CPSC 441
COMPUTER NETWORKS

FINAL EXAM SOLUTION

Department of Computer Science
University of Calgary
Professor Carey Williamson

April 18, 2018

This is a CLOSED BOOK exam. Textbooks, notes, laptops, personal digital assistants, tablets, and cellular phones are NOT allowed. However, **calculators are permitted**.

It is a 120-minute exam, with a total of 80 marks. There are 18 questions, and 10 pages (including this cover page). Please read each question carefully, and write your answers legibly in the space provided. You may do the questions in any order you wish, but please USE YOUR TIME WISELY.

When you are finished, please hand in your exam paper and sign out. Good luck!

Student Name: ________________________________

Student ID: ____________________

Score: ________ / 80 = _______ %

Multiple Choice

Choose the best answer for each of the following 12 questions, for a total of 12 marks.

1 1. The two most important protocols in the Internet protocol stack are:

(a) DNS and WiFi

(b) HTTP and ARP

(c) SSH and FTP

(d) TCP and IP

(e) YouTube and SnapChat

1 2. The person who saved the Internet from TCP "congestion collapse" in 1988 was:

(a) Tim Berners-Lee

(b) Vint Cerf

(c) Sally Floyd

(d) Van Jacobson

(e) Jennifer Rexford

1 3. The person who "invented" the World Wide Web in the early 1990's was:

(a) Tim Berners-Lee

(b) Vint Cerf

(c) Dina Katabi

(d) Jim Kurose

(e) Carey Williamson

1 4. In a domain name like `csg.cpsc.ucalgary.ca`, the Top-Level-Domain (TLD) is:

(a) `csg`

(b) `cpsc`

(c) `ucalgary`

(d) `ca`

(e) two, but not all of the above

1 5. The term “virtual circuit” refers to a:

(a) connection-less approach to the design of the network layer

(b) connection-oriented approach to the design of the network layer

(c) connection-less approach to the design of the datalink layer

(d) connection-oriented approach to the design of the datalink layer

(e) none of the above

1 6. What service class(es) is/are supported in Asynchronous Transfer Mode (ATM) networks?

(a) Constant Bit Rate (CBR)

(b) Variable Bit Rate (VBR)

(c) Available Bit Rate (ABR)

(d) Unspecified Bit Rate (UBR)

(e) all of the above

1 7. The typical Maximum Segment Size (MSS) for TCP on the Internet is:

(a) 64 bytes

(b) 1024 bytes

(c) 1460 bytes

(d) 1500 bytes

(e) 8888 bytes

1 8. The most prominent new feature(s) in IPv6 compared to IPv4 is/are:

(a) 128-bit IP addresses

(b) simpler header for streamlined datagram processing

(c) removing the need for IP datagram fragmentation

(d) better support for quality of service (QoS), mobility, and security

(e) all of the above

1 9. Routers and switches are similar in that they both:

(a) are connection-oriented

(b) use BGP

(c) are manufactured by Microsoft

(d) start with the letter “r”

(e) operate in a store-and-forward fashion, using a “forwarding table”

1 10. Routers and switches are different because:

(a) routers operate at the Network Layer, while switches operate at the Datalink Layer

(b) switches operate at the Network Layer, while routers operate at the Datalink Layer

(c) routers are for wired networks, while switches are for wireless networks

(d) switches are for wired networks, while routers are for wireless networks

(e) this is a trick question, because they are actually the same!

1 11. In IEEE 802.11 WiFi wireless networks, the link-layer protocol:

(a) allows variable size frames

(b) automatically retransmits unsuccessful frames (up to a max retry limit)

(c) explicitly acknowledges successful frames

(d) uses MAC addresses in the header to identify the sender and receiver

(e) all of the above

1 12. The Cyclic Redundancy Check (CRC) used on data frames in Ethernet LANs provides:

(a) very powerful error detection

(b) very powerful error correction

(c) very powerful error detection and error correction

(d) very strong encryption

(e) very weak encryption

Internet Protocol Stack

12 13. Below is a fairly random scatterplot of protocol acronyms, similar to the PowerPoint slide that we saw in early January. Using your knowledge of the Internet protocol stack, **circle any five** of these acronyms, and **copy them** into the relevant spaces given below, making sure to identify at least one protocol for each layer. Please write the **full name** of the protocol (i.e., expand its acronym), and provide at most **one sentence** describing what that protocol does in the Internet protocol stack.

```
  TCP          CSMA/CD          SLIP             MAC                   DNS
         UDP              PCM               IPv4          ATM                OFDM
IPv6                WiFi        MIMO                 UDP             PLCP
     HTTP                   DHCP        SSH                  NNTP       FDM
 CSMA/CA               SMTP                 QAM         FTP                  FDDI
           POP                  ARP                  IMAP            ICMP
RIP              RARP                   CDMA                 OSPF            HTTPS
       TDM               VLAN                  BGP               PPP
```

Layer 5: Application Layer (2 marks)
Example protocol: HTTP: Hyper-Text Transfer Protocol
What it does: Allows client browser to request Web pages (objects) from a Web server

Layer 4: Transport Layer (2 marks)
Example protocol: TCP: Transmission Control Protocol
What it does: Everything! Reliable byte stream protocol, end-to-end basis

Layer 3: Network Layer (2 marks)
Example protocol: IP: Internet Protocol
What it does: Best-effort datagram delivery on a host-to-host basis

Layer 2: Datalink Layer (2 marks)
Example protocol: CSMA/CD: Carrier Sense Multiple Access with Collision Detection
What it does: Very efficient MAC protocol for classic Ethernet LANs

Layer 1: Physical Layer (2 marks)
Example protocol: TDM: Time Division Multiplexing
What it does: Shares use of a physical channel on a time slot basis

Bonus (2 marks)
One other protocol from the list above that I know is: WiFi (Wireless Fidelity)
It belongs to layer: Datalink layer
What it does: Provides IEEE 802.11 wireless LAN services to mobile users

Networking Concepts and Definitions

12 14. For each of the following pairs of terms, **explain each term**, making sure to identify the similarities (if any) and the **key differences** between the two terms.

(a) (3 marks) “forwarding” and “routing”

```
Both are activities that take place at a router in the Network Layer
F: moving incoming datagrams from input   R: making decisions about the paths
port to proper output port of router      used for datagrams to reach destination
Done using info in forwarding table       Done in software
Done in HW at link speeds (very fast)     Done at time scales of minutes or hours
Also known as "data plane"                Also known as "control plane"
```

(b) (3 marks) “DHCP” and “NAT”

```
Both are network-layer middleboxes to improve sustainability of IPv4 addresses
Dynamic Host Configuration Protocol.     Network Address Translation.
Allows device to lease an IP address.    Use private IP addresses inside,
Serve has pool of IP addresses.          and one public IP address outside.
Borrowed for an hour at a time.          NAT box does the port translation.
```

(c) (3 marks) “Medium Access Control (MAC)” and “Logical Link Control (LLC)”

```
These are both sub-layers of the Datalink layer.
MAC: Medium Access Control               LLC: Logical Link Control
Regulates access to a shared channel.    Defines frame format, addresses, etc.
Only needed on broadcast channels.       Needed in all link-layer protocols.
```

(d) (3 marks) “Ethernet” and “WiFi”

```
These are both very popular LAN technologies.
Ethernet: wired network, with CSMA/CD   WiFi: wireless network, with CSMA/CA
as the MAC protocol. Limited distance.  as the MAC protocol. Limited distance.
Highly reliable, low error rate.        Higher error rate. Allows roaming.
IEEE 802.3 standard.                    IEEE 802.11 standard.
```

Routing Protocols

12 15. The current Internet uses several different mechanisms and/or protocols to deliver IP datagrams from a source host to a destination host. In class, we studied several of these protocols, as well as the design of Internet routing as a whole.

(a) (3 marks) One of the biggest challenges in Internet routing is making routing work at the large scale of the Internet, with over a billion IP-addressable devices. What are the three main keys to making Internet routing scalable?

```
1. Routing is based on networks, not hosts. IP address has network ID and host ID.
2. Classless Inter-Domain Routing (CIDR) uses addresses judiciously, and can
aggregate similar network prefixes where appropriate in a routing table.
3. Autonomous System (AS) concept is used to simplify scale of routing problem.
```

(b) (3 marks) What is an **Autonomous System**? What role does an AS play in Internet datagram delivery?

```
AS: a subset of routers on the Internet that are all owned and operated by same
organization. They can choose their own internal intra-AS routing algorithm.
Can talk to other ASes using BGP to determine good AS paths to destinations.
Routing involves getting to right AS, then right network, then right host.
```

(c) (2 marks) Give an example of an **intra-AS** routing protocol, and provide a sentence or two to describe its operation.

```
OSPF: Open Shortest Path First. A complicated intra-AS routing protocol that
allows one to define a two-level hierarchy. Link state routing protocol.
Learns status of links. Builds global view of topology inside AS, and then
calculates good routing paths.
```

(d) (2 marks) Give an example of an **inter-AS** routing protocol, and provide a sentence or two to describe its operation.

```
BGP: Border Gateway Protocol
This is the "glue" that makes Internet routing work. Each AS talks to
the other ASes using BGP, and figures out good AS paths to traverse in
order to reach the destination network. Can also enforce policies.
```

(e) (2 marks) What is the **Address Resolution Protocol**? What role does ARP play in Internet datagram delivery?

```
This is the last step of IP datagram delivery. A router can use ARP to determine
the MAC address of a device with a particular IP address, and then deliver an IP
datagram to them in an Ethernet frame (for example) on the destination LAN.
```

Networking Details

10 16. The output below shows the result of a **traceroute** command. Use your knowledge of Internet protocols to answer as many of the following questions as you can.

(a) (2 marks) What protocol is used to solicit the routing information displayed below? Be as specific as possible.

```
ICMP echo request (and reply)
```

(b) (2 marks) How many routing hops does it take to reach the destination host? What is the approximate round-trip time (RTT) for this network path?

```
16 hops           13 milliseconds (ms)
```

(c) (2 marks) List the IP address and name for any device on the U of S network.

```
cs.usask.ca has IP address 128.233.236.236
```

(d) (2 marks) Give an example of a private IP address that is visible within this trace.

```
172.17.10.1 is the private IP (NAT) for deptNFSgate
```

(e) (2 marks) What is the most unusual or anomalous feature evident in this specific trace? Why is it unusual?

```
In this particular trace, the latency for Shaw (bigpipeinc) was 28 ms at the
time that it was queried, but the latency to U of S in Saskatoon was only 12 ms.
This indicates a lot of variability in the queueing delay in the network!
(one could also comment on the routing path, such as Edmonton vs Regina)
```

```
% traceroute cs.usask.ca
traceroute to cs.usask.ca (128.233.236.236), 30 hops max, 60 byte packets
 1  deptNFSgate (172.17.10.1)  0.315 ms  0.304 ms  0.291 ms
 2  10.58.48.1 (10.58.48.1)  0.843 ms  0.835 ms  0.902 ms
 3  10.16.18.1 (10.16.18.1)  0.459 ms  0.457 ms  0.450 ms
 4  10.16.18.4 (10.16.18.4)  0.283 ms  0.249 ms  0.244 ms
 5  10.16.17.1 (10.16.17.1)  0.571 ms  0.519 ms  0.552 ms
 6  10.59.226.26 (10.59.226.26)  0.446 ms  0.418 ms  0.392 ms
 7  h74.gpvpn.ucalgary.ca (136.159.199.74)  2.597 ms  2.596 ms  2.655 ms
 8  h66-244-233-17.bigpipeinc.com (66.244.233.17)  28.075 ms  29.477 ms  27.701 ms
 9  h66-244-233-30.bigpipeinc.com (66.244.233.30)  0.939 ms  0.933 ms  0.890 ms
10  clgr2rtr1.canarie.ca (205.189.32.212)  0.890 ms  0.887 ms  1.043 ms
11  edmn1rtr1.canarie.ca (205.189.32.168)  7.533 ms  7.500 ms  6.619 ms
12  sask1rtr1.canarie.ca (205.189.32.189)  11.547 ms  11.506 ms  11.512 ms
13  srnet-reg.srnet.ca (205.189.32.221)  11.441 ms  11.615 ms  11.546 ms
14  208.75.72.83 (208.75.72.83)  13.666 ms  11.837 ms  11.759 ms
15  128.233.16.2 (128.233.16.2)  11.727 ms  13.569 ms  11.598 ms
16  cs.usask.ca (128.233.236.236)  13.869 ms  13.833 ms  12.118 ms
```

Medium Access Control (MAC) Protocols

12 17. Within the Data Link Layer, we studied a variety of Medium Access Control (MAC) protocols to regulate access to a broadcast channel shared by many stations.

(a) (4 marks) If there is a fixed number of stations, and they always have data to send, then **static channel allocation** protocols make the most sense. List **two examples** of static channel allocation protocols, and briefly describe how each works.

TDM: Time Division Multiplexing. Allocates a time slot for each station on a round robin basis. Give all of the channel, part of the time.
An example would be classroom scheduling into a lecture hall.
FDM: Frequency Division Multiplexing. Allocates a range of frequencies for each station on a permanent basis. Give part of the channel, all of the time.
An example would be radio stations or TV stations.

(b) (6 marks) If the number of stations vary, and the stations are unpredictable (i.e., bursty) in their data transmission needs, then **random channel access** protocols make sense. List any **three examples** of dynamic random access protocols, and provide a very brief description how each operates.

Pure ALOHA: send when ready. Works good at low load, but prone to collisions at high load. As a result, the overall efficiency is only about 18%.
Slotted ALOHA: add global time slots to Pure ALOHA, to reduce vulnerable period, and improve channel efficiency. Doubles it, up to about 37%.
CSMA: Carrier Sense Multiple Access. Listen to the channel before transmitting.
If somebody else is using it, then stay off! Wait longer for access, but the channel efficiency improves a lot (over 50% now).

(c) (2 marks) A third alternative for MAC protocol design is **turn-taking** protocols. Give **one example** of a turn-taking protocol, and briefly describe how it works.

Token ring: special token circulates around the network visiting all stations.
If you have data to send, then grab the token, send your data. Need to remove your data when it comes back around. Don't forget to put the token back too!

The Future Internet

10 18. The Internet has grown and evolved in many different ways over the past few decades, and will continue to do so in the decades ahead.

(a) (4 marks) In your opinion, what is the **single greatest challenge** facing the future of the Internet? Why is this issue a challenge, and why is it an important one to solve?

```
Many possible answers here. I chose security as an example.
Security: the number of miscreants using the Internet for ill-gotten gains
has increased immensely, placing many Internet users at risk. These are big
risks for society: fraud, identity theft, exploitation, harassment,
cyber bullying, privacy violations, and many more.
This is a problem since it discourages people from embracing the Internet.
Makes the good guys work extra hard to keep things functional and safe.
```

(b) (6 marks) What are some approaches to solving the challenge that you identified? Give at least **two ideas for solutions** to the problem. Make sure to clarify whether these approaches are technical (e.g., network architecture, protocol design, international standards, etc.) non-technical (e.g., political, economic, social, etc.), or a combination of both.

```
The most obvious thing is encryption, since end-to-end encryption can help
protect our data packets. However, this seems to run counter to the open
philosophy in the design of the original Internet and its protocol stack. :-(

Other technological solutions:
 - IDS: Intrusion Detection System. Automated way to look for known attacks,
    and block them from getting in.
 - better network forensic tools to diagnose attacks and detect perpetrators
 - better software, or more thoughtful design to include security
    considerations from the outset, rather than rushing to market with
    vulnerable products (e.g., IoT devices), and trying to fix problems later.

Non-technical solutions:
 - education and training for Internet users (especially kids and seniors)
 - stronger law enforcement to detect/protect against cybercriminal activities
 - stronger legal system to prosecute across international boundaries
```

*** THE END ***