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
Domain Name Space

Up to 127 levels

Null string (root zone)

Top level domain

edu

cs

washington

"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.

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

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
dig (domain information groper)

Unix utility to query DNS service

Root name servers

/etc/resolv.conf
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 authoritative name servers

TTLs
86400 = 24 hours
144024 = 40 hours
Reverse DNS lookup

PTR record for IP => name

```
! => 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:

; 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:ffff: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
```
DNS cache

chrome://net-internals/#dns

We check this before doing a DNS call

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Family</th>
<th>Addresses</th>
<th>TTL</th>
<th>Expires</th>
<th>Network changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounts.google.com</td>
<td>IPV4</td>
<td>216.58.216.173</td>
<td>300000</td>
<td>2017-10-04</td>
<td>23:21:00.095</td>
</tr>
<tr>
<td>ajax.googleapis.com</td>
<td>IPV4</td>
<td>216.58.216.138</td>
<td>172.217.3.202</td>
<td>216.58.193.74</td>
<td></td>
</tr>
<tr>
<td>api.github.com</td>
<td>IPV4</td>
<td>192.30.255.117</td>
<td>192.30.255.116</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apis.google.com</td>
<td>IPV4</td>
<td>216.58.216.174</td>
<td>60000</td>
<td>2017-10-04</td>
<td>23:16:56.835</td>
</tr>
<tr>
<td>apps.canvas.uw.edu</td>
<td>IPV4</td>
<td>69.91.245.45</td>
<td>1000</td>
<td>2017-10-04</td>
<td>23:17:02.273</td>
</tr>
<tr>
<td>assets-cdn.github.com</td>
<td>IPV4</td>
<td>151.101.52.133</td>
<td>30000</td>
<td>2017-10-04</td>
<td>23:16:56.836</td>
</tr>
<tr>
<td>avatars0.githubusercontent.com</td>
<td>IPV4</td>
<td>151.101.52.133</td>
<td>28000</td>
<td>2017-10-04</td>
<td>23:16:58.419</td>
</tr>
<tr>
<td>avatars1.githubusercontent.com</td>
<td>IPV4</td>
<td>151.101.52.133</td>
<td>30000</td>
<td>2017-10-04</td>
<td>23:16:56.776</td>
</tr>
<tr>
<td>avatars2.githubusercontent.com</td>
<td>IPV4</td>
<td>151.101.52.133</td>
<td>30000</td>
<td>2017-10-04</td>
<td>23:16:56.776</td>
</tr>
<tr>
<td>avatars3.githubusercontent.com</td>
<td>IPV4</td>
<td>151.101.52.133</td>
<td>30000</td>
<td>2017-10-04</td>
<td>23:16:56.776</td>
</tr>
<tr>
<td>canvas.uw.edu</td>
<td>IPV4</td>
<td>52.20.24.113</td>
<td>60000</td>
<td>2017-10-04</td>
<td>23:17:02.292</td>
</tr>
<tr>
<td>chatenabled.mail.google.com</td>
<td>IPV4</td>
<td>216.58.216.167</td>
<td>69000</td>
<td>2017-10-04</td>
<td>23:17:09.088</td>
</tr>
<tr>
<td>clients2.google.com</td>
<td>IPV4</td>
<td>216.58.216.174</td>
<td>11000</td>
<td>2017-10-04</td>
<td>23:17:50.097</td>
</tr>
<tr>
<td>clients5.google.com</td>
<td>IPV4</td>
<td>216.58.216.174</td>
<td>106000</td>
<td>2017-10-04</td>
<td>23:17:50.617</td>
</tr>
<tr>
<td>clients6.google.com</td>
<td>IPV4</td>
<td>216.58.216.174</td>
<td>112000</td>
<td>2017-10-04</td>
<td>23:17:50.672</td>
</tr>
<tr>
<td>collector.githubapp.com</td>
<td>IPV4</td>
<td>52.86.68.196</td>
<td>60000</td>
<td>2017-10-04</td>
<td>23:16:56.875</td>
</tr>
</tbody>
</table>
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)

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>bar.example.com</td>
<td>CNAME</td>
<td>foo.example.com</td>
</tr>
<tr>
<td>foo.example.com</td>
<td>A</td>
<td>192.0.2.23</td>
</tr>
</tbody>
</table>
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.
<table>
<thead>
<tr>
<th>Interface</th>
<th>Traffic</th>
<th>Link-layer Header</th>
<th>Promisc</th>
<th>Snaplen (B)</th>
<th>Buffer (MB)</th>
<th>Monitor</th>
<th>Capture Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wi-Fi en0</td>
<td></td>
<td>802.11 plus radiotap header</td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>p2p0</td>
<td></td>
<td>Raw IP</td>
<td></td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>aadv1</td>
<td></td>
<td>Ethernet</td>
<td></td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thunderbolt Bridge: bridge0</td>
<td></td>
<td>Ethernet</td>
<td></td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>utun0</td>
<td></td>
<td>BSD loopback</td>
<td></td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thunderbolt 1: en1</td>
<td></td>
<td>Ethernet</td>
<td></td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thunderbolt 2: en2</td>
<td></td>
<td>Ethernet</td>
<td></td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loopback: lo0</td>
<td></td>
<td>BSD loopback</td>
<td></td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>gf0</td>
<td></td>
<td>BSD loopback</td>
<td></td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>stf0</td>
<td></td>
<td>BSD loopback</td>
<td></td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco remote capture: cisco</td>
<td></td>
<td>Remote capture dependent DLT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Random packet generator: randpkt</td>
<td></td>
<td>Generator dependent DLT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSH remote capture: ssh</td>
<td></td>
<td>Remote capture dependent DLT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enable promiscuous mode on all interfaces

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

Compile BPFs

Help

Close

Start
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>657</td>
<td>4.566303</td>
<td>172.28.7.97</td>
<td>23.54.18.152</td>
<td>TCP</td>
<td>145</td>
<td>Seq=1 Ack=1 Win=4096 Len=0 TSecr=25754545806</td>
</tr>
<tr>
<td>565</td>
<td>4.566305</td>
<td>172.28.7.97</td>
<td>23.54.18.152</td>
<td>TCP</td>
<td>145</td>
<td>Seq=1 Ack=1 Win=5255 Len=0 TSecr=2575451893</td>
</tr>
<tr>
<td>565</td>
<td>4.566307</td>
<td>151.101.52.249</td>
<td>151.101.54.166</td>
<td>TCP</td>
<td>145</td>
<td>Seq=1 Ack=1 Win=4096 Len=0 TSecr=39946710008</td>
</tr>
<tr>
<td>560</td>
<td>4.566310</td>
<td>172.28.7.97</td>
<td>151.101.54.166</td>
<td>TCP</td>
<td>145</td>
<td>Seq=1 Ack=1 Win=4096 Len=0 TSecr=3994679015</td>
</tr>
<tr>
<td>661</td>
<td>4.566312</td>
<td>172.28.7.97</td>
<td>151.101.52.249</td>
<td>TCP</td>
<td>145</td>
<td>Seq=2 Ack=1 Win=4096 Len=0 TSecr=271526016</td>
</tr>
<tr>
<td>662</td>
<td>4.566314</td>
<td>172.28.7.97</td>
<td>172.28.7.1</td>
<td>DNS</td>
<td>155</td>
<td><a href="http://www.en.wikipedia.org">www.en.wikipedia.org</a></td>
</tr>
<tr>
<td>663</td>
<td>4.566316</td>
<td>172.28.7.97</td>
<td>172.28.7.1</td>
<td>DNS</td>
<td>159</td>
<td>Standard query A0x4a33 A upload.wikimedia.org</td>
</tr>
<tr>
<td>664</td>
<td>4.566318</td>
<td>172.28.7.97</td>
<td>172.28.7.1</td>
<td>DNS</td>
<td>152</td>
<td>Standard query A0x4e09 A wikipedia.org</td>
</tr>
<tr>
<td>667</td>
<td>4.568337</td>
<td>151.101.54.166</td>
<td>172.28.7.97</td>
<td>TCP</td>
<td>138</td>
<td>Seq=2 Ack=59 Win=59 Len=0 TSecr=3994672916</td>
</tr>
<tr>
<td>669</td>
<td>4.568633</td>
<td>151.101.52.249</td>
<td>172.28.7.97</td>
<td>TCP</td>
<td>134</td>
<td>Seq=1 Ack=3 Win=4096 Len=0 TSecr=3454675676</td>
</tr>
<tr>
<td>671</td>
<td>4.568903</td>
<td>151.101.54.166</td>
<td>Apple_13:3a:69:7</td>
<td>TCP</td>
<td>145</td>
<td>Seq=2 Ack=2 Win=4096 Len=0 TSecr=3994672916</td>
</tr>
<tr>
<td>673</td>
<td>4.569058</td>
<td>Apple_13:3a:69:7</td>
<td>b8.02.11</td>
<td>UDP</td>
<td>45</td>
<td>Clear-to-send, Flags=........C</td>
</tr>
<tr>
<td>674</td>
<td>4.569183</td>
<td>151.101.52.175</td>
<td>172.28.7.97</td>
<td>TCP</td>
<td>134</td>
<td>Seq=1 Ack=3 Win=4096 Len=0 TSecr=3454675691</td>
</tr>
<tr>
<td>675</td>
<td>4.569190</td>
<td>151.101.52.249</td>
<td>172.28.7.97</td>
<td>TCP</td>
<td>138</td>
<td>Seq=1 Ack=2 Win=4096 Len=0 TSecr=3994672916</td>
</tr>
<tr>
<td>676</td>
<td>4.569459</td>
<td>Apple_13:3a:69:7</td>
<td>b8.02.11</td>
<td>UDP</td>
<td>39</td>
<td>Clear-to-send, Flags=........C</td>
</tr>
<tr>
<td>677</td>
<td>4.569579</td>
<td>151.101.52.249</td>
<td>151.101.54.166</td>
<td>TCP</td>
<td>145</td>
<td>Seq=2 Ack=2 Win=4096 Len=0 TSecr=3454675676</td>
</tr>
<tr>
<td>680</td>
<td>4.569873</td>
<td>23.54.18.152</td>
<td>172.28.7.97</td>
<td>TCP</td>
<td>134</td>
<td>Seq=1 Ack=2 Win=1140 Len=0 TSecr=271526016</td>
</tr>
<tr>
<td>681</td>
<td>4.569879</td>
<td>23.54.18.152</td>
<td>172.28.7.97</td>
<td>TCP</td>
<td>138</td>
<td>Seq=1 Ack=2 Win=939 Len=0 TSecr=271526016</td>
</tr>
</tbody>
</table>
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
-60 is “good” for Wi-Fi
Disconnects at around -90dBm

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

20MHz
Max data Rate
Convert SNR from dB value
2.4GHz:
Three non-overlapping channels in the US
1, 6, 11
20MHz bandwidths

5Hz:
Variable bandwidths: 20, 40, 80MHz
More room
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>657</td>
<td>4.566303</td>
<td>172.28.7.97</td>
<td>23.54.18.152</td>
<td>TCP</td>
<td>145</td>
<td>55537 → 80 [FIN, ACK] Seq1 Ack=1 Win=4096 Len=0 TSecr=257526016 TSecr=2575454806</td>
</tr>
<tr>
<td>656</td>
<td>4.566305</td>
<td>172.28.7.97</td>
<td>23.54.18.152</td>
<td>TCP</td>
<td>145</td>
<td>55535 → 80 [FIN, ACK] Seq1 Ack=1 Win=5255 Len=0 TSecr=257526016 TSecr=2575451893</td>
</tr>
<tr>
<td>658</td>
<td>4.566307</td>
<td>151.101.52.249</td>
<td>151.101.54.166</td>
<td>TCP</td>
<td>145</td>
<td>55533 → 80 [FIN, ACK] Seq1 Ack=1 Win=4096 Len=0 TSecr=257526016 TSecr=3994671008</td>
</tr>
<tr>
<td>659</td>
<td>4.566310</td>
<td>151.101.52.249</td>
<td>151.101.54.166</td>
<td>TCP</td>
<td>145</td>
<td>55534 → 80 [FIN, ACK] Seq1 Ack=1 Win=4096 Len=0 TSecr=257526016 TSecr=3994679015</td>
</tr>
<tr>
<td>660</td>
<td>4.566312</td>
<td>172.28.7.97</td>
<td>151.101.52.249</td>
<td>TCP</td>
<td>145</td>
<td>[TCP Previous segment not captured] 55542 → 80 [FIN, ACK] Seq2 Ack=1 Win=4096 Len=0 TSecr=271526016</td>
</tr>
<tr>
<td>661</td>
<td>4.566314</td>
<td>172.28.7.97</td>
<td>172.28.7.1</td>
<td>DNS</td>
<td>155</td>
<td>Standard query 8x6A08 A en.wikipedia.org</td>
</tr>
<tr>
<td>662</td>
<td>4.566316</td>
<td>172.28.7.97</td>
<td>172.28.7.1</td>
<td>DNS</td>
<td>159</td>
<td>Standard query 8x6A08 A upload.wikimedia.org</td>
</tr>
<tr>
<td>665</td>
<td>4.566354</td>
<td>Apple_13:a6:97</td>
<td>b8.08.21:11部</td>
<td>Block Ack</td>
<td>57</td>
<td>[ACK] Seq2 Ack=2 Win=59 Len=0 TSecr=3994672916 TSecr=271526016</td>
</tr>
<tr>
<td>666</td>
<td>4.568279</td>
<td>ArubaNet_eb:69:10</td>
<td>b8.08.21:11部</td>
<td>Block Ack</td>
<td>45</td>
<td>Request-to-send, Flags=        C</td>
</tr>
<tr>
<td>667</td>
<td>4.568337</td>
<td>151.101.54.166</td>
<td>172.28.7.97</td>
<td>TCP</td>
<td>138</td>
<td>80 → 55543 [FIN, ACK] Seq1 Ack=2 Win=59 Len=0 TSecr=3994672916 TSecr=271526016</td>
</tr>
<tr>
<td>668</td>
<td>4.568537</td>
<td>ArubaNet_eb:69:10</td>
<td>b8.08.21:11部</td>
<td>Block Ack</td>
<td>45</td>
<td>Request-to-send, Flags=        C</td>
</tr>
<tr>
<td>669</td>
<td>4.568633</td>
<td>151.101.52.249</td>
<td>172.28.7.97</td>
<td>TCP</td>
<td>138</td>
<td>80 → 55542 [FIN, ACK] Seq1 Ack=2 Win=61 Len=0 TSecr=3454675676 TSecr=3454675687</td>
</tr>
<tr>
<td>670</td>
<td>4.568789</td>
<td>Apple_13:a6:97</td>
<td>b8.08.21:11部</td>
<td>Block Ack</td>
<td>39</td>
<td>Clear-to-send, Flags=        C</td>
</tr>
<tr>
<td>671</td>
<td>4.568903</td>
<td>172.28.7.97</td>
<td>151.101.54.166</td>
<td>TCP</td>
<td>145</td>
<td>55543 → 80 [ACK] Seq2 Ack=2 Win=4096 Len=0 TSecr=271526029 TSecr=394672916</td>
</tr>
<tr>
<td>672</td>
<td>4.568942</td>
<td>ArubaNet_eb:69:10</td>
<td>b8.08.21:11部</td>
<td>Block Ack</td>
<td>57</td>
<td>[ACK] Seq2 Ack=2 Win=61 Len=0 TSecr=394672916 TSecr=271526029</td>
</tr>
<tr>
<td>673</td>
<td>4.569058</td>
<td>ArubaNet_eb:69:10</td>
<td>b8.08.21:11部</td>
<td>Block Ack</td>
<td>45</td>
<td>Request-to-send, Flags=        C</td>
</tr>
<tr>
<td>674</td>
<td>4.569183</td>
<td>151.101.52.175</td>
<td>172.28.7.97</td>
<td>TCP</td>
<td>134</td>
<td>[TCP ACKed unseen segment] 80 → 55527 [FIN, ACK] Seq1 Ack=3 Win=66 Len=0 TSecr=3346676991 TSecr=3346676991</td>
</tr>
<tr>
<td>675</td>
<td>4.569198</td>
<td>151.101.52.249</td>
<td>172.28.7.97</td>
<td>TCP</td>
<td>138</td>
<td>80 → 55553 [FIN, ACK] Seq1 Ack=2 Win=60 Len=0 TSecr=3994672916 TSecr=271526016</td>
</tr>
<tr>
<td>676</td>
<td>4.569459</td>
<td>Apple_13:a6:97</td>
<td>b8.08.21:11部</td>
<td>Block Ack</td>
<td>39</td>
<td>Clear-to-send, Flags=        C</td>
</tr>
<tr>
<td>677</td>
<td>4.569579</td>
<td>172.28.7.97</td>
<td>151.101.52.249</td>
<td>TCP</td>
<td>145</td>
<td>55542 → 80 [ACK] Seq2 Ack=2 Win=4096 Len=0 TSecr=271526029 TSecr=3454675676</td>
</tr>
<tr>
<td>678</td>
<td>4.569620</td>
<td>ArubaNet_eb:69:10</td>
<td>b8.08.21:11部</td>
<td>Block Ack</td>
<td>57</td>
<td>80.21:11 Block Ack, Flags=        C</td>
</tr>
<tr>
<td>679</td>
<td>4.569744</td>
<td>Apple_13:a6:97</td>
<td>b8.08.21:11部</td>
<td>Block Ack</td>
<td>45</td>
<td>Request-to-send, Flags=        C</td>
</tr>
<tr>
<td>680</td>
<td>4.569873</td>
<td>23.54.18.152</td>
<td>172.28.7.97</td>
<td>TCP</td>
<td>134</td>
<td>80 → 55535 [ACK] Seq1 Ack=2 Win=1140 Len=0 TSecr=2574582998 TSecr=271526016</td>
</tr>
<tr>
<td>681</td>
<td>4.569879</td>
<td>23.54.18.152</td>
<td>172.28.7.97</td>
<td>TCP</td>
<td>134</td>
<td>80 → 55525 [ACK] Seq1 Ack=2 Win=1399 Len=0 TSecr=2574582998 TSecr=271526016</td>
</tr>
<tr>
<td>682</td>
<td>4.570879</td>
<td>Apple_13:a6:97</td>
<td>b8.08.21:11部</td>
<td>Block Ack</td>
<td>39</td>
<td>Clear-to-send, Flags=        C</td>
</tr>
</tbody>
</table>
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]
Internet Layer

Internet Protocol Version 4, Src: 172.28.7.97, Dst: 172.28.7.1

- Version: 4
- 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
  - ... .... = 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]

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:c7:89e: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]
Physical layer

- Radiotap Header v0, Length 59
  - Header revision: 0
  - Header pad: 0
  - Header length: 59
  - Present flags
    - MAC timestamp: 3089947722
  - Flags: 0x00
    - Channel frequency: 5320 MHz
    - Channel flags: 0x0100, 5 GHz spectrum, HT Channel (20MHz Channel Width)
      - .... .... .... .... .... .... = Turbo: False
      - .... .... .... .... .... .... = Complementary Code Keying (CCK): False
      - .... .... .... .... .... .... = Orthogonal Frequency-Division Multiplexing (OFDM): False
      - .... .... .... .... .... .... = 2 GHz spectrum: False
      - .... .... .... .... .... .... = 5 GHz spectrum: True
      - .... .... .... .... .... .... = Passive: False
      - .... .... .... .... .... .... = Dynamic CCK-OFDM: False
      - .... .... .... .... .... .... = Gaussian Frequency Shift Keying (GFSK): False
      - .... .... .... .... .... .... = GSM (900MHz): False
      - .... .... .... .... .... .... = Static Turbo: False
      - .... .... .... .... .... .... = Half Rate Channel (10MHz Channel Width): False
      - .... .... .... .... .... .... = Quarter Rate Channel (5MHz Channel Width): False
      - .... .... .... .... .... .... = HT Channel (20MHz Channel Width): True
      - .... .... .... .... .... .... = HT Channel (40MHz Channel Width with Extension channel above): False
      - .... .... .... .... .... .... = 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]
Beacon frames
Wi-Fi send these to announce their presence
Broadcasted to everyone

Wi-Fi adapts bitrate based on SNR

Ethernet = \{10, 100, 1000, 10k, \ldots\}\text{MBps}