

CSI 2470 Home Assignment 2

Winter 2019

Total points: 50 Points

Note: This is individual assignment. You can't take help from colleagues. Your solution (answers of all questions) should be in one-word file and submitted to Moodle. Follow naming convention given in syllabus file. No late submission will be accepted. For questions relevant to Wireshark and Packet Tracer, screen shots should be submitted as evidence to support your answer, i.e., you should provide your explanation based on the screen shot.

Question 1 (9 points)

Refer packet tracer lab 02 uploaded on the Moodle and answer following questions.

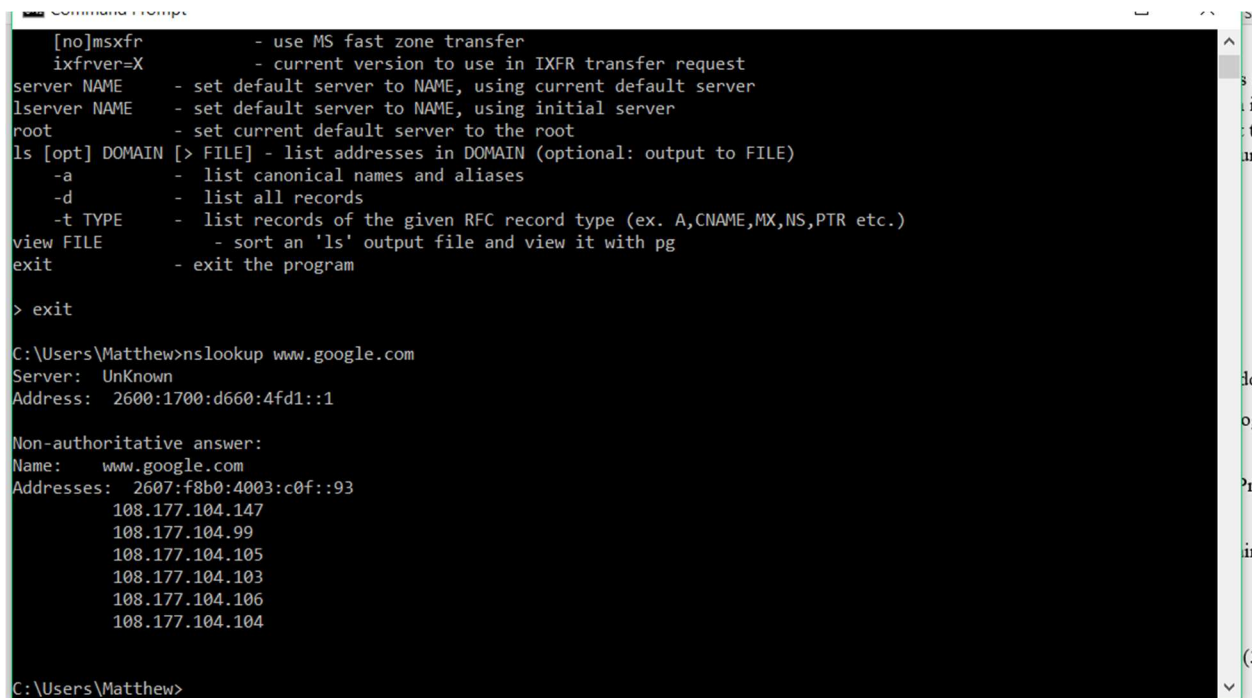
Question 1.1. What is purpose of DHCP and DNS protocols (2 points)?

DHCP (Dynamic Host configuration Protocol) is usually run by a server. It assigns users an IP address.

DNS (Domain name System) this naming system translates easy to understand addresses, like google.com and converts it to an IP address.

Question 1.2. What is purpose of lookup? Try nslookup command from any PC to DNS server. Print the output (2 points)

Nslookup stands for name server lookup. This tool allows you to lookup the IP address of a domain name, or look up the reverse.



```
[no]msxfr      - use MS fast zone transfer
ixfrver=X      - current version to use in IXFR transfer request
server NAME    - set default server to NAME, using current default server
ls server NAME - set default server to NAME, using initial server
root           - set current default server to the root
ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)
  -a           - list canonical names and aliases
  -d           - list all records
  -t TYPE      - list records of the given RFC record type (ex. A,CNAME,MX,NS,PTR etc.)
view FILE      - sort an 'ls' output file and view it with pg
exit           - exit the program

> exit

C:\Users\Matthew>nslookup www.google.com
Server:  UnKnown
Address:  2600:1700:d660:4fd1::1

Non-authoritative answer:
Name:     www.google.com
Addresses: 2607:f8b0:4003:c0f::93
          108.177.104.147
          108.177.104.99
          108.177.104.105
          108.177.104.103
          108.177.104.106
          108.177.104.104

C:\Users\Matthew>
```

CSI 2470 Home Assignment 2

Winter 2019

Question 1.3. Explain the purpose of any of three DNS records (e.g. Type A, NS, MX , NS etc.) (3 points)

Type A (Address mapping record) : stores host name and ipv4 ip address

NS record (Name server Record) : specifies the Domain name's DNS.

Cert record (Certification Record): stores encryption certificates.

Question 1.4: Explain why DNS runs on top of UDP and not TCP (1 points)

UDP is the faster option than TCP. It also has less overhead.

Question 1.5: What did you learn in this lab that you believe is useful in your professional network engineer/programmer role? (1 points) I learned how to find the ip address of a domain name.

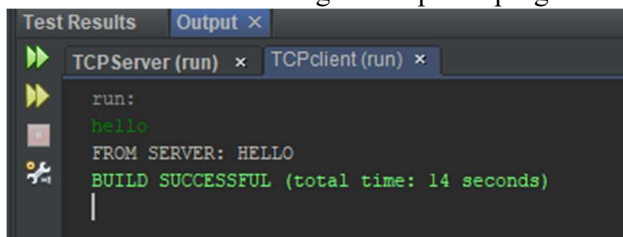
Question 2 (2 points)

If the TCP server were to support n simultaneous connections, each from a different client host, how many sockets would the TCP server need?

The client host would need 'n' number of sockets.

Question 3 (2+1points)

- Run the sample example of client server application given in lecture slides that uses TCP sockets. Attach screen shot showing the output of program



```
Test Results Output x
TCPClient (run) x TCPServer (run) x
run:
hello
FROM SERVER: HELLO
BUILD SUCCESSFUL (total time: 14 seconds)
```

- For the client-server application over TCP, why must the server program be executed before the client program? For the client-server application over UDP, why may the client program be executed before the server program?

The server needs to be executed before the client, so that when the client looks to connect, the server is there to respond and complete the handshake.

For UDP applications. The server does not need to respond in order communicate. The server just reads anything that is sent to it, and responds.

CSI 2470 Home Assignment 2

Winter 2019

Question 4 (1+1+2+2+2=8 points)

Using Wireshark capture HTTP GET message (i.e., this is the actual content of an HTTP GET message). Add screenshots to support your answers.

No.	Time	Source	Destination	Protocol	Length	Info
21	3.048680	192.168.1.81	96.17.112.108	HTTP	247	GET /Market.svc/AppTileV3?symbols=&contentType=3&tileType=0&lc
22	3.049154	192.168.1.81	96.17.112.108	HTTP	271	GET /Market.svc/AppTileV3?symbols=30.10.%21DJI.30.%24INDU&cont
23	3.052448	192.168.1.81	96.17.112.108	HTTP	268	GET /Market.svc/AppTileV3?symbols=29.10.%40CCO.29.COMP&content
26	3.082114	96.17.112.108	192.168.1.81	HTTP/X...	602	HTTP/1.1 200 OK
30	3.083504	96.17.112.108	192.168.1.81	HTTP/X...	766	HTTP/1.1 200 OK
34	3.087153	96.17.112.108	192.168.1.81	HTTP/X...	772	HTTP/1.1 200 OK
67	6.244936	192.168.1.81	128.119.245.12	HTTP	591	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
69	6.316219	128.119.245.12	192.168.1.81	HTTP	293	HTTP/1.1 304 Not Modified
84	8.866379	192.168.1.81	128.119.245.12	HTTP	591	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
85	8.938379	128.119.245.12	192.168.1.81	HTTP	292	HTTP/1.1 304 Not Modified
87	9.379877	192.168.1.81	128.119.245.12	HTTP	591	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
88	9.451158	128.119.245.12	192.168.1.81	HTTP	292	HTTP/1.1 304 Not Modified
98	9.527468	192.168.1.81	128.119.245.12	HTTP	591	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
125	9.600574	128.119.245.12	192.168.1.81	HTTP	292	HTTP/1.1 304 Not Modified
216	47.150897	192.168.1.81	128.119.245.12	HTTP	361	HEAD /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
218	47.221759	128.119.245.12	192.168.1.81	HTTP	411	HTTP/1.1 200 OK

a) What is the URL of the document requested by the browser?

/wireshark-labs/INTRO-wireshark-file.html

b) What version of HTTP is the browser running?

Its running HTTP 1.1

c) Does the browser request a non-persistent or a persistent connection?

HTTP 1.1 is persistent by default

d) What is the IP address of the host on which the browser is running?

192.168.1.81

e) What type of browser initiates this message? Why is the browser type needed in an HTTP request message?

Mozilla 5.0

Browser type is needed because each browser will display the html in a different way.

Question 5 (1+1+2+2=6 points)

Using Wireshark capture reply sent from the server in response to the HTTP GET message in the question above. Add screenshots to support your answers. Answer the following questions, indicating where in the message below you find the answer:

a) Was the server able to successfully find the document or not? What time was the document reply provided?

Yes, the server found the document.

The document reply was at 9.379877

b) When was the document last modified?

Thursday Feb 07 2019 6:59:01 GMT

c) How many bytes are there in the document being returned?

591 bytes

CSI 2470 Home Assignment 2

Winter 2019

- d) What are the first 5 bytes of the document being returned? Did the server agree to a persistent connection?
the first 5 bytes contain the addresses, yes the server agreed to a persistent connection.

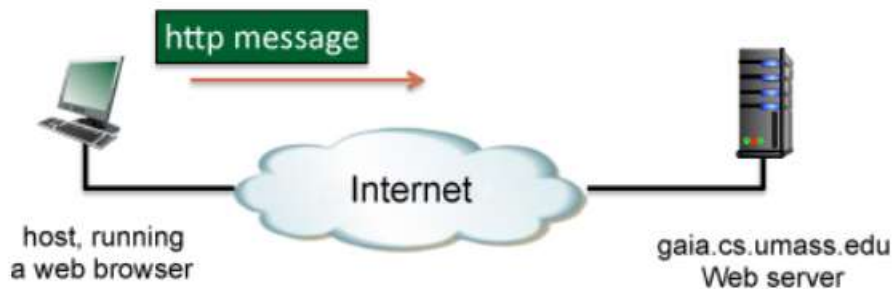
Question 6 (2+2+2=6 points)

Using Wireshark, capture the “http” packets of www.yahoomail.com. Answer the following questions. Provide a screenshot and mark the answer:

- a) Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
Both are running HTTP 1.1
- b) What languages (if any) does your browser indicate that it can accept to the server?
- c) What is the IP address of the Yahoo! Mail server?

Question 7 (10 points)

Consider the figure below, where a client is sending an HTTP GET message to a web server, gaia.cs.umass.edu.



Suppose the client-to-server HTTP GET message is the following:

```
GET /kurose_ross/interactive/quotation7.htm HTTP/1.1
Host: gaia.cs.umass.edu
Accept: text/plain, text/html, text/xml, image/png, image/gif,
audio/mpeg, audio/basic, video/mp4, video/mpeg, application/*, */*
Accept-Language: en-us, en-gb;q=0.9, en;q=0.5, fr, fr-ch, zh, fi,
ar, cs
If-Modified-Since: Fri, 25 Jan 2019 09:28:59 -0800
User Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64;
Trident/5.0)
```

Answer the following questions:

CSI 2470 Home Assignment 2

Winter 2019

- What is the name of the file that is being retrieved in this GET message?

quotation7.htm

- What version of HTTP is the client running? Ver. 1.1
- What formats of text, images, audio, and video does the client browser prefer to receive? [Note: for this and the following questions on browser media and language preferences, you will need to do a bit of additional reading on the Web.]

text/plain, text/html, text/xml, image/png, image/gif, audio/mpeg, audio/basic, video/mp4, video/mpeg, application/*, */*

HERE is a good place to start.]

- What do the strings "application/*" and "*/*" signify in the Accept: header?

It means all types of applications, and all types of media types.

- What languages is the browser indicating that it is willing to accept? [Note: you can look at your own browser preferences to get a listing of language codes.]

English, queens English, French, French (Switzerland), Chinese, Finnish, Arabic, Czech.

en-us, en-gb;q=0.9, en;q=0.5, fr, fr-ch, zh, fi, ar, cs

- What is the meaning of the "relative quality factor," q, associated with the various version of English? [Note: **HERE** is a good place to start. See also **[RFC 2616]**.]

specifies what language the user would prefer.

- What is the client's preferred version of English? What is the browser's least preferred version of English?

The client's preferred English is United kingdom English, and least preferred is American English

- Does the browser sending the HTTP message prefer Swiss French over traditional French? Explain.

No, there is no rating given to either of the choices

- Does the client already have a (possibly out-of-date) copy of the requested file? Explain. If so, approximately how long ago did the client receive the file, assuming the GET request has just been issued?

Possibly, the file was last modified on January 25th

CSI 2470 Home Assignment 2

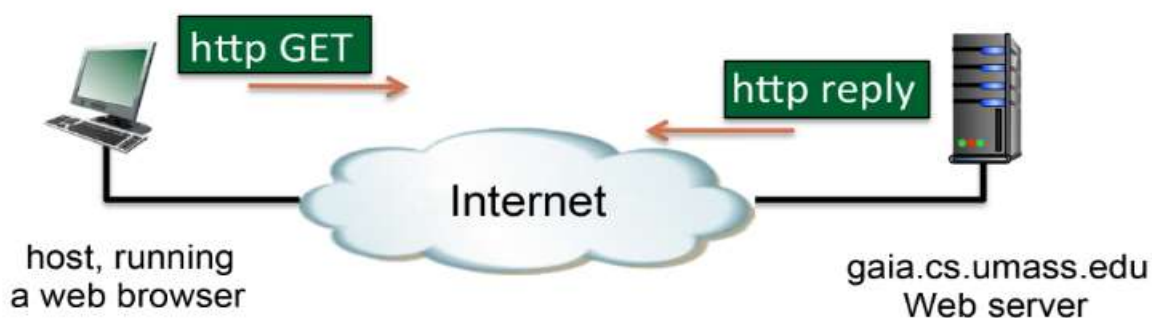
Winter 2019

- What is the type of client browser and the client's operating system? [Note: To answer this, you'll need to understand the User Agent: header field. **HERE** is a good place to start.]

Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)

Question 8 (6 points)

Consider the figure below, where the server is sending a HTTP RESPONSE message back the client.



Suppose the server-to-client HTTP RESPONSE message is the following:

```
HTTP/1.0 404 Not Found
Date: Fri, 25 Jan 2019 17:49:31 +0000
Server: Apache/2.2.3 (CentOS)
Content-Length: 443
Connection: Close
Content-type: text/html
```

Answer the following questions:

- Is the response message using HTTP 1.0 or HTTP 1.1? Explain.

The response message could be HTTP 1.1 since 1.0 return a error 404

- Was the server able to send the document successfully? Explain

No, the server sent an error and closed the connection

- At what date and time was this response sent?

Fri, 25 Jan 2019 17:49:31 +0000

- How many bytes are there in the document being returned by the server?

CSI 2470 Home Assignment 2

Winter 2019

443 bytes

- what is the default mode of connection for http protocol? Is the connection reply persistent or non persistent? Explain.

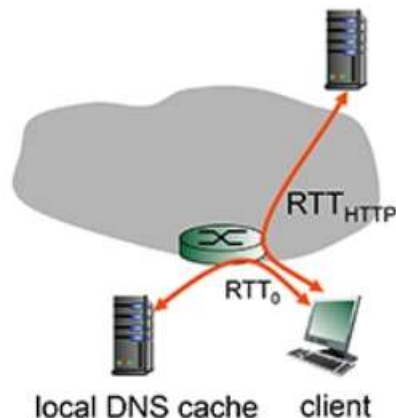
For http 1.0, the default connection mode is non-persistent

- What is the name of the server and its version?

Apache/2.2.3

Question 8 (Extra credit 5 points)

Suppose within your Web browser you click on a link to obtain a Web page. The IP address for the associated URL is not cached in your local host, so a DNS lookup is necessary to obtain the IP address. Suppose that only one DNS server, the local DNS cache, is visited with an with an RTT delay of $RTT_0 = 5$ msec. Initially, let's suppose that the Web page associated with the link contains exactly one object, consisting of a small amount of HTML text. Suppose the RTT between the local host and the Web server containing the object is $RTT_{HTTP} = 34$ msec.



8.1 Assuming zero transmission time for the HTML object, how much time elapses from when the client clicks on the link until the client receives the object?

CSI 2470 Home Assignment 2

Winter 2019

8.2 Now suppose the HTML object references 3 very small objects on the same web server. Neglecting transmission times, how much time elapses from when the client clicks on the link until the base object and all 3 additional objects are received from web server at the client, assuming non-persistent HTTP and no parallel TCP connections?

8.3 Repeat 2. above but assume that the client is configured to support a maximum of 5 parallel TCP connections, with non-persistent HTTP.

8.4 Repeat 2. above but assume that the client is configured to support a maximum of 5 parallel TCP connections, with persistent HTTP.

8.5 What do you notice about the overall delays (taking into account both DNS and HTTP delays) that you computed in cases 2., 3. and 4. above?