CSE 461: Introduction to Computer Communication Networks

Justin Chan

TODO

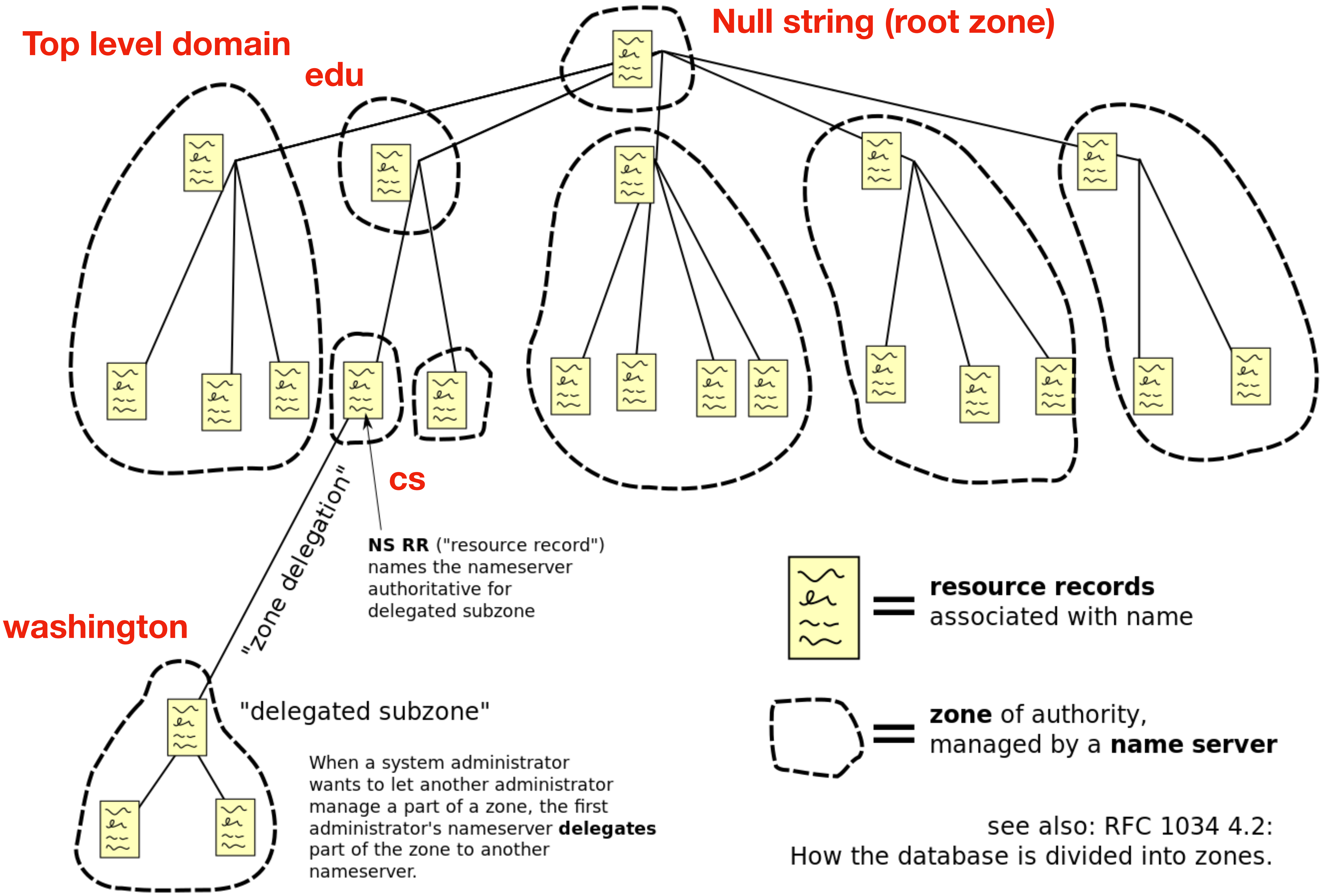
- DNS
- Wireshark
- Project 0 help

DNS

- Application level protocol
- Map human-readable domain name to IP address
  - Different users can return different IP addresses depending on their location. Why?
- Returns other information related to domain name
- Distributed database. Nodes are name servers

Up to 127 levels

Domain Name Space



Null string (root zone)

Top level domain

edu

cs

washington

"zone delegation"

NS RR ("resource record")
names the nameserver
authoritative for
delegated subzone

"delegated subzone"

When a system administrator wants to let another administrator manage a part of a zone, the first administrator's nameserver **delegates** part of the zone to another nameserver.

= **resource records** associated with name

= **zone** of authority, managed by a **name server**

see also: RFC 1034 4.2:
How the database is divided into zones.

DNS

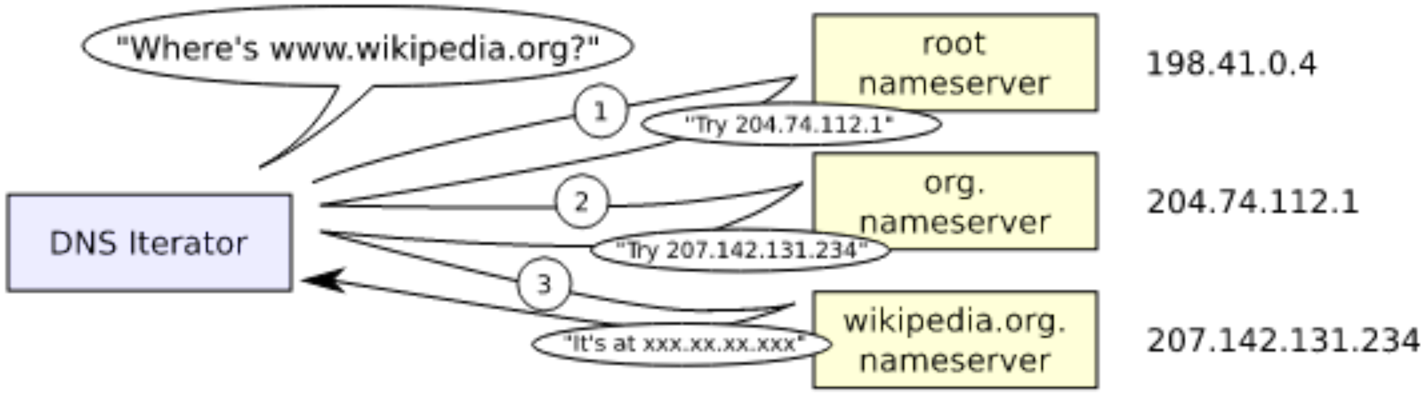
- Each domain has one authoritative name server. It has information about all the sub-domains as well
    - Master server: holds original master copies
    - Slave server: maintains copies of master records
- TLDs served by root name servers
- All records have a TTL in seconds, cached servers refresh their records after TTL expires

Looking up an address

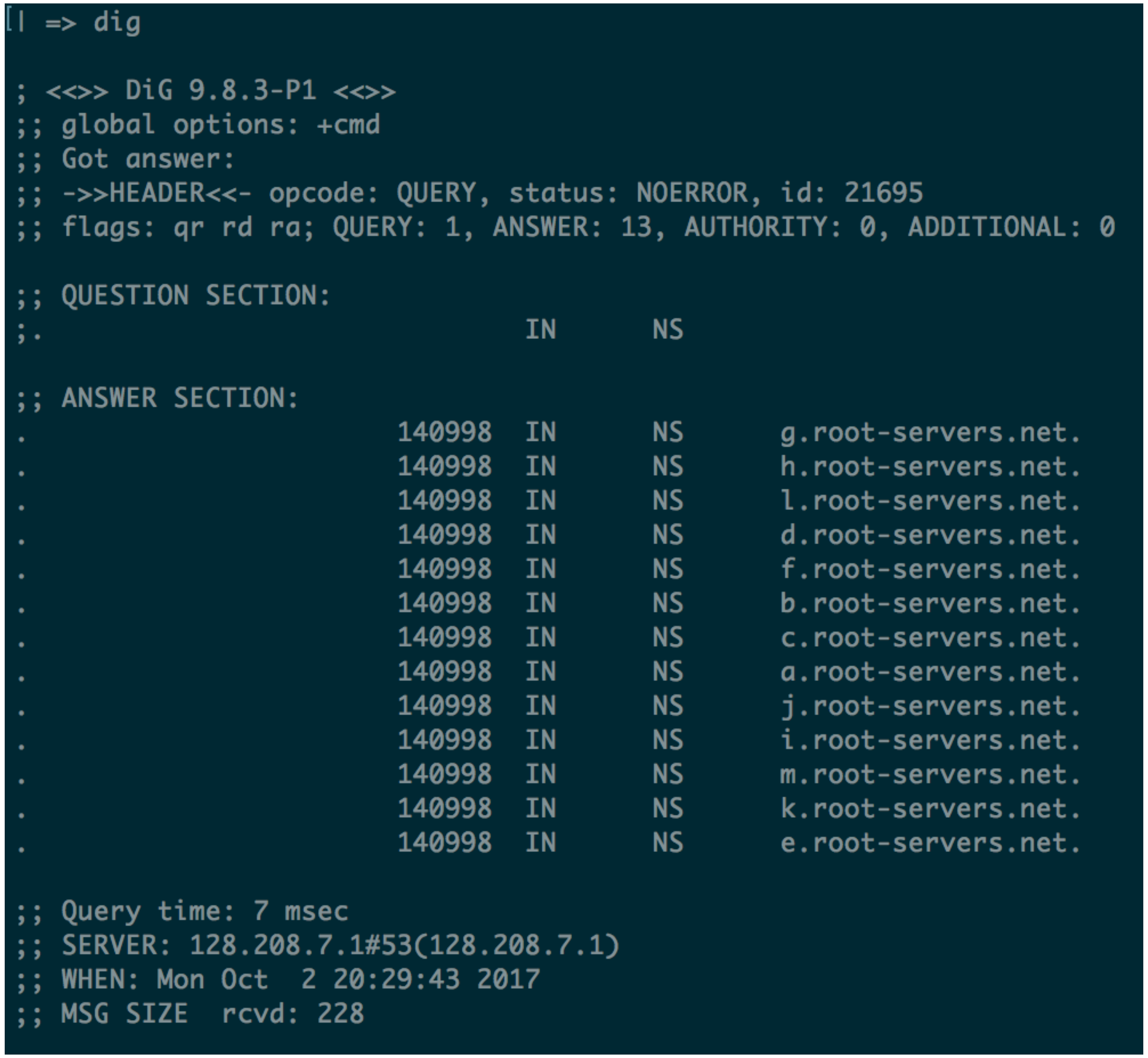
- Hosts know the IPs of several root name servers (this is updated)
- Roots refer to other authoritative name servers, first the TLD NS then lower subdomain NSs
- Caching done to avoid all web requests going to root name server
- Typically a UDP request, sometimes TCP
- This is done by ISPs and home routers

Iterative search

Recursive search



dig (domain information groper)



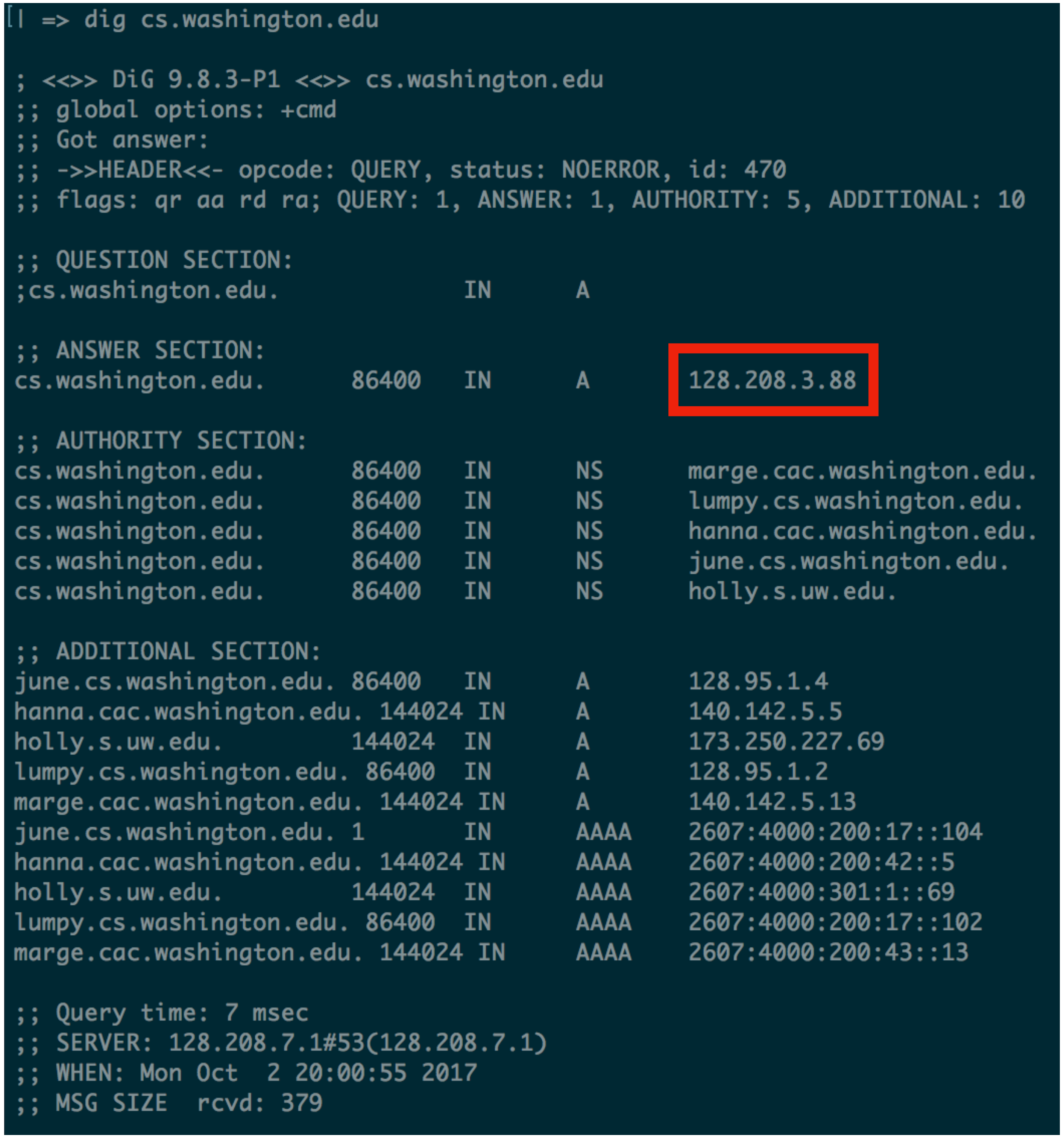
```
[| => dig

; <<>> DiG 9.8.3-P1 <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21695
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       140998  IN      NS      g.root-servers.net.
.                       140998  IN      NS      h.root-servers.net.
.                       140998  IN      NS      l.root-servers.net.
.                       140998  IN      NS      d.root-servers.net.
.                       140998  IN      NS      f.root-servers.net.
.                       140998  IN      NS      b.root-servers.net.
.                       140998  IN      NS      c.root-servers.net.
.                       140998  IN      NS      a.root-servers.net.
.                       140998  IN      NS      j.root-servers.net.
.                       140998  IN      NS      i.root-servers.net.
.                       140998  IN      NS      m.root-servers.net.
.                       140998  IN      NS      k.root-servers.net.
.                       140998  IN      NS      e.root-servers.net.

;; Query time: 7 msec
;; SERVER: 128.208.7.1#53(128.208.7.1)
;; WHEN: Mon Oct  2 20:29:43 2017
;; MSG SIZE  rcvd: 228
```

Unix utility to query DNS service

Root name servers

/etc/resolv.conf

dig



```
[| => dig cs.washington.edu

; <<>> DiG 9.8.3-P1 <<>> cs.washington.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 470
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 10

;; QUESTION SECTION:
;cs.washington.edu.             IN      A

;; ANSWER SECTION:
cs.washington.edu.      86400   IN      A       128.208.3.88

;; AUTHORITY SECTION:
cs.washington.edu.      86400   IN      NS      marge.cac.washington.edu.
cs.washington.edu.      86400   IN      NS      lumpy.cs.washington.edu.
cs.washington.edu.      86400   IN      NS      hanna.cac.washington.edu.
cs.washington.edu.      86400   IN      NS      june.cs.washington.edu.
cs.washington.edu.      86400   IN      NS      holly.s.uw.edu.

;; ADDITIONAL SECTION:
june.cs.washington.edu. 86400   IN      A       128.95.1.4
hanna.cac.washington.edu. 144024 IN     A       140.142.5.5
holly.s.uw.edu.         144024  IN      A       173.250.227.69
lumpy.cs.washington.edu. 86400  IN      A       128.95.1.2
marge.cac.washington.edu. 144024 IN     A       140.142.5.13
june.cs.washington.edu. 1       IN      AAAA    2607:4000:200:17::104
hanna.cac.washington.edu. 144024 IN     AAAA    2607:4000:200:42::5
holly.s.uw.edu.         144024  IN      AAAA    2607:4000:301:1::69
lumpy.cs.washington.edu. 86400  IN      AAAA    2607:4000:200:17::102
marge.cac.washington.edu. 144024 IN     AAAA    2607:4000:200:43::13

;; Query time: 7 msec
;; SERVER: 128.208.7.1#53(128.208.7.1)
;; WHEN: Mon Oct  2 20:00:55 2017
;; MSG SIZE  rcvd: 379
```

We are sending a query

We are requesting an A record

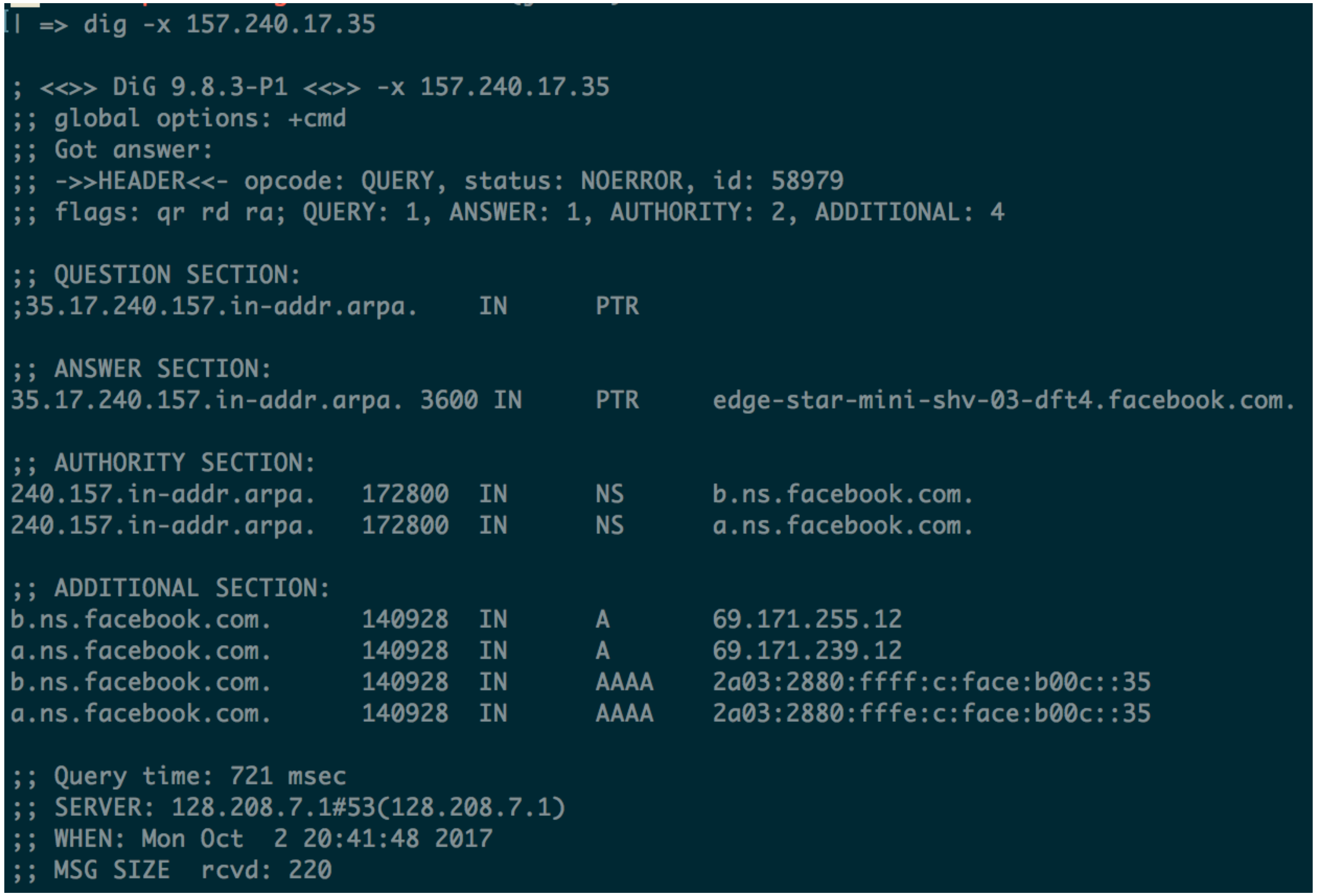
IP address is the answer

Here are the authoritative name servers

IP addresses of authoratative name servers

TTLs
86400 = 24 hours
144024 = 40 hours

dig



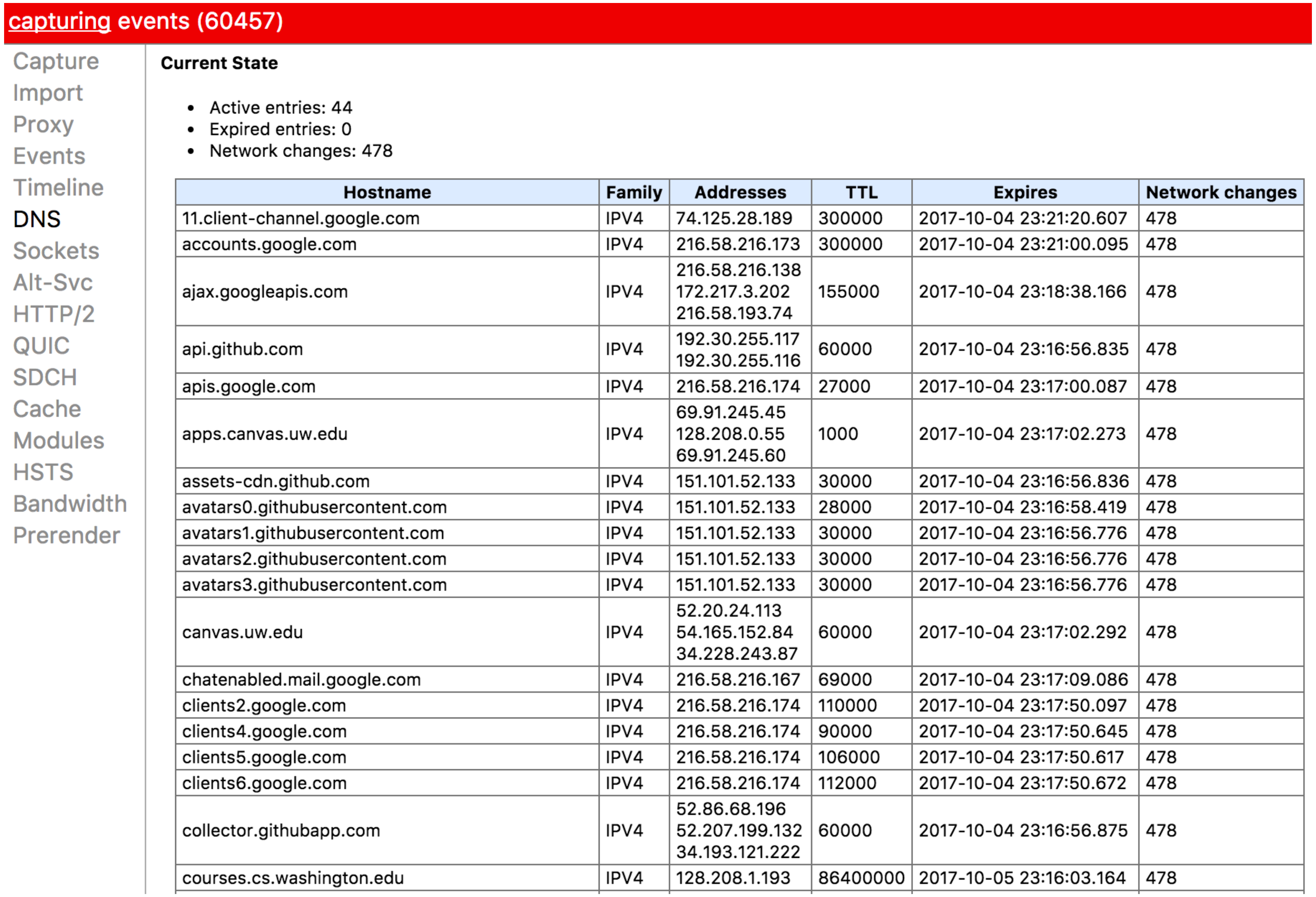
```
[| => dig -x 157.240.17.35

; <<>> DiG 9.8.3-P1 <<>> -x 157.240.17.35
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58979
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 4

;; QUESTION SECTION:
;35.17.240.157.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
35.17.240.157.in-addr.arpa. 3600 IN     PTR     edge-star-mini-shv-03-dft4.facebook.com.

;; AUTHORITY SECTION:
240.157.in-addr.arpa.   172800  IN      NS      b.ns.facebook.com.
240.157.in-addr.arpa.   172800  IN      NS      a.ns.facebook.com.

;; ADDITIONAL SECTION:
b.ns.facebook.com.      140928  IN      A       69.171.255.12
a.ns.facebook.com.      140928  IN      A       69.171.239.12
b.ns.facebook.com.      140928  IN      AAAA    2a03:2880:ffff:c:face:b00c::35
a.ns.facebook.com.      140928  IN      AAAA    2a03:2880:fffe:c:face:b00c::35

;; Query time: 721 msec
;; SERVER: 128.208.7.1#53(128.208.7.1)
;; WHEN: Mon Oct  2 20:41:48 2017
;; MSG SIZE  rcvd: 220
```

Reverse DNS lookup

PTR record for IP => name

DNS cache

chrome://net-internals/#dns



Current State

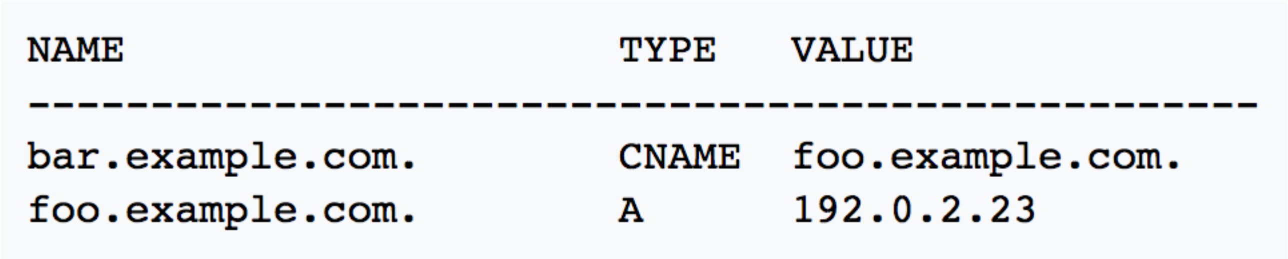
- Active entries: 44
- Expired entries: 0
- Network changes: 478

Hostname	Family	Addresses	TTL	Expires	Network changes
11.client-channel.google.com	IPV4	74.125.28.189	300000	2017-10-04 23:21:20.607	478
accounts.google.com	IPV4	216.58.216.173	300000	2017-10-04 23:21:00.095	478
ajax.googleapis.com	IPV4	216.58.216.138 172.217.3.202 216.58.193.74	155000	2017-10-04 23:18:38.166	478
api.github.com	IPV4	192.30.255.117 192.30.255.116	60000	2017-10-04 23:16:56.835	478
apis.google.com	IPV4	216.58.216.174	27000	2017-10-04 23:17:00.087	478
apps.canvas.uw.edu	IPV4	69.91.245.45 128.208.0.55 69.91.245.60	1000	2017-10-04 23:17:02.273	478
assets-cdn.github.com	IPV4	151.101.52.133	30000	2017-10-04 23:16:56.836	478
avatars0.githubusercontent.com	IPV4	151.101.52.133	28000	2017-10-04 23:16:58.419	478
avatars1.githubusercontent.com	IPV4	151.101.52.133	30000	2017-10-04 23:16:56.776	478
avatars2.githubusercontent.com	IPV4	151.101.52.133	30000	2017-10-04 23:16:56.776	478
avatars3.githubusercontent.com	IPV4	151.101.52.133	30000	2017-10-04 23:16:56.776	478
canvas.uw.edu	IPV4	52.20.24.113 54.165.152.84 34.228.243.87	60000	2017-10-04 23:17:02.292	478
chatenabled.mail.google.com	IPV4	216.58.216.167	69000	2017-10-04 23:17:09.086	478
clients2.google.com	IPV4	216.58.216.174	110000	2017-10-04 23:17:50.097	478
clients4.google.com	IPV4	216.58.216.174	90000	2017-10-04 23:17:50.645	478
clients5.google.com	IPV4	216.58.216.174	106000	2017-10-04 23:17:50.617	478
clients6.google.com	IPV4	216.58.216.174	112000	2017-10-04 23:17:50.672	478
collector.githubapp.com	IPV4	52.86.68.196 52.207.199.132 34.193.121.222	60000	2017-10-04 23:16:56.875	478
courses.cs.washington.edu	IPV4	128.208.1.193	86400000	2017-10-05 23:16:03.164	478

We check this before doing a DNS call

Record types

- Start of authority (SOA)
  - Details of server that supplied information, administrator of the zone, current version of data
- IP addresses (A and AAAA, IPv4 and IPv6)
- SMTP (MX)
- Name servers (NS)
- Reverse DNS lookup (PTR)
- Domain name alias (CNAME)

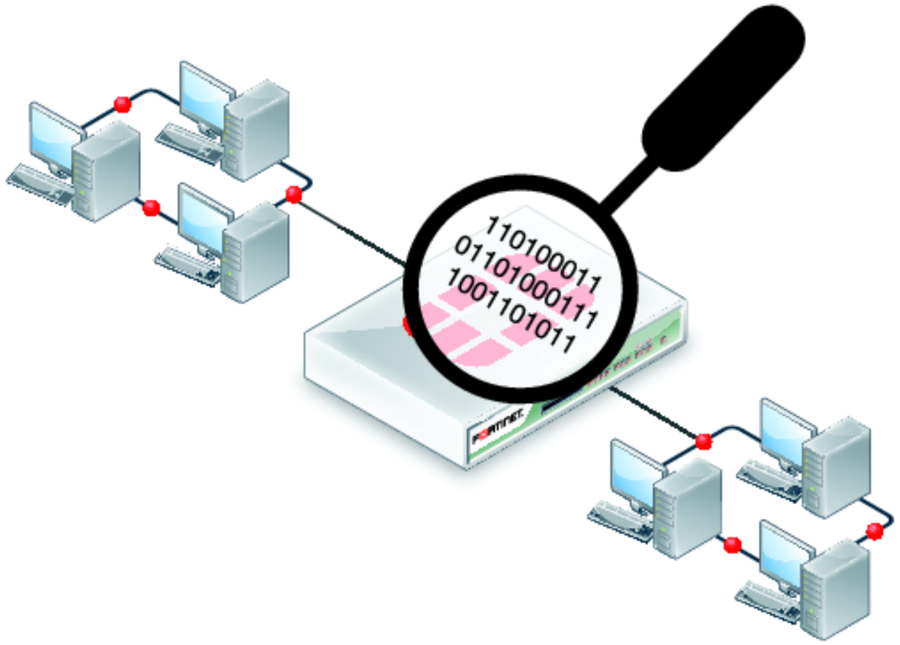


```
NAME                        TYPE   VALUE
--------------------------------------------------
bar.example.com.            CNAME  foo.example.com.
foo.example.com.            A      192.0.2.23
```

What happens when you type google.com into your browser and press enter?

https://github.com/alex/what-happens-when

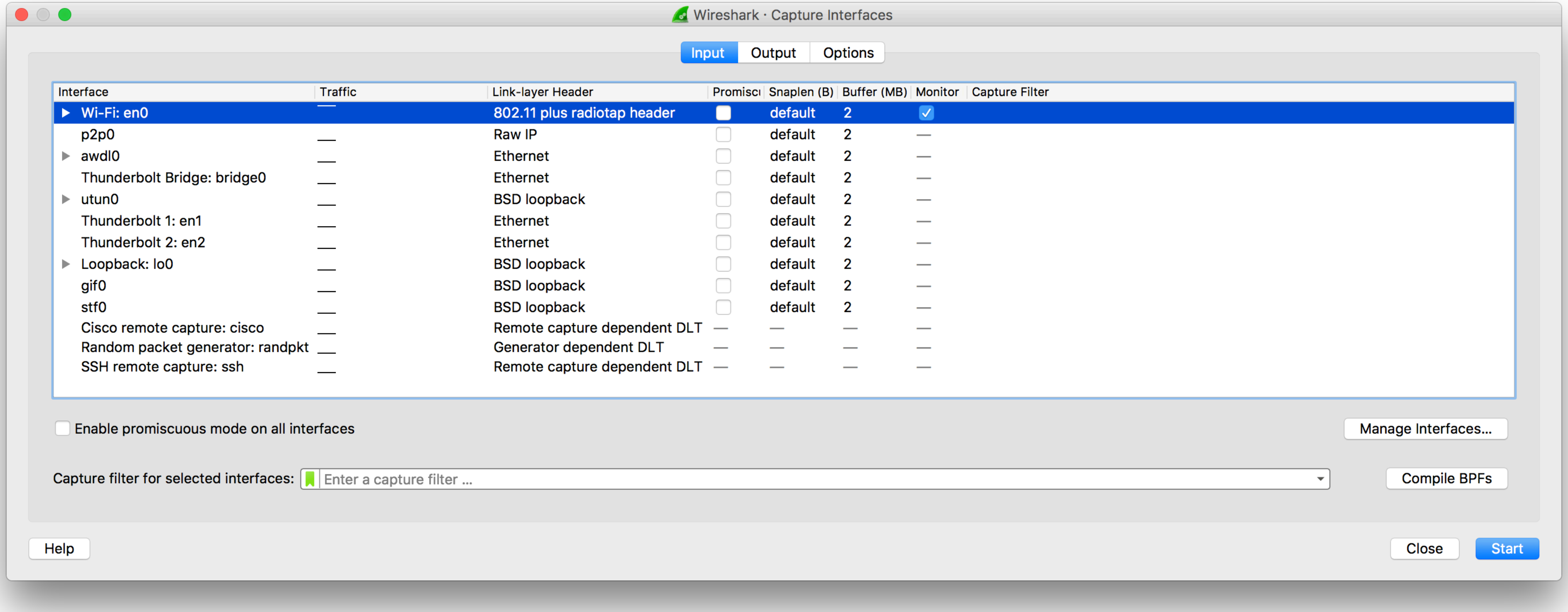
Wireshark



- Network debugger
- See details of all packets being sent around you

Wireshark

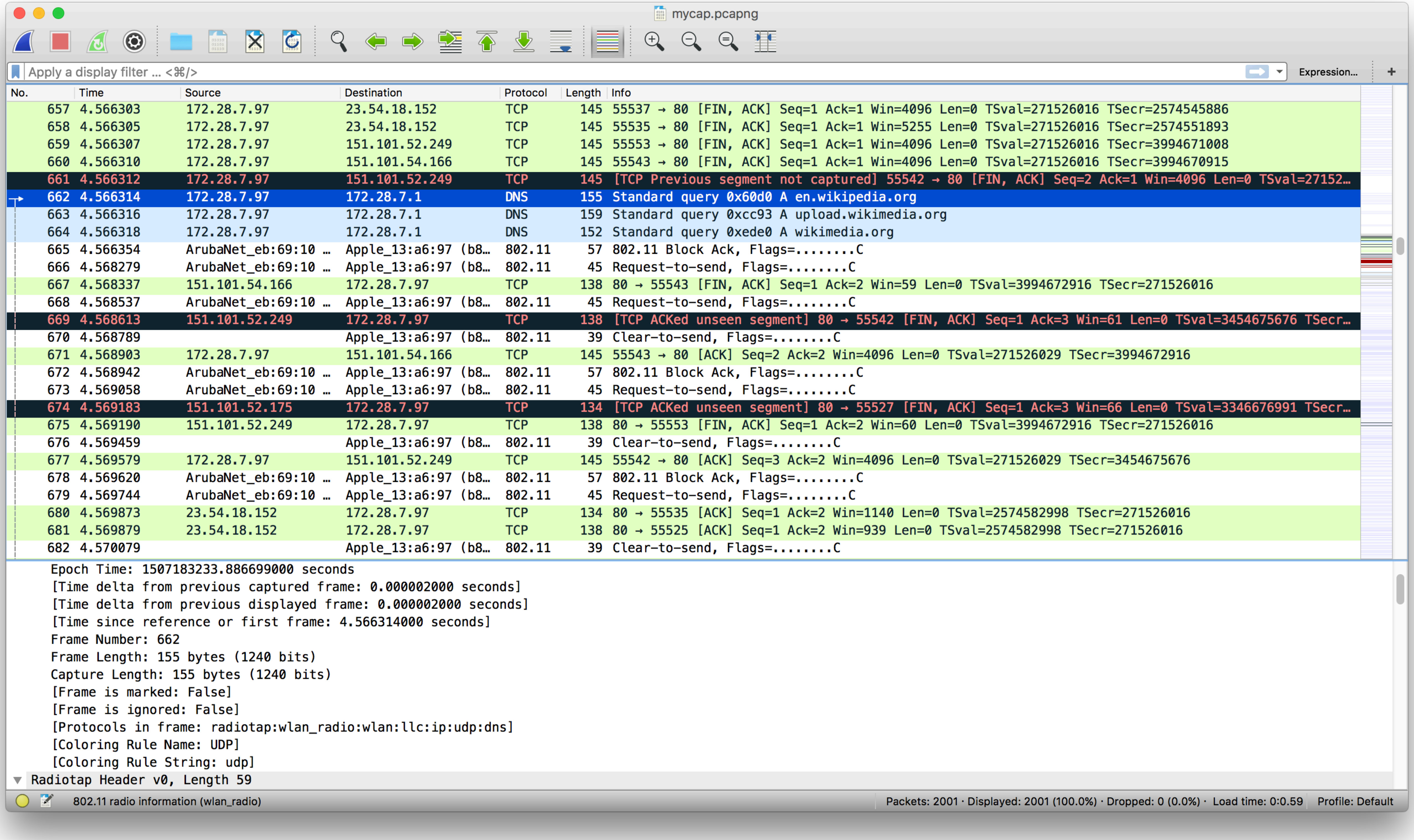
- Monitor mode:
  - Capture all wireless traffic, without having to associate with an AP.
  - You can see corrupted packets that don’t pass CRC
  - You cannot transmit in monitor mode (typically).
- Promiscuous mode:
  - WNIC forwards traffic to CPU.
  - WNIC typically drops all packets intended for others. Now you can look at broadcast messages intended for other parties



Interface	Traffic	Link-layer Header	Promiscı	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
▶ Wi-Fi: en0	—	802.11 plus radiotap header	☐	default	2	☑	
p2p0	—	Raw IP	☐	default	2	—	
▶ awdl0	—	Ethernet	☐	default	2	—	
Thunderbolt Bridge: bridge0	—	Ethernet	☐	default	2	—	
▶ utun0	—	BSD loopback	☐	default	2	—	
Thunderbolt 1: en1	—	Ethernet	☐	default	2	—	
Thunderbolt 2: en2	—	Ethernet	☐	default	2	—	
▶ Loopback: lo0	—	BSD loopback	☐	default	2	—	
gif0	—	BSD loopback	☐	default	2	—	
stf0	—	BSD loopback	☐	default	2	—	
Cisco remote capture: cisco	—	Remote capture dependent DLT	—	—	—	—	
Random packet generator: randpkt	—	Generator dependent DLT	—	—	—	—	
SSH remote capture: ssh	—	Remote capture dependent DLT	—	—	—	—	

☐ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...



```
No.  Time      Source              Destination         Protocol Length Info
 657 4.566303  172.28.7.97         23.54.18.152        TCP       145 55537 → 80 [FIN, ACK] Seq=1 Ack=1 Win=4096 Len=0 TSval=271526016 TSecr=2574545886
 658 4.566305  172.28.7.97         23.54.18.152        TCP       145 55535 → 80 [FIN, ACK] Seq=1 Ack=1 Win=5255 Len=0 TSval=271526016 TSecr=2574551893
 659 4.566307  172.28.7.97         151.101.52.249      TCP       145 55553 → 80 [FIN, ACK] Seq=1 Ack=1 Win=4096 Len=0 TSval=271526016 TSecr=3994671008
 660 4.566310  172.28.7.97         151.101.54.166      TCP       145 55543 → 80 [FIN, ACK] Seq=1 Ack=1 Win=4096 Len=0 TSval=271526016 TSecr=3994670915
 661 4.566312  172.28.7.97         151.101.52.249      TCP       145 [TCP Previous segment not captured] 55542 → 80 [FIN, ACK] Seq=2 Ack=1 Win=4096 Len=0 TSval=27152…
 662 4.566314  172.28.7.97         172.28.7.1          DNS       155 Standard query 0x60d0 A en.wikipedia.org
 663 4.566316  172.28.7.97         172.28.7.1          DNS       159 Standard query 0xcc93 A upload.wikimedia.org
 664 4.566318  172.28.7.97         172.28.7.1          DNS       152 Standard query 0xede0 A wikimedia.org
 665 4.566354  ArubaNet_eb:69:10 … Apple_13:a6:97 (b8… 802.11     57 802.11 Block Ack, Flags=........C
 666 4.568279  ArubaNet_eb:69:10 … Apple_13:a6:97 (b8… 802.11     45 Request-to-send, Flags=........C
 667 4.568337  151.101.54.166      172.28.7.97         TCP       138 80 → 55543 [FIN, ACK] Seq=1 Ack=2 Win=59 Len=0 TSval=3994672916 TSecr=271526016
 668 4.568537  ArubaNet_eb:69:10 … Apple_13:a6:97 (b8… 802.11     45 Request-to-send, Flags=........C
 669 4.568613  151.101.52.249      172.28.7.97         TCP       138 [TCP ACKed unseen segment] 80 → 55542 [FIN, ACK] Seq=1 Ack=3 Win=61 Len=0 TSval=3454675676 TSecr…
 670 4.568789                      Apple_13:a6:97 (b8… 802.11     39 Clear-to-send, Flags=........C
 671 4.568903  172.28.7.97         151.101.54.166      TCP       145 55543 → 80 [ACK] Seq=2 Ack=2 Win=4096 Len=0 TSval=271526029 TSecr=3994672916
 672 4.568942  ArubaNet_eb:69:10 … Apple_13:a6:97 (b8… 802.11     57 802.11 Block Ack, Flags=........C
 673 4.569058  ArubaNet_eb:69:10 … Apple_13:a6:97 (b8… 802.11     45 Request-to-send, Flags=........C
 674 4.569183  151.101.52.175      172.28.7.97         TCP       134 [TCP ACKed unseen segment] 80 → 55527 [FIN, ACK] Seq=1 Ack=3 Win=66 Len=0 TSval=3346676991 TSecr…
 675 4.569190  151.101.52.249      172.28.7.97         TCP       138 80 → 55553 [FIN, ACK] Seq=1 Ack=2 Win=60 Len=0 TSval=3994672916 TSecr=271526016
 676 4.569459                      Apple_13:a6:97 (b8… 802.11     39 Clear-to-send, Flags=........C
 677 4.569579  172.28.7.97         151.101.52.249      TCP       145 55542 → 80 [ACK] Seq=3 Ack=2 Win=4096 Len=0 TSval=271526029 TSecr=3454675676
 678 4.569620  ArubaNet_eb:69:10 … Apple_13:a6:97 (b8… 802.11     57 802.11 Block Ack, Flags=........C
 679 4.569744  ArubaNet_eb:69:10 … Apple_13:a6:97 (b8… 802.11     45 Request-to-send, Flags=........C
 680 4.569873  23.54.18.152        172.28.7.97         TCP       134 80 → 55535 [ACK] Seq=1 Ack=2 Win=1140 Len=0 TSval=2574582998 TSecr=271526016
 681 4.569879  23.54.18.152        172.28.7.97         TCP       138 80 → 55525 [ACK] Seq=1 Ack=2 Win=939 Len=0 TSval=2574582998 TSecr=271526016
 682 4.570079                      Apple_13:a6:97 (b8… 802.11     39 Clear-to-send, Flags=........C
```

```
    Epoch Time: 1507183233.886699000 seconds
    [Time delta from previous captured frame: 0.000002000 seconds]
    [Time delta from previous displayed frame: 0.000002000 seconds]
    [Time since reference or first frame: 4.566314000 seconds]
    Frame Number: 662
    Frame Length: 155 bytes (1240 bits)
    Capture Length: 155 bytes (1240 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: radiotap:wlan_radio:wlan:llc:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
▼ Radiotap Header v0, Length 59
```

```
802.11 radio information (wlan_radio)    Packets: 2001 · Displayed: 2001 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.59    Profile: Default
```

Filters

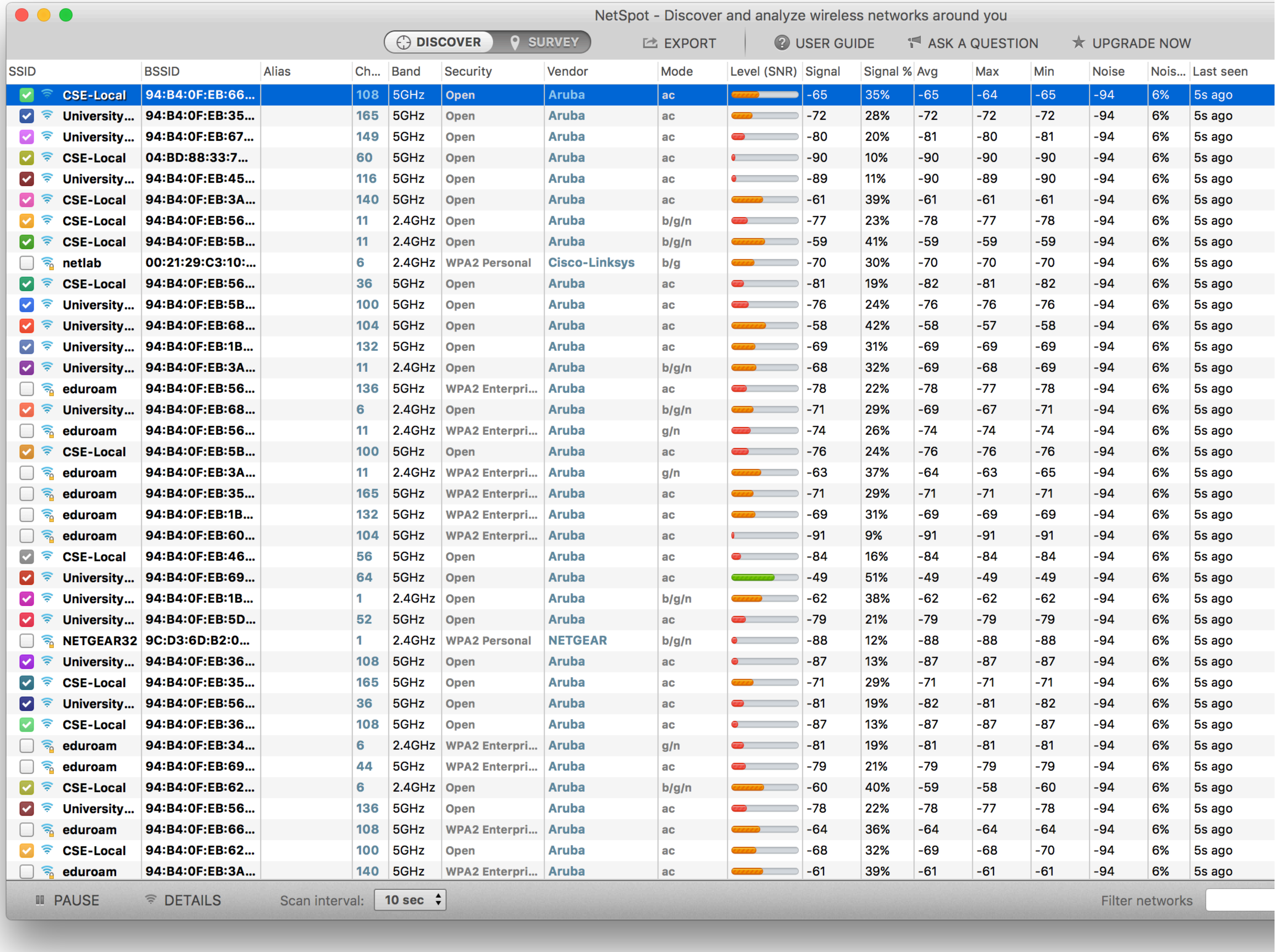
- Transport:
  tcp.srcport ==80
  tcp.port==80

- IP:
  ip.dst==172.28.7.97
  ip.src==172.28.7.97

- Link:
  wlan.addr==00:11:22:33:44:55
  wlan.sa==00:11:22:33:44:55

- Protocol:
  dns
  tcp
  udp

NetSpot



SSID	BSSID	Alias	Ch...	Band	Security	Vendor	Mode	Level (SNR)	Signal	Signal %	Avg	Max	Min	Noise	Nois...	Last seen
☑ CSE-Local	94:B4:0F:EB:66...		108	5GHz	Open	Aruba	ac		-65	35%	-65	-64	-65	-94	6%	5s ago
☑ University...	94:B4:0F:EB:35...		165	5GHz	Open	Aruba	ac		-72	28%	-72	-72	-72	-94	6%	5s ago
☑ University...	94:B4:0F:EB:67...		149	5GHz	Open	Aruba	ac		-80	20%	-81	-80	-81	-94	6%	5s ago
☑ CSE-Local	04:BD:88:33:7...		60	5GHz	Open	Aruba	ac		-90	10%	-90	-90	-90	-94	6%	5s ago
☑ University...	94:B4:0F:EB:45...		116	5GHz	Open	Aruba	ac		-89	11%	-90	-89	-90	-94	6%	5s ago
☑ CSE-Local	94:B4:0F:EB:3A...		140	5GHz	Open	Aruba	ac		-61	39%	-61	-61	-61	-94	6%	5s ago
☑ CSE-Local	94:B4:0F:EB:56...		11	2.4GHz	Open	Aruba	b/g/n		-77	23%	-78	-77	-78	-94	6%	5s ago
☑ CSE-Local	94:B4:0F:EB:5B...		11	2.4GHz	Open	Aruba	b/g/n		-59	41%	-59	-59	-59	-94	6%	5s ago
☐ netlab	00:21:29:C3:10:...		6	2.4GHz	WPA2 Personal	Cisco-Linksys	b/g		-70	30%	-70	-70	-70	-94	6%	5s ago
☑ CSE-Local	94:B4:0F:EB:56...		36	5GHz	Open	Aruba	ac		-81	19%	-82	-81	-82	-94	6%	5s ago
☑ University...	94:B4:0F:EB:5B...		100	5GHz	Open	Aruba	ac		-76	24%	-76	-76	-76	-94	6%	5s ago
☑ University...	94:B4:0F:EB:68...		104	5GHz	Open	Aruba	ac		-58	42%	-58	-57	-58	-94	6%	5s ago
☑ University...	94:B4:0F:EB:1B...		132	5GHz	Open	Aruba	ac		-69	31%	-69	-69	-69	-94	6%	5s ago
☑ University...	94:B4:0F:EB:3A...		11	2.4GHz	Open	Aruba	b/g/n		-68	32%	-69	-68	-69	-94	6%	5s ago
☐ eduroam	94:B4:0F:EB:56...		136	5GHz	WPA2 Enterpri...	Aruba	ac		-78	22%	-78	-77	-78	-94	6%	5s ago
☑ University...	94:B4:0F:EB:68...		6	2.4GHz	Open	Aruba	b/g/n		-71	29%	-69	-67	-71	-94	6%	5s ago
☐ eduroam	94:B4:0F:EB:56...		11	2.4GHz	WPA2 Enterpri...	Aruba	g/n		-74	26%	-74	-74	-74	-94	6%	5s ago
☑ CSE-Local	94:B4:0F:EB:5B...		100	5GHz	Open	Aruba	ac		-76	24%	-76	-76	-76	-94	6%	5s ago
☐ eduroam	94:B4:0F:EB:3A...		11	2.4GHz	WPA2 Enterpri...	Aruba	g/n		-63	37%	-64	-63	-65	-94	6%	5s ago
☐ eduroam	94:B4:0F:EB:35...		165	5GHz	WPA2 Enterpri...	Aruba	ac		-71	29%	-71	-71	-71	-94	6%	5s ago
☐ eduroam	94:B4:0F:EB:1B...		132	5GHz	WPA2 Enterpri...	Aruba	ac		-69	31%	-69	-69	-69	-94	6%	5s ago
☐ eduroam	94:B4:0F:EB:60...		104	5GHz	WPA2 Enterpri...	Aruba	ac		-91	9%	-91	-91	-91	-94	6%	5s ago
☑ CSE-Local	94:B4:0F:EB:46...		56	5GHz	Open	Aruba	ac		-84	16%	-84	-84	-84	-94	6%	5s ago
☑ University...	94:B4:0F:EB:69...		64	5GHz	Open	Aruba	ac		-49	51%	-49	-49	-49	-94	6%	5s ago
☑ University...	94:B4:0F:EB:1B...		1	2.4GHz	Open	Aruba	b/g/n		-62	38%	-62	-62	-62	-94	6%	5s ago
☑ University...	94:B4:0F:EB:5D...		52	5GHz	Open	Aruba	ac		-79	21%	-79	-79	-79	-94	6%	5s ago
☐ NETGEAR32	9C:D3:6D:B2:0...		1	2.4GHz	WPA2 Personal	NETGEAR	b/g/n		-88	12%	-88	-88	-88	-94	6%	5s ago
☑ University...	94:B4:0F:EB:36...		108	5GHz	Open	Aruba	ac		-87	13%	-87	-87	-87	-94	6%	5s ago
☑ CSE-Local	94:B4:0F:EB:35...		165	5GHz	Open	Aruba	ac		-71	29%	-71	-71	-71	-94	6%	5s ago
☑ University...	94:B4:0F:EB:56...		36	5GHz	Open	Aruba	ac		-81	19%	-82	-81	-82	-94	6%	5s ago
☑ CSE-Local	94:B4:0F:EB:36...		108	5GHz	Open	Aruba	ac		-87	13%	-87	-87	-87	-94	6%	5s ago
☐ eduroam	94:B4:0F:EB:34...		6	2.4GHz	WPA2 Enterpri...	Aruba	g/n		-81	19%	-81	-81	-81	-94	6%	5s ago
☐ eduroam	94:B4:0F:EB:69...		44	5GHz	WPA2 Enterpri...	Aruba	ac		-79	21%	-79	-79	-79	-94	6%	5s ago
☑ CSE-Local	94:B4:0F:EB:62...		6	2.4GHz	Open	Aruba	b/g/n		-60	40%	-59	-58	-60	-94	6%	5s ago
☑ University...	94:B4:0F:EB:56...		136	5GHz	Open	Aruba	ac		-78	22%	-78	-77	-78	-94	6%	5s ago
☐ eduroam	94:B4:0F:EB:66...		108	5GHz	WPA2 Enterpri...	Aruba	ac		-64	36%	-64	-64	-64	-94	6%	5s ago
☑ CSE-Local	94:B4:0F:EB:62...		100	5GHz	Open	Aruba	ac		-68	32%	-69	-68	-70	-94	6%	5s ago
☐ eduroam	94:B4:0F:EB:3A...		140	5GHz	WPA2 Enterpri...	Aruba	ac		-61	39%	-61	-61	-61	-94	6%	5s ago

Scan interval: 10 sec

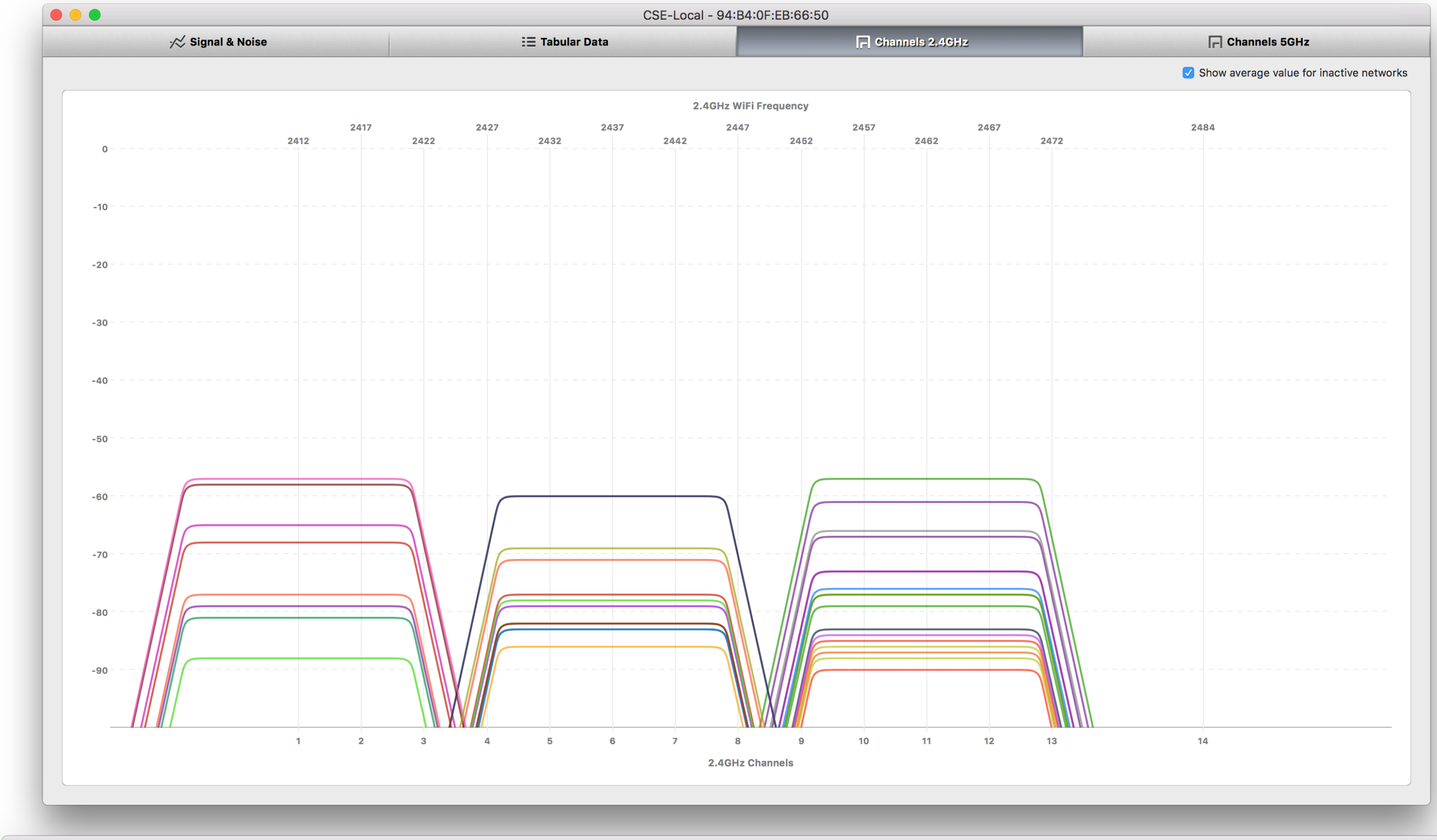
-60 is “good” for Wi-Fi
Disconnects at around -90dBm

$$C = B \log_2 \left(1 + \frac{S}{N}\right)$$

Max data Rate

20MHz

Convert SNR from dB value



CSE-Local - 94:B4:0F:EB:66:50

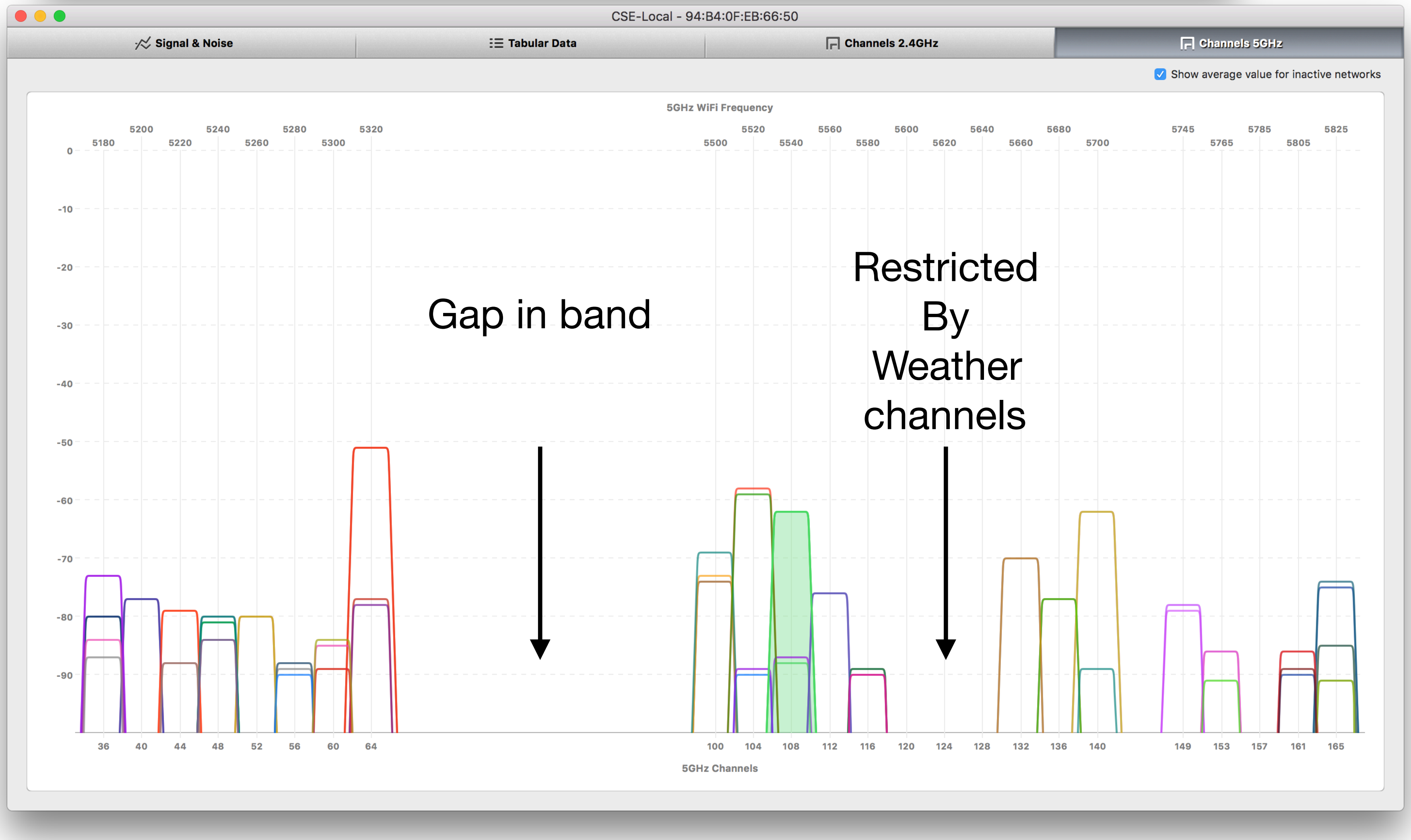
☑ Show average value for inactive networks

2.4GHz:

Three non-overlapping channels in the US

1, 6, 11

20MHz bandwidths



CSE-Local - 94:B4:0F:EB:66:50

☑ Show average value for inactive networks

Gap in band

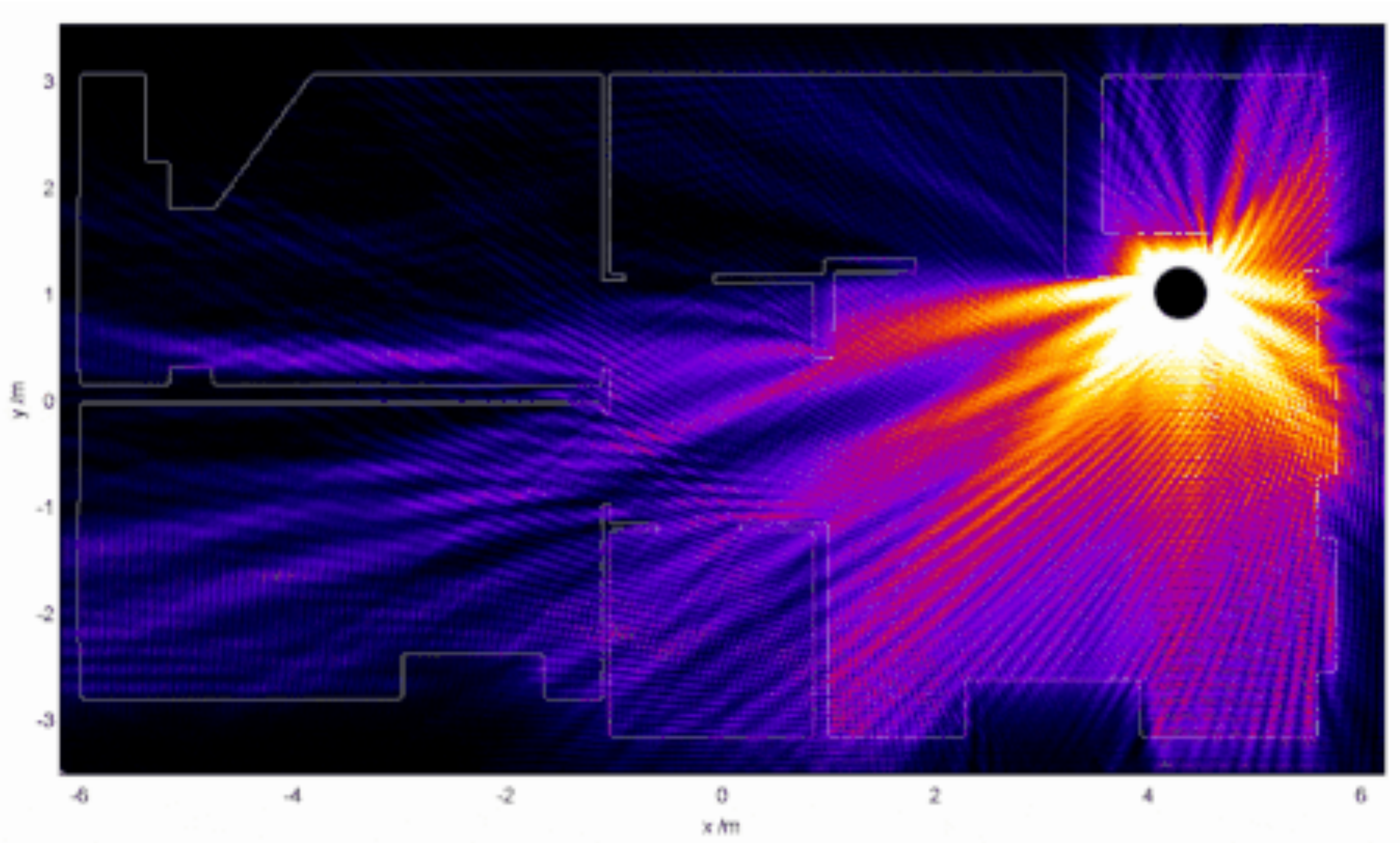
Restricted By Weather channels

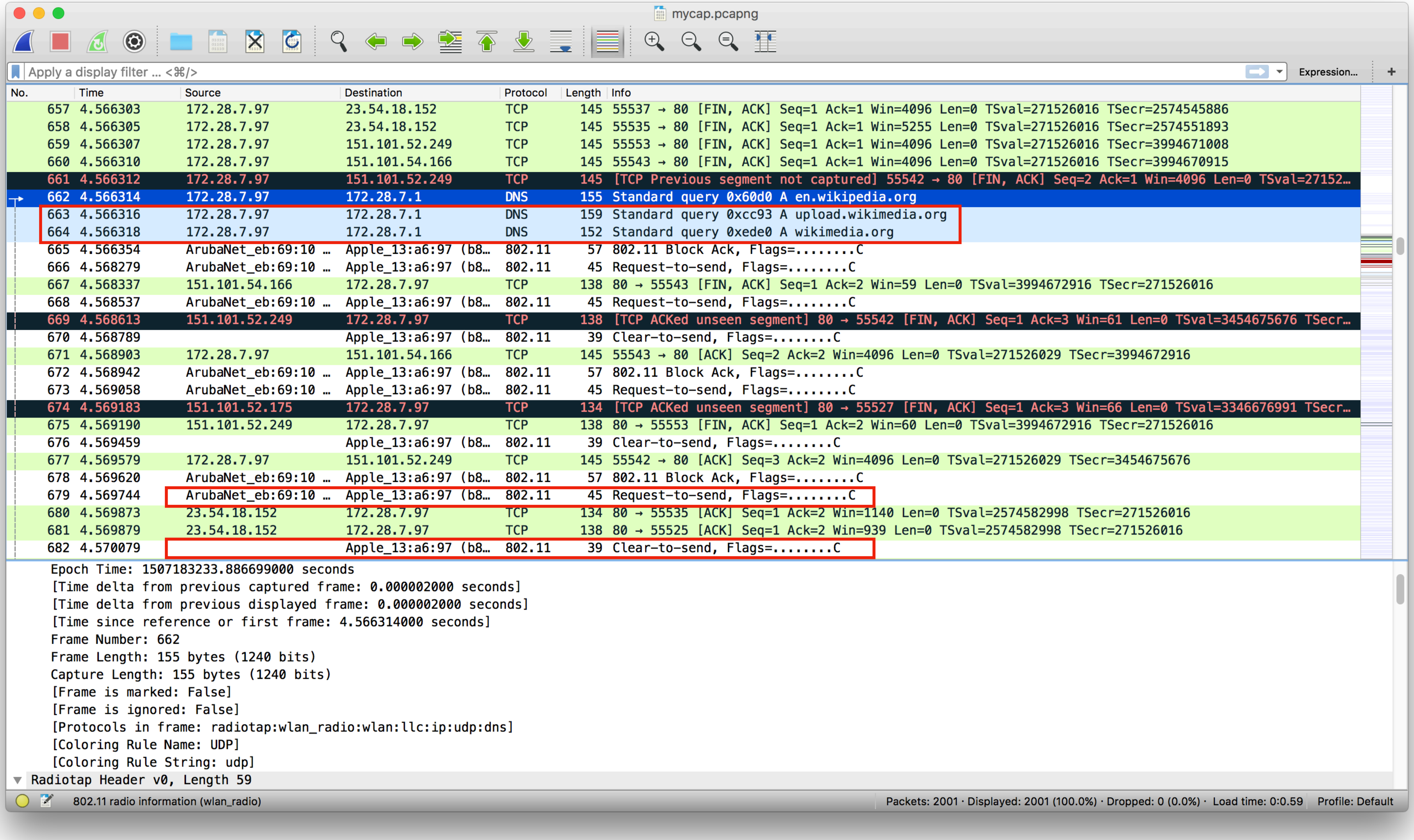
5Hz:

Variable bandwidths:

20, 40, 80MHz

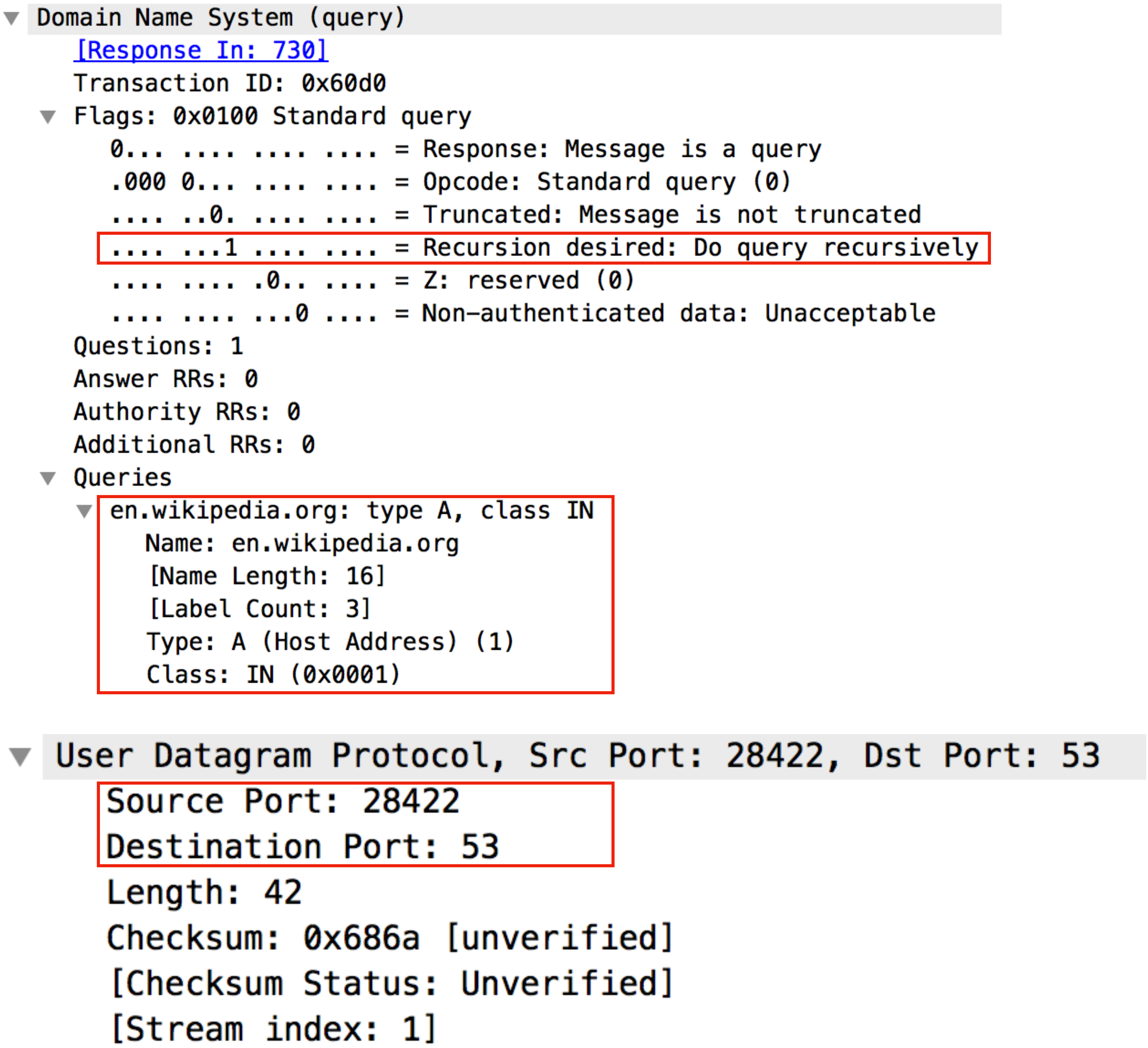
More room


3
2
1
0
-1
-2
-3
y /m
-6
-4
-2
0
2
4
6
x /m


mycap.pcapng
Apply a display filter ... <⌘/>
Expression...
+
802.11 radio information (wlan_radio)
Packets: 2001 · Displayed: 2001 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.59
Profile: Default

```
No.   Time      Source               Destination          Protocol  Length  Info
657  4.566303  172.28.7.97          23.54.18.152         TCP        145  55537 → 80 [FIN, ACK] Seq=1 Ack=1 Win=4096 Len=0 TSval=271526016 TSecr=2574545886
658  4.566305  172.28.7.97          23.54.18.152         TCP        145  55535 → 80 [FIN, ACK] Seq=1 Ack=1 Win=5255 Len=0 TSval=271526016 TSecr=2574551893
659  4.566307  172.28.7.97          151.101.52.249       TCP        145  55553 → 80 [FIN, ACK] Seq=1 Ack=1 Win=4096 Len=0 TSval=271526016 TSecr=3994671008
660  4.566310  172.28.7.97          151.101.54.166       TCP        145  55543 → 80 [FIN, ACK] Seq=1 Ack=1 Win=4096 Len=0 TSval=271526016 TSecr=3994670915
661  4.566312  172.28.7.97          151.101.52.249       TCP        145  [TCP Previous segment not captured] 55542 → 80 [FIN, ACK] Seq=2 Ack=1 Win=4096 Len=0 TSval=27152…
662  4.566314  172.28.7.97          172.28.7.1           DNS        155  Standard query 0x60d0 A en.wikipedia.org
663  4.566316  172.28.7.97          172.28.7.1           DNS        159  Standard query 0xcc93 A upload.wikimedia.org
664  4.566318  172.28.7.97          172.28.7.1           DNS        152  Standard query 0xede0 A wikimedia.org
665  4.566354  ArubaNet_eb:69:10 …  Apple_13:a6:97 (b8…  802.11      57  802.11 Block Ack, Flags=........C
666  4.568279  ArubaNet_eb:69:10 …  Apple_13:a6:97 (b8…  802.11      45  Request-to-send, Flags=........C
667  4.568337  151.101.54.166       172.28.7.97          TCP        138  80 → 55543 [FIN, ACK] Seq=1 Ack=2 Win=59 Len=0 TSval=3994672916 TSecr=271526016
668  4.568537  ArubaNet_eb:69:10 …  Apple_13:a6:97 (b8…  802.11      45  Request-to-send, Flags=........C
669  4.568613  151.101.52.249       172.28.7.97          TCP        138  [TCP ACKed unseen segment] 80 → 55542 [FIN, ACK] Seq=1 Ack=3 Win=61 Len=0 TSval=3454675676 TSecr…
670  4.568789                       Apple_13:a6:97 (b8…  802.11      39  Clear-to-send, Flags=........C
671  4.568903  172.28.7.97          151.101.54.166       TCP        145  55543 → 80 [ACK] Seq=2 Ack=2 Win=4096 Len=0 TSval=271526029 TSecr=3994672916
672  4.568942  ArubaNet_eb:69:10 …  Apple_13:a6:97 (b8…  802.11      57  802.11 Block Ack, Flags=........C
673  4.569058  ArubaNet_eb:69:10 …  Apple_13:a6:97 (b8…  802.11      45  Request-to-send, Flags=........C
674  4.569183  151.101.52.175       172.28.7.97          TCP        134  [TCP ACKed unseen segment] 80 → 55527 [FIN, ACK] Seq=1 Ack=3 Win=66 Len=0 TSval=3346676991 TSecr…
675  4.569190  151.101.52.249       172.28.7.97          TCP        138  80 → 55553 [FIN, ACK] Seq=1 Ack=2 Win=60 Len=0 TSval=3994672916 TSecr=271526016
676  4.569459                       Apple_13:a6:97 (b8…  802.11      39  Clear-to-send, Flags=........C
677  4.569579  172.28.7.97          151.101.52.249       TCP        145  55542 → 80 [ACK] Seq=3 Ack=2 Win=4096 Len=0 TSval=271526029 TSecr=3454675676
678  4.569620  ArubaNet_eb:69:10 …  Apple_13:a6:97 (b8…  802.11      57  802.11 Block Ack, Flags=........C
679  4.569744  ArubaNet_eb:69:10 …  Apple_13:a6:97 (b8…  802.11      45  Request-to-send, Flags=........C
680  4.569873  23.54.18.152         172.28.7.97          TCP        134  80 → 55535 [ACK] Seq=1 Ack=2 Win=1140 Len=0 TSval=2574582998 TSecr=271526016
681  4.569879  23.54.18.152         172.28.7.97          TCP        138  80 → 55525 [ACK] Seq=1 Ack=2 Win=939 Len=0 TSval=2574582998 TSecr=271526016
682  4.570079                       Apple_13:a6:97 (b8…  802.11      39  Clear-to-send, Flags=........C
```

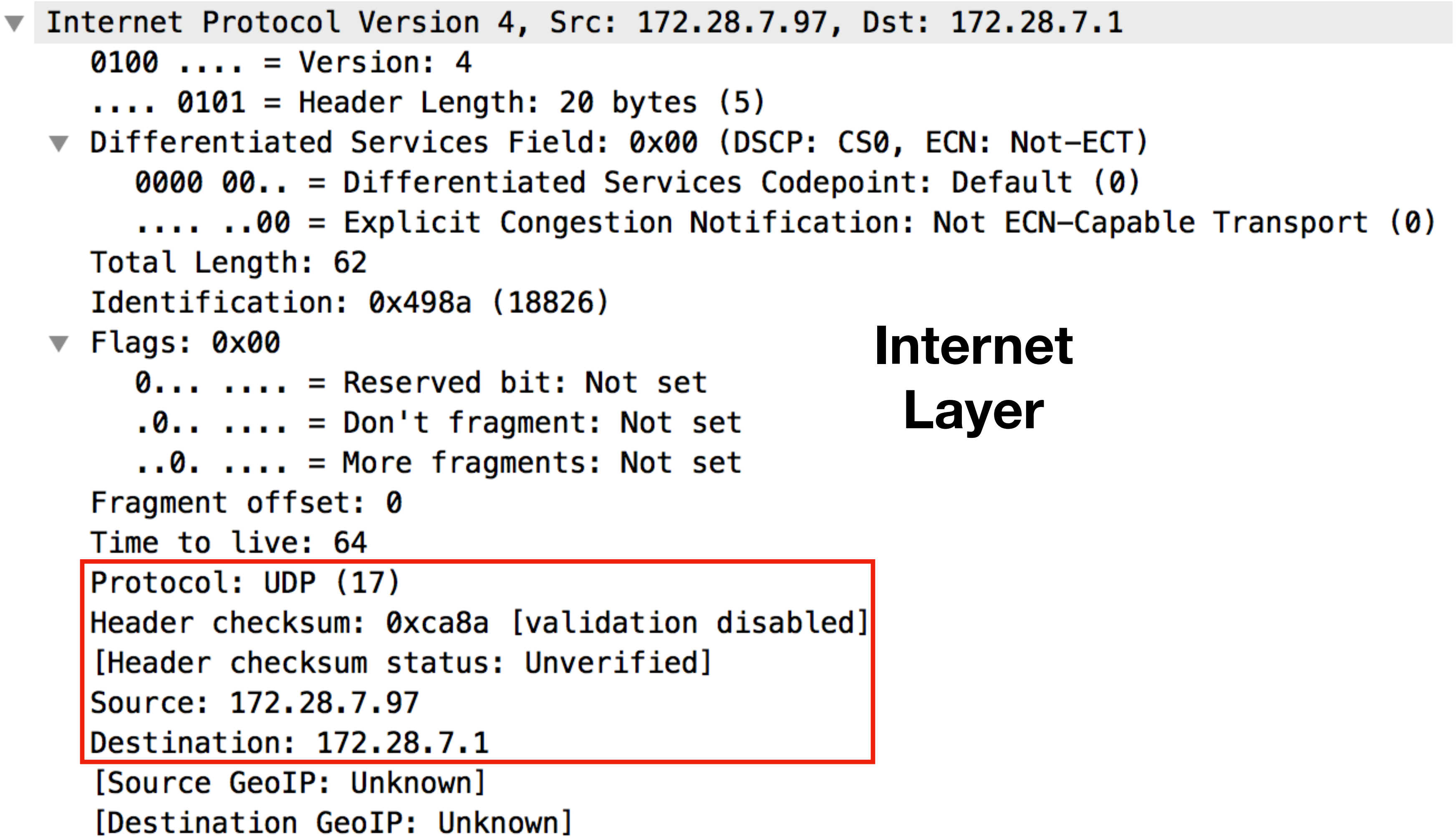
```
    Epoch Time: 1507183233.886699000 seconds
    [Time delta from previous captured frame: 0.000002000 seconds]
    [Time delta from previous displayed frame: 0.000002000 seconds]
    [Time since reference or first frame: 4.566314000 seconds]
    Frame Number: 662
    Frame Length: 155 bytes (1240 bits)
    Capture Length: 155 bytes (1240 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: radiotap:wlan_radio:wlan:llc:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
▼ Radiotap Header v0, Length 59
```



```
▼ Domain Name System (query)
    [Response In: 730]
    Transaction ID: 0x60d0
  ▼ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▼ en.wikipedia.org: type A, class IN
        Name: en.wikipedia.org
        [Name Length: 16]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)

▼ User Datagram Protocol, Src Port: 28422, Dst Port: 53
    Source Port: 28422
    Destination Port: 53
    Length: 42
    Checksum: 0x686a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
```

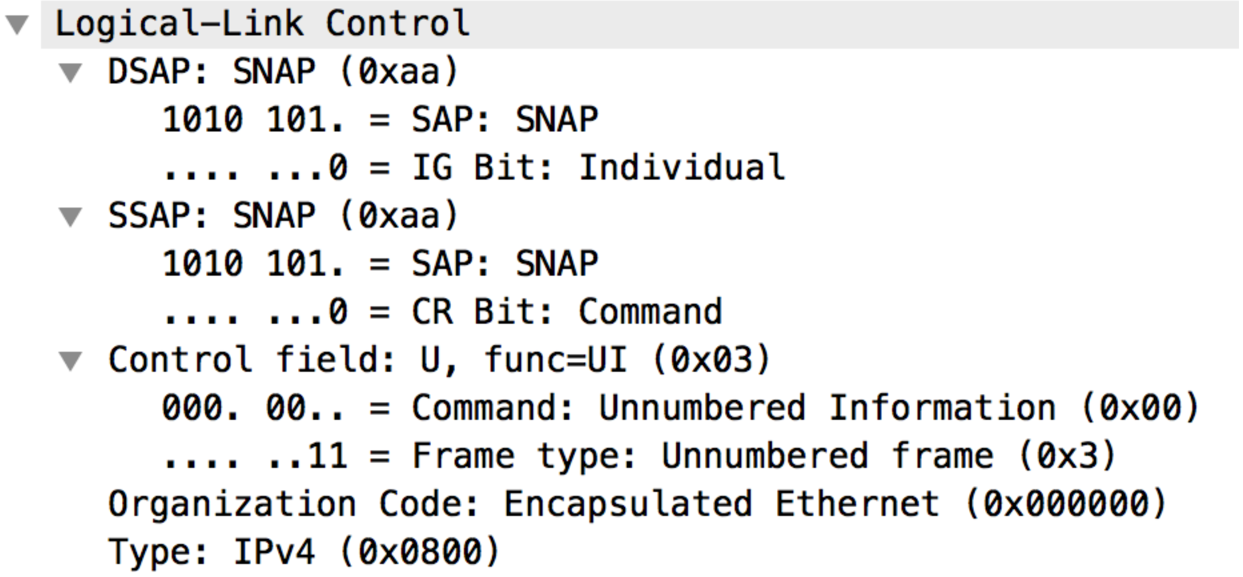
Application Layer

Transport Layer



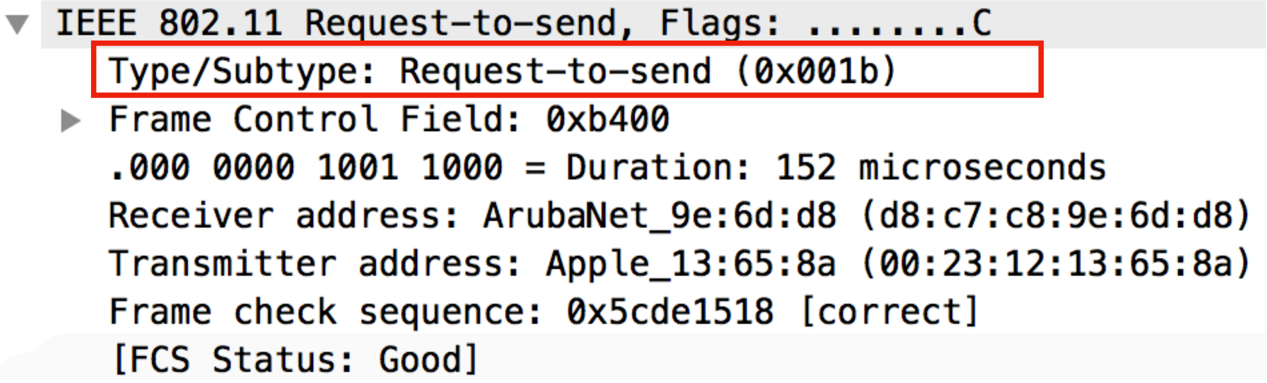
```
▼ Internet Protocol Version 4, Src: 172.28.7.97, Dst: 172.28.7.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 62
    Identification: 0x498a (18826)
  ▼ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0xca8a [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.28.7.97
    Destination: 172.28.7.1
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

Internet Layer

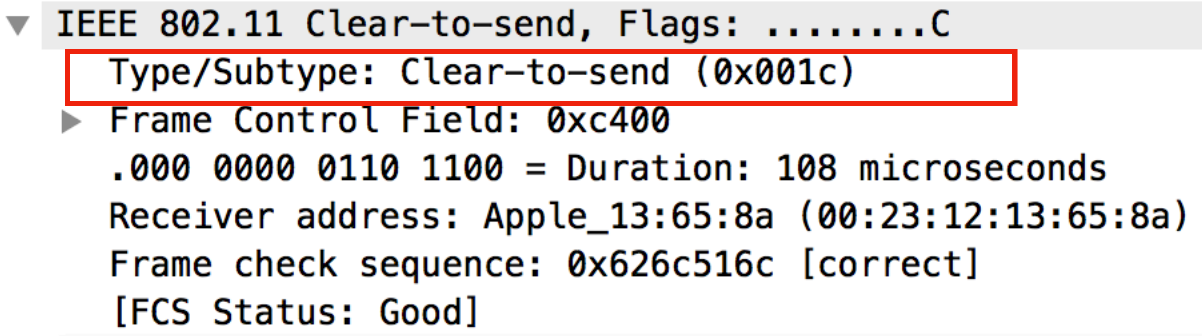


```
▼ Logical-Link Control
  ▼ DSAP: SNAP (0xaa)
      1010 101. = SAP: SNAP
      .... ...0 = IG Bit: Individual
  ▼ SSAP: SNAP (0xaa)
      1010 101. = SAP: SNAP
      .... ...0 = CR Bit: Command
  ▼ Control field: U, func=UI (0x03)
      000. 00.. = Command: Unnumbered Information (0x00)
      .... ..11 = Frame type: Unnumbered frame (0x3)
    Organization Code: Encapsulated Ethernet (0x000000)
    Type: IPv4 (0x0800)
```

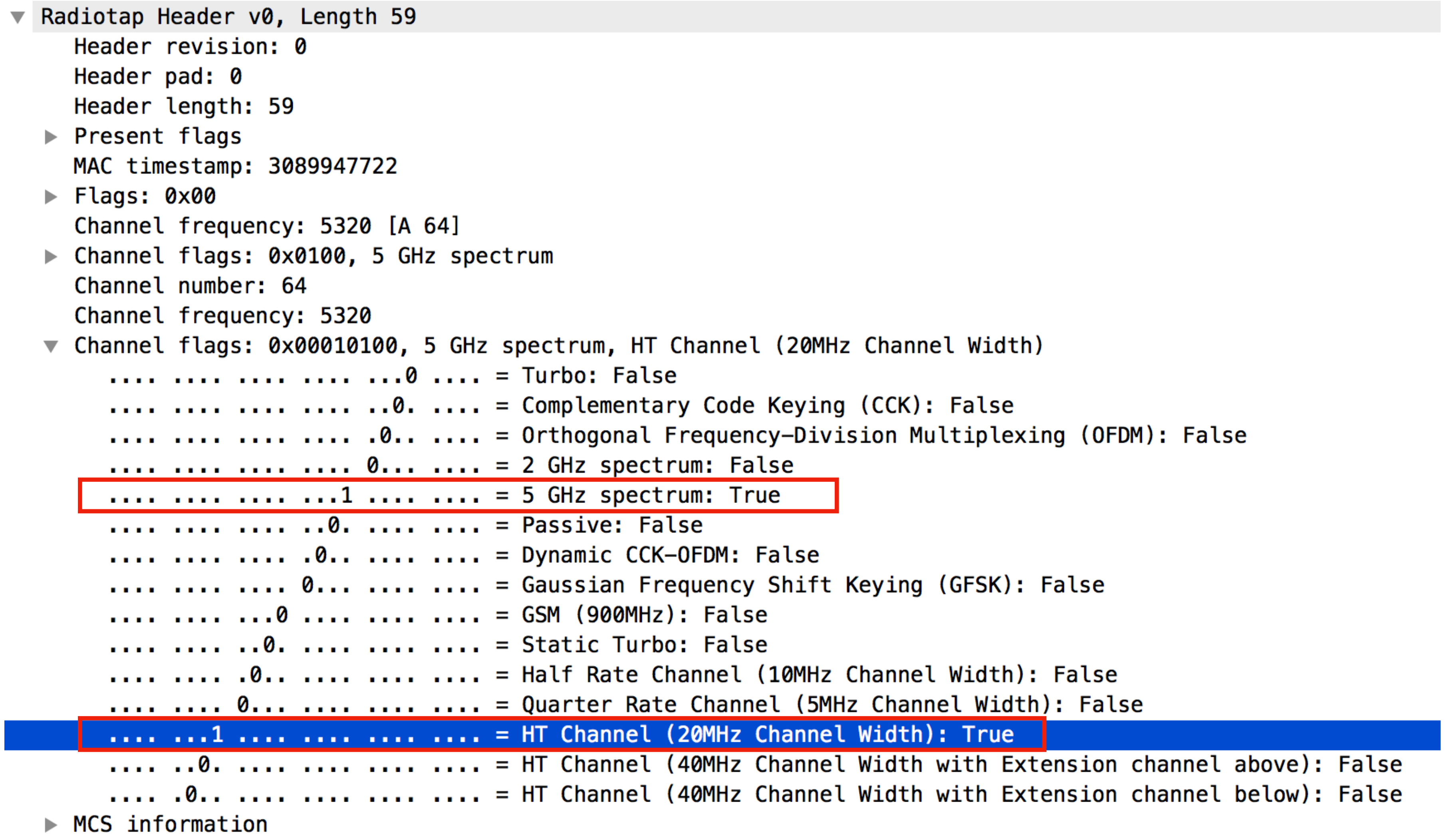
Link layer



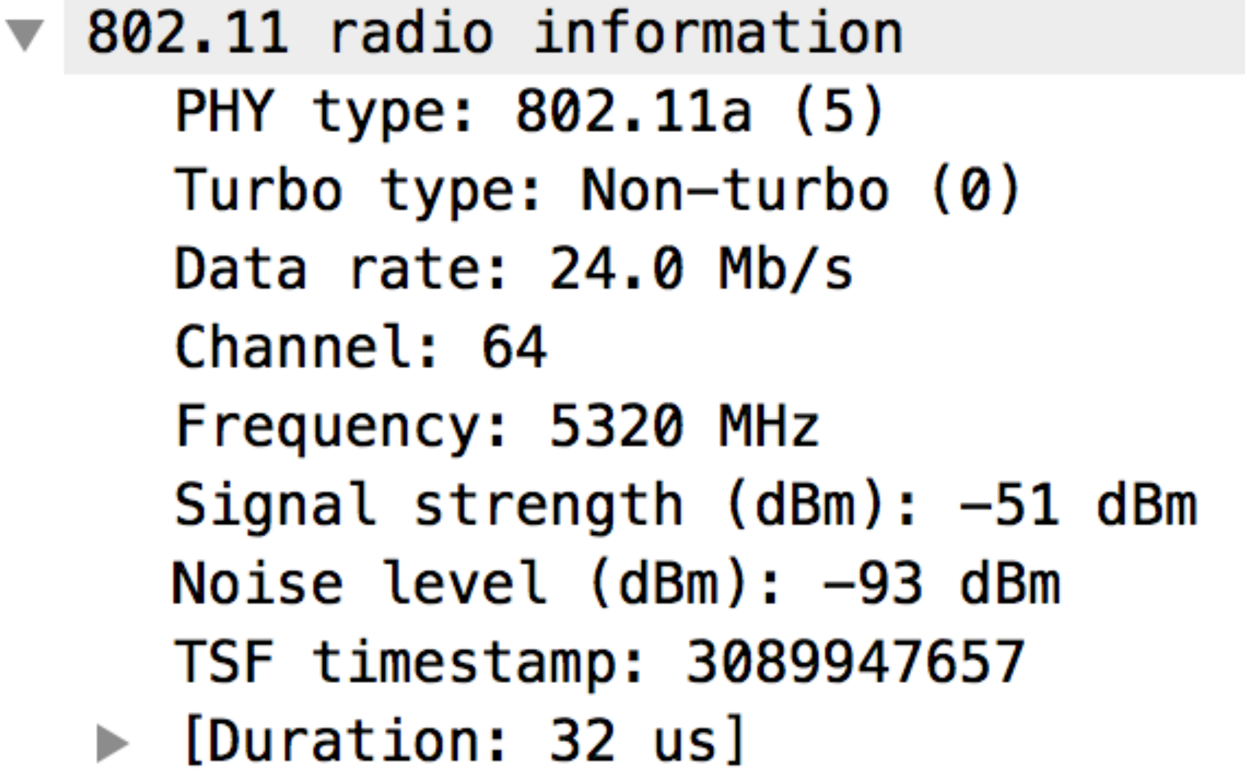
```
▼ IEEE 802.11 Request-to-send, Flags: ........C
    Type/Subtype: Request-to-send (0x001b)
  ▶ Frame Control Field: 0xb400
    .000 0000 1001 1000 = Duration: 152 microseconds
    Receiver address: ArubaNet_9e:6d:d8 (d8:c7:c8:9e:6d:d8)
    Transmitter address: Apple_13:65:8a (00:23:12:13:65:8a)
    Frame check sequence: 0x5cde1518 [correct]
    [FCS Status: Good]
```



```
▼ IEEE 802.11 Clear-to-send, Flags: ........C
    Type/Subtype: Clear-to-send (0x001c)
  ▶ Frame Control Field: 0xc400
    .000 0000 0110 1100 = Duration: 108 microseconds
    Receiver address: Apple_13:65:8a (00:23:12:13:65:8a)
    Frame check sequence: 0x626c516c [correct]
    [FCS Status: Good]
```



```
▼ Radiotap Header v0, Length 59
    Header revision: 0
    Header pad: 0
    Header length: 59
  ▶ Present flags
    MAC timestamp: 3089947722
  ▶ Flags: 0x00
    Channel frequency: 5320 [A 64]
  ▶ Channel flags: 0x0100, 5 GHz spectrum
    Channel number: 64
    Channel frequency: 5320
  ▼ Channel flags: 0x00010100, 5 GHz spectrum, HT Channel (20MHz Channel Width)
      .... .... .... .... ...0 .... = Turbo: False
      .... .... .... .... ..0. .... = Complementary Code Keying (CCK): False
      .... .... .... .... .0.. .... = Orthogonal Frequency-Division Multiplexing (OFDM): False
      .... .... .... .... 0... .... = 2 GHz spectrum: False
      .... .... .... ...1 .... .... = 5 GHz spectrum: True
      .... .... .... ..0. .... .... = Passive: False
      .... .... .... .0.. .... .... = Dynamic CCK-OFDM: False
      .... .... .... 0... .... .... = Gaussian Frequency Shift Keying (GFSK): False
      .... .... ...0 .... .... .... = GSM (900MHz): False
      .... .... ..0. .... .... .... = Static Turbo: False
      .... .... .0.. .... .... .... = Half Rate Channel (10MHz Channel Width): False
      .... .... 0... .... .... .... = Quarter Rate Channel (5MHz Channel Width): False
      .... ...1 .... .... .... .... = HT Channel (20MHz Channel Width): True
      .... ..0. .... .... .... .... = HT Channel (40MHz Channel Width with Extension channel above): False
      .... .0.. .... .... .... .... = HT Channel (40MHz Channel Width with Extension channel below): False
  ▶ MCS information
```



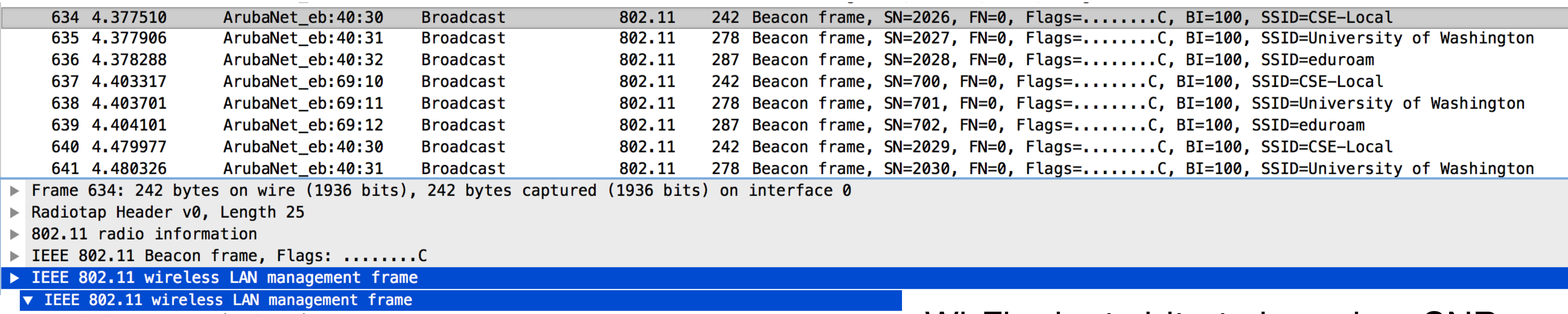
```
▼ 802.11 radio information
    PHY type: 802.11a (5)
    Turbo type: Non-turbo (0)
    Data rate: 24.0 Mb/s
    Channel: 64
    Frequency: 5320 MHz
    Signal strength (dBm): -51 dBm
    Noise level (dBm): -93 dBm
    TSF timestamp: 3089947657
  ▶ [Duration: 32 us]
```

Physical layer

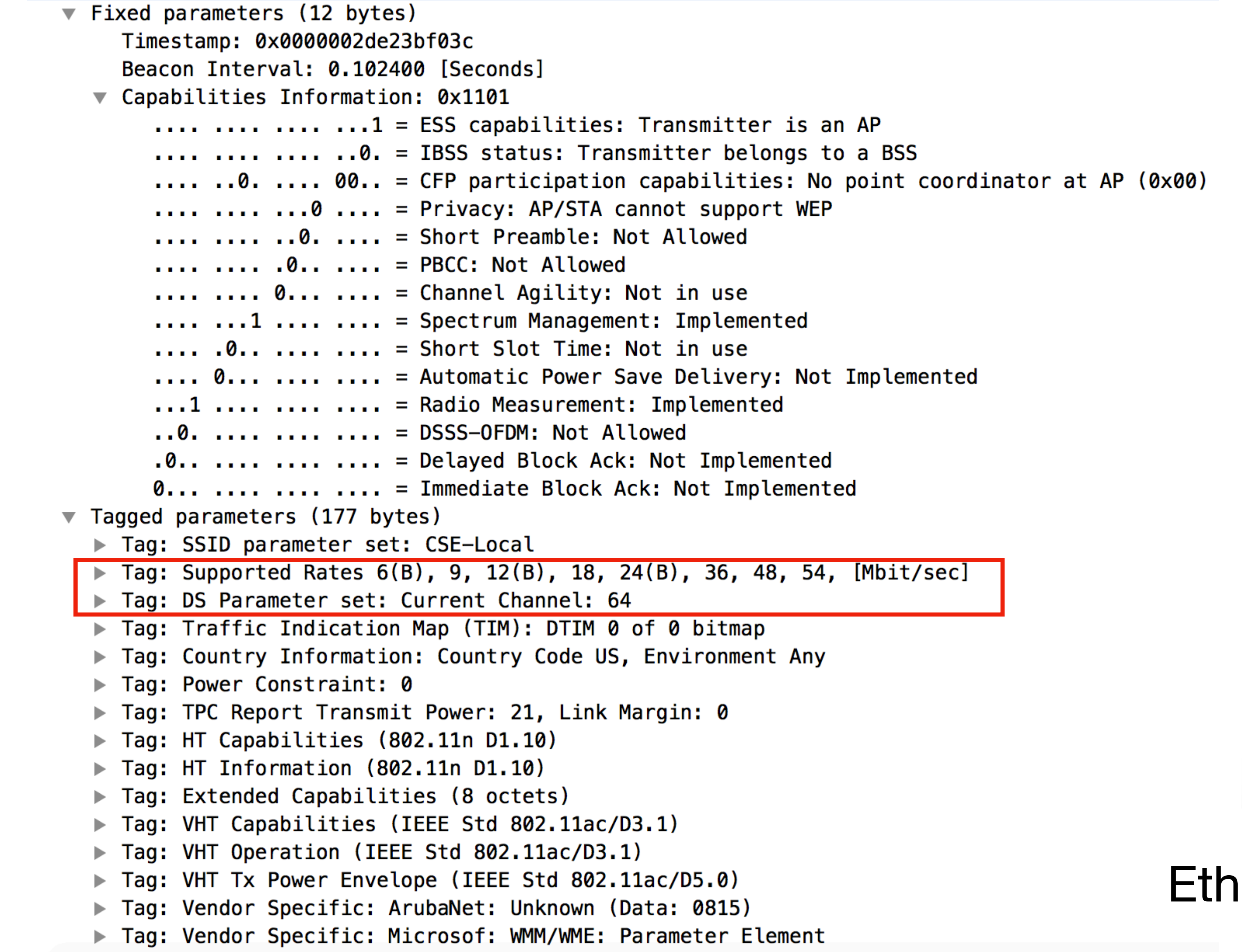
Beacon frames

Wi-Fi send these to announce their presence
Broadcasted to everyone

Physical layer message



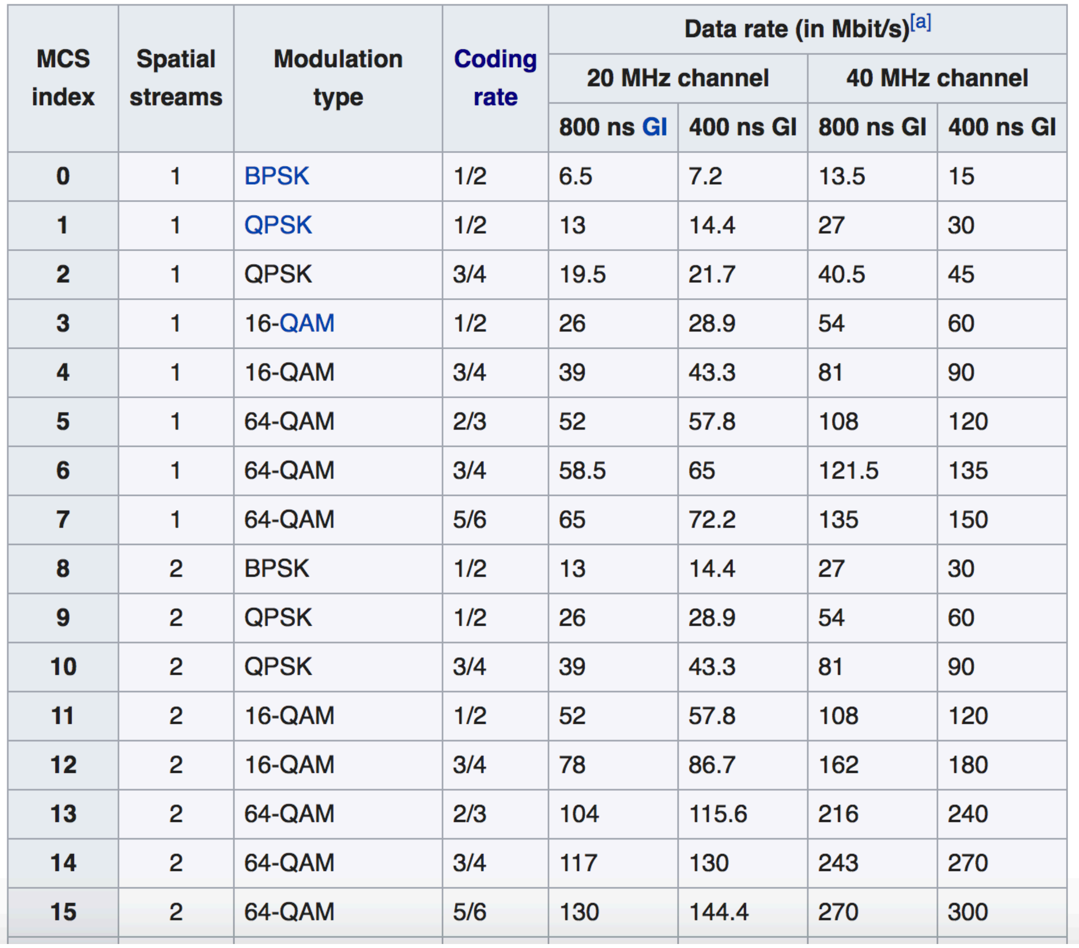
```
634 4.377510   ArubaNet_eb:40:30   Broadcast   802.11   242 Beacon frame, SN=2026, FN=0, Flags=........C, BI=100, SSID=CSE-Local
635 4.377906   ArubaNet_eb:40:31   Broadcast   802.11   278 Beacon frame, SN=2027, FN=0, Flags=........C, BI=100, SSID=University of Washington
636 4.378288   ArubaNet_eb:40:32   Broadcast   802.11   287 Beacon frame, SN=2028, FN=0, Flags=........C, BI=100, SSID=eduroam
637 4.403317   ArubaNet_eb:69:10   Broadcast   802.11   242 Beacon frame, SN=700, FN=0, Flags=........C, BI=100, SSID=CSE-Local
638 4.403701   ArubaNet_eb:69:11   Broadcast   802.11   278 Beacon frame, SN=701, FN=0, Flags=........C, BI=100, SSID=University of Washington
639 4.404101   ArubaNet_eb:69:12   Broadcast   802.11   287 Beacon frame, SN=702, FN=0, Flags=........C, BI=100, SSID=eduroam
640 4.479977   ArubaNet_eb:40:30   Broadcast   802.11   242 Beacon frame, SN=2029, FN=0, Flags=........C, BI=100, SSID=CSE-Local
641 4.480326   ArubaNet_eb:40:31   Broadcast   802.11   278 Beacon frame, SN=2030, FN=0, Flags=........C, BI=100, SSID=University of Washington
▶ Frame 634: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits) on interface 0
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▶ IEEE 802.11 Beacon frame, Flags: ........C
▶ IEEE 802.11 wireless LAN management frame
```



```
▼ IEEE 802.11 wireless LAN management frame
  ▼ Fixed parameters (12 bytes)
      Timestamp: 0x0000002de23bf03c
      Beacon Interval: 0.102400 [Seconds]
    ▼ Capabilities Information: 0x1101
        .... .... .... ...1 = ESS capabilities: Transmitter is an AP
        .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
        .... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x00)
        .... .... ...0 .... = Privacy: AP/STA cannot support WEP
        .... .... ..0. .... = Short Preamble: Not Allowed
        .... .... .0.. .... = PBCC: Not Allowed
        .... .... 0... .... = Channel Agility: Not in use
        .... ...1 .... .... = Spectrum Management: Implemented
        .... .0.. .... .... = Short Slot Time: Not in use
        .... 0... .... .... = Automatic Power Save Delivery: Not Implemented
        ...1 .... .... .... = Radio Measurement: Implemented
        ..0. .... .... .... = DSSS-OFDM: Not Allowed
        .0.. .... .... .... = Delayed Block Ack: Not Implemented
        0... .... .... .... = Immediate Block Ack: Not Implemented
  ▼ Tagged parameters (177 bytes)
    ▶ Tag: SSID parameter set: CSE-Local
    ▶ Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 64
    ▶ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▶ Tag: Country Information: Country Code US, Environment Any
    ▶ Tag: Power Constraint: 0
    ▶ Tag: TPC Report Transmit Power: 21, Link Margin: 0
    ▶ Tag: HT Capabilities (802.11n D1.10)
    ▶ Tag: HT Information (802.11n D1.10)
    ▶ Tag: Extended Capabilities (8 octets)
    ▶ Tag: VHT Capabilities (IEEE Std 802.11ac/D3.1)
    ▶ Tag: VHT Operation (IEEE Std 802.11ac/D3.1)
    ▶ Tag: VHT Tx Power Envelope (IEEE Std 802.11ac/D5.0)
    ▶ Tag: Vendor Specific: ArubaNet: Unknown (Data: 0815)
    ▶ Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element
```

Wi-Fi adapts bitrate based on SNR

Modulation and coding schemes



MCS index	Spatial streams	Modulation type	Coding rate	Data rate (in Mbit/s)[a]			
				20 MHz channel		40 MHz channel	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	1	BPSK	1/2	6.5	7.2	13.5	15
1	1	QPSK	1/2	13	14.4	27	30
2	1	QPSK	3/4	19.5	21.7	40.5	45
3	1	16-QAM	1/2	26	28.9	54	60
4	1	16-QAM	3/4	39	43.3	81	90
5	1	64-QAM	2/3	52	57.8	108	120
6	1	64-QAM	3/4	58.5	65	121.5	135
7	1	64-QAM	5/6	65	72.2	135	150
8	2	BPSK	1/2	13	14.4	27	30
9	2	QPSK	1/2	26	28.9	54	60
10	2	QPSK	3/4	39	43.3	81	90
11	2	16-QAM	1/2	52	57.8	108	120
12	2	16-QAM	3/4	78	86.7	162	180
13	2	64-QAM	2/3	104	115.6	216	240
14	2	64-QAM	3/4	117	130	243	270
15	2	64-QAM	5/6	130	144.4	270	300

Ethernet = {10, 100, **1000**, 10k,…}MBps