Sidharth Shanker

Computer Networks

April 21, 2012

Written Assignment 5

1

Wireshark Lab:

1. The SSID’s of the two access points issuing the most number of beacon frames in this trace are “30 Monroe St.” and “linksys\_SES\_24086”.
2. From the 30 Monroe St. access point, the intervals of time between transmissions of the beacon frames is .1024 seconds, while from linksys\_ses\_24086 it is also .1024 seconds.
3. The source MAC address on the beacon frame from 30 Monroe St is (00:16:b6:f7:1d:51).
4. The destination MAC address on the beacon frame from 30 Monroe St. is (ff:ff:ff:ff:ff:ff).
5. The MAC BSS id on the beacon frame from 30 Monroe St. is (00:16:b6:f7:1d:51), the same as the source address.
6. The extended rates given in the beacon frames are 6 mbps, 9, mbps, 12 mbps, 24 mbps, 36 mbps, 48 mbps, and 54 mbps.
7. The three MAC address fields in the 802.11 frame are (00:13:02:d1:b6:4f), (00:16:b6:f7:1d:51), and (00:16:b6:f7:1d:51). The MAC address of the host sending the packet is (00:13:02:d1:b6:4f), the MAC address corresponding to the access point is (00:16:b6:f7:1d:51). Since the access point is the first-hop router to which the source host is connected, the MAC address of the first-hop router is naturally (00:16:b6:f7:1d:51). The IP address of the wireless host sending this TCP segment is 192.168.1.109, and the destination IP is 128.199.245.12. The destination corresponds to final destination of the packet, which is whatever server hosts gaia.cs.umass.edu.
8. The three MAC address fields contained in the 802.11 frame are (92:2a:b0:49:b6:4f), (00:16:b6:f7:1d:51), and (00:16:b6:f7:1d:51). The MAC address of the host that sends this packet is (00:16:b6:f4:eb:a8), the MAC address of the destination is (91:2a:b0:49:b6:4f). The first-hop router that the host is connected to is (00:16:b6:f4:eb:a8). The sender MAC address in the frame does not correspond to the IP address of the device that sent the TCP segment in the datagram, it in fact corresponds to the first-hop router to which the host is connected.
9. The two actions taken by the host in the trace to end the association with the 30 Monroe St. AP that was initially in place are first a DHCP release at the IP layer, followed by a deauthentication at the 802.11 layer. Based on the 802.11 spec, it looks like a disassociation should have also been sent.
10. There are 5 authentication messages sent from the wireless host to the Linksys\_ses\_24086 AP.
11. The host wants the authentication to be open, as in the fixed parameters Authentication Algorithms: Open System is specified.
12. There is no reply from the Linksys\_ses\_24086 AP in the trace.
13. At t=63.168087 an Authentication frame is sent from the host to the AP (30 Monroe St.), and at t=63.169071 there is a reply Authentication sent from the AP to the wireless host.
14. At t=63.169910 there is an Association request sent from the wireless host to the AP, and at t=63.192101 there is an association response sent from the AP to the wireless host.
15. The wireless host specifies the transmission reates it is willing to use in the Association request frame as 1 mbps, 2 mbps , 5.5 mbps, 11, 6 mbps, 9 mbps, 12 mbps, 18 mbps, 24 mbps, 32 mbps, 48 mbps, and 54 mbps.
16. In the PROBE REQUEST frames, the sender MAC address is 00:12:f0:1f:57:13 and the BSS and receiver MAC Addresses are given as the broadcast address, or ff:ff:ff:ff:ff:ff. In the PROBE RESPONSE frames, the source is given as (00:16:b6:f7:1d:51), the destination is 00:12:f0:1f:57:13, and the BSS given is (00:16:b6:f7:1d:51). The purpose of these frames is to find an access point, and the probe response is sent from the AP to the requesting host when the AP is found.

2

1. The probability of a single device not transmitting is . In order for a device to transmit successfully, that means that no other device can be transmitting during the time in which the single device needs to transmit. Given that it takes L microseconds to transmit, the probability of no device transmitting in a time period of size L is . The probability then of all but one device not transmitting in that time period is
2. Since the probability of an unslotted ALOHA device not transmitting is in time period L microseconds, the probability of an unslotted ALOHA device transmitting successfully is going to be the probability of no slotted devices but one transmitting, multiplied by the probability of no unslotted ALOHA device transmitting:
3. The probability of successful transmission for a uniformly selected device is simply the weighted average of the two probabilities.

3

1. It is possible for B to collide with A, and then for A to finish transmitting before noticing the collision and then assuming that the frame transmitted successfully. This can happen because the limit on A sending bits is the size of the Ethernet bus, but the speed at which bits reach host B is determined by the propagation delay. So if A transmits its bits faster than it takes bits from B to reach A, then the collision will not be detected and A will think the frame was successfully sent.
2. A solution to this problem can be constructed by setting a minimum frame size. This guarantees that A will take at least the time that it takes for a bit from B to arrive at A to finish sending the bits in the frame that it is sending. For nodes at a distance of d and a propagation speed of , a minimum frame size can be determined as follows:

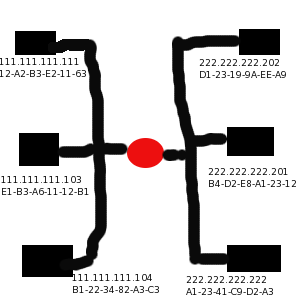
Let t = time it takes for a single bit to propagate from B to A, and then return from A to B

let m = minimum frame size

For d=2km:

4

1. IP addresses are 24 bits.



1. The physical addresses of devices cannot be the same as the IP addresses of those devices because the MAC addresses of devices uses a completely different protocol. Rather than being 24 bits, MAC addresses are 48 bits. While IP addresses can be dynamically assigned, MAC addresses belong to the device. See the above diagram (for number 1) to see the addressing of the devices.
2. In the IP datagram sent from A to E, the only IP addresses stored are the IP address of the source device, and the IP address of the destination. A already knows what its IP address is, so it simply includes it in the packet, and must know E’s IP address to know to send an IP datagram to E. Therefore it simply includes these two IP addresses in the datagram, and then sends them to the router, which is addressed by its MAC address on the link-layer. The source IP address in the datagram would be 111.111.111.111, and the destination IP address would be 222.222.222.222. The LAN addresses needed for the data link layer frame, which would contain the MAC addresses of the source and destination nodes, would be determined through ARP, in which each device keeps an ARP table which maps IP addresses of neighboring devices to MAC addresses. ARP gains this information by for each unknown IP, sending ARP packets to all other nodes in a subnet to determine the MAC address of that IP address.
3. IP addresses would change since as there is a bridge, all the machines in the network are on the same subnet. The MAC addresses would not change, as the LAN addresses are specific to the machines. A learning bridge learns the addresses of the attached hosts by keeping a switch table that for each device that sends a frame to it, the switch records the MAC address of that node and the interface that the frame came from. The table also records the time at which the frame was sent so that if a computer disconnects from the switch, it’s MAC address will eventually be removed from the table after an aging time.