

TK1100

FORELESNING 0x09 NETTVERKSLAGET

1. Nettverkslaget

- a) Forklar kort hva hovedoppgaven til nettverkslaget er.

Nettverkslaget inneholder protokoller som gjør det mulig å overføre pakker fra avsender til mottaker via en rute i nettverket. Her brukes nettverksprotokollen hos avsender og mottaker, men også på hver mellomlanding i nettverkstjeneren. Det er nettverkslaget som «finner veien» som pakken skal transporteres via. Her er det også mulig å definere denne ruten før pakken sendes.

- b) Test å skriv in `netstat -r` eller `route print` i terminalen på din maskin, hva får du for informasjon?

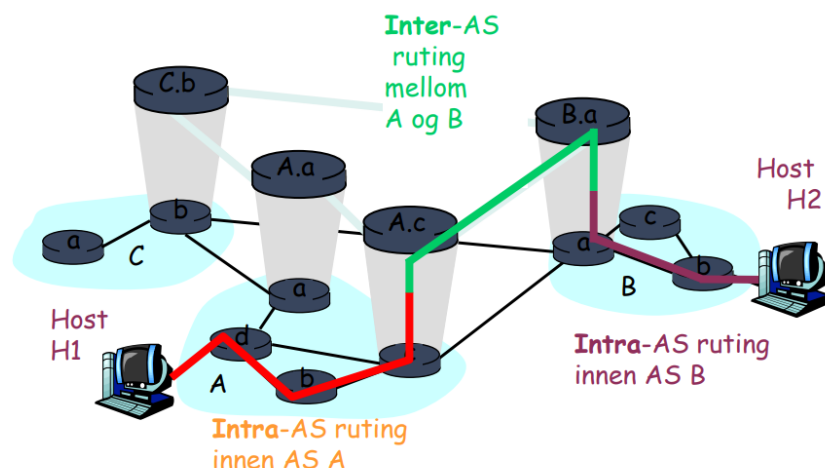
Interface list, IPv4/IPv6 Route table med aktive ruter, og eventuelle Persistent Routes.

- c) Hva menes med «Routing av datagram»?

Routing er det som gjøres for å finne ut hvilken vei datagrammet skal bevege seg over nettverket, fra avsender til mottaker. Dette bestemmes før datagrammet sendes ut.

- d) Hva er forskjellen mellom Intra-AS og Inter-AS ruting?

Intra-AS er for ruting lokalt på et nettverk og Inter-AS er for ruting mellom to nettverk, Intra-AS inneholder altså interne gateways/routere og Inter-AS inneholder eksterne gateways/routere.



- e) Hva er adresse til localhost?

127.0.0.1

2. IPv4

- a) Hvor lang er en IPv4 adresse og hvorfor kalles det for en adresse?

En IPv4 adresse er 32-bit lang og fungerer som en slags id på internett for maskiner. Adressen sier også hvilket nettverk maskinen er koblet til. Man kan tenke på det som en gateadresse, som posten bruker for å finne frem til riktig gate, og til slutt det spesifikke huset du sitter i.

- b) Skriv in `ipconfig` (Windows) eller `ifconfig` (OSX/Linux) i terminalen, hvilken informasjon får du frem?

Ip adresse, subnet maske og default gateway for hver adapter koblet til TCP/IP.

- c) Hva er din «Default Gateway» på din maskin akkurat nå?

Bruk `ipconfig` eller `ifconfig` i terminalen for å finne ut av dette. Dette vises også på slideserie fra dagens forelesning.

- d) Hvordan får du tildelt din IPv4 adresse i et Local Area Network?

Det er mulig å sette en IPv4 adresse manuelt og få denne til å bli statisk i et LAN, men det som er vanligst er å ta i bruk DHCP (Dynamic Host Configuration Protocol) for å tildele IP-adresser i et LAN.

- e) Forklar kort hvordan et datagram transporteres fra avsender til mottaker, de er på ulike nettverk.

1. Avsender finner nettverksadresse til mottaker
2. Avsender finner ut om mottaker er på samme nettverk eller ikke, for å se om de er direkte forbundet
3. Ruting-tabellen gir beskjed om hvor neste stopp/hopp er på veien for avsender for å nå frem til mottaker
4. Link blir laget til de nødvendige stoppene/hoppene
5. Datagram sendes gjennom nettverket av stopp/hopp ved hjelp av linker og til den kommer frem til mottakers gateway og til slutt mottaker

- f) Hva trengs for å finne nettverksprefixen?

Nettmaske og IP-adresse, med hjelp av disse er det mulig å finne ut av om to maskiner er på samme nettverk eller ikke.

- g) Hva er en Nettmaske og hvorfor brukes den?

Det er nettmasken som bestemmer hvilken del av IP-adressen som er prefix og hvilken del som er host, det er altså på denne måten man finner ut av om maskiner er på samme IP-nettverk og om de har mulighet å sende data direkte mellom hverandre eller om de må utenfor nettverket.

- h) Hvilken operasjon brukes for å regne ut adresse med nettmaske?

AND operasjonen

- i) Kan 10.21.3.5 med nettmaske 255.255.254.0 sende direkte til 10.21.2.255 med nettmaske 255.255.254.0? Hint: Se slideserien fra forelesning for hvordan du skal regne ut dette.

Regn først ut hvilket nettverk de ulike maskinene tilhører med hjelp av nettmaske og AND operasjonen

10.21.3.5
255.255.254.0

	0000	1010	.	0001	0101	.	0000	0011	.	0000	0101
AND	1111	1111	.	1111	1111	.	1111	1110	.	0000	0000
	0000	1010	.	0001	0101	.	0000	0010	.	0000	0000

Konverter svaret til desimal og regn hvor mange bit som er prefix.

Det lokale nettverket er: 10.21.2.0/23

Når du siden gjør det samme med 10.21.2.255 og nettmaske 255.255.254.0 kommer du merke at du får samme svar hvilket betyr at de er i samme nettverk og kan sende direkte til hverandre.

- j) Kan 10.21.3.5 med nettmaske 255.255.255.0 sende direkte til 10.21.2.255 med nettmaske 255.255.255.0? Hint: Se slideserien fra forelesning for hvordan du skal regne ut dette.

Regn først ut hvilket nettverk de ulike maskinene tilhører med hjelp av nettmaske og AND operasjonen

10.21.3.5
255.255.255.0

	0000	1010	.	0001	0101	.	0000	0011	.	0000	0101
AND	1111	1111	.	1111	1111	.	1111	1111	.	0000	0000
	0000	1010	.	0001	0101	.	0000	0011	.	0000	0000

Konverter svaret til desimal og regn hvor mange bit som er prefix.

Det lokale nettverket er: 10.21.3.0/24

Når du siden gjør det samme med 10.21.2.255 og nettmaske 255.255.255.0 kommer du merke at du ikke får samme svar, denne maskinen tilhører nettverket 10.21.2.0/23.

k) Hva menes med private adresser?

En privat IP-adresse er din adresse du har på det nettverket du er oppkoblet til og det er ikke den adressen som blir sendt ut til internett, her er det Internett-routere som automatisk dropper den private IP-adresse og gir pakken en IP-adresse som alle på ditt nettverk deler. At ta i bruk private IP-adresser gir en fleksibilitet for kommunikasjon internt i nettverk.

l) Hva er et subnet?

Subnet er et nettverk av maskiner som har samme prefix i sin IP-adresse og kan derfor kommunisere med hverandre uten å gå via en router. Ref. til oppgave i) og j) i dette oppgavesett, der fant vi ut av ved hjelp av nettmaske at maskinene hadde mulighet å kommunisere direkte med hverandre og da også om de var i samme subnet.

3. ICMP

a) Hvem er det som bruker ICMP?

Host, router og gateway, ICMP er da altså en protokoll som håndterer feil-rapportering.

b) Hva er en host, router og en gateway?

Host: En pc eller maskin som er koblet opp til internett.

Router: Dette er en enhet/tjeneste som har som funksjon å route IP-pakker mellom nettverk.

Gateway: Dette er en router som gir tilgang for IP-pakker å komme inn/ut mellom det lokale nettverket og resterende internett.

c) Hvorfor utnytter `tracert`/`traceroute` ICMP protokollen?

For at da er det enkelt å se hvor i ruten dataen skal transporteres kan ha forsinkelser eller problem, hvilket gjør at det er enklere å feil-søke.

- d) Test å «pinge» vg.no, hvilken informasjon får du av det?

```
C:\Users>ping vg.no

Pinging vg.no [195.88.55.16] with 32 bytes of data:
Reply from 195.88.55.16: bytes=32 time=5ms TTL=250
Reply from 195.88.55.16: bytes=32 time=4ms TTL=250
Reply from 195.88.55.16: bytes=32 time=3ms TTL=250
Reply from 195.88.55.16: bytes=32 time=4ms TTL=250

Ping statistics for 195.88.55.16:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 5ms, Average = 4ms
```

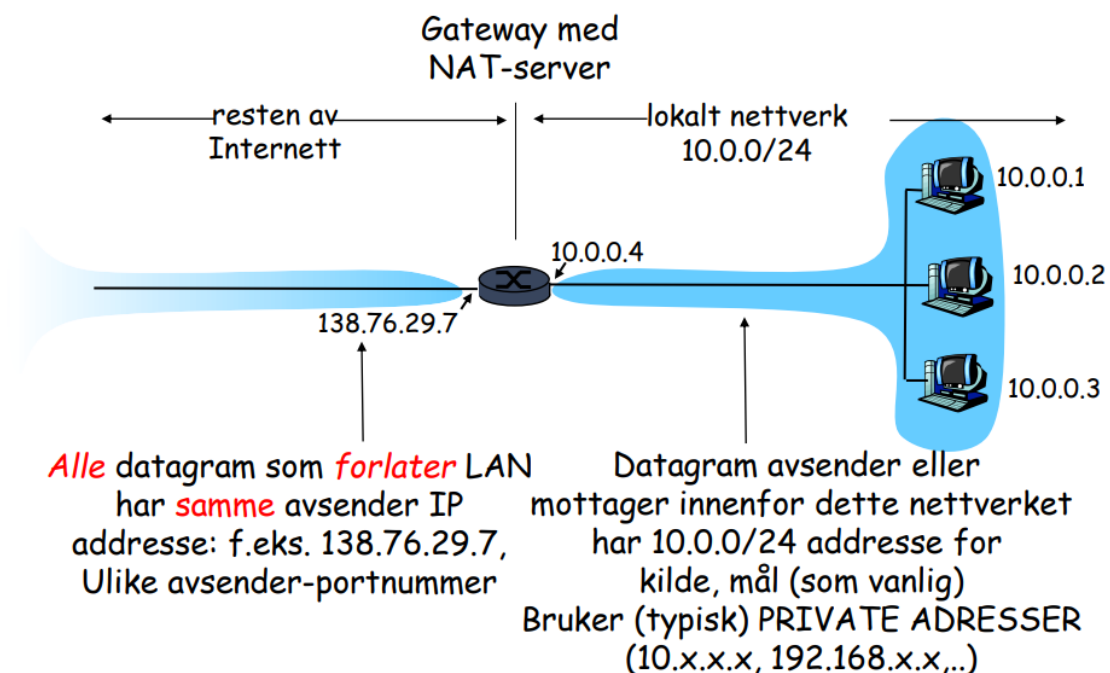
4. NAT

- a) Hva er problemet/problemene som NAT løser?

Imellom det store internettet og det lokale nettverket sitter det en gateway. Tenk på det som en dør inn til huset (området med datamaskiner på samme nettverk). Når en pakke blir sendt over internett, og til slutt kommer frem til mottakerens gateway, må vi vite hvilke av maskinene på det lokale nettet som er den *faktiske* mottakeren.

(Eks: *En* datamaskin har åpnet vg.no. Da ville det vært dumt om alle datamaskiner i samme hus fikk masse VG-reklamer helt plutselig.)

Dette er her NAT kommer inn i bildet. NAT serveren ligger i gateway-en, og ved hjelp av en tabell holder den styr på hva som er source- og destinasjonsadressene på internettsiden og LAN-siden. I den tabellen kan det for eksempel stå: «Mia sin pc gikk inn på vg.no, og venter nå på svar fra VG», men formulert med private ip-adresser.



- b) Hva er spesielt med 192.168.x.x og 10.x.x.x adresser?

Dette er starten på typiske private adresser, og disse brukes da i et lokalt nettverk. Med andre ord er det mest sannsynlig at din private adresse på nettverket du er koblet til nå starter på 192.168 eller 10, bruk ipconfig eller ifconfig i terminalen for å finne ut av dette.

- c) Sant/Usant: Du og din venn er koblet på samme LAN og sender datagram ut til internettet, dere har da ulike IP-adresser for å kunne identifiser seg.

Usant, hvis dere bruker samme gateway for å sende ut data, vil den gi dere samme IP-adresse. NAT finner ut av hvem av dere svar-pakkene skal til, så dere trenger ikke være skillbare på internettet.

- d) Forklar kort hva traversering-problemet med NAT betyr.

Traversering-problemet handler om at en avsender prøver å nå en mottaker inne på et lokalt nettverk, men har kun IP-adresse til den maskinen og vet da ikke at den skal gjennom NAT-en x.x.x.x, da det er IP-adressen til NAT-et som er synlig for avsenderen. Det finnes tre ulike løsninger til dette problemet, enten statisk konfigurering av NAT, bruk av UPnP og IGD, eller bruk av relaying.

5. IPv6

- a) Hva er de største forskjellene mellom IPv4 og IPv6?

IPv4	IPv6
32 bit Header inkluderer sjekksum Opsjoner i header opp til 40 bytes DNS A-records	128 bit Header inkluderer ikke sjekksum Utvidet header for opsjoner DNS AAAA-records

- b) Hvordan ser IPv6 notasjonen ut?

Notasjonen er på totalt 128 bit og er skrevet i heksadesimalt i 8 grupper på 2 byte/16 bit. Om det er kun 0 i en gruppe så kan hele adressen forkortes gjennom å skrive to kolon (::).

2001:0DB8:AC10:FE01:0000:0000:0000:0000

↓ ↓ ↓ ↓ ┌──────────┐
2001:0DB8:AC10:FE01:: Zeroes can be omitted

c) Forklar kort hva «Unicast», «Anycast» og «Multicast» er.

Unicast: Brukes for å nå en enkelt IPv6 adresse



Anycast: Brukes for å nå «hvem som helst», men sender til den første som tar imot



Multicast: Brukes for å sende til en gruppe, dette er IPv6 sin versjon av broadcast.



d) Hva er forskjellen på Dual stack og Tunneling, og hva brukes det til?

Det brukes for å IPv4 og IPv6 skal kunne samarbeide og det skal være mulig å bruke begge, ved Dual stack forstår routeren begge typer av adresser og oversetter, men ved Tunneling pakkes IPv6 adresser inn i IPv4 så at det er mulig å lese adressen.