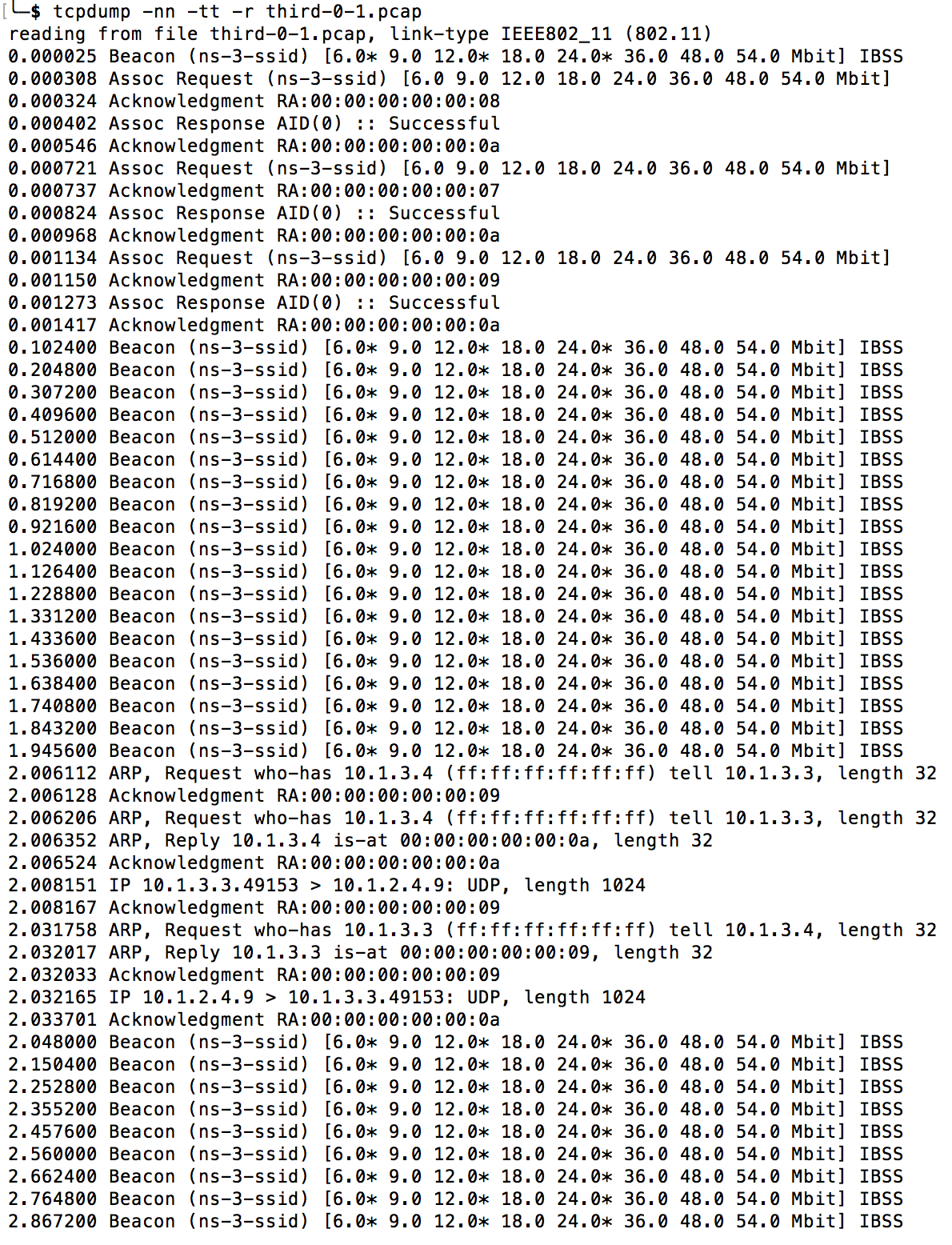
EE450: LAB 4

SESSION 4

Tushar Tiwari

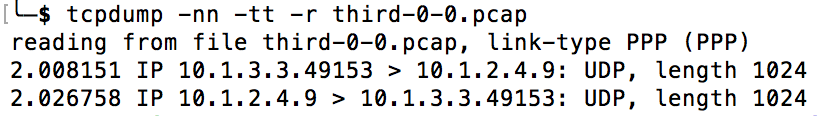
***Aim***: To simulate a combined network topology that includes a point to point link, an Ethernet link as well as Wireless links using ns-3.

***Trace file for Wi-Fi:***

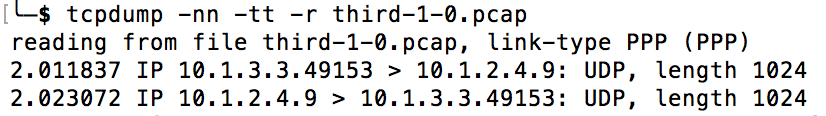


***The above beacon is transmitted for the remainder time.***

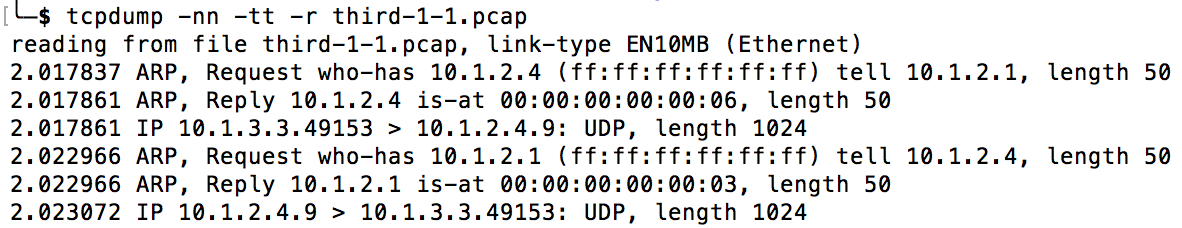
***Trace file for left side of Point to Point link:***



***Trace file for right side of point to point link:***



***Trace file for CSMA network:***



***Q1.1***

There are three ARP requests made in the Wi-Fi trace and two are made in the CSMA network. Total 5. The first two requests are made when the client (10.1.3.3) is trying to send its echo to the server and in order to do so must determine the mac address of the next hop which is the access point (10.1.3.4). The next ARP request is made by node 1 on the CSMA bus to determine the mac address of the server with IP address 10.1.2.4 so it can pass the message from the client. The next one is again made on the CSMA network when the server (10.1.2.4) receives the echo request and turns the packet around trying to send it back to the source. The server knows that this address is on another network that it reaches via IP address 10.1.2.1. This is because global routing is initialized and it has figured all of this out for us. But, the echo server node doesn’t know the MAC address of the first CSMA node, so it has to ARP for it just like the first CSMA node had to do. Finally, the last ARP request is made by the Access Point (10.1.3.4) to pass over the echo from the server to the client and in order to do so needs to determine the mac address of the client (10.1.3.3).

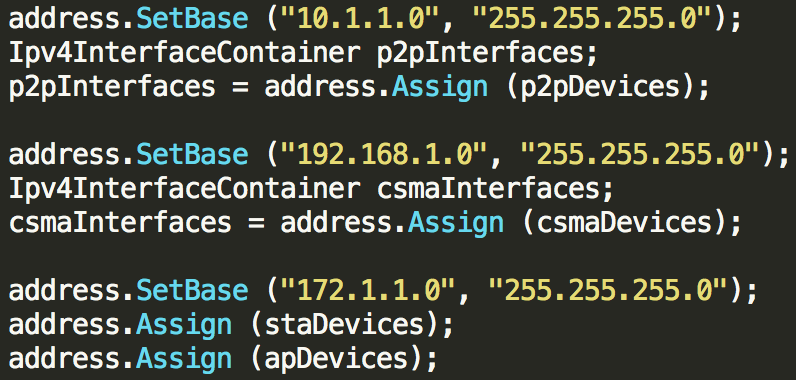
***Q1.2***

There are total 4 steps to establish connection with a wireless access point:

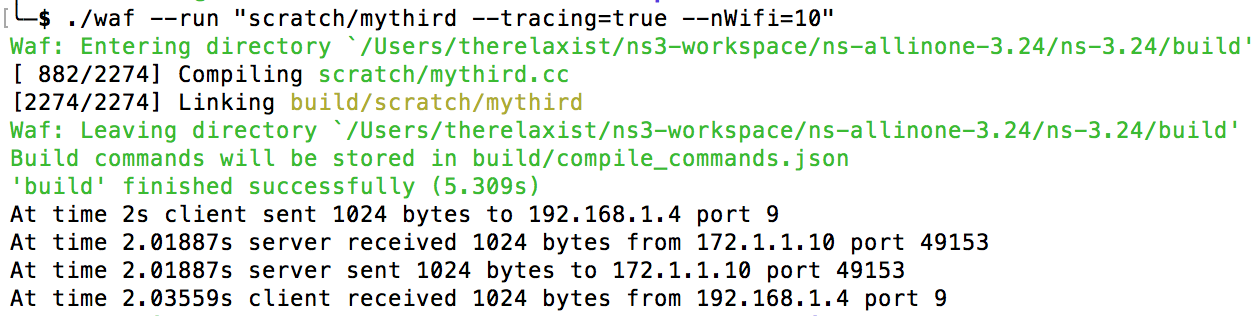
Initially the wireless access point (AP) is transmitting a beacon containing the SSID and supported rates.

1. This beacon is picked up by the wireless device which then sends an association request.
2. The AP provides an acknowledgement that it has received the request.
3. If the association is successful, then the AP sends a Successful Association Response, else Failure Association Response.
4. Finally, the wireless device acknowledges the Association Response.

IP address changes:

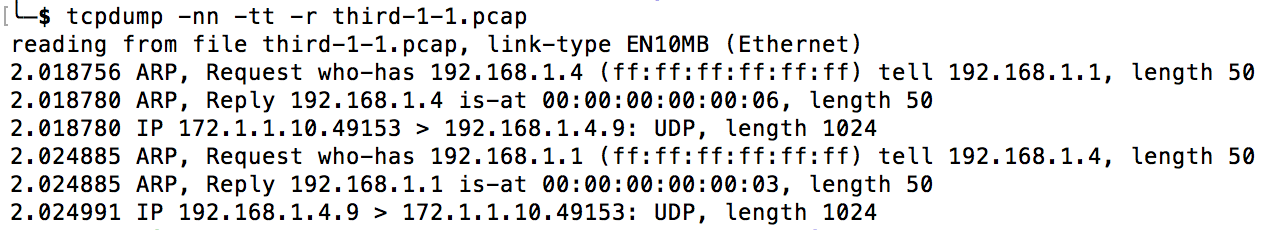


***Output:***

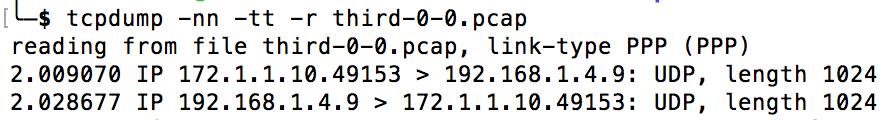


***Trace Files:***

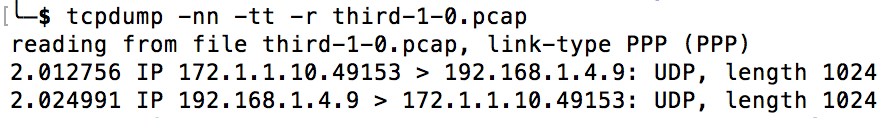
***Trace file for CSMA network:***

******

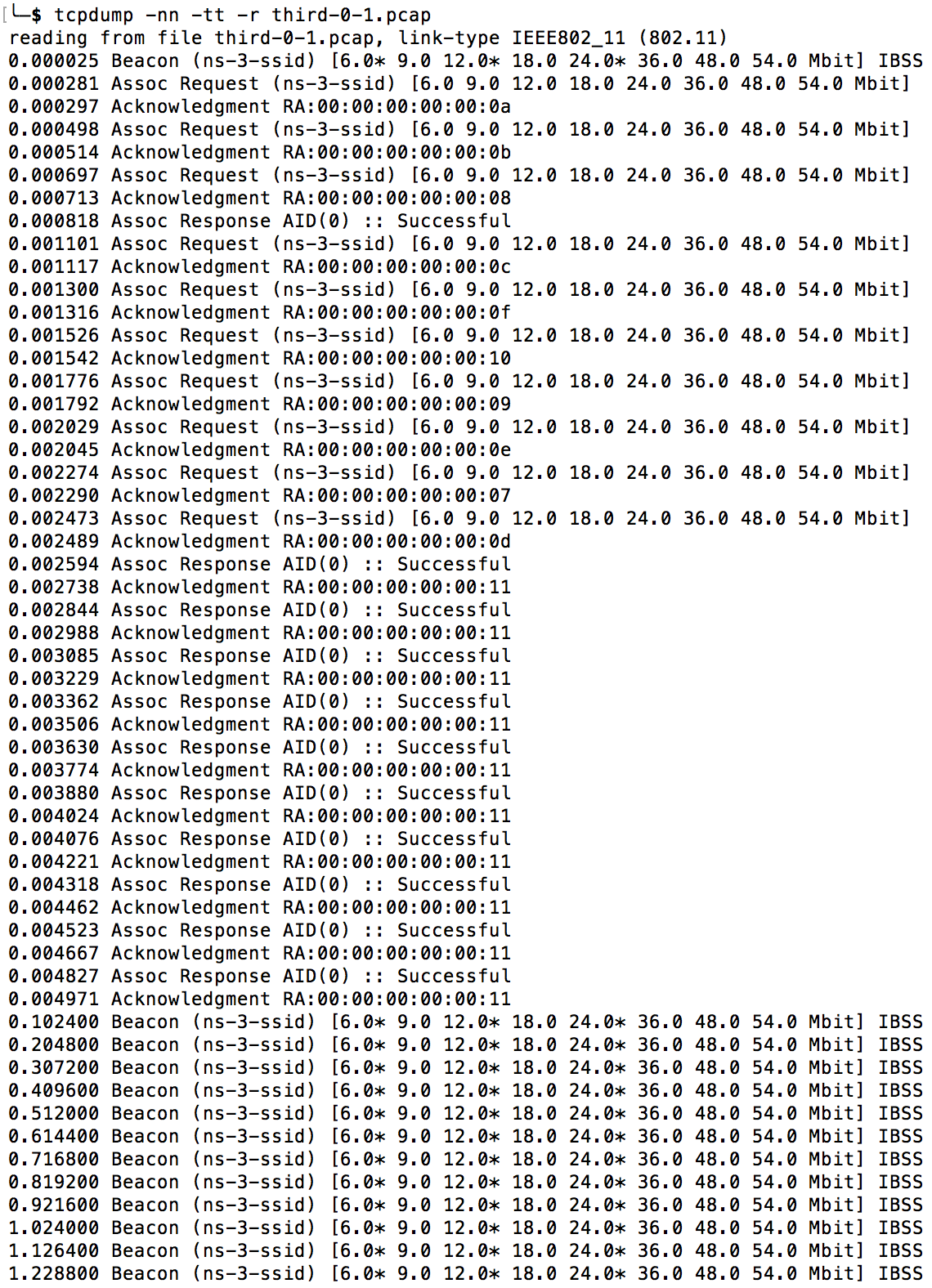
***Trace file for left side of Point to Point link:***

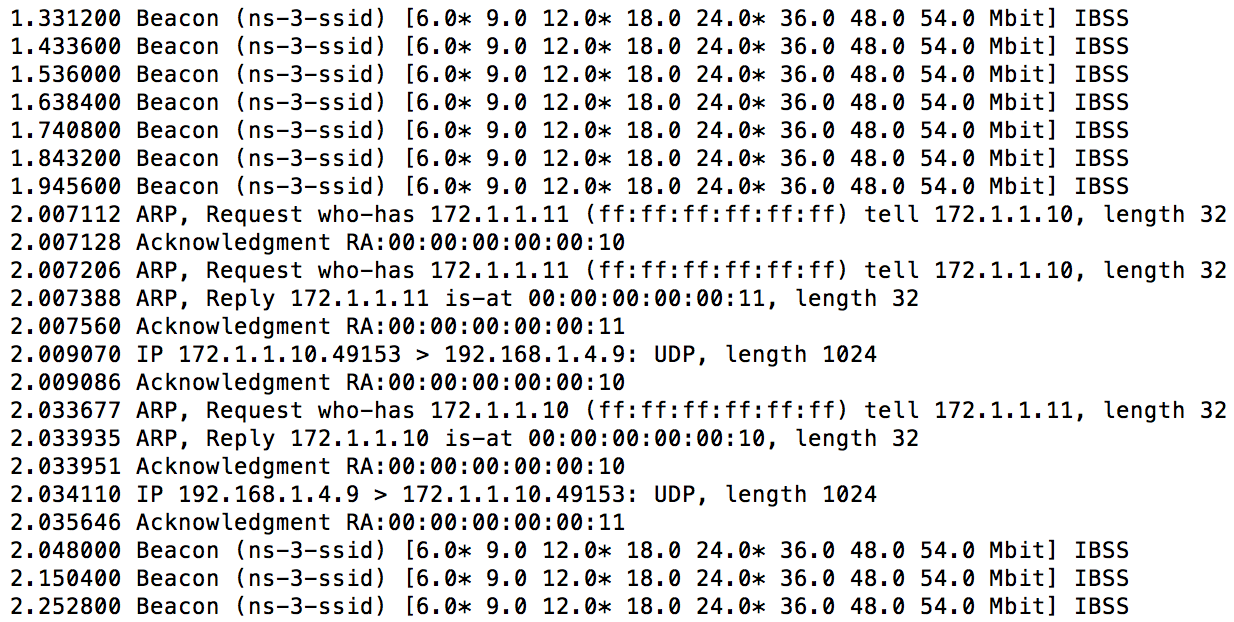
******

***Trace file for right side of point to point link:***

******

***Trace file for Wi-Fi:***

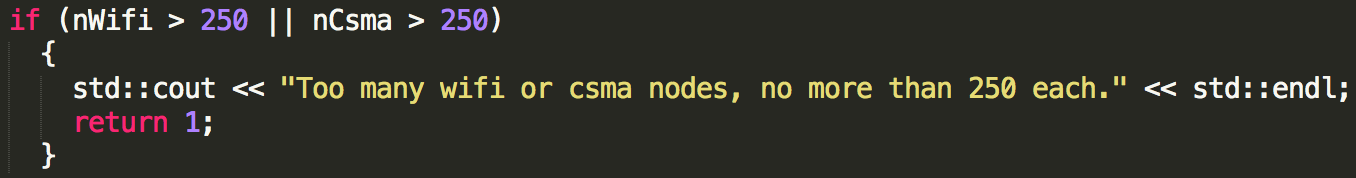
******

******

***The above beacon is transmitted for the remainder time.***

***Q2.1*** Count number of Association Responses that have status code successful and have unique destination mac addresses.

***Q2.2*** 250 due to programming constraints. Although this number depends on the subnet mask. Technically with subnet mask of 255.255.255.0 we could support 256 devices including AP.



***Q3.1***

In Passive mode that we have seen in the earlier problems the wireless device listens for beacons that are sent out by the AP. The disadvantage of this maybe that devices may have to wait for long periods for a valid beacon. However, an advantage in this method could be that the network traffic will be less.

Active probing is the process where in the wireless device (trying to connect) sends out a broadcast probe request to solicit a probe response from the AP. This probe response is picked up by the device and then followed up by the association steps which are similar to the passive mode. The major difference from passive mode is that the device does not have to wait for the beacon but causes lot of traffic on the network.

***Q3.2*** This lab was by far the best. I had never envisioned such sophistication in a network simulator. This lab showed me how easy it can be to simulate complex networks with simple code and also makes me wonder of its applications in the industry when making a choice in network topology.

***Conclusion:*** The ns-3 tool is a fantastic tool that can simulate complex network configurations with verbose logging and packet trace. Using this tool in this lab, I learnt how to create a basic network containing a wireless device, a CSMA network and a point to point network. I also learnt the differences in the probing techniques in wireless scanning.

