



# Traffic Analysis

---

รศ.ดร. อนันต์ ผลเพิ่ม

Assoc.Prof.Anan Phonphoem, Ph.D.

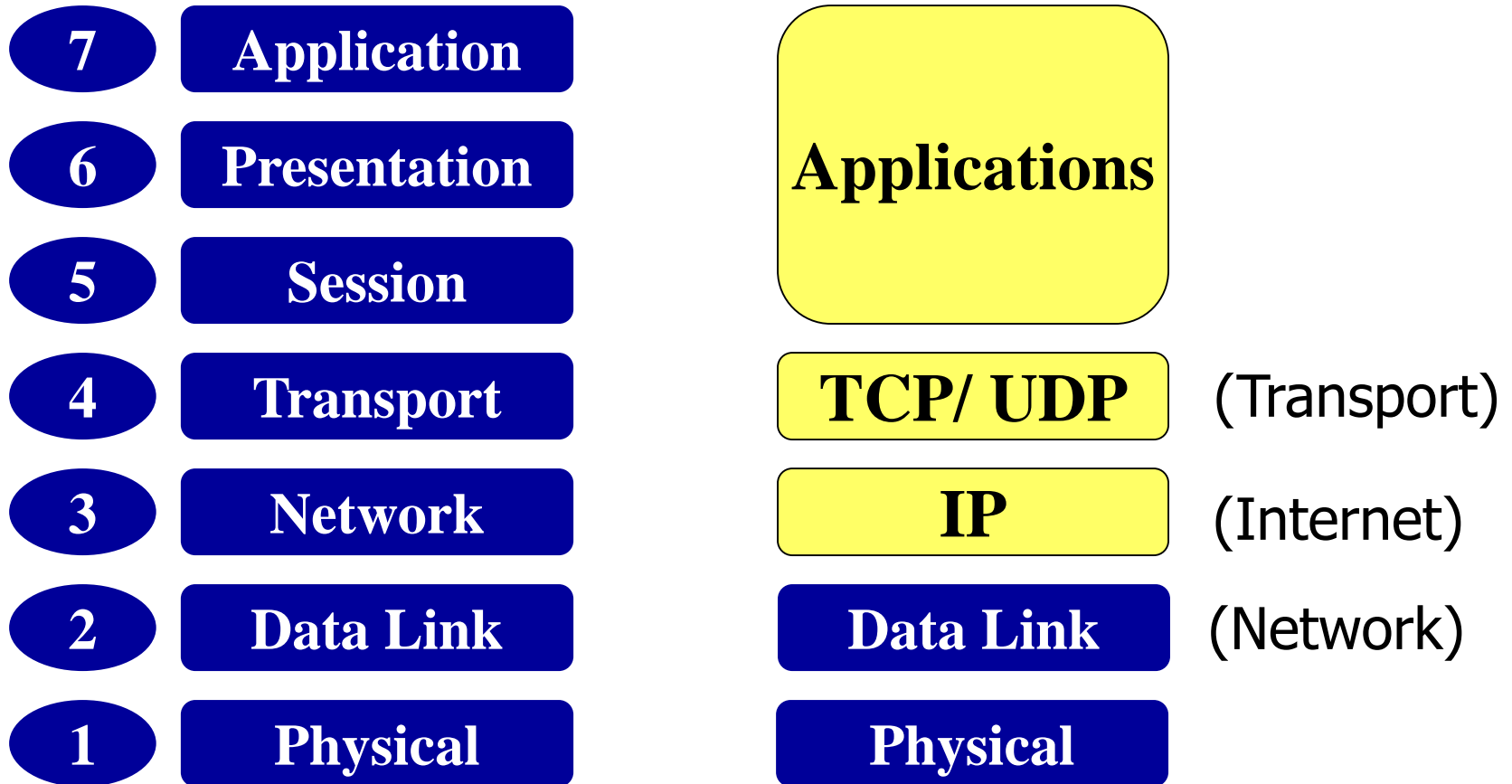
[anan.p@ku.ac.th](mailto:anan.p@ku.ac.th)

<http://www.cpe.ku.ac.th/~anan>

Computer Engineering Department

Kasetsart University, Bangkok, Thailand

# OSI Model and TCP/IP



# TCP/IP Encapsulation

**Applications**

Message

**TCP/ UDP**

User Datagram (segment)

**IP**

Datagram

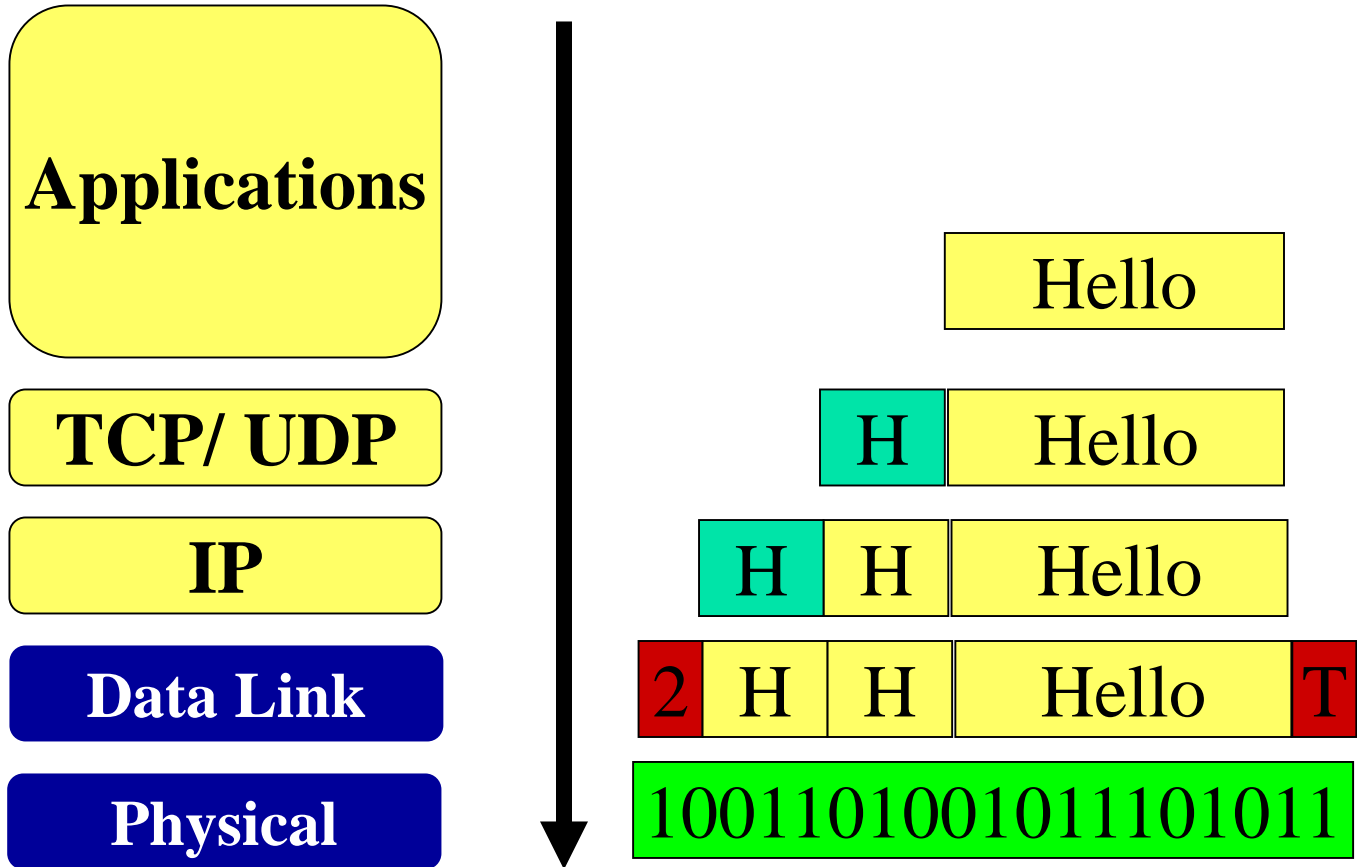
**Data Link**

Frame

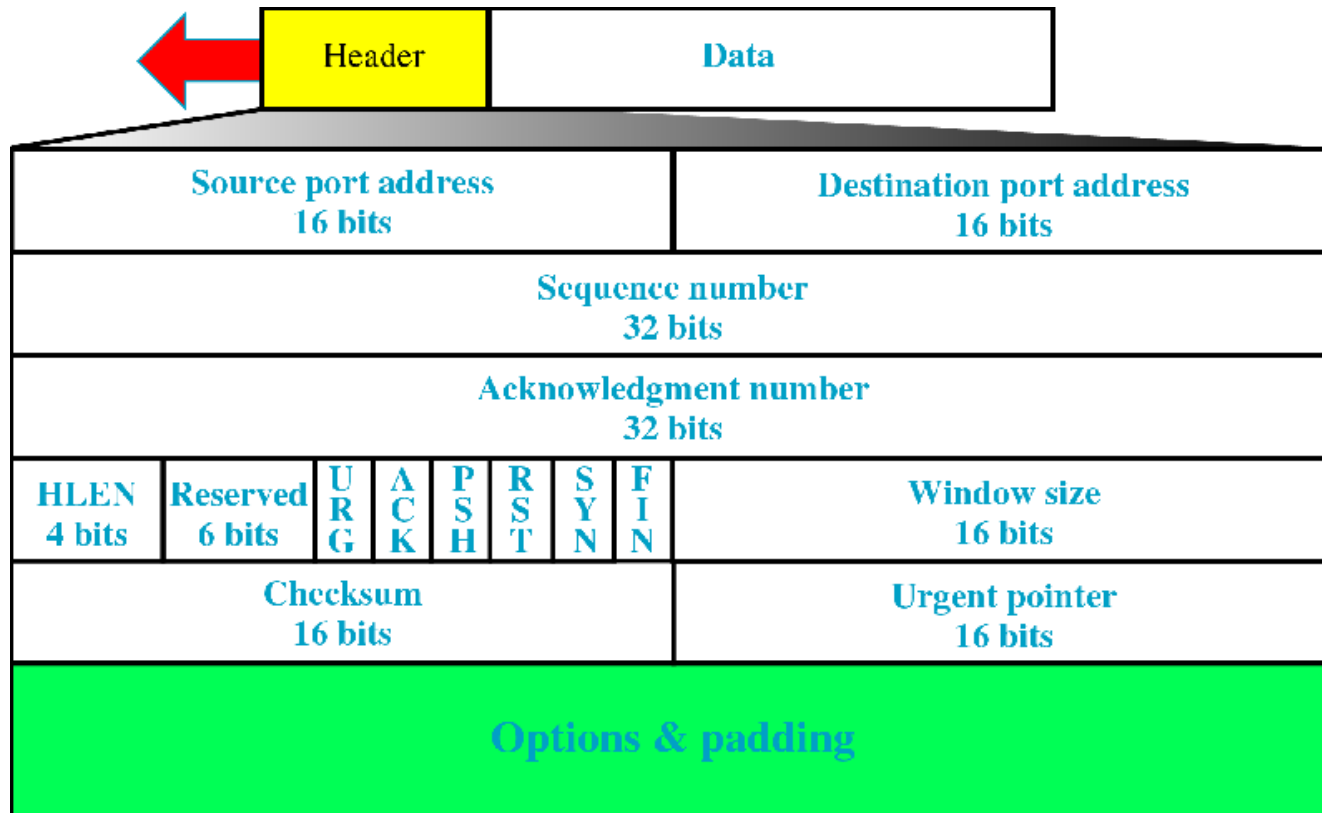
**Physical**

Bits

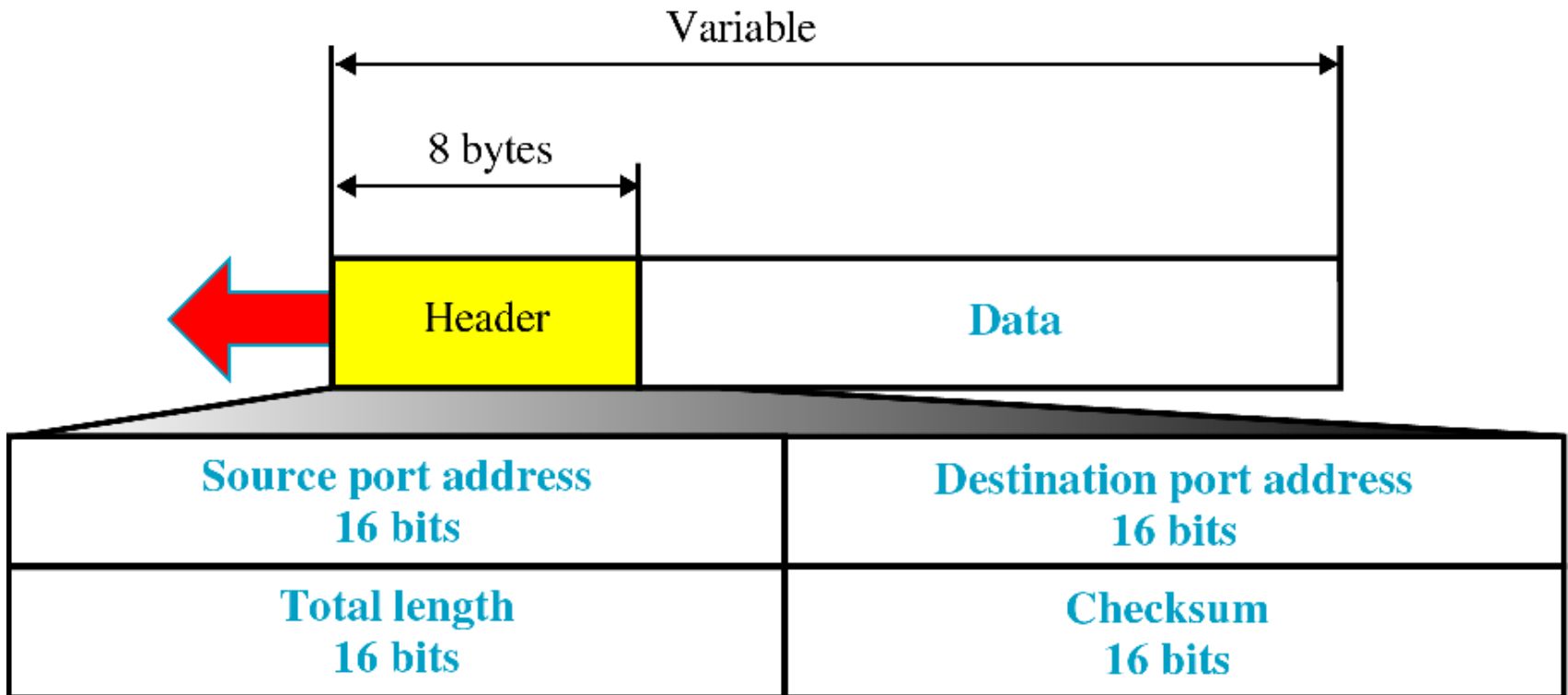
# Data Flow



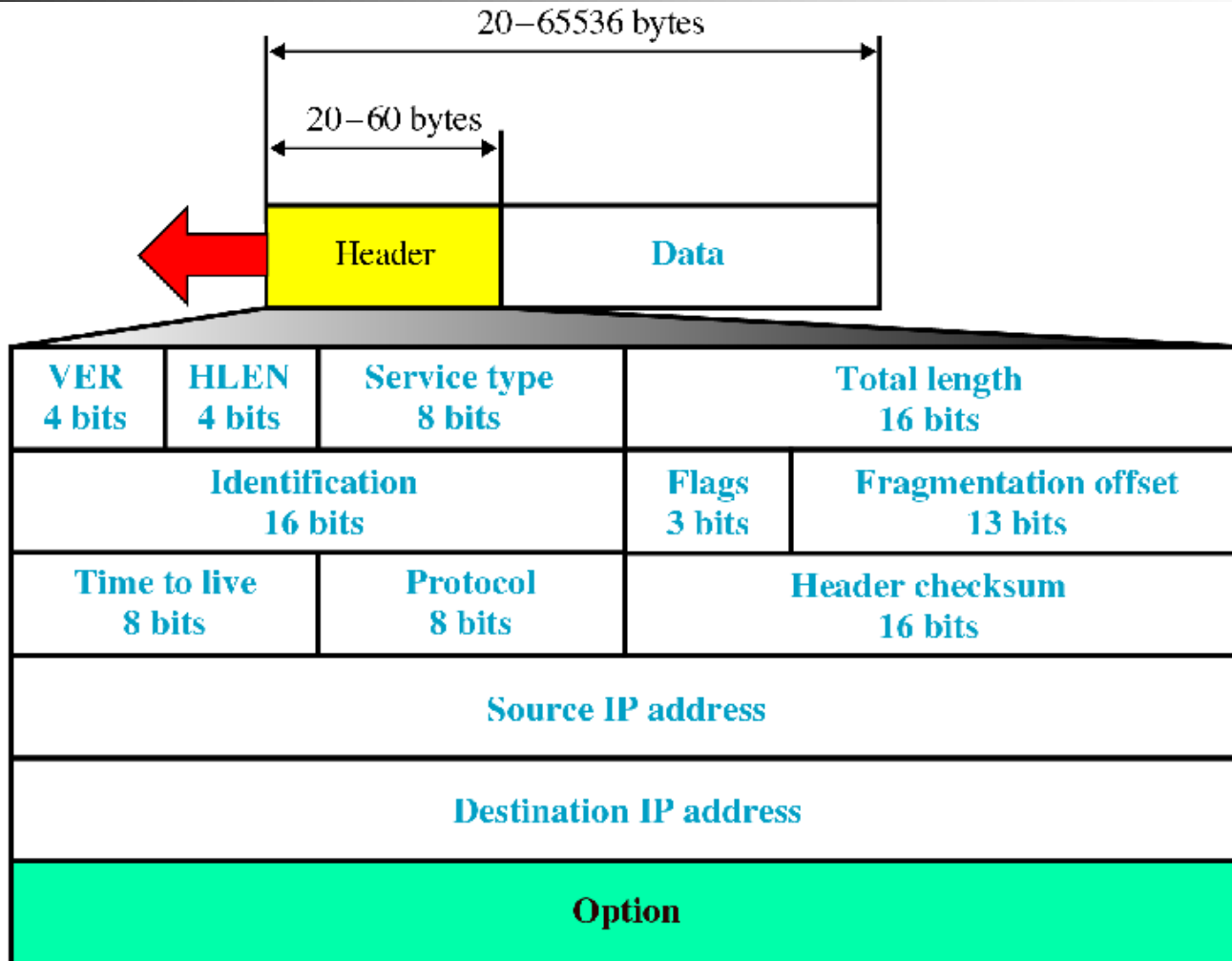
# TCP Segment Format



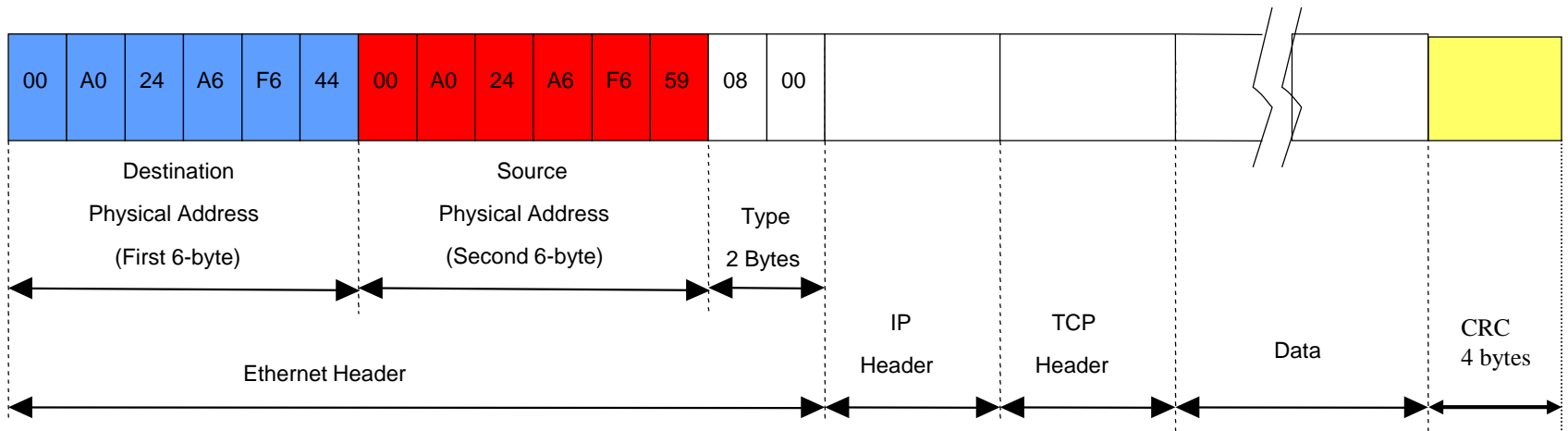
# UDP Datagram Format



# IP Datagram

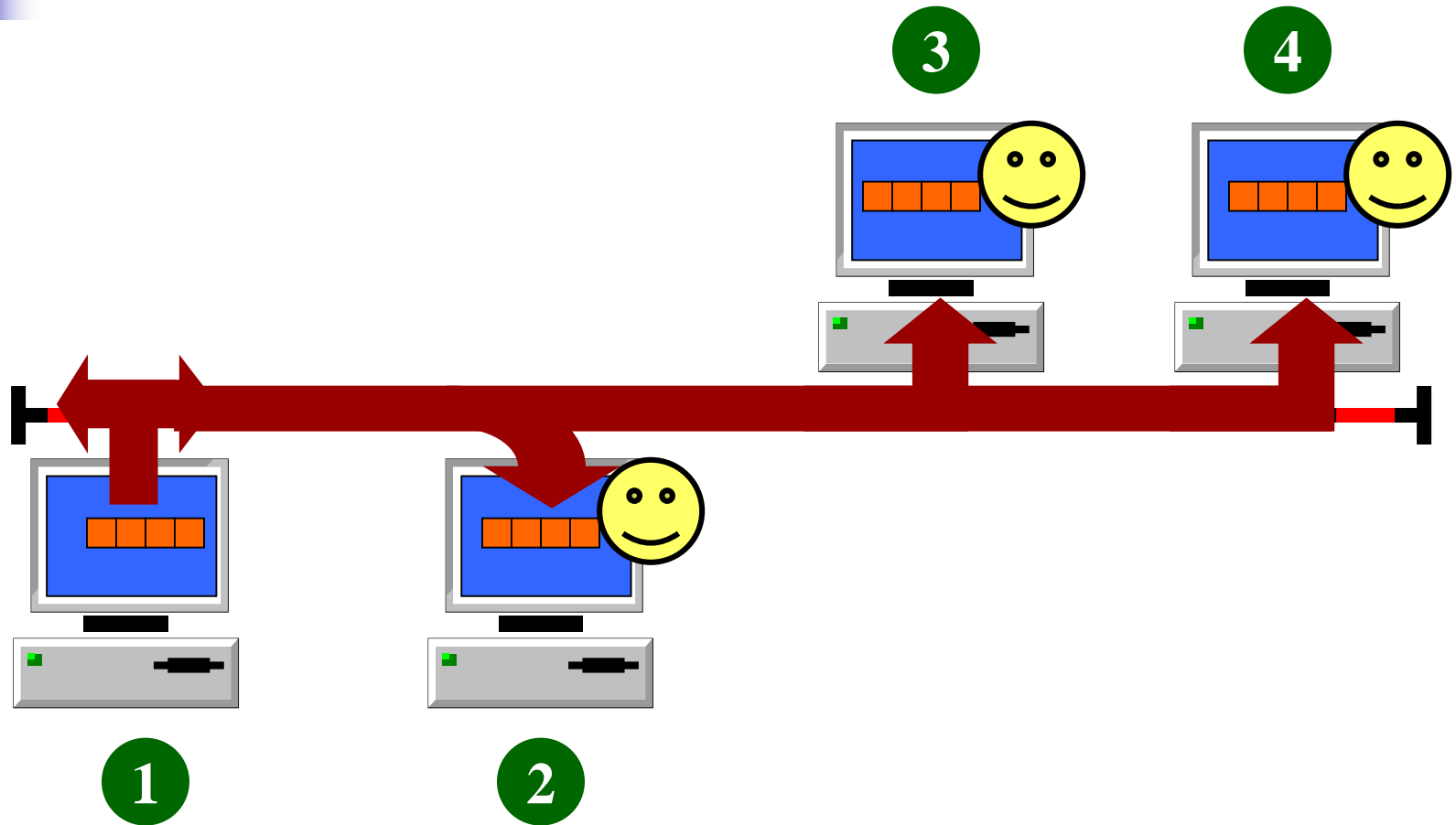


# Ethernet Frame



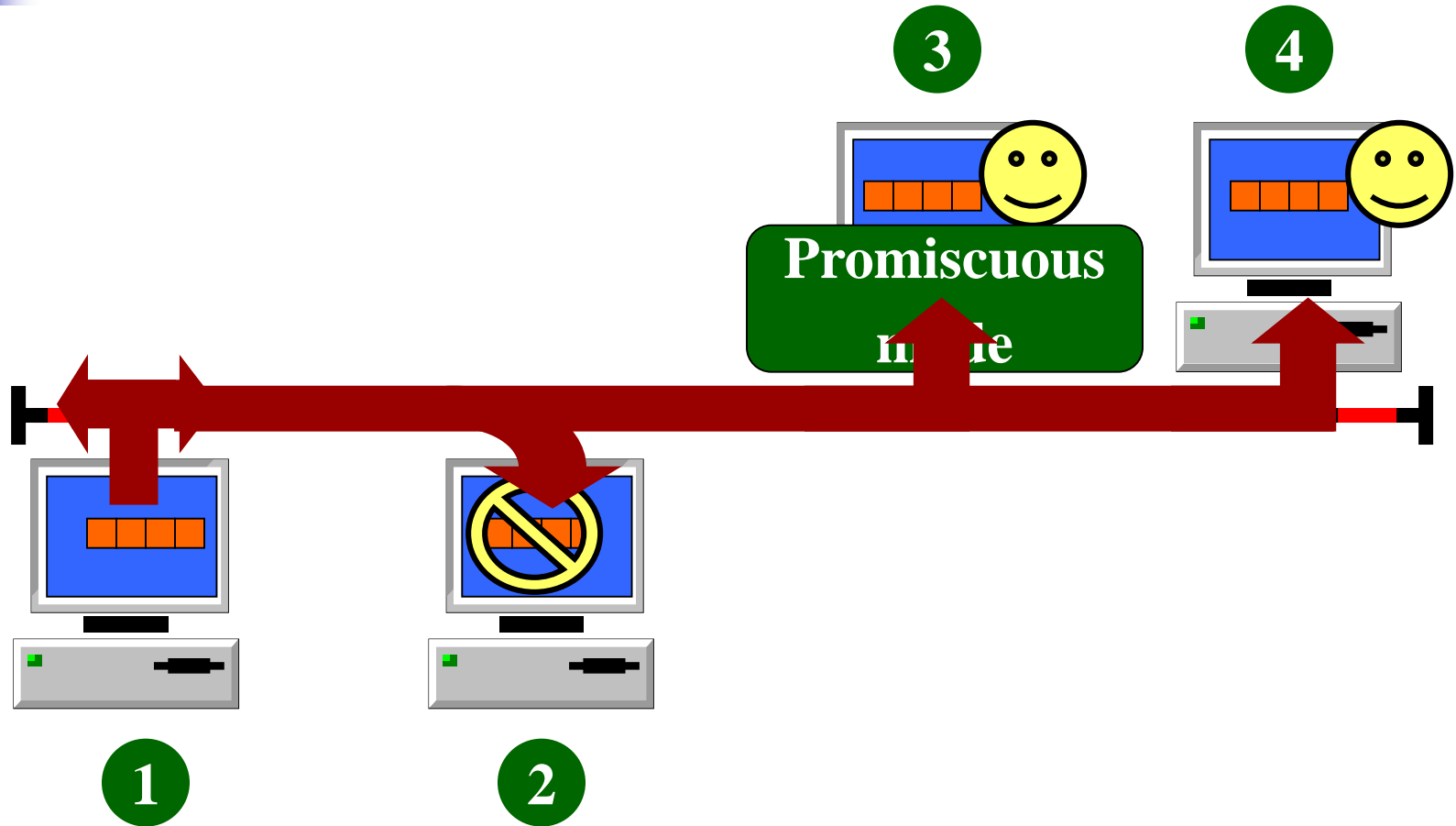


# Regular Ethernet



Station 1 transmits to all (broadcast)

# Regular Ethernet



Station 1 transmits to station 4



# Sniffer

---

- Network and protocol analyzer
- For network maintenance and trouble shooting
- Capture, monitor, analyze, trouble shooting
- Example: Etherpeek, Ethereal, Wireshark

# Wireshark

Wireshark interface showing network traffic capture on interface Wi-Fi: en0. The display filter is empty. The packet list shows various protocols including ICMPv6, ARP, SSL, TCP, and DNS. Packet 25 is selected, showing details for a TCP segment.

No.	Time	Source	Destination	Protocol	Length	Info
19	34.259607	fe80::b2aa:77ff:fe...	ff02::1	ICMPv6	86	Router Advertisement from b0:aa:77:a2:b3:7f
20	35.093637	CiscoInc_1f:de:c0	Broadcast	ARP	42	Gratuitous ARP for 158.108.139.253 (Reply)
21	36.975386	203.104.174.13	158.108.141.13	SSL	240	Encrypted Data, Continuation Data
22	36.975465	158.108.141.13	203.104.174.13	TCP	54	55525 → 443 [ACK] Seq=1 Ack=187 Win=6243 Le
23	36.977438	158.108.141.13	203.104.174.13	SSL	81	Encrypted Data, Continuation Data
24	37.287679	fe80::b2aa:77ff:fe...	ff02::1	ICMPv6	86	Router Advertisement from b0:aa:77:a2:b3:7f
25	37.546531	158.108.141.13	203.104.174.13	TCP	141	[TCP Retransmission] 55525 → 443 [PSH, ACK]
26	37.809781	203.104.174.13	158.108.141.13	TCP	66	[TCP ACKed unseen segment] 443 → 55525 [ACK
27	40.422159	fe80::b2aa:77ff:fe...	ff02::1	ICMPv6	86	Router Advertisement from b0:aa:77:a2:b3:7f
28	42.198186	158.108.141.13	158.108.0.2	DNS	77	Standard query 0x3e2d A www3.l.google.com
29	42.200449	158.108.0.2	158.108.141.13	DNS	469	Standard query response 0x3e2d A www3.l.goo
30	42.202253	158.108.141.13	202.28.85.187	TCP	78	55856 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS
31	42.203943	202.28.85.187	158.108.141.13	TCP	74	443 → 55856 [SYN, ACK] Seq=0 Ack=1 Win=2896
32	42.204014	158.108.141.13	202.28.85.187	TCP	66	55856 → 443 [ACK] Seq=1 Ack=1 Win=131744 Le
33	42.205662	158.108.141.13	202.28.85.187	TLSv1...	293	Client Hello
34	42.207238	202.28.85.187	158.108.141.13	TCP	66	443 → 55856 [ACK] Seq=1 Ack=228 Win=30080 L
35	42.271802	202.28.85.187	158.108.141.13	TLSv1...	1514	Server Hello
36	42.271808	202.28.85.187	158.108.141.13	TCP	666	[TCP segment of a reassembled PDU]
37	42.271883	158.108.141.13	202.28.85.187	TCP	66	55856 → 443 [ACK] Seq=228 Ack=2049 Win=1296
38	42.272000	202.28.85.187	158.108.141.13	TCP	1514	[TCP segment of a reassembled PDU]
39	42.272003	202.28.85.187	158.108.141.13	TCP	666	[TCP segment of a reassembled PDU]
40	42.272004	202.28.85.187	158.108.141.13	TLSv1...	258	Certificate

▶ Frame 30: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0

- ▶ Ethernet II, Src: Apple\_9b:91:ec (c8:69:cd:9b:91:ec), Dst: CiscoInc\_a2:b3:7f (b0:aa:77:a2:b3:7f)
- ▶ Internet Protocol Version 4, Src: 158.108.141.13, Dst: 202.28.85.187
- ▶ Transmission Control Protocol, Src Port: 55856 (55856), Dst Port: 443 (443), Seq: 0, Len: 0

```
0000  b0 aa 77 a2 b3 7f c8 69 cd 9b 91 ec 08 00 45 00  ..w....i.....E.
0010  00 40 11 75 40 00 40 06 dd f1 9e 6c 8d 0d ca 1c  .@.u@.@. ....l....
0020  55 bb da 30 01 bb f1 69 44 4f 00 00 00 00 b0 02  U..0...i DO.....
0030  ff ff 38 51 00 00 02 04 05 b4 01 03 03 05 01 01  ..8Q.....
0040  08 0a 0e f4 92 c1 00 00 00 00 04 02 00 00  ..0.....
```

wireshark\_pcapng\_en0\_20161130074250\_wF0Jz Packets: 6097 · Displayed: 6097 (100.0%) Profile: Default

# Raw Frame

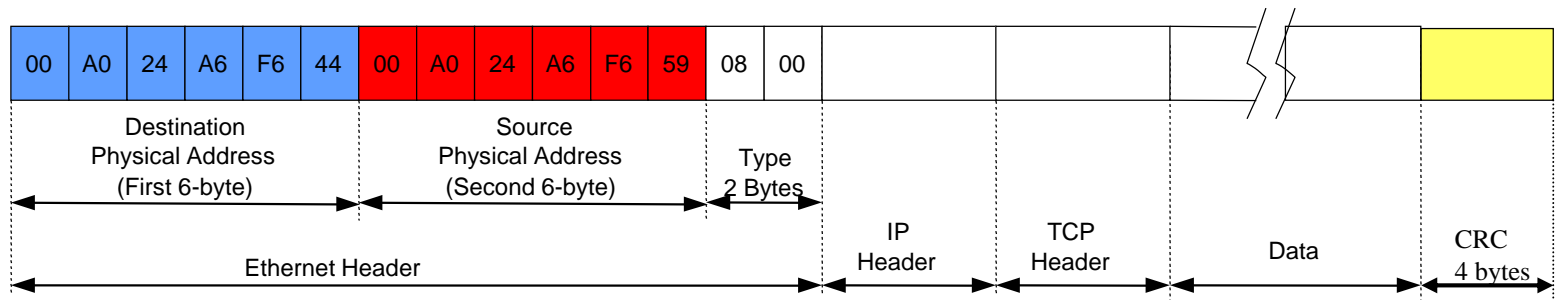
0000	00	0b	5d	51	ac	5b	00	04	dd	49	22	02	08	00	45	00	...	]Q.	[..	.I"	...E.
0010	00	28	5e	2a	40	00	3f	06	16	ff	9e	6c	02	45	9e	6c	..	(^*@.?.	...].E.]		
0020	87	89	00	50	06	51	4b	40	bd	a4	55	11	14	cf	50	11	...	P.QK@	..U...	P.	
0030	19	20	56	a6	00	00	00	00	00	00	00	00					V.....	.....			

# of Byte

Raw Frame

Ascii

# Ethernet Header/Trailer



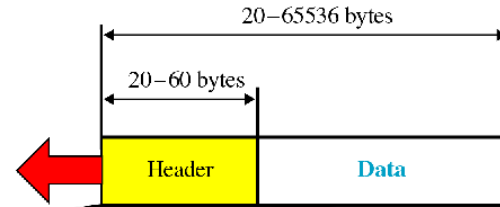
Ethernet Header

Ethernet Trailer

```

Ethernet II, Src: 00:04:dd:49:22:02, Dst: 00:0b:5d:51:ac:5b
  Destination: 00:0b:5d:51:ac:5b (128.199.0.2)
  Source: 00:04:dd:49:22:02 (158.108.128.1)
  Type: IP (0x0800)
  Trailer: 000000000000
  Internet Protocol, Src Addr: 158.108.2.69 (158.108.2.69), Dst Addr: 158.108.135.137 (158
  Transmission Control Protocol, Src Port: http (80), Dst Port: 1617 (1617), Seq: 130, Ack
0000  00 0b 5d 51 ac 5b 00 04 dd 49 22 02 08 00 45 00  ..]Q.[.. .I"...E.
0010  00 28 5e 2a 40 00 3f 06 16 ff 9e 6c 02 45 9e 6c  .(A*@.? ...].E.]
0020  87 89 00 50 06 51 4b 40 bd a4 55 11 14 cf 50 11  ...P.QK@ ..U...P.
0030  19 20 56 0f 00 00 00 00 00 00 00 00 00 00 00  . V.....
  
```

# IPv4 Header



Destination IP Address

**158.108.135.137**

Source IP Address

9e 6c 02 45

**158.108.2.69**

VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits	
Identification 16 bits			Flags 3 bits	Fragmentation offset 13 bits
Time to live 8 bits		Protocol 8 bits	Header checksum 16 bits	
Source IP address				
Destination IP address				
Option				

```

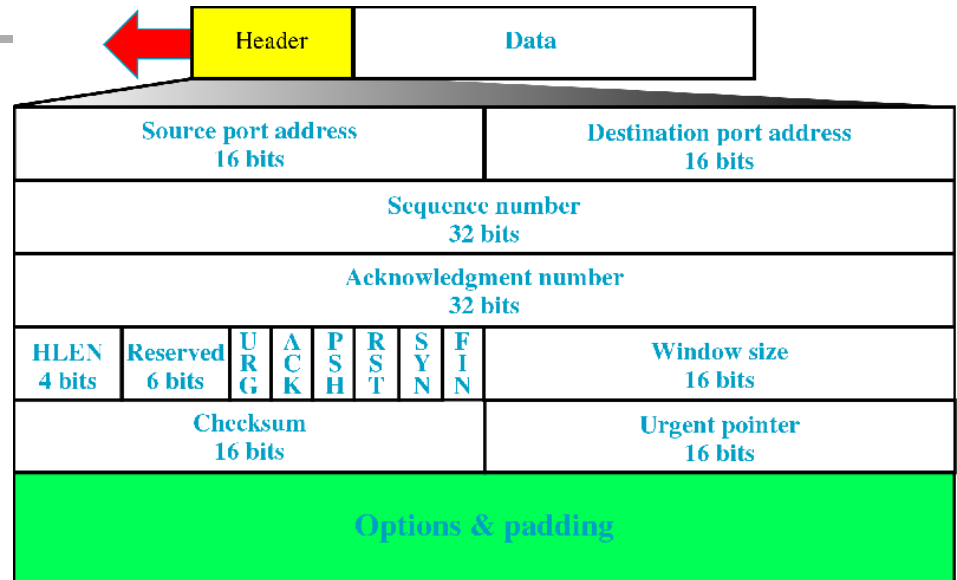
> Internet Protocol, Src Addr: 158.108.2.69 (158.108.2.69), Dst Addr: 158.108.135.137 (158.108.135.137)
> Transmission Control Protocol, Src Port: http (80), Dst Port: 1617 (1617), Seq: 130, Ack: 3
  
```

```

0000 00 0b 5d 51 ac 5b 00 04 dd 49 77 02 08 00 45 00  ..]Q.[...I"...E.
0010 00 28 5e 2a 40 00 3f 06 16 ff 9e 6c 02 45 9e 6c  .(A*@.?...|.E.]
0020 87 89 00 50 06 51 4b 40 bd a4 55 11 14 cf 50 11  ..P.QK@ ..U...P.
0030 19 20 56 a6 00 00 00 00 00 00 00 00  .. V.....
  
```

# TCP Header

TCP Header



```

▶ Transmission Control Protocol, Src Port: http (80), Dst Port: 1617 (1617), Seq: 130, Ack: 3
.....
0000  00 0b 5d 51 ac 5b 00 04 dd 49 22 02 08 00 45 00  ..]Q.[...I"...E.
0010  00 28 5e 2a 40 00 3f 06 16 ff 9e 6c 02 45 9e 6c  .(A*@.?. ...].E.]
0020  87 89 00 50 06 51 4b 40 bd a4 55 11 14 cf 50 11  ...P.QK@ ..U...P.
0030  19 20 56 a6 00 00 00 00 00 00 00 00  .. V... ..
    
```



# IPv6

Wi-Fi: en0

Apply a display filter ... <%%/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
24	37.287679	fe80::b2aa:77ff:fe...	ff02::1	ICMPv6	86	Router Advertisement from b0:aa:77:a2:b3:7f
25	37.546531	158.108.141.13	203.104.174.13	TCP	141	[TCP Retransmission] 5525 → 443 [PSH, ACK]
26	37.809781	203.104.174.13	158.108.141.13	TCP	66	[TCP ACKed unseen segment] 443 → 5525 [ACK]
27	40.422159	fe80::b2aa:77ff:fe...	ff02::1	ICMPv6	86	Router Advertisement from b0:aa:77:a2:b3:7f
28	42.198186	158.108.141.13	158.108.0.2	DNS	77	Standard query 0x3e2d A www3.l.google.com
29	42.200449	158.108.0.2	158.108.141.13	DNS	469	Standard query response 0x3e2d A www3.l.google.com

▶ Frame 27: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0

▶ Ethernet II, Src: CiscoInc\_a2:b3:7f (b0:aa:77:a2:b3:7f), Dst: Apple\_9b:91:ec (c8:69:cd:9b:91:ec)

▼ Internet Protocol Version 6, Src: fe80::b2aa:77ff:fea2:b37f, Dst: ff02::1

- 0110 .... = Version: 6
- ▶ .... 1110 0000 .... = Traffic class: 0xe0 (DSCP: CS7, ECN: Not-ECT)
- .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
- Payload length: 32
- Next header: ICMPv6 (58)
- Hop limit: 255
- Source: fe80::b2aa:77ff:fea2:b37f
- [Source SA MAC: CiscoInc\_a2:b3:7f (b0:aa:77:a2:b3:7f)]
- Destination: ff02::1
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]

▶ Internet Control Message Protocol v6

```
0000 c8 69 cd 9b 91 ec b0 aa 77 a2 b3 7f 86 dd 6e 00 .i.....w.....n.
0010 00 00 00 20 3a ff fe 80 00 00 00 00 00 00 b2 aa ... :...
0020 77 ff fe a2 b3 7f ff 02 00 00 00 00 00 00 00 W.....
0030 00 00 00 00 00 01 86 00 6f e0 40 c0 07 08 00 00 .....o.@.....
0040 00 00 00 00 00 00 01 01 b0 aa 77 a2 b3 7f 05 01 .....W.....
0050 00 00 00 00 05 dc .....
```

Source IPv6 Stateless Autoconfiguration MAC Address (ipv6.src\_sa\_mac), 6 bytes      Packets: 6097 · Displayed: 6097 (100.0%)      Profile: Default

# IPv6 Header

Destination IP Address

Source IP Address

Version	Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

- ▶ Frame 27: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on inte
- ▶ Ethernet II, Src: CiscoInc\_a2:b3:7f (b0:aa:77:a2:b3:7f), Dst: Apple\_9b:91:e
- ▶ **Internet Protocol Version 6, Src: fe80::b2aa:77ff:fea2:b37f, Dst: ff02::1**
- ▶ Internet Control Message Protocol v6

```

0000  c8 69 cd 9b 91 e0 b0 aa 77 a2 b3 7f 86 dd 6e 00  .i.....W.....n.
0010  00 00 00 20 3a ff fe 80 00 00 00 00 00 00 b2 aa  ...:.....
0020  77 ff fe a2 b3 7f ff 02 00 00 00 00 00 00 00 00  W.....
0030  00 00 00 00 00 01 86 00 6f e0 40 c0 07 08 00 00  .....o.@....
0040  00 00 00 00 00 00 01 01 b0 aa 77 a2 b3 7f 05 01  .....W....
0050  00 00 00 00 05 dc
  
```



# Live Capture

---

- Demo