COM2022/17/Sem 2 19/20

Academic Misconduct: Coursework will be routinely checked for academic misconduct.
Your submission must be your own work.
Please refer to the Student Handbook to ensure that you know what this means!

UNIVERSITY OF SURREY ©

Faculty of Engineering and Physical Sciences

Department of Computing

Undergraduate Programmes in Computing

COM2022 -
Computer Networking

Individual Coursework (worth 100%)

Submission Instructions:
Please submit your coursework as a ***zip file*** via SurreyLearn. The zip file should contain **a)** a **PDF** with your written answers to the questions and **b)** your python code for which you should supply a short README.txt with instructions on how to run it.

Work you submit must be your own work.

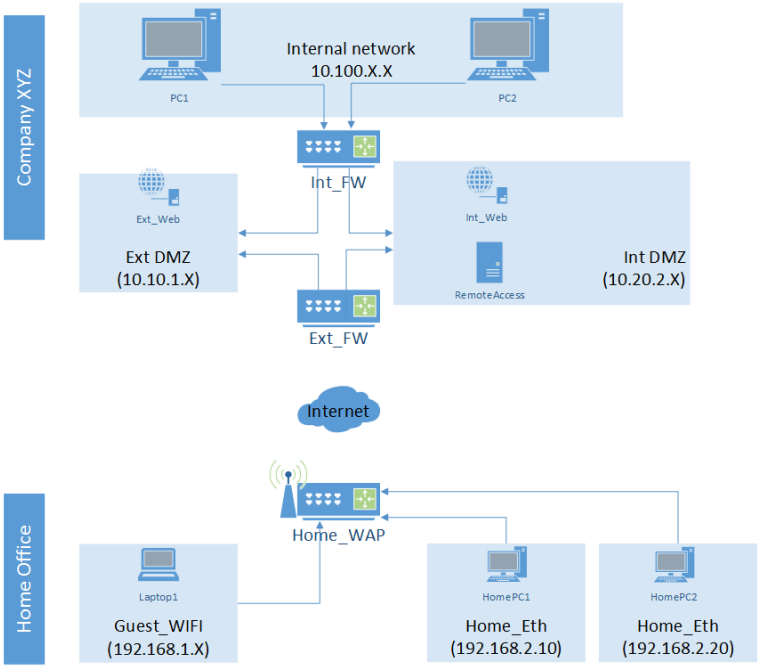
Include your declaration of originality(1st page) as part of your submission (submitting this will be regarded as you having signed it). Late submissions **will** incur the standard 10% penalty per day. If the work is submitted later than **TWO** days after the deadline, it will be marked as 0.

This is now the ONLY assessment for COM2022.

The original set of questions(CW1) contributes 75% while the three EXTENSION questions(ExtCW) are worth 25%. The overall mark is calculated as follows:
Assume x (out 100), y (out of 60) are your marks for CW1 and ExtCW respectively, then your overall grade for this coursework and hence module is:
$0.75x + 0.25\frac{100y}{60}$.

Deadline: 16:00, Wednesday, 27th May 2020
Returned by: Wednesday, 17th June 2020

1. **This question is worth 30%.** It is about setting up a network with firewall rules and different subnets and associated routing. It will demonstrate your understanding of network topology, dhcp and firewall rules. Consider the following diagram (note that it does not show switches that would usually be present):



All appliances in the above diagram run some recent version of Linux.

- Home_WAP is a typical home router with a wireless access point that also acts as a firewall. Its internal IP address is 192.168.**1**.1 for the wireless acess and 192.168.**2**.1 for the wired (ethernet) access. Its external internet IP address is 80.245.7.8 and is allocated via dhcp from the user's ISP.
- Laptop1 is configured via dhcp from the Home_WAP using the Guest_WIFI network and the last octet of its IP address is between 1 and 127, e.g. 192.168.1.64
- HomePC1 and HomePC2 are connect to the Home_WAP router via an ethernet cable as part of the Home_Eth network. Both HomePC1 and HomePC2 have static IP addresses of 192.168.2.10 and 192.168.2.20 respectively.
- Ext_FW is the external stateful firewall of company XYZ. It has 2 external IP addresses, 64.37.180.23 and 64.37.160.63. Its main purpose is to only allow traffic arriving on 64.37.180.23 to the external web server (Ext_Web) in the external DMZ and traffic arriving on 64.37.160.63 to the RemoteAccess server in the internal DMZ.
- Ext_Web is the companies web server which serves up the companies web site. It should be visible to all internet users. Its IP address is 10.10.1.20. The

SEE NEXT PAGE

webserver is configured to listen to request on port 8080 for http requests and port 8443 for https.

- Int_Web is the companies internal web server. Its IP address is 10.20.2.63. It should not be visible to outside users. However, the employees who are on the internal network should be able to access it. Like EXT_Web, Int_Web is also configured to listen to request on port 8080 for http requests and port 8443 for https.
- RemoteAccess is a server that allows home workers to log in using ssh and then access the resources on Int_Web. Its IP address is 10.20.2.22.
- Int_FW is the internal stateful firewall that separates the internal network of company XYZ from its DMZs and the internet.
- PC1 and PC2 are just two of many workstations connected to the internal network of 10.100.X.X. They should be able to connect to the internet, Int_Web, Ext_Web and RemoteAccess.

(a) Using the following table describe the firewall rules for Ext_FW which allow it to deal with traffic being initiated from the internet, eg a user surfing the company's website or a remote worker using ssh to log onto RemoteAccess. Ensure that you have a deny rule to block all other traffic! The first two lines in the table are just examples of the notation you should use in completing your table. Note that ***** means **any** and can be used in all columns except for the action column. You should use the same table format in subsequent questions, too. [3 marks]

source	port	destination	port	protocol	action
123.456.0.0\16	*	234.456.346.0\24	8000	tcp	deny
*	8000	234.567.8.9	9000	udp	allow
?	?	?	?	?	?

(b) Provide outgoing rules for Ext_FW that allows DNS lookups from the internal network as well as requests to external websites running on the standard ports for http and https. DNS lookups should also be possible from RemoteAccess but not from Int_Web. [3 marks]

(c) If the company website is www.companyxyz.com, what IP address should that resolve to? If remote.companyxyz.com is the address of the RemoteAccess server, what IP address should that resolve to? Give a short explanation for your answer. [3 marks]

(d) Explain what else needs to be done on Ext_FW before internet users can see the company's website using the standard ports for http and https? [3 marks]

QUESTION 1 CONTINUES ON NEXT PAGE

(e) Assume that users logged onto RemoteAccess can then ssh onto their workstation on the internal network. Provide the firewall rules of Int_FW for ssh traffic going from RemoteAccess to the internal network. [3 marks]

(f) Sometimes the webadmin would like to ssh onto Ext_Web from home to fix some issues. In the set-up so far, is this currently possible(assuming ssh is running on Ext_Web)? Give a short explanation for your answer. [2 marks]

(g) In the set-up so far, assuming there is switch to which both Int_Web and RemoteAccess are connected, can the webadmin ssh onto Int_Web from home to fix some issues (again assuming ssh is running on Int_Web). Give a short explanation for your answer. [2 marks]

(h) Provide the firewall rules for INT_FW that govern the traffic from the internal network to allow general web acess(http and https), DNS lookups and access to INT_WEB(http,https) and RemoteAccess(ssh). [3 marks]

(i) The Home_WAP is configured such that WIFI devices use a guest network on 192.168.1.0/255 and all wired devices are on 192.168.2.0/255. Like most people, the owner provides the access credentials for WIFI access on her Guest_WIFI to her friends and family who visit her. Assume that HomePC1 provides a Samba Share (i.e. the Linux equivalent of a Windows Share Folder) of private family documents and HomePC2 provides shared access to a printer via the Common UNIX Printing System (CUPS) daemon (the printer is not shown in the diagram).

- Why is there likely to be no direct access from the Guest_WIFI network to the Home_Eth network? [1 mark]
- Why would you provide a segregated WIFI network in the first place? [1 mark]
- Assume that the owner wants her own laptop to have access to both the share folder and the printer on the Home_Eth network while being connected to the Guest_WIFI. Recall that the Guest_WIFI uses dhcp. How could you configure dhcp and the firewall to only allow her laptop access to the services provided by the two PCs. [3 marks]
- When accessing XYZ's website from HomePC2 (192.168.2.20) and from a mobile phone (192.168.1.101),which is connected to the Guest_WIFI, what IP addresses will show up in the access logs of the webserver for these devices. Provide a short explanation for your answer. [3 marks]

SEE NEXT PAGE

2. **This question is worth 30%.** This question is about some of the theory that was covered in the lectures and will test your understanding of network latency, bandwidth and packet loss.

   (a) Suppose there is exactly one packet switch between a sending host and a receiving host. The transmission rates between the sending host and the switch and between the switch and the receiving host are R_1 and R_2 , respectively. Assuming that the switch uses store-and-forward packet switching, what is the total end-to-end delay to send a packet of length L? (Ignore queuing, propagation and processing delay.) [1 mark]

   (b) Suppose users share a 2 Mbps link. Also suppose each user transmits continuously at 1 Mbps when transmitting, but each user transmits only 20 percent of the time.

      (i). When circuit switching is used, how many users can be supported? [1 mark]

      (ii). For the remainder of this problem, suppose packet switching is used. Why will there be essentially no queuing delay before the link if two or fewer users transmit at the same time? Why will there be a queuing delay if three users transmit at the same time? [2 marks]

      (iii). Find the probability that a given user is transmitting. [1 mark]

      (iv). Suppose now there are three users. Find the probability that at any given time, all three users are transmitting simultaneously. [1 mark]

   (c) Suppose Host A wants to send a large file to Host B. The path from Host A to Host B has three links, of rates $R1 = 500$ kbps, $R2 = 2$ Mbps, and $R3 = 1$ Mbps.

      (i). Assuming no other traffic in the network, what is the throughput for the file transfer? [1 mark]

      (ii). Suppose the file is 4 million bytes. Dividing the file size by the throughput, roughly how long will it take to transfer the file to Host B? Show working to support your answer which must be stated in seconds. [1 mark]

      (iii). Repeat 2(c)(i) and 2(c)(ii), but now with $R2$ reduced to 100 kbps. [2 marks]

   (d) $d_{\text{end-to-end}} = N\frac{L}{R}$ gives a formula for the end-to-end delay of sending one packet of length L over N links of transmission rate R. Explain why the generalized formula for sending P such packets back-to-back over the N links

QUESTION 2 CONTINUES ON NEXT PAGE

is:
$N(L/R) + (P-1)(L/R) = (N+P-1)(L/R)$
Hint: How long does the first packet take to arrive? When the first packet is received where are all the remaining packets and how long does the 2^{nd} packet then take to arrive. Generalise from that scenario for the solution. [3 marks]

(e) What information is used by a process running on one host to identify a process running on another host? [2 marks]

(f) List the four broad classes of services that a transport protocol can provide. For each of the service classes, indicate if either UDP or TCP (or both) provides such a service. [4 marks]

(g) A UDP server usually only needs one socket, whereas a basic TCP server needs two sockets. Why? If a TCP server were to support n simultaneous connections, each from a different client host, how many sockets would the TCP server need? [3 marks]

(h) Assume you request a webpage consisting of one document and five images. The document size is 1 kbyte, all images have the same size of 50 kbytes, the download rate is 1 Mbps, and the Round Trip Time (RTT) is 100 ms. How long does it take to obtain the whole webpage under the following conditions? (Assume no DNS name query is needed and the impact of the request line and the headers in the HTTP messages is negligible).

(i). Nonpersistent HTTP with serial connections. [1 mark]

(ii). Nonpersistent HTTP with six parallel connections. [1 mark]

(iii). Persistent HTTP with one connection. [1 mark]

(i) Suppose Client A requests a web page from Server S through HTTP and its socket is associated with port 33000.

(i). What are the source and destination **ports** for the segments sent from A to S? [1 mark]

(ii). What are the source and destination **ports** for the segments sent from S to A? [1 mark]

(iii). Can Client A contact Server S using UDP as the transport protocol, instead? Justify your answer. [1 mark]

(j) Assume that a host receives a UDP segment with 01011101 11110010 (we separated the values of each byte with a space for clarity) as the checksum.

QUESTION 2 CONTINUES ON NEXT PAGE

The host adds the 16-bit words over all necessary fields excluding the checksum and obtains the value 00110010 00001101. Is the segment considered correctly received or not? What does the receiver do? [2 marks]

SEE NEXT PAGE

3. **This question is worth 20%.**. It is about network traffic analysis and uses Wireshark as the capturing tool. It will test your understanding of different application protocols and the type of traffic they generate.

   (a) Consider the following string of ASCII characters that were captured by Wireshark when the browser sent an HTTP GET message (i.e., this is the actual content of an HTTP GET message). The characters <cr><lf> are carriage return and line-feed characters (that is, the character string <cr> in the text below represents the single carriage-return character that was contained at that point in the HTTP header). Answer the following questions, indicating where in the HTTP GET message below you find the answer:

```
GET /cs453/index.html HTTP/1.1<cr><lf>Host: gai
a.cs.umass.edu<cr><lf>User-Agent: Mozilla/5.0 (
Windows;U; Windows NT 5.1; en-US; rv:1.7.2) Gec
ko/20040804 Netscape/7.2 (ax) <cr><lf>Accept:ex
t/xml, application/xml, application/xhtml+xml, text
/html;q=0.9, text/plain;q=0.8,image/png,*/*;q=0.5
<cr><lf>Accept-Language: en-us,en;q=0.5<cr><lf>Accept-
Encoding: zip,deflate<cr><lf>Accept-Charset: ISO
-8859-1,utf-8;q=0.7,*;q=0.7<cr><lf>Keep-Alive: 300<cr>
<lf>Connection:keep-alive<cr><lf><cr><lf>
```

   (i). What is the URL of the document requested by the browser? [1 mark]

   (ii). What version of HTTP is the browser running? [1 mark]

   (iii). Does the browser request a non-persistent or a persistent connection? [1 mark]

   (iv). What type of browser initiated this message? Why is the browser type needed in an HTTP request message? [2 marks]

   (b) The text below shows the reply sent from the server in response to the HTTP GET message in the question above. Answer the following questions, indicating where in the message below you find the answer.

```
HTTP/1.1 200 OK<cr><lf>Date: Tue, 07 Mar 2008
12:39:45GMT<cr><lf>Server: Apache/2.0.52 (Fedora)
<cr><lf>Last-Modified: Sat, 10 Dec2005 18:27:46
GMT<cr><lf>ETag: "526c3-f22-a88a4c80"<cr><lf>Accept-
Ranges: bytes<cr><lf>Content-Length: 3874<cr><lf>
Keep-Alive: timeout=max=100<cr><lf>Connection:
```

QUESTION 3 CONTINUES ON NEXT PAGE

```
Keep-Alive<cr><lf>Content-Type: text/html; charset=
ISO-8859-1<cr><lf><cr><lf><!doctype html public "-
//w3c//dtd html 4.0transitional//en"><lf><html><lf>
<head><lf> <meta http-equiv="Content-Type"
content="text/html; charset=iso-8859-1"><lf> <meta
name="GENERATOR" content="Mozilla/4.79 [en] (Windows NT
5.0; U) Netscape]"><lf> <title>CMPSCI 453 / 591 /
NTU-ST550ASpring 2005 homepage</title><lf></head><lf>
<much more document text following here (not shown)>
```

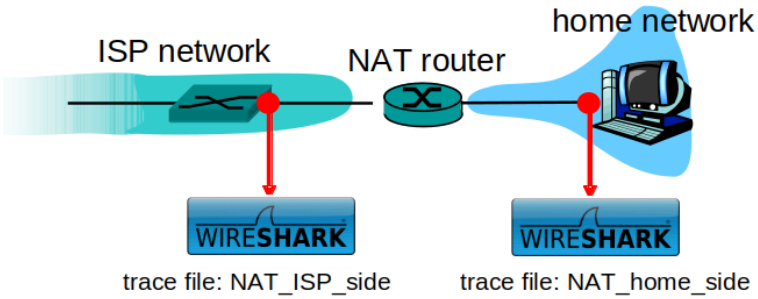
(i). Was the server able to successfully find the document or not? What time was the document reply provided? [2 marks]

(ii). When was the document last modified? [1 mark]

(iii). How many bytes are there in the document being returned? [1 mark]

(iv). What are the first 5 bytes of the document being returned? Did the server agree to a persistent connection? [2 marks]

(c) This question is about Network Address Translation (NAT). Consider the folowint set-up(typical of most home network set-ups):



You will need to use the provided NAT_home_side.pcap and NAT_ISP_side.pcap capture files available on SurreyLearn. Open the NAT_home_side file and answer the following questions. You might find it useful to use a Wireshark filter so that only frames containing HTTP messages are displayed from the trace file.

(i). What is the IP address of the client? [1 mark]

(ii). The main Google server that will serve up the main Google web page has the IP address 64.233.169.104. In order to display only those frames containing HTTP messages that are sent to/from this Google, server, enter the expression "`http && ip.addr == 64.233.169.104`" (without quotes) into the Filter: field in Wireshark. Consider now the HTTP GET sent

QUESTION 3 CONTINUES ON NEXT PAGE

from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET? [2 marks]

(d) Recall that before a GET command can be sent to a HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? At what time is the ACK received at the client? (Note: to find these segments you will need to clear the Filter expression you entered previously. If you enter the filter "tcp", only TCP segments will be displayed by Wireshark). [1 mark]

(e) In the following we'll focus on the two HTTP messages (GET and 200 OK) and the TCP SYN and ACK segments identified above. Our goal below will be to locate these two HTTP messages and two TCP segments in the trace file (NAT_ISP_side) captured on the link between the router and the ISP. Because these captured frames will have already been forwarded through the NAT router, some of the IP address and port numbers will have been changed as a result of NAT translation. Open the NAT_ISP_side. Note that the time stamps in this file and in NAT_home_side are not synchronized since the packet captures at the two locations were not started simultaneously. (Indeed, you should discover that the timestamps of a packet captured at the ISP link is actually less that the timestamp of the packet captured at the client PC).

(i). In the NAT_ISP_side trace file, find the HTTP GET message that was sent from the client to the Google server at time 7.109267 (where t=7.109267 is time at which this was sent as recorded in the NAT_home_side trace file). At what time does this message appear in the NAT_ISP_side trace file? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET (as recording in the NAT_ISP_side trace file)? Which of these fields are the same as, and which are different to, your answer to 3(c)(ii) above? [2 marks]

(ii). Have any fields in the HTTP GET message changed? Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change. [3 marks]

SEE NEXT PAGE

4. **This question is worth 20%.** It is about implementing two networking scenarios in Python and to demonstrate them running.

   (a) Your task is to write a UDPPing client. You are given the complete code for the UDPPing server (UDPPingServer.py available on SurreyLearn). You need to compile and run this code before running your client program. You do not need to modify the server code. In this server code, 30% of the client's packets are simulated to be lost. You should study this code carefully, as it will help you write your UDPPing client.

   The server sits in an infinite loop listening for incoming UDP packets. When a packet comes in and if a randomized integer is greater than or equal to 4, the server simply capitalizes the encapsulated data and sends it back to the client.

   You need to implement the following client program. The client should send 10 pings to the server. Because UDP is an unreliable protocol, a packet sent from the client to the server may be lost in the network, or vice versa. For this reason, the client cannot wait indefinitely for a reply to a ping message. You should get the client to wait up to one second for a reply; if no reply is received within one second, your client program should assume that the packet was lost during transmission across the network. You will need to look up the Python documentation to find out how to set the timeout value on a datagram socket.

   Specifically, your client program should

   (i). send the ping message using UDP (Note: Unlike TCP, you do not need to establish a connection first, since UDP is a connectionless protocol). [1 mark]

   (ii). print the response message from server, if any. [1 mark]

   (iii). calculate and print the round trip time (RTT), in seconds, of each packet, if server responses; [1 mark]

   (iv). otherwise, print "Request timed out". [1 mark]

   (v). During development, you should run the UDPPingerServer.py on your machine, and test your client by sending packets to localhost (or, 127.0.0.1). After you have fully debugged your code, you should see how your application communicates across the network with the ping server and ping client running on different machines. (You might want to use OpenNebula for this.) [2 marks]

   (vi). The ping messages in this exercise are formatted in a simple way. The client message is one line, consisting of ASCII characters in the following

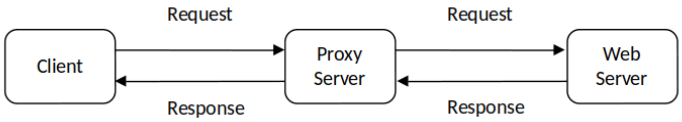
QUESTION 4 CONTINUES ON NEXT PAGE

format:
Ping sequence_number time
where sequence_number starts at 1 and progresses to 10 for each successive ping message sent by the client, and time is the time when the client sends the message. [1 mark]

Please submit the complete client code including screenshots of the client verifying that your ping program works as required. [1 mark]

(b) Your task is to develop a small web proxy server which is able to cache web pages. It is a very simple proxy server which only understands simple GET-requests, but is able to handle all kinds of objects - not just HTML pages, but also images.

Generally, when the client makes a request, the request is sent to the web server. The web server then processes the request and sends back a response message to the requesting client. In order to improve the performance we create a proxy server between the client and the web server. Now, both the request message sent by the client and the response message delivered by the web server pass through the proxy server. In other words, the client requests the objects via the proxy server. The proxy server will forward the client's request to the web server. The web server will then generate a response message and deliver it to the proxy server, which in turn sends it to the client as shown in the following figure:



Run the proxy server program using your command prompt and then request a web page from your browser. Direct the requests to the proxy server using your IP address and port number, e.g. `http://localhost:8888/www.google.com`

(i). The skeleton code (ProxyServer.py) for the proxy server is available on SurreyLearn. You are to complete the skeleton code. The nine places where you need to fill in code are marked with **#Fill in start** and **#Fill in end**. Each place may require one or more lines of code. [9 marks]

(ii). Currently the proxy server does no error handling. This can be a problem especially when the client requests an object which is not available, since the "404 Not found" response usually has no response body and the proxy assumes there is a body and tries to read it. Implement handling a "404 Not found" error. [2 marks]

QUESTION 4 CONTINUES ON NEXT PAGE

Please submit the complete proxy server code and include screenshots of the client side verifying that you indeed get web pages and handle 404 errors via the proxy server. [1 mark]

SEE NEXT PAGE

5. **EXTENSION: This question is worth 20 points.** It is about reading RFCs and interpreting them:

   (a) Read RFC 5321 for SMTP.

      (i). Quoting the paragraph of the RFC in which it is first defined, what does MTA stand for ? [1 mark]

      (ii). A user sends the same email to 80 recipients, ie not 80 separate emails but one email with 80 recipients. The server returns a 552 error message-"Too many recipients". Quoting the relevant paragraphs in the RFC: Answer the following questions:

         (A) Why is or isn't the error code correct? [2 marks]

         (B) Why is or isn't the response of the server compliant with the RFC? [2 marks]

      (iii). Again quoting the relevant paragraphs from the RFC:

         (A) Explain the purpose of the intial 220 message [2 marks]

         (B) State its timeout and whether its length is compulsory [2 marks]

         (C) Explain whether or not a TCP connection has been established when waiting for the initial 220 message. [2 marks].

      (iv). Explain why an SMTP server retries to transmit a message even though TCP is used to connect with the destination? [4 marks]

   (b) Read the DNS SRV RFC, RFC 2782. What is the purpose of the SRV record? [5 marks]

SEE NEXT PAGE

6. **EXTENSION: This question is worth 20 points.** It is about security

(a) Consider RSA with $p = 11$ and $q = 19$.

(i). What are n and z? [1 mark]

(ii). Let e be 17. Why is this an acceptable choice for e? [1 mark]

(iii). Find d such that $de = 1 \pmod{z}$. [1 mark]

(iv). Encrypt the message $m = 7$ using the key (n, e). Let c denote the corresponding ciphertext. Verify that you can decrypt c as well by using the private key. Show all work. [1 mark]

(b) This question deals with the Diffie-Hellman (DH) public-key encryption algorithm, which allows two entities to agree on a shared key. The DH algorithm makes use of a large prime number p and another large number g less than p. Both p and g are made public (so that an attacker would know them). In DH, Alice and Bob each independently choose secret keys, S_A and S_B, respectively. Alice then computes her public key, T_A, by raising g to S_A and then taking $\pmod{p}$. Bob similarly computes his own public key T_B by raising g to S_B and then taking $\pmod{p}$. Alice and Bob then exchange their public keys over the Internet. Alice then calculates the shared secret key S by raising T_B to S_A and then taking $\pmod{p}$. Similarly, Bob calculates the shared key S' by raising T_A to S_B and then taking $\pmod{p}$.

(i). Prove that, in general, Alice and Bob obtain the same symmetric key, that is, prove $S = S'$. [2 marks]

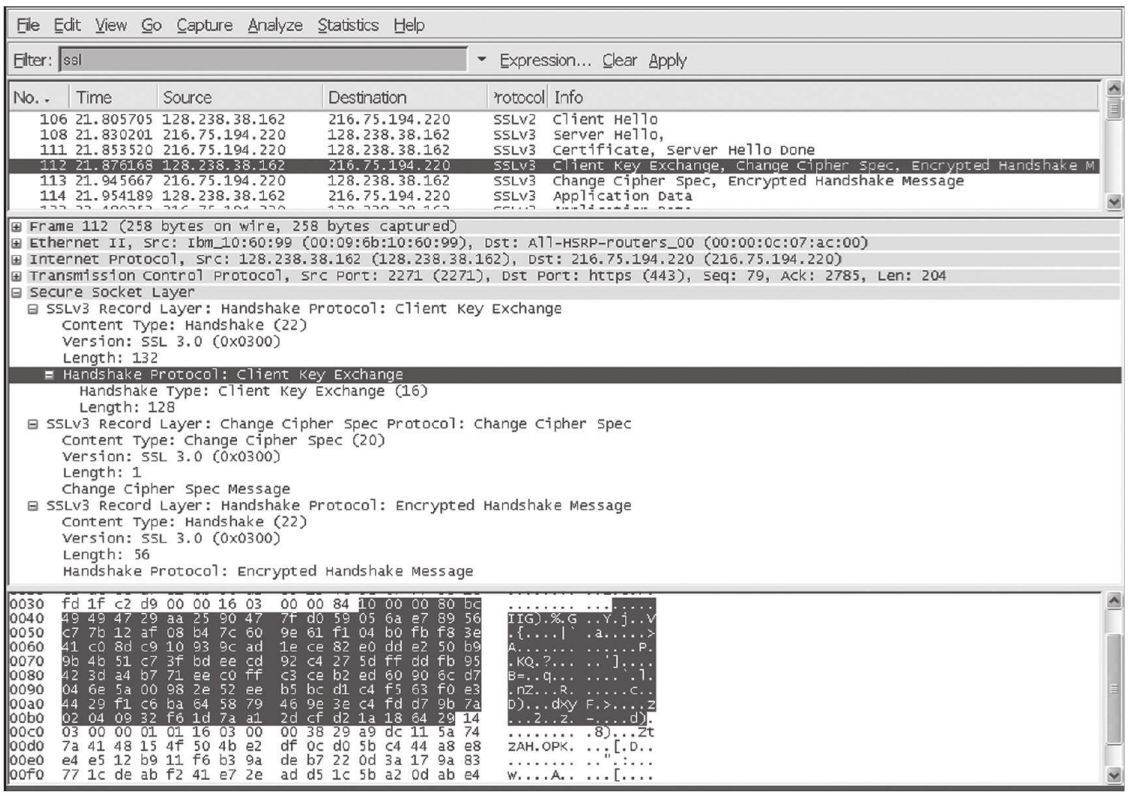
(ii). With $p = 11$ and $g = 2$, suppose Alice and Bob choose private keys $S_A = 5$ and $S_B = 12$, respectively. Calculate Alice's and Bob's public keys, T_A and T_B . Show all work. [1 mark]

(iii). Following up on part (b), now calculate S as the shared symmetric key. Show all work. [1 mark]

(iv). Provide a description that explains how Diffie-Hellman can be attacked by a man-in-the-middle. The description should be in terms of the honest parties Alice and Bob and the attacker, Eve. [4 marks]

(c) Consider the Wireshark output below for a portion of an SSL session.

QUESTION 6 CONTINUES ON NEXT PAGE



(i). Is Wireshark packet 112 sent by the client or server? [1 mark]

(ii). What is the server's IP address and port number? [1 mark]

(iii). Assuming no loss and no retransmissions, what will be the sequence number of the next TCP segment sent by the client? [1 mark]

(iv). How many SSL records does Wireshark packet 112 contain? [1 mark]

(v). Does packet 112 contain a Master Secret or an Encrypted Master Secret or neither? [1 mark]

(vi). Assuming that the handshake type field is 1 byte and each length field is 3 bytes, what are the values of the first and last bytes (in hex) of the Master Secret (or Encrypted Master Secret)? [1 mark]

(d) When Bob signs a message, Bob must put something on the message that is unique to him. Bob could consider attaching a MAC for the signature, where the MAC is created by appending his key (unique to him) to the message, and then taking the hash. Will it cause any problem when Alice would try verification? [2 marks]

SEE NEXT PAGE

7. **EXTENSION: This question is worth 20 points.** It is about wireless and mobile networks

   (a) What does it mean for a wireless network to be operating in "infrastructure mode"? If the network is not in infrastructure mode, what mode of operation is it in, and what is the difference between that mode of operation and infrastructure mode? [3 marks]

   (b) If a node has a wireless connection to the Internet, does that node have to be mobile? Explain. Suppose that a user with a laptop walks around her house with her laptop, and always accesses the Internet through the same access point. Is this user mobile from a network standpoint? Explain. [2 marks]

   (c) Describe the role of the beacon frames in 802.11. [2 marks]

   (d) An access point periodically sends beacon frames. What are the contents of the beacon frames? [2 marks]

   (e) Why are acknowledgements used in 802.11 but not in wired Ethernet? [2 marks]

   (f) What is the difference between passive scanning and active scanning? [2 marks]

   (g) Suppose there are two ISPs providing WiFi access in a particular coffee shop, with each ISP operating its own AP and having its own IP address block.

      (i). Further suppose that by accident, each ISP has configured its AP to operate over channel 11. Will the 802.11b protocol completely break down in this situation? Discuss what happens when two stations, each associated with a different ISP, attempt to transmit at the same time. What is the (theoretical) maximum transmission rate available to the clients? [4 marks]

      (ii). Now suppose that one AP operates over channel 1 and the other over channel 11. How do your answers change? [2 marks]

      (iii). After selecting the AP with which to associate, a wireless host sends an association request frame to the AP, and the AP responds with an association response frame. Once associated with an AP, the host will want to join the subnet (in the IP addressing sense) to which the AP belongs. What does the host do next? [1 mark]

INTERNAL EXAMINER: Steve Wesemeyer