

INF105 - 19
VPN / CGI

David Grellscheid

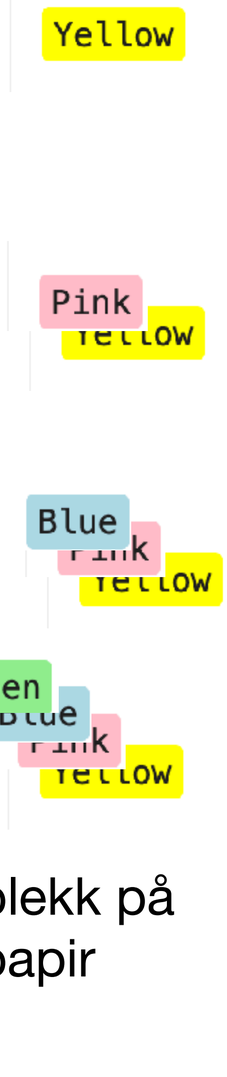
Milestone 1

- Fortsatt ikke løst problemet med fellesvurderinger
- Skal sende et spørreskjema på mitt.uib for å kartlegge

Sluttprosjekt

- En nettside med dynamisk generert innhold + database
- Grupper av 3, kan velge selv, eller bli tildelt om du ønsker
- Milestone 2 handler om planen
- Sluttpresentasjon = Milestone 3 i første uke desember
- Mer detalj kommer snart på mitt.uib

Layer	Colour	Protocol Data Units
5 Application	Yellow	Content / data
4 Transport	Pink	Segment / datagram
3 Network	Blue	IP packet
2 Data link	Green	Frame
1 Physical	-	Raw bits (0101)



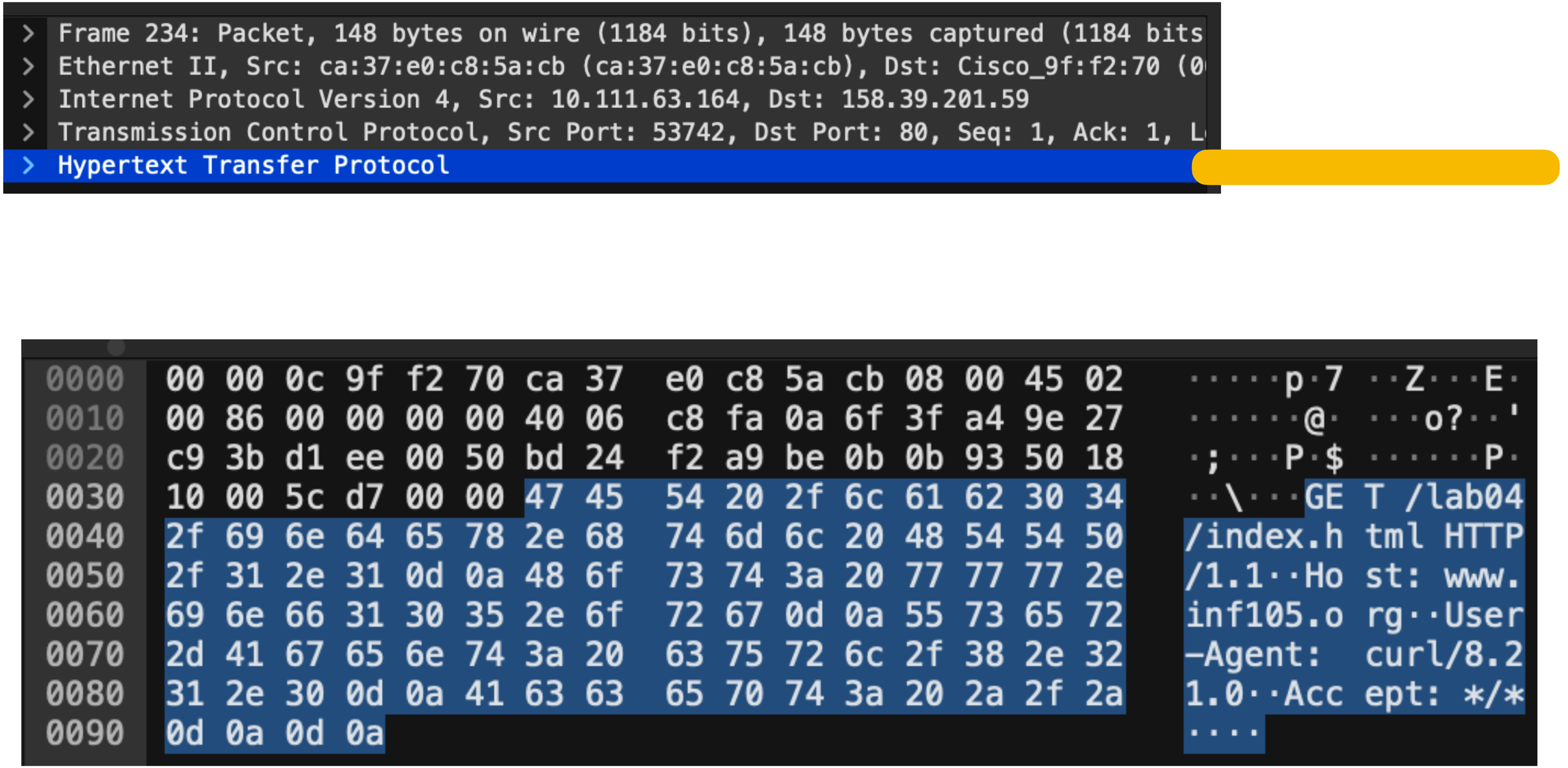
blekk på papir

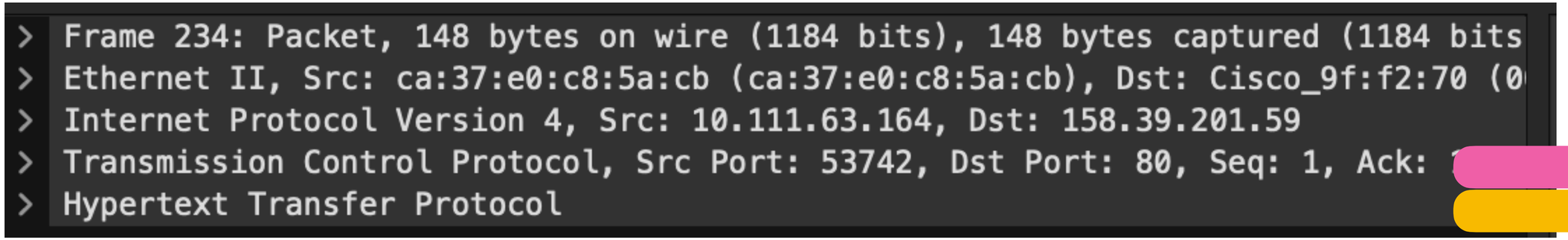
Gruppetimen

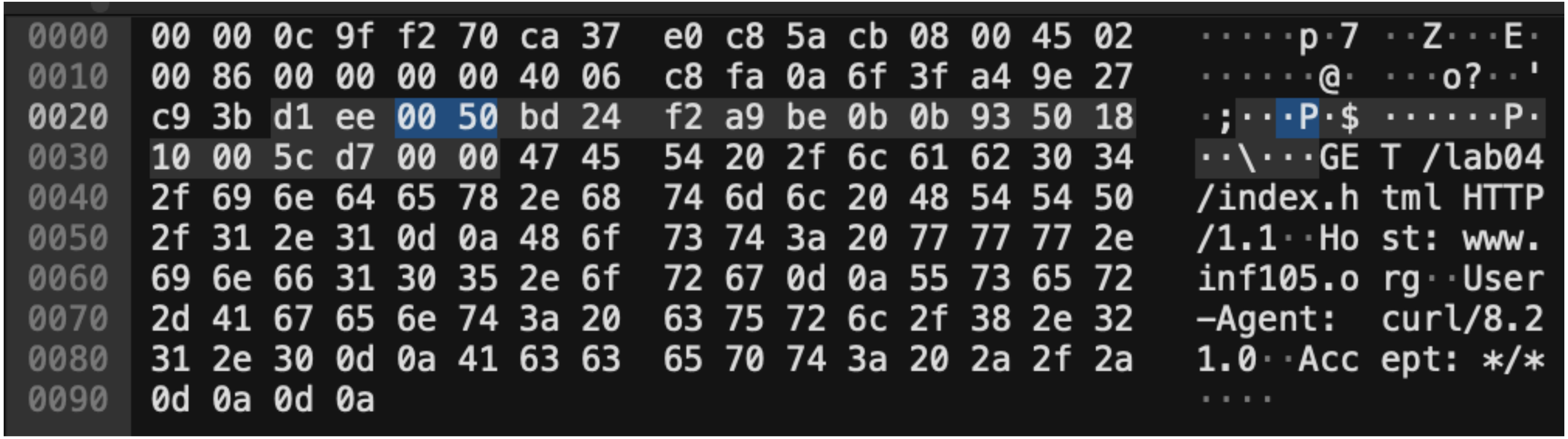
hvis IP ikke er lokal, gi til ruter

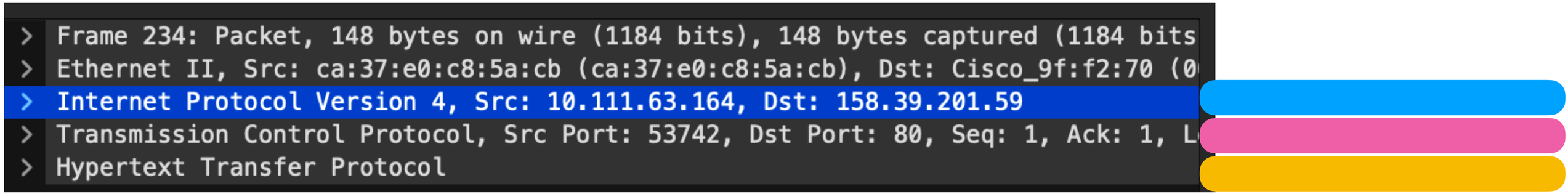
Ethernet MAC-adresse:
alle lokale enhetene er tilgjengelig

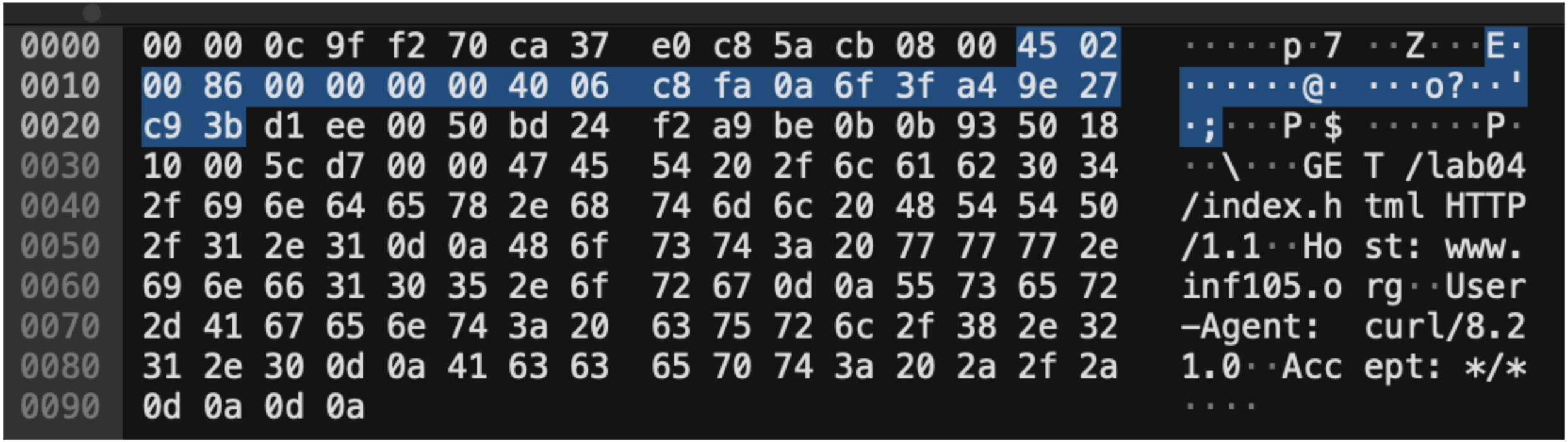
hver enhet lager en
lokal IP-MAC liste ved bruk av ARP

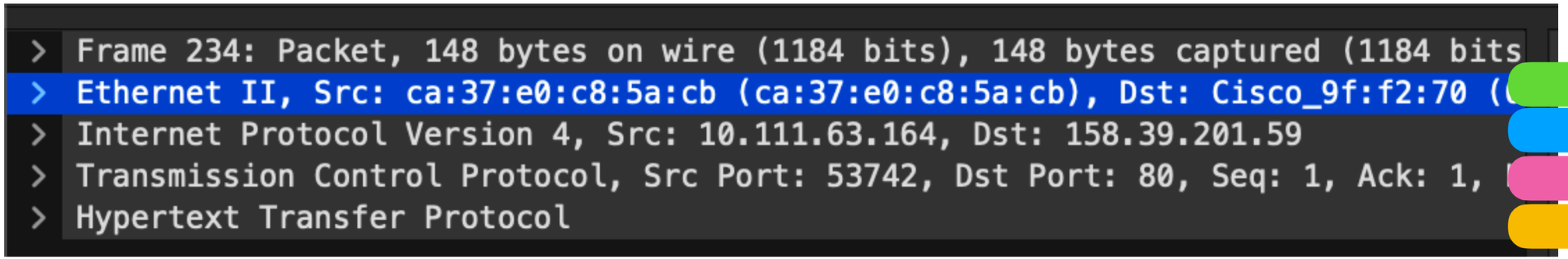

> Frame 234: Packet, 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits
> Ethernet II, Src: ca:37:e0:c8:5a:cb (ca:37:e0:c8:5a:cb), Dst: Cisco_9f:f2:70 (0
> Internet Protocol Version 4, Src: 10.111.63.164, Dst: 158.39.201.59
> Transmission Control Protocol, Src Port: 53742, Dst Port: 80, Seq: 1, Ack: 1, L
> Hypertext Transfer Protocol
0000 00 00 0c 9f f2 70 ca 37 e0 c8 5a cb 08 00 45 02 ·····p·7 ··Z···E·
0010 00 86 00 00 00 00 40 06 c8 fa 0a 6f 3f a4 9e 27 ·····@· ···o?··'
0020 c9 3b d1 ee 00 50 bd 24 f2 a9 be 0b 0b 93 50 18 ·;···P·$ ·····P·
0030 10 00 5c d7 00 00 47 45 54 20 2f 6c 61 62 30 34 ··\···GE T /lab04
0040 2f 69 6e 64 65 78 2e 68 74 6d 6c 20 48 54 54 50 /index.h tml HTTP
0050 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1··Ho st: www.
0060 69 6e 66 31 30 35 2e 6f 72 67 0d 0a 55 73 65 72 inf105.o rg··User
0070 2d 41 67 65 6e 74 3a 20 63 75 72 6c 2f 38 2e 32 -Agent: curl/8.2
0080 31 2e 30 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 1.0··Acc ept: */*
0090 0d 0a 0d 0a ····

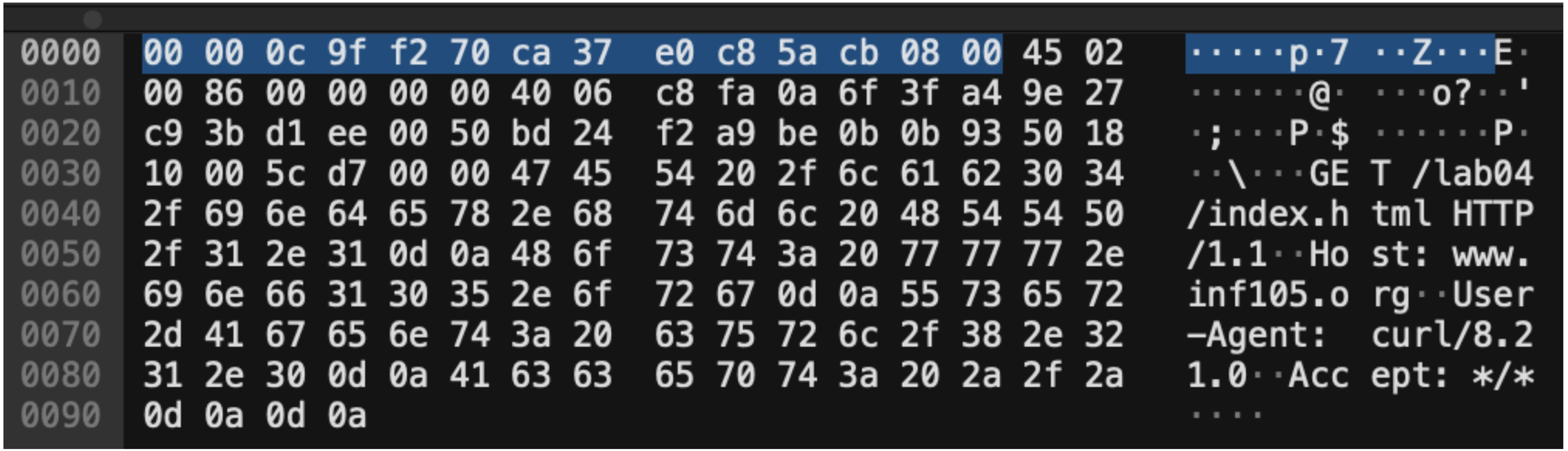

> Frame 234: Packet, 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits
> Ethernet II, Src: ca:37:e0:c8:5a:cb (ca:37:e0:c8:5a:cb), Dst: Cisco_9f:f2:70 (0
> Internet Protocol Version 4, Src: 10.111.63.164, Dst: 158.39.201.59
> Transmission Control Protocol, Src Port: 53742, Dst Port: 80, Seq: 1, Ack:
> Hypertext Transfer Protocol


0000 00 00 0c 9f f2 70 ca 37 e0 c8 5a cb 08 00 45 02 ·····p·7 ··Z···E·
0010 00 86 00 00 00 00 40 06 c8 fa 0a 6f 3f a4 9e 27 ·····@· ···o?··'
0020 c9 3b d1 ee 00 50 bd 24 f2 a9 be 0b 0b 93 50 18 ·;···P·$ ·····P·
0030 10 00 5c d7 00 00 47 45 54 20 2f 6c 61 62 30 34 ··\···GE T /lab04
0040 2f 69 6e 64 65 78 2e 68 74 6d 6c 20 48 54 54 50 /index.h tml HTTP
0050 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1··Ho st: www.
0060 69 6e 66 31 30 35 2e 6f 72 67 0d 0a 55 73 65 72 inf105.o rg··User
0070 2d 41 67 65 6e 74 3a 20 63 75 72 6c 2f 38 2e 32 -Agent: curl/8.2
0080 31 2e 30 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 1.0··Acc ept: */*
0090 0d 0a 0d 0a ····


Frame 234: Packet, 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits
Ethernet II, Src: ca:37:e0:c8:5a:cb (ca:37:e0:c8:5a:cb), Dst: Cisco_9f:f2:70 (0
Internet Protocol Version 4, Src: 10.111.63.164, Dst: 158.39.201.59
Transmission Control Protocol, Src Port: 53742, Dst Port: 80, Seq: 1, Ack: 1, L
Hypertext Transfer Protocol


0000 00 00 0c 9f f2 70 ca 37 e0 c8 5a cb 08 00 45 02 ·····p·7 ··Z···E·
0010 00 86 00 00 00 00 40 06 c8 fa 0a 6f 3f a4 9e 27 ·····@· ···o?··'
0020 c9 3b d1 ee 00 50 bd 24 f2 a9 be 0b 0b 93 50 18 ·;···P·$ ·····P·
0030 10 00 5c d7 00 00 47 45 54 20 2f 6c 61 62 30 34 ··\···GE T /lab04
0040 2f 69 6e 64 65 78 2e 68 74 6d 6c 20 48 54 54 50 /index.h tml HTTP
0050 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1··Ho st: www.
0060 69 6e 66 31 30 35 2e 6f 72 67 0d 0a 55 73 65 72 inf105.o rg··User
0070 2d 41 67 65 6e 74 3a 20 63 75 72 6c 2f 38 2e 32 -Agent: curl/8.2
0080 31 2e 30 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 1.0··Acc ept: */*
0090 0d 0a 0d 0a ····

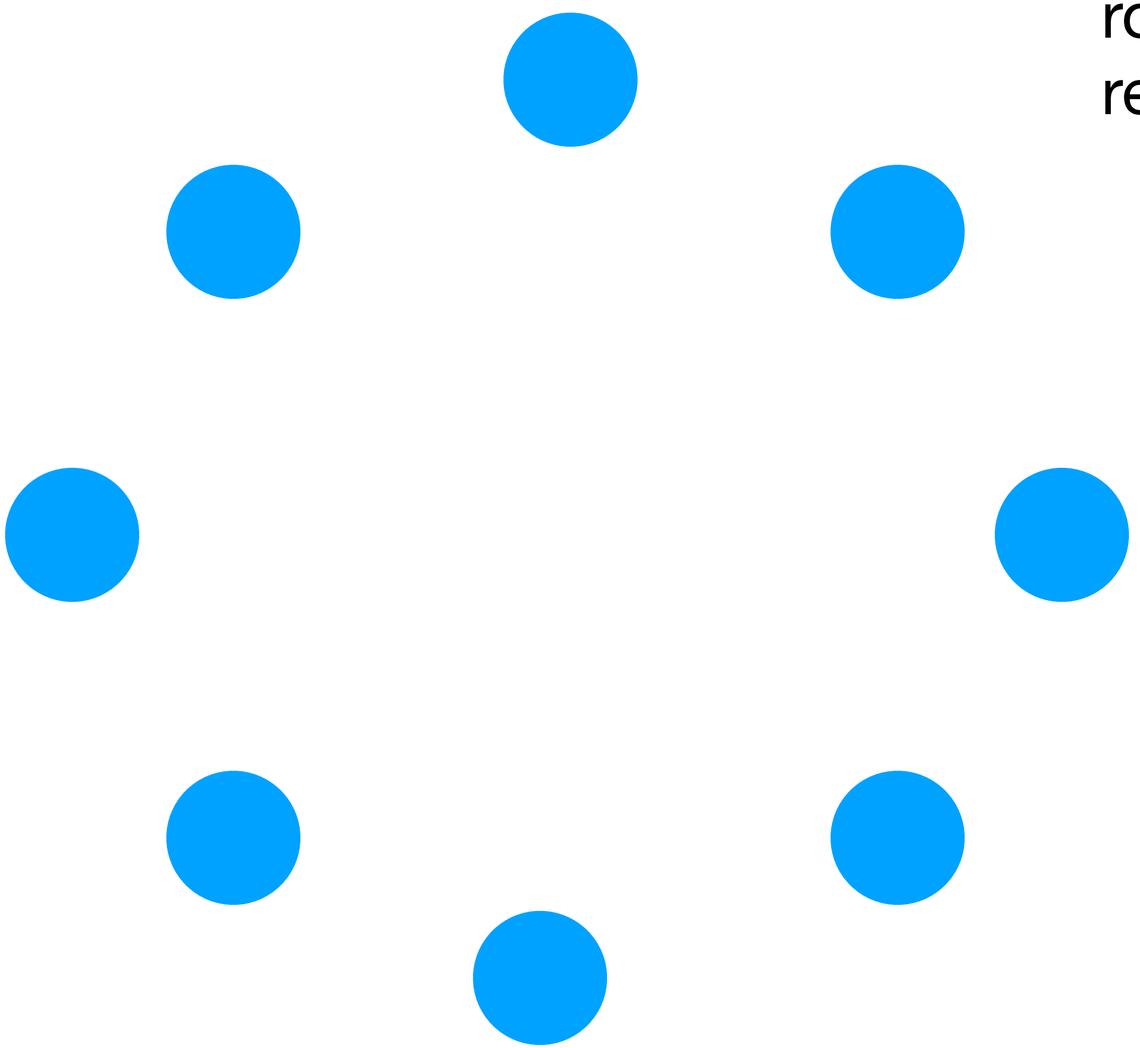

> Frame 234: Packet, 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits
> Ethernet II, Src: ca:37:e0:c8:5a:cb (ca:37:e0:c8:5a:cb), Dst: Cisco_9f:f2:70 (
> Internet Protocol Version 4, Src: 10.111.63.164, Dst: 158.39.201.59
> Transmission Control Protocol, Src Port: 53742, Dst Port: 80, Seq: 1, Ack: 1,
> Hypertext Transfer Protocol


0000 00 00 0c 9f f2 70 ca 37 e0 c8 5a cb 08 00 45 02 ·····p·7 ··Z···E·
0010 00 86 00 00 00 00 40 06 c8 fa 0a 6f 3f a4 9e 27 ·····@· ···o?··'
0020 c9 3b d1 ee 00 50 bd 24 f2 a9 be 0b 0b 93 50 18 ·;···P·$ ·····P·
0030 10 00 5c d7 00 00 47 45 54 20 2f 6c 61 62 30 34 ··\···GE T /lab04
0040 2f 69 6e 64 65 78 2e 68 74 6d 6c 20 48 54 54 50 /index.h tml HTTP
0050 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1··Ho st: www.
0060 69 6e 66 31 30 35 2e 6f 72 67 0d 0a 55 73 65 72 inf105.o rg··User
0070 2d 41 67 65 6e 74 3a 20 63 75 72 6c 2f 38 2e 32 -Agent: curl/8.2
0080 31 2e 30 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 1.0··Acc ept: */*
0090 0d 0a 0d 0a ····

rutere bare ser på IP adresser, bytter ethernet header

har fysisk forbindelse til noen nabonettverk

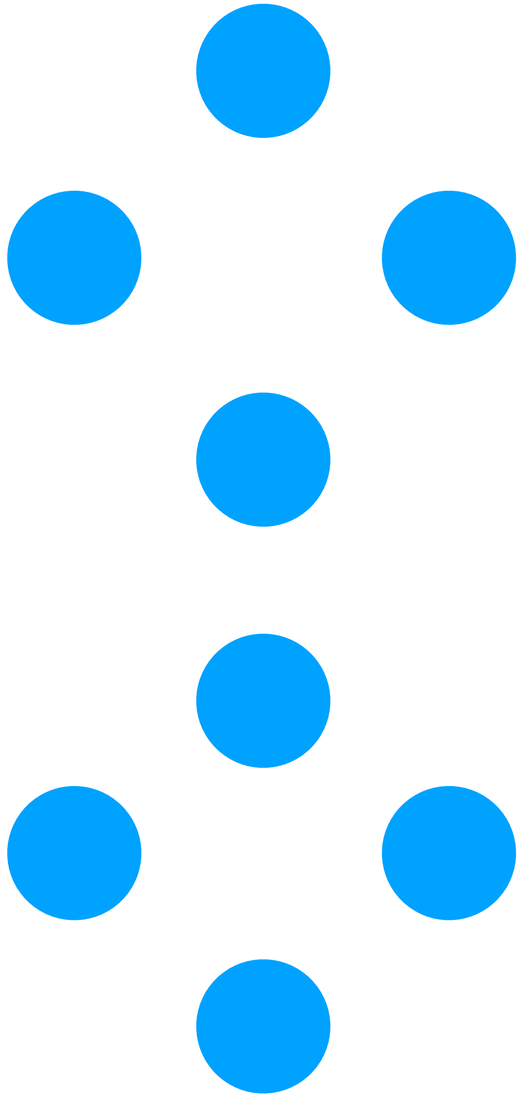
routing table avgjør i hvilken retning pakkene blir sendt



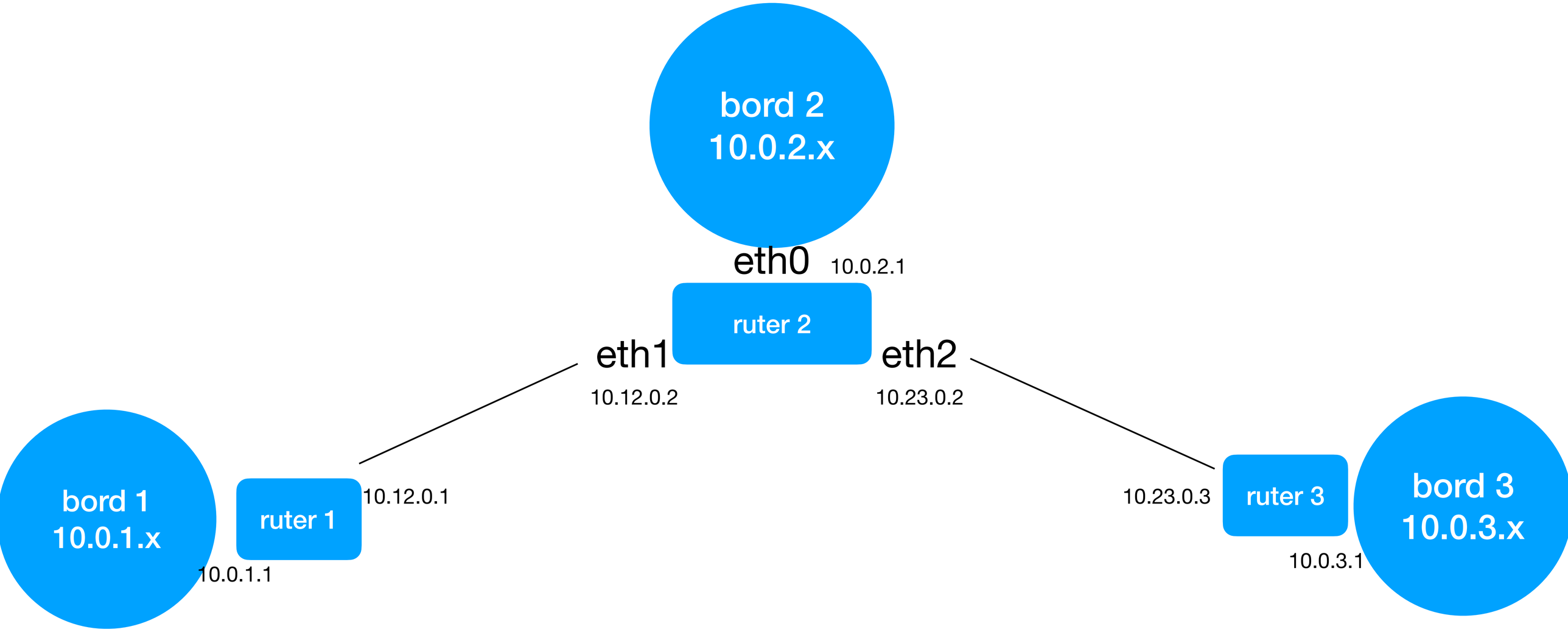
rutere bare ser på IP adresser, bytter ethernet header

har fysisk forbindelse til noen nabonettverk

routing table avgjør i hvilken retning pakkene blir sendt

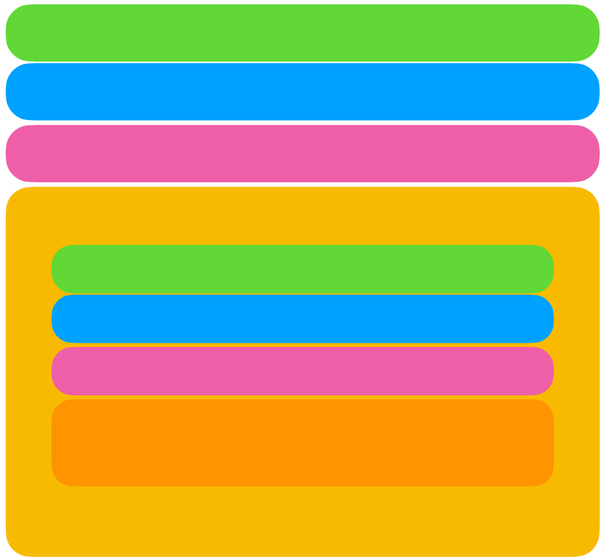


en ruter er med i flere nettverk, hvert nettverksport i et annet



Tunneling / VPN

- kan sende hele layer-2 eller layer-3 frames som layer-5 **data**



- knytte sammen 2 fysisk avskilte nettverk til ett Virtual Private Network (VPN)
- ytre pakke er på offentlig internett, kan ha kryptert data-segment
- indre pakke er hentet ut på mottakersiden og rutes videre som vanlig

Tunneling / VPN

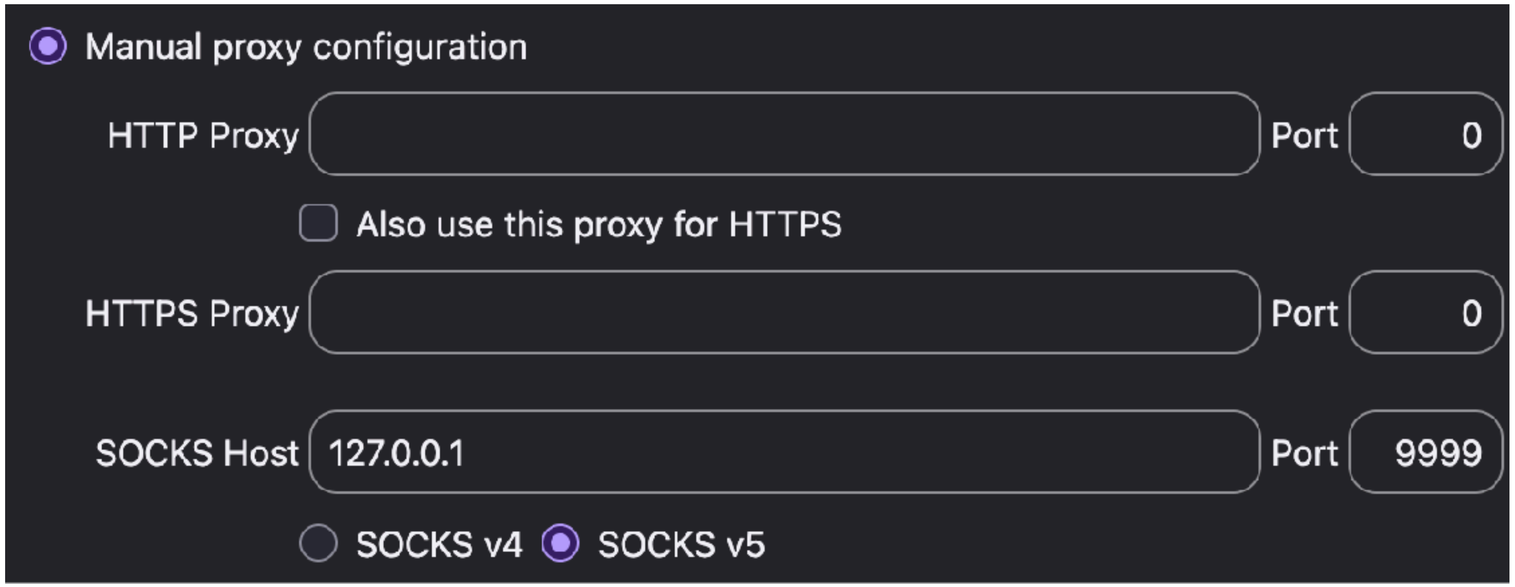
- Det finnes mange tunneling-protokoller, ikke aller lager en VPN
  L2TP, OpenVPN, PPPoE, ...
  https://en.wikipedia.org/wiki/Tunneling_protocol

- Enklest å komme i gang med for å opprette en privat tunnel mellom to egne enheter: Wireguard https://www.wireguard.com/

Tunneling / VPN

- SSH tilbyr tunneling: ssh -D9999 inf105

  åpner en "SOCKSv5 proxy" localhost:9999 som kan brukes f.eks i browser



så blir all browsertrafikk sent gjennom inf105-maskinen

Tilbake til www:

Dynamiske nettsider

statisk vs dynamisk

"Statisk":

- webserver sender filer fra sitt filsystem til klienten
- all beregning skjer på klienten / i browser
- selv om der er en nettside med interaktive Javascript-elementer!
- kan betjene hundrevis av klienter fra en liten maskin

"Dynamisk":

- webserveren beregner (deler av) en ny HTML fil "on demand" og sender den
- mye mer fleksibel, egnet til oppgaver som ikke kan utføres hos klienten (login, datavern, ...)
- kan koble til hva som helst dataprogramm
- serverbelastning *kan* bli høy

CGI

- En tidlig mulighet til dynamiske nettsider: CGI (common gateway interface)
- Idé 1993, version 1.1 definert i 1997
- Fungerer som g*ateway* mellom andre datasystemer og webservere
- informasjon fra videre URL blir sent som environment-variabler
- ikke støttet i nginx, bedre metoder tilgjengelig

CGI

- Server mottar et GET på /cgi-bin/foobar
- /cgi-bin/ er definert som en mappe med CGI-skripter i config
- kjører skriptet foobar
- tar output fra skriptet som HTTP header / HTML body
- sender til klienten

CGI

- demo bash
- demo python
- demo injection problem