Yulong Tan

INFO 341

10.16.2016

Lab 3: TCP/IP Frames

For this lab, we use Ethernet cables as well for the primary connection. The destination IP address was 192.168.100.5. which was the access point.

Wireshark was used to capture the frames on the LAN. To specifically look for TCP packets, we looked at ones with the protocol of TCP by using Wireshark’s filtering feature. You can view the packets that are displayed in the packet list pane by clicking on a packet in the packet list pane, which will bring up the selected packet in the tree view and byte view panes.

The data in the TCP packets also showed us a sequence number to identify each byte of data. It’s important, because it identifies the ordering of the bytes sent from each computer, so that even if there are errors during transmission, the data can be reconstructed. They show you where you are in the connection. If a station expected one sequence number but received another, the number it expected will be transmitted back to the sender in hopes of receiving the correct packet and sequence number. This ensures proper data delivery. Similarly, the acknowledgement number indicates the next sequence number that the receiver is expecting. This is why sequence and acknowledgement numbers are very good for troubleshooting.

There are two types of internet traffic: UDP and TCP. UDP is suitable fort applications that need fast and efficient transmission. It would be used on reliable media because we don’t want many errors, since UDP does not do error correction and does not want to retransmit. The protocol does support error detection via checksum but when an error is detected, the packet is discarded. UDP is a connectionless protocol, and does not resend lost data, which makes it good applications like gaming, watching movies and voice over IP. On the other hand, TCP is a connection oriented protocol, so it is used over unreliable media. TCP transmissions are sent in a sequence and they are received in the same sequence. In the event of data segments arriving in wrong order, TCP reorders and delivers application. It rearranges data packets in the order specified and the transmission time is less critical, so it can take its time. TCP is really good at error checking and provides retransmission of data if packets are lost or corrupted, which happens when using less reliable media.

TCP/UDP ports indicate which application you’re using, since different ports are for different applications.

A device ARPs anytime a session is started and you need to establish a connection to a new device. An ARP is needed to get the destination MAC address that matches the IP address. It broadcasts to all machines on the LAN to see if one machine knows that it has an IP address associated with it.