



Nettverkslaget og brannmurer

Datakommunikasjon inft1007

Helge Hafting

6. februar 2024

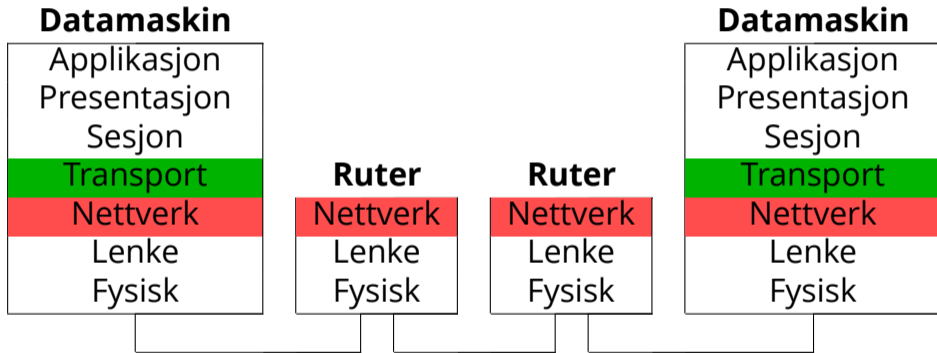
Nettverkslaget og IP

- ▶ 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

0	15	16	31	
4-bit versjon	4-bit h.len	8-bit TOS	16-bit totalle (i byte)	
16-bit id		3-bit flagg	13 bit fragmentering	
8-bit time to live		8-bit protokoll	16-bit headersjekksum	
32-bit avsenderadresse				
32 bit mottakeradresse				
tilleggsinfo (lite brukt)				
Nyttelast. Nettside, epost, o.l.				

←20 byte header→

IP-pakke i wireshark

Wireshark · Packet 3 · any

- ▶ Frame 3: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface any, id 0
- ▶ Linux cooked capture v1
- ▼ Internet Protocol Version 4, Src: 34.107.243.93, Dst: 10.24.21.122
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 52
 - Identification: 0xe178 (57720)
 - ▶ 000. = Flags: 0x0
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 50
 - Protocol: TCP (6)
 - Header Checksum: 0x71f1 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 34.107.243.93
 - Destination Address: 10.24.21.122
 - ▶ Transmission Control Protocol, Src Port: 443, Dst Port: 38440, Seq: 25, Ack: 29, Len: 0

0000	00 00 00 01 00 06 74 ad 98 6c 8f 7f 00 00 08 00t..l.....
0010	45 00 00 34 e1 78 00 00 32 06 71 f1 22 6b f3 5d	E..4.x..2.q"K.]
0020	0a 18 15 7a 01 bb 96 28 7e f1 30 09 1c d9 43 9a	...z]..(~0...C.
0030	80 10 01 1d b8 be 00 00 01 01 08 0a ca ee c0 ba
0040	b4 03 a0 88

No.: 3 · Time: 0.016349550 · Source: 34.107.243.93 · Destination: 10.24.21.122 · Protocol: TCP · Length: 68 · Info: 443 → 38440 [ACK] Seq=25 Ack=29 Win=285

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 routes
- ▶ Mottaker setter fragmentene sammen, ved hjelp av feltene:
 - ▶ flagg, fragmentering og id

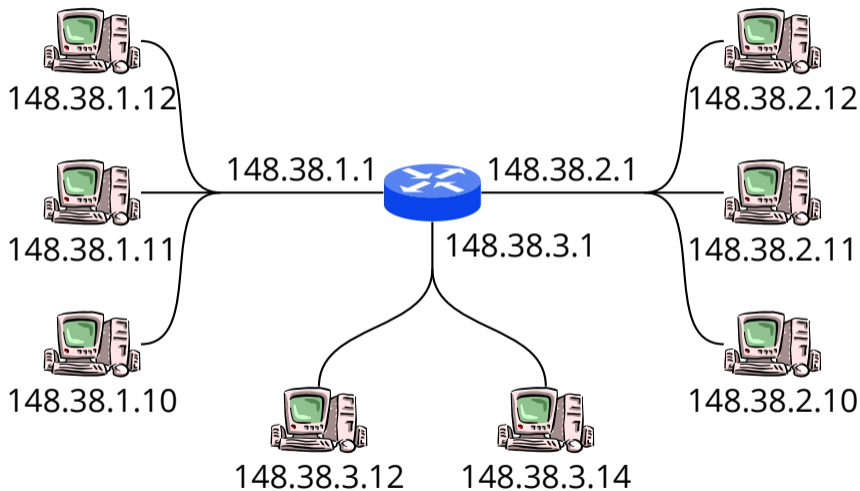
IP-adressering (IPv4)

- ▶ 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 ruter
- ▶ Beskytter oss, ved å avbryte uønsket kommunikasjon
- ▶ Eksempel:



Typer brannmurer

- ▶ Pakkefilter
- ▶ Innholdsfiltere
- ▶ 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 applikasjonsnivå
 - ▶ 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