Week.1.txt

- January 11th, 2021
    - Introduction
        - This course is about the history of the internet, and its logistics
        - For this week, the required reading is chapter 1 of the textbook
            - Textbook: Computer Networking By Kurose & Ross
    - Computer Networks
        - A computer network is a system for communicating among two or more computers
            - This system includes both hardware and software
                - The softare is crucial because it implements the protocols and services
                    - i.e. Software that runs on network routers
            - Computers are not limited to end-user devices, but includes machines responsible for facilitating interchange of information and communication
                - i.e. Routers, Gateways, etc.
            - Communication in the network is about the bits being transferred from one node to another
                - Note: A node is a machine in a network
        - There are many forms of networks
            - i.e.
                - Local Area Network (LAN)
                - Home Network
                - Dedicated Network
                    - i.e. Missile Control
                - Wide Area Network (WAN)
    - Trivia Questions
        - In 1971, a computer engineer named Ray Tomlinson sent the first [Email]
            - Inside that email, he said [QWERTYUIOP]
        - In 1980, Tim Berners-Lee, a computer scientist, invented [HTML]
            - He got a Turing Award for this
        - In 1994, [Al Gore] said, "I took the initiative in creating the Internet"
            - Fact: Al Gore helped in funding the internet's creation
        - Instagram was launched in [2010]
        - [Twitter] blocked President Trump's account in Jan. 2021
    - History Of The Internet
        - 1961-1970
            - DARPA started the development of packet switching technology
        - 1972-1980
            - The rise of proprietary networks and internetworking
                - i.e. ALOHA, Ethernet, Defense Networks, Etc.
            - Development of TCP, UDP, IP, etc. started ramping up

    - 1980-1990
        - Networks started to proliferate
            - This led to the standardization of networking protocols
                - i.e. TCP/IP, DNS, Etc.
            - i.e. The NSF builds the NSFNET as backbone and connects 10,000 computers
    - 1990s
        - Internet exploded as people realized the potential of the internet
            - i.e. Emails, sharing files, instant messaging, etc.
        - The emergence of the World Wide Web (WWW)
            - Invented by Tim Berners-Lee
    - 2000s
        - More than 1 billion hosts including smartphones and tablets
        - 2001 :: BitTorrent
            - Peer-to-peer file sharing protocol
        - 2004 :: FaceBook
            - Social networking site
        - 2011 :: Snapchat
            - Photo sharing social media service
        - 2020 :: 5G cellular data networks are on the rise
        - Currently, there are so many devices connected that IPV4 addresses have run out, and we have now resorted to IPV6 addreses
- Why Learn Computer Networks
    - Understand how things work
        - This will help in fixing day-to-day problems
    - Develop distributed applications
    - Configure and to operate (as a system administrator)
        - Requires knowledge of WireShar
            - WireShark is a software that allows you to see network traffic, and debug what network entities are having issues
    - Improve and design
        - Emerging new network architecture and types of networks
            - i.e.
                - Peer-to-Peer (P2P)
                - Content Distribution Networks (CDN)
                - Software defined networking
                - Quantum networks
    - Defend against cyber attacks
        - i.e. DDOS attacks
    - Find security holes/bugs
    - Contribute to public discourse and policy making
- The Instructor
    - Rong Zheng
        - MacID: rzheng
    - Office Hours:

        - Monday 4:30 - 5:30pm (Zoom)
        - Or by appointment
    - Research Area
        - Mobile computing
        - Wireless system research (WiSeR)
            - Intersection of Wireless Networking, Sensing, and Data Analytics
                - i.e. Wireless data center infrastructure management, Wearable based health monitoring, Indoor navigation and target tracking, and Non-contact, ambient sensing
- The TAs
    - Yongyong Wei (weiy49)   :: Week 2, 3, 4
    - Wei Zhao (zhaow9)   :: Week 5, 7, 8
    - Seyed Tayefeh (tayefehs)   :: Week 9, 10, 11
    - Somayye Rostami (rostami) :: Week 12, 13, 14
- Textbook
    - James F. Kurose, Keith W. Ross, "Computer Networking: A Top-Down Approach Featuring the Internet"
        - 7th or 8th Ed
            - Earlier editions are fine but note changes in current content
    - Note: Take advantage of student resources, like Applets that detail how networks and protocols behave
    - https://wps.pearsoned.com/ecs_kurose_compnetw_6/216/55463/14198700.cw/index.html
- Organization Of The Course
    - Scope
        - Internet architecture
        - Applications & socket programming
        - Transport layer
        - Routing
        - Link layer
        - Network Security
    - Grading
        - Online quizzes :: (5 x 5%) = 25%
        - Assignments   :: (4 x 5%) + (2 x 10%) = 40%
        - Final   :: 35%
- Online Quizzes
    - The quizzes are primarily designed to review the materials taught in classes
    - Simple questions, usually takes 20 - 30 mins to finish
    - Auto-graded and grades released upon expiration of deadline
        - You can check the answers online after the deadline
        - Remember to click the submit button
- Assignments
    - 3 Wireshark Assignments
        - Wireshark is a packet capture & analysis tool
            - This will give you first hand understanding of Internet protocols

            - Great tool for network administrators and distributed applications
            - You are expected to capture packet traces themselves
        - Questions are mainly short answers; no programming involved
    - 1 Python Programming Assignment
        - Design and implement a miniature peer-to-peer (P2P) file sharing app
        - You will be provided with a test server to debug your client site
        - MOSS used for plagiarism check
    - 2 Mininet Assignments
        - Mininet is an instant virtual network on your computer
            - This will help you develop a better understanding of interconnectivity
        - You must know how to navigate around the Linux command line
            - Use of basic network commands and utilities
                - i.e. ifconfig, netstat, tcpdump, ping, traceroute, dig, etc.
- Teaching Tools
    - Avenue
        - Lecture content
        - Quiz
        - Assignments
        - Grades
        - Announcements
    - Piazza
        - Online discussions
        - Invites will be sent out during week 2
        - Code of conduct:
            - Only course related discussions
            - Code snippets are allowed, but do not post complete solutions
    - Zoom
        - Lectures, tutorials, instructor office hours
    - Microsoft Teams
        - Recorded lecture and tutorial videos
- Questions
    - Post on piazza
        - Top students who answer most questions OR ask good questions will get a 3% bonus
    - Email rzheng@mcmaster.ca with subject as "4C03"
        - She uses email filters
- MSAF Policy
    - Missing assignments with MSAF approvals will be counted toward the total grade of assignments of the SAME category

- January 13th, 2021
    - Outline

    - Topic
        - Internet: Nuts and bolts
    - Readng
        - K & R : Chapter 1
- What Is The Internet
    - Highly distributed network of machines that share information
        - There is no single point of failure or central server
    - Hosts on the internet are not directly connected to other hosts
        - i.e. There isn't a direct cable from your home network to Google's servers
    - The internet is a network of networks
        - Switches and routers help us connect to end hosts
            - Each router you connect to is considered a hop
            - If a single router fails, then the traffic is rerouted
    - There are over a billion connected computing devices
        - Hosts are the end systems
        - Each device is running network applications to communicate
    - Communication is done through:
        - Fiber, copper cable, radio, satellite, etc.
            - The transmission rate is measured in bandwidth
                - Fiber optical cables have a very high transmission rate
    - Inside each network, there are packet switches that forward packets
        - i.e. Routers and switches
        - Packets are chunks of data
- Examples Of Network Components
    - Links
        - Fiber optical links
            - Very fast and can support gigabit networks
        - Coaxial cable
            - Copper cables are slowly being phased out in favor of Fiber
    - Interfaces
        - Ethernet card
            - Used for wired connection, typically on a desktop
        - Wireless card
            - i.e. WiFi dongle
    - Switches/Routers
        - Large router
        - Switch
            - Switches and routers comprise the internal network of the internet
            - Your home router connects your devices to outside networks
- Internet Structure: Network Of Networks

    - Internet Service Provider (ISP)
        - Provide internet access to end-systems
            - i.e. Your phone, laptop, etc.
        - ISPs have different tiers
            - i.e.
                - Tier 1
                - Tier 2
                - Tier 3
                - Local ISP
        - ISPs connect to each other to form the backbone of the internet
            - The internet is a network of networks
    - Connection type:
        - Customers and providers
            - Customer pays provider for access to the Internet
        - Peering relationship
            - Peers provide transit between their respective customers
            - Peers do not provide transit between peers
- Customers and Providers
    - Customer pays provider access to the internet
        - i.e. You paying Rogers a monthly fee to connect to their network
        - i.e. Rogers pays a top tier ISP to connect to their network
    - This relationship allows your data to travel to the provider network
- The Peering Relationship
    - Peering relationships typically happen between ISPs of the same tier
        - Peers provide transit between their respective customers
            - However, peers do not provide transmit between peers, because it does not help the middle peer to process data that is not its own
    - Low tier ISPs only have regional connectivity, but they can connect to higher tier ISPs to connect to the global network
    - Peering relationships allow customers on different ISPs to connect/talk to each other
        - i.e. A peering connection between Canadian ISPs and American ISPs, allows Canadians to send data to Americans. The data travels like this: Canadian customer -> Canadian ISP -> American ISP -> American Customer
    - Peering relationships help to avoid additional charge(s)
    - In order to connect local ISPs, a top tier ISP is used to connect them
        - Top tier ISPs and local ISPs have a provider-customer relationship
            - Local ISPs pay money to top tier ISPs, to connect to their networks and other networks, indirectly

        - Can be done through a direct link or a Network Access Point; abbreviated as NAP
    - Internet Structure: Network Of Networks
        - Internet providers are not flat, they are organized in a hierarchical manner
        - At the center, there are Tier 1 ISPs
            - i.e. Sprint, AT&T, Cogent Communication, etc.
                - They provide national/multi-national coverage
                - These ISPs interconnect privately
                    - i.e. They have a peering relationship
        - Tier 2 ISPs are smaller, often regional, ISPs
            - Tier 2 ISPs connect to one or more tier-1 ISPs, through a customer-provider relationship
                - Each tier 1 ISP has many tier 2 customers
            - Tier 2 ISPs can peer directly with each other
                - This bypasses the tier 1 ISPs
        - Tier 3 ISPs and Local ISPs
            - These are customers of higher tier ISPs
                i.e. Customer-provider relationship with tier 2 and tier 1 ISPs
            - Very rarely do they have peer relationships among themselves
        - A message passes through many networks from source host to destination host
            - i.e. Your computer -> local ISP -> Tier 3 ISP -> Tier 2 ISP -> Tier 1 ISP -> Tier 1 ISP -> Tier 2 ISP -> local ISP -> Your friend
    - Traceroute
        - Is a tool to look inside the "blackbox" of the Internet
            - It provides delay measurements from source to router along end-to-end Internet path towards destination
        - Traceroute sends 3 packets from your machine to each network node
            - It records the interval time between transmission and reply
        - Traceroute sets a max number of hops
            - i.e. If traceroute sets 64 as max hops, and there are more than 64 nodes to connect to, then the program will fail. However, this is unlikely in the realm of the internet
            - The routing protocol sets limitations on a max number of hops
        - The first IP in traceroute is your private IP on your home network
        - The three numbers after the IP is the latency measured from your machine to the first hub/router

January 15th, 2021
    - Traceroute
        - Is a tool used to look inside the "blackbox" of the Internet

through an end-system, such as a laptop or desktop
  - It works by sending multiple probes/packets to each hop along the path from your computer to a destination host
    - The round trip time from your computer to each hop is measured
      - This gives the latency of reaching each router along the path
      - Traceroute returns 3 latency measurements for each hop
        - It is possible for the latency for a far away node to be less than the latency for a closer node, due to traffic variation and other factors
  - Traceroute is available on Windows, macOS, and Linux
    - On macOS and Linux it is in-built
- Examples of traceroute
  - i.e. traceroute www.uh.edu
  - i.e. traceroute www.google.com
- Packet Loss
  - If there is an asterisk instead of the latency time, then the packet took too long to get back or it never returned
    - In other words, the probe/packet was not recieved in a timely manner
- Packet Switching: Store & Forward
  - Packet switching technology was invented in 1960-1970s
    - It is now the foundation of the internet
  - Packets are small units of information
    - Each packet/unit is delievered individually, hop-by-hop, from source to destination
      - The entire packet must arrive at a router/hop before it can be transmitted to the next link/hop
        - This is called "store and forward"
          - The packet must be stored before it can be forwarded
      - An individual packet can be forwarded along different network paths
    - The size of the packet depends on the Operating system
      - Typically, the size of an ethernet packet is 1000 bytes
- Before packet switching was invented, telephones used circuit switching
  - You had to manually create the circuit between source and destination
    - Setting up this connection is time consuming
- Loss & Delay (1)
  - There are 4 types of packet delays and one type of packet loss
    - Packet Loss
      - If there are no free buffers, the arriving packets

are dropped
- By definition, this isn't really a delay, but it can affect the time it takes for packets to reach the destination, because packets need to be re-sent

- Queueing Delay
  - If there are packets in the buffer, then the arriving packets are placed into the buffer, and they must wait for their turn
- Processing Delay
  - The packet is checked for integrity, and the router ensures that it is not corrupted
  - The router determines where the packet needs to be sent to by performing a lookup in a router table
- Transmission Delay
  - When the packet is ready to be transmitted, it will take some time to transmit from the first bit of the packet to the last bit of the (same) packet
- Propagation Delay
  - Once the packet is transmitted, it needs to travel along the "wire" to reach the destination; and there is some delay to this
    - Propagation delay is determined by the distance between the source, and the (physical) maximum speed it can travel at

- Packet switching can cause packet loss and packet delay
  - Consider the following scenario:
    1. Packets arrive at an intermediate router, they are first stored in the router's buffer
       - Note: If the buffer is full, then the packets are dropped
    2. Once the entire packet arrives, the integrity of the packet is checked to make sure it is not corrupted
       - This is processing delay
    3. Then, the router decides where the packet needs to be forwarded to
       - i.e. Lookup, in a huge table, which network/ router it needs to be sent to. This is processing delay.
    4. Since this entire process is time consuming, the packets are put in a queue, and they wait their turn for processing
       - If packets arrive faster than they are sent, then they have to wait for their turn, causing you to experience higher latency
         - This is queueing delay
    5. Once packet is ready to be transmitted, it takes time for the packet to be sent from the first bit to the last bit

        - This is transmission delay
    6. The transmitted packet must now travel, wired or wirelessly, from the source to the destination
        - This is propagation delay
- Packet delay can be observed in traceroute
    - i.e. The 3 latency numbers
- Loss & Delay (2)
  - The ports on a switch are called interfaces
    - A switch will typically have multiple interfaces
      - Interfaces connect switches with other switches
    - Every interface on a switch has its own queue
      - Processing delay occurs in the incoming interface and outgoing interface
        - Most of the processing delay occurs in the outgoing interface
          - This is because the packet can arrive faster than it can be delievered
        - Processing in incoming interface is fast because the computation is done in hardware
    - The switch looks at the destination IP address in the packet, and uses it to determine which switch it needs to send the packet to
      - It does this by looking up information in a routing table
        - This is computed ahead of time
        - This causes processing delay
    - Once the lookup is done, the packet is sent to the outgoing interface through the switch fabric
  - Routers do not make any attempt to recover dropped/loss packets
    - The application is responsible for ensuring that all packets have been sent/recieved
- Four Sources Of Packet Delay
  1. Processing Delay (Computational)
    - Check bit errors
    - Determine output link
    - Deep packet inspection
      - Very expensive, computationally
      - Used for detecting virus signature in a packet
    - Measured in micro-seconds
  2. Queueing Delay
    - Time waiting at output link/interface for transmission
    - Depends on congestion level of router
      - i.e. Rush hour VS. Non-rush hour
    - Has the biggest variability
    - Measured in milli-seconds
    - Queueing delay occurs when the incoming traffic is faster than the rate of the outgoing link/interface
      - This can be measured with the following formula: TI = (L * (a / R))

                - Where:
                    - TI = Traffic Intensity
                    - R = Link bandwidth (bps)
                    - L = Packet length (bits)
                    - a = Average packet arrival rate (packet/s)
                - And If:
                    - (L * (a / R)) ~ 0
                        - If it is close to 0, then the average queueing delay becomes small
                    - (L * (a / R)) -> 1
                        - If it approaches 1, then the delays becomes large
                    - (L * (a / R)) > 1
                        - If it is greater than 1, then more "work" is arriving than what the switch can process, causing the average delay to be infinite
                            - This is true if the buffer is infinitely large
    3. Transmission Delay (Outgoing)
        - This is dictated by the link bandwidth
            - The time to send bits into the link is: (L / R)
                - Where,
                    - R = Link bandwidth (bps)
                    - L = Packet length (bits)
    4. Propagation Delay
        - This depends on time, because the delay is determined by the physical distance between two spaces
        - Propagation delay can be determined by: (d / s)
            - Where,
                - d = The length of the physical link
                - s = Propagation speed in medium
                    - Typically, propagation speed is the speed of light (c)
                        - c = (3 x 10^8) m/s
- Nodal Delay
    - Combining the four sources of delay yields the nodal delay
    - Every single hop that the packet traverses will incur those four kinds of delay
        - This is modeled by: (d_nodal = d_proc + d_queue + d_trans + d_prop)
            - Where:
                - d_proc = Processing delay
                    - Caused by error checking OR determining which outgoing interface the packet needs to be delivered to
                    - Typically a few micro-seconds or less
                - d_queue = Queueing delay
                    - Depends on the level of the network load
                        - i.e. How many packets are buffered in

                                the router's incoming and outgoing interface.
                        - If incoming traffic is greater than outgoing traffic, then the network will slow down, and latency will increase
                    - d_trans = Transmission delay
                        - Depends on the equation: (L / R)
                        - This is significant for low-speed links
                    - d_prop = Propagation delay
                        - Depends on the physical distance between the hops
                            - i.e. Greater distance equals more time to send packets
                        - A few micro-seconds to hundreds of milli-seconds
- Example
    - Question
        - In the movie, "The Martian", Houston sends a message of 50000 bytes to Mark on Mars over a radio link at speed 1 Kbps. Mars and Earth are at the orbital closest distance of 56 million km apart. How long does it take for the message to reach Mark from Houston?
          (Hint #1: Ignore the processing and queueing delay)
          (Hint #2: Speed of light = 3 x 10^8 m/s)
    - Answer
        - 1 Kbps = 1 Kilo-bit-per-second
            - Note: Uppercase 'B' is byte && lowercase 'b' is bit
        - You only need to consider transmission delay and propagation delay
            - Transmission delay:
                - TD = L/R
                     = 50000 x 8 / 1000
                     = 400 seconds
                - The 50000 bytes is converted into bits by multiplying it by 8
                - L = Length of message
                - R = Rate (speed)
            - Propagation delay:
                - PD = d/c
                     = (56 x 10^9) / (3 x 10^8)
                     = 186 seconds
                - The distance is converted into meters
                - d = Distance between source and destination
                - c = Speed of light
            - Total Delay = Transmission Delay + Propagation Delay
                          = 400 + 186
                          = 586 seconds
- Numerical Example
    - Question
        - Houston to send a message of 50000 bytes to Mark on Mars

over a radio link at a speed of 1 Kbps. Mars and Earth are at the orbital furthest distance of 140 million km apart. From the previous question, what has changed? How long does it take for the message to reach Mark from Houston?
(Hint #1: Ignore the processing and queueing delay)
(Hint #2: Speed of light = 3 x 10^8 m/s)
    - Answer
        - The only thing that has changed is the propagation delay
            - Propagation delay:
                - PD = d/c
                = (140 x 10^9) / (3 x 10^8)
                = 466.666666666
                ~ 466.67
            - Transmission delay:
                - 400 seconds
                    - See above
            - Total Delay = Transmission Delay + Propagation Delay
                = 400 + 466.67
                = 866.67 seconds
- Packet Losses
    - In addition to packet delay, packet can also get lost when they are transitioning through the network
    - There are a number of reasons why packets can get lost
        - Transmission links can be unreliable
            - Radio links are notorious for their unreliability
                - Bit error rate of ~10^-6 in radios
                    - In a transfer of 1 million bits, 1 bit will be corrupted
                - Bits can be corrupted due to noise at source or host
            - Optical links have a very high reliability rate, because optical cables are highly insulated
                - Bit error rate of ~10^-15
        - Network congestion can cause packet loss
            - Lots of traffic fills up the queue/buffer, causing new packets to be dropped when they arrive to the switch
    - When packets are corrupted or lost, the routers can detect it
        - The routers cannot recieve the message at all, or they detect some error in the message
            - Typically, the router discards the packet, and does not try to repair it
- Review Of Lecture/Week 1
    - Internet is a network of networks consisting of different ISPs at different tiers
        - ISPs can have two relationships:
            1. Customer-Provider
            2. Peering

    - Since the internet is a network of network, it is quite resilient, and does not have one point of failure
        - i.e. Local outage won't affect other areas
    - It is possible to have multiple ISPs as your provider
        - This is "multi-homing"
- Traceroute allows end hosts to "probe" the paths that packets follow to a specified destination
    - With traceroute, you can also see the approximate roundtrip delay for a particular hub, the IP address or domain name, etc.
- Packets are delivered hop-by-hop through the internet by routers and switches
    - There can be losses and delays at the routers/switches
        - Packet losses are caused by network congestion
        - Delays are caused by the store-and-forward networks