Group 1: June Stochel, Safayet Zamil, Tatyana Ricketts, Justin Batson
Professor Motovidlak
04:547:331:04
28 April 2021

Super Quiz 2 Study Guide

I. Local Area Networks, Frames, and Topologies
   A. **Multiplexing** - Many sources compete to share one packet over a shared medium (one at a time)
   B. Different categories of Packet Switched Networks
      1. **Local** Area Network - small network usually connected by a switch. Typically in a building, home, or office (< 100 computers). Uses Ethernet protocol.
      2. **Metropolitan** Area Network - Connects various LANs. Covers larger areas like cities or towns.
      3. **Wide** Area Network - Most expensive. Spans multiple cities
   C. Topology shapes
      1. **Star** - Computers connect to a central point (the hub). Hub receives a signal and sends it to the appropriate location
      2. **Bus** - All computers are directly connected to a cable, and all of them receive a signal. Must coordinate so that only one computer sends at a time.
      3. **Ring** - Closed-loop. Computers may connect to a small device, so even if some are disconnected the ring can continue to operate
      4. **Mesh** - Direct connection between each computer. Most expensive, the number of connections needed vastly increases with the number of computers
   D. IEEE supports three types of addresses
      1. **Unicast** - Identifies single computer
      2. **Multicast** - Identifies subset of computers, each computer in the subnet will receive a packet
      3. **Broadcast** - To all computers, every computer on the network will get a copy of the packet

Week 9

1. TCP/IP Troubleshooting Toolkit
   a. Nmap
      i. Add-on tool
      ii. network mapping tool
      iii. While netstat shows you open TCP or UDP ports on your local computer, nmap shows you open TCP or UDP ports on remote computers
      iv. (You can also use nmap to scan your local computer)

v. Passing nmap an IP range instructs it to find any responding computers in that range.

b. wireshark / tcpdump
   i. Wireshark = Add-on tool
   ii. Does packet capture
   iii. Aka "sniffer"
   iv. Display and capture filters possible (to revisit this later)
   v. tcpdump = command line tool that does something similar

2. Scanning / Sniffing review
   a. "Sniffing" = promiscuous packet viewing / capture
      i. promiscuous? (contrast to normal ethernet behavior)
      ii. security implications
      iii. effects of using a hub vs switch
   b. Some basic Wireshark expressions for display filtering
      i. Vs. capture filtering (can only be modified before capture starts)
   c. Drilling down into packets to observe packets at different layers
      i. layers not purely a concept

Week 11

1. UDP (user datagram protocol)
   a. Best-effort delivery: Uses IP for transmission with no further steps to ensure transmission or correct errors. All the delivery problems of IP (messages can be lost, duplicated, delayed, corrupted or delivered out of order) still exist and are not detected or corrected. Remember: IP is also best-effort.
   b. Connectionless: Applications do not need to set up or tear down a connection before sending data; it can be sent at any time. No state information is used or saved; No control messages are used. Data is the only element of the transmission.
   c. Message paradigm: Does not regroup or combine application data before delivery data received exactly as sent by sending application (each message must fit into single IP datagram).
   d. Multiple / arbitrary modes of interaction: Can send 1-to-1, 1-to-many, many-to-1 or many-to-many.
2. TCP (Transmission Control Protocol)
   a. Guaranteed delivery: Uses IP for transmission but takes additional steps, uses "control" information (overhead) to add reliability to the communication (performs retransmission, error correction, and reordering as necessary).
   b. Connection oriented: Applications must request a connection before sending data. Virtual circuit is established before and monitored while data is exchanged for reliable startup and graceful shutdown of connections.

c. Stream paradigm: Sends a continuous sequence of data; application data may be repackaged before delivery (data can span IP datagrams).
d. Point-to-point communication: Each TCP session has exactly 2 endpoints.

Week 12

1. Topology tie-in
    a. Topology = "shape" or map of your network, major defining points, key players
    b. Physical vs logical
    c. LAN vs WAN
        i. At local scale, it's about functionality and connectivity: making stuff work, efficiently
        ii. At wider scale, mostly about reducing bottlenecks and single points of failure, balancing trade-offs between redundancy and cost (e.g., rings or "mesh" between sites, not computers)
    d. Most topologies are "hybrid" – i.e., no single, "ideal" layout
    e. What is the "topology" of your home network? Identify the key players:
        i. Wiring (TP, cat 5, coax) or other "media" (radio waves) – WiFI, Bluetooth, IR?
        ii. Switches, hubs, or access points (including those that may bridge WiFi to Ethernet or your home network to your ISP's)
        iii. Routers that act as switches, perform other services such as NAT, DMZ, VPN

Week 13

1. **Network**
    a. 2 or more devices connected through some medium
2. **Wired world -**
    a. The media are usually copper, fiber optic.
    b. There are different rules (protocols) for defining how to share access to the medium and minimize collisions, when transmission can occur, how to handle lost packets: e.g., CSMA/CD (carrier sense /collision detection), CDMA (code division), FDMA (frequency division)
3. **Wireless world**
    a. Media are things like radio or light waves at different frequencies / parts of the spectrum.
    b. The same fundamental needs as the wired world exist but perhaps in different forms because of specific challenges in the media – e.g., line of sight, penetration of objects, distance from remote nodes ("missing stations"). E.g., instead of "collision detection" (assuming reliability, dealing with problems if they arise) must actively provide ACKs (acknowledging less reliability, actively confirming connectivity and minimizing problems) problems manifest a bit differently and therefore so do the solutions but it's all just "networking"

4. **TCP/IP**
    a. provides the same seamless continuity regardless of things happening at these lower layers.
5. **WiFi**
    a. Is to wireless networking what Ethernet is to wired
    b. Not as established as Ethernet, many protocol variants. But WiFi is roughly your wireless equivalent (WLANs)
    c. WiFi variants essentially boil down to different speeds, frequency bands (2.4 vs 5Ghz), distances. To some extent, the latest is the greatest but some variants may be chosen for specific challenges.
6. **Encryption**
    a. Standards – from WEP to WPA2+
7. **Major modes**
    a. Ad-hoc (peer to peer) vs infrastructure mode (AP manages communications between nodes).
8. **Concept overlap**
    a. Ad-hoc is like mesh, infrastructure like star; bridging can connect wireless segment with wired (e.g., many home networks do this – same IP space, layer 2 communication possible)
9. WiFi > LANS
10. WiMax (microwaves – .3-300Ghz), cells, satellite WANs
11. Fixed (backhaul) vs Mobile
12. PANs
    a. Bluetooth
        i. classes by range, power; varying speeds and distances (speed and distance inversely related in general) – 2.4Ghz
        ii. "profiles" based on functionality
        iii. Bluetooth is to peripheral connectivity as WiFi is to LAN cabling
        iv. Infrared (light)

Week 14, Chapter 29:

1) Get familiar with the Major security problems with details:
    a) Phishing
    b) Misrepresentation
    c) Scams
    d) Denial of Service
    e) Loss of Control
    f) Loss of Data
2) Specific techniques that attackers use, with details:
    a) Wiretapping
    b) Replay

c) Buffer Overflow
d) Address Spoofing
e) DoS and DDoS
f) SYN Flood
g) Password Breaking
h) Port Scanning
i) Packet Interception

3) Different Security policy regarding Data:
a) Data Integrity
b) Data Availability
c) Data Confidentiality
d) Privacy
e) Accountability
f) Authorization

4) Security Technologies:
a) Hashing
b) Encryption
c) Digital Signatures
d) Firewalls
e) VPN

5) Private key and public Key encryption
6) Firewalls and DPI
7) High-level details on VPN

Multiple Choice Questions:

1) In the conventional Ethernet frame, the payload cannot be more than 1500 bytes; in the IEEE 802.3 standard, it cannot be more than 1492 bytes.
a) True
b) False

2) Twisted Pair Ethernet uses which type of Connector?
a) VGA
b) USB
c) RJ-45
d) RJ-11

3) There is a distinction to be made between using the Internet in an incidental way to commit a crime versus a crime that is inherently Internet-based.
a) True
b) False

4) “TCP” stands for transmission control protocol.
a) True

b) False

5) Major security problems. Check all that apply.

1. Scams
2. Ddos
3. Phishing
4. Replay