# Ethernet en WiFi

D. Leeuw

6 december 2023
v.0.9.0

# Over Dit Document

## 0.1 Leerdoelen

Dit document gaat over ethernet. Het leert je wat ethernet is. Om meer te weten te komen over wat er op je netwerk gebeurt maak je ook kennis met de tools: `arp` en `wireshark`.

Na het bestuderen van dit document heb je een basis kennis van ethernet, weet je wat het adres-formaat is van ethernet en kan je informatie over het netwerk opvragen via verschillende tools.

In de praktijk opdrachten leer je om je eigen kabel te maken en deze te testen. Tevens maak je je eigen Wi-Fi netwerk.

## 0.2 Voorkennis

- Voor het snappen van subnet-masks is kennis van binaire getallen noodzakelijk en moet men de boolean OR-functie kennen.
- Voor het snappen van MAC-adressen is enige kennis van hexadecimale getallen vereist.
- Het is handig, maar niet strikt vereist als de lezer iets af weet van UTP en coax kabels.

# Inhoudsopgave

# Hoofdstuk 1

# Ethernet

Ethernet is ooit bedacht om data over een kabel te kunnen versturen. Om te zorgen dat iedereen op de kabel elkaar kan verstaan is het noodzakelijk om allemaal dezelfde taal te spreken. De collectieve taal voor ethernet heet CSMA/CD, waarop we later terug zullen komen.

In 1973 stuurde Robert Metcalfe een memo aan zijn bazen van Xerox Parc over de mogelijkheden van ethernet. Het idee werd verder ontwikkeld wat uiteindelijk het document "Ethernet: Distributed Packet-Switching For Local Computer Networks" opleverde dat in 1976 werd gepubliceerd door Robert Metcalfe en David Boggs.

Metcalfe verliet in 1979 Xerox om 3Com op te richten. Het doel was om LAN's populair te maken, hiervoor zocht hij de samenwerking op met Dec, Intel en zijn oud werkgever Xerox. Met dit trio werd de DIX-standaard gepubliceerd zodat netwerk componenten van deze verschillende bedrijven met elkaar konden samenwerken. De formele standaard voor ethernet kwam er in 1983 toen de IEEE de IEEE 802.3 standaard publiceerde. Met deze laatste publicatie was er een officiële werelwijde standaard.

De IEEE802.3 kent allerlei subsecties die worden aangegeven met een letter. Zo is 100 Mbit/s ethernet over twisted-pair kabel IEEE802.3u. We zullen hier verder niet op ingaan, maar het is wel handig om te weten dat er voor elke snelheid en elk medium (coax, twisted-pair, glas) een standaard is die beschrijft waaraan zowel het medium als de aangesloten netwerkkaarten moeten voldoen (Wikipedia heeft een overzicht van de verschillende standaarden: https://en.wikipedia.org/wiki/IEEE_802.3)

## 1.1 Het Ethernet Protocol: CSMA/CD

Het protocol dat door ethernet gebruikt wordt om data over een kabel te versturen is CSMA/CD, Carrier Sense Multiple Access with Collision Detection. Het is een mondvol, maar kan vrij simpel opgehakt worden in 3 stukken:

De ethernetkaart luistert naar het netwerk (Carrier Sense). Als het data te versturen heeft wacht het tot het geen activiteit meer hoort op het netwerk, als de kabel "leeg" is kan er een frame verstuurd worden.

Het gevolg is dat meerdere netwerkkaarten tegelijk hun data kunnen gaan versturen (Multiple Access).

Als er meerdere tegelijk hun data versturen wordt het natuurlijk een zooitje, net zoals dat meerdere personen tegelijkertijd door elkaar gaan praten. Er moet dus een meganisme zijn om te ontdekken dat iedereen door elkaar praat (Collision Detection). Het detecteren van de bosting van data zorgt ervoor dat iedereen stopt met zenden. De zendende netwerkkaarten berekenen een random-nummer en gebruiken dit om daarmee een random-tijd hun mond te houden (back-off-time) voordat ze weer opnieuw beginnen met hun data te versturen. Doordat de back-off-time random is, is de kans dat er weer twee stations tegelijk gaan beginnen met verzenden van hun data zeer onwaarschijnlijk is.

Met dit simpele protocol regelt ethernet de toegang tot de carrier (kabel). Je kunt je voorstellen dat als er steeds meer netwerkkaarten op het netwerk aangesloten worden de kans toeneemt dat twee of meer netwerkkaarten tegelijkertijd hun data willen versturen en dat dus de kans op collisions toeneemt. Dit was vooral vroeger van belang toen er veelvuldig gebruik gemaakt werd van hubs; met de komst van switches is dit probleem sterk afgenomen.

Alle netwerkkaarten die zo zijn aangesloten dat ze een collision kunnen horen behoren tot hetzelfde collision domain. Switches (en bridges) scheiden collision domains.

## 1.2 Ethernet Adressen

Elke server kan meerdere netwerkkaarten bevatten. Om die een eigen frame te kunnen sturen moet een netwerkkaart een uniek adres hebben. Dit adres is het MAC-adres, dit is dus een fysiek adres en onderdeel van de netwerkkaart. Het MAC-adres is uniek op de wereld, er is geen tweede netwerkkaart met hetzelfde adres.

Het MAC-adres bestaat uit 6 blokjes van 2 hexadecimale digits. Bij de

notatie van dit adres kunnen de blokjes gescheiden zijn door een dubbele punt of door een streepje: 01:12:23:ab:bc:cd of 01-12-23-ab-bc-cd. De notatie verschilt per operating system. Het MAC-adres is opgedeeld in twee delen, namelijk de eerste 3 blokjes en de tweede 3 blokjes. De eerste drie blokjes zijn de Organisation Unique Identifier (OUI). De OUI is het ID dat gegeven is aan een organisatie (Apple, Broadcom, D-Link). De tweede set van drie blokjes is het deel dat het adres uniek maakt. Is een organisatie door zijn adressen heen dan vraagt het een nieuwe OUI aan voor de productie van meer netwerkkaarten.

Ethernet is een OSI-layer 2 (data link) protocol. De data die over het netwerk gaat heten dan ook frames. Elk frame heeft zowel het source als het destination adres in het frame zitten:

| preamble | DMAC | SMAC | length | packet | FCS |
|---|---|---|---|---|---|

**preamble**

**DMAC** Destination MAC address

**SMAC** Source MAC address

**length** De lengte van het frame

**data** informatie van hogere lagen uit het OSI-model (laag 3)

**FCS** Frame Check Sequence een controle nummer om te zien of alle bits goed zijn overgekomen (CRC)

De IEEE is degene die de OUI's uitgeeft. De lijst met uitgegeven OUI's is een publieke lijst en kan gevonden worden op `https://standards-oui.ieee.org/oui/oui.txt`. Omdat deze lijst publiek is kun je dus aan de frames op het netwerk zien van welk type netwerkkaart de data afkomstig is en waar de data naartoe gaat. Op een netwerk met alleen Apple machines heb je daar niet veel aan, behalve als er opeens een frame langs komt van een Broadcom netwerkkaart, dan is er kennelijk wat aan de hand dat om onderzoek vraagt.

De ethernetkaart filtert frames van het netwerk als het destination address overeenkomt met het MAC-adres van de kaart, alle andere frames worden genegeerd. Er is één uitzondering, namelijk het MAC-adres `ff:ff:ff:ff:ff:ff`, dit is het ethernet broadcast adres. Alle netwerkkaarten die dit adres zien als destination address zullen het frame doorgeven naar de hogere lagen in de network stack.

## 1.3 Ethernet Bekabeling

Ethernet is ooit ontworpen om gebruikt te worden over coax-kabel. Alle aangesloten netwerkkaarten waren fysiek aangesloten op dezelfde kabel. Er was één kabel met daarop meerdere netwerkkaarten die de kabel met elkaar moesten delen. Het oorspronkelijke design was op een hele dikke gele coax-kabel, later werd dit een veel dunnere RG-58 kabel waarbij de kabel via bajonet connectoren aangesloten werd op de netwerkkaart.

Een ethernet-kabel met de aangesloten netwerkkaarten mocht maximaal 100 meter lang zijn, omdat anders het signaal te veel zou verzwakken. De kabel met aangesloten netwerkkaarten vormt het collision domain.

Later ontstond een ontwikkeling naar UTP-kabel. Het netwerk kreeg daardoor een ster-structuur met een hub (naaf/as) in het midden. Een hub is een actief electronisch apparaat die werkt als een repeater. Een repeater zal het binnenkomende signaal weer netjes maken en daarna doorsturen naar elke poort die hij heeft. Er kan dus vanaf elke poort van een hub een kabel gelegd worden van 100 meter, wat een spanweidte van het netwerk oplevert van 200 meter. Omdat een hub het binnenkomende signaal van een poort netjes maakt en naar elke andere poort doorstuurt (repeat) vormt de hub met de aangesloten netwerkkaarten een collision domain. Let op: ook de collisions worden gerepeat.

## 1.4 Ethernet Devices

### 1.4.1 Repeater

Een repeater is een actief elektronisch apparaat dat het netwerksignaal van het netwerk leest en er weer een mooi signaal van maakt waarna het het op een andere kabel weer uitzendt. Een repeater is verder een dom apparaat met weinig intelligentie, het zal een collosion dan ook domweg repeaten.

Er bestaan repeaters met twee netwerk aansluitingen die er alleen voor zorgen dat er meer afstand overbrugd kan worden. In het verleden waren er ook HUBs die de basis van het netwerk vormden. Deze laatste zijn vervangen door switches in moderne netwerken.

### 1.4.2 Bridge

Als je binnen ethernet netwerken wil bouwen die over de grens van een collision domain gaan heb je een bridge nodig. Een bridge scheidt twee

collision domains en zorgt ervoor dat een collision niet wordt doorgezet van de ene kabel op de andere kabel. Een bridge moet dan ook het volledige CSMA/CD protocol ondersteunen.

Omdat het kan gebeuren dat er op een poort van de bridge data binnenkomt die hij niet direct kwijt kan aan een andere poort, omdat daar al een netwerkkaart data aan het sturen is, moet een bridge instaat zijn om data tijdelijk op te slaan. Dus naast de volledige ondersteuning van het CSMA/CD-protocol moet een bridge ook voldoende geheugen hebben om data tijdelijk op te slaan. Ook de repeater functie zit in een bridge, want het uitgestuurde signaal moet volledig voldoen aan de ethernet standaard.

Een bridge is daardoor een complexer apparaat. De techniek die gebruikt wordt heet store-and-forward, dat betekent dat een frame eerst wordt opgeslagen, er gekeken wordt waar het naar toe moet en daarna wordt doorgezet naar de uitgaande poort.

Een belangrijke vraag hierbij is hoe de bridge weet op welke ethernetpoort hij het frame moet uisturen. Omdat ethernet-frames altijd het source en destination MAC adres in zich hebben, kan de bridge van het netwerk leren welke destinations er op welke poort zitten door de source-adressen te verzamelen, want de verzender (source) zit aan de poort waarop het frame is binnengekomen. Als een bridge niet weet op welke poort een destination zit, dan zal het het frame naar alle poorten sturen.

### 1.4.3 Switch

De switch is een opvolger van de bridge. Het bevat alle functies die een bridge ook heeft.

Een switch maakt het netwerk sneller door elke ethernetkaart direct op zijn eigen bridge-port aan te sluiten. Op elke switchport sluit je dus één machine aan. Dit heeft als voordeel dat het collision domain terug gebracht wordt tot 2 netwerkkaarten, de netwerkkaart van het aangesloten station en de netwerk-poort van de switch. Er kunnen daardoor bijna geen collisions meer plaats vinden want als de een aan het zenden is dan weet de ander het, en omgekeerd.

Doordat er geen collisions meer plaatsvinden, heeft een switch minder geheugen nodig om frames op te slaan. De snelheid in de switch (backplane) bepaalt de kwalitiet van de switch. Hoe sneller de backplane hoe duurder een switch vaak is.

Een andere techniek die de switch sneller maakt dan een bridge is dat een switch het begin van een frame inleest, kijkt naar het destination MAC

address en daarop vast "sckakelt"zodat het source en destination netwerk aan elkaar gekoppeld zijn. Er hoeft dus niet eerst het hele frame ingelezen te worden en dan weer doorgestuurd. Een franme gaat door het switchen sneller van de ene naar de andere poort.

Switches kunnen natuurlijk ook aan elkaar gekoppeld worden om grotere netwerken te bouwen met meer netwerkpoorten. Dit heeft echter wel gevolgen voor de snelheid van het netwerk. Als we een switch hebben met 24 poorten van 100 Mbps en we verbinden 1 poort met een andere switch die ook 100 Mbps poorten heeft dan is de verbinding tussen de twee switches 100 Mbps. Als nu twee systemen tegelijk met machines aan de andere switch willen praten dan moeten die enkele 100 Mbps verbinding tussen de switches gedeeld worden, effectief blijft er dus 50 Mbps over.

### 1.4.4 Configuratie

Om bridges en switches zijn soms op afstand beheerbaar. Een ouderwets protocol dat gebruikt werd om ze te beheren is telnet, modernere protocollen zijn ssh en natuurlijk de web-interface. Om te een switch of een bridge remote te kunnen beheren moeten we kunnen inloggen op het apparaat. We moeten dus een gebruikersnaam en wachtwoord kunnen opgeven en deze data wordt over het netwerk verzonden. Als iemand het netwerk kan afluisteren dan heeft hij dus onze gebruikersnaam en wachtwoord en dat is iets dat we niet willen. Dit geldt voor telnet en http, de veilige protocollen zijn ssh en https. Het https en ssh protocol encrypt alle data voordat die over het netwerk gaat zodat afluisteraars niets met de ontvangen data kunnen.

Als je dus een nieuwe switch of bridge in je netwerk plaatst en deze kan remote beheerd worden, zorg er dan als eerste voor dat je de onveilige protocollen uit zet, de veilige protocollen aan zet en het wachtwoord op de machine wijzigt.

# Hoofdstuk 2

# WiFi

Je zal je misschien afvragen waarom in een document over ethernet ook WiFi wordt behandeld. Het antwoord is vrij eenvoudig: omdat WiFi ethernet is met een paar aanpassingen.

Ook WiFi gebruikt MAC-addressen en ook het gebruikte protocol is bijna hetzelfde als ethernet. Er is bewust gekozen voor deze gelijkenis. Tijdens het ontwerp van WaveLAN, de voorloper van WiFi, was ethernet al een veel gebruikte standaar, hierdoor waren de chips voor de interfaces goedkoop. Door bij ethernet aan te sluiten werd er gekozen voor relatief goedkope chips en bij bestaande kennis.

WiFi is ontwikkeld onder de naam WaveLAN door NCR Systems Engineering in Nieuwegein gedurende 1986-1987. In 1991 werd het gestandardiseerd door de IEEE als IEEE802.11 en werd het bekend onder de naam Wi-Fi.

De naam WaveLAN werd nog langer gebruikt als de productnaam waaronder NCR, later AT&T en weer later Lucent Technologies producten die voldeden aan de IEEE-standaard op de markt brachten.

## 2.1 Het WiFi Protocol: CSMA/CA

Het protocol dat door WiFi gebruikt wordt om data door de lucht te versturen is CSMA/CA, Carrier Sense Multiple Access with Collision Avoidance. Het is een mondvol, het lijkt enorm veel op het ethernet protocol. Er wordt geluisterd of er geen signaal in de lucht is, als de "carrier"vrij is mag iedereen gaan zenden, maar om collisions te voorkomen (avoidance) wordt er eerst gebruik gemaakt van de back-off-time. Doordat er standaard gebruik wordt gemaakt van een back-off is WiFi iets trager dan ethernet, maar is de kans op collisions vele malen kleiner.

## 2.2 WiFi Devices

Een Access Point of AP is een bridge die de verbinding legt tussen het draadloze netwerk en een bedraad ethernet netwerk.

Moderen varianten van de Access Point kunnen ook de koppeling naar Internet maken en ondersteunen naast ethernet ook het TCP/IP protocol (het protocol om via IP adressen te communiceren met machines over de gehele wereld). Deze slimmere apparaten hebben vaak ook een firewall en een DHCP-server.

De meest eenvoudige en oorspronkelijke vorm van het AP was een apparaat met de bridge functionaliteit en dat is nog steeds de basis van een AP.

# Hoofdstuk 3

# Opdrachten

## 3.1 Opdracht: Wat zijn de MAC-adressen van je eigen netwerkkaarten?

In deze opdracht gaan we informatie verzamelen van de netwerk-interfaces op onze eigen machine. Dit kunnen we natuurlijk ook op andere machines doen. De verschillende operating systems hebben hiervoor verschillende commando's, ga naar de command line van het besturingssysteem en gebruik het commando dat bij jouw os hoort:

**Windows** ipconfig

**Linux** ip link show

**Mac OS X** ifconfig

Noteer van elke interface het MAC-adres.

## 3.2 Opdracht: Welke speciale MAC-adressen zijn er?

- Wat is het 00:00:00:00:00:00 MAC-address?
- Wat is het ff:ff:ff:ff:ff:ff MAC-address?

## 3.3 Opdracht: MAC-adressen in Wireshark

Start wireshark, start capturing en na een minuut stop de capturing. Zoek een frame uit waar een van je eigen MAC-adressen het source MAC ad-

dress is en het destination MAC address is ingevuld, het destination MAC address mag niet ff:ff:ff:ff:ff:ff zijn.

- Noteer het gevonden destination MAC adressen. Neem hiervan de OUI en zoek hierbij de naam van de organisatie die bij deze OUI hoort.
- Naar wat voor soort apparaat was jou machine data aan het sturen?

## 3.4 Opdracht: De ARP-tabel

Het Internet gebruikt een protocol dat TCP/IP heet. TCP/IP op een lokaal bedraad en draadloos netwerk (LAN - Local Area Network) gebruikt ethernet adressen om frames lokaal af te leveren. Om uit te zoeken welke adressen er bij welke machine horen wordt er gebruik gemaakt van het ARP-protocol. Het protocol heeft ook een commando genaamd `arp` dat je gebruiken om te zien welke machines jouw machine kent. Gebruik om je machine, afhankelijk van je besturingssysteem het volgende commando:

**Windows** arp -a

**Linux** arp -a

**Mac OS X** arp -a

In de voorgaande opdracht heb je een MAC-adres genoteerd van een destination waar je machine mee communiceerde. Zoek dat MAC-adres op de de arp-tabel die je zojuist hebt opgevraagd en noteer welke machine (naam en/of IP-adres) daarbij hoorde.

# Hoofdstuk 4

# Praktijk opdrachten

## 4.1 Opdracht: Maak je eigen UTP-kabel

In deze opdracht gaan we onze eigen UTP-patch-cable maken. De huidige ethernet standaarden voor ethernet over UTP-kabel zeggen dat de totale kabellengte vanaf de switch naar de netwerkkaart 100 meter lang mag zijn. Van deze 100 meter mag er 2x 5 meter getwijnde twisted pair koperkabel zijn, de zogenaamde patch-kabels. De rest van de kabe moet solid koper zijn.

De solid koper kabel is een acht-aderige kabel waarbij elke ader van massief koper is. Deze kabel wordt gebruikt om patch-panelen te verbinden met wall-outlets op de verschillende kamers van een gebouw. De kabel ligt meestal door kabelgoten.

Patch kabels zijn gemaakt van getwijnt koper (Engels: stranded copper). Dat betekent dat elke draad van de acht-aderige kabel, bestaat uit allemaal fijne draadjes. Deze opbouw zorgt ervoor dat de kabel flexibel is en makkelijk in bochtjes gebogen kan worden. De patch-kabel wordt gebruikt om de patch-panelen aan te sluiten op de switch en om werkstations aan te sluiten op de wall-outlet op de werkkamer.

De solid-koper kabels worden vaak gelegd door installatie bedrijven en patch-kabels worden meestal ingekocht, maar het kan weleens gebeuren dat je even snel een eigen patch-kabel moet maken. Dat is wat we in deze opdracht gaan oefenen. Wat heb je nodig:

- Een stuk stranded koper kabel (1 meter)
- 2 RJ45 connectoren voor stranded koper
- Een RJ45 krimptang

- Een kabel stripper
- Een kabelkniptang
- Een kabel-tester

Alle aders binnen een 8-aderige kabel hebben hun eigen kleur en moeten op de juiste manier in de RJ45 connector terecht komen. De juiste manier voor ethernet kan op twee manieren namelijk via de EIA/TIA-568-A of -B standaard. In Europa gebruiken we bijna allemaal de B-standaard. Zoek op Internet op wat de volgorde van de kabel moet zijn in de RJ45 connector (zoeken op plaatjes met de term TIA-568-B).

Volg de aanwijzingen op https://www.ditecpro.be/data/document/311/1561390222-UTP-kabel-maken.pdf om je eigen kabel te maken. Let op dat je aan beide zijden van de kabel een connector zet.

Test je kabel op een correcte werking. Dit kan door hem in een netwerk te gebruiken, door gebruik te maken van een simpele kabel-tester (deze controleert alleen of de aders op de juiste plek zijn aangesloten), je kan ook een kwaliteitstest doen, dan heb je een duurdere tester nodig, de controleert of de kabel ook voor de geleiding aan alle kwaliteitseisen voldoet.

## 4.2 Opdracht: Maak je eigen Wi-Fi netwerk

Als je niet in het bezit bent van twee smart-phones, doe de opdracht dan met zijn tweeën.

Benodigdheden:

- 2 mobiele telefoons
- op beide telefoons de applicatie Network Analyzer van Jiri Techet

Stappenplan:

1. Zoek op beide telefoons de MAC-adressen op die gebruikt worden voor de Wi-Fi en noteer deze.
2. Maak van 1 telefoon een hotspot (of wel een access point). Verbindt de andere telefoon met dit netwerk.
3. Gebruik Network Analyzer op de telefoon die je geconnect hebt met het Wi-Fi netwerk om de gegevens om te zoeken van het netwerk (Menu - Information). Welk MAC adres tref je aan bij het BSSID?