

Lecture 04 addendum tutorial:

Study the TCP Flow Graph that you obtained in Tutorial4 (copy on Moodle) and answer the following questions:

1. Describe activities in frames 11,13,15

11	4.090733	172.16.8.1	130.194.64.145	TCP	66	61981 → 80	[SYN] Seq=0 Win=8192 Len=0 MSS=12...
12	4.353041	172.16.8.1	130.194.64.145	TCP	66	61982 → 80	[SYN] Seq=0 Win=8192 Len=0 MSS=12...
13	4.757967	130.194.64.145	172.16.8.1	TCP	66	80 → 61981	[SYN, ACK] Seq=0 Ack=1 Win=50400 ...
14	4.758114	172.16.8.1	130.194.64.145	TCP	54	61981 → 80	[ACK] Seq=1 Ack=1 Win=66780 Len=0
15	4.758506	172.16.8.1	130.194.64.145	HTTP	360	GET /~app/tute/	HTTP/1.1

TCP 3-way handshake

The first two handshakes in the TCP three-way handshake between frame 11 and frame 13.

Frame 11 sends a segment with seq 0 to the host with ip address 172.16.8.1 to the host with ip address 130.194.64.145.

Frame 13 is sent by the host with the ip address 130.194.64.145 to ack and seq to the host with the ip address 172.16.8.1.

HTTP connection gets GET command on frame 15

2. In the frame 32 why we have Ack=10043

31	6.906357	130.194.64.145	172.16.8.1	TCP	1314	80 → 61981 [PSH, ACK] Seq=8783 Ack=643 Win=50400 Len=1260	[TCP segment of a reassembled PDU]
32	6.906507	172.16.8.1	130.194.64.145	TCP	54	61981 → 80 [ACK] Seq=643 Ack=10043 Win=66780 Len=0	
33	6.906617	130.194.64.145	172.16.8.1	TCP	1314	[TCP Previous segment not captured] 80 → 61981 [ACK] Seq=11303 Ack=643 Win=50400 Len=1260	[TCP segment of a reassembled PDU]
34	6.906619	130.194.64.145	172.16.8.1	TCP	1314	80 → 61981 [PSH, ACK] Seq=12563 Ack=643 Win=50400 Len=1260	[TCP segment of a reassembled PDU]
35	6.906662	172.16.8.1	130.194.64.145	TCP	66	[TCP Dup ACK 32#1] 61981 → 80 [ACK] Seq=643 Ack=10043 Win=66780 Len=0 SLE=11303 SRE=12563	
36	6.906682	172.16.8.1	130.194.64.145	TCP	66	[TCP Dup ACK 32#2] 61981 → 80 [ACK] Seq=643 Ack=10043 Win=66780 Len=0 SLE=11303 SRE=13823	
37	7.110490	172.16.8.1	221.6.4.66	DNS	78	Standard query 0xa520 A wpad.AD.MONASH.EDU	
38	7.119613	221.6.4.66	172.16.8.1	DNS	149	Standard query response 0xa520 A wpad.AD.MONASH.EDU A 220.250.64.225 SOA ns0.its.monash.edu	
39	7.120809	172.16.8.1	220.250.64.225	TCP	66	61983 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=4 SACK_PERM=1	
40	7.148661	220.250.64.225	172.16.8.1	TCP	66	80 → 61983 [SYN, ACK] Seq=0 Ack=1 Win=50400 Len=0 MSS=1380 WS=1 SACK_PERM=1	
41	7.148816	172.16.8.1	220.250.64.225	TCP	54	61983 → 80 [ACK] Seq=1 Ack=1 Win=66780 Len=0	
42	7.149132	172.16.8.1	220.250.64.225	HTTP	139	GET /wpad.dat HTTP/1.1	
43	7.177093	220.250.64.225	172.16.8.1	TCP	60	80 → 61983 [ACK] Seq=1 Ack=86 Win=50315 Len=0	
44	7.177473	220.250.64.225	172.16.8.1	HTTP	189	[TCP Previous segment not captured] Continuation	
45	7.177475	220.250.64.225	172.16.8.1	TCP	298	[TCP Out-of-order] 80 → 61983 [PSH, ACK] Seq=1 Ack=86 Win=50400 Len=204	

Internet Protocol Version 4, Src: 130.194.64.145, Dst: 172.16.8.1

Transmission Control Protocol, Src Port: 80, Dst Port: 61981, Seq: 8783, Ack: 643, Len: 1260

Source Port: 80

Destination Port: 61981

[Stream index: 5]

[TCP Segment Len: 1260]

Sequence number: 8783 (relative sequence number)

[Next sequence number: 10043 (relative sequence number)]

Acknowledgment number: 643 (relative ack number)

0101 ... = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

ACK=segment len+seq = Next sequence number

Because the next sequence number of frame 31 is 10043, need the next sequence number is 10043 so the ACK for frame 32 is 10046.

3. Ack=10043 has been repeated in many frames after the frame 32. What does it mean?

35	6.906662	172.16.8.1	130.194.64.145	TCP	66	[TCP Dup ACK 32#1] 61981 → 80 [ACK] Seq=643 Ack=10043 Win=66780 Len=0 SLE=11303 SRE=12563	
36	6.906682	172.16.8.1	130.194.64.145	TCP	66	[TCP Dup ACK 32#2] 61981 → 80 [ACK] Seq=643 Ack=10043 Win=66780 Len=0 SLE=11303 SRE=13823	

Indicates that the data segment has been lost, 32 is the location where the data was lost, #1 represents the lost one, #2 means lost twice.

4. What is happening in the frame 86?

86	8.271522	130.194.64.145	172.16.8.1	TCP	1314	[TCP Retransmission] 80 → 61981 [ACK] Seq=10043 Ack=643 Win=50400 Len=1260	
87	8.271525	130.194.64.145	172.16.8.1	TCP	1314	80 → 61981 [PSH, ACK] Seq=21383 Ack=643 Win=50400 Len=1260	[TCP segment of a reassembled PDU]
88	8.271630	172.16.8.1	130.194.64.145	TCP	54	61981 → 80 [ACK] Seq=643 Ack=21383 Win=66780 Len=0	
89	8.271782	172.16.8.1	130.194.64.145	TCP	54	61981 → 80 [ACK] Seq=643 Ack=22643 Win=66780 Len=0	
90	8.272324	130.194.64.145	172.16.8.1	TCP	1314	80 → 61981 [PSH, ACK] Seq=22643 Ack=643 Win=50400 Len=1260	[TCP segment of a reassembled PDU]

ame 86: 1314 bytes on wire (10512 bits), 1314 bytes captured (10512 bits)

hernet II, Src: Hangzhou_e5:c2:85 (74:25:8a:e5:c2:85), Dst: Dell_3d:05:97 (d0:67:e5:3d:05:97)

ternet Protocol Version 4, Src: 130.194.64.145, Dst: 172.16.8.1

anmission Control Protocol, Src Port: 80, Dst Port: 61981, Seq: 10043, Ack: 643, Len: 1260

Source Port: 80

Destination Port: 61981

[Stream index: 5]

[TCP Segment Len: 1260]

Sequence number: 10043 (relative sequence number)

[Next sequence number: 11303 (relative sequence number)]

Acknowledgment number: 643 (relative ack number)

TCP Retransmission

Frame 86 retransmits the packet with seq = 10043 ack = 643

5. Are there any retransmissions occurring. In which frames?

115,143,150,151,153,159,160,164,165,169,171,176,177,180,220,228,229,235,236,243,245,246,247,251,255,256.

6. Indicate frames related to the congestion control. What is happening after such frames have been received?

21	6.235946	130.194.64.145	172.16.8.1	TCP	60 80 → 61981 [ACK] Seq=1223	Ack=643	Win=50400 Len=0
22	6.238276	130.194.64.145	172.16.8.1	TCP	1314 80 → 61981 [ACK] Seq=1223	Ack=643	Win=50400 Len=1260 [TCP segment of a reassembled PDU]
23	6.238279	130.194.64.145	172.16.8.1	TCP	1314 80 → 61981 [ACK] Seq=2483	Ack=643	Win=50400 Len=1260 [TCP segment of a reassembled PDU]

When the sender continuously receives more than 3 identical acknowledgments, it means that the packet is lost, immediately uses fast retransmission, and enters the fast recovery state. After receiving these frames, $ssthresh = cwnd / 2$, and $cwnd = ssthresh$.

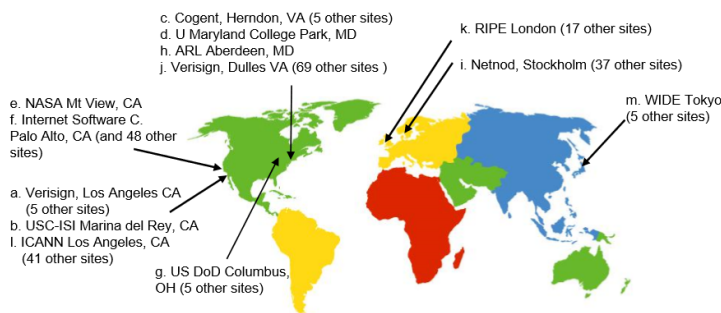
Q13

Where are the DNS root servers?

List of Root Servers

HOSTNAME	IP ADDRESSES	MANAGER
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

13 root name "servers" worldwide



Compare with:
[Root Name Servers](#)

The root server is mainly used to manage the home directory of the Internet. There are only 13 root servers in the world, and one is the main root server in the United States. The remaining 12 are secondary root servers, 9 of which are in the United States, two in Europe, in the United Kingdom and Sweden, and one in Asia in Japan.

But I believe that there will be more DNS root servers in the world in the future.

Q14

Open the command window and practice using nslookup command

app> nslookup zz.cn

Server: ns1.its.monash.edu.au

Address: 130.194.1.99

Non-authoritative answer:

Name: zz.cn

Address: 211.100.61.67

```
C:\Users\MyPC>nslookup zz.cn  
服务器: public1.alidns.com  
Address: 223.5.5.5
```

非权威应答:

```
名称:    zz.cn  
Address: 106.75.105.235
```

Nslookup (name server lookup) is used to query the DNS records, check whether the domain name resolution is normal, and use it to diagnose network problems when the network is faulty.

From this we know the list of IP addresses of the zz.cn server group.