NTNU

Norges teknisk-naturvitenskapelige universitet

Nettverkslaget og brannmurer

Datakommunikasjon inft1007

Helge Hafting

6. februar 2024

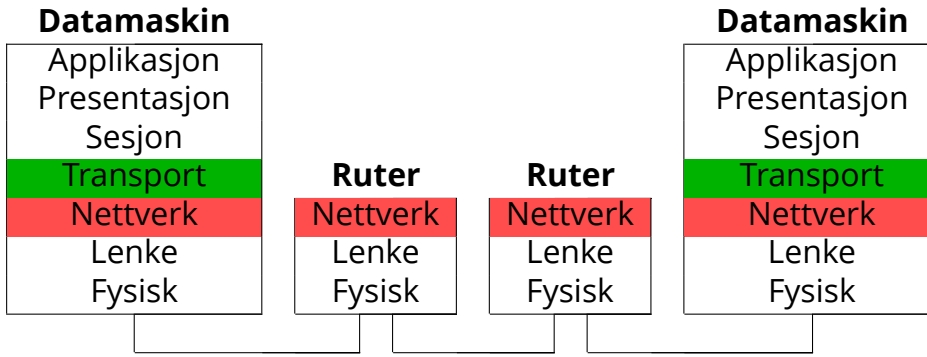
Nettverkslaget og IP

- Vi ser nærmere på:
  - Nettverkslaget
  - IP – Internettprotokollen
    - Format
    - Fragmentering
    - IP-adresser
- Brannmurer
  - Hva de gjør
  - Ulike typer

Nettverkslaget

- Overfører data fra transportlaget gjennom Internettet
  - Internet Protocol (IP), pakker og adresser
  - ruting basert på adresser
  - Feilrapportering og informasjonsprotoller
- Internett tilbyr en datagramtjeneste (IP-pakke) på nettverkslaget
- IP må være implementert i alt utstyr som pakkene passerer
  - Se illustrasjon på neste side

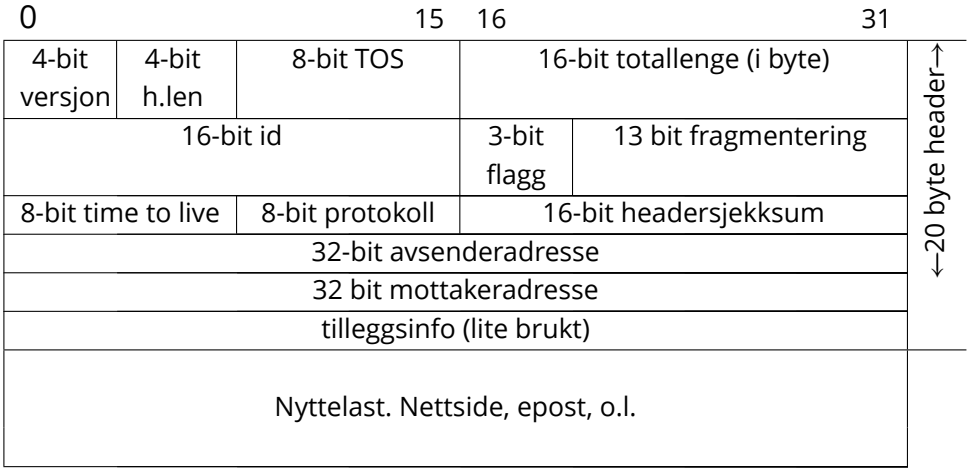
Nettverkslaget



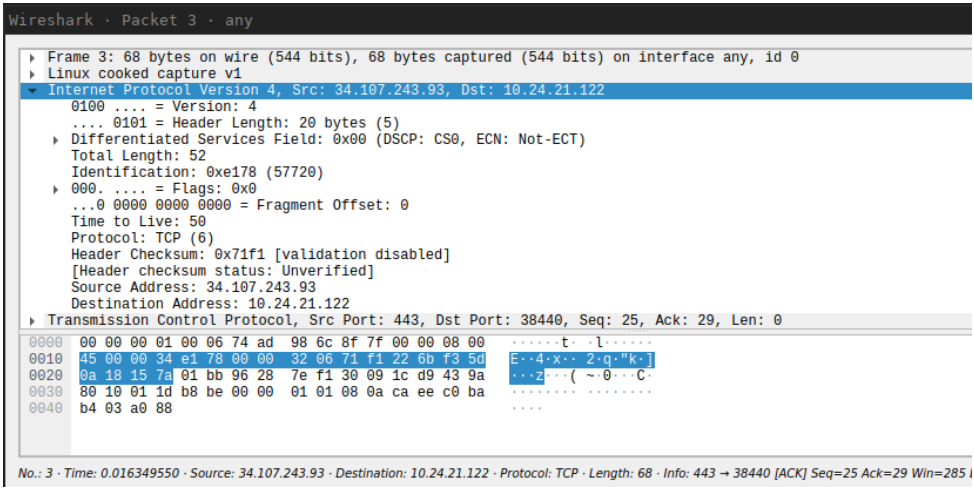
Internettprotokollen (IPv4)

- Er en upålitelig protokoll
  - ingen sekvens- feil- eller flytkontroll
  - slikt overlates til transportlaget
- Opererer forbindelsesløst
  - Ingen oppkobling
- Nyttelasten kan være hva som helst
  - TCP, UDP, ICMP og IGMP benytter IP-pakker

Format på en IP-pakke



IP-pakke i wireshark



Fragmentering i IPv4

- Pakker for store for lenkelaget, fragmenteres
- Utføres av avsender, eller mellomliggende rutere
  - Et fragment kan deles videre, hvis neste overføringsmedium trenger enda mindre pakker
- Hvert fragment har fullstendig header, så det kan rutes
- Mottaker setter fragmentene sammen, ved hjelp av feltene:
  - flagg, fragmentering og id

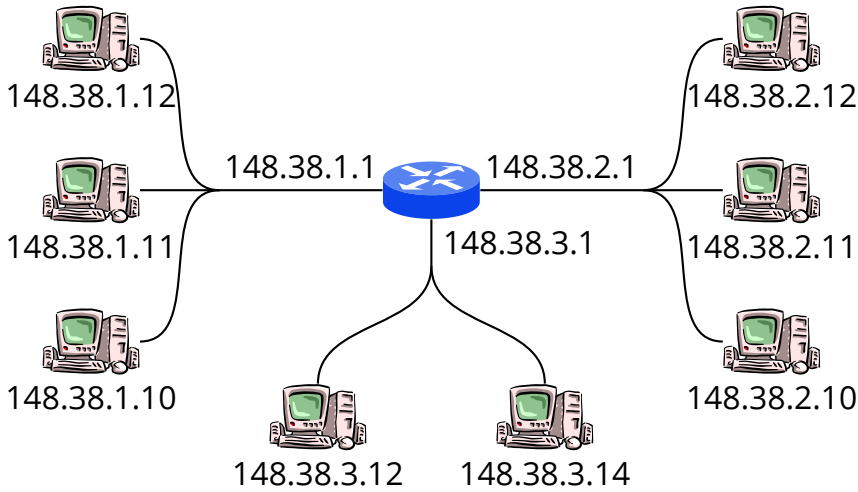
IP-adressering (IPv4)

- Kommunikasjon krever adressering
- På Internett brukes IP-adresser som er hierarkisk oppbygd
- Alle nettkort har sin unike adresse

IP-adressering (IPv4)

- En IPv4-adresse er 32 bit
  - vi skriver dem som 4 byte: a.b.c.d
  - hver byte er et tall mellom 0 og 255.
- Adressen består av en nettadressedel og en nodeadresse
- Adresseområde 0.0.0.0 – 255.255.255.255
- IPv6 bruker lignende system, men 128 bit i stedet.

IP-adressering (IPv4), 3 nettverk med ruter



Private adresser

- Deler av IPv4-adresserommet er satt av til private adresser:
  - 10.0.0.0–10.255.255.255
  - 172.16.0.0–172.31.255.255
  - 192.168.0.0–192.168.255.255
- Private adresser brukes internt, de rutes ikke på Internettet
- Slike interne nett kan likevel kobles til Internettet med en NAT-ruter

Brannmurer

- En brannmur plasseres mellom våre nett og verden utenfor
  - kan være en egen boks
  - kan være en del av ruteren
- Beskytter oss, ved å avbryte uønsket kommunikasjon
- Eksempel:

Typer brannmurer

- Pakkefilter
- Innholdsfiltre
- Personlig brannmur

Pakkefilter

- Ser på én og én IP-pakke, som enten får passere eller stoppes
  - basert på hva pakka inneholder
- Vurderer headerfeltene i ip-pakka:
  - til-adresse
  - fra-adresse
  - tcp/udp-felter som
    - protokoll (http/ftp/smtp/imap,...)
    - tcp-flagg
- Ser vanligvis ikke på nyttelasten i pakka, fordi:
  - dette krever forståelse av innholdet
  - innholdet er gjerne delt opp over mange pakker

Innholdsfilter

- Forstår en eller flere protokoller, på applikasjonslagnivå
  - http for filtrere web, smtp for å filtrere post, ...
- Tar imot flere pakker (en hel epostmelding eller nettside)
  - kan dermed gjøre avanserte tester som virusscan
- Kan blokkere eller slippe gjennom hele sider/meldinger
- Kan fjerne virus fra vedlegg i epost

Personlig brannmur

- Kjører på brukerens pc, derfor «personlig»
- I tillegg til IP-felter, kan den se på hvilke programmer som forsøker å kommunisere
- Kan hindre programmer/apper som gjør uønsket kommunikasjon
  - «Får dette programmet lov til å bruke denne tjenesten på nett?»

Inn-og utgående brannmur

- Inngående: beskytter oss, mot farer på nettet
  - Det de fleste tenker på, når det gjelder brannmurer
- Utgående: beskytter verden mot oss!
  - nyttig, hvis en av våre maskiner blir hacket og forsøkt brukt i et angrep
  - vi slipper å få skyld for slike angrep