

### Review Questions

R1 - List five nonproprietary Internet applications and the application-layer protocols that they use

1. The web - HTTP
2. Electronic mail - SMTP
3. File transfer - FTP
4. Remote login - Telnet
5. Internet telephony - SIP

R5 - What information is used by a process running on one host to identify a process running on another host?

- The IP address of the destination host and the port number of the destination socket

R11 - Why do HTTP, FTP, SMTP, and POP3 run on top of TCP rather than UDP?

- The applications that use these protocols require that the data be received in the correct order without any gaps and since TCP provides this rather than UDP, TCP is used.

### Problems

P1 - True or false?

- a. False
- b. True
- c. False
- d. False
- e. False

P4 - Consider the following string of ASCII characters that were captured by Wireshark when the browser sent an HTTP GET message

- a. What is the URL of the document requested by the browser?
  - `gaia.cs.umass.edu/cs453/index.html`
- b. What version of HTTP is the browser running?
  - 1.1
- c. Does the browser request a non-persistent or a persistent connection?
  - Persistent
- d. What is the IP address of the host on which the browser is running?
  - No IP address has been listed
- e. Mozilla/5.0

P9 - Consider Figure 2.12, for which there is an institutional network connected to the internet.

- a. Find the total average response time
  - $\Delta = (850,000)/(15,000,000) = .0567$

- $16(.0567) = 0.907$
  - $.0567/(1-.907)=.6$
  - $.6 + 3 = 3.6$
- b. Now suppose a cache is installed in the institutional LAN. Suppose the miss rate is 0.4. Find the total response time.
- $.0567/(1-(.4)(.907))=.089$  seconds
  - $.089 + 3 = 3.089$  seconds for cache misses (40% of the time)
  - $.4*3.089=1.24$  seconds

#### P17 - Consider accessing your e-mail with POP3

- a. Suppose you have configured your POP mail client to operate in the download-and-delete mode. Complete the following transaction
- C: dele 1
  - C: retr 2
  - S: blah blah ...
  - S: .....blah
  - S: .
  - C: dele 2
  - C: quit
  - S: +OK POP3 server signing off
- b. Suppose you have configured your POP mail client to operate in the download-and-keep mode. Complete the following transaction
- C: retr 2
  - S: blah blah...
  - S: ..... Blah
  - S: .
  - C: quit
  - S: +OK POP3 server signing off
- c. Suppose you sign off and sign back on five minutes later
- C: list
  - C: retr 1
  - S: ~ERR no new messages
  - C: quit
  - S: +OK POP3 server signing off

#### P18 - Questions

- a. What is a whois database?
- A database which is used to store the registered users or assignees of an Internet resource such as a domain name, IP address block or autonomous system
- b. Use various whois databases to obtain the names of two DNS servers
- Using <http://www.tucowsdomains.com/whois>

- Facebook DNS Server: a.ns.facebook.com
  - Twitter DNS server: NS1.P34.DYNECT.NET
- c. Use nslookup on your local host to send DNS queries to three DNS servers: your local DNS server and the two above.
- Local DNS server: cdns-1.comcast.net

Server	Type	Result
twitter.com	mx	preference=30, mail exchanger = aspmx2.googlemail.com
twitter.com	a	Addresses: 192.59.150.7
twitter.com	ns	ns2.p34.dynect.net
facebook.com	ns	a.ns.facebook.com
facebook.com	a	173.252.120.68
facebook.com	mx	preference=10, mail exchanger = msgin.vvv.facebook.com
local	a	75.75.75.75, 75.75.75.76
Local	mx	Primary name server =dns101.comcast.net Mail address = domregtech.comcastonline.com

- d. Use nslookup to find a Web server that has multiple IP addresses. Does the webserver of your school have multiple?
- oregonstate.edu only has one IP address.
  - Twitter.com has 4 different IP addresses

```
→ ~ nslookup -type=a oregonstate.edu
Server:      10.128.128.128
Address:     10.128.128.128#53

Non-authoritative answer:
Name:   oregonstate.edu
Address: 128.193.4.112

→ ~ nslookup -type=a twitter.com
Server:      10.128.128.128
Address:     10.128.128.128#53

Non-authoritative answer:
Name:   twitter.com
Address: 199.59.150.7
Name:   twitter.com
Address: 199.59.148.10
Name:   twitter.com
Address: 199.59.150.39
Name:   twitter.com
Address: 199.59.148.82

→ ~
```

- e. Use the ARIN whois database to determine the IP address range used by your university.
  - 128.193.0.0-128.193.255.255
- f. Describe how an attacker can use whois databases and the nslookup tool to perform reconnaissance on an institution before launching an attack
  - Someone could use nslookup to find the range of IP addresses of an institution, so they would have a large number of IPs that they could target. They could then lookup those IP addresses for more target information
- g. Discuss why whois databases should be publicly available
  - It allows for the discovery of information regarding domains easy, and prevents people from having to contact certain individuals who would know that info.

## P19 - Dig tool

- a. Starting with a root DNS server, initiate a sequence of queries for the IP address for your department's Web server by using dig. Show the list of the names of DNS servers in the delegation chain in answering your query

```
→ ~ dig +norecurse @a.root-servers.net any oregonstate.edu

; <<>> DiG 9.8.3-P1 <<>> +norecurse @a.root-servers.net any oregonstate.edu
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 31452
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 7

;; QUESTION SECTION:
;oregonstate.edu.                IN      ANY

;; AUTHORITY SECTION:
edu.          172800  IN      NS      a.edu-servers.net.
edu.          172800  IN      NS      c.edu-servers.net.
edu.          172800  IN      NS      d.edu-servers.net.
edu.          172800  IN      NS      f.edu-servers.net.
edu.          172800  IN      NS      g.edu-servers.net.
edu.          172800  IN      NS      l.edu-servers.net.

;; ADDITIONAL SECTION:
a.edu-servers.net. 172800  IN      A       192.5.6.30
c.edu-servers.net. 172800  IN      A       192.26.92.30
d.edu-servers.net. 172800  IN      A       192.31.80.30
f.edu-servers.net. 172800  IN      A       192.35.51.30
g.edu-servers.net. 172800  IN      A       192.42.93.30
l.edu-servers.net. 172800  IN      A       192.41.162.30
g.edu-servers.net. 172800  IN      AAAA    2001:503:cc2c::2:36

;; Query time: 90 msec
;; SERVER: 2001:503:ba3e::2:30#53(2001:503:ba3e::2:30)
;; WHEN: Wed Apr 20 18:28:07 2016
;; MSG SIZE rcvd: 268

→ ~
```

- b. Repeat part a) for several popular web sites such as google.com, yahoo.com or amazon.com

```
+ ~ dig +norecurse @a.root-servers.net any google.com

; <<> DiG 9.8.3-P1 <<> +norecurse @a.root-servers.net any google.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 39770
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 14

;; QUESTION SECTION:
;google.com.                IN      ANY

;; AUTHORITY SECTION:
com.      172800 IN      NS      a.gtld-servers.net.
com.      172800 IN      NS      b.gtld-servers.net.
com.      172800 IN      NS      c.gtld-servers.net.
com.      172800 IN      NS      d.gtld-servers.net.
com.      172800 IN      NS      e.gtld-servers.net.
com.      172800 IN      NS      f.gtld-servers.net.
com.      172800 IN      NS      g.gtld-servers.net.
com.      172800 IN      NS      h.gtld-servers.net.
com.      172800 IN      NS      i.gtld-servers.net.
com.      172800 IN      NS      j.gtld-servers.net.
com.      172800 IN      NS      k.gtld-servers.net.
com.      172800 IN      NS      l.gtld-servers.net.
com.      172800 IN      NS      m.gtld-servers.net.

;; ADDITIONAL SECTION:
a.gtld-servers.net. 172800 IN      A      192.5.6.30
b.gtld-servers.net. 172800 IN      A      192.33.14.30
c.gtld-servers.net. 172800 IN      A      192.26.92.30
d.gtld-servers.net. 172800 IN      A      192.31.80.30
e.gtld-servers.net. 172800 IN      A      192.12.94.30
f.gtld-servers.net. 172800 IN      A      192.35.51.30
g.gtld-servers.net. 172800 IN      A      192.42.93.30
h.gtld-servers.net. 172800 IN      A      192.54.112.30
i.gtld-servers.net. 172800 IN      A      192.43.172.30
j.gtld-servers.net. 172800 IN      A      192.48.79.30
k.gtld-servers.net. 172800 IN      A      192.52.178.30
l.gtld-servers.net. 172800 IN      A      192.41.162.30
m.gtld-servers.net. 172800 IN      A      192.55.83.30
a.gtld-servers.net. 172800 IN      AAAA   2001:503:a83e::2:30

;; Query time: 92 msec
;; SERVER: 2001:503:ba3e::2:30#53(2001:503:ba3e::2:30)
;; WHEN: Wed Apr 20 18:40:53 2016
;; MSG SIZE rcvd: 488

+ ~
```

Google.com

```
+ ~ dig +norecurse @a.root-servers.net any yahoo.com

; <<> DiG 9.8.3-P1 <<> +norecurse @a.root-servers.net any yahoo.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 1121
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 14

;; QUESTION SECTION:
;yahoo.com.                IN      ANY

;; AUTHORITY SECTION:
com.      172800 IN      NS      a.gtld-servers.net.
com.      172800 IN      NS      b.gtld-servers.net.
com.      172800 IN      NS      c.gtld-servers.net.
com.      172800 IN      NS      d.gtld-servers.net.
com.      172800 IN      NS      e.gtld-servers.net.
com.      172800 IN      NS      f.gtld-servers.net.
com.      172800 IN      NS      g.gtld-servers.net.
com.      172800 IN      NS      h.gtld-servers.net.
com.      172800 IN      NS      i.gtld-servers.net.
com.      172800 IN      NS      j.gtld-servers.net.
com.      172800 IN      NS      k.gtld-servers.net.
com.      172800 IN      NS      l.gtld-servers.net.
com.      172800 IN      NS      m.gtld-servers.net.

;; ADDITIONAL SECTION:
a.gtld-servers.net. 172800 IN      A      192.5.6.30
b.gtld-servers.net. 172800 IN      A      192.33.14.30
c.gtld-servers.net. 172800 IN      A      192.26.92.30
d.gtld-servers.net. 172800 IN      A      192.31.80.30
e.gtld-servers.net. 172800 IN      A      192.12.94.30
f.gtld-servers.net. 172800 IN      A      192.35.51.30
g.gtld-servers.net. 172800 IN      A      192.42.93.30
h.gtld-servers.net. 172800 IN      A      192.54.112.30
i.gtld-servers.net. 172800 IN      A      192.43.172.30
j.gtld-servers.net. 172800 IN      A      192.48.79.30
k.gtld-servers.net. 172800 IN      A      192.52.178.30
l.gtld-servers.net. 172800 IN      A      192.41.162.30
m.gtld-servers.net. 172800 IN      A      192.55.83.30
a.gtld-servers.net. 172800 IN      AAAA   2001:503:a83e::2:30

;; Query time: 96 msec
;; SERVER: 2001:503:ba3e::2:30#53(2001:503:ba3e::2:30)
;; WHEN: Wed Apr 20 18:41:21 2016
;; MSG SIZE rcvd: 487

+ ~
```

Yahoo.com

```
+ ~ dig +norecurse @a.root-servers.net any amazon.com

; <<> DiG 9.8.3-P1 <<> +norecurse @a.root-servers.net any amazon.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 54818
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 14

;; QUESTION SECTION:
;amazon.com.              IN      ANY

;; AUTHORITY SECTION:
com.      172800 IN      NS      a.gtld-servers.net.
com.      172800 IN      NS      b.gtld-servers.net.
com.      172800 IN      NS      c.gtld-servers.net.
com.      172800 IN      NS      d.gtld-servers.net.
com.      172800 IN      NS      e.gtld-servers.net.
com.      172800 IN      NS      f.gtld-servers.net.
com.      172800 IN      NS      g.gtld-servers.net.
com.      172800 IN      NS      h.gtld-servers.net.
com.      172800 IN      NS      i.gtld-servers.net.
com.      172800 IN      NS      j.gtld-servers.net.
com.      172800 IN      NS      k.gtld-servers.net.
com.      172800 IN      NS      l.gtld-servers.net.
com.      172800 IN      NS      m.gtld-servers.net.

;; ADDITIONAL SECTION:
a.gtld-servers.net. 172800 IN      A      192.5.6.30
b.gtld-servers.net. 172800 IN      A      192.33.14.30
c.gtld-servers.net. 172800 IN      A      192.26.92.30
d.gtld-servers.net. 172800 IN      A      192.31.80.30
e.gtld-servers.net. 172800 IN      A      192.12.94.30
f.gtld-servers.net. 172800 IN      A      192.35.51.30
g.gtld-servers.net. 172800 IN      A      192.42.93.30
h.gtld-servers.net. 172800 IN      A      192.54.112.30
i.gtld-servers.net. 172800 IN      A      192.43.172.30
j.gtld-servers.net. 172800 IN      A      192.48.79.30
k.gtld-servers.net. 172800 IN      A      192.52.178.30
l.gtld-servers.net. 172800 IN      A      192.41.162.30
m.gtld-servers.net. 172800 IN      A      192.55.83.30
a.gtld-servers.net. 172800 IN      AAAA   2001:503:a83e::2:30

;; Query time: 97 msec
;; SERVER: 2001:503:ba3e::2:30#53(2001:503:ba3e::2:30)
;; WHEN: Wed Apr 20 18:41:39 2016
;; MSG SIZE rcvd: 488

+ ~
```

<- Amazon.com

P22 - Consider distributing a file of  $F = 15$  Gbits to  $N$  peers. The server has an upload rate of  $u_s = 30$  Mbps, and each peer has a download rate of  $d_i = 2$  Mbps and an upload rate of  $u$ . For  $N = 10, 100$ , and  $1,000$  and  $u = 300$  Kbps,  $700$  Kbps, and  $2$  Mbps, prepare a chart giving the minimum distribution time for each of the combinations of  $N$  and  $u$  for both client-server distribution and P2P Distribution.

$$D_{cs} = \max\{NF/u_s, F/d_{\min}\}$$

$$d_{\min} = d_i$$

#### Client Server

	<b>N = 10</b>	<b>N = 100</b>	<b>N = 1000</b>
<b>300</b>	7680	51200	512000
<b>700</b>	7680	51200	512000
<b>2000</b>	7680	51200	512000

#### Peer to Peer

	<b>N = 10</b>	<b>N = 100</b>	<b>N = 1000</b>
<b>300</b>	7680	25904	47559
<b>700</b>	7680	15616	21525
<b>2000</b>	7680	7680	7680

P26 - Suppose Bob joins a BitTorrent torrent, but he does not want to upload any data to any other peers (so called free-riding)

- Bob claims that he can receive a complete copy of the file that is shared by the swarm. Is Bob's claim possible? Why or why not?
  - Yes it is possible as long as there are enough peers within the swarm.
- Bob further claims that he can further make his "free-riding" more efficient by using a collection of multiple computers in the computer lab of his department. How can he do that?

- He can run a client on each machine and let it do the “free-riding” and combine those chunks from the different machines into one file.

P33 - Can you configure your browser to open multiple simultaneous connections to a web site?

- Yes you can configure a browser to open multiple simultaneous connections. The advantages of having a large number of simultaneous TCP connections is that the data will be transferred reliably with the packets in order and any lost packets will be retransmitted.