerst interpreteert de browser de drie delen van de URL
  + http (het protocol of schema)
  + www.cisco.be (de servernaam)
  + index.html (het specifieke bestandsnaam dat gevraagd is)
* de browser kijkt met een naamserver (DNS) na om www.cisco.com te converteren naar een numeriek adres
* het gebruik van het http protocol vraagt het verzenden van een GET request naar de server en vragen nar het index.html bestand
* de server zendt de html code voor deze pagina
* de browser ontcijfert de html code en deelt de pagina in

#### HTTP and HTTPS

* Ontwikkeld om html pagina’s te publiceren en terug te krijgen
* Gebruikt voor data verzending
* Specifieert een vraag/antwoord protocol
* Drie veelvoorkomende berichttypes zijn GET, POST en PUT
* GET is een cliënt vraag voor data
* POST en PUT worden gebruikt om berichten te zenden die data upload naar de web server
* HTTP Secure (HTTPS)
* Secure Socket Layer (SSL)
* Bij HTTPS wordt de data versleuteld met SSL voor het verzonden wordt

#### SMTP, POP, and IMAP

* SMTP: email zenden naar een mail server, of tussen mail servers
* Het ontvangen van mail van een mailserver
  + POP: houdt en organiseert mail lokaal
  + IMAP: houdt en organiseert mail op een server
  + http: web mail
  + email verzenden naar de emailserver of tussen emailservers 🡺 SMTP
  + om mail te ontvangen bij de cliënt 🡺 POP of IMAP

#### SMTP, POP, and IMAP (cont.)

* SMTP zet mails in een rij om deze later opnieuw te verzenden als de bestemming niet online is. De server kijkt deze rij regelmatig na. Als de mail nog niet geleverd kan worden na een verloop van tijd, krijgt de verzender een undeliverable mail terug

#### SMTP, POP, and IMAP (cont.)

* POP: email wordt afgehaald naar de cliënt en op de server verwijdert

#### SMTP, POP, and IMAP (cont.)

* IMAP: een kopie van de email wordt afgehaald, het origineel blijft op de server bewaard tot deze manueel worden verwijdert

### Providing IP Addressing Services

#### Domain Name Service

* Een menselijk legale naam wordt opgezet naar zijn numerieke netwerk apparaat adres door het DNS protocol
* Als de numeriek adres verandert is dit geen probleem, de naam blijft dezelfde

#### DNS Message Format

* Berkeley Internet Name Domain (BIND)
* A: een eindgebruiker
* NS: een gezaghebbende server
* CNAME: de volledige domein naam, gebruikt wanneer meerdere services gebruik maken van een netwerkadres maar elk zijn eigen invoer in de DNS
* MX: mail exchange, legt een domein naam aan bij de lijst van mail exange servers
* ‘ipconfig /displaydns’: toont alle opgeslagen DNS ingaven

#### DNS Hierarchy

* Voorbeelden van top-level domeinen
  + .au Austrialie
  + .co Colombia
  + .com bedrijven en industrie
  + .jp Japan
  + .org non-profit organisatie
* Voorbeeld [www.cisco.com](http://www.cisco.com)
  + .com top-level
  + Cisco.com ligt een level onder.com

#### Nslookup

* Zet de domain naam ([www.blabla.be](http://www.blabla.be)) om naar het numerieke adres

#### Dynamic Host Configuration Protocol

* DHCP laat een host toe om een IP adres dynamisch te verkrijgen
* DHCP server wordt gecontacteerd en een adres wordt aangevraagd. – kiest een adres uit een geconfigureerde range van adressen (een pool genoemd) en leent het aan de host voor een vooraf gekende periode
* DHCP gebruikt hosts zoals eindgebruikers voor algemene doelen, en statische adressering wordt gebruikt voor netwerkapparaten zoals gateways, switches, servers en printers

#### DHCP Operation

* Client stuurt DHCP DISCOVER
* Server antwoord met een DHCP OFFER
* Client antwoord dan met een DHCP REQUEST
* Server antwoordt tenslotte met een DHCP ACK of DHCP NAK (niet ack)

### Providing File Sharing Services

#### File Transfer Protocol

* FTP laat toe dat data verzonden wordt tussen een server en een cliënt
* FTP cliënt is een applicatie die loopt op een computer die gebruikt wordt om data te pushen en pullen van een server die loopt op een FTP deamon
* Om data succesvol de verzenden heeft FTP 2 verbindingen nodig tussen cliënt en server, een voor de commando’s en hun antwoord, de andere voor de echte bestands uitwisseling

#### Server Message Block

* SMB
* Client brengt een langdurige verbinding met servers toe stand
* Nadat de verbinding tot stand is gebracht kan de gebruiker toegang krijgen tot de bronnen op de server alsof de bron lokaal is op de cliënt host

# It’s a Network

## Create and Grow

### Devices in a Small Network

#### Small Network Topologies

* Wat is een typisch klein netwerk topologie
  + Pc’s, opslagserver, printer, VoIP telefoon, …

#### Device Selection for a Small Network

* Factoren waar rekening mee gehouden moet worden wanneer tussenliggende apparaten worden geselecteerd:
  + Kost
  + Aantal poorten
  + Snelheid
  + Uitbreidbaar/ modulair
  + handelbaarheid

#### IP Addressing for a Small Network

* IP adressering schema zou gepland, gedocumenteerd en onderhouden worden gebaseerd op het type apparaten die het adres ontvangen
* Voorbeelden van apparaten die deel zullen uitmaken van het IP ontwerp:
  + Eind apparaten voor gebruikers
  + Servers en randapparatuur
  + Hosts die bereikbaar zijn vanaf het internet
  + Tussenliggende apparaten
* De IP schema’s plannen helpt de administrator om:
* De apparaten na te gaan en te problemen op te lossen
* Controleren van bronnen

#### Redundancy in a Small Network

* Redundancy helpt om enkele punten van mislukking te elimineren
* Verbeterd de betrouwbaarheid van het netwerk

#### Design Considerations for a Small Network

* Het volgende zou in een netwerk plan moeten zitten
  + Beveiligde bestand en mail servers op een centrale locatie
  + De locatie beschermen zowel fysieke als logische beveiliging maatregelen
  + Creëren van redunancy in het server park
  + Configureren van redundante paden naar de servers.

### Protocols in a Small Network

#### Common Applications in a Small Network

* Netwerk aplicaties
  + Programma’s om over het internet te communiceren
  + Vb. email, webbrowser
* Applicatie laag services
  + Vb. bestandsuitwisseling
  + Sommige programma’s hebben dit nodig om aan de bronnen te raken

#### Common Protocols in a Small Network

* DNS server: service die het IP adres van een web site of domein naam geeft om te verbinden
* Tenet server: service die administrators toelaat in te loggen op een host vanop afstand
* E-mail server (IMAP, POP, SMTP): gebruikt om e-mails te sturen van cliënt naar server over het internet
* DHCP server: service die IP adres, subnet mask, default gateway en andere informatie toewijst
* Web server: HTTP, gebruikt om informatie tussen web cliënt en web server uit te wisselen
* FTP server: laat toe om bestanden te downloaden en uploaden tussen server en cliënt

#### Real-Time Applications for a Small Network

* Infrastructuur: moet geëvalueerd worden om zeker te zijn dat het netwerk de voorgestelde real time applicaties ondersteunt
* VoIP wordt uitgevoerd in bedrijven die nog steeds traditionele telefoons gebruiken
* IP telephony: de IP telefoon zelf doet voice-to-IP omzetting
* Real time Video Protocols: gebruik:
  + Real-Time Transport Protocol (RTP)
  + Real-Time Transport Control Protocol (RTCP)
  + Dit laat QoS mecanismes toe

### Growing to Larger Networks

#### Scaling a Small Network

* Belangrijke overwegingen wanneer een groot netwerk wordt gecreëerd:
  + Documentatie: fysieke en logische topologie
  + Apparaat inventaris: lijst van apparaten die gebruik maken van het netwerk of het omvatten
  + Budget: specifieer het IT budget, inclusief fiscaal jaarlijks gereedschap aankoop budget
    - TCO: Total Cost of Ownership
    - Voorbeelden: Printer: hoeveel inkt, hoeveel stroom, …
  + Verkeer analyses: protocols, applicaties en services en hun respectieve verkeerseisen zouden gedocumenteerd moeten worden

#### Protocol Analysis of a Small Network

* Informatie wordt verzamelt door protocol analyse kan gebruikt worden om beslissingen te maken over hoe verkeer efficiënter te beheren
* Om de flow patronen te ontdekken
  + Vang het verkeer op tijdens piekmomenten
  + Doe de vangst op verschillende netwerksegmenten

#### Evolving Protocol Requirements

* Netwerk administrator kan IT snapshots van werknemer applicatie gebruik krijgen
* Snapshots sporen netwerk gebruik en verkeer flow eisen op
* Snapshots helpen informeren van netwerk aanpassingen nodig om werknemer productiviteit te verhogen

## Keeping the Network Safe

### Network Device Security Measures

#### Categories of Threats to Network Security

* Informatie diefstal
* Data verlies en manipulatie
* Identiteitsdiefstal
* Onderbreking van service

#### Physical Security

* Vier classen van fysieke bedreigingen zijn:
* Hardware bedreiging: fysieke schade aan servers, routers, switches, kabel boom en werkstations
* Omgevingsbedreigingen: extreme temperaturen of extreme luchtvochtigheid
* Elektrische bedreigingen: voltage pieken, te weinig stroom toevoer, volledige stoomverlies
* Onderhoudsbedreigingen: slecht behandelen van elektrische componenten, te weinig reserve onderdelen, slechte bekabeling, slechte labeling

#### Types of Security Vulnerabilities

* Technologische zwakheden
* Configuratie zwakheden
* Veiligheidsbeleid zwakheden

### Vulnerabilities and Network Attacks

#### Viruses, Worms, and Trojan Horses

* Virussen: software verbonden aan een ander programma om ongewenste functie uit te voeren op een workstation
* Wormen: afzonderlijk programma dat een systeem aanvalt en probeert om een specifieke zwakheid uit te buiten. De worm kopieert zijn programma van de aanvallende host naar het nieuwe uitgebuite systeem om de cirkel opnieuw te beginnen
* Trojaans paard: verschilt enkel in dat de hele applicatie geschreven is om als iets anders uit te zien, wanneer het eigenlijk een aanval tool is

#### Reconnaissance Attacks

* Ongeautoriseerd ontdekken en indelen van systemen, services of zwakheden
* Enkele voorbeelden
  + Internet queries
  + Pingsweeps
  + Port scans
  + Packet sniffers

#### Access Attacks

* Valt zwakheden aan in authenticate
* Laat toe dat iemand toegang krijgt tot informatie die ze niet mogen zien

#### DoS Attacks

* DoS
* DDoS 🡺 met overgenomen PC’s

### Mitigating Network Attacks

#### Backup, Upgrade, Update, and Patch

* Blijf bij met de laatste versie van antivirus software
* Instaleer geüpdatete beveiligingspatches
* Hoe een worm kwijt raken: containment, inoculation, quarantine, treatment

#### Authentication, Authorization, and Accounting

* AAA of triple A
* Authenticatie: gebruikers en administrators moeten hun identiteit bewijzen. Autenticatie kan verkregen worden door gebruik van een username en wachtwoord combinaties, vraag en antwoord vragen, token kaarten, en andere methodes
* Autorisatie: tot welke bronnen de gebruiker toegang heeft en welke operaties de gebruiker toegestaan is uit te voeren
* Accounting: houdt bij wat gebruikers openen, de tijd dat de bron was geopend en elke gemaakte verandering

#### Firewalls

* Een firewall bevindt zich tussen twee of meer netwerken. Het controleert het verkeer en voorkomt ongeautoriseerd toegang. Gebruikte methodes:
  + Packet Filtering: toegang op basis van IP of MAC adressen
  + Application Filtering: toegang voor applicatie gebaseerd op de poorten
  + URL Filtering: toegang voor websites gebaseerd op specifieke URL’s of sleutelwoorden
  + Stateful Packet Inspection (SPI): binnenkomende pakketten moeten legale antwoorden zijn op aanvragen van interne hosts
* Soorten firewalls
  + Appliance-based
  + Server-based firewalls system
  + Integrated firewalls
  + Personal firewalls

#### Endpoint Security

* Veelvoorkomende eindpunten zijn laptoppen, desktoppen, servers, smartphones en tabletten
* Werknemers moeten de door het bedrijf opgestelde veiligheidsbeleid opvolgen om hun apparaten te beveiligen
* Veiligheidsbeleid bevatten meestal het gebruik van antivirus software en host inbraakpreventie

### Securing Devices

#### Introduction to Securing Devices

* Deel van netwerk beveiliging zijn beveiligingsapparaten, inclusief eindapparaten en tussenliggende apparaten
* Standaard wachtwoorden en usernames zouden onmiddellijk moeten worden verandert
* Toegang tot systeem bronnen zou beperkt moeten zijn tot enkel de personen die voor die bronnen te gebruiken geautoriseerd zijn
* Alle onnodige services en applicaties zouden uitgezet en verwijdert moeten worden
* Update met beveiligingspatches zodra deze vrij komen

#### Passwords

* Zwakke wachtwoorden:
  + Woorden uit het woordenboek
  + Moeder haar meisjes naam
  + Automerk
  + Naam en of geboortedatum
  + Simple woorden en nummers
* Sterke wachtwoorden:
  + Combinatie van alfanumerieke karakters
  + Combinatie van alfanumerieke karakters, symbolen en spaties
* Enkele richtlijnen
  + Complex wachtwoord
  + Minstens 8 tekens lang
  + Vermijd makkelijke wachtwoorden (woordenboek woorden, persoonlijke data, …)
  + Spel opzettelijk woorden fout
  + Verander regelmatig je wachtwoorden
  + Schrijf wachtwoorden niet op

#### Basic Security Practices

* Encrypteert wachtwoorden / service password-encryption
* Vraag een minimum lengte voor de wachtwoorden / security passwords min-length
* Blokkeer brute kracht aanvallen / login block-for 120 attempts 3 within 60
* Gebruik banner berichten/ banner motd #message#
* Zet EXEC time-out (log uit indien geen actie binnen x aantal tijd)/ line vty 0 4 daarna exec-timeout 10

#### Enable SSH

* Telnet is niet veilig, de data is niet versleuteld
* Hoe SSH instellen
  + Conf t
  + IP domain-name span.com
  + Crypto key generate rsa general-keys modulus 1024
  + Username Bob secret cisco
  + Line vty 0 4
  + Login local
  + Transport input ssh
  + exit

## Basic Network Performance

### Ping

#### Interpreting Ping Results

* ! geeft de ontvangst van een ICMP echo antwoord aan
* . geeft een tijd verlopen terwijl wachten een ICMP echo antwoord aan
* U een ICMP onbereikbaar bericht is ontvangen

#### Extended Ping

* Cisco IOS biedt een extended mode van ping commando
* R2# **ping**
* Protocol [IP]:
* Target IP address: **192.168.10.1**
* Repeat count [5]:
* Datagram size [100]:
* Timeout in seconds [2]:
* Extended commands [n]: **y**
* Source address or interface: **10.1.1.1**
* Type of service [0]:

#### Network Baseline

* Rapporten over de gezondheid van het netwerk op een zeker punt in de tijd

### Tracert

#### Interpreting Tracert Messages

* Tracert IP adres

### Show Commands

#### Common show Commands Revisited

* De status van bijna elk proces of functie van de router kan getoond worden door het gebruik van het show commando
* Vaak gebruikte show commando’s
  + show running-config
  + show interfaces
  + show IP interface brief
  + show ARP
  + show IP route
  + show protocols
  + show version

### Host and IOS Commands

#### ipconfig Command Options

* ipconfig: toont IP adressen, subnet mask, default gateway
* ipconfig /all: toont ook de MAC adressen
* ipconfig /displaydns: toont alle opgeslagen DNS ingaven in een windows systeem

#### ARP Command Options

* ARP –a: alle apparaten die momenteel in de ARP geheugen van de host zitten
* ARP –d: maakt het ARP geheugen van de host leeg

#### Show cdp neighbors Command Options

* geeft volgende weer
  + Device identifiers
  + Address list
  + Port identifier
  + Capabilities list
  + Platform
* show cdp neighbors detail commando geeft de IP adressen van naburige aparaten

#### Using the show IP interface brief Command

* Kan gebruikt worden om de status van alle netwerk interfaces op een router of switch te verifieren

## Managing IOS Configuration Files

### Router and Switch File Systems

#### Router File Systems

* Show file system commando: geeft alle beschikbare bestandssystemen op een Cisco 1941 router
* Show file system commando geeft weer hoeveel geheugen nog vrij is, type file system en hun toestemmingen
* \* asterisk toont dat dat de huidige default file system is

#### Switch File Systems

* show file systems commando: geeft alle beschikbare file systems op een catalyst 2960 switch

### Back up and Restore Configuration files

#### Backing up and Restoring using Text Files

#### Backing up and Restoring using TFTP

* Configuration files kunnen opgeslagen worden op een Trivial File Transfer Protocol (TFTP) server
* copy running-config tftp: slaat de lopende configuratie op naar een tftp server
* copy startup-config tftp: slaat de start-up configuratie op naar een tftp server

#### Using USB Ports on a Cisco Router

* USB flash drive moet geformatteerd worden in FAT 16 formaat
* Kan meerdere kopieën van de Cisco IOS en meerdere router configuraties
* Laat de administrator toe om makkelijk configuraties over te nemen van router naar router
* Voorbeeld
  + Router# dir usbflash0:
  + Directory of usbflash0:/
  + 1 -rw- 30125020 Dec 22 2032 05:31:32 +00:00 c3825-entservicesk9-mz.123-14.T
  + 63158272 bytes total (33033216 bytes free)

#### Backing up and Restoring using a USB

* Het is slim om eerst de show file systems commando uit te voeren