Juan Dominguez
Salissa Hernandez
Noah Nyabadza

Assignment 2

1. Fiber has several advantages over copper as a transmission medium. First, it can handle much higher bandwidth than copper. Second, it is not affected by power surges, electromagnetic interference, power failures, or corrosive chemicals in the air. Third, it does not leak light and is a bit difficult to tap. Finally, it is thin and lightweight, resulting in much lower installation costs. However, there are also several disadvantages for using fiber optics over copper. First, it can be damaged easily by being bent too much. Second, optical communication is unidirectional, which requires either two fibers or two frequency bands on one fiber for two-way communication. Finally, fiber interfaces cost more than electrical interfaces.

2. When a mobile user crosses from one cell to another, the network needs to perform a handoff by assigning a new frequency in the target cell to continue the call. Since frequencies cannot be reused in adjacent cells, the new cell must have a free channel available. If all the frequencies in that cell are already in use, the handoff cannot be completed, therefore resulting in the call being abruptly dropped, even though the transmitters and receivers are functioning correctly.

3. The output after stuffing is “A B ESC ESC C ESC ESC ESC FLAG ESC FLAG D”.

4. Yes, it is possible for the sender to start the timer when it is already running each time it transmits a new frame. If the time was already running, it resets to allow another full interval. After transmitting a frame and starting the timer, the sender waits for something exciting to happen. If a valid acknowledgement comes in, the sender fetches the next packet from its network layer and puts it in the buffer, overwriting the previous packet and advancing the sequence number. If a damaged frame arrives or the timer expires, neither the buffer nor the sequence number is changed so that a duplicate can be sent. Duplicates and damaged frames are not passed to the network layer, but they cause the last correctly received frame to be acknowledged to signal the sender to advance to the next frame or retransmit a damaged frame.

5. Yes, this change would affect the protocol’s correctness. It might lead to deadlock. Suppose that a batch of frames arrived correctly and was accepted. The receiver would advance its window. Now if we suppose that all the acknowledgements were lost, the sender would eventually time out and send the first frame again. The receiver would then send a NAK. If this packet were lost, from that point on, the sender would keep timing out and sending a frame that had already been accepted, but the receiver would just ignore it. Setting the auxiliary timer results in a correct acknowledgement being sent back eventually instead, which resynchronizes.

Juan Dominguez
Salissa Hernandez
Noah Nyabadza

Assignment 2

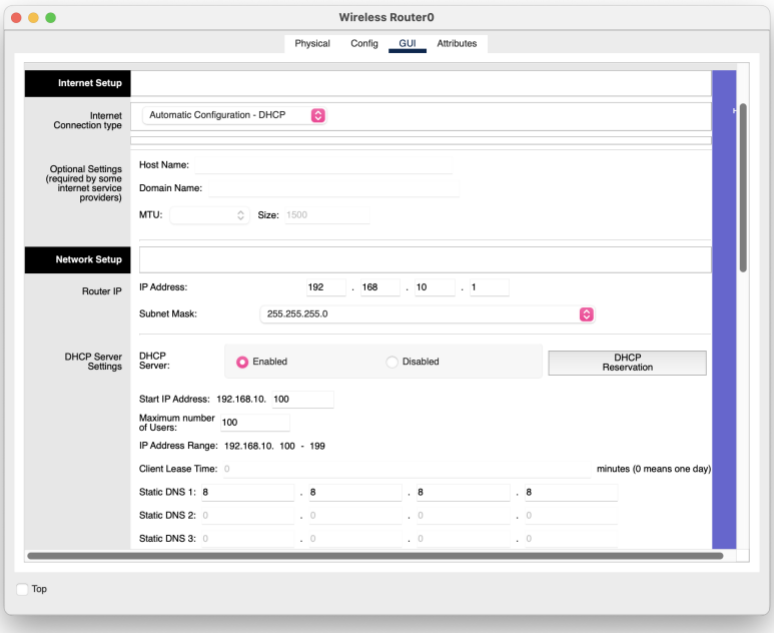
6. It would affect both the correctness of the protocol and the performance. It would lead to deadlock because this is the only place that incoming acknowledgements are processed. Without this code, the sender would keep timing out and never make any progress.

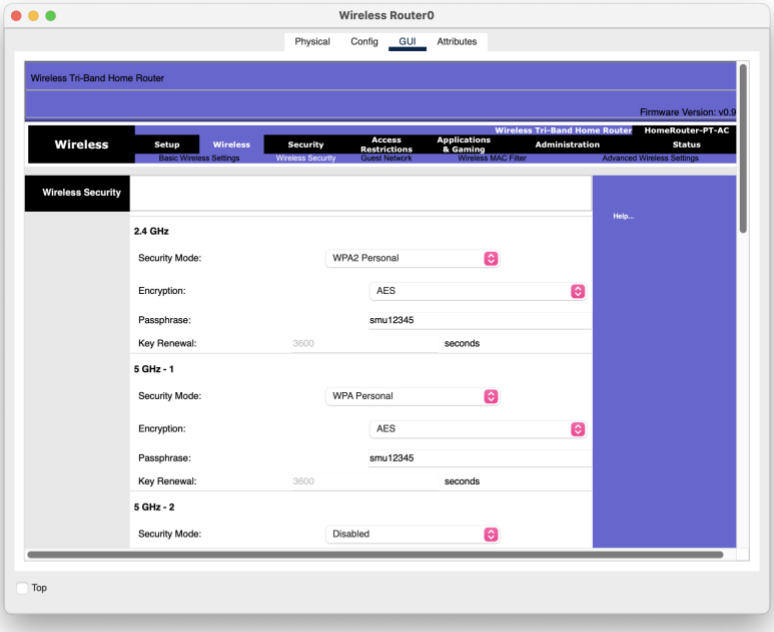
7. In this lab, I implemented a small LAN for eight laptops using Cisco Packet Tracer. All laptops connect wirelessly to a Wireless Router (SSID: *SMU-Lab*), which is configured with WPA2-PSK encryption for secure access. The router's LAN IP is 192.168.10.1 and it runs a DHCP service that automatically assigns client addresses from 192.168.10.100 to 192.168.10.199. The router uplinks to a 2960 switch, which in turn connects to a server configured with the static IP 192.168.10.10. The server is running HTTP services, allowing all laptops to reach its webpage over the network.

   Testing confirmed the design worked as intended. In Realtime Mode, laptops successfully received IP addresses, pinged both the router and server, and accessed the server's web page via http://192.168.10.10. In Simulation Mode, I observed the DHCP DORA sequence, ARP requests, ICMP Echo/Reply packets, and HTTP GET/OK messages. These demonstrate proper end-to-end communication across layers: at the physical layer, Cat6 cabling connected the router, switch, and server while Wi-Fi handled client access; at the data link layer, Ethernet (802.3) and Wi-Fi (802.11) protocols ensured reliable frame delivery using CRC/FCS error detection and retransmissions; and at the application layer, HTTP successfully delivered web content.

Juan Dominguez
Salissa Hernandez
Noah Nyabadza

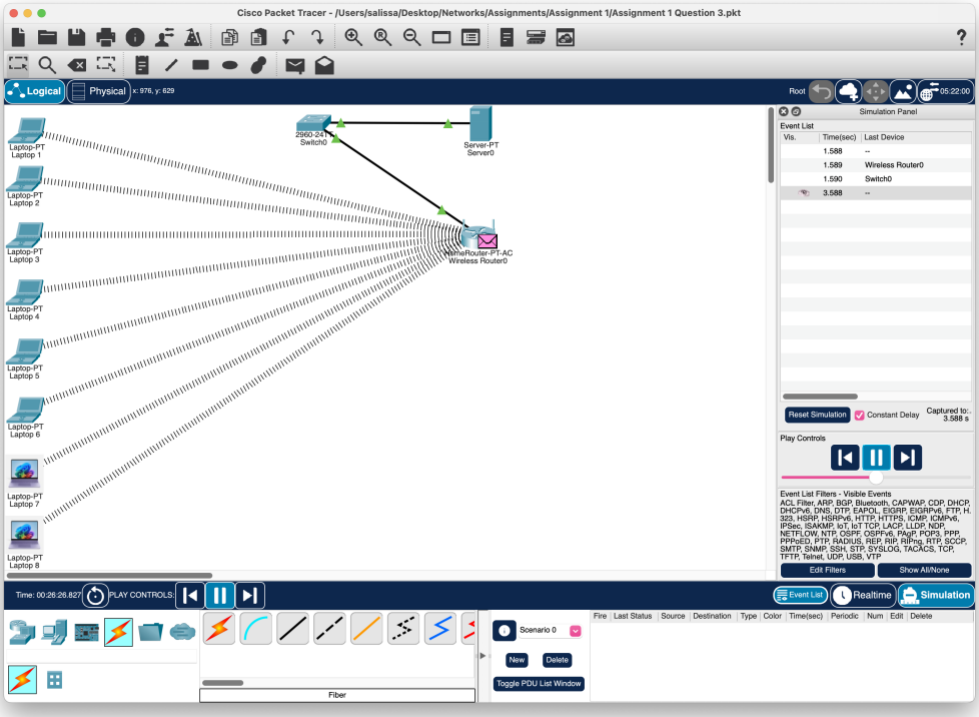
Assignment 2





Juan Dominguez
Salissa Hernandez
Noah Nyabadza

Assignment 2



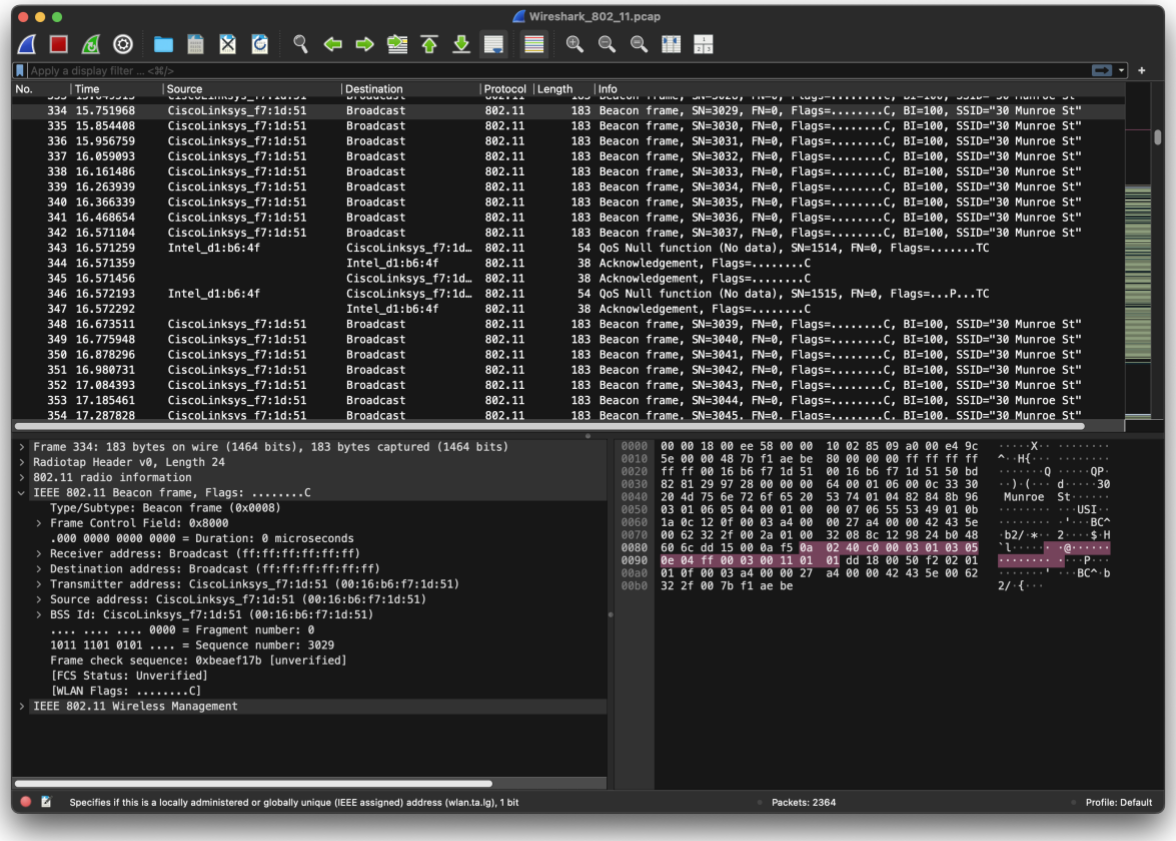
8. Data Link Layers Protocols Identified:

Juan Dominguez
Salissa Hernandez
Noah Nyabadza

Assignment 2

1. IEEE 802.11 Beacon
2. IEEE 802.11 Data Frames
3. IEEE 802.11 Control Frames
4. LLC Logical Link Control
5. ARP Address Resolution Protocol
6. EAPOL Authentication – WPA

Beacon



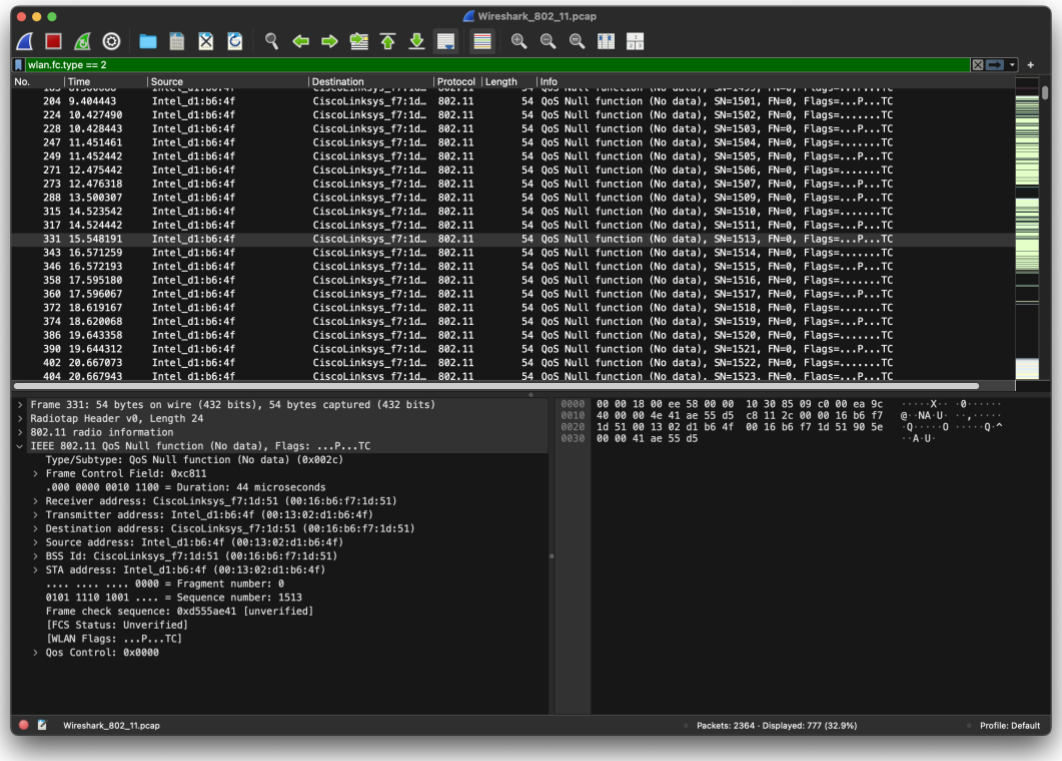
In this capture, we observe an IEEE 802.11 Beacon frame, which is a management frame broadcast by the access point to announce the presence of the wireless network. The source address is the AP (CiscoLinksys_f7:1d:51), while the destination address is the broadcast address (ff:ff:ff:ff:ff:ff), indicating it is sent to all nearby clients. Each beacon frame has a fixed length of 183 bytes in this trace, reflecting its role as a small, repetitive signal rather than a data-carrying packet. The packet list shows many beacon frames with sequential sequence numbers (3029, 3031, 3033), which confirms they are sent at regular intervals (~100 ms). A consistent pattern is observed where the source remains the same (the AP), the destination is always

Juan Dominguez
Salissa Hernandez
Noah Nyabadza

Assignment 2

broadcast, and the SSID field advertises the network name “30 Munroe St.” This highlights how beacon frames provide essential network discovery information but do not vary in size or payload content the way data frames do.

Data Frame

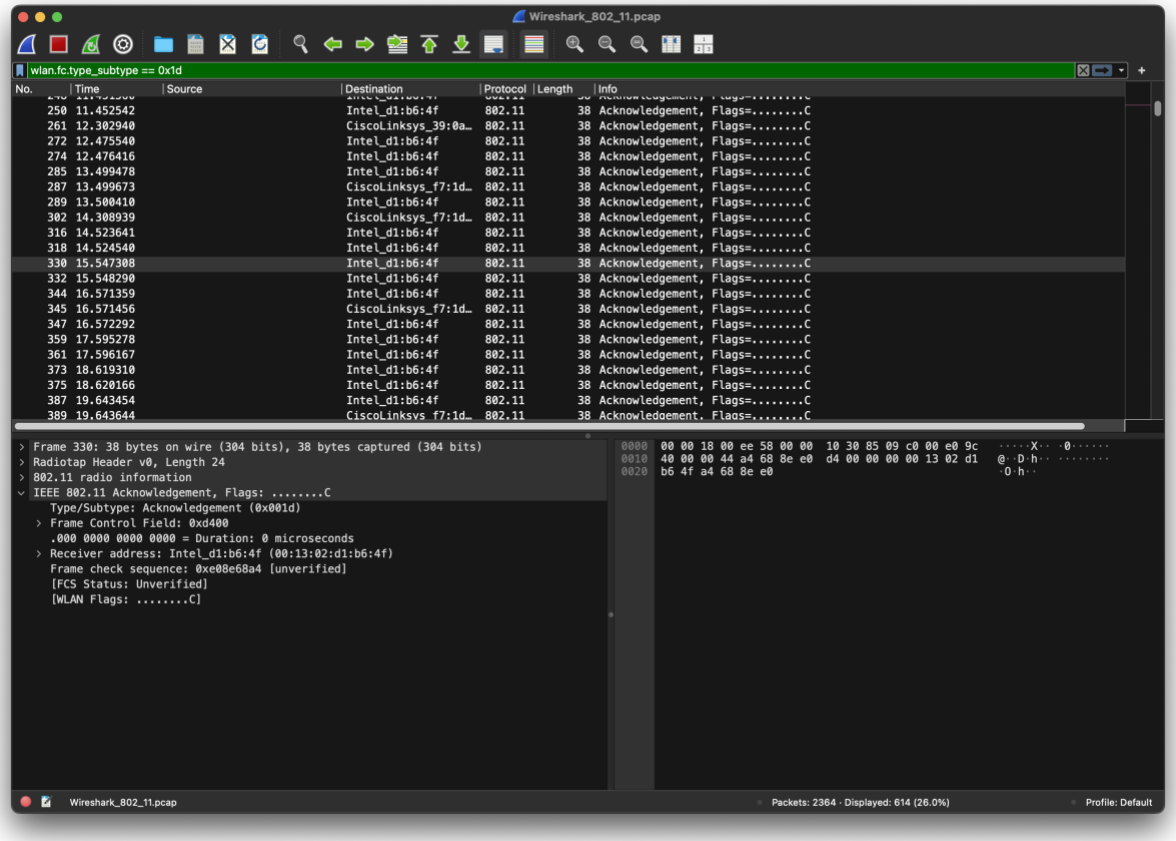


In this capture, we observe an IEEE 802.11 Data frame with subtype QoS Null function, which is used by wireless stations to signal Quality of Service and power management features without carrying actual data payloads. The source address is the wireless client (Intel_d1:b6:4f), and the destination address is the access point (CiscoLinksys_f7:1d:51), showing typical client-to-AP communication. Unlike beacon frames, these packets are smaller in size here, only 54 bytes because they carry no upper-layer data. The sequence numbers (1513, 1514, 1515) increment sequentially, indicating an ordered transmission stream from the client. This pattern differs from beacons, as the traffic is unicast rather than broadcast and reflects client activity rather than AP announcements.

ACK

Juan Dominguez
Salissa Hernandez
Noah Nyabadza

Assignment 2

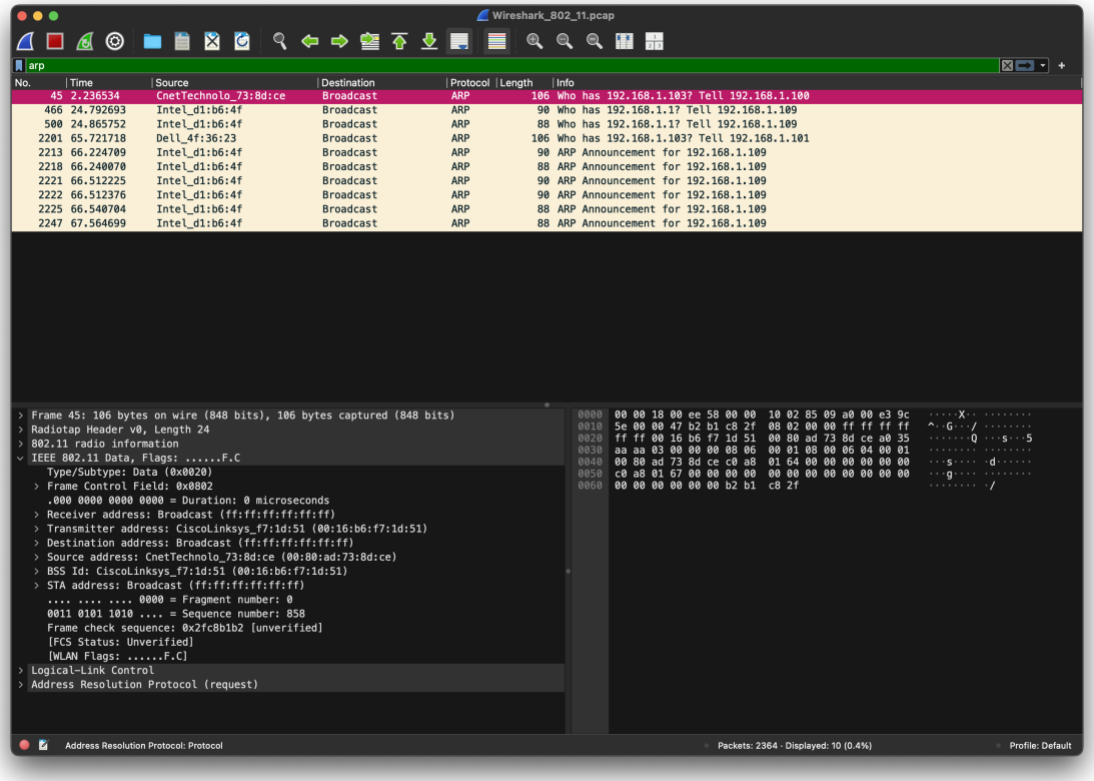


In this capture, we see an IEEE 802.11 Acknowledgment (ACK) frame, which is a control frame used to confirm the successful receipt of a transmitted packet. The **s**ource address alternates between the access point (CiscoLinksys_f7:1d:51) and the client (Intel_d1:b6:4f), depending on who is acknowledging the prior transmission. The destination address is always the intended sender of the original frame, making this unicast rather than broadcast traffic. ACKs are very small, only 38 bytes, because they do not carry any data payload; their sole function is reliability. The sequential bursts of ACKs in the packet list reflect ongoing communication between client and AP, ensuring that each transmitted data frame is properly received before the next one is sent. This behavior contrasts sharply with broadcast-only beacons, highlighting how ACKs enforce reliable delivery in Wi-Fi.

ARP

Juan Dominguez
Salissa Hernandez
Noah Nyabadza

Assignment 2

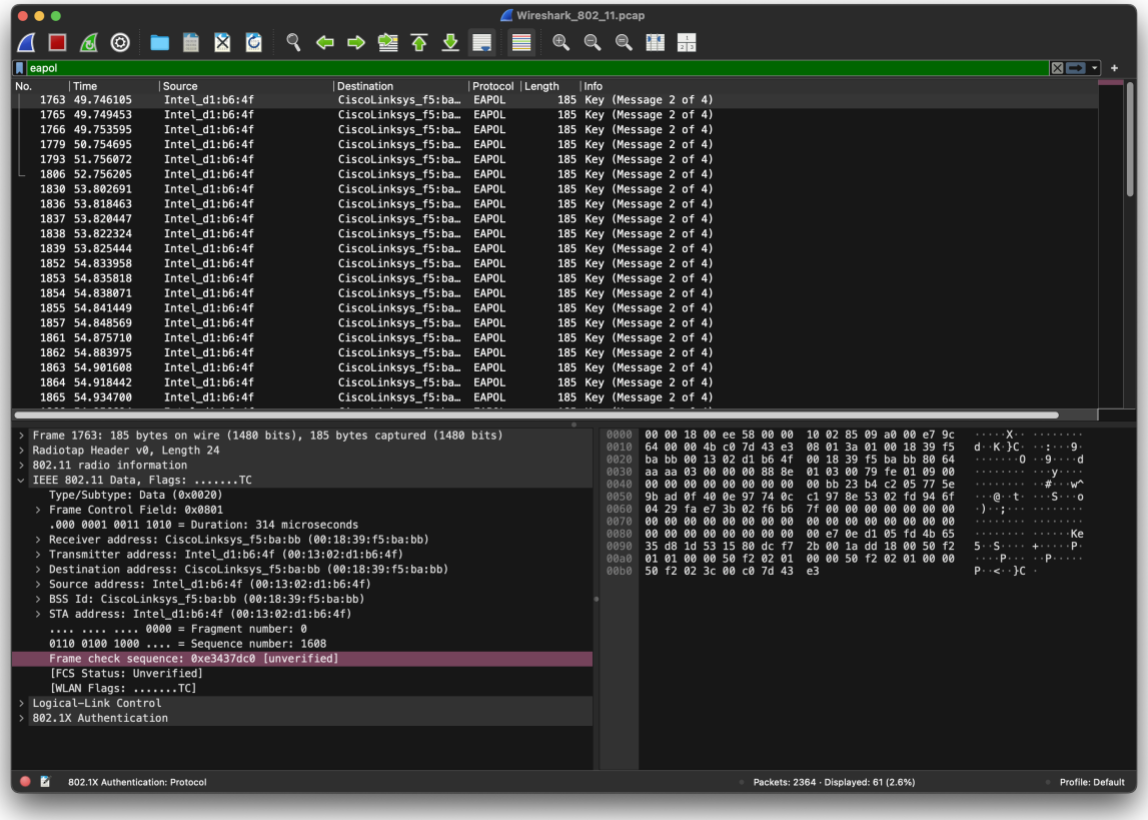


In this capture, we observe an Address Resolution Protocol (ARP) request, which is used to map an IP address to a MAC address within the local network. The highlighted packet shows a host (CnetTechno_73:8d:ce) broadcasting a query asking, *"Who has 192.168.1.103? Tell 192.168.1.100."* The source is the sender's MAC address, and the destination is the broadcast address (ff:ff:ff:ff:ff:ff), ensuring that every device on the subnet receives the request. These packets are relatively small, here only 106 bytes, and they always follow a clear pattern: ARP requests are broadcast to all, while ARP replies are unicast back to the requester. This behavior contrasts with beacon or ACK frames, as ARP operates to resolve addressing for upper-layer IP traffic, acting as a vital handshake between the data link and network layers.

EAPOL

Juan Dominguez
Salissa Hernandez
Noah Nyabadza

Assignment 2



In this capture, we observe an EAPOL (Extensible Authentication Protocol over LAN) frame, specifically part of the WPA/WPA2 four-way handshake used for authentication and key exchange when a client joins the wireless network. The source address is the client device (Intel_d1:b6:4f), and the destination address is the access point (CiscoLinksys_f5:ba:bb), showing direct unicast communication between the two. Each EAPOL packet is relatively small here, 185 bytes and is identified as a numbered step in the handshake sequence (e.g., *Message 2 of 4*). Unlike beacons or ARP, these frames appear only during the connection setup phase rather than continuously. This highlights their role in establishing encryption keys and securing the link at the data link layer before higher-level protocols such as IP can be used.

9. Separate file

10. Separate file

Juan Dominguez
Salissa Hernandez
Noah Nyabadza

Assignment 2

11. **Point-to-Point Protocol (PPP)** is a data link layer protocol used to set up a direct connection between two nodes. PPP is very common for internet connections and linking networks over a WAN. PPP is pretty flexible and can work with various physical layer protocols like serial lines and DSL.

    Specify which functionalities are common and which are different between PPP and protocol 6: Selective Repeat that we studied in class.

    PPP and Selective Repeat are distinct data link layer protocols with different primary functions. PPP is a comprehensive protocol for managing a point-to-point link, while Selective Repeat is a specific algorithm for efficient flow and error control.

    Common Functionalities

    Both protocols are fundamental to reliable data transfer at the data link layer.

    - **Error Detection**: Both PPP and Selective Repeat are concerned with data integrity. They use mechanisms like **checksums** or **Cyclic Redundancy Checks (CRC)** to detect corrupted frames during transmission. PPP's frame trailer contains an FCS (Frame Check Sequence) for this purpose, and Selective Repeat similarly uses error detection to identify frames that need retransmission.

    - **Flow Control**: Both protocols manage data flow to prevent the sender from overwhelming the receiver. However, they handle this differently, which highlights their distinct purposes. PPP's flow control is simpler, often relying on higher-layer protocols like TCP, whereas Selective Repeat has a complex, built-in windowing mechanism.

    Different Functionalities

    The key difference lies in their scope. PPP is a broader protocol suite for link establishment, while Selective Repeat is a focused ARQ (Automatic Repeat Request) algorithm for efficient error recovery.

    - **Primary Purpose**:

        - **PPP**: Its main function is to **establish, configure, and manage** a direct connection between two devices. It's a suite of three protocols—LCP, AP,

and NCP—that handle everything from link negotiation and authentication to multiplexing different network protocols.

  - **Selective Repeat**: This is a specific **error recovery and retransmission** algorithm. Its sole purpose is to efficiently handle packet loss. Instead of retransmitting all subsequent packets after a single lost one (like Go-Back-N), it only retransmits the frames that were actually lost or corrupted.

- **Error Handling and Retransmission**:

  - **PPP**: PPP's error handling is primarily about **detection and link quality monitoring**. It detects errors using the FCS field but typically relies on higher-layer protocols (like TCP) for the actual retransmission and error correction logic. It is not an ARQ protocol.

  - **Selective Repeat**: This protocol is all about **retransmission efficiency**. It uses a sliding window and sequence numbers on both the sender and receiver. The receiver can accept and buffer out-of-order frames, and the sender maintains a timer for each packet, retransmitting only the specific packets for which it has not received an acknowledgment.

- **Complexity and Components**:

  - **PPP**: PPP is a modular protocol with separate components for different functions (LCP for link management, AP for security, NCP for network layer negotiation). This makes it highly flexible.

  - **Selective Repeat**: This is a complex flow control mechanism. The receiver requires a buffer to store out-of-order packets, and the sender must manage a timer for each individual packet, making it more intricate to implement than simpler ARQ protocols.