# **Labøving 4 – IP og nettlaget**

Hensikten med øvingen er å undersøke IP-protokollen og kommandoer man kan kjøre fra PC på nettlaget.

**Øvingen**

# 1. Konfigureringer på egen PC

Få oversikt over mulighetene med ipconfig ved å skrive et spørsmåltegn bak kommando. Legg pesielt merke til to

|  |  |
| --- | --- |
| >ipconfig | Viser grunnleggende IP-parametere for aktive nettverkskort |
| >ipconfig /all | Viser flere opplysninger |

Undersøk **IPv4** med >ipconfig:

1. Hva er egen IP-adresse?

10.22.62.71

1. Hva er IP-adressen til default gateway?

10.22.60.1

1. Disse har samme Prefiks, nettverksdel av IP-adressen, og hva er det?

Nettmaske: 0xfffffc00 som tilsvarer 255.255.252.0 i desimal.

Dette blir:

* 2 x 255 = 8 bits (1111 1111) og 252 = 6 bits (1111 1100).
* 8+8+6 = 22 bits utgjør nettverksdelen.

10.22.60.0/22

Undersøk **IPv6** med >ipconfig (På NTNU får IPv6 om du ikke gjør det på hjemmenettet)

1. Du har en «Link-local» IPv6 adresse. Dette er en egengenerert adresse som bare benyttes innenfor eget IP-subnett (på samme link). Hva er innholdet av de første 64 bit, prefikset? Skriv på IPv6 kortform.

fe80::/64

1. Hva er prefikset til IPv6 default gateway? Sammenlikne med det du fant i oppgave 1.

fe80::/64

1. Hva er din (globalt unike) IPv6-adresse, og hva er 64-bit prefikset her? (gjør gjerne oppslag på lenke gitt i forelesning)

Min globale unike IPv6-adresse: 2001:700:300:400f:1cc6:af9d:e002:361a

64 bits prefikset: 2001:700:300:400f::/64

Undersøk **egen MAC-adresse** med >ipconfig

1. Hva er din MAC-adresse?

c4:35:d9:b0:ba:e1

1. Hvem er produsent av nettverkskortet?  
   *Tips: de første 3 byte angir produsent. Man kan enten google på «network mac producer 12-34-AB» eller bruke Wireshark med View/Name resolution/fysisk»*

*Apple, Inc.*

# 2. Subnetting

Du er gitt adresserommet 192.168.0.128/25. Netteier ønsker å dele dette adresserommet i to like store subnett for å skille ansatte og gjester..

1. Hva blir prefiksene for disse to subnettene? Hva blir laveste og høyeste IPv4 adresse i de to subnettene?

/25 forteller oss at 25 bits er reservert til nettverksdelen. I en IPv4 adresse blir det:  
32-25 = 7 🡺 2^7 = 128 gyldige adresser i det opprinnelige nettverksrommet.

Ved å dele /25 til et /26-nettverk, får vi to like store subnett. Prefikset for subnettene blir:

* 192.168.0.128/26 (ansatte)
  + Laveste 192.168.0.129
  + Høyeste 192.168.0.191
* 192.168.0.192/26 (gjest)
  + Laveste 192.168.0.193
  + Høyeste 192.168.0.255

Subnettet med høyeste adresser deles i ytterlige to like store subnett

1. Hva blir prefiksene for disse to subnettene? Hva blir laveste og høyeste IPv4 adresse i de to subnettene?

Øker fra /26 til /27 🡺 32-27 = 5 🡺2^5=32

* 192.168.0.192/27
  + Laveste 192.168.0.193
  + Høyeste 192.168.0.222
  + Broadcast 192.168.0.223
* 192.168.0.224/27
  + Laveste 192.168.0.225
  + Høyeste 192.168.0.254
  + Broadcast 192.168.0.255

# 3. Nettverkskommandoer fra terminalvindu

PING

Ping en webtjener mens du fanger pakker med Wireshark. Bruk displayfilter ICMP eller ICMPv6.

Vi pinget “ping google.com”

1. Hvor mange pakker sender ping for å beregne gjennomsnittlig RTT?

* Antall pakker med ping -
* Gjennomsnittlig RTT - 61.145

1. Hvor stor er nyttelasten?

48 bytes

1. Hva er innholdet av nyttelasten?

Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637

Dette er et mønster som ofte går igjen for å teste at pakker blir sendt og kommer i retur på riktig måte.

Bonus/Frivillig

1. Du kan endre nyttelasten til f.eks 10kB. Hva skjer med IP-pakkene da?   
   *CMD> ping -l 10000*

Timeout: Får svar tilbake at meldingen er for lang.

1. Du kan redusere nyttelasten til 1 byte. Hva skjer med innholdet da?

Innholdet er en byte. Data: 00

TRACEROUTE

Kjør traceroute (tracert) til en ekstern webtjener mens du fanger pakker med Wireshark. Bruk igjen displayfilter ICMP eller ICMPv6.

1. Hvor mange pakker sender traceroute til hver ruter i kjeden?

3 pakker

1. Hvilken endring gjøres med TTL/Hop Limit fra første ruter som svarer til neste ruter?

TTL økes med 1 fra hver ruter til neste. Altså fra 1. ruter er TTL 1, fra 2. ruter er TTL 2, osv.

1. Så altså, hvordan finner Traceroute ut hvilke rutere en pakke passerer på vei til destinasjonen?

Traceroute sender pakker med økende TTL. Hver ruter reduserer TTL, og når TTL når 0, sendes en ICMP Time Exceeded-melding tilbake. Dette gjør at Traceroute kan identifisere rutene pakken har tatt til målet.