COSC 4377 – Introduction to Computer Networking

Solutions to Mid-Term Examination

Spring 2018

_____

Your Name

_____

Your PeopleSoft ID #

65 minutes targeted, 75 minutes allowed
Closed book, one page of notes, study guide, and calculator permitted

Problem #	Problem Name	Points	Est Time	Pts Deducted
1	Basics	16	5	
2	Tracing Protocols	17	5	
3	Wireshark	9	10	
4	End-to-End Delay	18	15	
5	Protocol Diagram	16	10	
6	Persistent Connections	10	5	
7	DNS	14	15	
	Total	100		

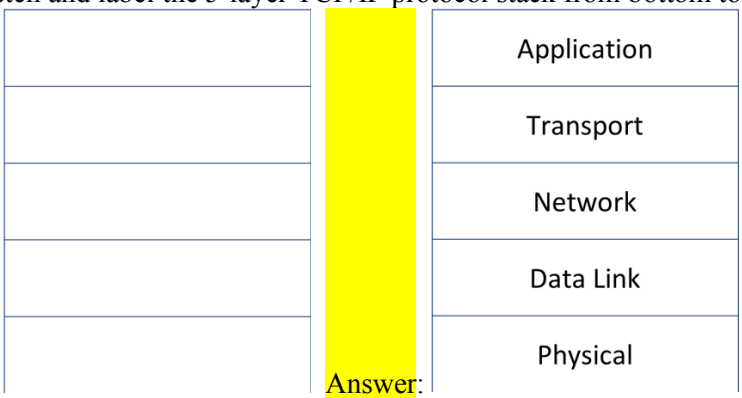
STOP

Do not turn the page until we announce that we can start.

1. Basics (16 pts)

a. (4 pts) Sketch and label the 5-layer TCP/IP protocol stack from bottom to top.

Answer:



If we see a packet on an Internet-bound Ethernet or WiFi network, it has been encapsulated (nested) with various headers and/or trailers by the different layers of the TCP/IP stack. Specifically, three headers and one trailer.

b. (4 pts) Label each of the four blocks below to indicate which layer is responsible. One layer is used twice – for a header and the block after the Data (the trailer or footer). You will use Data Link, Network and Transport. The Data block shown was created by the Application layer.

Answer:

Data Link	Network	Transport	Data	DL CRC

c. (1 pts) Which layer is the one where your programs usually run?

Answer: Application

d. (6x.5 pts) If a packet arrives via WiFi at a router but it is ignored or otherwise not delivered correctly. What could be the possible reasons? Mark all correct answers.

___ The packet was sent to IP address 255.255.255.255 and thus is ignored since routers ignore all IP broadcasts.

___ The packet belongs to a device on the local LAN and the router doesn't need to forward it.

___ The packet is requesting DNS service and the router never forwards DNS requests to a server elsewhere in the network – there must be a server on each subnet.

___ The packet was discovered to be corrupted by the data link layer in the router's network card and was discarded

___ The packet arrived with a broadcast MAC address instead of the router's MAC address

___ The packet needs to be forwarded to another link from the router but outgoing buffer for that link is full, so the router discards the packet

e. (1 pt) What do we call the addresses used at the Transport layer?

Answer: ports

f. (1 pts) What do we call the addresses used at the Network layer?

Answer: IP addresses

g. (1 pts) What are the addresses we use most of the time at the Data Link layer called?

Answer: MAC or hardware or Ethernet addresses

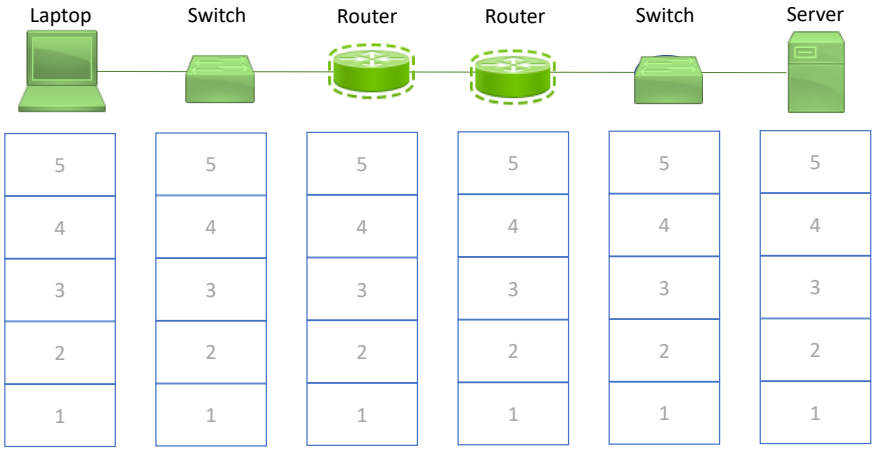
h. (1 pt)Once an IP datagram arrives at its destination host, what type of address from the answers above is used to direct the information to the proper program?

Answer: port number

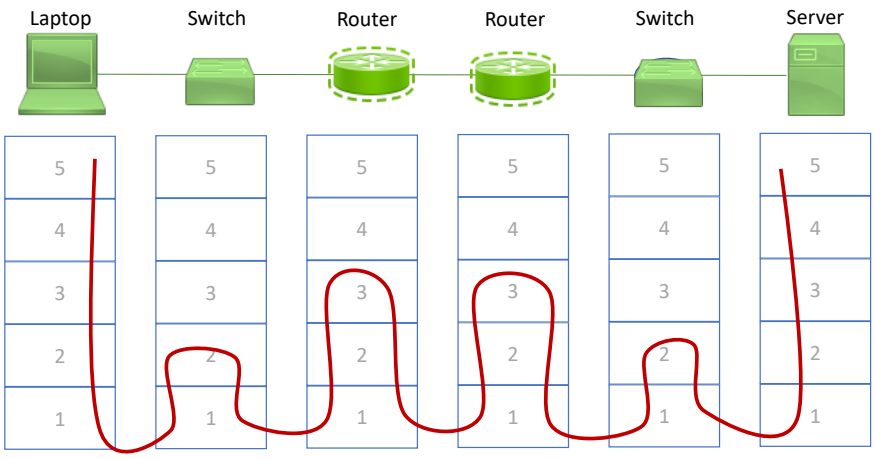
2. Tracing Protocols (18 pts)

We have the following diagrams showing a laptop as it attempts to retrieve a web page from the server on the right.

a. Draw a trace of the path a single packet takes from the browser on a laptop to the server at the other end. The trace should pass through each layer in exactly the order it would be handled.

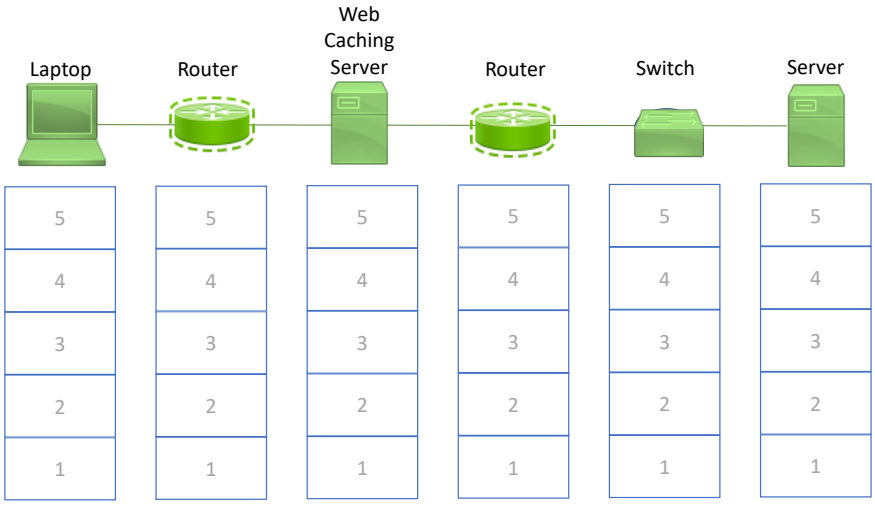


Answer in red (6 pts, one for hitting the right layer in each device):

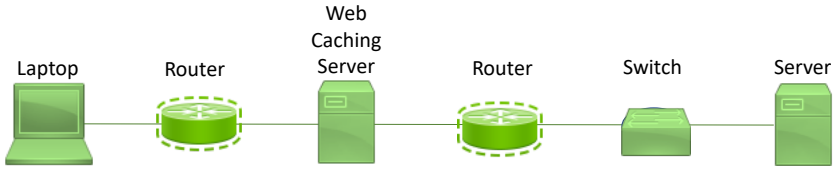


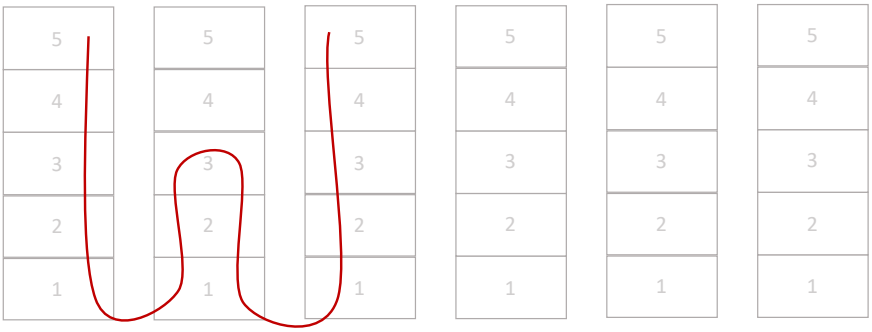
Now we add a web caching server. Think very carefully.

b) Show the trace for one-packet, one-way from the laptop to its destination assuming the object it is requesting is on the web-caching server

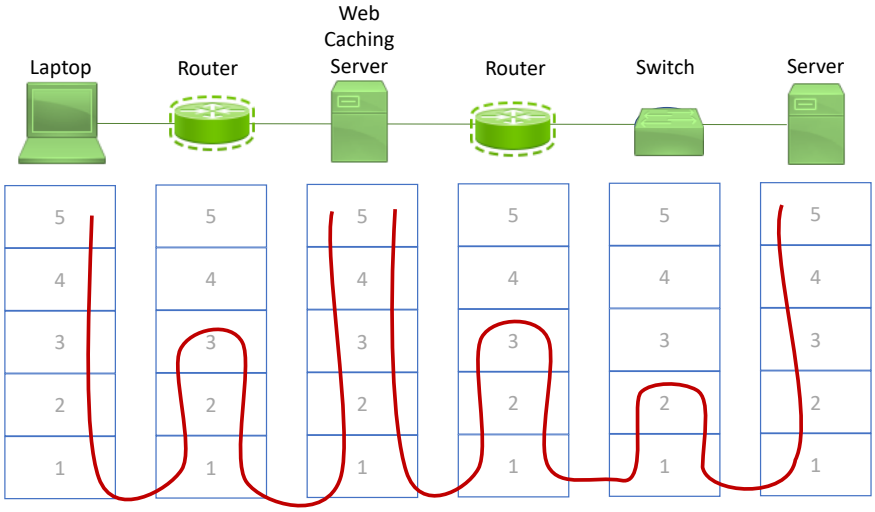


Answer in red: (4 pts total – 3 points for tracing to the correct layer in each of the first 3 columns, and 1 point for stopping at the web-caching server. Ignore any continuation beyond the WCS):





c) Show the pair of traces an HTTP request takes if the caching server does not have the desired object. Remember web caching servers act as a "man in the middle".
Answer in red (7 pts – 1 each for landing at the right layer in each column, and 1 point for breaking the connection at the WCS so that it's two traces and not one):



3. Wireshark Trace (7 pts: 7x1)

Refer to the following expanded Wireshark trace:

```
Frame 10: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on
interface 0
    Interface id: 0 (en1)
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar  4, 2018 14:09:53.220780000 CST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1520194193.220780000 seconds
    [Time delta from previous captured frame: 0.062563000 seconds]
    [Time delta from previous displayed frame: 0.062563000 seconds]
    [Time since reference or first frame: 3.051136000 seconds]
    Frame Number: 10
    Frame Length: 126 bytes (1008 bits)
    Capture Length: 126 bytes (1008 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
```

```
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: Nokia_82:33:b6 (00:d0:f6:82:33:b6), Dst: Apple_96:2d:52
(10:40:f3:96:2d:52)
    Destination: Apple_96:2d:52 (10:40:f3:96:2d:52)
        Address: Apple_96:2d:52 (10:40:f3:96:2d:52)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Nokia_82:33:b6 (00:d0:f6:82:33:b6)
        Address: Nokia_82:33:b6 (00:d0:f6:82:33:b6)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.213.5.15, Dst: 10.196.21.63
    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: 112
    Identification: 0x0000 (0)
    Flags: 0x02 (Don't Fragment)
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 60
    Protocol: UDP (17)
    Header checksum: 0x0e97 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.213.5.15
    Destination: 10.196.21.63
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 53, Dst Port: 50790
    Source Port: 53
    Destination Port: 50790
    Length: 92
    Checksum: 0xff16 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
Domain Name System (response)
    [Request In: 9]
    [Time: 0.062563000 seconds]
    Transaction ID: 0xd06e
    Flags: 0x8180 Standard query response, No error
        1... .... .... .... = Response: Message is a response
        .000 0... .... .... = Opcode: Standard query (0)
        .... .0.. .... .... = Authoritative: Server is not an authority for
domain
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... 1... .... = Recursion available: Server can do recursive
queries
        .... .... .0.. .... = Z: reserved (0)
        .... .... ..0. .... = Answer authenticated: Answer/authority portion was
not authenticated by the server
        .... .... ...0 .... = Non-authenticated data: Unacceptable
        .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
```

```
Additional RRs: 0
Queries
    scss-prod-ue1-notif-21.adobesc.com: type A, class IN
        Name: scss-prod-ue1-notif-21.adobesc.com
        [Name Length: 34]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
Answers
    scss-prod-ue1-notif-21.adobesc.com: type A, class IN, addr 35.168.84.254
        Name: scss-prod-ue1-notif-21.adobesc.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 60
        Data length: 4
        Address: 35.168.84.254
    scss-prod-ue1-notif-21.adobesc.com: type A, class IN, addr 54.174.89.245
        Name: scss-prod-ue1-notif-21.adobesc.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 60
        Data length: 4
        Address: 54.174.89.245
```

a. What application-layer protocol generated the contents of this packet? _____
   Answer: DNS
b. What transport-layer protocol is being used? _____
   Answer: UDP
c. What type of layer-2 network is the frame on? _____
   Answer: Ethernet (probably WiFi)
d. We learned two addresses of the authoritative name server for an Internet domain. Circle those two addresses in the trace.
   Answer: 35.168.84.254 and 35.174.89.245
e. If I am using a device made by Apple, who manufactured the network interface card at the other end of the link?

   _____
   Answer: Nokia
f. How big overall is this frame, in bytes? _____
   Answer: 126 bytes
g. How large is the IP datagram inside of it, in bytes? _____
   Answer: 112 bytes
h. Assuming all the error-checking looks good, I have a program running waiting to receive the data that is arriving in this packet. On what port is my program listening?

   _____
   Answer: 50790
i. On what port number was the server part of the protocol running when it sent data back to me?

   _____
   Answer: 53

4. Calculating end-to-end delay (18 pts, 6x3)

a. How is end-to-end delay different from RTT?

Answer: E-2-E is just one way.

b. If it takes 1ms for a bit to travel 250km on a network with a propagation speed of 2.5 * 10^8 m/s, how long does it take a bit to propagate over a link of distance 1,000km?

Answer: 4ms.

If the packet travels over four links totaling 5,000 km, how long does it spend propagating?

Answer: 20ms

c. If a network has a transmission speed of 2Mbps, how long does it take to transmit a 1,000-byte packet?

Answer: 8,000 bits / 2,000,000 bits/second = 4ms.

d. In calculating delay, if a packet visits three routers with a combined delay of 12ms between queueing and processing delay, does it matter how that delay is distributed? In other words, if it was all in one router versus spread out evenly, would it change the end-to-end delay?

Answer: No.

A packet travels from a host to a server. It travels through 3 routers. They add delay as shown below. Four links connect the three routers to the host and server. They are the lengths shown below. Assume each network operates at 2Mbps.

Link 1	1,000 km	Router 1 – 1ms queue delay, 1ms processing delay
Link 2	1,500 km	Router 2 – 2ms queue delay, 2ms processing delay
Link 3	1,200 km	Router 3 – 3ms queue delay, 3ms processing delay
Link 4	1,300 km	

e. Calculate the end-to-end delay of a single 1,500-byte packet from host to server. Ignore all delay inside the host and server. We care only about the network.

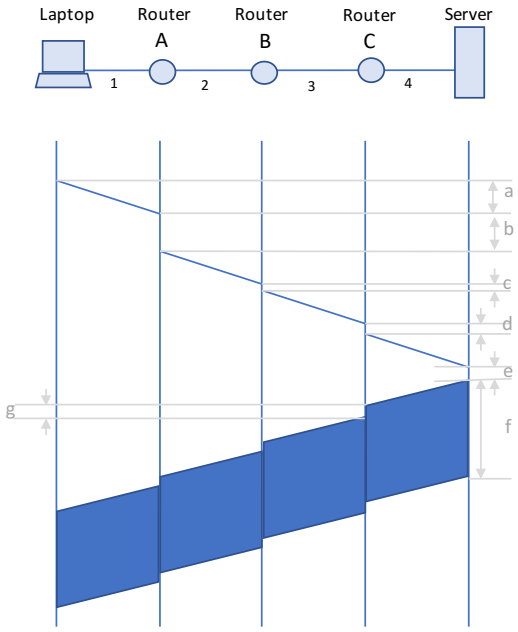
Answer: 20ms for propagation, 12ms for router delay, 6ms for transmission delay * 3 routers = 50ms

f. Is sending a packet over one 10,000km network the same delay as sending it over 5 2,000km networks connected with routers if they have no queueing or processing delay? If not, why not?

Answer: it's not the same; you still have independent transmission delay

5. Protocol Diagram (16 pts, 4x4)

Here's a diagram showing various delays:



a. If the slope of all of the line segments from laptop to server are the same, what does that indicate? Choose one.

___ all of the distances are the same

___ all of the packets are the same size

___ the routers have all the same delay

___ the propagation speeds (meters/second) on this particular type of media are the same

b. If these routers all have other incoming and outgoing communications links, which one seems to be handling the most traffic taking the same path we are?

_____

Answer: A. It has the longest delay to put traffic onto link 2, suggesting more queueing.

c. Based on what you observe in the diagram, which are plausible applications that would generate this pattern of traffic? Choose two.

___ a streaming radio service

___ a CDN distributing the latest large update to Microsoft Word

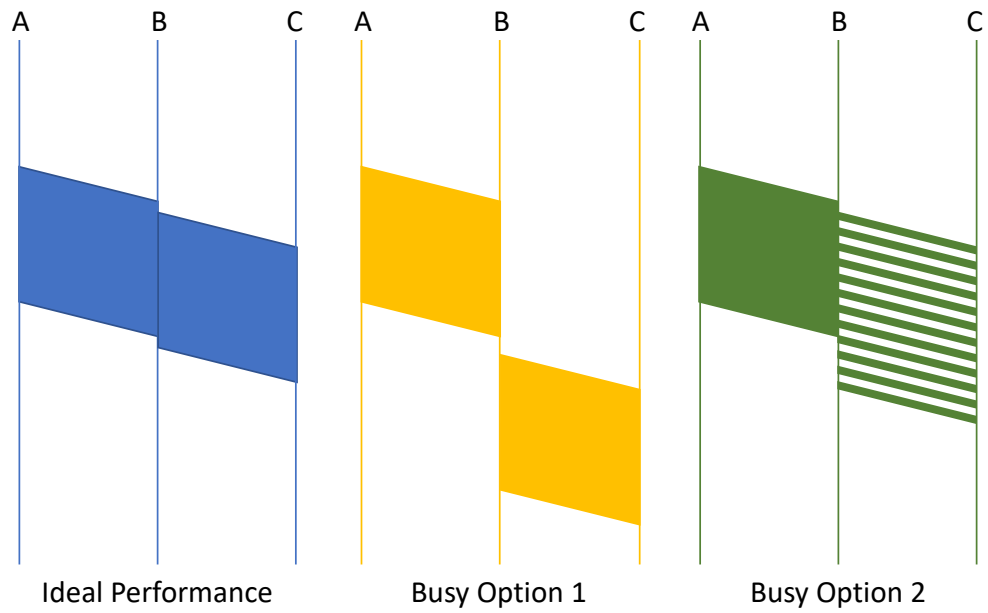
___ a user gathering the parts of a large file from a torrent community

___ a web server using a persistent connection to deliver many objects

___ a web server using a non-persistent connection to deliver many of objects

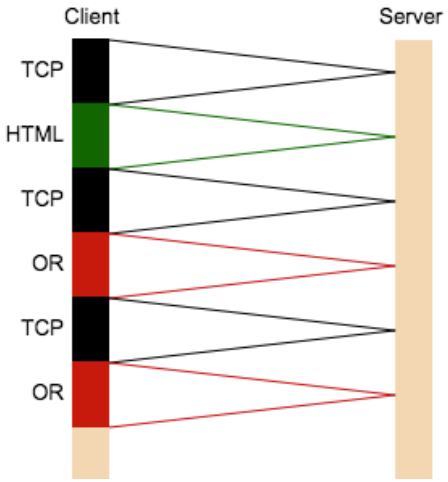
Answer: streaming and persistent web server

d. Consider the diagram below. Ideally our traffic travels from A to B to C as shown in blue. But today router B is overloaded. Although it has enough buffer space, it is introducing delay in forwarding our traffic as it is intermingled with other users' traffic in the outgoing buffer for our communication link to C. Which busy option correctly reflects this situation and why?



Answer: Option 2, because in the ideal situation, it's clearly multiple packets.

6. Persistent Connections (10 pts)
Recall our HTTP Delay Estimator problem.



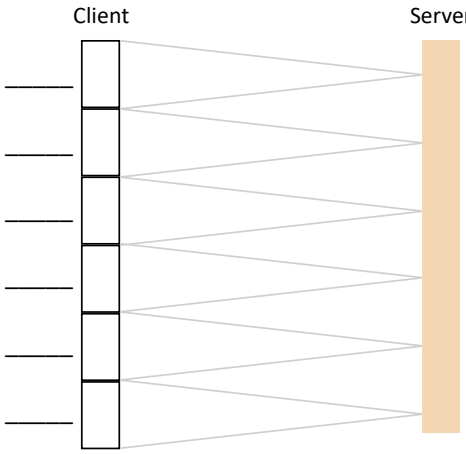
a. Is this connection persistent or non-persistent? (Circle your answer)
Answer: (3 pts) non-persistent – multiple TCP handshakes

b. If this connection has 2 parallel connections, how many packets could have been transmitted? Circle all correct answers:

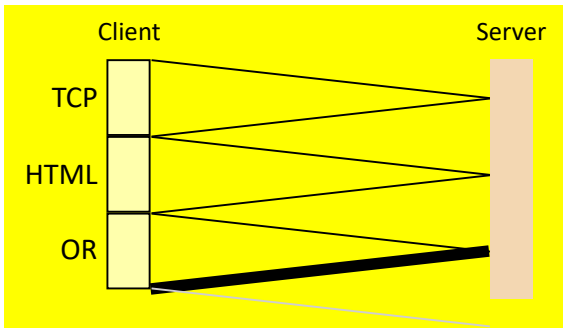
2 3 4 5 6 7 8

Answer: (2 pts) 3 & 4

c. Assume we have a total of 5 packets and have a persistent connection with limitless pipelining. Redraw the diagram.

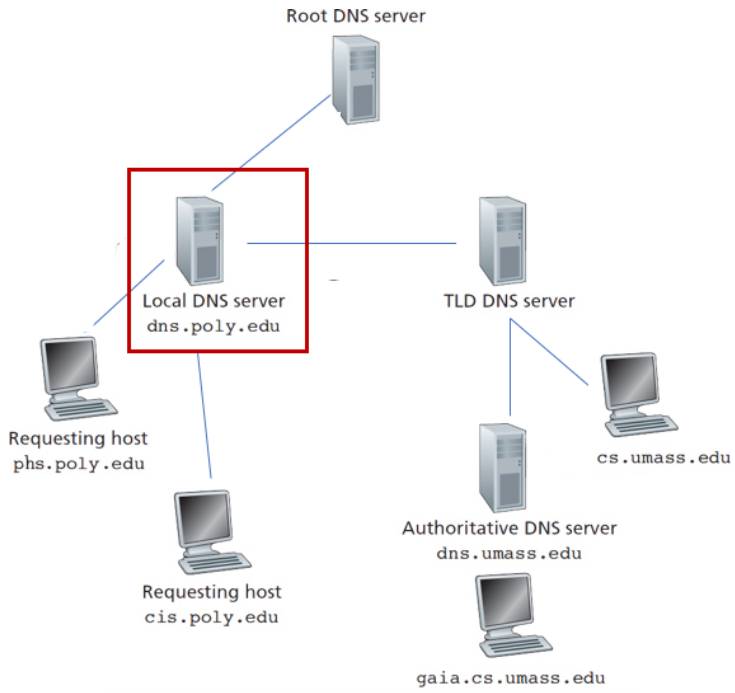


Answer (5 pts):



7. DNS (14 pts)

READ CAREFULLY



This is the same DNS diagram from class, with two new computers added: phs.poly.edu and cs.umass.edu.

ALL QUESTIONS ARE ABOUT THE CONTENTS OF THE DNS TABLE IN **DNS.POLY.EDU**.

All entries are good for one hour. Show what is added at each stage by using a plus "+". Abbreviate to just the first part of a name. For example, +cs 60 means the cs.umass.edu host is added to poly's table for 60 minutes. When an entry expires, use minus "-". For example, "-cs" means the cs.umass.edu entry has disappeared from poly's table.

There are four items always in dns.poly.edu's table – Root, the TLD, the IP for cis.poly.edu and phs.poly.edu. Those are in the table forever, and I've added those for you. Only show the changes at each stage. Some have no changes.

Contents of dns.poly.edu DNS table

Time	Event	Contents
12:00	Start	+Root ∞, +TLD ∞, +cis ∞, +phs ∞
12:15	cis.poly.edu asks for IP for gaia	
12:30	phs asks for IP for gaia	
12:45	cis asks for cs.umass.edu	
1:00	phs asks for cs	
1:15	phs asks for gaia	

At 1:30, what are the final contents of the table and the time remaining for each entry?

Root ∞, TLD ∞, cis ∞, phs ∞, what else? _____

Answer – 2 pts for each correct row. Showing what is in the table in every row is OK – do not deduct points for that. You must at least have the entries shown. 2 points for each row starting at 12:15:

Time	Event	Contents

12:00	Start	+Root ∞, +TLD ∞, +cis ∞, +phs ∞
12:15	cis.poly.edu asks for IP for gaia	+gaia 60, +dns.umass 60
12:30	phs asks for IP for gaia	
12:45	cis asks for cs.umass.edu	+cs 60
1:00	phs asks for cs	
1:15	phs asks for gaia	+gaia 60, +dns.umass 60

Root ∞, TLD ∞, cis ∞, phs ∞, what else? _____

Answer (4 pts – 2 for gaia 45, 2 for dns.uass 45. Deduct 1 point if they show other still on the list):
gaia 45, dns.umass 45