WEEK 2 Study Questions

Self-Check Exercises: Lecture 5

1. In terms of physical media, what is multiplexing
   1. combining several signals into one medium by sending in distinct frequency ranges
   2. managing multiple communication streams onto the same medium
2. What is the role of physical media in access networks.
   1. Access Networks = LAN, Wireless, Home
      1. Provides the required link between sender and receiver pairs
         1. guided and unguided
      2. Analog signlas relating to bits propagate over/through physical media
3. What are some examples of guided media, and where are they used?
   1. Cups with a string
   2. twisted copper wire
      1. high speed LAN
   3. coaxial cable
      1. baseband
      2. broadband
   4. twisted pair connectors
      1. connector
4. What are some examples of unguided media, and where are they used?
   1. Human Speech
   2. LAN
      1. Wifi
   3. Microwave
      1. directional
   4. Wide Area
      1. cellular
   5. Satellite
5. What is the benefit of broadband cabling over baseband cabling?
   1. Broadband – uses a larger part of the wave spectrum and FDM whereas baseband only sends one signal at a time on a limited portion of the wave spectrum
6. Communication via guided media is complex enough by itself, but communication via unguided (wireless) media is even more complicated. What are some additional difficulties of wireless networking?
   1. Reflection
   2. Obstruction by Objects
   3. Interference

Self-Check Exercises: Lecture 6

1. What are the five layers in the Internet Protocol Stack?
   1. Physical
   2. Data-Link
   3. Network
   4. Transport
   5. Application
2. What are some responsibilities of the Application Layer?
   1. Supporting network applications such as HTTP, FTP SMTP (email, web etc), implement presentation and session in the ISO model
   2. Determine destination IP address
   3. Support network applications
   4. Decide which data which will transit the internet
3. The \_\_\_\_\_\_\_\_\_\_\_\_\_\_ layer manages communications from process to process.
   1. transport
4. As a packet is being constructed and passed “down” to the next layer of the internet protocol stack, a new “header” is added. This process is called \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
   1. Encapsulation
5. The payload (non-header portion) of a transport-layer segment is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
   1. Application Data
6. What are some reasons for the layering of network protocols?
   1. Protocols can be tested independently of one another
   2. When Maintenance is required at one level, changes do not affect the other levels
   3. Can update the inner working of a protocol as long as input/output remain the same
   4. The complication of dealing with the intermeshed types of hosts and data is lessened.
7. What are the seven layers in the ISO protocol stack?
   1. Physical Layer
   2. Link Layer
   3. Network Layer
   4. Transport Layer
   5. Session Layer
   6. Presentation Layer
   7. Application Layer

Self-Check Exercises: Lecture 7

1. Viruses and spyware both infect a host computer by being (usually accidentally) downloaded. How is a computer virus different from spyware?
   1. Virus- Corrupts files on host
      1. designed to destroy files and cause a computer to malfunction in some way
   2. Spyware- records keystrokes and other info to collection site
      1. acts like a server, it can request and receive info once connected
2. A \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a group of computers all controlled for a common objective, possibly by an infection in the system, used cooperatively to process and/or send information in mass amounts (DDoS, distributed computing).
   1. botnet
3. An attack which attempts to make network resources unavailable to legitimate users by flooding a system with illegitimate traffic is called a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ attack.
   1. DOS –Denial of service attack
4. If a botnet or another large group of hosts is used to execute this attack it is called a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ attack
   1. DDOS … Distributed denial of service
5. What is “packet sniffing”?
   1. Promiscuous network reads/records all packets passing through
   2. An attacker gets access to communication hardware at some point in the route from a packet’s source to its destination. By intercepting and deconstructing it the attacker can find out the source/destination info and can inspect the actual data message
6. What is “IP spoofing”?
   1. sending a packet with a fake source address ie Sender IP address

Self-Check Exercises: Lecture 8

1. What are some application-layer protocols, and what are they used for?
   1. HTTP,
      1. web
   2. FTP,
      1. file transfer
   3. SMTP,
      1. Mail
   4. DNS
      1. Domain Name
   5. SCCP
      1. VoIP
2. How is client-server architecture different from peer-to-peer (P2P) architecture?
   1. Client-Server
      1. always on server
      2. client and server communicate directly
      3. clients do not communicate with other clients
      4. Client initiates contact
   2. p2p
      1. no always on server
      2. peers intermittently connected on unfixed IP addresses
3. We call a program that is running on a host a \_\_\_\_\_\_\_\_\_\_\_\_.
   1. Process
4. What is the minimum necessary information for identifying a process on a remote host? What do we call this identifier? What do we call a pair of these identifiers (one on each end host)
   1. IP address and Port Number (process)
   2. Socket
   3. Paired set of sockets is called a **connection**
5. What internet service uses default (“well-known”) port #606? (Hint: This is quite deeply buried in RFC #1700.) Request for comments = RFC
   1. Cray Unified Resource Manager
6. How does a client application communicate with a server application, after the connection has been established?
   1. via sockets involved in the connection

Self-Check Exercises: Lecture 9

1. What must an application layer protocol specify?
   1. Type of message (request, response)
   2. Message syntax (field delineation, structure)
   3. Message semantics (meaning of info in fields)
   4. Rules for when and how processes send and respond (how and when)
2. Protocol \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ allows multiple protocols to work together.
   1. **interoperability**
3. What are some applications which would have stringent data integrity requirements?
   1. email, file transfer, web services
4. What are some applications which would have stringent bandwidth requirements?
   1. multimedia, audio, gaming, large databases
5. What are some applications which would have stringent timing requirements?
   1. audio, visual, VoIP, video games
6. What are some applications which would have stringent security requirements?
   1. email, payment services, identity services
7. Application layer protocols must specify transport requirement by selecting a transport protocol from the transport layer.
   1. Give an example of an application that uses TCP, and explain why it uses TCP.
      1. email
         1. needs reliable transport
         2. without need for certain bandwidth
      2. file downloading
         1. provides reliable transfer so that every bit arrives in the correct order
   2. Give an example of an application that uses UDP, and explain why it uses UDP.
      1. Gaming
         1. needs fast transfer speeds
      2. Streaming Video
         1. requires fast data transfer
         2. usually does not provide enough jitter to affect performance
8. What are some services the TCP protocol does not provide?
   1. timing
   2. bandwidth