Name_____ Student ID_____ Department/Year_____

1st Examination

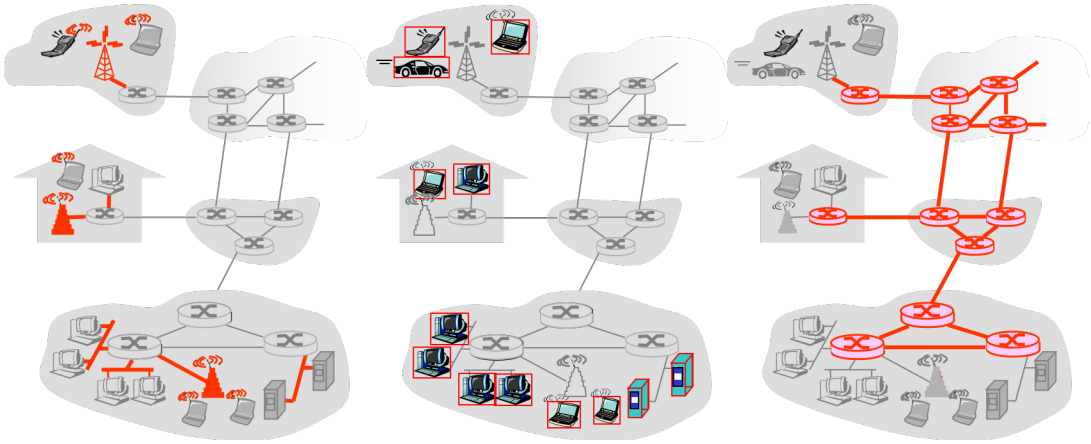
Introduction to Computer Networks (Online)
Class#: EE 4020, Class-ID: 901E31110
Fall 2021

10:20-12:10 Thursday
October 28, 2021

Cautions

1. There are in total 100 points to earn. You have 90 minutes to answer the questions. Skim through all questions and start from the questions you are more confident with.
2. Use only English to answer the questions. Misspelling and grammar errors will be tolerated, but you want to make sure with these errors your answers will still make sense.

1. (ch11, 3pt) Consider the 3 figures below that highlight different parts of the mini-Internet we've seen several times in class.



(a) (b) (c)

(1) Which highlights the access links of the mini-Internet (1pt)?
(2) Which highlights the end systems of the mini-Internet (1pt)?
(3) Which highlights the routers of the mini-Internet (1pt)?

Sample Solution:

(1) (a)
(2) (b)
(3) (c)

2. (ch11, 4pt) Which of the following can be seen in a communication protocol?
   (1) A set of rules that define the functionality of the entities in the communication (1pt).
   (2) A set of rules that articulate the terms used in the communication (1pt).
   (3) A set of rules that define the flow of communication (1pt).
   (4) In the communication flow, a set of events that are triggered by receiving different messages (1pt).

Sample Solution:

All T

3. (ch12, 4pt) Which of the following are access network technologies?
   (1) USB (1pt).
   (2) ADSL (1pt).
   (3) 802.11ax (1pt).
   (4) Bluetooth (1pt).

Sample Solution:

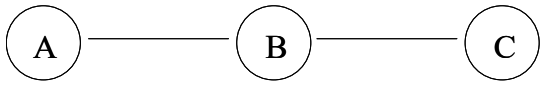
F, T, T, F

4. (ch13, 5pt) Give an example of transporting substances in circuit switching fashion vs. packet switching fashion. Please exclude the water, vehicle, and the knowledge transportation example we've went through in the class, quiz#4, and sp21 exam#1.
   (1) Identify the substance being transported (1pt).
   (2) Identify a circuit switching way to transport the substance (1pt).
   (3) Identify a packet switching way to transport the substance (1pt).
   (4) Justify why the former is circuit switching like (1pt).
   (5) Justify why the latter is packet switching like (1pt).

Sample Solution:

Any example (other than the water, vehicle, and knowledge example) that makes sense will be accepted

5. (ch13, 11pt) Consider a simple network as follows. 12P bits of data need to be sent from node A, through node B, to node C. Link A-B and link B-C are identical. The link bandwidth is R bits per second. The link speed is S meter per second. The length of the link is D meters. Suppose the packet header containing necessary information to delivery any amount of data from A to C is P bits. And the queuing and processing delays are negligible.



(1) If we send all the 12P bits data in one packet, the total numbers of bits in the packet to send is 13P bits (including the P bits necessary for the packet header). What is the total delay (in terms of R, P, S, or D) for all the data to arrive at C (2pt)?

(2) Let's send the 12P bits in 2 equal parts. 6P bits in each part. Each part is sent in a packet. The total number of bits in a packet to send is then 7P bits (including the P bits necessary for the packet header). The two packets are sent back-to-back (i.e., in the pipelined fashion). What is the total delay (in terms of R, P, S, or D) for all the data to arrive at C? (2pt)

(3) Let's send the 12P bits in 3 equal parts. 4P bits in each part. Each part is sent in a packet. The total number of bits in a packet to send is then 5P bits (including the P bits necessary for the packet header). The three packets are sent back-to-back (i.e., in the pipelined fashion). What is the total delay (in terms of R, P, S, or D) for all the data to arrive at C? (2pt)

(4) Let's send the 12P bits in 4 equal parts. 3P bits in each part. Each part is sent in a packet. The total number of bits in a packet to send is then 4P bits (including the P bits necessary for the packet header). The four packets are sent back-to-back (i.e., in the pipelined fashion). What is the total delay (in terms of R, P, S, or D) for all the data to arrive at C? (2pt)

(5) Let's send the 12P bits in 6 equal parts. 2P bits in each part. Each part is sent in a packet. The total number of bits in a packet to send is then 3P bits (including the P bits necessary for the packet header). The six packets are sent back-to-back (i.e., in the pipelined fashion). What is the total delay (in terms of R, P, S, or D) for all the data to arrive at C? (2pt)

(6) What is the optimal number of parts to break the 12P data to minimize the delay? (1pt)

Sample Solution:

(1) 26P/R + 2D/S

(2) 21P/R + 2D/S
(3) 20 P/R + 2D/S
(4) 20 P/R + 2D/S
(5) 21 P/R + 2D/S
(6) 3 or 4 parts

6. (ch14, 12pt) `ping` provides another way to investigate the round-trip time (RTT) to a remote machine. The way it works it very simple – sending a request to the remote machine and the remote machine sending back a response. By calculating the difference in the timestamp of the request and response, `ping` shows the measured RTT on the screen. Using the `–c` flag, one can limit the number of request-response probes.

   Let's `ping` to Amazon and investigate the delay to the popular e-commerce service.

   (1) Login to the PA workstation with your exam account. `ping` to www.amazon.com and create a file `amazon–us.txt` to contain the output as follows. You should see 5 RTT measurements in the output file. Leave the file there for us to grade (4pt).

   ```
   $ ping –c 5 www.amazon.com > amazon-us.txt
   ```

   (2) Examine the output file. You should see the 5 RTT measurements are different. Why? Provide at least 2 reasons (2pt).

   (3) Examine the output file. What is the IP address and the hostname of the server physically answering the Web requests for `www.amazon.com` (2pt)?

   (4) Continue from (3). The domain part of the hostname is obviously different from `amazon.com`. Why is there such a difference (4pt)?

Sample Solution:

(1) Check `amazon–us.txt` on PA workstation

(2) varying queuing delay; varying routes between each of the probes; processing delay

(3) 162.219.225.118, www-amazon-com.customer.fastly.net
Or, 163.28.225.60, e15316.a.akamaiedge.net

(4) Operation of www.amazon.com is out-sourced to another (CDN) company using a different domain name.

7. (ch21, 4pt) Delay, loss, throughput, and security are the major QoS metrics discussed in the lecture. Tell for each of the following, whether you consider it also a QoS metric and why.
   (1) User interface
   (2) Content
   (3) Price
   (4) Customer service

Sample Solution:

Whatever you think with explanations that make sense.

8. (ch21, 10pt) In the traditional crypto system, we generate just one key, which is called often the master key. Everyone involved in the communication share the same master key to encrypt and to decrypt data. Encryption is to apply a function such that F(data, master) = secret. Decryption is to apply a function such that F(secret, master) = data. All holders of the master key can see the data.

   In the public key crypto system, each one involved in the communication generates a key pair, i.e., the public key and private key. The public key is given openly to the public. The private key is kept secret to the owner of the key pair. Encryption is to apply a function such that G(data, public) = secret. Decryption is G(secret, private) = data. In this crypto system, only the holder of the private key can see the data which means only the key pair owner can see the data. This way distribution of key is easier and yet the data is kept absolutely private.

   The magic lies in finding a function (G) and a key pair (e and d) such that the two keys can encrypt and decrypt for each other. RSA, a well-known public key crypto, identifies the function and key pair as follow.

   $$G: (input)^{key} \bmod n$$
   $$(data)^{e} \bmod n = secret$$
   $$(secret)^{d} \bmod n = data$$

   According to the literature, for n=pq, where p and q are integers, a key pair e and d will result in d*e mod w = 1, where w=(p-1)(q-1).

   (1) Encrypt 23 using e=5 and n=91. Show the derivation and outcome (4pt).
   (2) For e=7 and n=91, find the d. Show the derivation and outcome (6pt).

Sample Solution:

(1) 4
(2) 31, 103, and etc (31+72k for all k=1, 2…)

9. (ch22, 8pt) Consider 4 different connection modes in HTTP – (1) non-persistent connection, (2) non-persistent + parallel connection, (3) persistent connection without pipelining, and (4) persistent connection + pipelining. Let's assume the transmission time is negligible for simplicity. Tell the response time in RTT to download a Web page of 1 base html and 4 reference objects in two cases.
   (1) The base html and 4 reference objects all on the same server (4pt).
   (2) The base html and 4 reference objects on 5 different servers (4pt).

Sample Solution:

(3) Non-persistent: 10RTT
Non-persistent + parallel conn: 4RTT
Persistent + no pipelining: 6RTT
Persistent + pipelining: 3RTT

(4) Non-persistent: 10RTT
Non-persistent + parallel conn: 4RTT
Persistent + no pipelining: 10RTT
Persistent + pipelining: 10RTT

10. (ch23, 6pt) Email scam is very common these days. Therefore, we receive frequent warnings from NTU's Computing Center (NTU CC) similar to the example below. The Computing Center advises that we check the sender email address (@ntu.edu.tw) to tell if an email is legitimate. Well. We can't really trust @ntu.edu.tw senders, not even the sender of the warning email – mailadmin@ntu.edu.tw. Follow the instructions below and spoof as NTU CC's admin – mailadmin@ntu.edu.tw – to send a phishing email.

【計中緊急通知】惡意郵件提醒，您的帳號收到主旨【IT Helpdesk】的惡意郵件，切勿點擊連結!! phishing × pollyhuang@ntu.edu.tw ×

Mail2.0系統管理 <mailadmin@ntu.edu.tw> Wed, Sep 22, 6:29 PM

to

Chinese (Traditional) English Translate message Turn off for: Chinese (Traditional)

敬致各位師長同仁、同學：

您的計中email信箱於 110.9.21接到一封詐騙信件，該信件相關資訊如下：

==========

寄件者: Aversenq Patrice <Patrice.Aversenq@ac-bordeaux.fr>
寄件日期: 2021年9月21日 下午 02:17
主旨: IT Helpdesk

尊敬的台大電子郵箱用戶：

我們注意到有人未經授權嘗試登錄您的郵箱。 因此，我們建議您立即驗證您的帳戶。
請點擊這里以避免您的帳戶被禁用。 感謝您幫助我們保護您。

真摯地，
IT幫助台
國立台灣大學

==========

遇到釣魚信件，處理方式如下：
1. 請勿理會此信件，保護個人資訊與電腦安全。
2. 如果您已經輸入帳號及密碼或是點擊相關連結導致密碼被竊取：
2-1 請儘快至計中網頁修改密碼 (http://changepassword.cc.ntu.edu.tw)。
2-2 定期對電腦進行掃毒作業 (Sophos Antivirus，https://download.cc.ntu.edu.tw/index.php)。
以免信箱被盜用寄信！

若為校方寄出的通知信，必定會有聯絡人窗口，包含連絡人姓名、連絡電話(02-3366~)、連絡信箱(@ntu.edu.tw)，
如有任何問題，請來電計資中心服務櫃台，謝謝。

敬祝 健康順心

計算機及資訊網路中心
諮詢電話：33665022~3
諮詢信箱：cchelp@ntu.edu.tw

(1) Log in to the PA server with your exam account. telnet to the mail server of the EE department by this command: `telnet cc.ee.ntu.edu.tw 25`.

(2) Type up the following. Hit the enter key at the end of each line. The points will be awarded when Polly receives the email.

```
HELO blah
MAIL FROM: mailadmin@ntu.edu.tw
RCPT TO: pollyhuang@ntu.edu.tw
RCPT TO: <your email address>
DATA
To: <pollyhuang@ntu.edu.tw>
From: <mailadmin@ntu.edu.tw>
Subject: f21 email spoofing

Your NTU email account is compromised. Please provide the
following information immediately to reset the account
password.

Username:
Old Password:
New Password:
.
QUIT
```

(3) If you've received the above email from the email address you give to the 2nd `RCTP TO:` command, you should be successful sending the email to Polly's NTU email account as well.

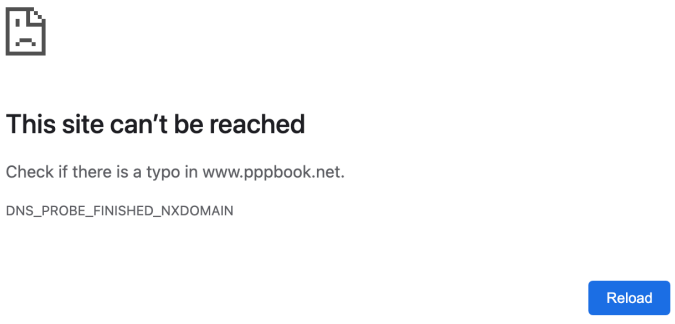
Sample Solution:

check incoming email

11. (ch24, 14pt) Petbook was successful getting seed money from angel investors. The company went on to establish the IT infrastructure. Below were the tasks completed.

    a. connects the company network to the FTTH box leading to a major ISP
    b. acquires the domain name – pppbook.net
    c. acquires a block of IP addresses – 42.112.140.1-42.112.140.255
    d. sets up the authoritative DNS server
    e. gives the hostname and IP address – dns.pppbook.net and 42.112.140.8
    f. sets up the mail server
    g. gives the hostname and IP address – smtp.pppbook.net and 42.112.140.12
    h. sets up two web servers to host the petbook pages
    i. gives two IP addresses – 42.112.140.253 and 42.112.140.254
    j. gives one hostname – web.pppbook.net
    k. gives the nickname to the web service – www.pppbook.net
    l. connects the authoritative DNS server, mail server, and two web servers to the company network.

    The company started advertising. A prospective user tried to visit www.pppbook.net and this message below appeared on the browser, indicating that the DNS query failed. After receiving a number of complaint calls, the company fired its IT guy. You are interviewing for the position. Advise the company which DNS server and what RR entries, in terms of (name, value, type), to install to enable IP lookup for www.pppbook.net.



    (1) Is it necessary to install any RR in the prospective user's local DNS server? If yes, what RR entries to install? If not, why not?
    (2) Is it necessary to install any RR in the root DNS server? If yes, what RR entries to install? If not, why not?

(3) Is it necessary to install any RR in the .net TLD server? If yes, what RR entries to install? If not, why not?

(4) Is it necessary to install any RR in the authoritative DNS server in the company? If yes, what RR entries to install? If not, why not?

(5) Do you think the DNS lookup for the mail server will work? And why?

Sample Solution:

(1) Not necessary. Local DNS can forward queries to the DNS hierarchy

(2) Not necessary. The root DNS server stores only TLD server entries. .net TLD entry must have been in place in the root DNS server for other .net websites to work.

(3) Yes. 2 RR entries missing in the .net TLD server
(pppbook.net, dns.pppbook.net, NS)
(dns.pppbook.net, 42.112.140.8, A)

(4)-(5) are related.
If one says for (4), "yes and 3 RR entries missing in the authoritative DNS server."
(www.pppbook.net, web.pppbook.net, CNAME)
(web.pppbook.net, 42.112.140.253, A)
(web.pppbook.net, 42.112.140.254, A)
For (5), it will be "no and 2 RR entries are missing in the authoritative DNS server."
(pppbook.net, smtp.petbook.com, MX)
(smtp.pppbook.net, 42.112.140.12, A)

If one says for (4), yes and 5 RR entries are missing and list all 5.
For (5), it'll be yes, the MX and A entries are already.

(Giving only the RR entry types gets partial credits.)

12. (PA2, 9pt) Develop exam1-p12.go such that it reads a text-based file and prints the characters on the screen as usual except for two unprintable characters – \r and \n. When the character is \r, prints '\r' on the screen. When the character is \n, prints '\n' on the display.

Sample Solution:

Check `exam1-p12.go` on the PA workstation

13. (PA3, 10pt) Develop exam1-p13.go such that is works like a file upload client which:
    (1) connects to the server that polly implements and runs already on the PA workstation at port 11000
    (2) prompts the user for the upload filename
    (3) sends the file content (the entire file)
    (4) sends a line containing only a period (a string like this -- ".\n")
    (5) receives a message back from the server
    (6) prints what the server says
    (7) closes the connection and terminates the program

Sample Solution:

Check `exam1-p13.go` on the PA workstation