Netwerkanalysetechnieken:

Een Praktische Verkenning met

Wireshark

Xander P

Datum: 7 juni 2025

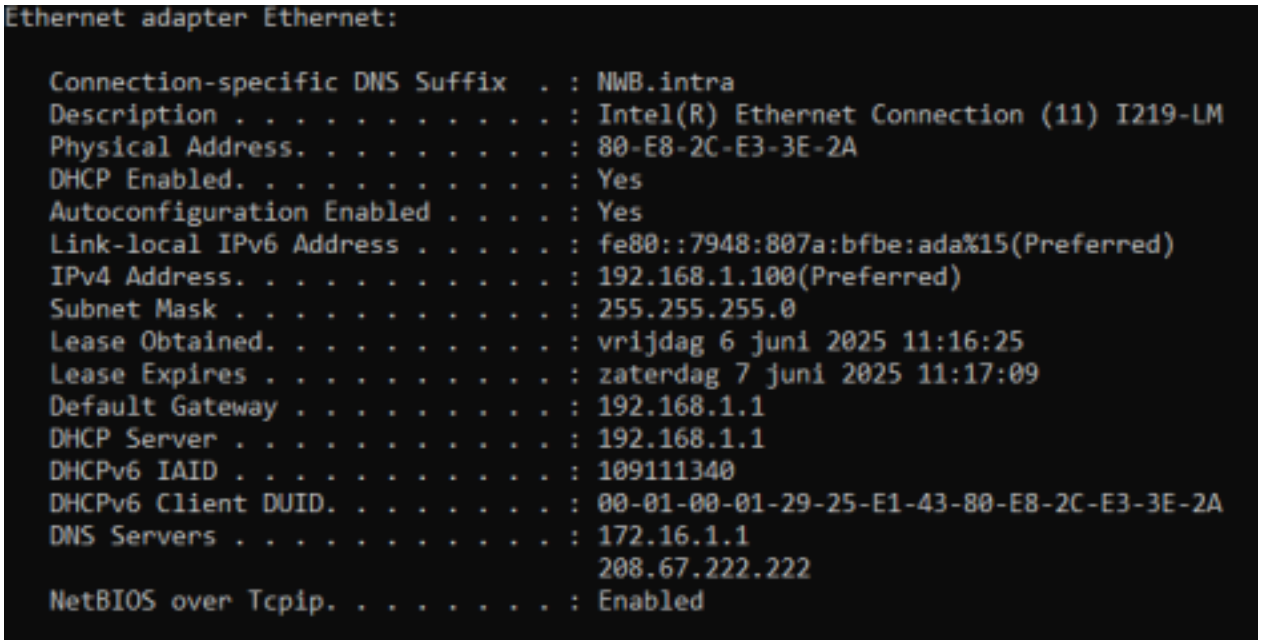
Inhoudsopgave

1. Inleiding

Dit verslag documenteert een praktische oefening in netwerkanalyse, uitgevoerd met de netwerkprotocolanalysator Wireshark. De kern van deze opdracht was het verkrijgen van inzicht in diverse cruciale netwerkprotocollen, waaronder ICMP, DNS, HTTP, HTTPS, Telnet en SSH. Door hun gedrag op de Data Link- (Laag 2) en Netwerk-lagen (Laag 3) van het OSI model te observeren, konden fundamentele concepten zoals IP- en MAC-adressering, protocolwerking en de implicaties van versleuteling worden gedemonstreerd. Specifieke verkeersstromen werden geïsoleerd en geanalyseerd door middel van pakketopnames en filtering, wat een gedetailleerd inzicht in de netwerkcommunicatie opleverde.

2. Voorbereiding en Initiële Netwerkparameters

Ter voorbereiding op de netwerkanalyse werden alle actieve applicaties afgesloten om ongewenst achtergrondverkeer te minimaliseren. Een essentiële eerste stap was het vastleggen van de IP-parameters en het MAC-adres van het gebruikte toestel. Deze parameters omvatten doorgaans het IP-adres van het lokale toestel (bijvoorbeeld 192.168.1.100 in een lokaal netwerksegment), het bijbehorende subnetmasker, de standaardgateway (vaak het IP-adres van de router, zoals 192.168.1.1), en de geconfigureerde DNS-server(s). Het MAC-adres van de netwerkinterfacekaart (NIC) van het toestel werd eveneens nauwkeurig genoteerd, gezien zijn cruciale rol in Layer 2- communicatie. Voor deze oefening werd specifiek een Linksys draadloze router gebruikt, waarbij de standaardtoegangsinstellingen – IP-adres 192.168.1.1, gebruikersnaam admin, en wachtwoord admin – werden vastgelegd.



3. Analyse van ICMP- en DNS-Verkeer

Na het configureren van een Wireshark-pakketopname op de actieve netwerkinterface van het toestel, werd een reeks gerichte netwerktests uitgevoerd om het gedrag van het ICMP en DNS-protocol te observeren.

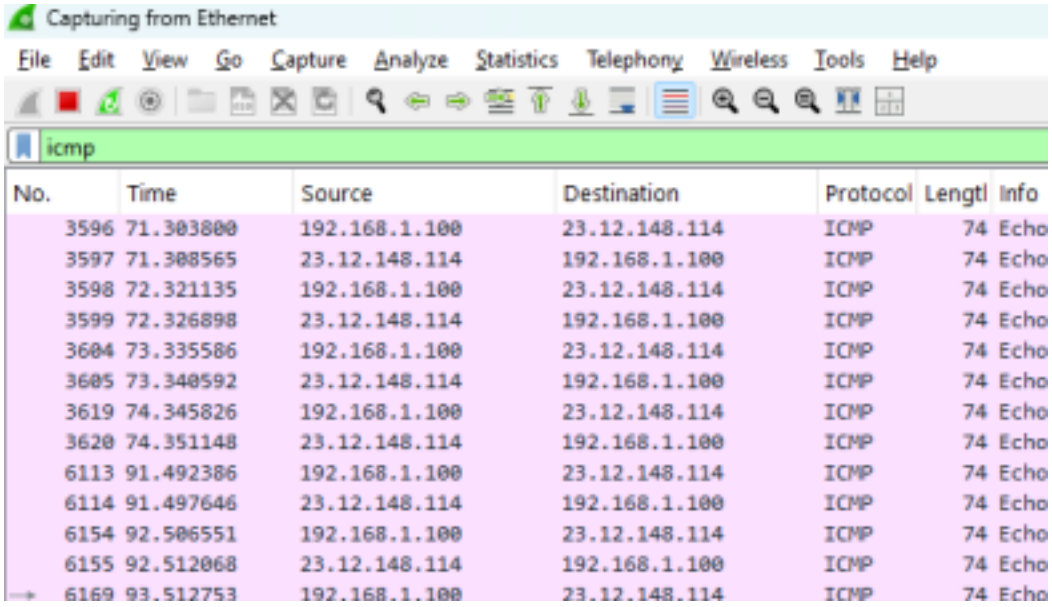
3.1. ICMP (Ping) Verkeer

Ping-commando's, die het ICMP-protocol benutten, werden uitgevoerd naar diverse bestemmingen: 8.8.8.8 (een publieke DNS-server van Google), www.cisco.com, en www.vdab.be. De corresponderende IP-adressen werden genoteerd als 8.8.8.8, 23.12.148.114 voor www.cisco.com, en 193.53.226.200 voor www.vdab.be.

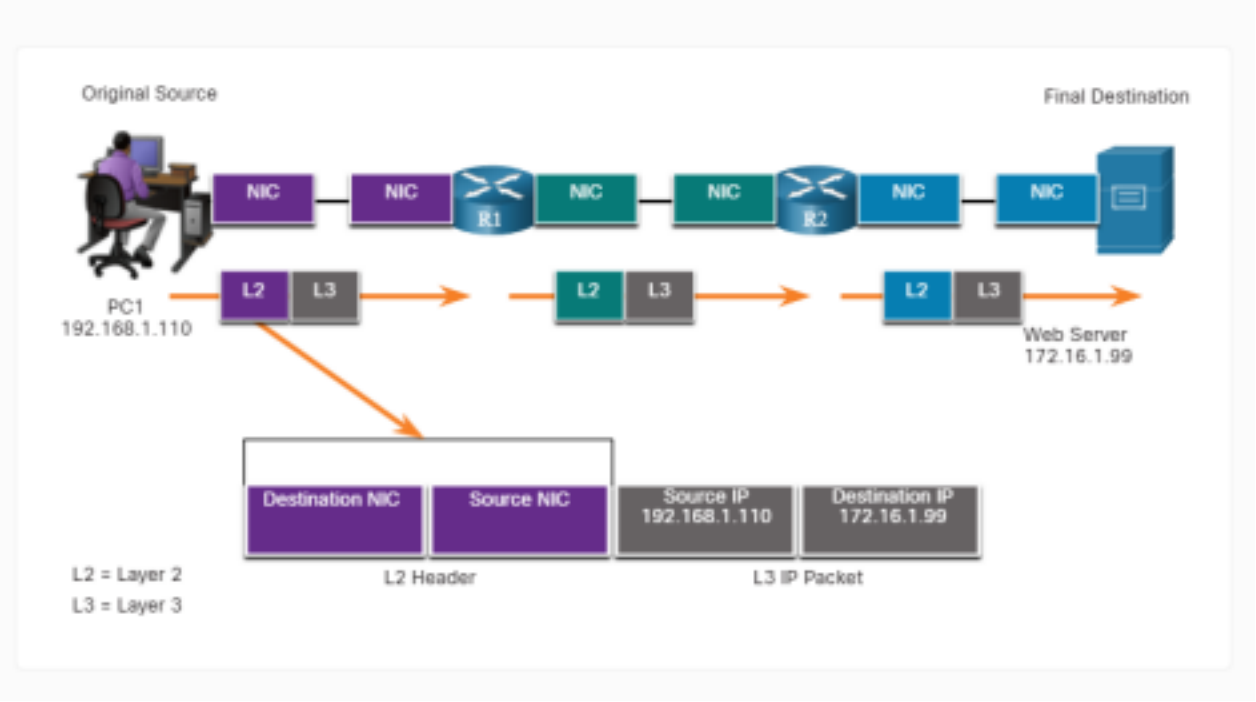
Door een Wireshark display filter van icmp toe te passen, kon alle ICMP-trafiek effectief worden geïsoleerd. Bij de analyse van een "Echo (ping) request" pakket gericht aan www.vdab.be (IP-adres 193.53.226.200), bleek het source IP-adres 192.168.1.100 (het lokale IP-adres van het eigen toestel) en het destination IP-adres 193.53.226.200.

Om enkel het verkeer van en naar www.vdab.be te krijgen gebruik je filter Imcp and ip

== www.vdab.be



Op de Data Link Laag werden tegelijkertijd de MAC-adressen geobserveerd. Het source MAC-adres van de "Echo (ping) request" was dat van het eigen PC, terwijl het destination MAC-adres dat van de router (192.168.1.1) was. Dit is correct, aangezien frames op een lokaal netwerk altijd worden geadresseerd aan de volgende "hop" op de lokale link. In dit scenario is die volgende hop de router, die verantwoordelijk is voor het routeren van het pakket naar externe netwerken buiten het lokale segment.

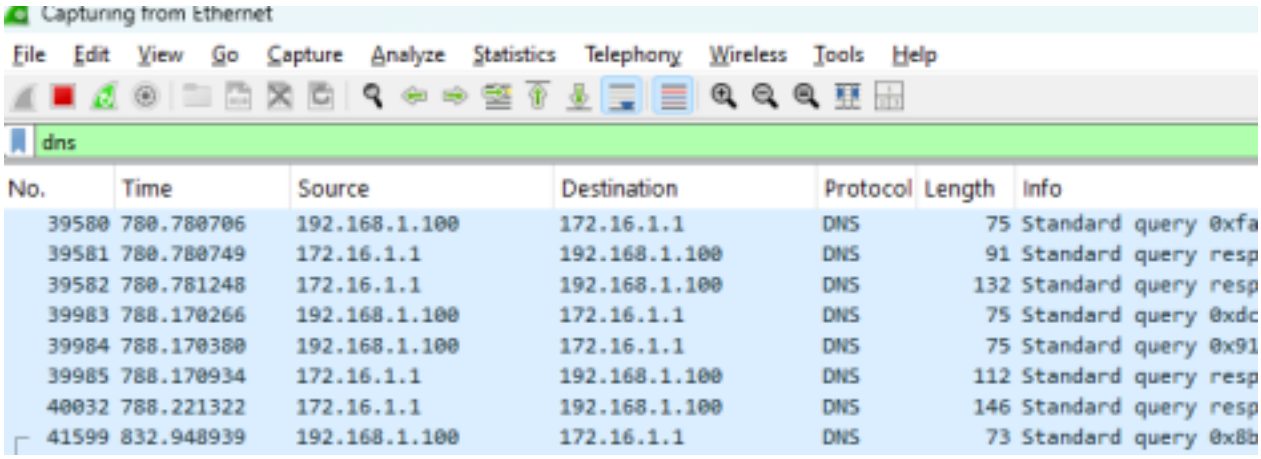


Figuur 1 Netacad

Bij het bekijken van de "Echo (ping) reply" pakketten trad een opmerkelijke bijzonderheid op: pings naar www.vdab.be ontvingen geen antwoord, wat duidt op een time-out. Echter, bij succesvolle pings (zoals naar www.cisco.com), zou het MAC-adres van het antwoordpakket als source dat van de router zijn en als destination dat van het eigen PC. Dit bevestigt het fundamentele principe dat Layer 2 MAC-adressen enkel relevant zijn voor communicatie binnen hetzelfde lokale netwerksegment, specifiek tussen de direct verbonden apparaten.

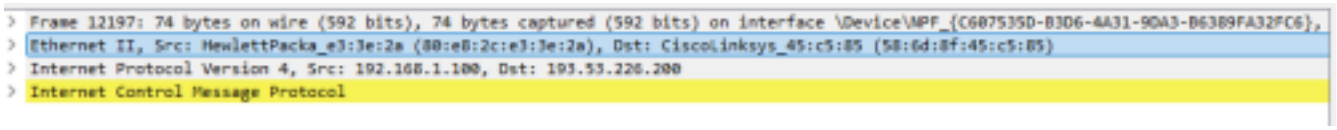
3.2. DNS-Resolutie Verkeer

Een nieuwe Wireshark display filter, dns, werd geactiveerd om alle DNS-trafiek te isoleren. Een analyse van een DNS-request toonde dat het source IP-adres 192.168.1.100 was (het lokale IP van het toestel), maar het destination IP-adres bleek 172.16.1.1. Dit was initieel een onverwacht resultaat, aangezien een direct IP van een publieke DNS-server (zoals die van een internetprovider) werd verwacht. Nader onderzoek onthulde echter dat de Linksys router waarschijnlijk is geconfigureerd als een DNS proxy of DNS forwarder. Dit houdt in dat het lokale toestel zijn DNS-verzoeken stuurt naar het IP-adres van de router, waarna de router deze verzoeken doorstuurt naar de daadwerkelijke externe DNS-servers. De MAC adressen die in deze DNS-requests werden gebruikt, waren consistent opnieuw die van het eigen PC (source) en de router (destination), wat aantoont dat de Layer 2-route voor lokaal verkeer onveranderd blijft.



Om de IP-resolutie van een specifieke domeinnaam te verifiëren, werd de Wireshark-filter dns.resp.name == "www.cisco.com" gebruikt. Deze filter toont specifiek DNS-reply pakketten waarin www.cisco.com wordt opgelost naar zijn corresponderende IP-adres, wat een efficiënte methode is om specifieke antwoorden binnen een Wireshark-capture te lokaliseren.

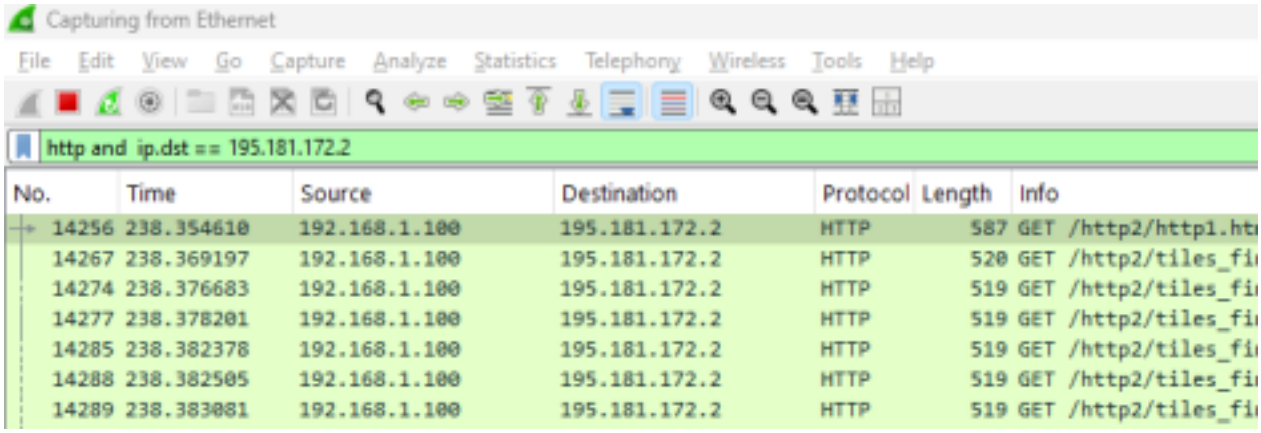
In de DSN-reply kun je het IP-adres van www.vdab.be terug vinden.



4. Analyse van Webverkeer (HTTP en HTTPS)

Voor de analyse van webverkeer werd een webbrowser gebruikt om te navigeren naar http://www.http2demo.io/ en https://www.vdab.be.

Voor het verkeer naar http://www.http2demo.io/ werd een display filter gebruikt om enkel de pakketten te tonen die naar de server werden verzonden. Een geschikte filter hiervoor was bijvoorbeeld http.request. Deze filter onthulde de ongecodeerde HTTP-requests die rechtstreeks vanuit de browser werden verzonden, wat het gebrek aan beveiliging van standaard HTTP-communicatie aantoont.



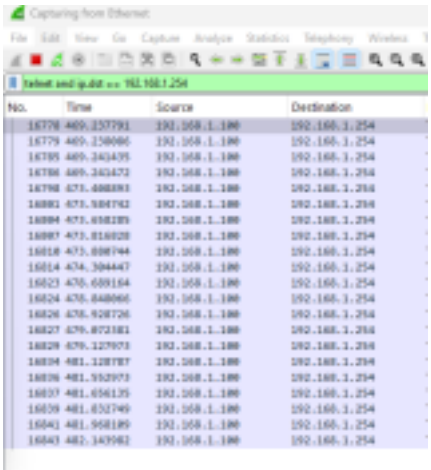
5. Beveiligde en Onbeveiligde Beheerverbindingen

Om het cruciale verschil tussen beveiligde en onbeveiligde beheerprotocollen te illustreren, werd een extra Cisco switch in het lokale netwerk geïnstalleerd, strategisch geplaatst tussen de Linksys router en het PC. Deze switch werd geconfigureerd met een specifiek IP adres (in dit geval 192.168.1.254) en voorzien van gebruikersauthenticatie voor beheer via de line VTY (Virtual Teletype Terminal).

5.1. Telnet-sessie analyse

Nadat een Wireshark-capture was gestart, werd een Telnet-sessie naar de zojuist geconfigureerde switch (192.168.1.254) opgezet via Putty. De geconfigureerde gebruikersnaam en het wachtwoord werden ingevoerd om in te loggen. Met de Wireshark filter telnet and ip.dst == 192.168.1.254 konden alle Telnet-pakketten die naar de switch werden verzonden, effectief worden geïsoleerd.

Bij het "Follow TCP Stream" van een Telnet-pakket, was alle ingevoerde tekst, inclusief de gebruikersnaam, duidelijk leesbaar. Dit komt doordat Telnet-data niet versleuteld wordt verzonden, wat het protocol uiterst kwetsbaar maakt voor afluisteren (eavesdropping). De waarneming van dubbele karakters bij het typen van de gebruikersnaam (maar niet bij het wachtwoord) is typerend voor Telnet-sessies: de server stuurt elke getypte letter terug (een "echo") als bevestiging om op het scherm van de terminal te tonen. Het wachtwoord wordt daarentegen lokaal niet weergegeven en ook niet ge-echo'd door de server, vandaar de afwezigheid van dubbele karakters in de stream.



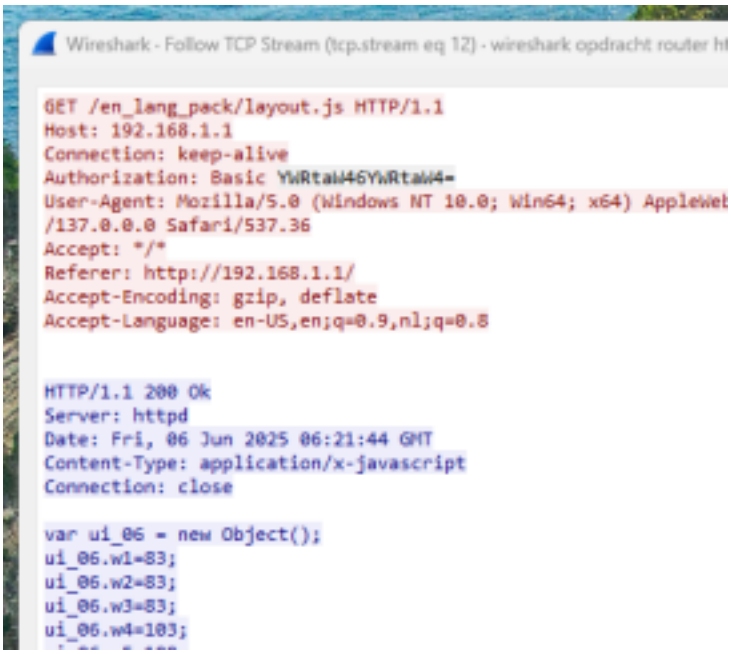
5.2. SSH-sessie analyse

Na het afsluiten van de Telnet-sessie en het starten van een nieuwe Wireshark-capture, werd een SSH-sessie naar dezelfde switch opgezet. Met de filter ssh and ip.dst == 192.168.1.254 werden de SSH-pakketten geïsoleerd.

Bij het "Follow TCP Stream" van een SSH-pakket was, in tegenstelling tot Telnet, geen leesbare inhoud te zien. Dit is de kern van SSH's veiligheidsmechanisme: de communicatie is versleuteld. Hieruit kan eenduidig worden geconcludeerd dat SSH een aanzienlijk veiliger alternatief is voor Telnet, aangezien potentiële afluisteraars de pakketten niet eenvoudig kunnen meelezen.

5.3. HTTP- en HTTPS-toegang tot Netwerkapparaten

Een verdere analyse van HTTP-toegang tot de router en switch toonde aan dat HTTP authenticatie (voor inloggen op de webinterface) vaak gebruik maakt van Base64-codering voor gebruikersnaam en wachtwoord. Hoewel Base64-codering de data niet versleutelt, maakt het de data wel onleesbaar in platte tekst voor een snelle blik. Met Wireshark is het echter eenvoudig om deze Base64-gecodeerde authenticatiegegevens te decoderen, waardoor gebruikersnamen (admin) en wachtwoorden (admin1pass) in platte tekst zichtbaar worden. Dit bevestigt dat HTTP-beheerinterfaces, zonder de implementatie van HTTPS, inherent onveilig zijn voor het verzenden van gevoelige inloggegevens.



Bij pogingen om via HTTPS verbinding te maken met de router of de switch konden geen verbindingen worden gemaakt. Dit suggereert dat de standaardconfiguratie van deze specifieke apparaten mogelijk geen HTTPS-server toestaat, of dat de benodigde SSL/TLS certificaten niet aanwezig of correct geconfigureerd zijn. Dit resultaat onderstreept nogmaals het cruciale belang van het correct configureren en afdwingen van HTTPS voor alle beheerinterfaces, om veilige communicatie te garanderen en ongeautoriseerde toegang tot inloggegevens te voorkomen door middel van versleuteling. Het principe van versleuteling bij HTTPS is identiek aan dat van SSH: de inhoud van de pakketten is onleesbaar voor afluisteraars.


Wireshark - Follow TCP Stream (tcp.stream eq 3) - wireshark opdracht https sporza.pcapng
sporza.be.

6. Conclusie

Deze praktische Wireshark-oefening heeft een diepgaand inzicht verschaft in de werking van verschillende netwerkprotocollen op de Data Link- en Netwerk-lagen. Het belang van fysieke en logische topologieën, de cruciale rol van MAC- en IP-adressering in pakket- en
frame-forwarding, en de kritieke verschillen tussen onversleutelde (Telnet, HTTP) en versleutelde (SSH, HTTPS) protocollen zijn duidelijk gedemonstreerd. De analyse heeft bevestigd dat Layer 2 MAC-adressen lokaal zijn voor elke "hop" op het netwerk, terwijl Layer 3 IP-adressen end-to-end routering mogelijk maken over verschillende netwerksegmenten heen. Tevens werd het fundamentele beveiligingsrisico van onversleutelde beheerprotocollen benadrukt, wat de absolute noodzaak van SSH en HTTPS voor netwerkbeheer onderstreept om de vertrouwelijkheid en integriteit van communicatie te waarborgen.

7. Referenties

- Figuur 1 Netacad; NetAcad/Cisco Networking Academy. (z.d.). *[Afbeelding van netwerktopologie/MAC-adressering]*. Geraadpleegd op [Datum van raadpleging, bijv. 7 juni 2025] via NetAcad.
  https://www.netacad.com/launch?id=c4da38fe-1cac-4094-b90c-1884c1c40a3a&tab=curriculum&view=add0a3e8-97e7-526c-8c2e-853990ac1ddc