Velkommen!

Uke 43: Hvordan fungerer ruteren din? Kryptering og sikkerhet

Gruppetime 10, 2. November

(Hanne-)Kristin Schrøder Leiros

hkleiros@uio.no

Plan for dagen

- Repetisjon av ukas pensum
  - Prøvde å gjøre den kort men veldig mye nytt og viktig
- Ukesoppgaver
- Tidligere eksamensoppgaver

Repetisjon av lagene i nettverk

5: Applikasjonslaget

4: Transportlaget

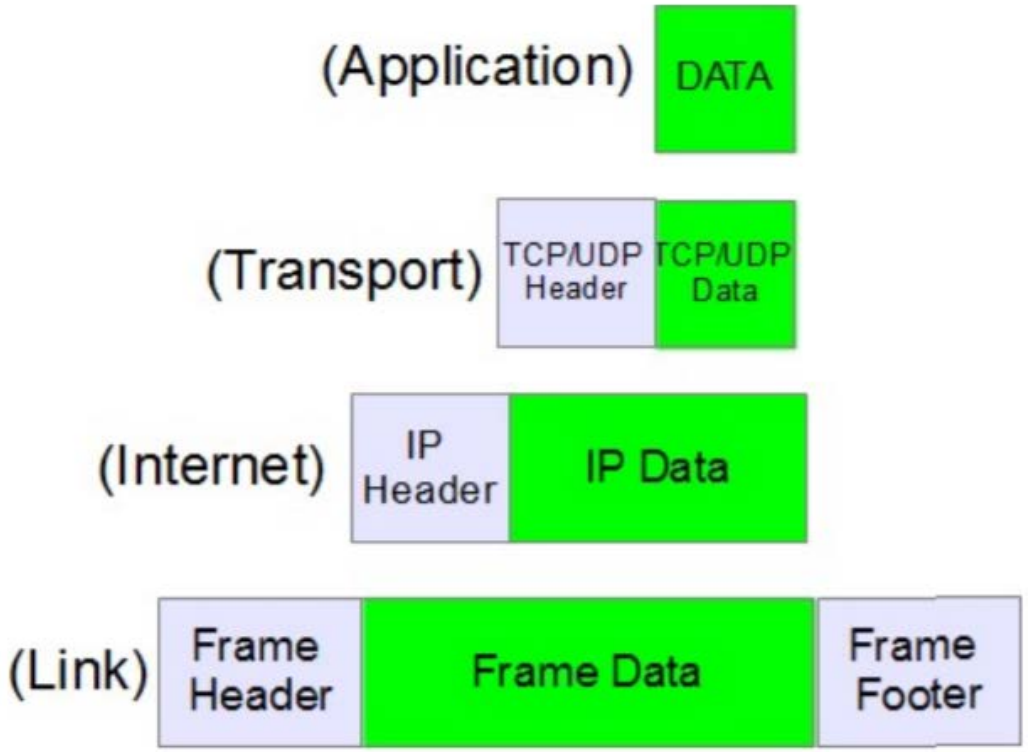
3: Nettverkslaget

2: Linklaget

1: Det fysiske laget

Lagene i Bruk

- Hva skjer med en melding i de forskjellige lagene når vi prøver å åpne en nettside?
- På Internett blir ofte nettverkslaget og transportlaget blandet
  - Transportprotokoll TPC og nettverksprotokoll IP



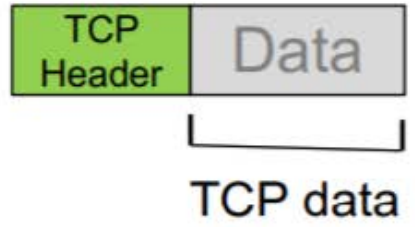
Data

Kan også inneholde en header, men det bestemmer applikasjonen

Lag 5 - Applikasjonslaget

- Lag med tjenester for applikasjoner:
- Eksempler:
  - Nettlesere (WWW)
  - E-post
  - Filoverføring
  - P2P

- *Mer om dette 2. november (Tjenester i Internett)!*



Lag 4 - Transportlaget

- TCP: HTTP, E-post, filoverføring, etc.
- UDP: Strømming av video og lyd

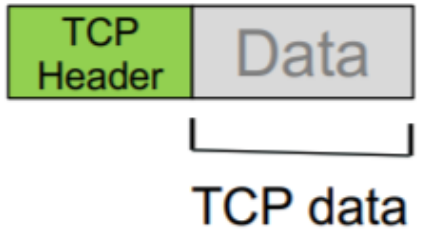
- Bruker «port» som en unik identifikator.
  - Representeres med et 16-bit heltall

TCP Segment Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Sequence Number			
64	Acknowledgment Number			
96	Data Offset	Res	Flags	Window Size
128	Header and Data Checksum		Urgent Pointer	
160...	Options			

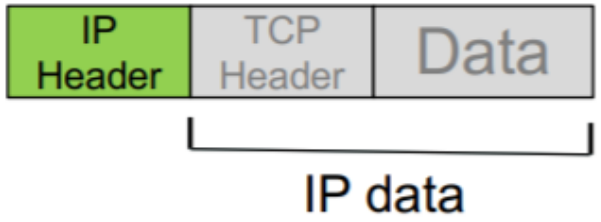
UDP Datagram Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Length		Header and Data Checksum	



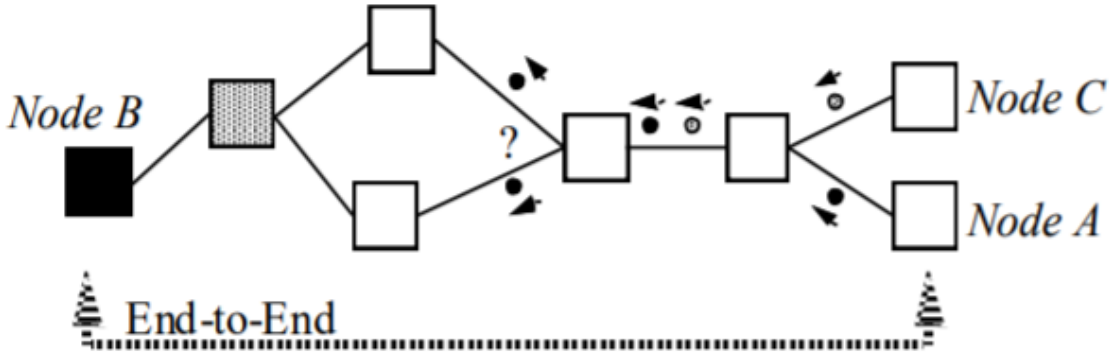
Lag 4 - Transportlaget

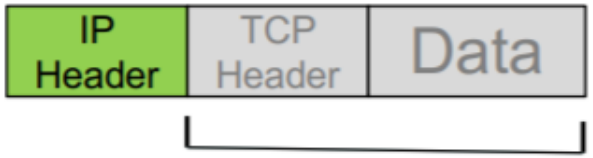
- **TCP:**
  - Oppsett av forbindelse (3-way handshake)
  - Garanterer at pakkene leveres i riktig rekkefølge
  - *Pålitelighet* – Pakker sendes på nytt hvis kvitteringen (ACK) ikke kommer frem
  - Flytkontroll og meningskontroll
- **UDP:**
  - Tilkoblingsløs forbindelse
  - Ingen garantier
  - «Best-effort» levering av data



Lag 3 - Nettverkslaget

- **Kobler sammen systemene ende-til-ende**
- **Ruting**
  - Statisk, definert under tilkobling eller dynamisk
  - Meningskontroll (for mange pakker på en sti)
  - Tjenestekvalitet (QoS)
- En «ruter» jobber på lag 3
- Eksempler:
  - IP (tilkoblingsløst)

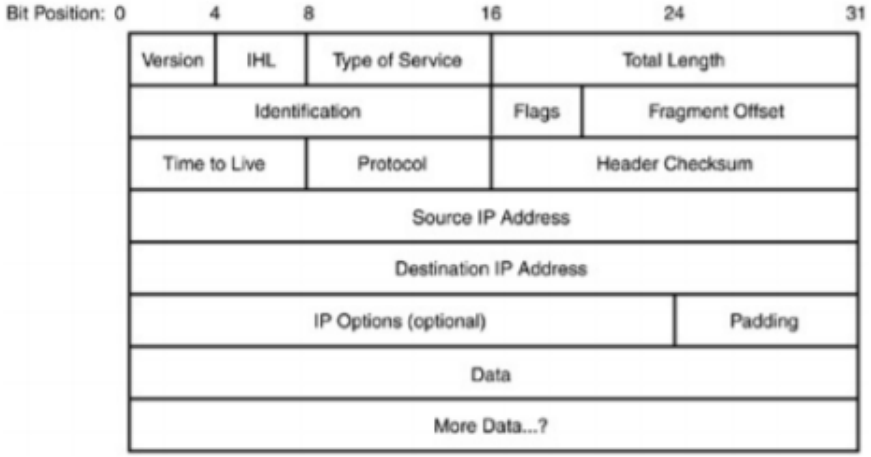


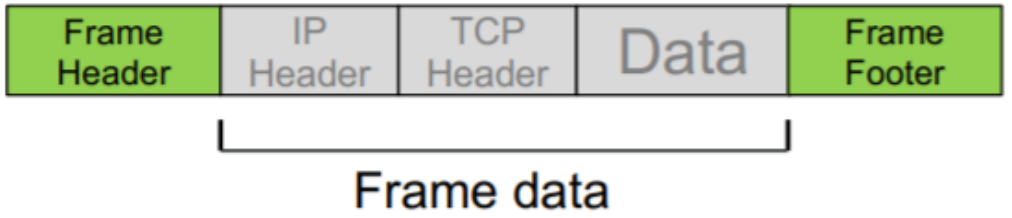


Lag 3 - Nettverkslaget

- Den mest brukte nettverkslagsprotokollen i dag er Internet Protocol (IP). Den mest brukte versjonen er IPv4.

- IPv4 bruker en 32-bit adresse, (4.3×10^9)
- Den nye versjonen, IPv6 har 128-bit adresser (3.4×10^{38})
  - Representeres med fire 8-bit heltall: 192.168.1.101

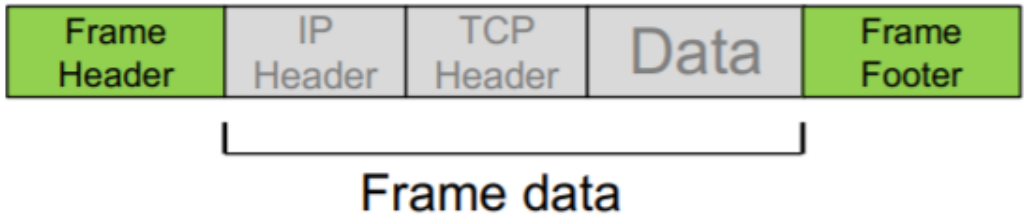




Lag 2 - Linklaget

- **Pålitelig overføring mellom to enheter.**
  - Pakker som overføres i linklaget kalles «frames»
  - Feildeteksjon or retting innenfor en «frame»
- En «switch» vil kun jobbe på lag 2
- Lag 2 vil kunne ha enkel flytkontroll
  - Rask sender, treg mottaker
- Medium Access Control (MAC)

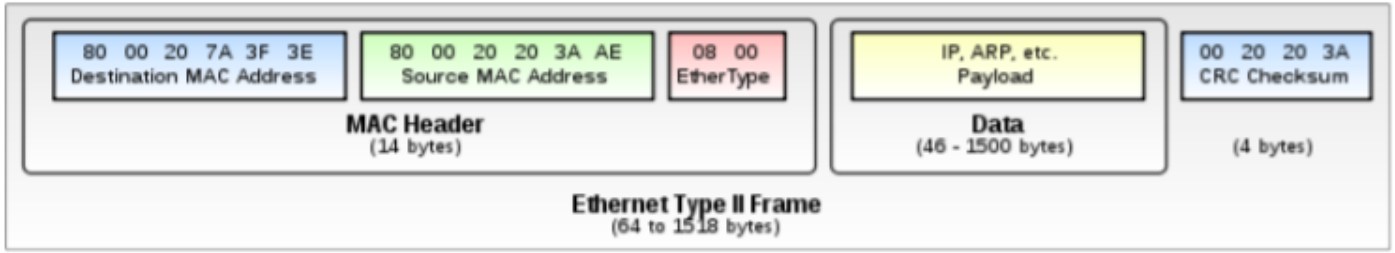




Lag 2 - Linklaget

- Det vanligste linklagene er ”Ethernet”, og ”WiFi”. Disse er ganske like, men har noen forskjeller.

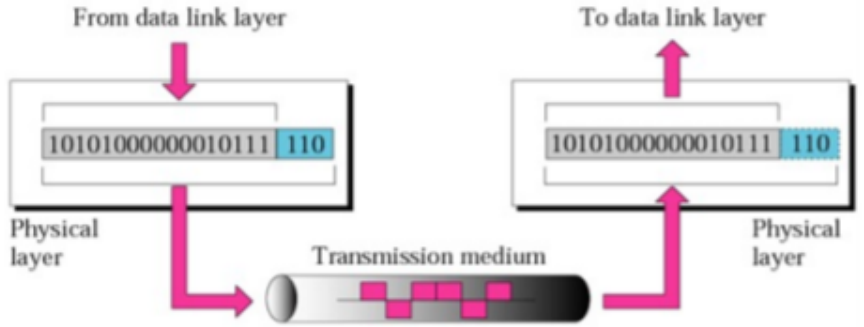
- Bruker en 6-byte adresse (48-bit) som ofte er lagret i nettverkskortet
  - MAC-adresse, brukes både på WiFi og Ethernet.
  - Hver *byte* representeres med en *heksadesimal* verdi: 07:01:02:01:2C:4B



Lag 1 – Det fysiske laget

- **Signalrepresentasjonen av bits:**
- Sørger for at 1-bit også blir mottatt som 1-bit (og ikke et 0-bit)
- Mekanikk: Koblingstype, kabler/medium,..
- Elektronikk: Spenning, bit-lengde,..
- Formelle regler for kommunikasjon:
  - Enveis (unidirectional) – half-duplex
  - Toveis (bidirectional) – full-duplex
  - *Hva skal markere starten og slutten på overføringer*

– Eksempler: RS-232-C, 1000BASE-X



Repetisjon:

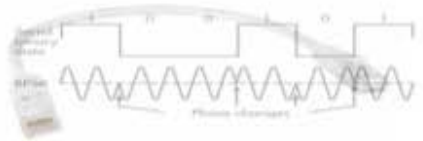
Lagene i Internett (TCP/IP referansemodellen)





Applikasjonslag	**http://www.uio.no**		Applikasjonslag
Transportlag	**192.168.1.5:80**		Transportlag
Nettverkslag	**192.168.1.5**	Nettverkslag	Nettverkslag
Linklag	**A1:B2:C3:D4:E5:F6**	Linklag	Linklag
Fysiske lag		Fysiske lag	Fysiske lag



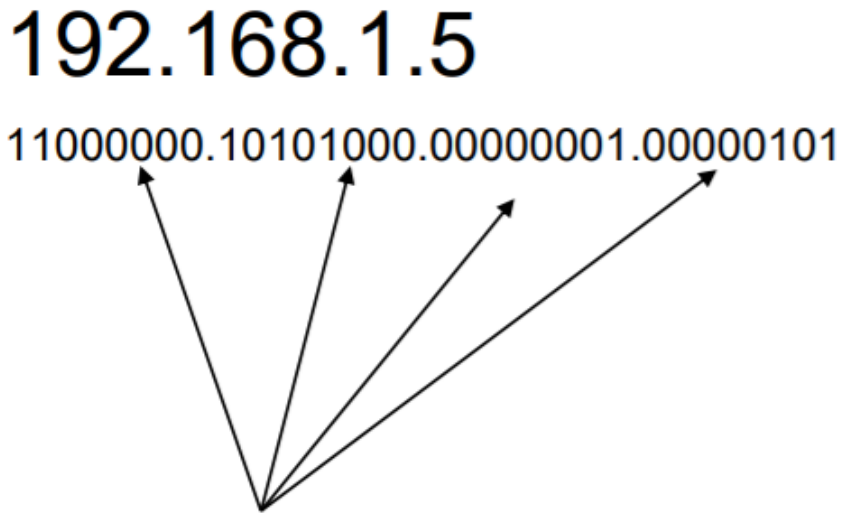




Fra: Hvordan fungerer en hjemmeruter?

Hva er en IP-adresse?

- En «unik» adresse på hele Internett
  - Postadresse-prinsipp
- Skiller bare mellom adresser innenfor og utenfor det lokale nettverket
- Om adressen er utenfor det lokale nettverket sendes pakken til ruteren som sender den vider på Internett
- Består av fire oktetter på 8 bit hver.



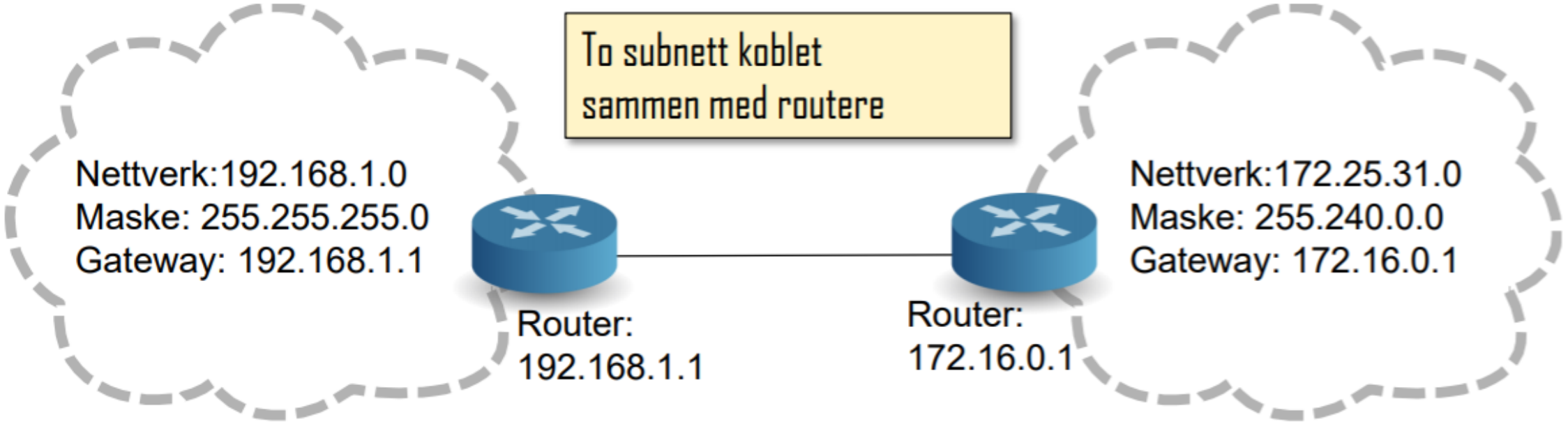
Oktetter:
Består av 8 bits hver. Maks verdi for hver oktett er 255

Lokalnettverk (LAN) og subnett

- Internett er et sammenkobling av mindre, separate nettverk.
- Koblet sammen med switch og/eller HUB (lag 2*)
  - Switch: filtrerer og videresender.
  - HUB: Videresender det som kommer inn på alle porter



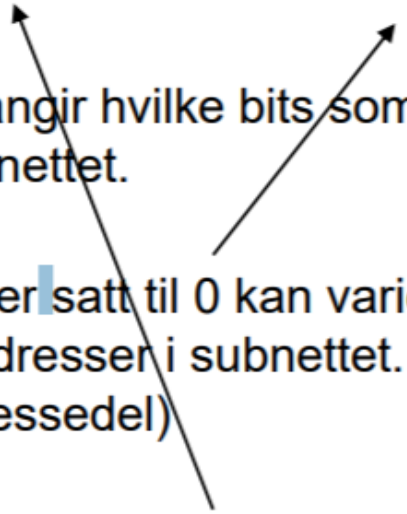
- For å sende en pakke til en maskin utenfor ditt lokale nettverk må den sendes til en router som vet hvor den skal videresendes.



Nettverksmaske

255.255.0.0

11111111.11111111.00000000.00000000



Masken angir hvilke bits som definerer dette subnettet.

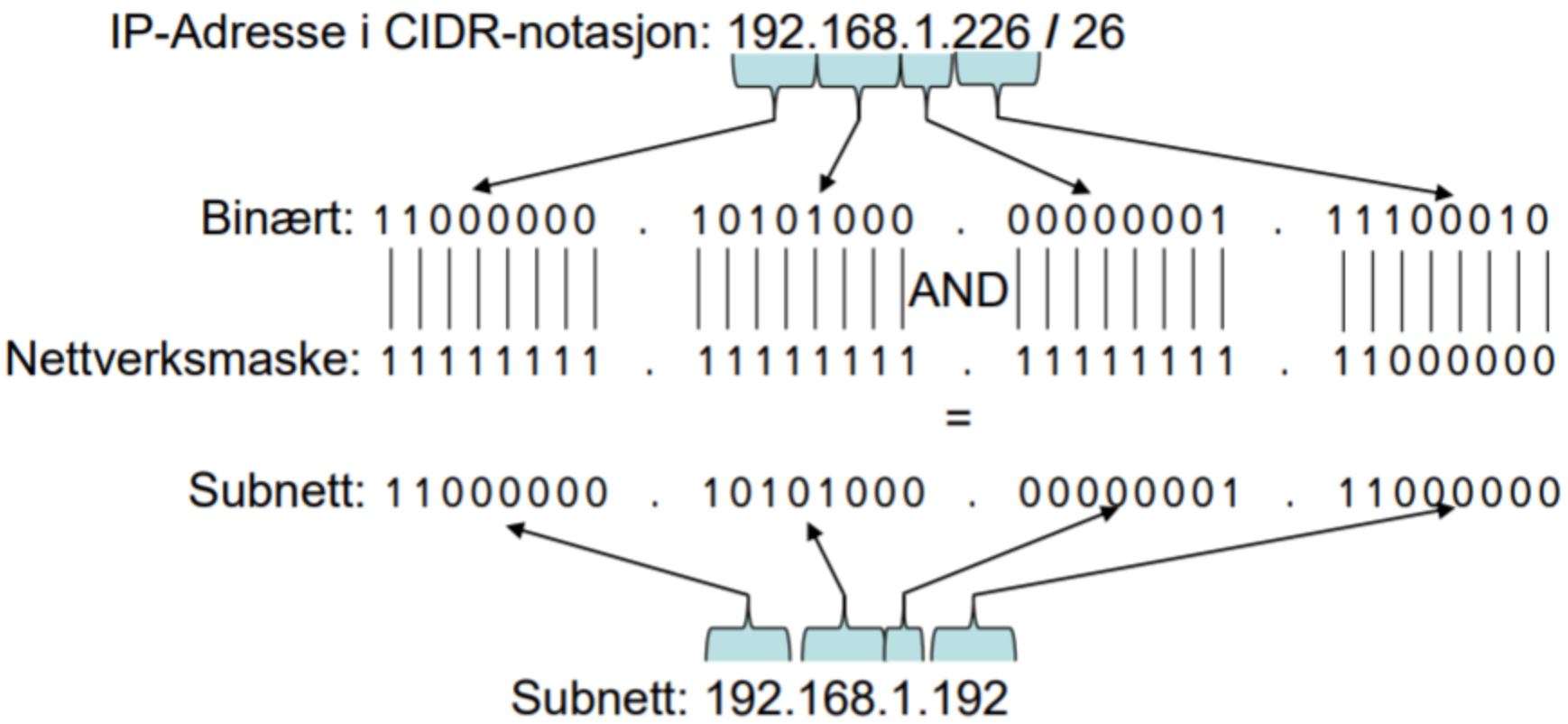
Bits som er satt til 0 kan varieres for å angi IP-adresser i subnettet. (vertsadressedel)

Bits som er satt til 1 angir delen av IP-adressen som definerer hvilket nettverk vertene tilhører.

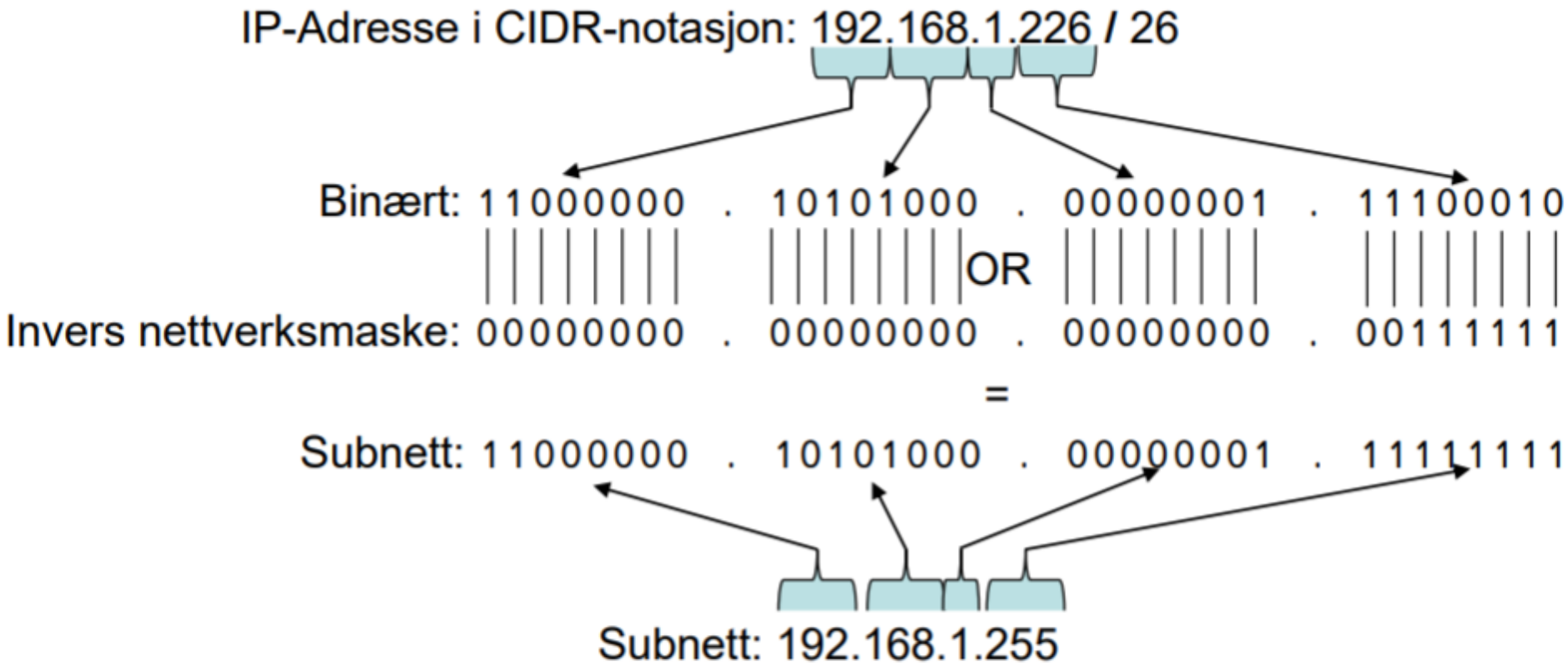
Kringkastingsadresse

- En reservert IP-adresse
- En melding som sendes ut på denne leveres til alle enheter på Local-Area Netowrk (LAN)
- IP: 255.255.255.255

Eksempel: subnettadresse fra IP / nettverksmaske



Eksempel: kringkastingsadresse fra IP / nettverksmaske



Hva er en IP-adresse?

ARP – koblingen mellom nettverk og IP

- Adress Resolution Protocol
- Nettverkskortene har en 6 byte lang MAC-adresse (media access control) som brukes til å identifisere maskinen innenfor et kringkastingsdomene
  - MAC skrives på heksadesimal med to og to symboler
    - Eks: AA:BB:CC:DD:EE:FF
- For at IP skal fungere, må avsenderen vite hvilken MAC-adresse pakken skal sendes til
- Samme teknikk som DHCP

Porter og NAT

- Porter skiller forskjellige tjenester på samme maskin fra hverandre
  - Skrives som et tall etter IP-adressen 192.168.1.5**:22**
- NAT: hack fordi vi har for få IP-adresser
- Låner port-abstraksjon på nettverkslaget for å gjøre opp for mangel på IP-adresser
  - Bryter lagdeling litt
- NAT er en av hovedoppgavene til hjemmeruteren
  - Lagres i en NAT-tabell
- Ruteren har en offentlig IP-adresse som vises på Internett (WAN)
  - og en privat IP-adresse som brukes innad i LAN
- NAT får altså alle enheter på samme LAN til å fremstå som én enhet på WAN

Private IP-adresser

RFC1918 name	IP address range	number of addresses	largest CIDR block (subnet mask)	host id size	mask bits
24-bit block	10.0.0.0 – 10.255.255.255	16,777,216	10.0.0.0/8 (255.0.0.0)	24 bits	8 bits
20-bit block	172.16.0.0 – 172.31.255.255	1,048,576	172.16.0.0/12 (255.240.0.0)	20 bits	12 bits
16-bit block	192.168.0.0 – 192.168.255.255	65,536	192.168.0.0/16 (255.255.0.0)	16 bits	16 bits

- Private IP-adresser er adresser som er reservert for bruk I lukkede nettverk og nettverk med NAT mot Internett
- Disse IPene skal ikke være direkte koblet mot Internett!
- En hjemmeruter er vanligvis satt opp til å gi deg et LAN med et subnett fra en av disse segmentene.

Fra Wikipedia: https://en.wikipedia.org/wiki/Private_network

Ulemper med NAT

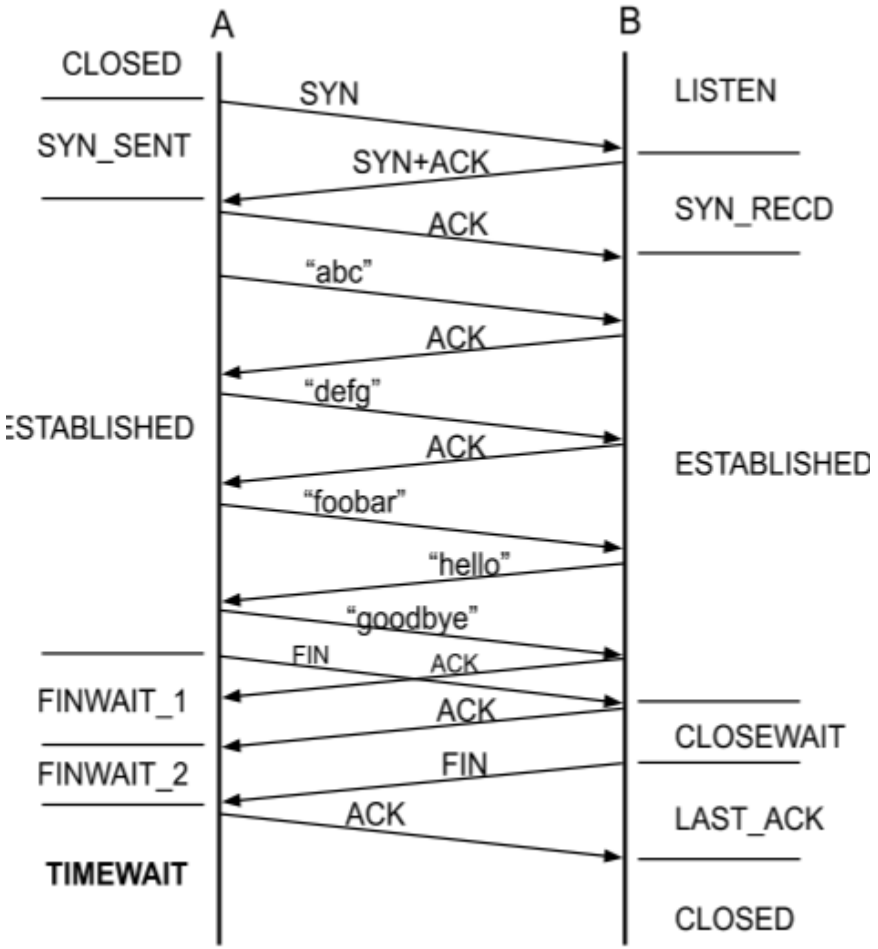
- Ekstra kompleksitet i nettverket
- Ruteren må bevare tilstanden til forbindelsene
- Nye forbindelser MÅ initieres fra innsiden av NAT-nettverket
- Gjør det vanskelig å koble til utenifra

Løsning: IPv6

- Lang prosess med å få i drift siden det må støttes i alle noder fra ende-til-ende
- 128-bits IP-adresse fremfor 32-bit i IPv4
- 2^{128} (eller $3.4 \times 10^{38)}$ mulige adresser

TCP – Transmission Control Protocol

- Vanligste protokollen på Transportlaget
- Forbindelsesorientert
  - Settes opp ved et 3-veis-håndtrykk
- Flytkontroll
  - Sender ikke informasjon fortere enn mottakeren kan ta imot
- ***Meningskontroll***
- Byte-strøm og levering i rekkefølge
- Pålitelighet
  - Implementert ved at bekreftelser på hver pakke sendes tilbake fra mottakeren
- Feilsjekking av nyttelasten (sjekksum)



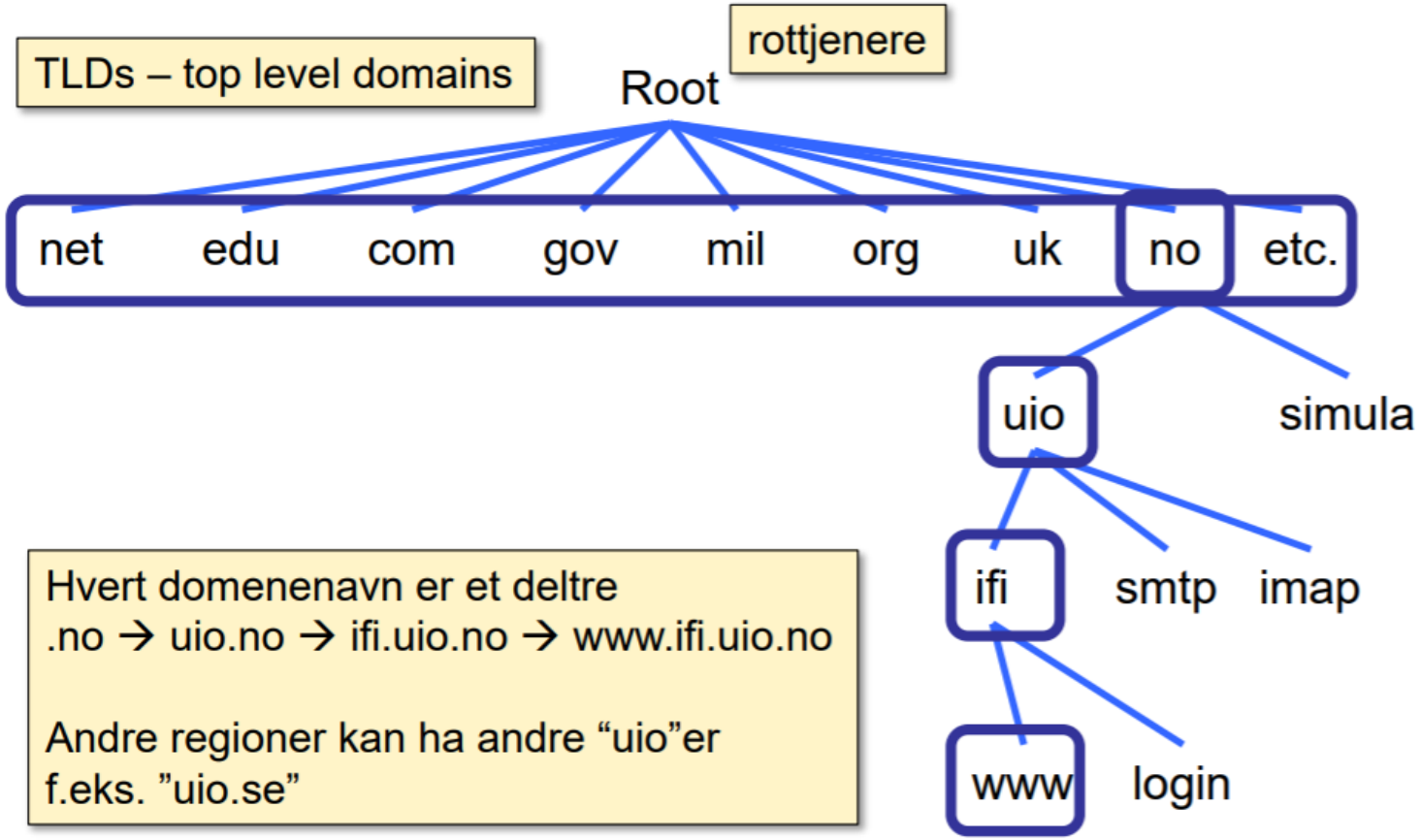
Metningskontroll

- Fordi en ruter i utgangspunktet bare er en kø vil for mye trafikk føre til stopp
- For å unngå dette har TCP mekanismer for å tilpasse senderaten til nettverksforholdene
- Meningskontroll sørger for at alle enheter på ruteren deler kapasiteten over flaskehalsen likt selv noen av dem i teorien har mer kapasitet enn andre.
- Ressursene deles teoretisk sett likt mellom forbindelser
  - Hvis noen trenger mer kapasitet: åpne flere forbindelser parallelt
  - Ingen god metode for å fordele ressurser i Internett rettverfir per maskin eller per bruker i dag

DNS – Domain Name System

- Hierarkisk navnetilordning av nettverksadresser (domener)
- Gjør at man slipper å huske alle IP-adresser man ønsker å koble seg til
- Enkel klient / tjener arkitektur
  - UDP eller TCP port 53 satt av til dette

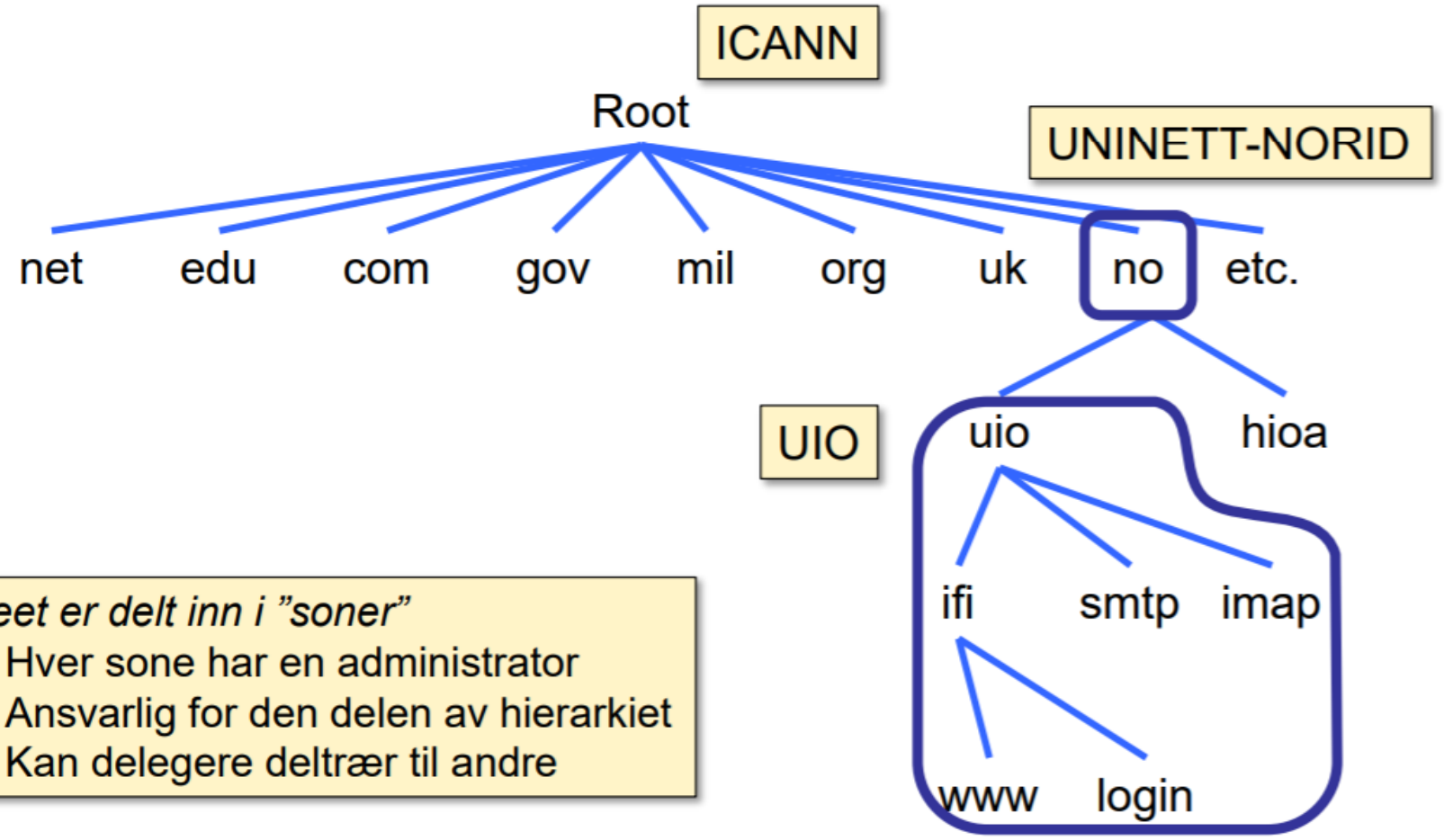
Navnehierarki:



Hvert domenenavn er et deltre
.no → uio.no → ifi.uio.no → www.ifi.uio.no

Andre regioner kan ha andre “uio”er
f.eks. ”uio.se”

Administrasjon av navnehierarkiet



Treet er delt inn i "soner"

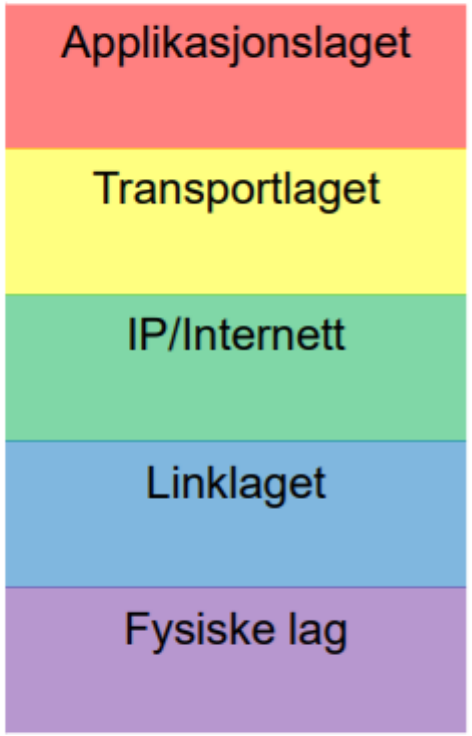
- Hver sone har en administrator
- Ansvarlig for den delen av hierarkiet
- Kan delegere deltrær til andre

Fra: En enkel introduksjon til kryptografi

Kryptografi

- Hva er det?
- Hvorfor trenger vi det?
- Hvordan «knekke» en kryptering
- Hemmelig nøkkel kryptering
- Offentlig nøkkel kryptering
- Hash-algoritmer

Kryptering / sikkerhet i lagene



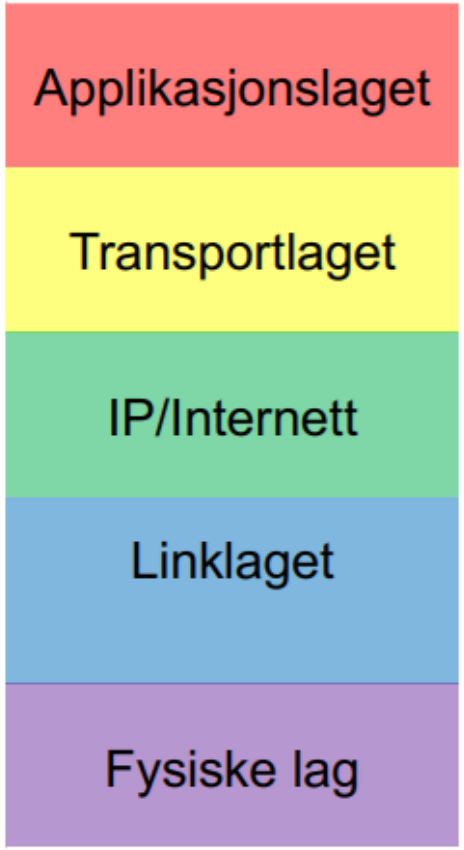
Secure Sockets Layer – kryptering for ende-til-ende
Applikasjoner – f.eks. nettbank eller butikker.

F.eks. *tcpcrypt*– har som mål at alle TCP-forbindelser som settes opp skal være kryptert

VPN (IPSEC etc.) – kobler to subnett sammen så det fungerer som ett LAN selv om de er fysisk adskilt

Kryptering på flere lag gjør det vanskeligere for uvedkomne å lytte til kommunikasjonen.
Adressen (avsender / mottakeren) er vanskelig å kryptere, da routere må vite hvor pakken skal leveres.

Kryptering og sikkerhet i nettverket



Secure Sockets Layer – (**https**) Kryptering for ende-til-ende Applikasjoner – f.eks. nettbank eller butikker.

VPN (IPSEC etc.) – Kobler to nettverk sammen så det fungerer som ett LAN selv om de er fysisk adskilt

WPA – WiFi Protected Access - Kryptering på trådløse nettverk, krypterer forbindelsen mellom deg og aksesspunkt/ruter.

Kryptering på flere lag gjør det vanskeligere for uvedkomne å lytte til kommunikasjonen. Adressen (avsender / mottakeren) er vanskelig å kryptere, da router må vite hvor pakken skal leveres.

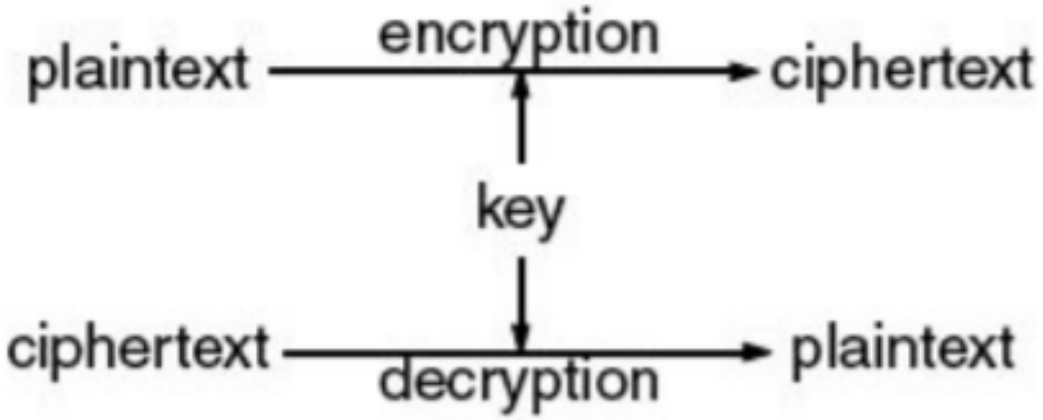
Definisjoner

- Beskjerder
  - Klartekst – plaintext
  - Kryptert tekst – ciphertext
- Algoritmer
- Nøkler
- Kryptograf
- Kroptoanalytiker



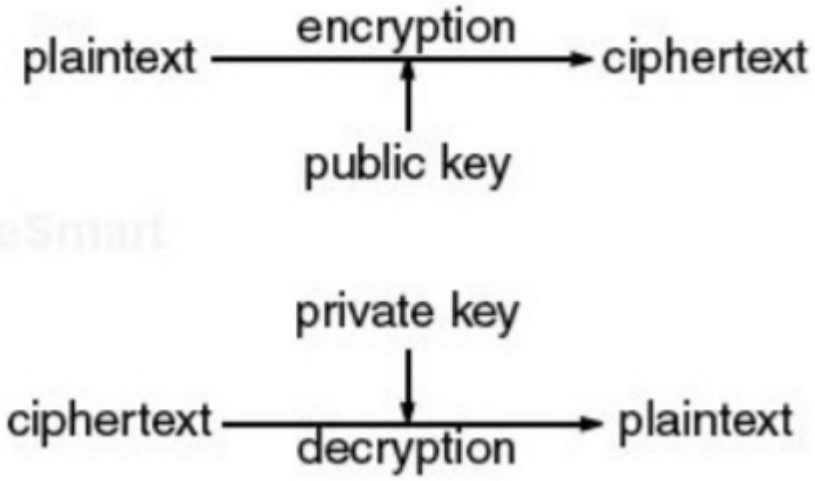
Symmetrisk kryptering

- Hemmelig nøkkelkryptering
- Nøkkelen må deles mellom sender og mottaker
- To typer:
  - Block cipher (DES, 3DES, AES)
  - Stream cipher (RC4)
- Block cipher merst brukt, gjene blokker på 128-bits
- Brukes for overførser over en usikker kanal
- Ofte brukers autentiseirng med asymmetrisk kryptering før man deler nøkler



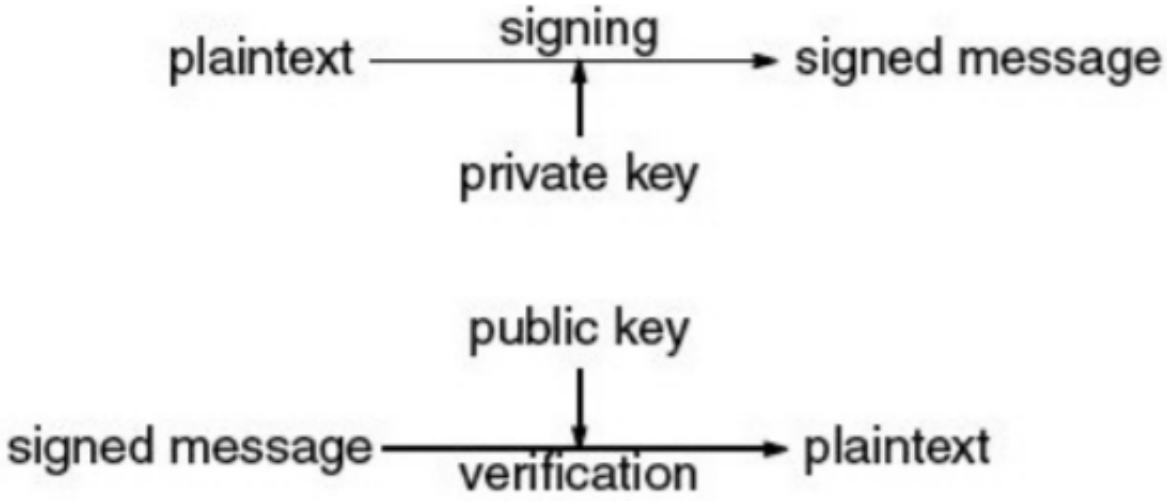
Asymmetrisk kryptering

- Offentlig nøkkelkryptering
  - En offentlig nøkkel som låser
  - En privat nøkkel som låser opp
- Utfordringer:
  - Effektivitet
    - Mange ganger tregere enn symmetrisk kryptering
- Løsning:
  - Offentlig nøkkel brukes for å bli enig om en midlertidig symmetrisk nøkkel som brukes for resten av kommunikasjonen



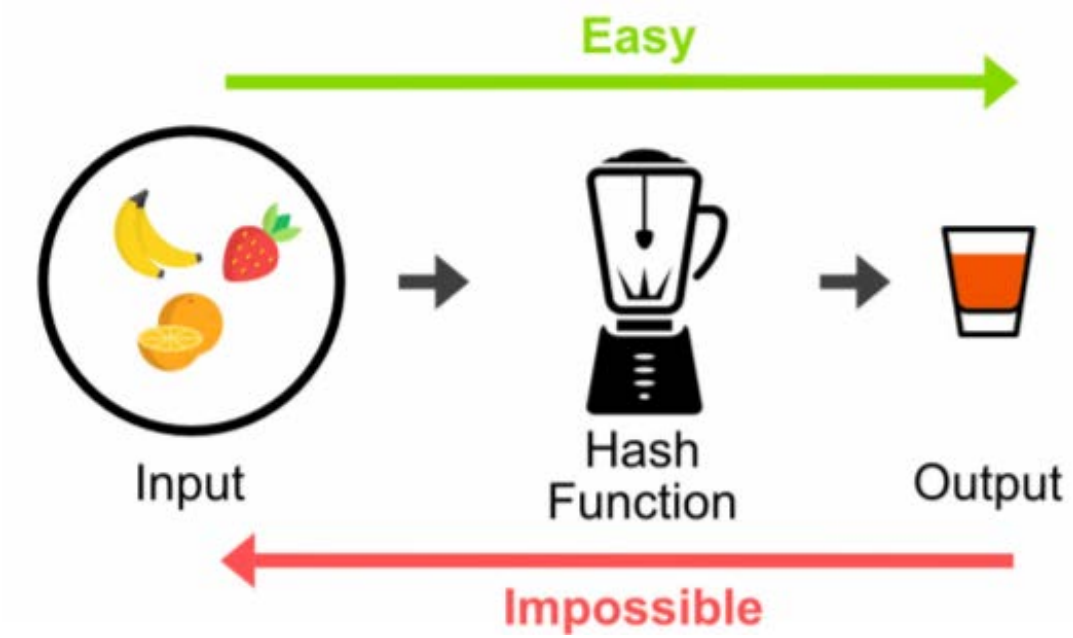
Digital signatur

- Signatur kan kun bli generert av eier ell noen som kjenner privat nøkkel
- Signatur kan bli veridisert av alle som h tilgang til offentlig nøkkel
- En korrekt verifisert signatur bekrefter avsenderens identitet, og at meldingen ble endret fra sending til mottak



Kryptografiske Hash-funksjoner

- Kryptografiske enveisfunksjoner
- Skramler en beskjed til nummer av gitt lengde
- Brukes for å sjekke dataintegritet
- Ikke reverserbar
- En sjekksumalgoritme må være:
  - Enkel å regne ut
  - Teoretisk umulig å reversere
  - Teoretisk umulig å endre beskjeden uten at sjekksummen blir endret
  - Teoretisk umulig å finne to forskjellige beskjeder med samme sjekksum



Ukesoppgaver

Eksamensoppgaver H2019