CSIK

YOUR FIRST NETWORK LAB

LAB 1.0

TABLE OF CONTENTS

INTRODUKTION

I denne lab skal vi etablere og arbejde med dit første mindre netværk i kurset Netværksarkitektur på PBA i Cybersikkerhed. Vi vil bygge et lokalt netværk (LAN) og lære om grundlæggende netværkskoncepter gennem praktiske øvelser.

LÆRINGSMÅL

Efter gennemførelse af denne lab vil du kunne:

Del 1

- Identificere forskellige typer netværksudstyr
- Etablere et mindre lokalt netværk ([[LAN]])
- Forstå Automatic Private IP Addressing (APIPA)

Del 2

- Konfigurere statiske og dynamiske IPv4-adresser
- Anvende grundlæggende netværkskommandoer i kommandolinjen

UDSTYR OG MATERIALER

GRUPPENS FÆLLES UDSTYR

- 1x **Netværksswitch** (8-port umanaged, f.eks. Netgear ProSAFE GS108)
- 4x **Ethernet patchkabler** (Cat5e eller bedre, 1-2 meter)
- **Strømforsyning** til switch

PERSONLIGT UDSTYR (HVER STUDERENDE)

- Bærbar computer med Ethernet-forbindelse (RJ45 stik)
  - Hvis din laptop ikke har RJ45: USB-til-Ethernet adapter (kan lånes)
- Laboratoriejournal (notesbog eller digital dokument)
- Smartphone/tablet til research og backup-dokumentation

FREMGANGSMÅDE

Sørg først for at have alt det nødvendige udstyr fra listen ovenfor. Husk altid: ***Hvis du er i tvivl og ikke kan finde en løsning i gruppen, så spørg om hjælp.***

⚠️ **Vigtigt:** Sørg altid for at have den rigtige strømforsyning til udstyret. Forkert strømforsyning kan beskadige udstyret.

Når vi arbejder med netværksteknologi, laver vi gerne et skematisk diagram over systemet for at bevare overblikket og hurtigt kunne søge, finde og rette fejl.

NETVÆRKSTOPOLOGI

Dit første netværk består af 5 enheder: 4 laptops og én netværksenhed, som vi kalder en switch.

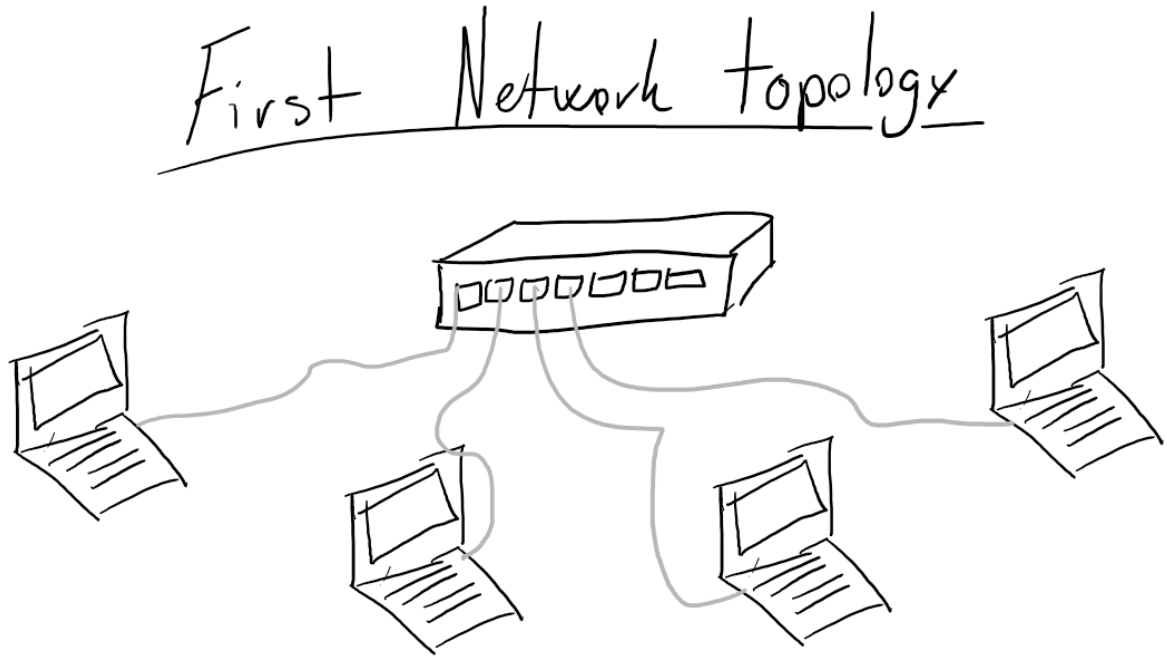


FIGURE 1: NETWORK TOPOLOGY OF YOUR FIRST LAB

Som du kan se på diagrammet, er netværket ikke komplekst og består af 5 enheder: 4 laptops og én netværksenhed, som vi kalder en switch. Vi kategoriserer disse enheder som intermediære netværksenheder (Intermediary Devices), der forbinder slutenheder. Laptopsene omtales ofte som slutenheder eller end-devices. Topologien omfatter også 4 netværksmedier.

Kontekst: I dette tilfælde refererer "netværksmedier" til de 4 Ethernet-kabler, der forbinder laptopsene til switchen. Det er den fysiske infrastruktur, som dataene transporteres gennem.

INTERMEDIARY DEVICES

Intermediary device forbinder slutenheder og sørger for, at data flyder gennem netværket. Eksempler inkluderer

- Switches og trådløse adgangspunkter (netværksadgang)
- Routere (internetworking)
- Firewalls (sikkerhed)

Network Media

Network media er den fysiske vej, som elektriske signaler følger mellem komponenter. Twisted-pair kabel bruges til telefon og moderne Ethernet-netværk. Snoningen af ledningerne beskytter mod crosstalk (støj fra tilstødende ledningspar).

Del 1 - Opsætning af netværk

Forbered switchen:

- Tilslut netværksswitchen til strøm og sørg for den er tændt
- Tilslut alle netværkskabler startende fra port 1
- Tilslut ***IKKE*** jeres laptops endnu

Forbered laptops:

- Slå Wi-Fi forbindelsen fra på alle laptops
- Test at I ikke har internetadgang ved at bruge en browser
- Test også i terminal/kommandoprompt ved at pinge Googles navneserver:
  - ping 8.8.8.8

Dokumentér jeres skridt med screenshots i laboratoriejournalen

Før tilslutning af laptops:

- Kør netværkskommandoen og dokumentér outputtet:
  - Windows: `ipconfig`
  - Mac/Linux: `ifconfig`

Tilslut laptops:

- Tilslut alle laptops til switchen
- Observér lysene på switchen - hvilke informationer kan du få fra denne observation?
- Hvilken type netværksmedie bruger I?
  - (inkl. kategori og længde af kabel)

Forbindelsestest

Lad laptopsene forbinde til netværket. Nu skal vi teste om vi kan etablere forbindelse mellem alle laptops ved hjælp af ping-kommandoen.

Efter et minut, åbn kommandolinjen på din laptop:

```
# Windows

ipconfig



# Mac/Linux
```

ifconfig

DOKUMENTÉR OUTPUTTET

- Hvad er subnet masken på din enhed?

Opret en tabel analog på et stykke papir, eller i Excel, Google Sheets eller lignende med minimum:

- Navne
- IPv4-adresser
- Subnet mask
- Fysisk adresse (MAC-adresse) af hver enhed
    - Hint til fysisk adresse:
    - Windows: `ipconfig /all`
    - Mac: `ifconfig` (vises direkte)

NAVN	IPv4 addr	Subnet mask	Fysisk addr

Undersøg og dokumentér:

- Hvad er en fysisk adresse, og hvad kaldes den også inden for netværksteknologi?
- Af de værdier I indsamler - hvilke er ens for alle i gruppen, og hvilke er forskellige?

Test forbindelse:

- Brug IPv4-adresserne fra jeres tabel til at pinge de andre enheder i gruppen
- Test forbindelsen mellem alle enheder

Undersøg APIPA:

- Søg og undersøg hvad "Automatic Private IP Addressing (APIPA)" er
- Forklar det kort med dine egne ord og inkludér reference til hvor du fandt informationen.

HUSK dokumentation.

FIGURE 2: IFCONFIG ON MACOS, ON MACOS THE SUBNET MASK (NETMASK) IS OUTPUT IN HEXADECIMAL FORMAT FF IN HEX = 255 IN DECIMAL.

💡 Citationer: Når vi bruger andre personers idéer i vores forskning, skal vi inkludere en kort notation ved siden af idéen for at lade vores læsere vide, hvem der udviklede den. Dette kaldes en in-text citation.[2]

Dette er slutningen på del 1. Du bør nu vide:

- Hvad en intermediær netværksenhed er og dens formål
- Hvad netværksmedier er
- Hvordan vi undgår crosstalk i netværkskabler
- Hvordan en Automatic Private IP-adresse ser ud
- Hvad vi bruger in-text citater til

Gennemgå ovenstående punkter i gruppen og sørg for, at alle forstår og kan redegøre for dem.

DEL 2 - STATISK IP-KONFIGURATION

I denne del arbejder vi videre med netværket fra del 1. Det er muligt at kommunikere mellem enheder ved hjælp af APIPA-adresserne, men det er ikke optimalt.

- Diskutér i gruppen: Hvilken service (eller server) mangler i netværket, siden enhederne tildeles APIPA-adresser?

I et LAN kan det være nyttigt at have statiske IP-adresser til slutenheder, derfor vil vi øve os i at sætte statiske IP-adresser på jeres laptops.

HVORDAN ÆNDRER MAN NETVÆRKSKONFIGURATION

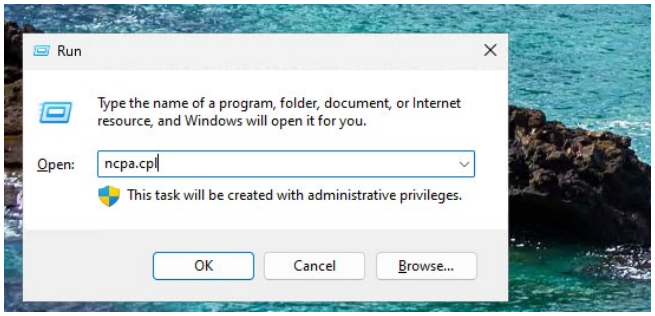
På en enhed der skal kommunikere over et TCP/IP netværk, skal vi give enheden information om konfiguration. Ligesom du skal have et mobilnummer for at bruge din telefon, ellers er det bare en enhed uden kommunikationsmuligheder.

I vores lille LAN har vi ikke adgang til en server, der kører Dynamic Host Configuration Protocol (DHCP), som automatisk konfigurerer slut-enhederne. Derfor skal vi gøre arbejdet manuelt.

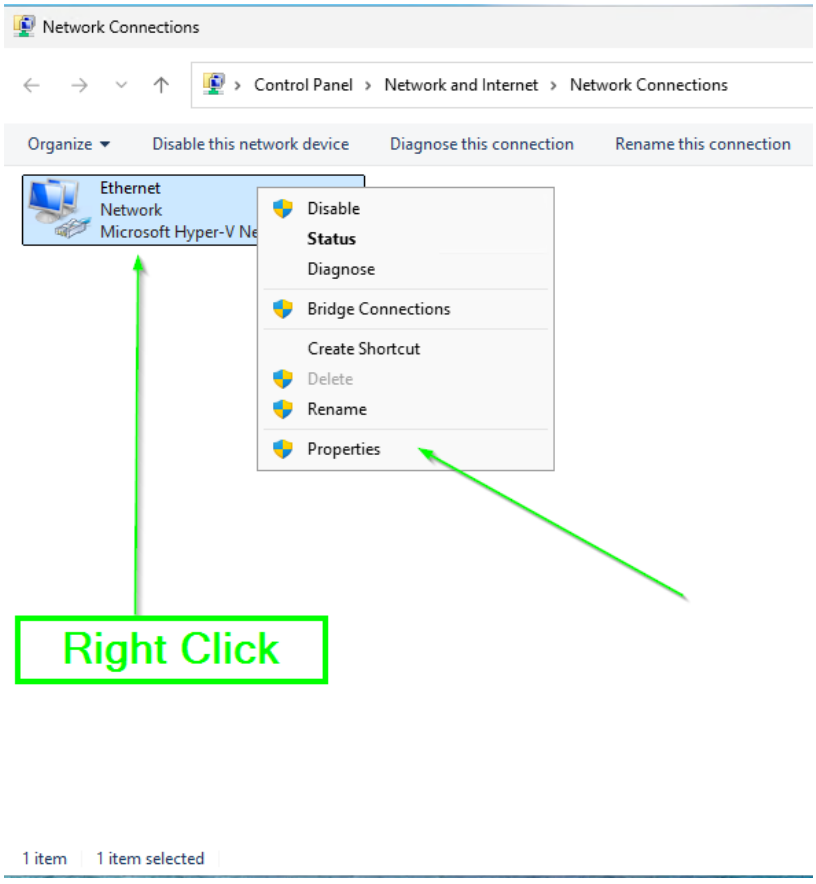
FIGURE 3: AN IOT MAILBOX [3]

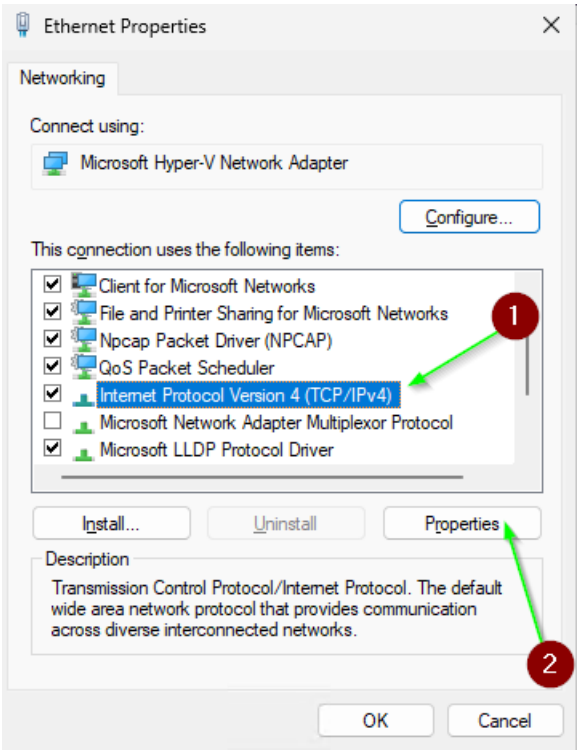
WINDOWS 11 PC:

- Windows + r
- Skriv: ncpa.cpl + ENTER
    - https://support.microsoft.com/da-dk/topic/how-to-run-control-panel-tools-by-typing-a-command-bce95b4d-e8c2-1cd0-ee0d-027679d520a6



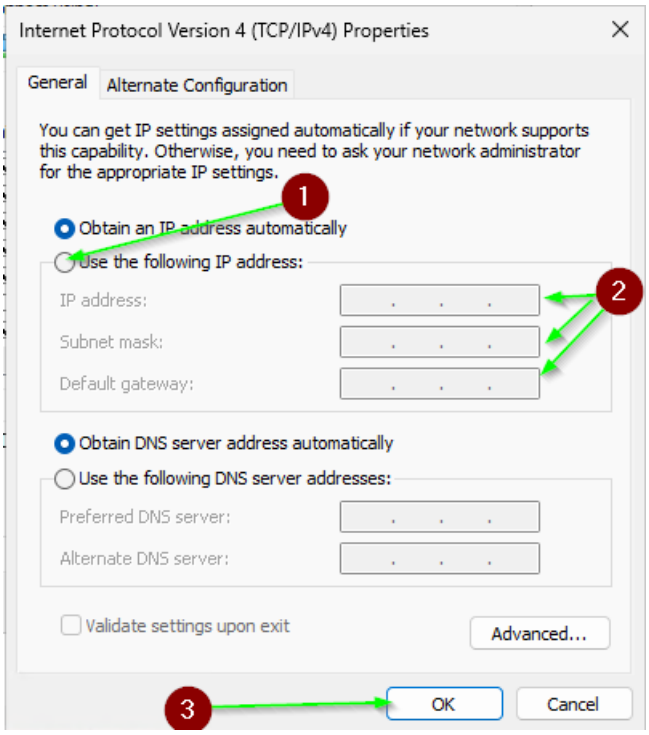
Højreklik på den interface du vil ændre og klik Egenskaber / Properties





Vælg Internet Protocol Version 4 (TCP/IPv4) og klik **Egenskaber**

Vælg **Brug følgende IP-adresse:**



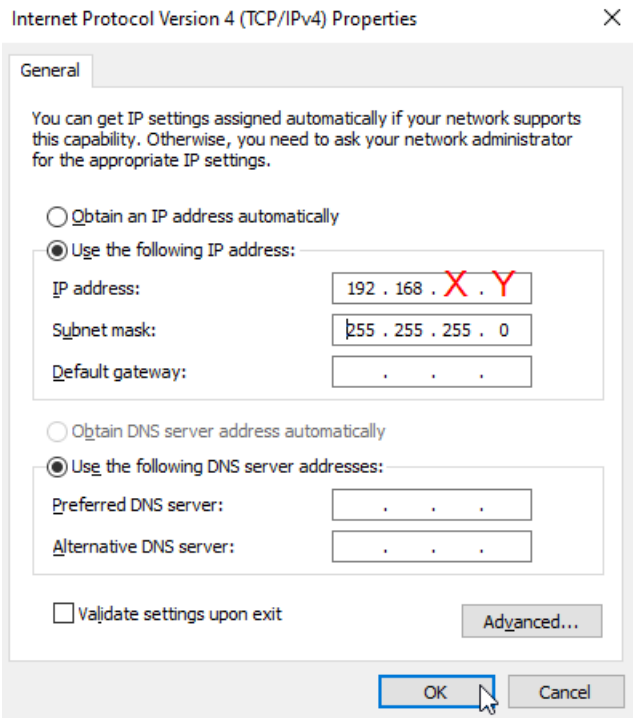


FIGURE 4: MANUALLY CONFIGURATION FOR THE ETHERNET CONNECTION ON A WINDOWS 10 PC

IP-ADRESSE SKEMA

Hvad er X og Y?

Hvis I er i gruppe 42, så er X = 42 osv.

Y er host-delen af jeres IPv4-adresse - I kan beslutte i gruppen hvem der har hvilket nummer

Det er en 8-bit adresse, og I kan IKKE bruge:

Første adresse (netværks-ID): 192.168.42.0

Sidste adresse (broadcast-adresse): 192.168.42.255

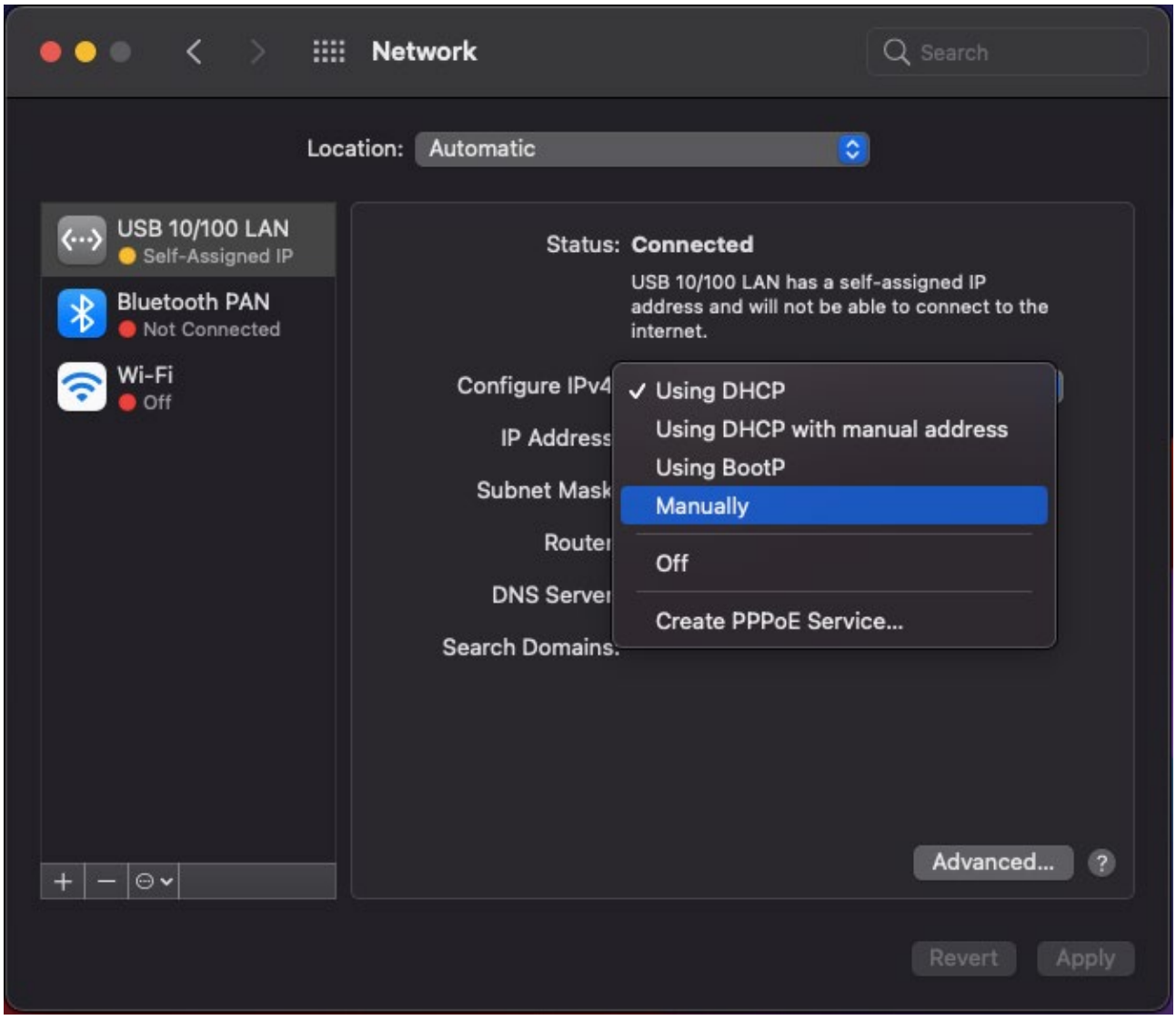
Indtast følgende information:

IP-adresse: 192.168.X.Y

Subnet mask: 255.255.255.0

PC RUNNING MACOS

- Klik på Systemindstillinger (eller brug cmd + space og søg)
- Klik på Netværk
- Vælg den netværksinterface du vil konfigurere
- Klik på Konfigurér IPv4: og sæt den til Manuelt



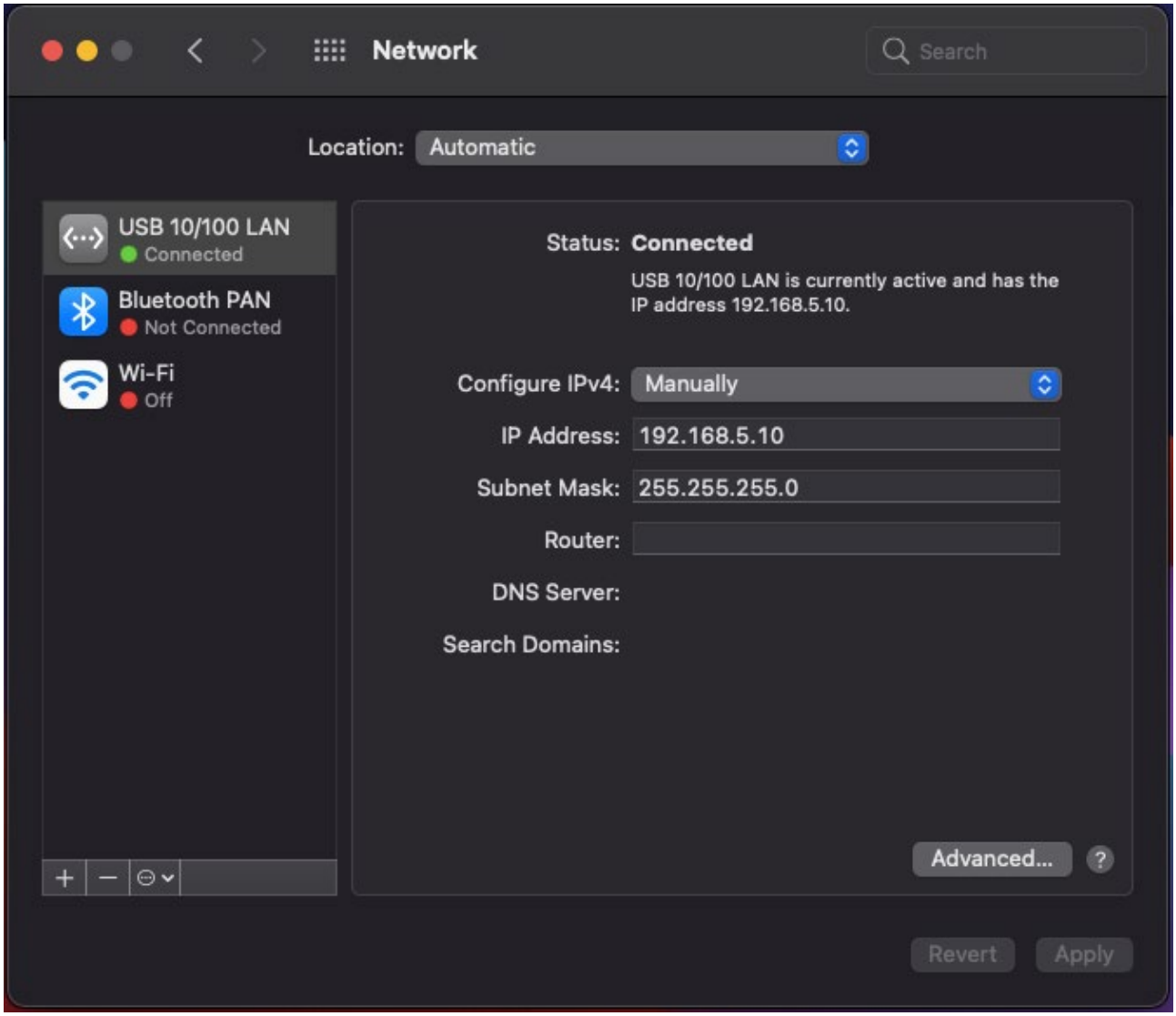


FIGURE 5: IN THIS EXAMPLE HERE ABOVE X = 5 AND Y = 10

Medtag denne nye tabel i jeres laboratoriejournal.

I skulle nu have en komplet tabel med følgende kolonneoverskrifter:

Name	Operating system	Physical Address	APIPA IPv4	Subnet mask (APIPA)	Static IPv4	Subnet mask (static)

EKSEMPEL

Jeg har opsat et testlab som eksempel. Det omfatter 3 laptops og en 8-port netværksswitch.

Tabellen for dette testlab ser ud som følger:

Name	Operating system	Physical Address	Static IPv4	Subnet mask (static)
PC1 mac air	macOS 11.6	28:ee:52:00:25:3a	192.168.42.10	0xffffff00 255.255.255.0
PC2 win PC	Win 10 21H1 Build 19043.1165	F4-30-B9-1A-C9-14	192.168.42.20	255.255.255.0
PC3 win work PC	Win 10 20H2 Build 19042.1237	38-22-E2-E5-3E-87	192.168.42.30	255.255.255.0

Jeg vælger min arbejds-PC med IP-adressen 192.168.42.30 som hovedterminal, og på denne computer vil vi starte med at anvende en ny netværkskommando ved navn arp

ARP-kommandoen

Vi bruger arp-kommandoen til at vise ARP-cachen. ARP-cachen er en simpel tabel, der bruges til at mappe IP-adresser til fysiske adresser (MAC-adresser).

Hjælp til ARP-kommando:

- Windows: arp /?
- Mac/Linux: man arp

Praktisk test

1. **Vælg én laptop** som "Hovedterminal"
2. **Test ARP-tabel** før kommunikation: arp -a
3. **Ping andre enheder** og observer ændringer i ARP-tabellen
4. **Dokumentér** alle trin med screenshots

OS-kommando cheatsheet:

What	Windows command	Mac command	Linux command
Test network connectivity: run 8 pings to an IPv4 address	ping -n 8 1.1.1.1	ping -c 8 1.1.1.1	ping -c 8 1.1.1.1

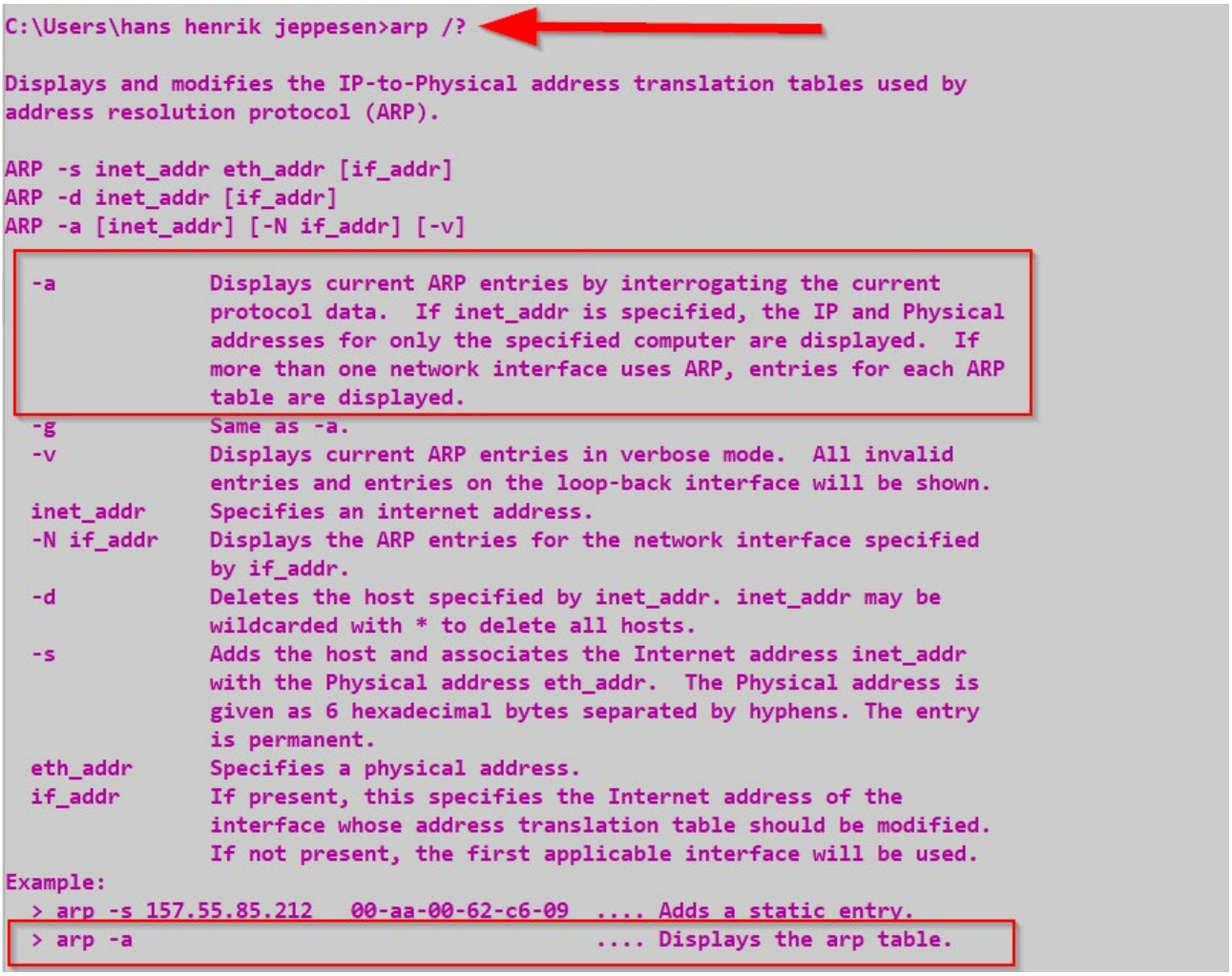


FIGURE 6: WE CAN SEE THE HELP SECTION FOR A WIN COMMAND USING /?

Fra denne hjælpetekst ser vi, at parameteren **-a** giver os det ønskede output.

Hvis du arbejder på en Mac med macOS, kan du læse mere om kommandoen og dens muligheder i den indbyggede manual. Brug kommandoen: **man arp**

Dette giver dig uddybende information om kommandoen og dens parametre. Du kan forlade manualen ved at trykke **Q**.

Det viser sig, at begge operativsystemer anvender parameteren -a til at vise arp-tabellen. Da ikke alle kommandoer har identiske parametre på tværs af systemer, er det klogt at kende grundlæggende kommandoer på flere operativsystemer end kun dit primære.

TILBAGE TIL TESTLABET OG VORES HOVEDTERMINAL

Vi kan udlæse forskellige informationer fra arp-tabellen ved hjælp af kommandoen arp -a. Outputtet vises på det følgende billede (alt terminaloutput fra PC3 er markeret med grøn baggrund).

```
C:\WINDOWS\system32>arp -a

Interface: 192.168.42.30 --- 0xf
  Internet Address      Physical Address      Type
  192.168.42.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Nu vil vi teste forbindelsen til PC2 (den private Windows-PC) med IP-adressen 192.168.42.20 fra vores hovedterminal PC3. Ping-kommandoen lykkes og producerer følgende output.

```
C:\WINDOWS\system32>ping 192.168.42.20

Pinging 192.168.42.20 with 32 bytes of data:
Reply from 192.168.42.20: bytes=32 time=1ms TTL=128
Reply from 192.168.42.20: bytes=32 time=1ms TTL=128
Reply from 192.168.42.20: bytes=32 time=1ms TTL=128
Reply from 192.168.42.20: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.42.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Nu hvor vi har bekræftet, at vi kan pinge fra PC3 til PC2, kan vi vende tilbage til arp-tabellen og undersøge om der er sket ændringer. Som det fremgår af det

følgende billede, har vi nu fået en ny post i arp-tabellens cache for den private PC. Vi har nu kendskab til opløsningen mellem IP-adressen og den fysiske adresse (MAC). Se tabellen fra starten af del 2, der indeholder oplysninger om komponenterne i mit testlab.

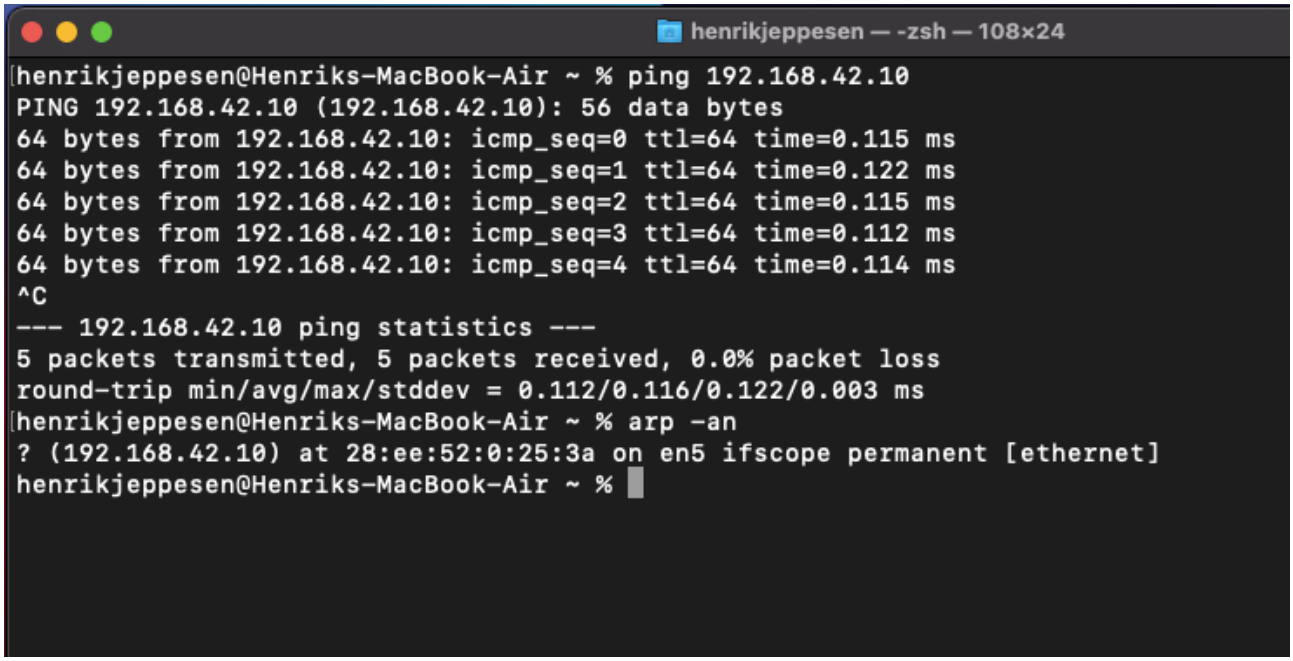
```
C:\WINDOWS\system32>arp -a

Interface: 192.168.42.30 --- 0xf
  Internet Address      Physical Address      Type
  192.168.42.20         f4-30-b9-1a-c9-14     dynamic
  192.168.42.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Hvis vi undersøger ***arp-tabellen*** på PC2, vil vi se, at vi nu har en indtastning for PC3 (IP 192.168.42.30), hvor vi kan se både IP-adressen og den fysiske adresse.

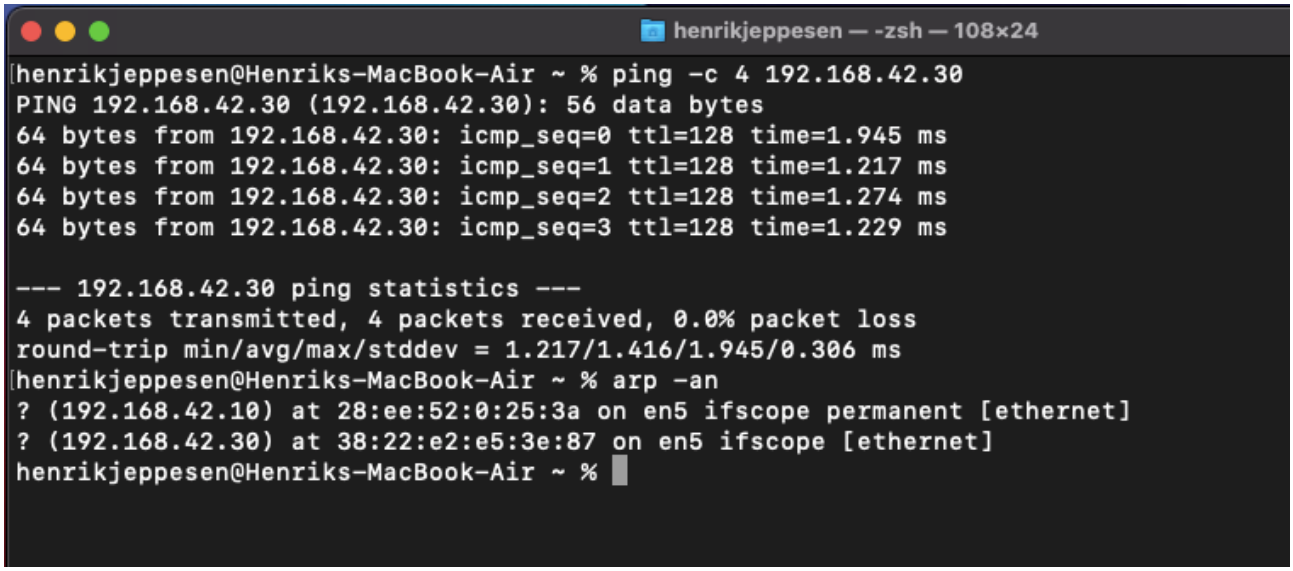
```
C:\Windows\system32>arp -a

Interface: 192.168.42.20 --- 0x2
  Internet Address      Physical Address      Type
  192.168.42.30         38-22-e2-e5-3e-87     dynamic
  192.168.42.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Nu vil vi undersøge den sidste computer i min lille testlab, PC1, som er en MacBook Air. Når vi først undersøger ***arp-tabellen*** på denne slutenhed, skulle vi ikke kunne se nogen poster.

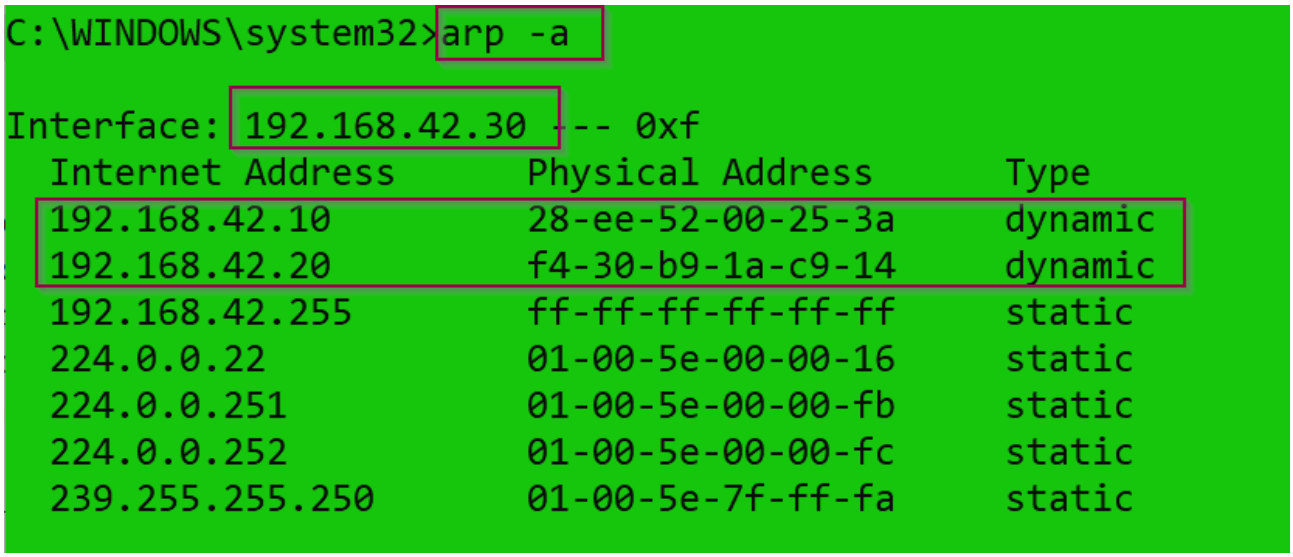
Derefter kan vi teste at pinge vores egen IP-adresse for at se hvad der sker med ***arp-tabellen***. Vi pinger 192.168.42.10 og kontrollerer efterfølgende ***arp-tabellen***. Som det fremgår af det følgende billede fra MacBook Air'en, lykkes ping'en, og ***arp-tabellen*** vil indeholde en post med både IP-adressen og den fysiske adresse:


henrikjeppesen — -zsh — 108×24
henrikjeppesen@Henriks-MacBook-Air ~ % ping 192.168.42.10
PING 192.168.42.10 (192.168.42.10): 56 data bytes
64 bytes from 192.168.42.10: icmp_seq=0 ttl=64 time=0.115 ms
64 bytes from 192.168.42.10: icmp_seq=1 ttl=64 time=0.122 ms
64 bytes from 192.168.42.10: icmp_seq=2 ttl=64 time=0.115 ms
64 bytes from 192.168.42.10: icmp_seq=3 ttl=64 time=0.112 ms
64 bytes from 192.168.42.10: icmp_seq=4 ttl=64 time=0.114 ms
^C
--- 192.168.42.10 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.112/0.116/0.122/0.003 ms
henrikjeppesen@Henriks-MacBook-Air ~ % arp -an
? (192.168.42.10) at 28:ee:52:0:25:3a on en5 ifscope permanent [ethernet]
henrikjeppesen@Henriks-MacBook-Air ~ %

Nu vil vi teste at pinge PC3 fra PC1 og derefter undersøge arp-tabellen igen. Det følgende billede viser resultatet af denne operation.

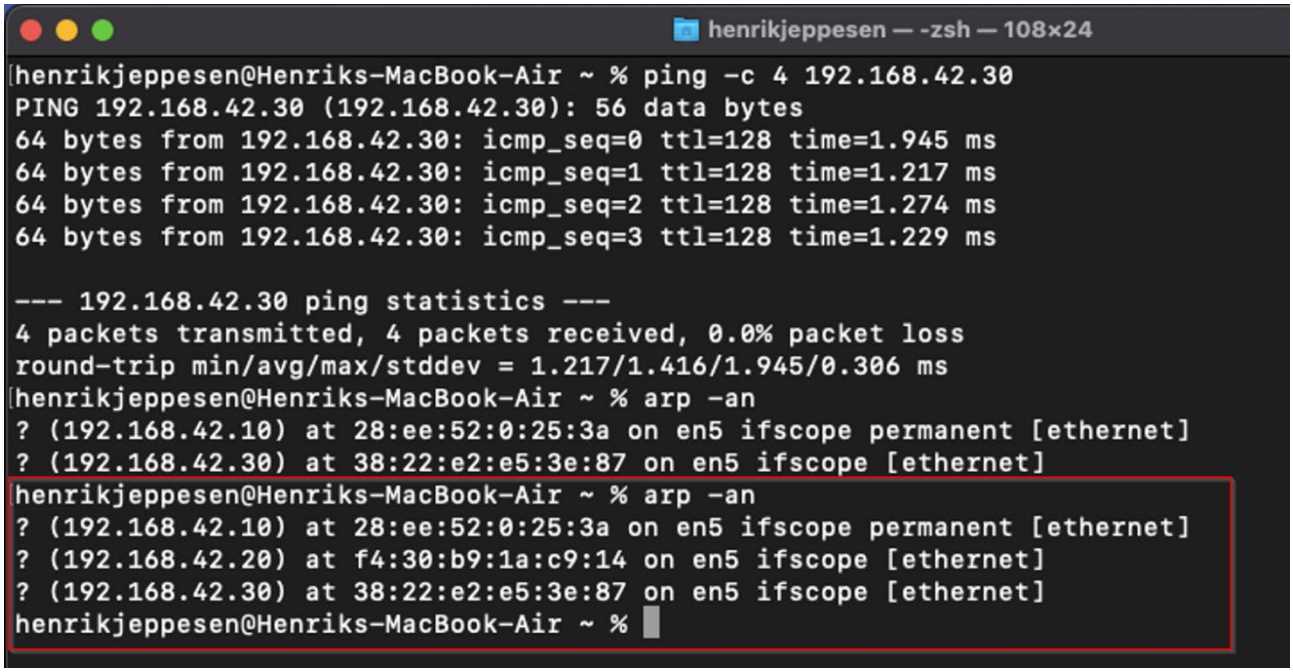


Vi har nu oplysninger om både PC1 og PC3 i ***arp-tabellen*** på PC1. Og hvis vi undersøger ***arp-tabellen*** på PC3, vil vi se, at der nu er en post for PC1 i ***arp-tabellen***. Det følgende billede viser outputtet fra PC3.



Vi kan konkludere dette lille testlab med at teste ping fra PC2 til PC1, og derefter kan vi på PC1 køre kommandoen **arp -an** for at se den fuldstændige ***arp-tabel*** for alle slutenheder i netværket. Det følgende billede viser resultatet. Nu

kan vi analysere disse data og kontrollere om de stemmer overens med oplysningerne i tabellen, vi oprettede i starten.



Name	Operating system	Physical Address	Static IPv4	Subnet mask (static)
PC1 mac air	macOS 11.6	28:ee:52:00:25:3a	192.168.42.10	0xffffff00 255.255.255.0
PC2 win10	Win 10 21H1 Build 19043.1165	F4-30-B9-1A-C9-14	192.168.42.20	255.255.255.0
PC3 win10	Win 10 20H2 Build 19042.1237	38-22-E2-E5-3E-87	192.168.42.30	255.255.255.0

Nu skal I selv gennemføre dette testlab med jeres egne enheder. Hvis I har flere end 3 slutenheder, er det ikke et problem. Husk at dokumentere alle jeres skridt i laboratoriejournalen og sørg for at medtage screenshots af kommandoresultaterne samt korte forklaringer skrevet med jeres egne ord eller ved brug af korrekte kildehenvisninger. I skal skiftes til at være "hovedterminal"

ARP-tabel rensning

Windows: arp -d (med administrator-rettigheder)

Mac/Linux: sudo arp -d -a

Dette er slutningen på del 2. Du bør nu vide:

- Hvad en DHCP-server er, og hvad vi bruger den til
- Forskellen mellem statiske og dynamiske IP-adresser
- Hvordan man sætter statiske IP-adresser på dit primære OS
- Hvilke to adresser i et netværk vi ikke kan bruge til slutenheder
- Hvad vi mener med NIC i netværksteknologi
- Hvilke informationer vi kan finde i ARP-tabellen
- Hvilken kommando vi bruger til at vise ARP-tabellen

Gennemgå ovenstående punkter i gruppen og sørg for, at alle forstår og kan redegøre for dem.

Rigtig god arbejdslyst

BONUS-OPGAVER

Opgave B: Netværksanalyse

1. Brug nslookup til at finde IP-adressen for google.com
2. Hvad sker der når I prøver at pinge denne adresse fra jeres isolerede netværk?
3. Forklar hvorfor det virker/ikke virker

REFERENCES

[1] 'Internet of everything', *OpenLearn*. https://www.open.edu/openlearn/science-maths-technology/internet-everything/content-section-overview (accessed Mar. 11, 2021).
[2] D. Longley, 'LibGuides: Research Skills Tutorial: What Is Citing?' https://subjectguides.esc.edu/c.php?g=234343&p=3001637 (accessed Sep. 22, 2021).
[3] 'Build an IoT Mailbox Sensor with a Twilio SIM and M2M Commands', *Twilio Blog*. https://www.twilio.com/blog/iot-mailbox-sensor-m2m-to-sms-functions (accessed Sep. 23, 2021).
[4] JasonGerend, 'Dynamic Host Configuration Protocol (DHCP)'. https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top (accessed Sep. 22, 2021).
[5] 'Network Administration: ARP Command', *dummies*. https://www.dummies.com/programming/networking/network-administration-arp-command/ (accessed Sep. 24, 2021).