Problem 1

Jason Lar
204995126

1. C
2. A D
3. B D
4. D
5. A B E
6. C E
7. B D
8. D

Problem 2

1. We want to maximize $Np(1-p)^{2(N-1)}$ which is the probability that any node has success. Take $N = 4 \Rightarrow 4p(1-p)^{2(4-1)} = 4p(1-p)^{6}$

2. CSMA/CD can best serve this scenario. Slotted ALOHA has very bad efficiency and throughput, polling-based MAC has polling overhead which goes against low latency, and TDMA is not well suited for variable-rate data transfer due to wasted slots. CSMA/CD is better because it's random access so it's good for variable rate and has high throughput since nodes transfer entire frames unless collision is detected, but the overall protocol has a high rate of success.

3. The two methods to implement TCP protocol in Project 2 were Selective Repeat, which keeps an individual retransmission timer for each packet in the window, and Go-Back-N, which only keeps a timer for the oldest unacked packet. They differ in that Selective Repeat retransmits individual segments when they timeout, and Go-Back-N retransmits the unacked segment and all subsequent segments in the window.

4. The ACK that is returned by the base station after the SIFS is mainly used to handle the hidden terminal problem in WiFi. The ACK basically notifies the sending node that its frame was received successfully in case there is a collision that occurs that the nodes on the network cannot detect. This differs in objective from the TCP ACK, as TCP ACKs are primarily used for reliable data transfer, so that the sender knows its packets reached the receiver successfully; the difference is that the WiFi ACK is for detecting a problem inherent to WiFi, whereas TCP is dealing with ensuring reliable data transfer.

Problem 2 Cont.

5. The man-in-the-middle attack is where an attacker sniffs a connection between two hosts and effectively intercepts messages sent between these two hosts and can send its own messages to either or both of the hosts, pretending to be one of them when "talking" to the other. The crux of the issue is authenticating that a received message is in fact from the right sender and not a man-in-the-middle; this can be defended against using a third party known as a Certification Authority. The Certification Authority is a party known to both end hosts which can sign the messages of the end hosts so that either of them can verify that a received message is from the correct sender.

6. IP packets are routed and forwarded in VPN using Security Associations, which makes the network layer connection-oriented for the purposes of VPN. Essentially, each endpoint on a link stores a Security Association Database, where it can locate specific state information about the connection and upon receiving a datagram it can reference the database using the Security Parameter Index in the IPSec header and know where to route and forward the datagram to, as the SAD stores the destination SA interface for the entry indexed by the datagram's SPI.

7. No, collisions can occur if a nearby Access Point is using a channel on an overlapping frequency with the one we're looking at, or if the request-to-send packets collide. To deal with collisions, CSMA/CA uses random backoff intervals, which determine when a node should begin transmitting with a certain probability. the hope is that only one node succeeds and transmits at a time, utilizing the RTS-CTS handshake.

Problem 3

1. ~~The three protocols are~~
Three protocols used are CSMA/CA for WiFi, DHCP for getting the IP, and UDP, which DHCP is built on.

2. Two protocols used are CSMA/CA for WiFi, and ARP to get the MAC address of the other host.

3. Two used protocols are DNS at the application layer and UDP at the transport layer.

4. Two transport-layer or above protocols are HTTP at the application layer and TCP at the transport layer.

5. Two routing protocols used are OSPF for intra-AS routing and eBGP for inter-AS routing, since Google's webserver is in another AS.

6. ~~ARP is a plug-and-play protocol,~~
ARP is a plug-and-play protocol, since it's self learning and requires no configuration

Problem 4

1. Using a a single Ethernet is essentially a single Broadcast domain, which has efficiency issues as ~~[illegible]~~ many nodes transmitting in the network could lead to collisions and decrease performance, as Ethernet uses CSMA/CD which only has collision detection and not avoidance.

2. a) VLAN algorithms will be needed to interconnect the Ethernets. No changes are necessary for the user devices due to the nature of port-based VLAN.

b) Yes, since we must connect the VLANs by their trunk port and ~~[illegible]~~ depending on the number of switches, we may need to assign groups of ports on one switch to a specific VLAN.

c) The solution is using VLANs, by configuring groups of ports to specific VLANS on a single switch, which essentially will separate data traffic of the two departments.

~~d) The routers will need to implement mobility functions to act as home agents and foreign agents. This can then be used to configure a mobile IP: [illegible] indirect routing infrastructure for mobility.~~

~~e) The CS department's routers must implement~~

d) The base-stations and mobile devices must implement passive scanning so that the mobile devices switch access points when the user is moving.

e) The EE department's routers must implement mobility to have ~~[illegible]~~ home agent functions, while the CS department routers must implement mobility to have foreign agent functions for indirect routing.

Problem 4 Cont.

3. a) Yes, collision affects the local area network, so separating by routers can reduce the number of nodes in the LAN and reduce collisions.

b)

c) The routers at EE must support mobility as well as the CS routers in order to implement indirect routing between correspondents, home agents, and foreign agents.

4. a) The broadcast-enabled router can advertise its IP to the mobile device via an ICMP advertisement, which the User can receive and then send its IP broadcast packets to. This makes it so that the broadcast enabled router receives the packets, but the other routers don't.

b)

Problem 5

1. Using certification authorities, ~~it's built into Alice's [illegible]~~ a CA can effectively sign Bob's public key with a secret key, then once Bob transmits it ~~or~~ to Alice, Alice can use the CA's public key to decrypt it to verify that ~~is~~ Bob's public key.

2. Certification authorities are built into the operating system, so Bob and Alice both know the CA's digital signature and can verify its authenticity.

3. Yes, use ~~the~~ Bob's public key to encrypt a shared, secret key on Alice's side. Then send this encrypted shared key to Bob, which Bob can then decrypt with his secret key. Both Bob and Alice now have the shared key to efficiently encrypt their data communications.

4. Alice can sign a dummy message with Bob's new key and then attempt to decrypt it with the previous public key. If the message is correctly decrypted, we can verify it's Bob's new key.

5. Tracy can launch a man-in-the-middle attack by sending messages to Alice requesting information for a malicious message, but with Bob's headers, ~~Tracy can't~~ to pretend that it's Bob sending the messages. Tracy can then intercept Alice's responses to get information.

6. Tracy can launch a playback (replay) attack on Bob, by recording Alice's previous sent message and replaying it to Bob later, since there is no nonce to indicate it's a repeat.