

INF105 - 17
kort om Layer 2, Hjemmeruter

David Grellscheid

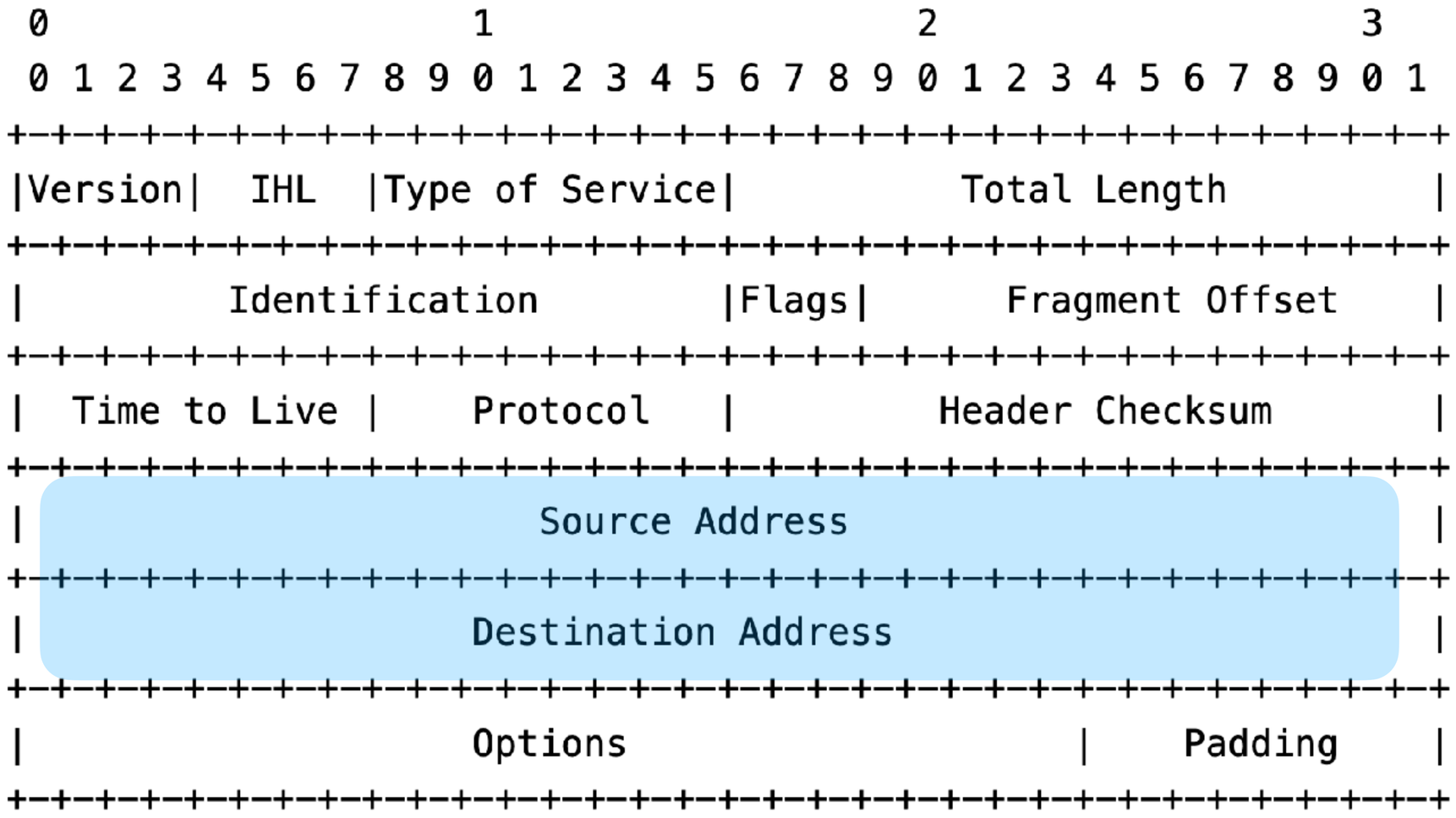
Quizene

- **Quiz 2 retake:** mandag 26.10. 16:15
- **Quiz 3:** i gruppetimen torsdag 22.10. og mandag 26.10.

5-layer model

- Application: HTTP, SMTP, FTP, SSH, DNS
- Transport: TCP / UDP
- **Network**: **IP** (ingen andre valg på Internet)
  sender "datagrams / packets"
  mellom end systems fra en router til den neste
- Link
- Physical

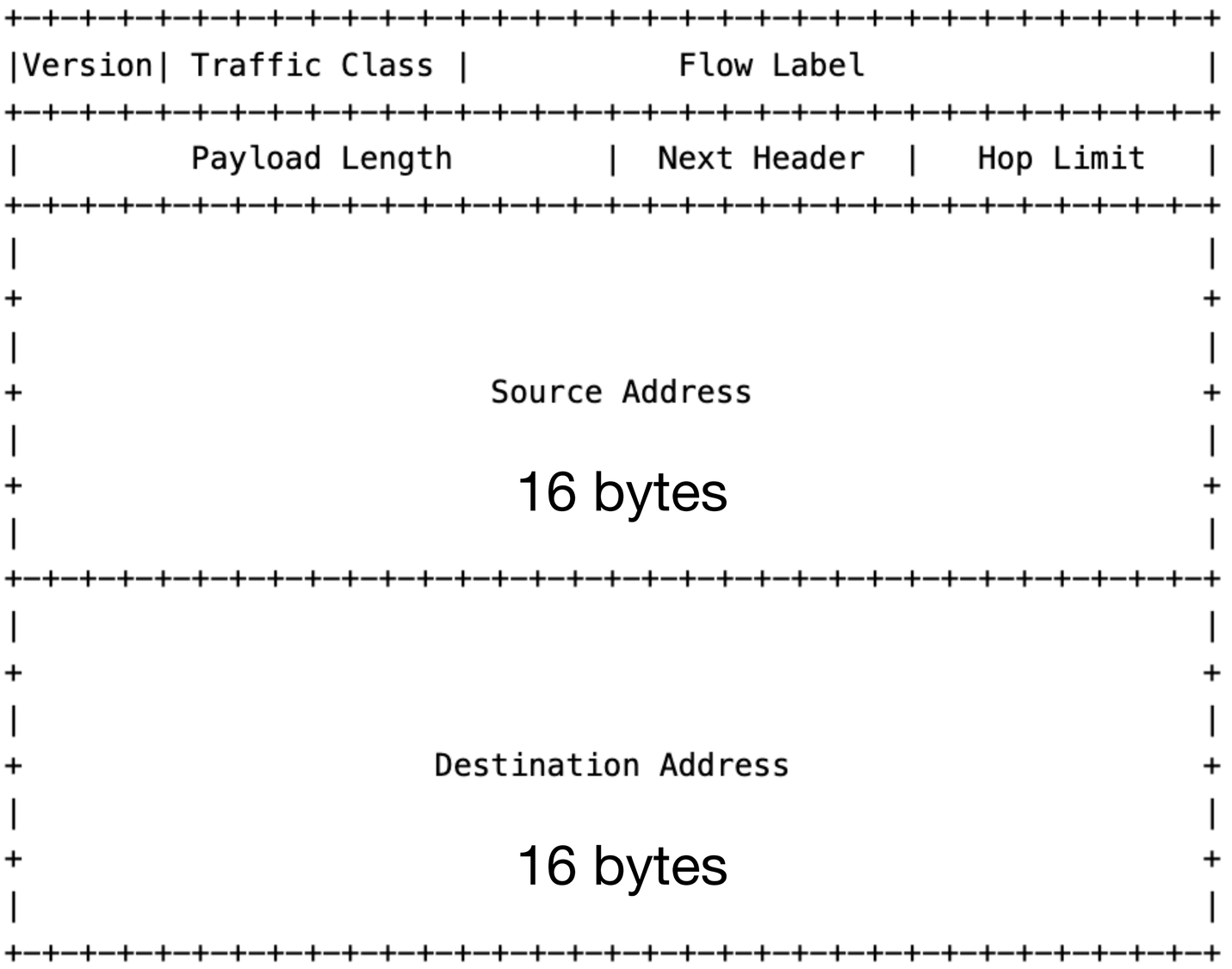
Layer 3 - IP



Example Internet Datagram Header

24 byte

IPv6-adresser



40 bytes

IPv6-adresser

- en adresse har 128 bit istedenfor 32 bit
- Vanlig skrivemåte i hex-base: 8 grupper med 2 byte (16 bit)

  0:0:..:0 kan avkortes med ::

  - 2001:700:2:8300::24b8
- ::1 - loopback (selve maskin)
- Private brukere burde få minst en /64 fra hjemme-ISP
  2001:db8:bacf:5010::/64
- 2^64 = 10^19 ledige adresser til hjemmenettverk

IPv6-adresser

- 2^64 = 10^19 ledige adresser til hjemmenettverk
- f.eks, hjemmenett er tildelt: **2001:db8:123:456**::/64
- klient-enheter kan velge siste 64bit fritt, f.eks basert på MAC-adresse (SLAAC) **2001:db8:123:456:**1140:bc72:6058:4674
- Servere som må ha en fast adresse kan få en statisk konfigurert **2001:db8:123:456**::f00
- en nettverkstilkobling kan ha mange IPv6-adresser
  (også mulig med IPv4, men ikke vanlig)

ICMP: meldinger om IP-layer

- ICMP er en enkel protokoll som sitter på toppen av IP-layer direkte
- brukes for meldinger om IP routing
  - ***ping***: echo request / echo reply
  - Destination network unreachable
  - Destination host unreachable
  - ...



brukes til feilsøking i layer 3

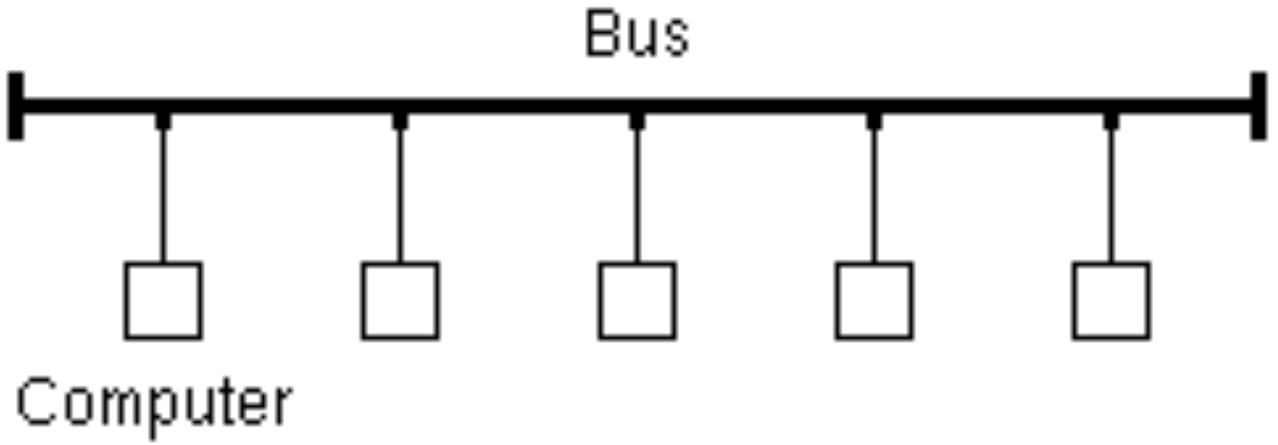
f.eks virker *ping -c3 1.1.1.1* ?

5-layer model

- Application: HTTP, SMTP, FTP, SSH, DNS
- Transport: TCP / UDP
- Network: IP
- **Link:** Ethernet, WiFi, PPP
  sender "frames" fra en enhet til den neste
- Physical

f.eks ethernet

første implementasjon: alle enhetene snakker over felles *bus*



Hver enhet har en **MAC-adresse** f.eks 00-00-5E-00-53-FF

alle enheter ser alle frames, aksepterer bare dem der MAC matcher

vanskelig med større nettverk, må kollisionssikre

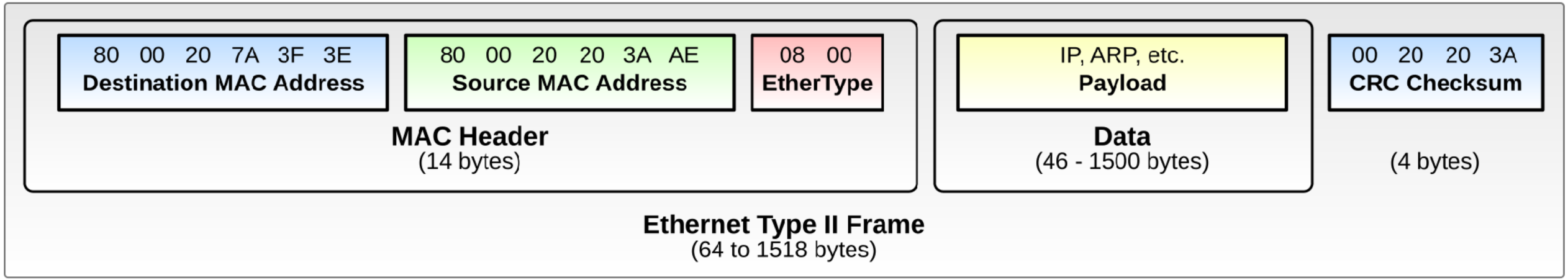
f.eks ethernet



wikipedia:Geek2003 CC-BY-SA

- collision-free kobling med **switches**
- switches husker hvem som er tilkoblet hvilken port,
  bare *broadcast* FF-FF-FF-FF-FF-FF blir sent til alle
- https://en.wikipedia.org/wiki/Network_switch

f.eks ethernet



https://en.wikipedia.org/wiki/Ethernet

Andre layer-2 eksempler:

- 802.11 Wifi: radiobølger på ulike frekvensbånd 2 GHz, 5 GHz, 6 GHz

  må løse f.eks kollisjonssikring, tilgangskontroll, kryptering

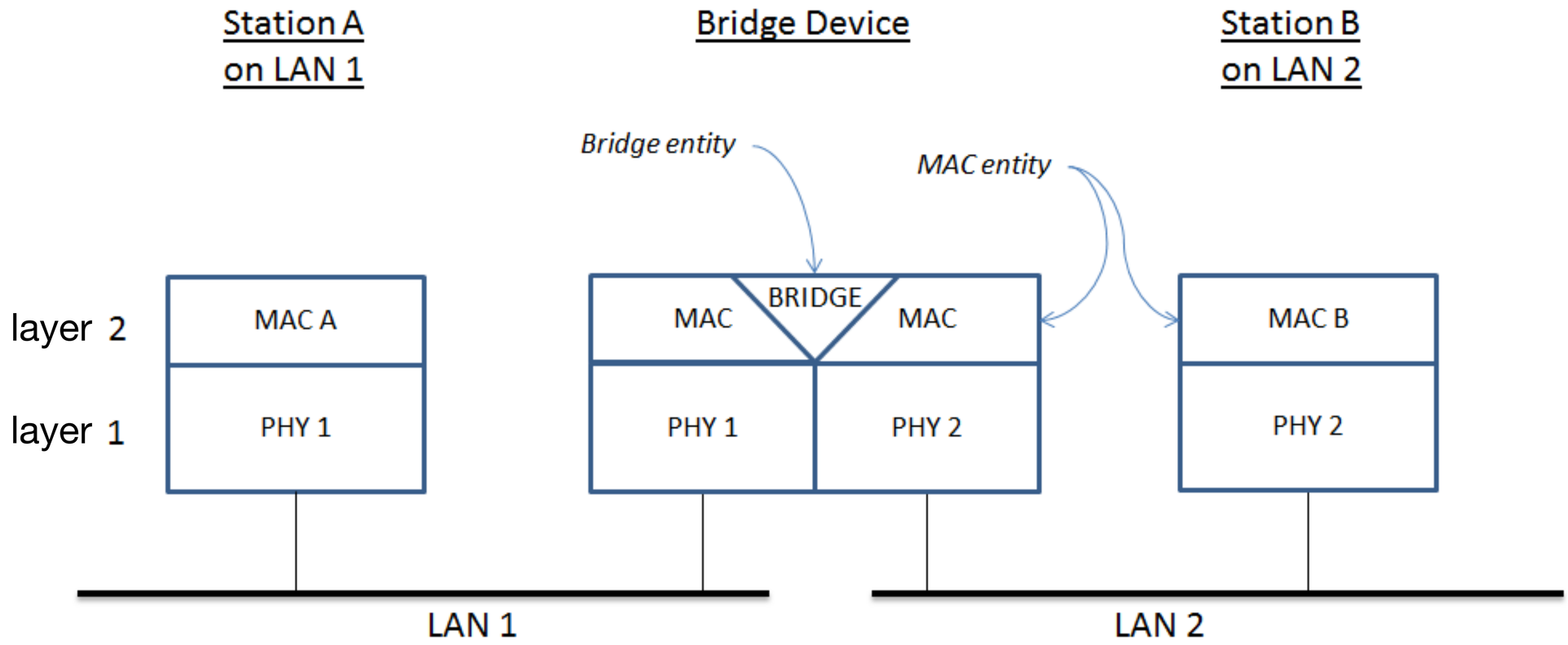
- PPP (brukt til dial-up modem, ADSL, network tunnels)
  https://en.wikipedia.org/wiki/Point-to-Point_Protocol

- mobile datanettverk 4G, 5G

  må løse f.eks lokalisering, handover

bridging

- bridges kan koble sammen to segmenter til ett nettverk

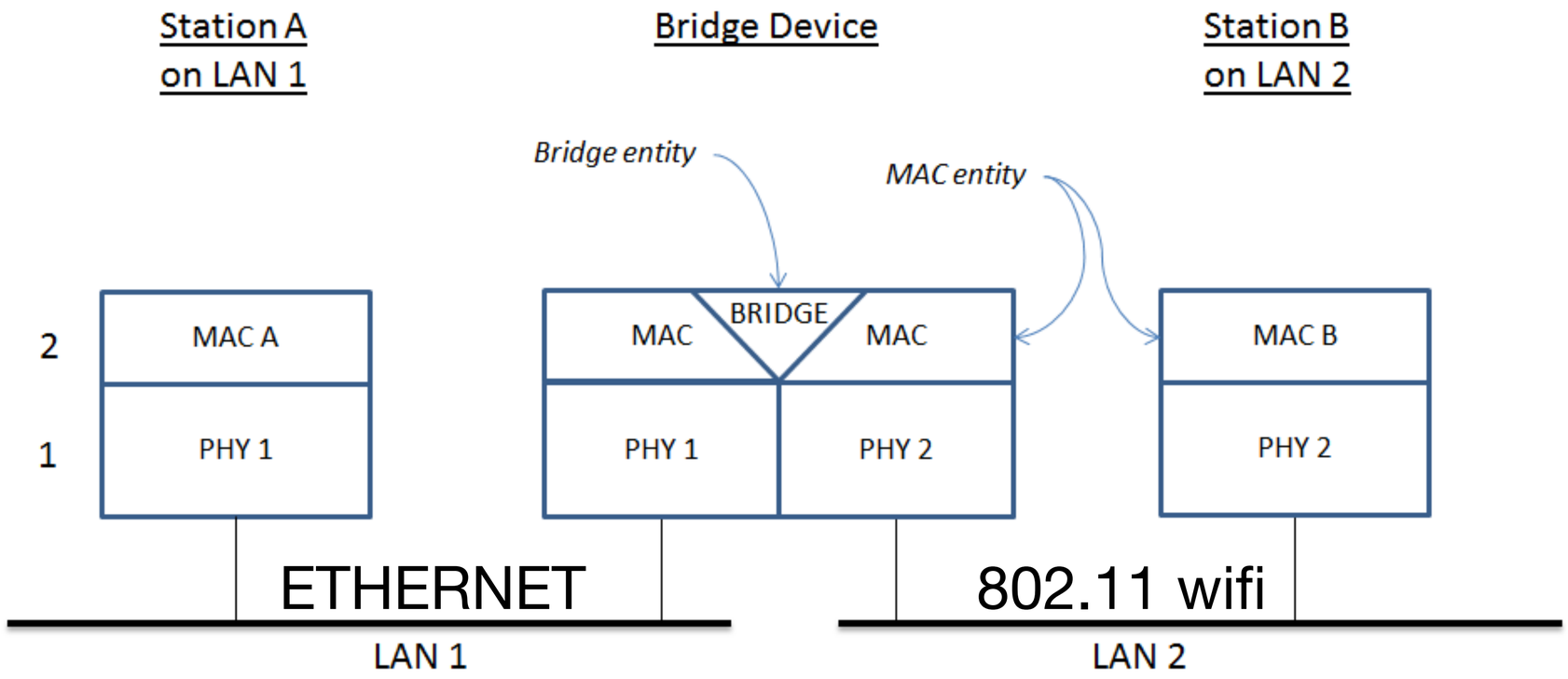


wikipedia:Crvincenzi CC-BY-SA

bridging

- WiFi access point er en bridge

  ethernet - wifi



wikipedia:Crvincenzi CC-BY-SA

VLAN

- utvidelse av Ethernet-protokollen som tillater uavhengige nettverk på samme kabler
- krever switches som støtter 802.1q



Hva gjør en hjemmesentral?

Hjemmesentral

- **Layer 1/2**
  - Bridge: fiber - ethernet på WAN-siden (wide area network)
    (kanskje en separat enhet)
- **Layer 2**
  - Switch: ethernet - ethernet på LAN-siden (local area network)
    oftest 4 ports
  - Wifi AP som er en bridge: wifi - ethernet (LAN-side)
- **Layer 5**
  - caching DNS server

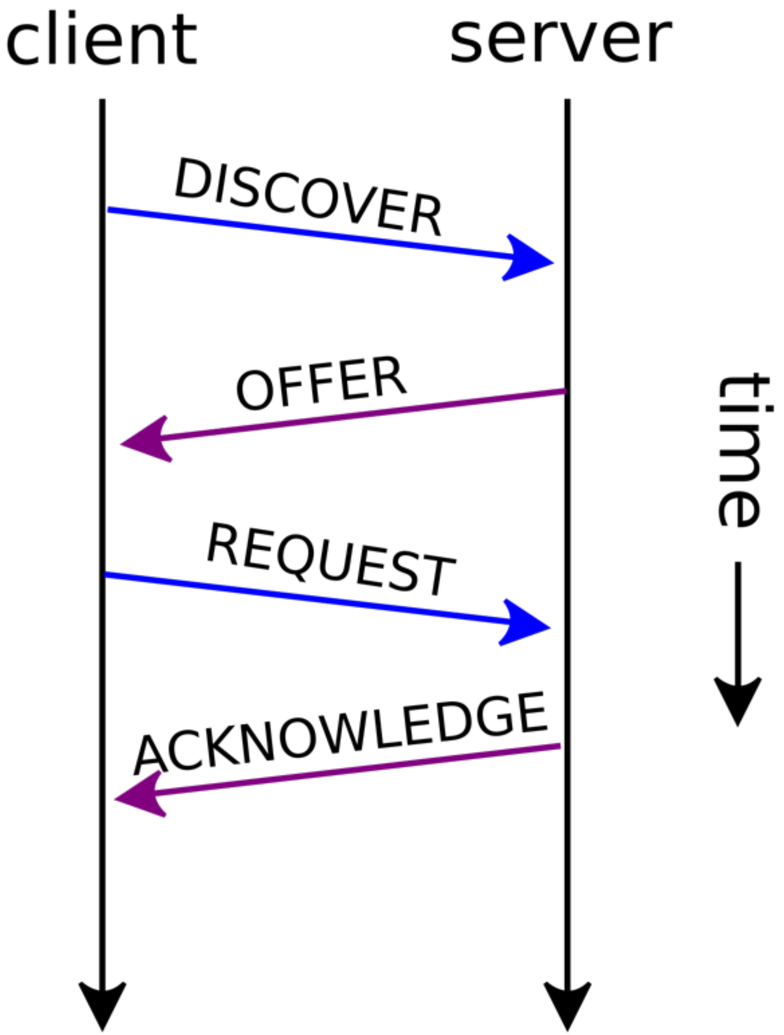
Hjemmesentral

- **Layer 2/3**
  - DHCP-server (tildeler IP adresser til LAN)
- **Layer 3**
  - IP router mellom LAN og WAN-nettverkene
  - NAT (network address translation)
  - brannmur (filtrere pakker på veien inn eller ut)

DHCP

DHCP - tildeling av IPv4-adresser

- Hver enhet setter sin egen IP-adresse, må konfigureres manuelt
- blir vanskelig med mange enheter
- DHCP automatiserer prosessen
- én enhet i det lokale nettverket matcher MAC-adresser til en liste med tilgjengelige IP-adresser. Lytter på UDP port 67, sender svar til UDP 68
- server må lyte på *broadcast* IP *255.255.255.255*



- OFFER inneholder IP adressen som skal brukes
- kan sende mer informasjon
  - adressen til extern ruter
  - adressen til DNS server
- server må lyte på *broadcast* IP *255.255.255.255*

wikipedia: Gelmo96 CC BY-SA 4.0

DHCP - tildeling av IPv4-adresser

- dynamic allocation:

  adresser blir tildelt i f.eks 24h, neste gang en ny adresse

  noen har cache slik at samme enhet får samme adresse neste gang

- static allocation:

  server har en liste av reserverte MAC-IP koblinger som skal deles ut fast

  nyttig til servere, som skal ha forutsigbar adresse

NAT

manglende IPv4 adresser

- ikke nok IPv4 til alle nettverk
- løsning: bruk en av de reserverte adressblokkene **internt** 192.168.0.0/16 eller 10.0.0.0/8 eller 172.16.0.0/12
- men: disse kan ikke routes på internett
- hvordan komme til en ekstern IP?

Network Address Translation

- Det er gateway router på LAN / WAN grensen som kjører NAT
- erstatter IP SRC adresse og port fra LAN med sin egen IP og port på WAN
- må holde en State- tabell:

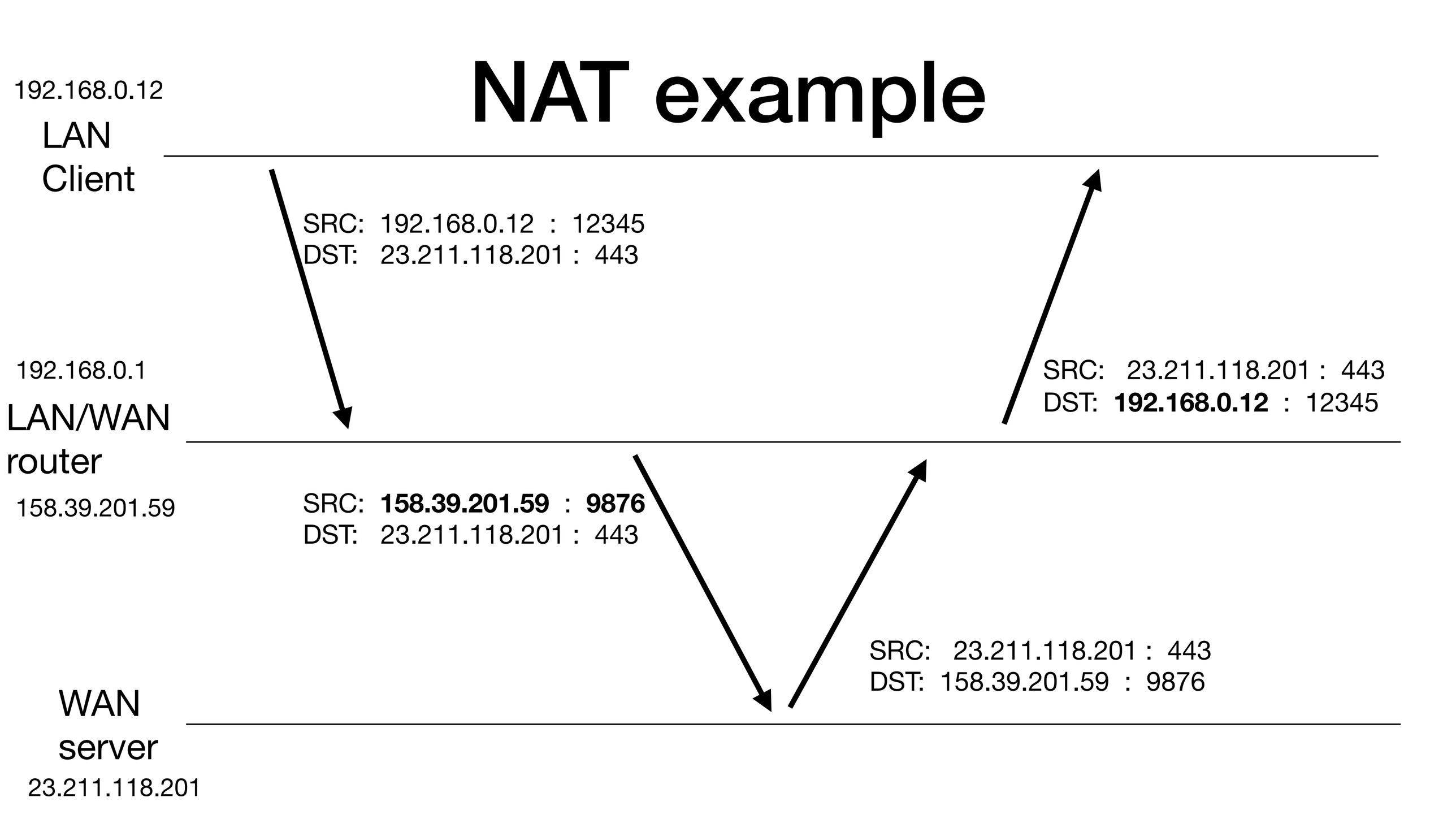
  SRC: 192.168.0.12 SRCPORT: 4567

  ble videresent som

  SRC: 158.39.201.59 SRCPORT: 6789

- Når et svar kommer med DST: 158.39.201.59 : 6789
  erstatter vi tilbake med: DST 192.168.0.12 : 4567

NAT example


192.168.0.12
LAN
Client
SRC: 192.168.0.12 : 12345
DST: 23.211.118.201 : 443
192.168.0.1
LAN/WAN
router
158.39.201.59
SRC: 158.39.201.59 : 9876
DST: 23.211.118.201 : 443
SRC: 23.211.118.201 : 443
DST: 158.39.201.59 : 9876
SRC: 23.211.118.201 : 443
DST: 192.168.0.12 : 12345
WAN
server
23.211.118.201

Network Address Translation

- NAT er greit for klienter som skal ut til offentlige servere
- hva med en server på intern nettverk?
- krever **port forwarding**
- **f.eks:**
  inngående forbindelser på router WAN port 80
  sendes videre til LAN maskin 192.168.12.12 port 80

(kan være ulike port)

Network Address Translation

- Hvis routeren selv ikke får en fast IP adresse er det vanskeligere å ha en server hjemme, må trikse f.eks med dynamisk oppdatert DNS
- Noen ISP nå går til Carrier grade NAT (CGNAT) der hjemmerouteren ikke får en offentlig IP lenger -> umulig å ha IPv4 server hjemme
- NAT bryter med end-to-end prinsippet, vanskelig for applikasjoner som trenger det. Videoconference, p2p med fast port på begge sider, tunnels
- layer-4 ports er ment til å identifisere prosesser, ikke maskiner
- løsning: god støtte til IPv6, faste /48 /60 /64 blokk til kunder

Brannmur / firewall

firewall

- Hovedbetydning: filtrere pakker basert på IP / TCP / UDP
- Kan kjøres på alle enheter som håndterer layers 2/3/4
  - vanligvis på end-systems og rutere
- Linux: netfilter / iptables / ufw
- BSD: pf / ...

firewall

- ser på IP og TCP/UDP headers
- avgjør om pakken skal blokkeres eller videresendes
- hovedkategorier:
  - INPUT: pakker adressert til denne maskinen
  - OUTPUT: pakker fra denne maskinen
  - FORWARD: pakker fra/til andre maskiner

Eksempler (pf syntax)

- block out proto tcp to 0.0.0.0/0
- block out proto tcp to 0.0.0.0/0 port 80
- pass in proto tcp from any to any port 22 # ssh tilgang
- block in all
  pass in proto tcp from 129.177.0.0/16 to any port 80
- pass in proto icmp all

firewall

- På sluttenhetene ofte:

  OUTPUT: allow

  INPUT: reject / drop

  FORWARD: reject / drop

- hvordan får svarene slippe in?

- stateful firewall: FW-systemet har en state table

  - når vi så en TCP SYN til a.b.c.d port 80 skal vi akseptere TCP ACK osv. fra a.b.c.d port 80 frem til vi ser FIN handshake (eller timeout etter en stund)

firewall

- mye mer kontroll:
  OUTPUT block, og legge inn eksplisitte regler hva som kan kontaktes
- upraktisk på vanlig brukt PC, siden så mange ulike tjenester skal kontaktes
- kan oppdage uønsket aktivitet på egen maskin

firewall

- Når du leker med en firewall på en ekstern maskin:

  pass på at du holder port 22 (SSH) åpent eksplisitt!

  med mindre du har en annen tilgang kan du låse deg ut!

Hjemmelekser

- se på router-konfigurasjon
- hvilke elementer kjenner du igjen?
- hvordan kommer du tilbake til en fungerende config?
- hvordan kobler du til uten wifi?
- hva kan du endre på?

  om du har andre som bruker nettet, spør først! :-)