MAC-adressering

Iedere NIC (Network Interface Card) heeft een uniek adres, het MAC-adres. Dit bestaat uit 6 bytes (= 48 bits) en wordt altijd weergegeven in het hexadecimaal stelsel met in totaal 12 tekens. De eerste 6 geven de fabrikant weer en de volgende 6 zijn hostspecifiek, wat een uniek adres maakt.

Een MAC-adres wordt op verschillende manieren weergegeven, maar de bekendste is deze met de dubbele punten: 00:50:BD:15:84:10

Als je even een opzoeking doet, kom je te weten dat dit MAC-adres afkomstig is van CISCO.

Via CMD met vervolgens ipconfig /all kom je je eigen MAC-adres te weten. Dit staat bij fysiek adres.

Op een LAN communiceert men altijd via een MAC-adres. Aangezien het internet (WAN) een hele grote verzameling is van alleen maar LAN's, is het MAC-adres dus heel belangrijk. Sterker nog, er is alleen maar netwerkcommunicatie mogelijk als de MAC-adressen en IP-adressen van de betrokken toestellen (in het volledige communicatieproces) worden opgenomen in de data van ieder pakket.

Door middel van een MAC-adres kan een betrokken toestel in een LAN gevonden worden. Het veel bekendere IP-adres heeft als hoofddoel om het juiste LAN op het internet te bereiken en intern aan te geven wat de karakteristieken (bv. subnetmasker, zie later) zijn van het netwerk.

Een MAC-adres dat zich bevindt in een ander LAN, kan niet rechtstreeks gevonden worden vanaf het LAN waarin je je bevindt. Om de juiste weg te vinden naar een ander LAN, is er altijd een IP-adres nodig.

Een netwerktoestel opzoeken in het LAN

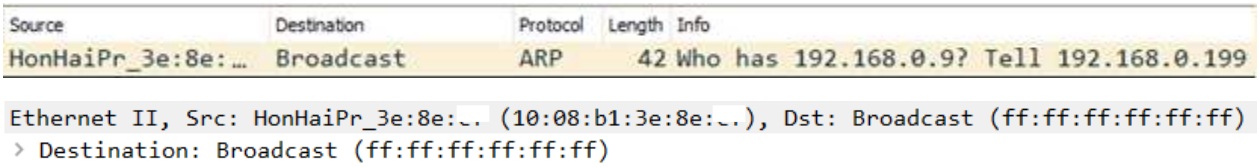
Je hebt net een nieuwe pc gekocht en geïnstalleerd. Op de nieuwe pc heb je een gedeelde map gemaakt om makkelijk bestanden te delen met je laptop. Ook heb je een IP-adres (192.168.0.9) ingesteld op je nieuwe pc.

Vanaf je laptop (die je net hebt opgestart) probeer je connectie te maken met je nieuwe pc door in de adresbalk van de verkenner het UNC-pad \\192.168.0.9 in te typen om de gedeelde mappen te zien op de nieuwe pc. Hierdoor wordt via de laptop een pakket opgesteld om de nieuwe pc te bereiken. In het pakket:

- wordt het IP-adres en het subnetmasker van de laptop en de nieuwe pc opgenomen om te controleren of de toestellen zich in hetzelfde LAN bevinden.
- wordt in de eigen ARP-tabel van de laptop gekeken of er een link is tussen het gevraagde IP en het nog onbekende MAC-adres. De ARP-tabel kunnen we zelf opvragen en deze tabel geeft het IP- met MAC-adres terug:

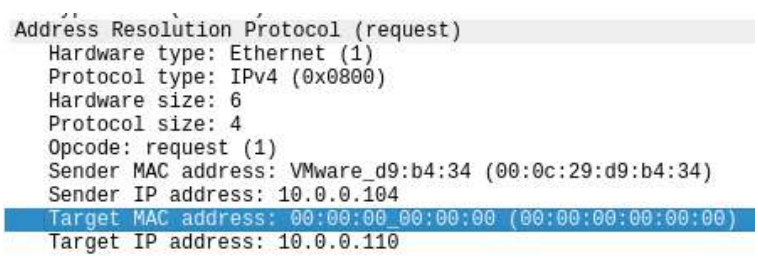
Het MAC-adres voor de nieuwe pc met IP 192.168.0.9 is momenteel voor de laptop nog onbekend. De laptop gaat het ARP-protocol (Address Resolution) gebruiken om via een broadcast het MAC-adres te achterhalen.

Een broadcast op het LAN (Ethernet) is altijd naar het MAC-adres FF:FF:FF:FF:FF:FF zodat alle netwerktoestellen in het LAN bereikt worden en deze een antwoord kunnen terugsturen naar het netwerktoestel die een vraag stelt.

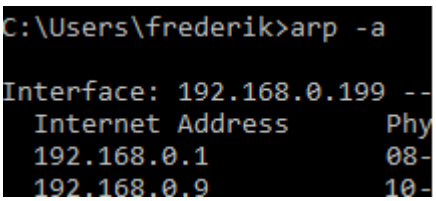


Bovenstaande en onderstaande afbeelding komen uit Wireshark (de bekende netwerksniffer). Ze geven het ARP-proces mee dat wordt uitgevoerd.

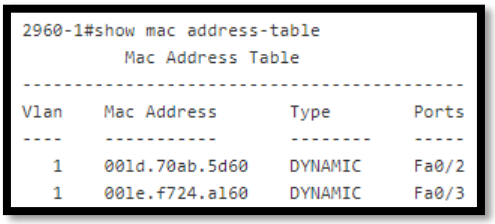
Naast de 12 F'en kan Wireshark ook 12 0'n meegeven als ARP-broadcastbericht:



Zo, nu kent de laptop het MAC-adres en het IP-adres van de nieuwe pc en kan communicatie opgezet worden. Ook kent de ARP-tabel van de laptop nu de link tussen beide adressen:



Bovenstaand ARP-proces speelt zich eigenlijk voortdurend automatisch af, waardoor de laptop hoogstwaarschijnlijk al wist waar de nieuwe pc zich bevond. Hier werd het enkel manueel nagespeeld. Dit kon door de ARP-tabel als administrator eerst leeg te maken: arp –d uitvoeren in cmd.



Aangezien de laptop en de nieuwe pc zich bevinden in hetzelfde netwerk, maar niet met elkaar gekoppeld zijn met dezelfde kabel, is er nog een tussenapparaat zoals een switch die de apparaten moet koppelen. Een standaardswitch werkt enkel met MAC-adressen en houdt een MAC-adrestabel bij.

Vorige afbeelding toont het uitlezen van de MAC-tabel in de CLI van een switch. Deze CLI-modus is meestal enkel aanwezig bij de geavanceerdere switchen. Een geavanceerdere switch heeft vaak ook een web-interface-GUI aan boord om details op te sporen of de configuratie aan te passen.

De MAC-adrestabel houdt het MAC-adres van ieder toestel bij met de daaraan verbonden poort.

Deze MAC-adrestabel wijzigt vanaf er nieuwe informatie, zoals de nieuwe pc die verbonden wordt, beschikbaar is. Om alle correcte info te blijven hebben, zal de switch ook automatisch de MAC-tabel vaak heropvullen.

In de MAC-tabel zal in dit voorbeeld opgenomen worden op welke poort de laptop met MAC-adres A zich bevindt en op welke poort de nieuwe pc met MAC-adres B zich bevindt. Zo ontstaat netwerkcommunicatie. De switch linkt enkel de juiste poorten met elkaar. In de pakketten van laptop naar pc en omgekeerd staan steeds elkaars MAC-adressen. Een switch heeft ook een MAC-adres, maar dit wordt niet vaak gebruikt.

De aankoop van een nieuwe switch

Bij de aankoop van een nieuwe switch zal wanneer een netwerktoestel communicatie opvraagt met MAC-adres A naar MAC-adres B:

- de switch de MAC-tabel vullen met MAC A geconnecteerd met de poort waar de aanvraag op gebeurde en zal hierna naar alle andere geconnecteerde poorten (flooding) de aanvraag doorsturen, aangezien de switch nog niet weet welke toestellen zich op de andere poorten bevinden.
  - ⇨ wanneer MAC-adres B reageert, kan de switch de MAC-tabel vullen met MAC B en de poort die de aanvraag heeft beantwoord.

Verschil tussen Layer2- en Layer3-switch

Een layer2-switch werkt enkel met MAC-adressen en werkt zoals de naam het beschrijft enkel op de datalinklaag. Dit zijn de standaardswitchen die als enig doel hebben te kunnen communiceren met andere netwerktoestellen op hetzelfde LAN.

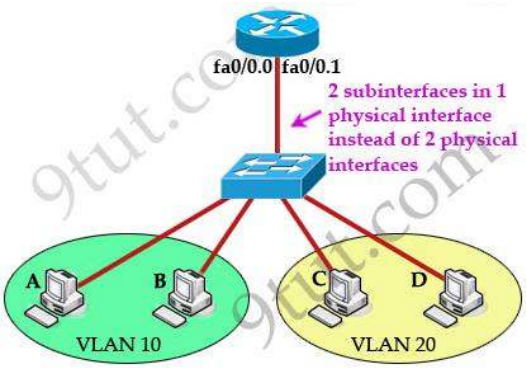
Een layer3-switch heeft routingmogelijkheden en werkt op de datalink- en netwerklaag. Een layer3-switch kan werken net zoals een layer2-switch, maar kan ook omgaan met IP-adressen. Natuurlijk hangt hier een groter prijskaartje aan vast.

Routing is de mogelijkheid om tussen verschillende LAN's en in het WAN te communiceren, de functie die de router op zich neemt. Het proces om te communiceren met een WAN kan een layer3-switch niet, waardoor de aanschaf van een router moet gebeuren om naar het internet te kunnen.

Met een layer3-switch maak je het wel mogelijk om je netwerk onder te verdelen in meerdere VLAN's en deze met elkaar te verbinden (Inter-VLAN routing). Een VLAN is letterlijk een apart beveiligd virtueel LAN met een eigen IP-adresbereik in een eigen broadcastdomein met toegangsregels bepaald door de firewall. Zo heb je de VLAN leerlingen en de VLAN secretariaat. De VLAN leerlingen

mogen niet in het VLAN secretariaat, maar dit mag wel omgekeerd. Ook moeten beide met internet kunnen verbinden. Dit zijn de toegangsregels die je instelt nadat je de VLAN's hebt opgezet.

Onder meer speelt QOS (Quality Of Service) een belangrijke rol bij VLAN's. Hiermee zeg je bv. dat het VLAN voor digitale telefonie veel belangrijker is dan de rest omdat je hier geen onderbrekingen mag op hebben.



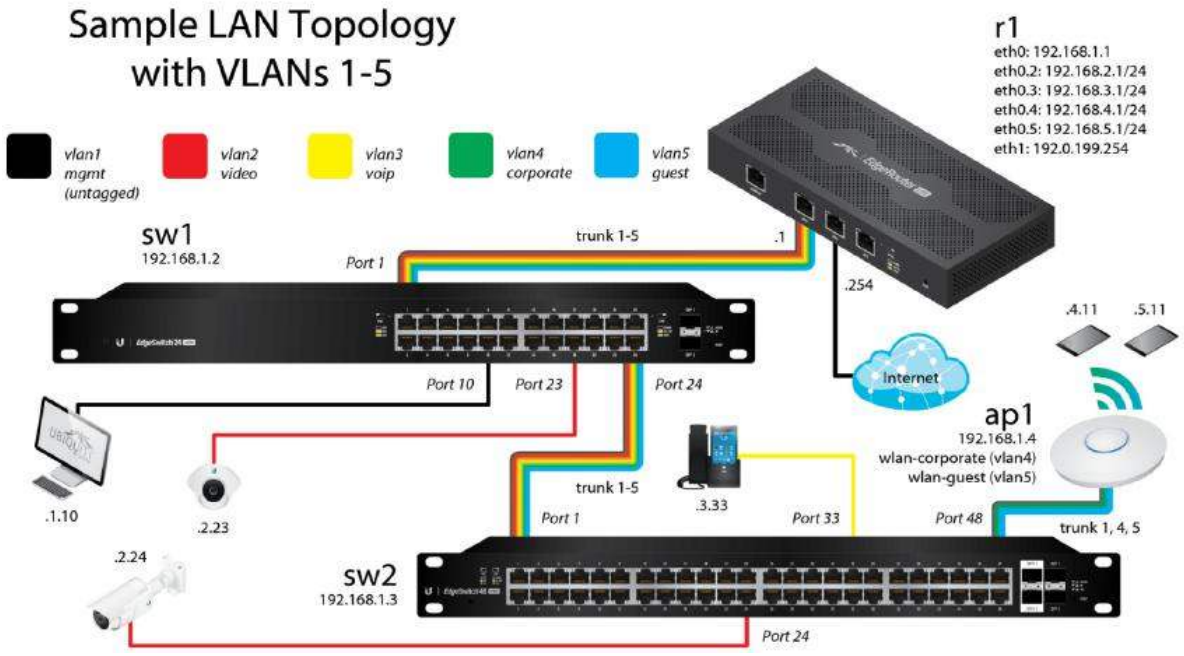
Een Layer2-switch kan omgaan met VLAN's, maar kan ze niet routeren. Een Layer3-switch is dus aangewezen.

VLAN's zorgen er voor om het netwerkverkeer van elkaar te scheiden en zo onder meer gasttoestellen (die al dan niet verbinden via Wi-Fi) af te scheiden van het "eigen" netwerkverkeer, maar bv. wel internettoegang ervoor te voorzien.

De afbeelding hiernaast toont dat je maar 1 switch nodig hebt om twee aparte beveiligde VLAN-netwerken te maken, i.p.v. dat je vroeger 2 switchen hiervoor ging gebruiken en aankopen. Kost is veel kleiner!

Bij VLAN's horen drie belangrijke termen die kunnen ingesteld worden op de fysieke poorten:

- tagged: toestel (switch, router, server, …) begrijpt VLAN's en kan ook VLAN's doorsturen.
- untagged: meestal eindapparaat (pc, …) begrijpt geen VLAN's en kan VLAN's niet doorsturen.
- trunk: meerdere VLAN's worden op deze ene verbinding doorgegeven naar volgend apparaat.

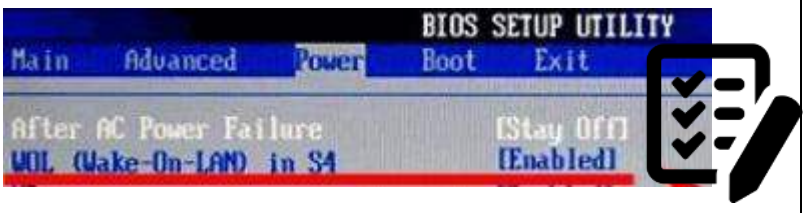


Video: VLAN explained (Afb. Ubiquiti)
https://www.youtube.com/watch?v=6_giEv20En0

WOL: Wake-On-LAN

EXTRA VERDIEPING

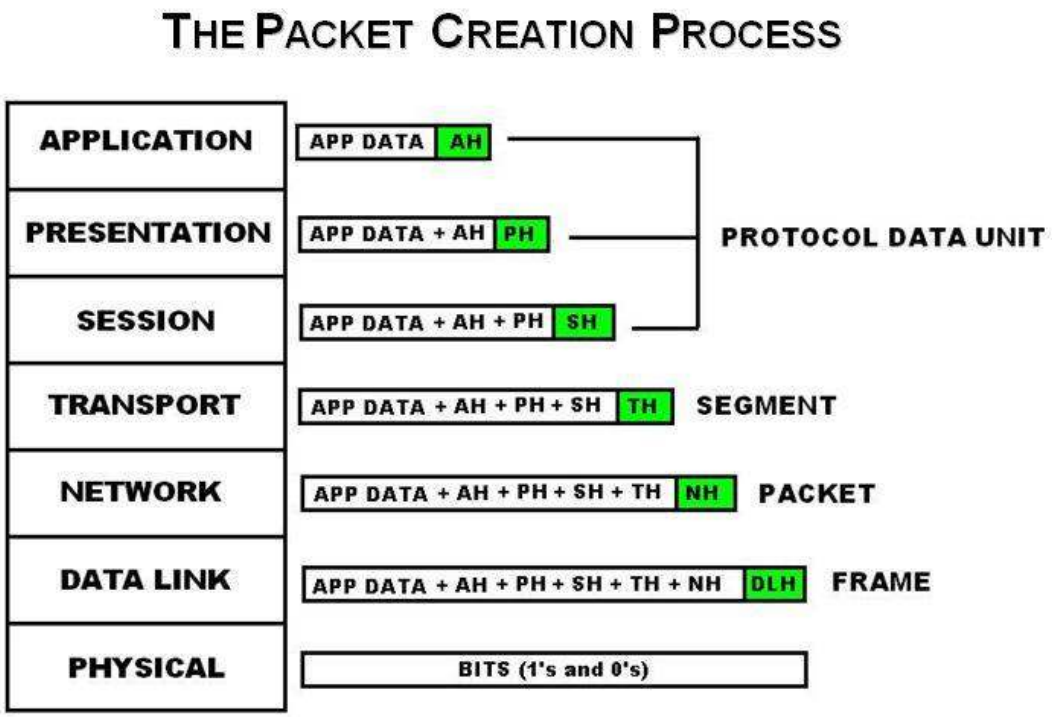
Als de netwerkadapter WOL ondersteunt, kan de pc actief worden gemaakt door een WOL-commando te sturen naar het MAC-adres van de NIC. Deze functie moet wel ingeschakeld staan in de BIOS van de pc. Dit kan onder meer vanaf een andere pc, maar ook vanaf een app, als deze zich bevinden in hetzelfde LAN.



IP-adressering

Een korte herhaling van het OSI-model is nodig om dit onderdeel door te nemen:

- Bestaat uit 7 lagen (applicatie-, presentatie-, sessie-, transport-, netwerk-, datalink- en fysieke laag) die top-down worden uitgevoerd, startend bij de applicatielaag en eindigend bij de fysieke laag.
- Iedere laag voegt een header met parameters met waarde toe die dienst doen om LAN- en/of internetverkeer mogelijk te maken.



(Afb. allroundcomputersolutions.weebly.com)

Een eerste netwerk werd gebouwd zonder in de commando's van Cisco te duiken.

Zoals reeds getoond, start netwerkbeheer met Cisco-apparatuur pas echt in de CLI. Een snelle indruk hiermee kan nooit geen kwaad:

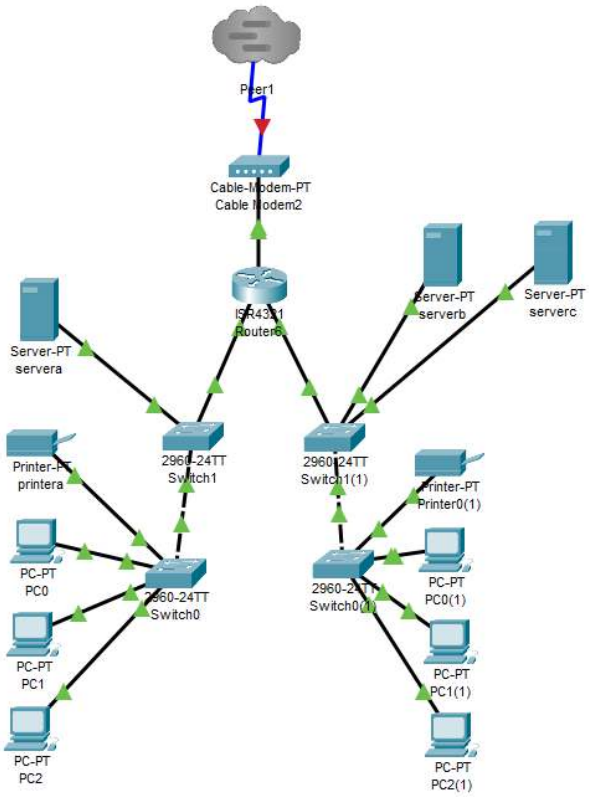
Open de router en zet deze nogmaals uit en opnieuw aan.

Ga nu meteen naar het tabblad CLI waarbij je heel wat regels tevoorschijn ziet komen. Eens de router is doorgestart, geef je een druk op de Enter-toets.

Hierdoor kom je in de usermodus terecht. Geef ? in waarbij je enkele mogelijke commando's ziet die gelijk welke gebruiker met fysieke toegang kan intikken.

Een belangrijke hierbij is show, bv. show ip route

Vervolgens type je enable om opnieuw in een andere geavanceerdere modus te komen. Daarna kan je ook nog configure terminal ingeven om nog meer acties uit te voeren enz.



Eveneens is het ook mogelijk om simulaties uit te voeren in Packet Tracer. Klik hiertoe op de knop "Simulation".

Ga aan de slag met volgend voorbeeld. Start eerst vanop een client in Cisco Packet Tracer de ping en speel vervolgens met de simulatie-mogelijkheden op je scherm voornamelijk aan de rechterkant.

Op je netwerkschema zal je allerlei acties zien gebeuren, zoals enveloppen die al dan niet toekomen.

Werken met pfSense

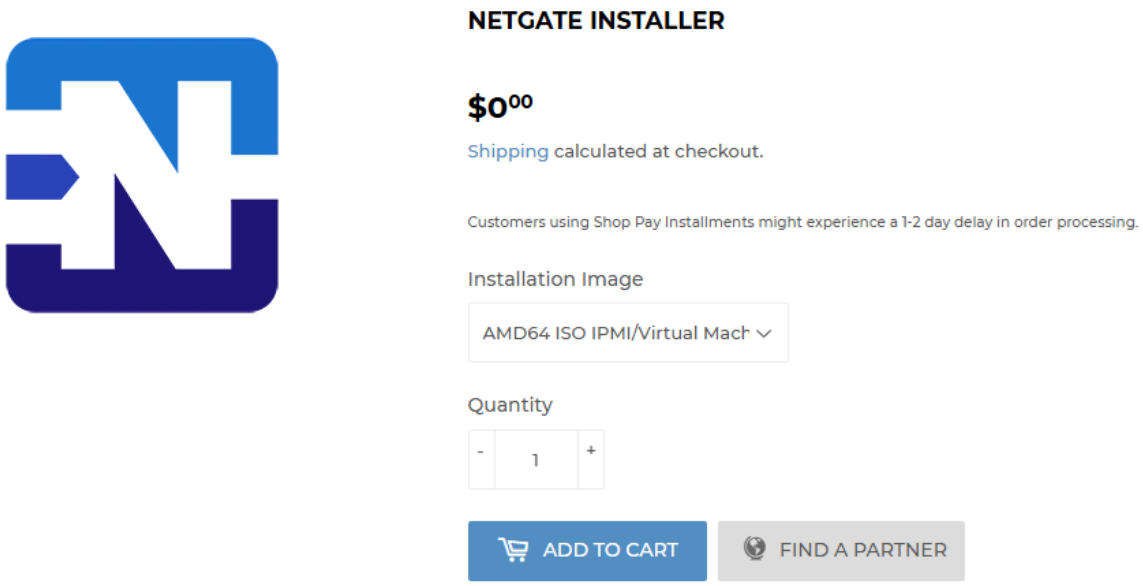
Tip voor dit project: als pfSense niet reageert en je hebt alles correct. Onthoud: herstart pfSense!

pfSense is een open source firewall (FW) softwaredistributie met onder meer routerfunctie, gebaseerd op FreeBSD. Het programma wordt geïnstalleerd op een fysieke computer of een virtuele machine. pfSense kan geconfigureerd en bijgewerkt worden via een web-interface en vereist geen kennis van het onderliggende FreeBSD-systeem om het te beheren.

In deze handleiding wordt Hyper-V gebruikt om meerdere internetconnecties op te zetten voor een WAN-, LAN- en gastnetwerk. Hierbij wordt een NAT- en private netwerkconnectie gebruikt.

Installeer binnen Hyper-V een virtuele machine (guest) met Windows Client (Gen2, 4GB/50GB, TPM, domain join user ict) en als netwerkconnectie Default Switch.

Surf op de fysieke pc (host) naar pfsense.org en download er de nieuwste versie als iso AMD64. Intussen heb je een account nodig en werkt dit met een gratis winkelmandsysteem. Pak de download uit tot je de .iso hebt. Hiertoe heb je bv. 7-zip nodig.



Opgelet betreffende eerdere versie:

De nieuwste versie kan fouten hebben…

Voorbeeldfout – In 2024 bevatte de nieuwste pfSense 2.7.2 een installatiefout. We maakten gebruik van de stabiele 2.7.0 waarvan de downloadlink verdwenen was. Maar archive.org had deze nog:

https://frafiles.netgate.com/mirror/downloads/pfSense-CE-2.7.0-RELEASE-amd64.iso.gz

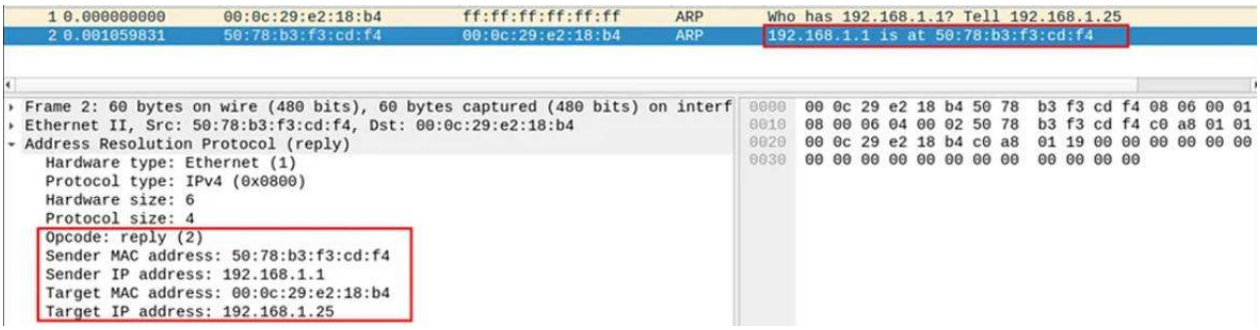
Nog enkele FTP reply codes

120	Service ready in xx minutes
200	Command okay
500	Syntax error
213	File Status

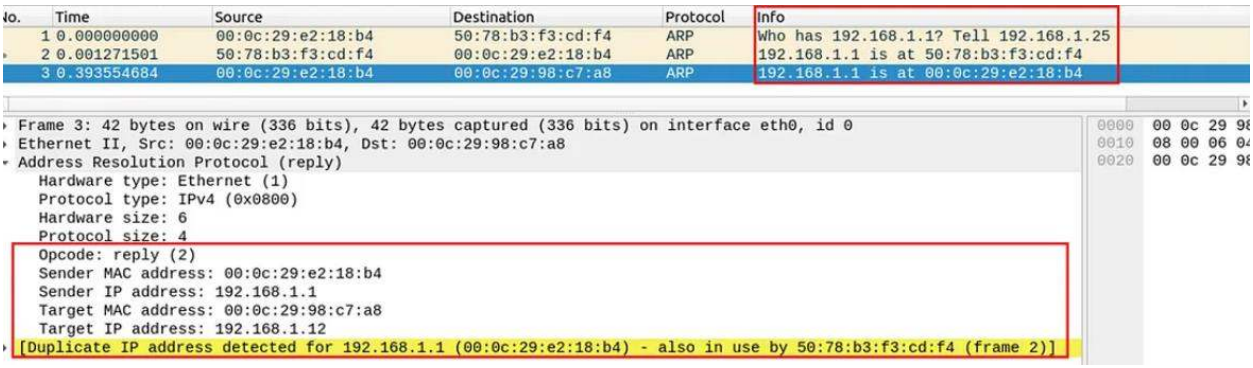
ARP

In een LAN-netwerk gebruikt de datalinklaag het MAC-adres van het toestel om het pakketje naar de juiste bestemming te brengen. ARP zorgt ervoor dat het MAC-adres van een toestel gevonden wordt aan de hand van het IP-adres. ARP bevindt zich dus tussen de netwerk en de datalink laag.

Zoals bij de start van dit Wireshark-onderdeel, kan ARP gebruikt worden om een MIM-attack waar te nemen. Hierbij zou dus IP- of MAC-spoofing kunnen gedetecteerd worden.



Bovenstaand kan je de ARP-communicatie waarnemen en hieronder merk je op dat nog een ander toestel aangeeft dat deze ook het IP-adres heeft waarnaar gevraagd wordt. Er is dus een IP-duplicatieprobleem dat door Wireshark gemeld wordt en dit kan slaan op IP-spoofing.



Dit zou dus een gewoon probleem kunnen zijn, maar even goed de basis voor een MIM-attack. Of je bent dit natuurlijk zelf die probeert alle andere pakketten in het netwerk te capteren die naar het