Task 10.1p

Module 10 Physical Layer and Connection Module.
Active class 10: Physical Connections and Protocols

Activity 1: Website Visit - Unveiling the Steps

Imagine you power on your laptop and want to visit a website. Your laptop initiates a conversation with your Wi-Fi network, like asking a phonebook (DNS) for the website's address. Depending on your setup, your network might consult the internet service provider (ISP) for further assistance. Once the address is found, your laptop politely requests the website's data using a protocol called HTTP. The website responds with the information you requested (text, images) using the same protocol. Finally, your laptop displays the website on your screen! If your network uses NAT (Network Address Translation), it acts like a middleman, changing your laptop's unique address to a public one for the internet.

Activity 2: Wireshark - Capturing the Website Conversation

Remember exploring the website visit process? This activity lets us see the actual conversation! We'll first clear any old website information stored on your laptop and network. Then, with a tool called Wireshark capturing everything, you'll visit a new website. We'll analyze the captured messages to understand the order in which protocols like DNS and HTTP work, what each one does, and the details of each message. Finally, we'll compare these findings with what we learned in Activity 1 to see if the messages match the website visit process.

Activity 3: Wired vs. Wireless Networks - Understanding Traffic Flow

This activity lets you play with a network simulation to compare wired and wireless connections. We'll send data packets from one computer to another, both using wires and Wi-Fi. We'll then analyze how these data packets (PDUs) travel in each case. While wired connections might only show the source and destination device's MAC addresses, wireless connections might show three. We'll explore why there are three MAC addresses involved in wireless communication - because the data travels through multiple devices like routers and access points before reaching its destination, unlike wired connections where it goes directly from one device to another.

Notes

Wireless vs. Wired Networks:

Prevalence of Wireless: The module highlights the dominance of wireless technologies. There are more wireless phone subscribers and mobile-broadband-connected devices than wired counterparts.

Challenges of Wireless: Wireless communication faces issues like signal degradation over distance, interference from other devices, and obstacles that can weaken signals. Additionally, managing mobility adds complexity compared to fixed wired connections.

Characteristics of Wireless Links:

Comparison of Technologies: The module provides a detailed comparison of popular wireless technologies. This includes their data rates (speed of data transfer), ranges (effective coverage area), and applications.

Examples include:

Wi-Fi (IEEE 802.11 Standards): Focus on different versions like 802.11ax (WiFi 6), 802.11ac, and earlier versions, noting their data rate improvements and range variations.

Cellular Networks (4G/5G): Explore their high data rates and wide coverage areas suitable for mobile internet access.

Bluetooth: Discuss its lower data rate but suitability for short-range connections between devices.

Elements of a Wireless Network:

Components: A wireless network consists of several key elements:

Wireless Hosts: These are the devices that connect to the network wirelessly, such as laptops, smartphones, tablets, and Internet of Things (IoT) devices.

Base Stations: These act as central points for communication in a wireless network. Examples include Wi-Fi routers, cellular towers, and access points.

Wireless Links: These are the invisible connections that carry data between wireless hosts and base stations using radio waves.

Wireless LAN (WLAN):

IEEE 802.11 Standards: This section dives deeper into the evolution of Wi-Fi technologies as defined by the IEEE 802.11 standards. Understand the progression from 802.11b (released in 1999) to the latest 802.11ax (WiFi 6) with improvements in speed, range, and capacity.

CSMA/CA for Access Control: The module explains how Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is used in Wi-Fi to manage access to the shared wireless medium and prevent data collisions.

4G/5G and 6G Cellular Networks:

Deployment and Usage: Explore the widespread adoption of 4G and 5G cellular networks. Understand their technical specifications, like frequency bands used and modulation techniques employed.

Similarities and Differences with Wired Internet: While cellular networks provide similar internet access as wired connections, they differ in terms of mobility, range, and potentially, data transfer speeds depending on the technology.

6G - A Glimpse into the Future: The notes can mention the ongoing development of 6G cellular networks, promising even faster data rates and potentially new applications.

TCP/IP Protocol Stack:

Layers and Functions: This section provides a more detailed explanation of each layer in the TCP/IP protocol stack and its role in data communication:

Application Layer: Defines protocols for applications like web browsing, email, and file transfer.

Transport Layer: Handles reliable data delivery between applications on different devices. (e.g., TCP for reliable data transfer, UDP for connectionless data transfer)

Network Layer: Routes data packets across networks based on logical IP addresses.

Data Link Layer (DLL) - Focus Area: We will delve deeper into this layer in the next section.

Physical Layer: Deals with the physical transmission of data bits over the network medium (e.g., cables, radio waves).

Data Link Layer (DLL):

Sub-layers:

The DLL consists of two sub-layers:

Logical Link Control (LLC): This sub-layer is responsible for multiplexing data streams from different applications into a single data stream for the MAC sub-layer. It also provides error detection, flow control, and acknowledgment mechanisms to ensure reliable communication between devices.

Media Access Control (MAC): This sub-layer manages access to the physical transmission medium. It handles addressing devices using Media Access Control (MAC) addresses, which are unique identifiers for network interfaces. It also employs techniques to avoid collisions between data transmissions from multiple devices.

Importance of the Data Link Layer:

Reliable Communication: The DLL plays a crucial role in ensuring reliable data communication within a network. It achieves this through:

Framing: Dividing data packets from the Network layer into smaller frames with headers and trailers

Some external resources I referred to

1. *What is a wireless network? Types of wireless network | Fortinet*. (n.d.). Fortinet.

   https://www.fortinet.com/resources/cyberglossary/wireless-network

2. *What Is a Wireless Network? - Wired vs Wireless*. (2021, July 1). Cisco.

   https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/wireless-network.html

3. Shukla, G. (2023, February 12). *What is Wi-Fi, and how does it work?* How-To Geek.

   https://www.howtogeek.com/865706/what-is-wi-fi/

Wi-Fi generation	IEEE standard	Adopted	Maximum link rate
Wi-Fi 0*	802.11 or 802.11-1997	1997	1-2Mbps
Wi-Fi 1*	802.11b	1999	1-11Mbps
Wi-Fi 2*	802.11a	1999	6-54Mbps
Wi-Fi 3*	802.11g	2003	6-54Mbps
Wi-Fi 4	802.11n	2008	72-600Mbps
Wi-Fi 5	**802.11ac**	2014	433-6933Mbps
Wi-Fi 6/ **Wi-Fi 6E**	802.11ax	2019/ 2020	574-9608Mbps
Wi-Fi 7	802.11be	(2024)	1376-46120Mbps
* Unofficial name			

Quiz 7

Module 7: Physical Layer and Connections

Total points 100/100

The respondent's email (**rnirosh134@cicracampus.net**) was recorded on submission of this form.

Ethernet over copper twisted-pair technologies use cables as the physical medium. There are different standards we use in computer networks. Compare the frame structures for 10BASE-T, 100BASE-T, and Gigabit Ethernet. How do they differ from one to another? 10/10

- Gigabit Ethernet supports a larger frame structure compared to 10BASE-T and 100BASE-T.
- Frame lengths of 10BASE-T > 100BASE-T > Gigabit Ethernet
- Frame lengths of 10BASE-T < 100BASE-T < Gigabit Ethernet
- **All three Ethernet technologies have identical frame structures** ✓

WiFi's media access control and physical layer protocols for implementing wireless local area network (WLAN) are defined by 10/10

- IEEE 802.4 standard
- **IEEE 802.11 standard** ✓
- IEEE 802.10 standard
- IEEE 802.3 standard

Which of the following statement is false? 10/10

- ○ WiFi link layer frames have enough fields to indicate more than two MAC addresses.
- ○ Ethernet frames indicate only two MAC addresses (source and destination).
- ○ Ethernet frames can have broadcast MAC address in the destination MAC address field.
- ◉ WiFi link layer frames always have two MAC addresses (source and destination). ✓

Which of the following statement are true regarding Hub, Switch and Router? 10/10

- [ ] Routers operates only on link-layer and can forward packets.
- [x] Hub has a single broadcast domain and anything comes in one port is sent out to all the other ports. ✓
- [x] Switch can filter and forward packets between different LAN segments connected to it as it can process at least up to the ink layer. ✓
- [ ] Operations of the routers and switches are very similar.

Assume that there are two WiFi networks associated with two WiFi APs belong to two different ISPs in a particular restaurant and apparently each of these APs are operating over the same WiFi channel. Which of the following statements are true regarding this scenario ? 10/10

- [x] Hosts will be able to connect to one network as each AP has a different SSID and unique MAC address. ✓
- [x] The frames send by a host connected to one AP will be received by both APs. ✓
- [ ] There will be no interference and both networks will work smoothly
- [ ] There would be a complete breakdown and none of the hosts would be able to connect.

One of the main functionalities of the physical layer is — 10/10

- (selected, correct) data must be converted into signals (with proper format) to be transmitted over channels.
- responsible for admission control
- connecting devices over only guided medium.
- responsible for multiple access control.

When your wireless device connects to a WiFi network, what would be the first networking protocol that your device runs from the given list? — 10/10

- HTTP
- (selected, correct) DHCP
- NAT
- DNS

Let's assume that you suddenly want to switch on your laptop in the middle of the night and you want to log in to unit site to check a quiz. What are the protocols that involved in the entire process from the start to end? — 10/10

- DHCP, HTTP, TCP, DNS
- (selected, correct) None of the answers are correct
- TCP, HTTP, DNS and UDP
- TCP and HTTP

Which of the following statement is correct regarding 4G and 5G networks? 10/10

- 4G and 5G are standardised by IEEE.
- 5G is the latest mobile network technology which can support data rates beyond 100 Gbps.
- They have the same protocols in all five layers as the wired network.
- Application, transport, and network layers run similar protocols as in the wired network. However, the data-link and physical layer implementations are different compared to wired network.

What are the two different frequency bands used in IEEE 802.11 networks? 10/10

- 5 GHz and 6.4 GHz
- 2.4 GHz and 5 GHz
- 2.4 GHz and 3.2 GHz
- 2.6 GHz and 5 GHz

Activity 1: Website Visit - Unveiling the Steps

Imagine you're trying to visit your friend's house (the website) on the internet.

Wake Up (Boot Up): You wake up (turn on your laptop) and get ready (startup routine).

Call a Friend (Router): You call your friend who lives closest to the internet (router) to ask for directions (connect to Wi-Fi).

Look Up Address (DNS): You look up your friend's address in a phone book (DNS) to get the exact location (IP address).

Send a Message (TCP): You send a reliable message (request) to your friend, asking if you can visit (website).

Follow the Signs (IP): Your message travels on the main roads (internet) using signs (IP) to find your friend's house.

Friend Invites You (Response): Your friend (server) agrees and sends you directions (website data).

Understand the Directions (HTTP): You translate the directions (website code) into something you understand.

Finally, There! (Website Display): You arrive at your friend's house (website is displayed)!

Bonus: With a translator (NAT): If your neighborhood has a translator (NAT router), they translate your home address (private IP) to a public address for the internet, then translate it back when your friend replies.

When I first power on my laptop and decide to access the SIT202 CloudDeakin site, here's what happens:

Step 1:

My laptop Powers on and Network Connection Initializes, and the network interface card (NIC) initializes.

DHCP (Dynamic Host Configuration Protocol) - My laptop sends a DHCPDISCOVER message to find a DHCP server and obtain an IP address. The server responds with a DHCPOFFER, and my laptop accepts it with a DHCPREQUEST. Finally, the server confirms with a DHCPACK.

This step assigns an IP address to my laptop, which is essential for network communication.

Step 2

After obtaining an IP address, my laptop needs to communicate with the local network, so it needs to know the MAC address of the default gateway (router).

ARP (Address Resolution Protocol) - My laptop sends an ARP request to ask "Who has the IP address of the default gateway?" The router responds with an ARP reply containing its MAC address.

ARP resolves IP addresses to MAC addresses, enabling my laptop to communicate with devices on the local network.

Step 3:

I open my browser and enter the URL (https://d2l.deakin.edu.au). My laptop needs to convert this URL into an IP address.

DNS (Domain Name System) - My laptop sends a DNS query to the configured DNS server to resolve the domain name into an IP address.

DNS translates human-readable URLs into IP addresses that computers can understand.

Step 4:

With the IP address obtained, my laptop initiates a TCP connection to the CloudDeakin server.

TCP (Transmission Control Protocol) - My laptop sends a SYN packet to the server, which responds with a SYN-ACK. My laptop then sends an ACK to establish the connection.

TCP ensures a reliable connection through a handshake process, enabling reliable data transmission.

Step 5:

My laptop sends an HTTP GET request to the server to fetch the webpage.

HTTP (Hypertext Transfer Protocol) - This protocol governs the request and delivery of web content.

HTTP facilitates the transfer of web resources from the server to my browser.

Step 6:

The server processes the request and sends back the webpage data.

The server uses these **TCP (for data transport) and HTTP (for web content)** to send the data back to my laptop.

TCP ensures the data is received correctly, and HTTP provides the web content.

3.

With **NAT**, my laptop would have a private IP address. The router would translate this private address to a public IP for internet communication. The steps remain the same, but the NAT device would modify the IP headers to ensure correct routing.

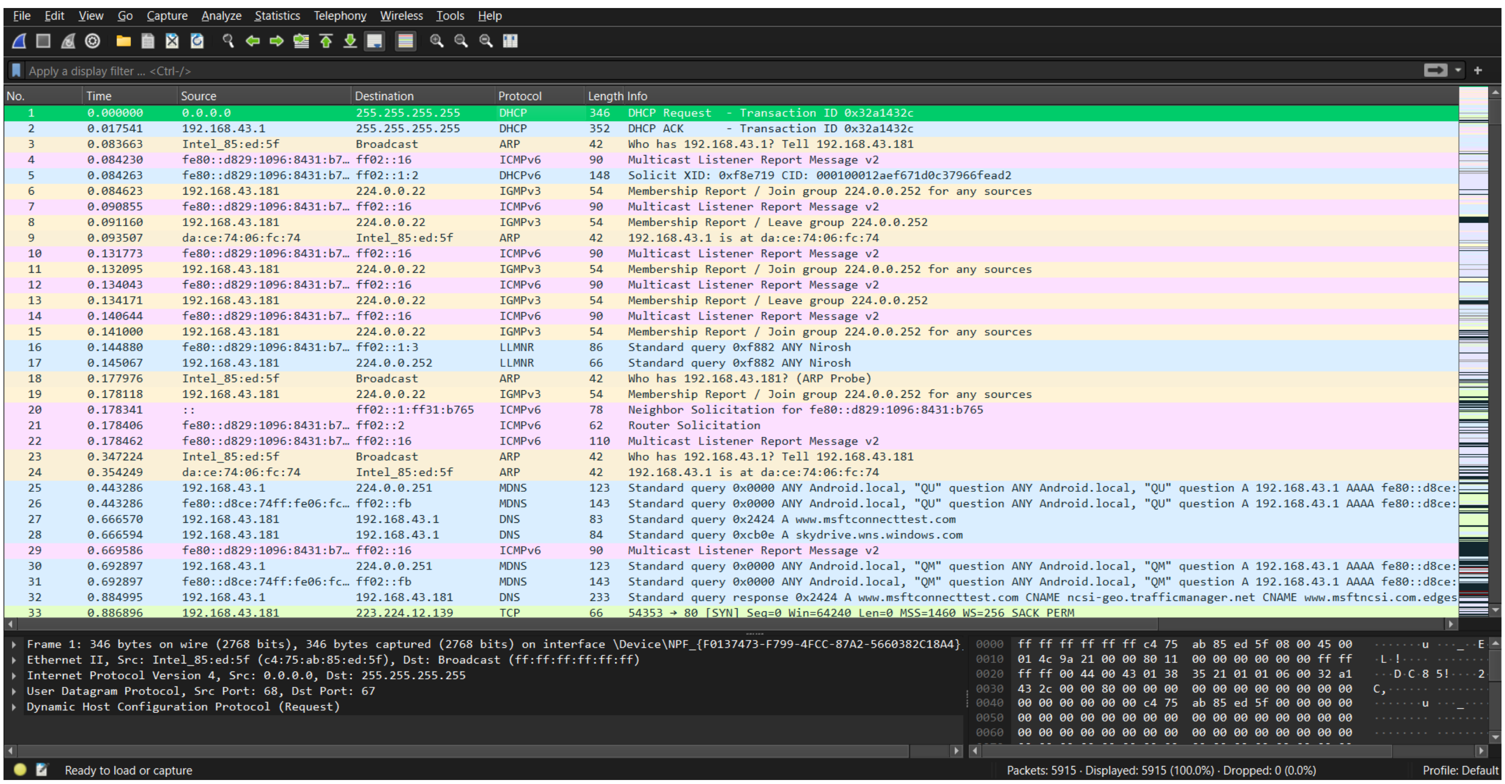
Activity 2: Wireshark - Capturing the Website Conversation

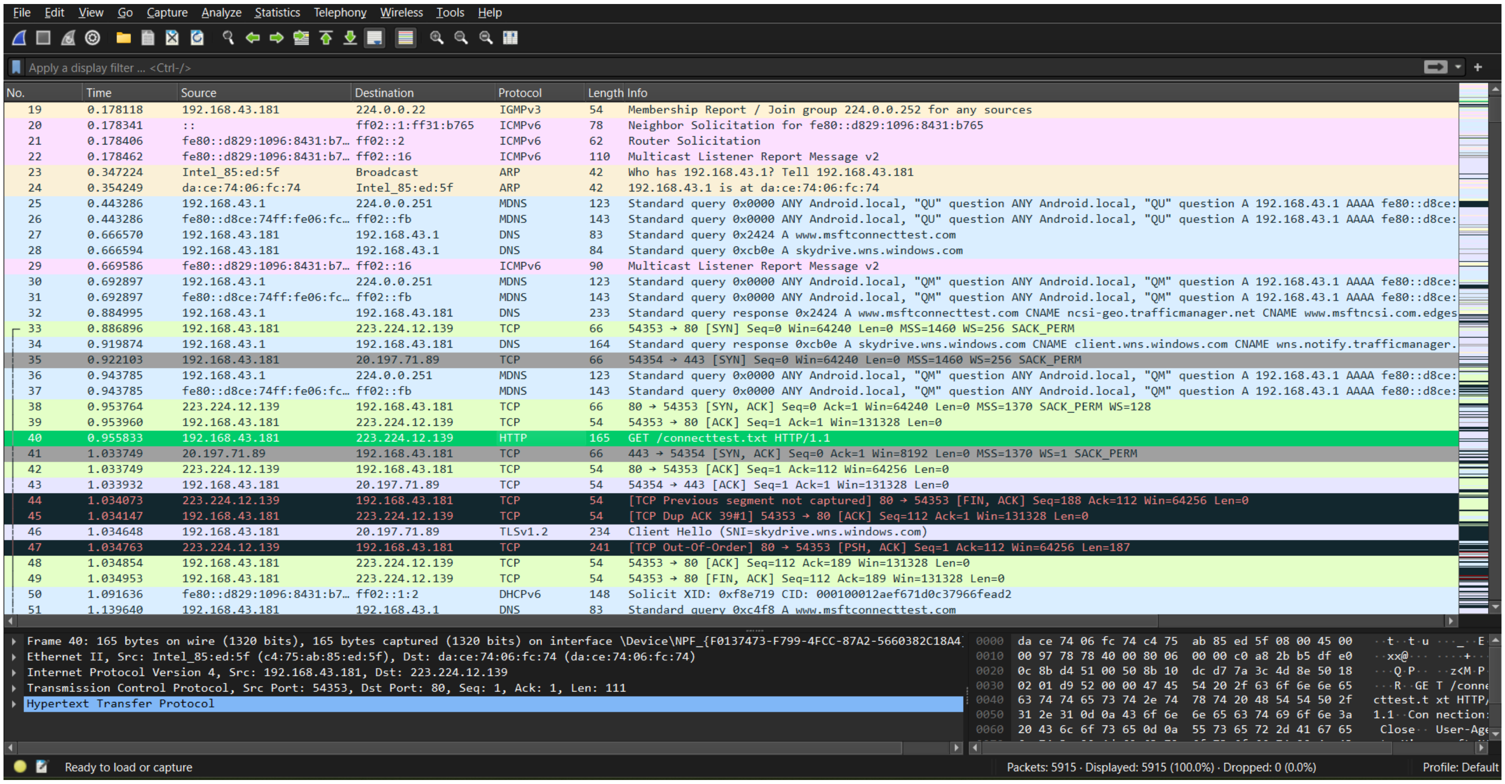
Alright,

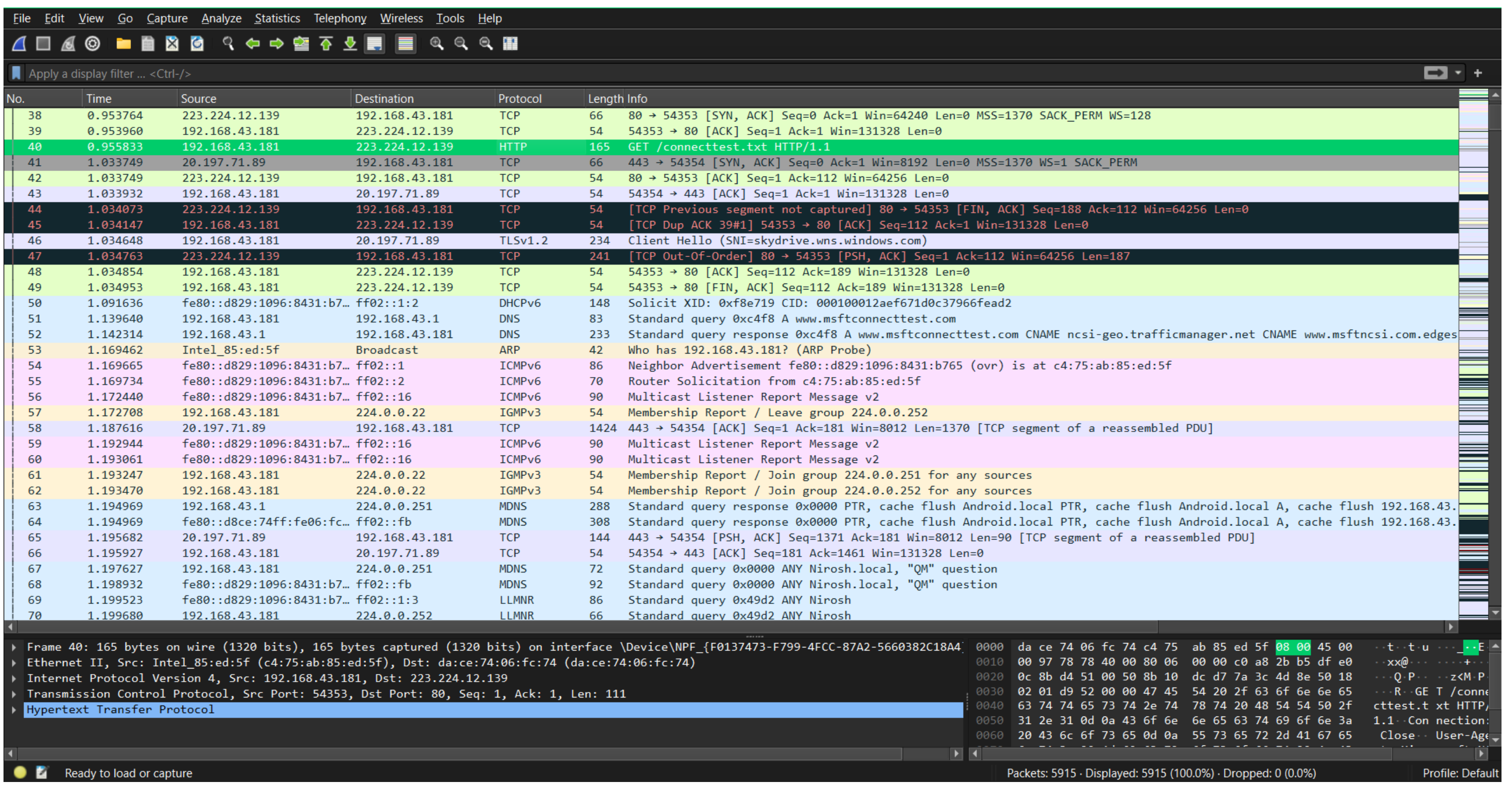
It's time to use Wireshark to see what happens behind the scenes when I visit a website! First, I gotta clean up my browsing history and make sure Wireshark has a fresh slate to work with. Then, I'll completely disconnect from the internet for a second. Now comes the cool part - I'll open Wireshark, which is like a tool that listens to all the conversations happening on my network. With Wireshark ready, I'll reconnect to the internet. Now, I can visit the website http://www.discoverourtown.com/ and tell Wireshark to stop listening. It's like capturing a snapshot of all the messages flying around while I visited the site.

The next step is like detective work! I'll use Wireshark to analyze these messages, figure out the order they happened in, and what each message said. Then, I'll need to understand what each message is for - some might be about finding the website's address, others about transferring the actual website data. To make things clear, I'll even take screenshots of important details. Finally, I'll compare what I learned from Wireshark with what I already knew about how websites work. This should help me become a real pro at understanding all the secret messages that make the internet work!

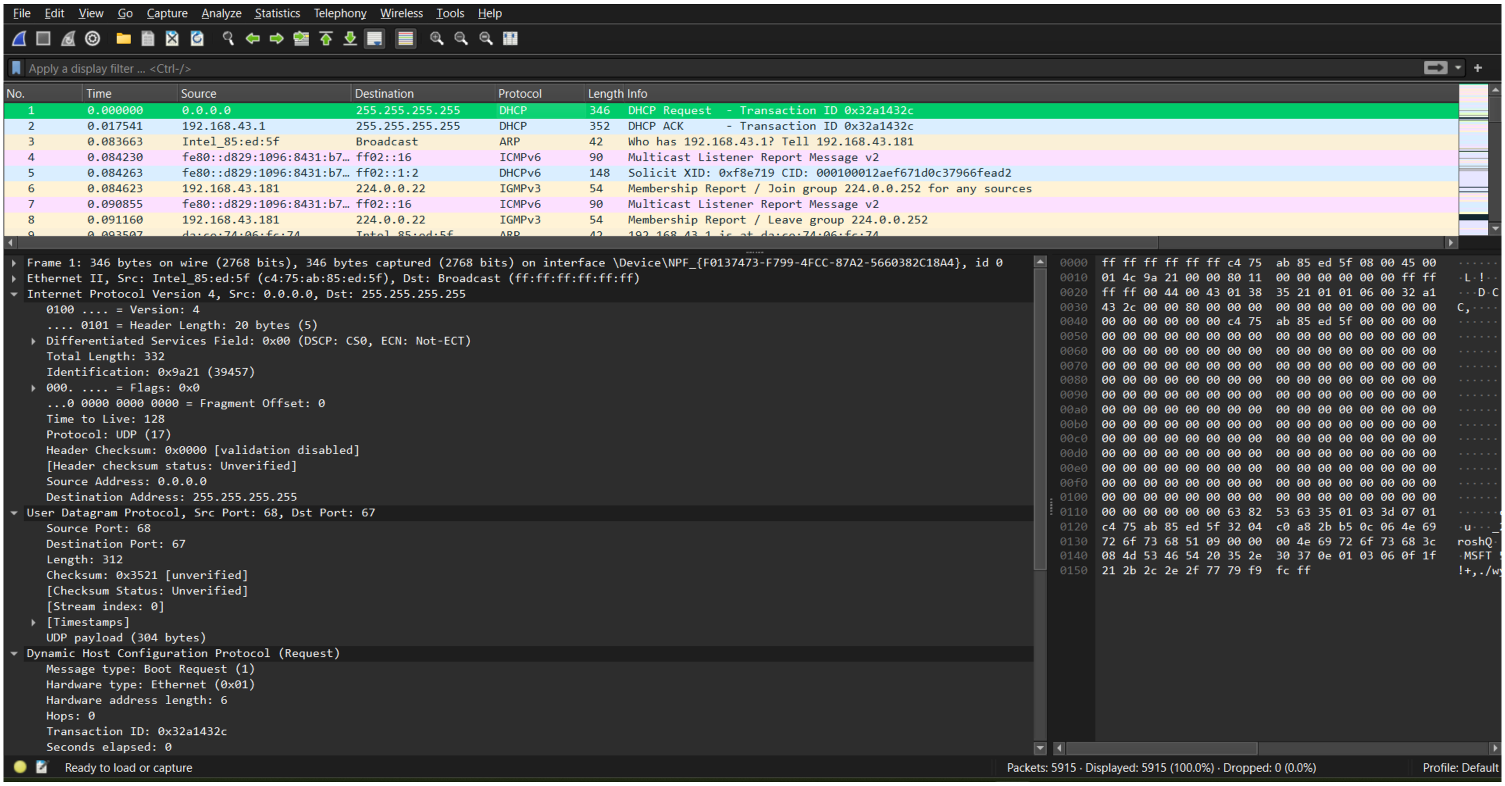
The whole capture

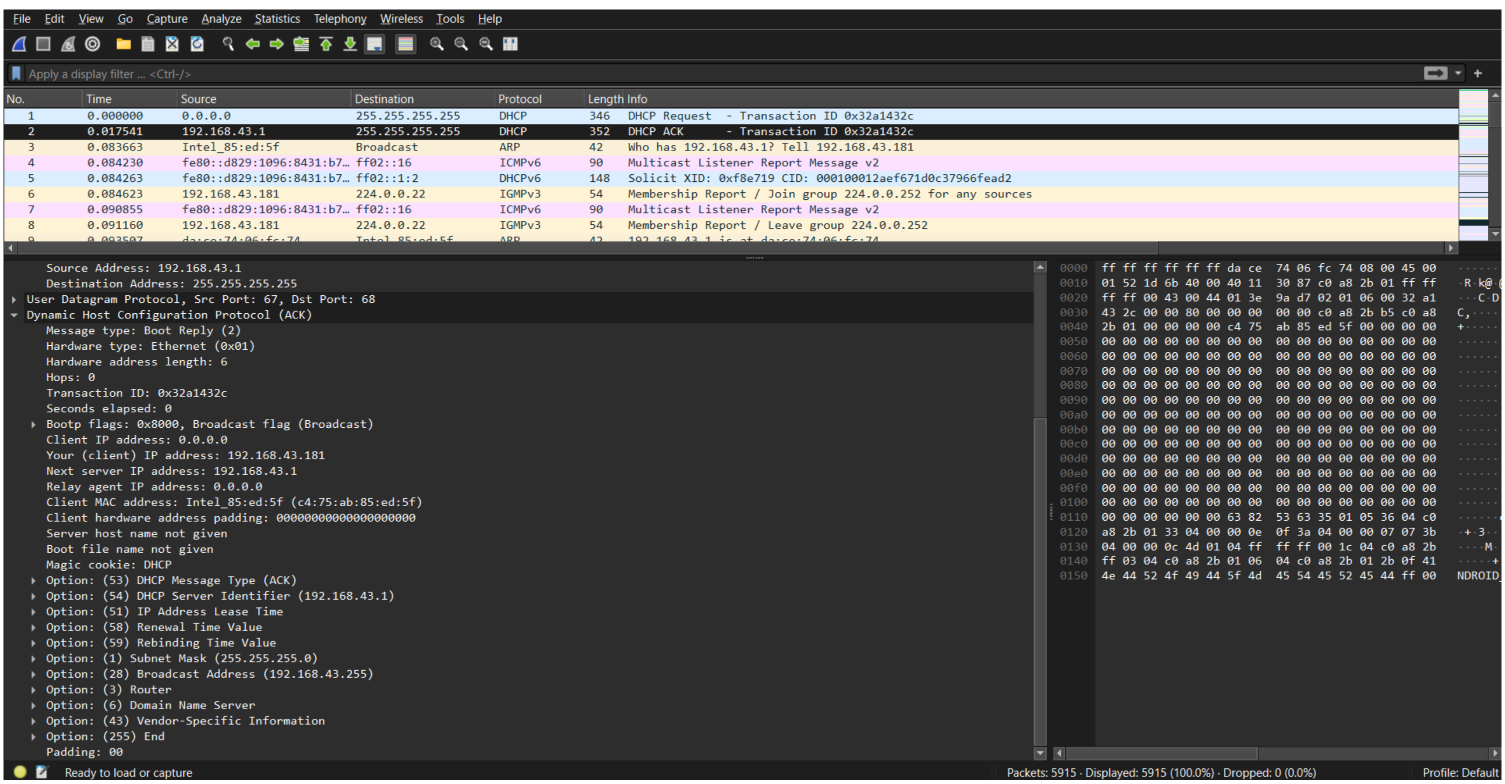



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
19 0.178118 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Join group 224.0.0.252 for any sources
20 0.178341 :: ff02::1:ff31:b765 ICMPv6 78 Neighbor Solicitation for fe80::d829:1096:8431:b765
21 0.178406 fe80::d829:1096:8431:b7… ff02::2 ICMPv6 62 Router Solicitation
22 0.178462 fe80::d829:1096:8431:b7… ff02::16 ICMPv6 110 Multicast Listener Report Message v2
23 0.347224 Intel_85:ed:5f Broadcast ARP 42 Who has 192.168.43.1? Tell 192.168.43.181
24 0.354249 da:ce:74:06:fc:74 Intel_85:ed:5f ARP 42 192.168.43.1 is at da:ce:74:06:fc:74
25 0.443286 192.168.43.1 224.0.0.251 MDNS 123 Standard query 0x0000 ANY Android.local, "QU" question ANY Android.local, "QU" question A 192.168.43.1 AAAA fe80::d8ce:
26 0.443286 fe80::d8ce:74ff:fe06:fc… ff02::fb MDNS 143 Standard query 0x0000 ANY Android.local, "QU" question ANY Android.local, "QU" question A 192.168.43.1 AAAA fe80::d8ce:
27 0.666570 192.168.43.181 192.168.43.1 DNS 83 Standard query 0x2424 A www.msftconnecttest.com
28 0.666594 192.168.43.181 192.168.43.1 DNS 84 Standard query 0xcb0e A skydrive.wns.windows.com
29 0.669586 fe80::d829:1096:8431:b7… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
30 0.692897 192.168.43.1 224.0.0.251 MDNS 123 Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 192.168.43.1 AAAA fe80::d8ce:
31 0.692897 fe80::d8ce:74ff:fe06:fc… ff02::fb MDNS 143 Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 192.168.43.1 AAAA fe80::d8ce:
32 0.884995 192.168.43.1 192.168.43.181 DNS 233 Standard query response 0x2424 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edges
33 0.886896 192.168.43.181 223.224.12.139 TCP 66 54353 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
34 0.919874 192.168.43.1 192.168.43.181 DNS 164 Standard query response 0xcb0e A skydrive.wns.windows.com CNAME client.wns.windows.com CNAME wns.notify.trafficmanager.
35 0.922103 192.168.43.181 20.197.71.89 TCP 66 54354 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
36 0.943785 192.168.43.1 224.0.0.251 MDNS 123 Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 192.168.43.1 AAAA fe80::d8ce:
37 0.943785 fe80::d8ce:74ff:fe06:fc… ff02::fb MDNS 143 Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 192.168.43.1 AAAA fe80::d8ce:
38 0.953764 223.224.12.139 192.168.43.181 TCP 66 80 → 54353 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1370 SACK_PERM WS=128
39 0.953960 192.168.43.181 223.224.12.139 TCP 54 54353 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
40 0.955833 192.168.43.181 223.224.12.139 HTTP 165 GET /connecttest.txt HTTP/1.1
41 1.033749 20.197.71.89 192.168.43.181 TCP 66 443 → 54354 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1370 WS=1 SACK_PERM
42 1.033749 223.224.12.139 192.168.43.181 TCP 54 80 → 54353 [ACK] Seq=1 Ack=112 Win=64256 Len=0
43 1.033932 192.168.43.181 20.197.71.89 TCP 54 54354 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
44 1.034073 223.224.12.139 192.168.43.181 TCP 54 [TCP Previous segment not captured] 80 → 54353 [FIN, ACK] Seq=188 Ack=112 Win=64256 Len=0
45 1.034147 192.168.43.181 223.224.12.139 TCP 54 [TCP Dup ACK 39#1] 54353 → 80 [ACK] Seq=112 Ack=1 Win=131328 Len=0
46 1.034648 192.168.43.181 20.197.71.89 TLSv1.2 234 Client Hello (SNI=skydrive.wns.windows.com)
47 1.034763 223.224.12.139 192.168.43.181 TCP 241 [TCP Out-Of-Order] 80 → 54353 [PSH, ACK] Seq=1 Ack=112 Win=64256 Len=187
48 1.034854 192.168.43.181 223.224.12.139 TCP 54 54353 → 80 [ACK] Seq=112 Ack=189 Win=131328 Len=0
49 1.034953 192.168.43.181 223.224.12.139 TCP 54 54353 → 80 [FIN, ACK] Seq=112 Ack=189 Win=131328 Len=0
50 1.091636 fe80::d829:1096:8431:b7… ff02::1:2 DHCPv6 148 Solicit XID: 0xf8e719 CID: 000100012aef671d0c37966fead2
51 1.139640 192.168.43.181 192.168.43.1 DNS 83 Standard query 0xc4f8 A www.msftconnecttest.com
Frame 40: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface \Device\NPF_{F0137473-F799-4FCC-87A2-5660382C18A4
Ethernet II, Src: Intel_85:ed:5f (c4:75:ab:85:ed:5f), Dst: da:ce:74:06:fc:74 (da:ce:74:06:fc:74)
Internet Protocol Version 4, Src: 192.168.43.181, Dst: 223.224.12.139
Transmission Control Protocol, Src Port: 54353, Dst Port: 80, Seq: 1, Ack: 1, Len: 111
Hypertext Transfer Protocol
0000 da ce 74 06 fc 74 c4 75 ab 85 ed 5f 08 00 45 00
0010 00 97 78 78 40 00 80 06 00 00 c0 a8 2b b5 df e0
0020 0c 8b d4 51 00 50 8b 10 dc d7 7a 3c 4d 8e 50 18
0030 02 01 d9 52 00 00 47 45 54 20 2f 63 6f 6e 6e 65
0040 63 74 74 65 73 74 2e 74 78 74 20 48 54 54 50 2f
0050 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a
0060 20 43 6c 6f 73 65 0d 0a 55 73 65 72 2d 41 67 65
Ready to load or capture
Packets: 5915 · Displayed: 5915 (100.0%) · Dropped: 0 (0.0%)
Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
38 0.953764 223.224.12.139 192.168.43.181 TCP 66 80 → 54353 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1370 SACK_PERM WS=128
39 0.953960 192.168.43.181 223.224.12.139 TCP 54 54353 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
40 0.955833 192.168.43.181 223.224.12.139 HTTP 165 GET /connecttest.txt HTTP/1.1
41 1.033749 20.197.71.89 192.168.43.181 TCP 66 443 → 54354 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1370 WS=1 SACK_PERM
42 1.033749 223.224.12.139 192.168.43.181 TCP 54 80 → 54353 [ACK] Seq=1 Ack=112 Win=64256 Len=0
43 1.033932 192.168.43.181 20.197.71.89 TCP 54 54354 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
44 1.034073 223.224.12.139 192.168.43.181 TCP 54 [TCP Previous segment not captured] 80 → 54353 [FIN, ACK] Seq=188 Ack=112 Win=64256 Len=0
45 1.034147 192.168.43.181 223.224.12.139 TCP 54 [TCP Dup ACK 39#1] 54353 → 80 [ACK] Seq=112 Ack=1 Win=131328 Len=0
46 1.034648 192.168.43.181 20.197.71.89 TLSv1.2 234 Client Hello (SNI=skydrive.wns.windows.com)
47 1.034763 223.224.12.139 192.168.43.181 TCP 241 [TCP Out-Of-Order] 80 → 54353 [PSH, ACK] Seq=1 Ack=112 Win=64256 Len=187
48 1.034854 192.168.43.181 223.224.12.139 TCP 54 54353 → 80 [ACK] Seq=112 Ack=189 Win=131328 Len=0
49 1.034953 192.168.43.181 223.224.12.139 TCP 54 54353 → 80 [FIN, ACK] Seq=112 Ack=189 Win=131328 Len=0
50 1.091636 fe80::d829:1096:8431:b7… ff02::1:2 DHCPv6 148 Solicit XID: 0xf8e719 CID: 000100012aef671d0c37966fead2
51 1.139640 192.168.43.181 192.168.43.1 DNS 83 Standard query 0xc4f8 A www.msftconnecttest.com
52 1.142314 192.168.43.1 192.168.43.181 DNS 233 Standard query response 0xc4f8 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edges
53 1.169462 Intel_85:ed:5f Broadcast ARP 42 Who has 192.168.43.181? (ARP Probe)
54 1.169665 fe80::d829:1096:8431:b7… ff02::1 ICMPv6 86 Neighbor Advertisement fe80::d829:1096:8431:b765 (ovr) is at c4:75:ab:85:ed:5f
55 1.169734 fe80::d829:1096:8431:b7… ff02::2 ICMPv6 70 Router Solicitation from c4:75:ab:85:ed:5f
56 1.172440 fe80::d829:1096:8431:b7… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
57 1.172708 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Leave group 224.0.0.252
58 1.187616 20.197.71.89 192.168.43.181 TCP 1424 443 → 54354 [ACK] Seq=1 Ack=181 Win=8012 Len=1370 [TCP segment of a reassembled PDU]
59 1.192944 fe80::d829:1096:8431:b7… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
60 1.193061 fe80::d829:1096:8431:b7… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
61 1.193247 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Join group 224.0.0.251 for any sources
62 1.193470 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Join group 224.0.0.252 for any sources
63 1.194969 192.168.43.1 224.0.0.251 MDNS 288 Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local A, cache flush 192.168.43.
64 1.194969 fe80::d8ce:74ff:fe06:fc… ff02::fb MDNS 308 Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local A, cache flush 192.168.43.
65 1.195682 20.197.71.89 192.168.43.181 TCP 144 443 → 54354 [PSH, ACK] Seq=1371 Ack=181 Win=8012 Len=90 [TCP segment of a reassembled PDU]
66 1.195927 192.168.43.181 20.197.71.89 TCP 54 54354 → 443 [ACK] Seq=181 Ack=1461 Win=131328 Len=0
67 1.197627 192.168.43.181 224.0.0.251 MDNS 72 Standard query 0x0000 ANY Nirosh.local, "QM" question
68 1.198932 fe80::d829:1096:8431:b7… ff02::fb MDNS 92 Standard query 0x0000 ANY Nirosh.local, "QM" question
69 1.199523 fe80::d829:1096:8431:b7… ff02::1:3 LLMNR 86 Standard query 0x49d2 ANY Nirosh
70 1.199680 192.168.43.181 224.0.0.252 LLMNR 66 Standard query 0x49d2 ANY Nirosh
Frame 40: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface \Device\NPF_{F0137473-F799-4FCC-87A2-5660382C18A4
Ethernet II, Src: Intel_85:ed:5f (c4:75:ab:85:ed:5f), Dst: da:ce:74:06:fc:74 (da:ce:74:06:fc:74)
Internet Protocol Version 4, Src: 192.168.43.181, Dst: 223.224.12.139
Transmission Control Protocol, Src Port: 54353, Dst Port: 80, Seq: 1, Ack: 1, Len: 111
Hypertext Transfer Protocol
0000 da ce 74 06 fc 74 c4 75 ab 85 ed 5f 08 00 45 00
0010 00 97 78 78 40 00 80 06 00 00 c0 a8 2b b5 df e0
0020 0c 8b d4 51 00 50 8b 10 dc d7 7a 3c 4d 8e 50 18
0030 02 01 d9 52 00 00 47 45 54 20 2f 63 6f 6e 6e 65
0040 63 74 74 65 73 74 2e 74 78 74 20 48 54 54 50 2f
0050 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a
0060 20 43 6c 6f 73 65 0d 0a 55 73 65 72 2d 41 67 65
Ready to load or capture
Packets: 5915 · Displayed: 5915 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

Step 1


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 0.0.0.0 255.255.255.255 DHCP 346 DHCP Request - Transaction ID 0x32a1432c
2 0.017541 192.168.43.1 255.255.255.255 DHCP 352 DHCP ACK - Transaction ID 0x32a1432c
3 0.083663 Intel_85:ed:5f Broadcast ARP 42 Who has 192.168.43.1? Tell 192.168.43.181
4 0.084230 fe80::d829:1096:8431:b7… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
5 0.084263 fe80::d829:1096:8431:b7… ff02::1:2 DHCPv6 148 Solicit XID: 0xf8e719 CID: 000100012aef671d0c37966fead2
6 0.084623 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Join group 224.0.0.252 for any sources
7 0.090855 fe80::d829:1096:8431:b7… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
8 0.091160 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Leave group 224.0.0.252
Frame 1: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits) on interface \Device\NPF_{F0137473-F799-4FCC-87A2-5660382C18A4}, id 0
Ethernet II, Src: Intel_85:ed:5f (c4:75:ab:85:ed:5f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 332
Identification: 0x9a21 (39457)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 0.0.0.0
Destination Address: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Source Port: 68
Destination Port: 67
Length: 312
Checksum: 0x3521 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
UDP payload (304 bytes)
Dynamic Host Configuration Protocol (Request)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x32a1432c
Seconds elapsed: 0
Ready to load or capture
Packets: 5915 · Displayed: 5915 (100.0%) · Dropped: 0 (0.0%)
Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 0.0.0.0 255.255.255.255 DHCP 346 DHCP Request - Transaction ID 0x32a1432c
2 0.017541 192.168.43.1 255.255.255.255 DHCP 352 DHCP ACK - Transaction ID 0x32a1432c
3 0.083663 Intel_85:ed:5f Broadcast ARP 42 Who has 192.168.43.1? Tell 192.168.43.181
4 0.084230 fe80::d829:1096:8431:b7… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
5 0.084263 fe80::d829:1096:8431:b7… ff02::1:2 DHCPv6 148 Solicit XID: 0xf8e719 CID: 000100012aef671d0c37966fead2
6 0.084623 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Join group 224.0.0.252 for any sources
7 0.090855 fe80::d829:1096:8431:b7… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
8 0.091160 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Leave group 224.0.0.252
Source Address: 192.168.43.1
Destination Address: 255.255.255.255
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (ACK)
Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x32a1432c
Seconds elapsed: 0
Bootp flags: 0x8000, Broadcast flag (Broadcast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.43.181
Next server IP address: 192.168.43.1
Relay agent IP address: 0.0.0.0
Client MAC address: Intel_85:ed:5f (c4:75:ab:85:ed:5f)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (ACK)
Option: (54) DHCP Server Identifier (192.168.43.1)
Option: (51) IP Address Lease Time
Option: (58) Renewal Time Value
Option: (59) Rebinding Time Value
Option: (1) Subnet Mask (255.255.255.0)
Option: (28) Broadcast Address (192.168.43.255)
Option: (3) Router
Option: (6) Domain Name Server
Option: (43) Vendor-Specific Information
Option: (255) End
Padding: 00
Ready to load or capture
Packets: 5915 · Displayed: 5915 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

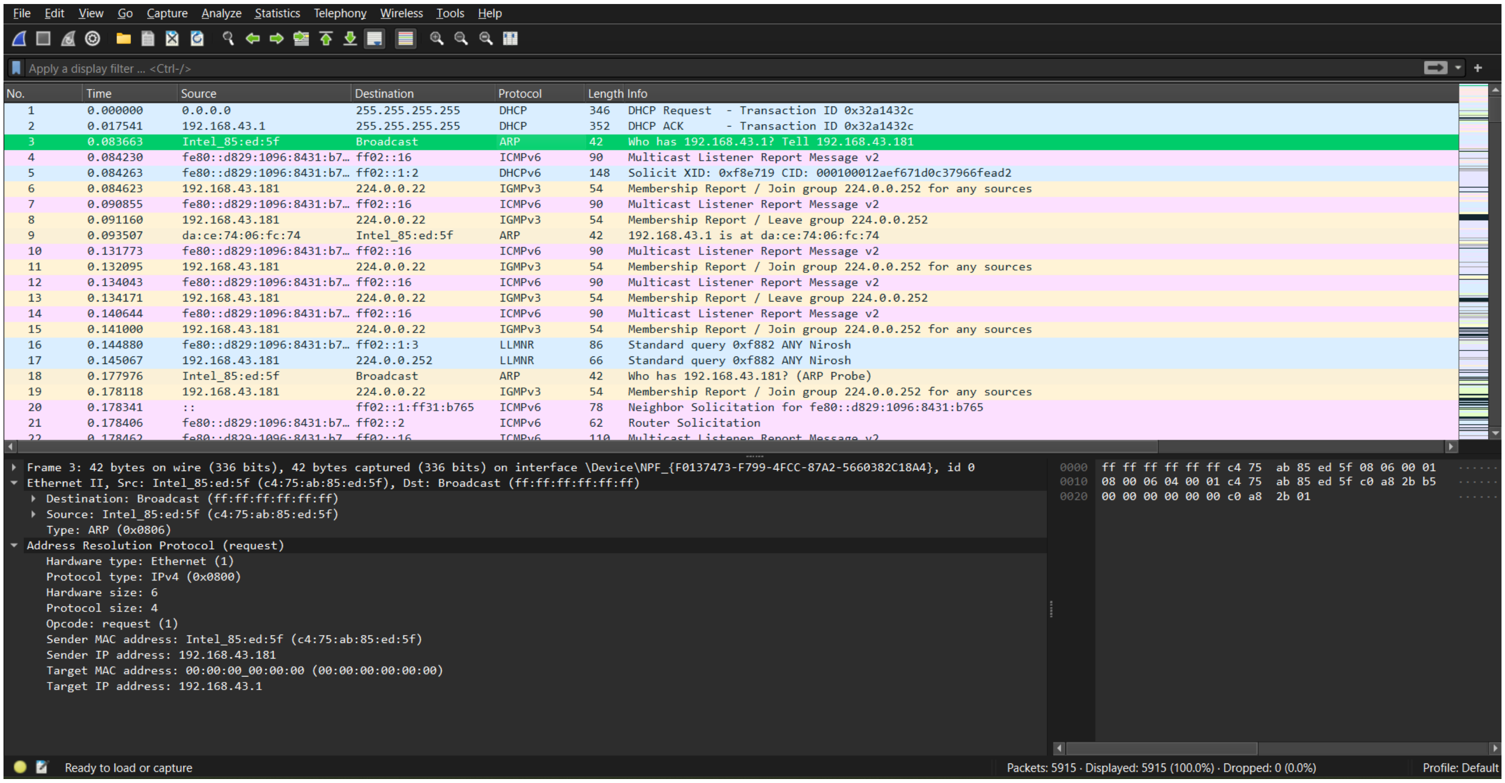
DHCP (Dynamic Host Configuration Protocol):

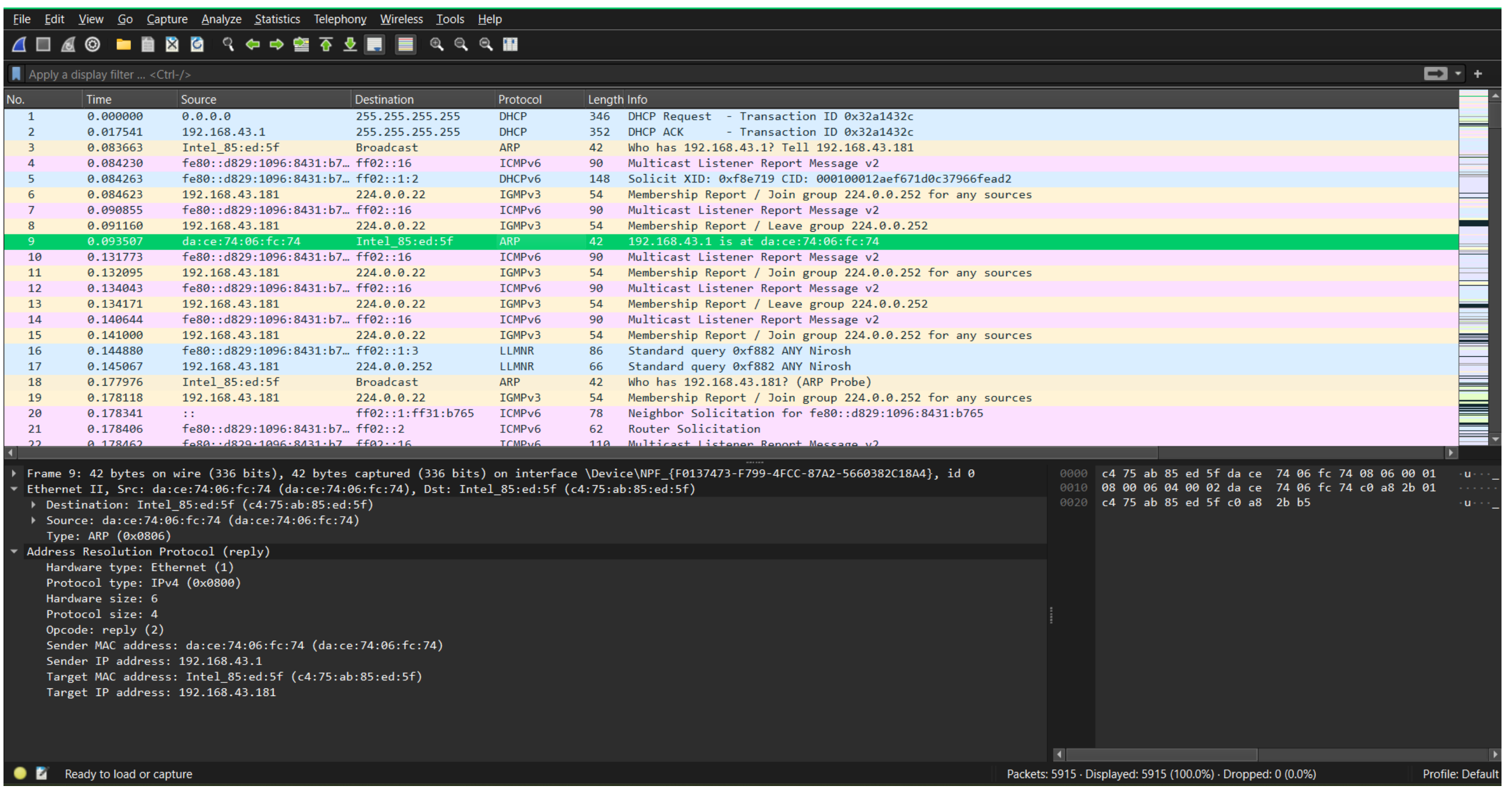
Layer: Application Layer

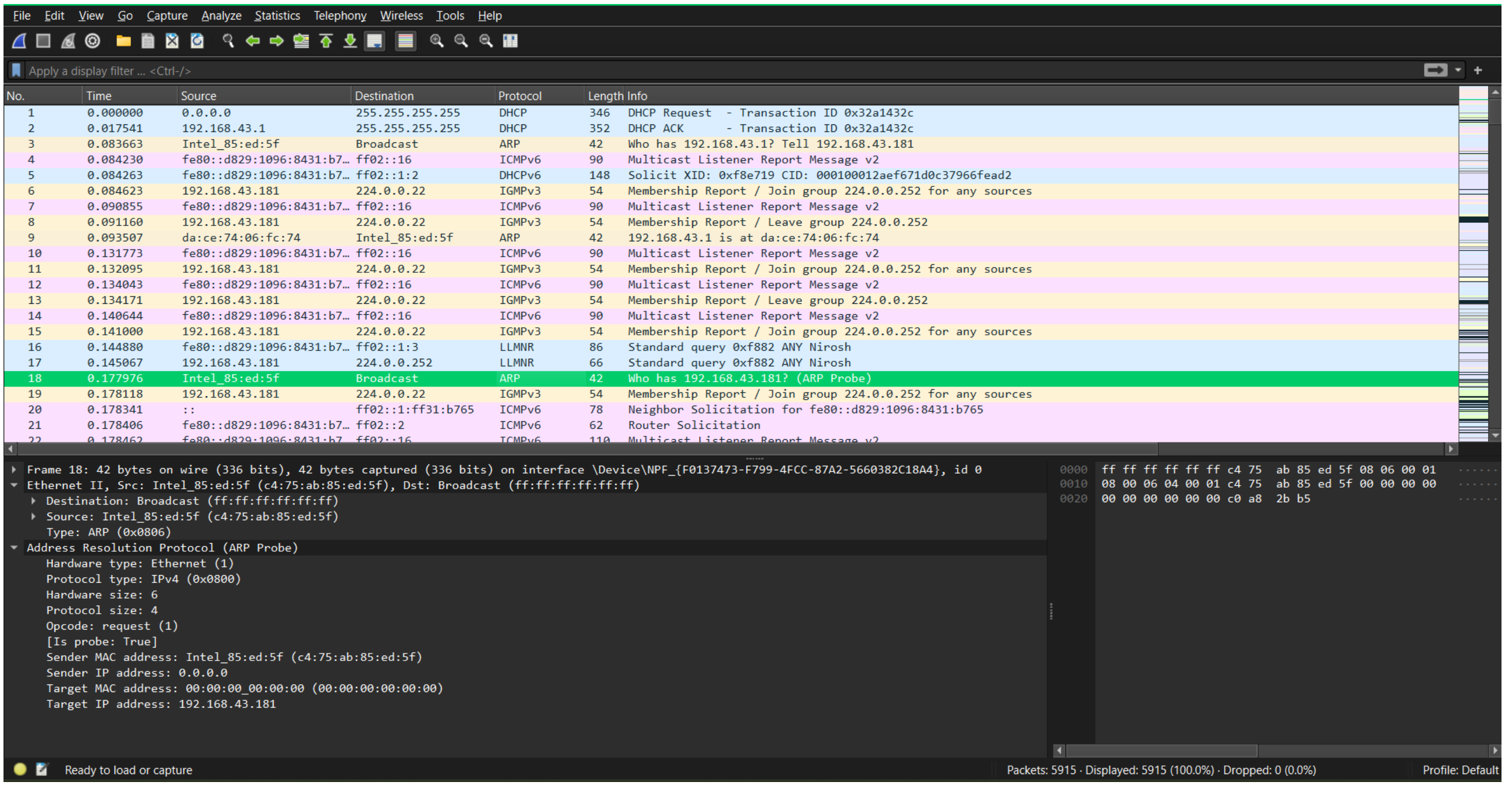
Use: Manages IP address allocation. My laptop sends a DHCPDISCOVER message to find a DHCP server, which responds with a DHCPOFFER. My laptop then sends a DHCPREQUEST, and the server confirms with a DHCPACK.

DHCP: Involves multiple messages: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, and DHCPACK. These messages allow my laptop to dynamically obtain an IP address from the DHCP server.

Step 2


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 0.0.0.0 255.255.255.255 DHCP 346 DHCP Request - Transaction ID 0x32a1432c
2 0.017541 192.168.43.1 255.255.255.255 DHCP 352 DHCP ACK - Transaction ID 0x32a1432c
3 0.083663 Intel_85:ed:5f Broadcast ARP 42 Who has 192.168.43.1? Tell 192.168.43.181
4 0.084230 fe80::d829:1096:8431:b7… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
5 0.084263 fe80::d829:1096:8431:b7… ff02::1:2 DHCPv6 148 Solicit XID: 0xf8e719 CID: 000100012aef671d0c37966fead2
6 0.084623 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Join group 224.0.0.252 for any sources
7 0.090855 fe80::d829:1096:8431:b7… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
8 0.091160 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Leave group 224.0.0.252
9 0.093507 da:ce:74:06:fc:74 Intel_85:ed:5f ARP 42 192.168.43.1 is at da:ce:74:06:fc:74
10 0.131773 fe80::d829:1096:8431:b7… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
11 0.132095 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Join group 224.0.0.252 for any sources
12 0.134043 fe80::d829:1096:8431:b7… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
13 0.134171 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Leave group 224.0.0.252
14 0.140644 fe80::d829:1096:8431:b7… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
15 0.141000 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Join group 224.0.0.252 for any sources
16 0.144880 fe80::d829:1096:8431:b7… ff02::1:3 LLMNR 86 Standard query 0xf882 ANY Nirosh
17 0.145067 192.168.43.181 224.0.0.252 LLMNR 66 Standard query 0xf882 ANY Nirosh
18 0.177976 Intel_85:ed:5f Broadcast ARP 42 Who has 192.168.43.181? (ARP Probe)
19 0.178118 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Join group 224.0.0.252 for any sources
20 0.178341 :: ff02::1:ff31:b765 ICMPv6 78 Neighbor Solicitation for fe80::d829:1096:8431:b765
21 0.178406 fe80::d829:1096:8431:b7… ff02::2 ICMPv6 62 Router Solicitation
Frame 3: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{F0137473-F799-4FCC-87A2-5660382C18A4}, id 0
Ethernet II, Src: Intel_85:ed:5f (c4:75:ab:85:ed:5f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: Intel_85:ed:5f (c4:75:ab:85:ed:5f)
Type: ARP (0x0806)
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: Intel_85:ed:5f (c4:75:ab:85:ed:5f)
Sender IP address: 192.168.43.181
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.43.1
0000 ff ff ff ff ff ff c4 75 ab 85 ed 5f 08 06 00 01
0010 08 00 06 04 00 01 c4 75 ab 85 ed 5f c0 a8 2b b5
0020 00 00 00 00 00 00 c0 a8 2b 01
Ready to load or capture
Packets: 5915 · Displayed: 5915 (100.0%) · Dropped: 0 (0.0%)
Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 0.0.0.0 255.255.255.255 DHCP 346 DHCP Request - Transaction ID 0x32a1432c
2 0.017541 192.168.43.1 255.255.255.255 DHCP 352 DHCP ACK - Transaction ID 0x32a1432c
3 0.083663 Intel_85:ed:5f Broadcast ARP 42 Who has 192.168.43.1? Tell 192.168.43.181
4 0.084230 fe80::d829:1096:8431:b7… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
5 0.084263 fe80::d829:1096:8431:b7… ff02::1:2 DHCPv6 148 Solicit XID: 0xf8e719 CID: 000100012aef671d0c37966fead2
6 0.084623 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Join group 224.0.0.252 for any sources
7 0.090855 fe80::d829:1096:8431:b7… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
8 0.091160 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Leave group 224.0.0.252
9 0.093507 da:ce:74:06:fc:74 Intel_85:ed:5f ARP 42 192.168.43.1 is at da:ce:74:06:fc:74
10 0.131773 fe80::d829:1096:8431:b7… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
11 0.132095 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Join group 224.0.0.252 for any sources
12 0.134043 fe80::d829:1096:8431:b7… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
13 0.134171 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Leave group 224.0.0.252
14 0.140644 fe80::d829:1096:8431:b7… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
15 0.141000 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Join group 224.0.0.252 for any sources
16 0.144880 fe80::d829:1096:8431:b7… ff02::1:3 LLMNR 86 Standard query 0xf882 ANY Nirosh
17 0.145067 192.168.43.181 224.0.0.252 LLMNR 66 Standard query 0xf882 ANY Nirosh
18 0.177976 Intel_85:ed:5f Broadcast ARP 42 Who has 192.168.43.181? (ARP Probe)
19 0.178118 192.168.43.181 224.0.0.22 IGMPv3 54 Membership Report / Join group 224.0.0.252 for any sources
20 0.178341 :: ff02::1:ff31:b765 ICMPv6 78 Neighbor Solicitation for fe80::d829:1096:8431:b765
21 0.178406 fe80::d829:1096:8431:b7… ff02::2 ICMPv6 62 Router Solicitation
Frame 9: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{F0137473-F799-4FCC-87A2-5660382C18A4}, id 0
Ethernet II, Src: da:ce:74:06:fc:74 (da:ce:74:06:fc:74), Dst: Intel_85:ed:5f (c4:75:ab:85:ed:5f)
Destination: Intel_85:ed:5f (c4:75:ab:85:ed:5f)
Source: da:ce:74:06:fc:74 (da:ce:74:06:fc:74)
Type: ARP (0x0806)
Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: da:ce:74:06:fc:74 (da:ce:74:06:fc:74)
Sender IP address: 192.168.43.1
Target MAC address: Intel_85:ed:5f (c4:75:ab:85:ed:5f)
Target IP address: 192.168.43.181
0000 c4 75 ab 85 ed 5f da ce 74 06 fc 74 08 06 00 01
0010 08 00 06 04 00 02 da ce 74 06 fc 74 c0 a8 2b 01
0020 c4 75 ab 85 ed 5f c0 a8 2b b5
Ready to load or capture
Packets: 5915 · Displayed: 5915 (100.0%) · Dropped: 0 (0.0%)
Profile: Default



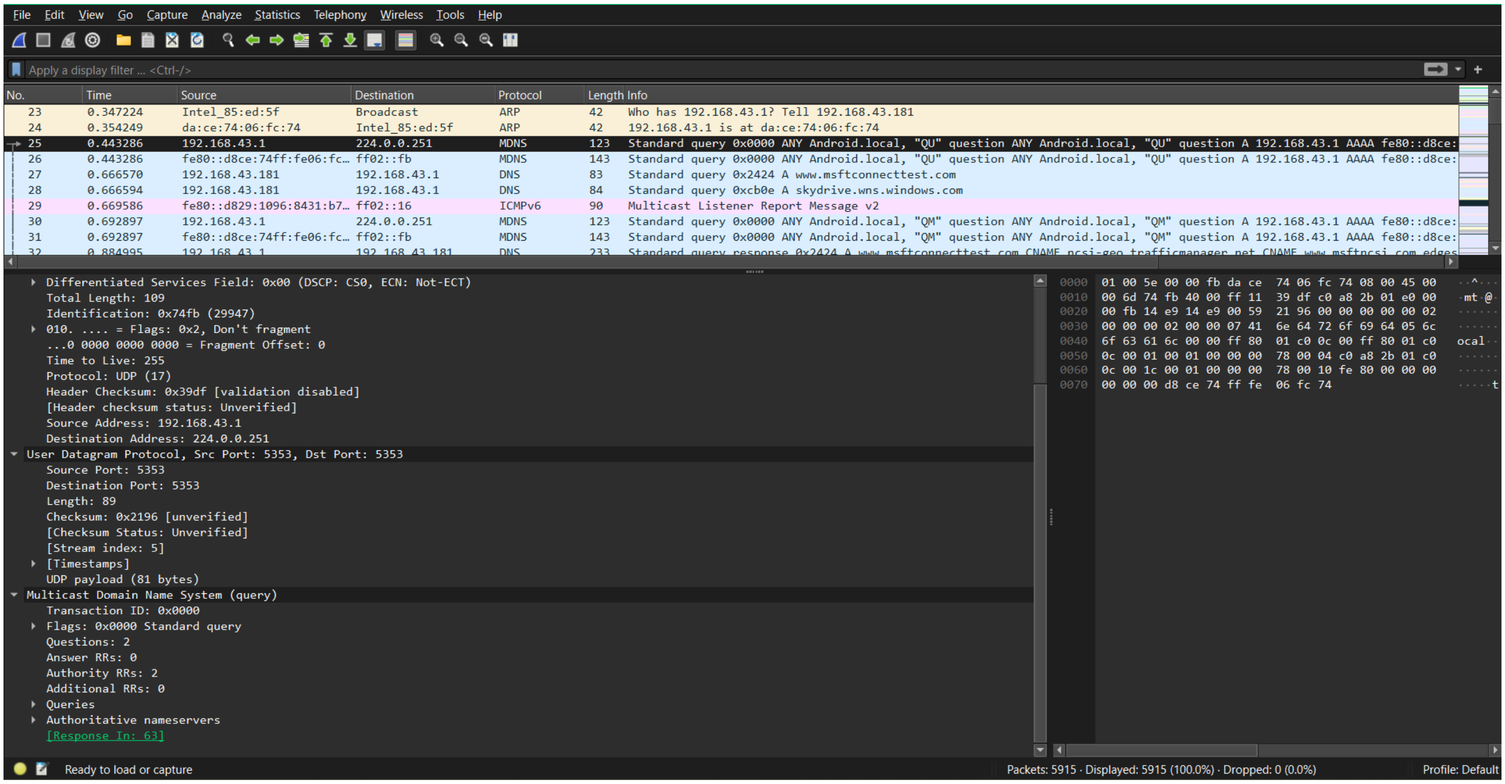
ARP (Address Resolution Protocol):

Layer: Data Link Layer

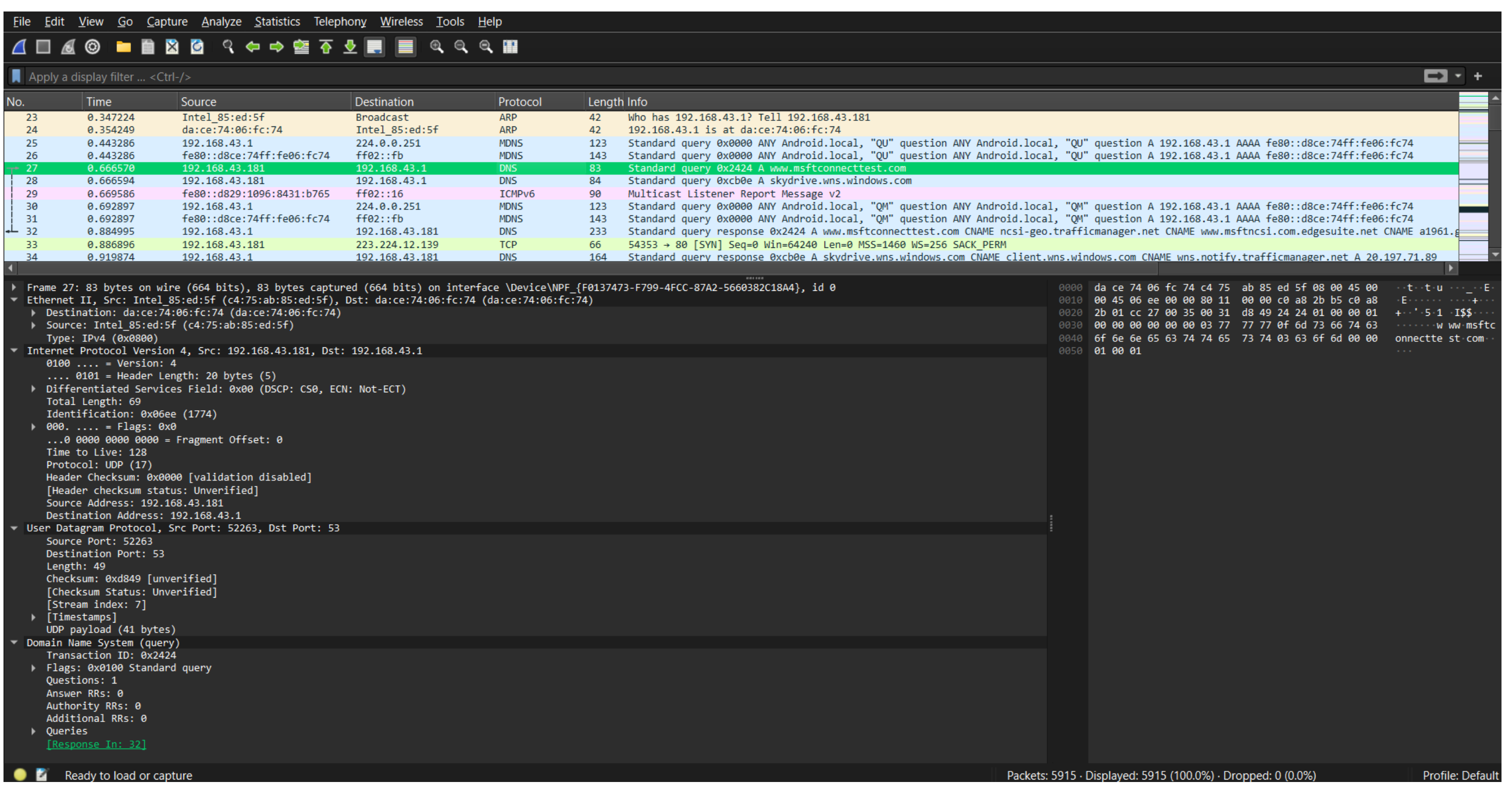
Use: Resolves IP addresses to MAC addresses. My laptop sends an ARP request to determine the MAC address of the default gateway, and the gateway responds with its MAC address.

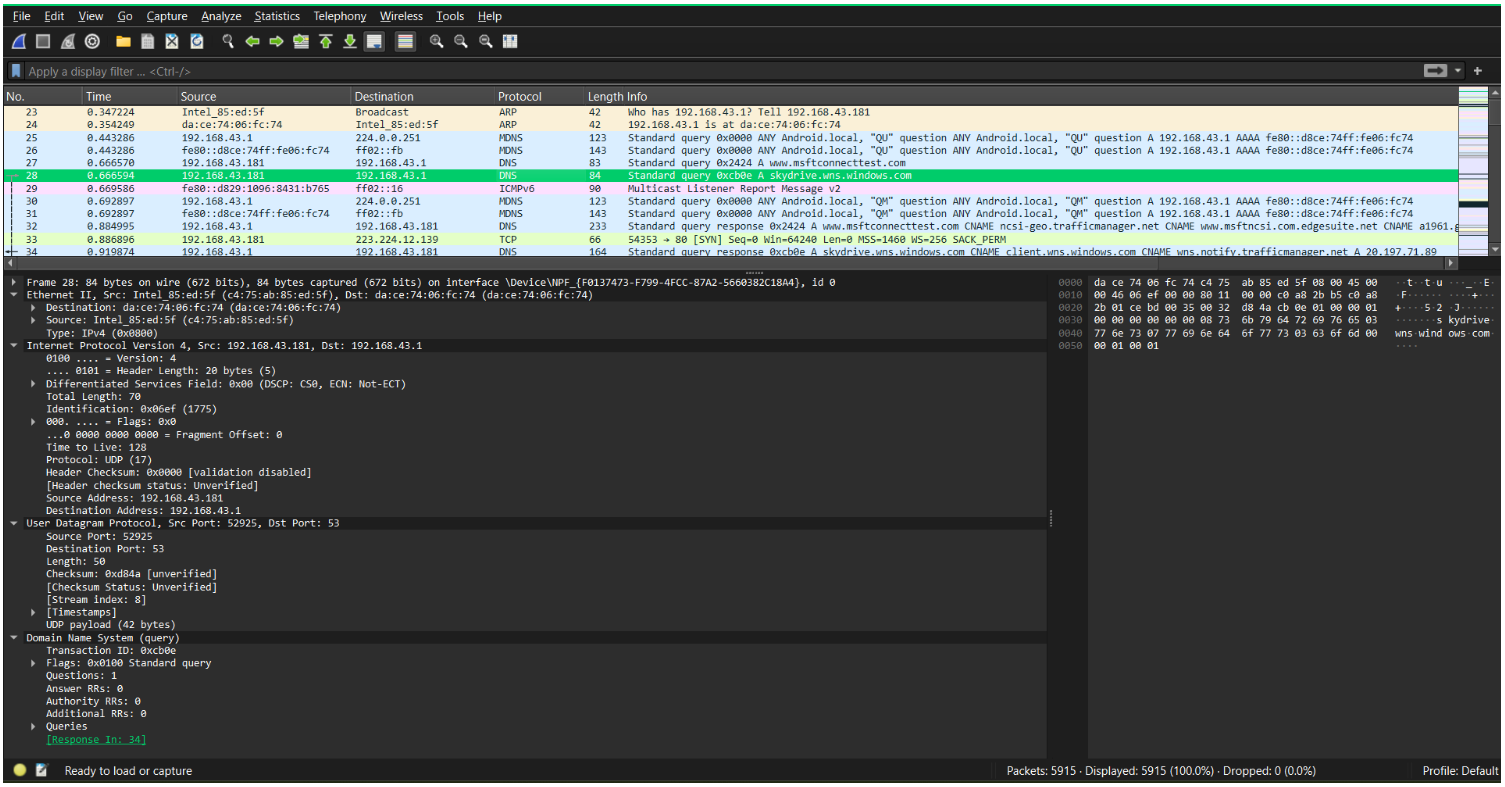
ARP: My laptop sends an ARP request ("Who has IP address **192.168.43.1**? Tell IP address **192.168.43.181**") and receives an ARP reply ("IP address **192.168.43.1** is at MAC address **da:ce:74:06:fc:74** "). This allows my laptop to map IP addresses to MAC addresses within the local network.

Step 3



MDNS (Multicast Domain Name System)





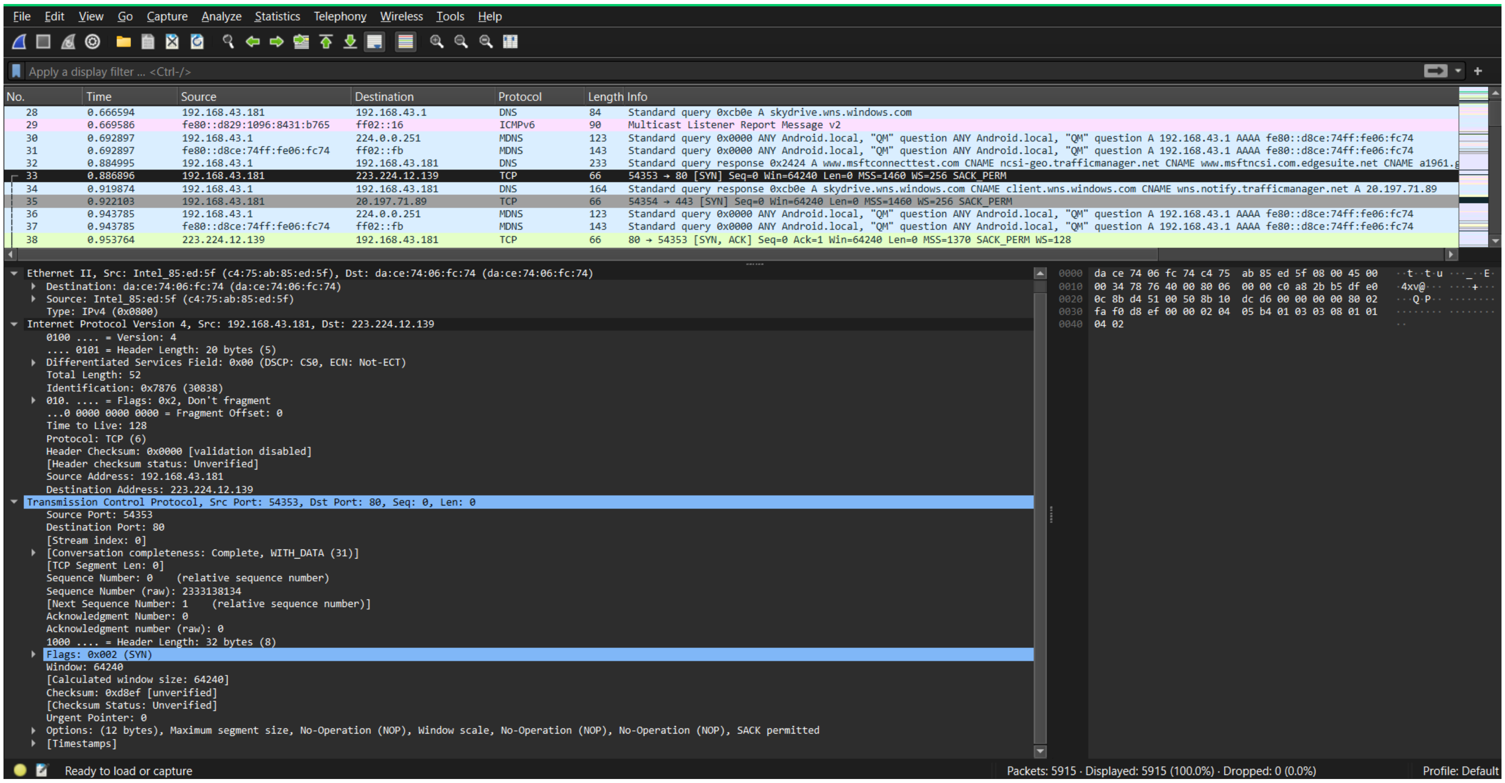
DNS (Domain Name System):

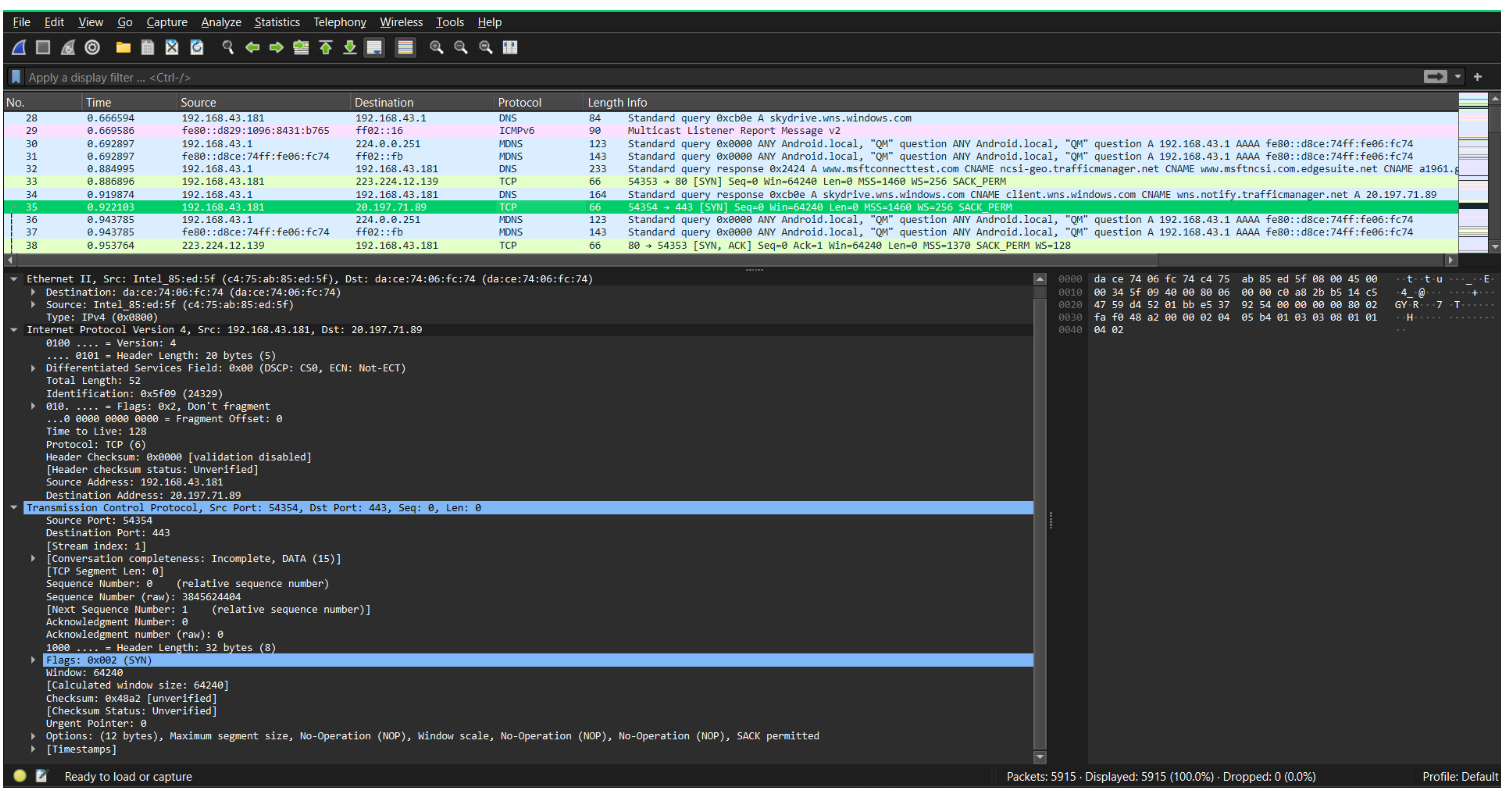
Layer: Application Layer

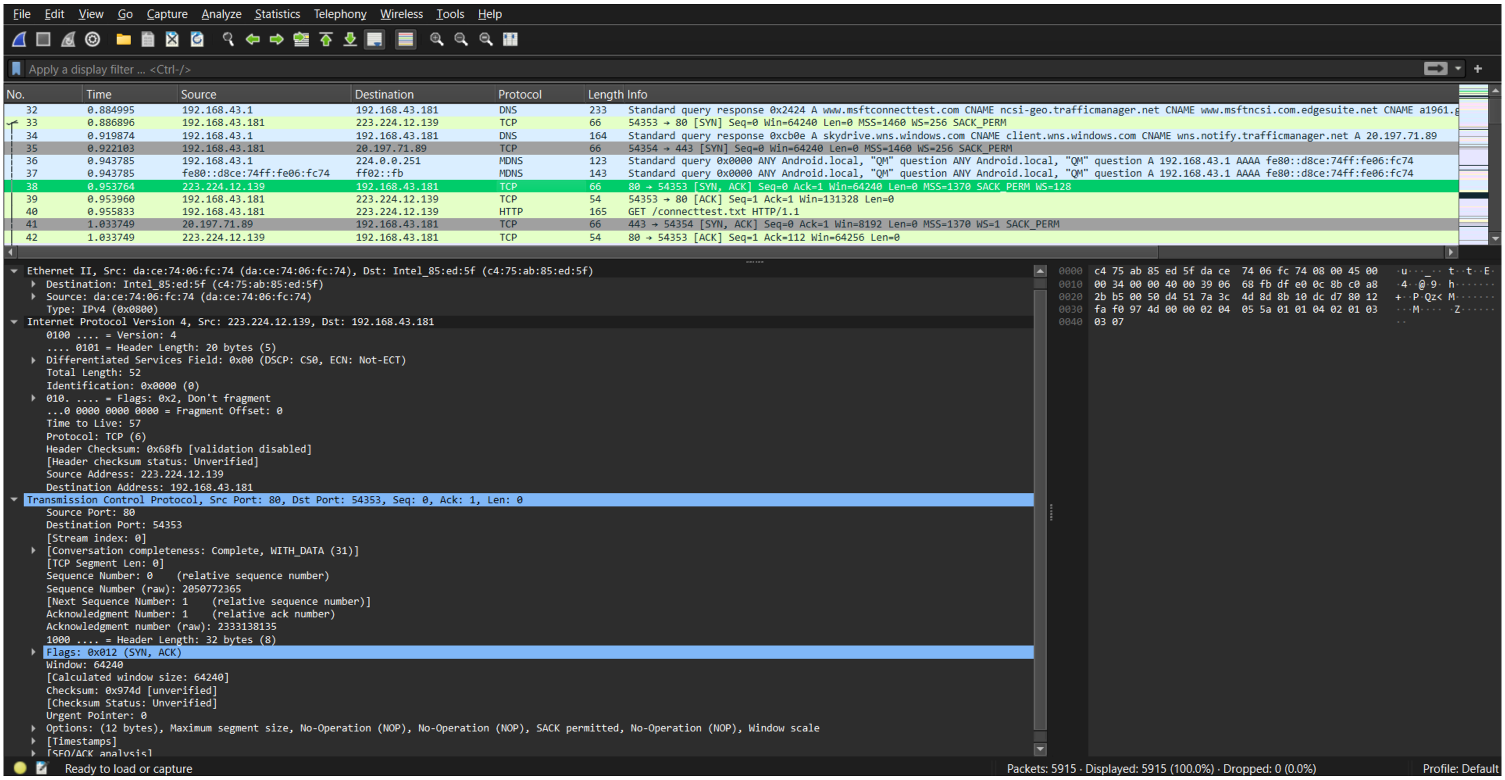
Use: Resolves domain names to IP addresses. My laptop sends a DNS query to the DNS server to get the IP address corresponding to the URL entered.

DNS: My laptop sends a DNS query to resolve the domain name (e.g., d2l.deakin.edu.au) to its corresponding IP address, and the DNS server replies with the IP address.

Step 4


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
28 0.666594 192.168.43.181 192.168.43.1 DNS 84 Standard query 0xcb0e A skydrive.wns.windows.com
29 0.669586 fe80::d829:1096:8431:b765 ff02::16 ICMPv6 90 Multicast Listener Report Message v2
30 0.692897 192.168.43.1 224.0.0.251 MDNS 123 Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 192.168.43.1 AAAA fe80::d8ce:74ff:fe06:fc74
31 0.692897 fe80::d8ce:74ff:fe06:fc74 ff02::fb MDNS 143 Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 192.168.43.1 AAAA fe80::d8ce:74ff:fe06:fc74
32 0.884995 192.168.43.1 192.168.43.181 DNS 233 Standard query response 0x2424 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a1961.g
33 0.886896 192.168.43.181 223.224.12.139 TCP 66 54353 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
34 0.919874 192.168.43.1 192.168.43.181 DNS 164 Standard query response 0xcb0e A skydrive.wns.windows.com CNAME client.wns.windows.com CNAME wns.notify.trafficmanager.net A 20.197.71.89
35 0.922103 192.168.43.181 20.197.71.89 TCP 66 54354 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
36 0.943785 192.168.43.1 224.0.0.251 MDNS 123 Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 192.168.43.1 AAAA fe80::d8ce:74ff:fe06:fc74
37 0.943785 fe80::d8ce:74ff:fe06:fc74 ff02::fb MDNS 143 Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 192.168.43.1 AAAA fe80::d8ce:74ff:fe06:fc74
38 0.953764 223.224.12.139 192.168.43.181 TCP 66 80 → 54353 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1370 SACK_PERM WS=128
Ethernet II, Src: Intel_85:ed:5f (c4:75:ab:85:ed:5f), Dst: da:ce:74:06:fc:74 (da:ce:74:06:fc:74)
Destination: da:ce:74:06:fc:74 (da:ce:74:06:fc:74)
Source: Intel_85:ed:5f (c4:75:ab:85:ed:5f)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.43.181, Dst: 223.224.12.139
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0x7876 (30838)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.43.181
Destination Address: 223.224.12.139
Transmission Control Protocol, Src Port: 54353, Dst Port: 80, Seq: 0, Len: 0
Source Port: 54353
Destination Port: 80
[Stream index: 0]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2333138134
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
Window: 64240
[Calculated window size: 64240]
Checksum: 0xd8ef [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
[Timestamps]
0000 da ce 74 06 fc 74 c4 75 ab 85 ed 5f 08 00 45 00
0010 00 34 78 76 40 00 80 06 00 00 c0 a8 2b b5 df e0
0020 0c 8b d4 51 00 50 8b 10 dc d6 00 00 00 00 80 02
0030 fa f0 d8 ef 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02
Ready to load or capture
Packets: 5915 · Displayed: 5915 (100.0%) · Dropped: 0 (0.0%)
Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
28 0.666594 192.168.43.181 192.168.43.1 DNS 84 Standard query 0xcb0e A skydrive.wns.windows.com
29 0.669586 fe80::d829:1096:8431:b765 ff02::16 ICMPv6 90 Multicast Listener Report Message v2
30 0.692897 192.168.43.1 224.0.0.251 MDNS 123 Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 192.168.43.1 AAAA fe80::d8ce:74ff:fe06:fc74
31 0.692897 fe80::d8ce:74ff:fe06:fc74 ff02::fb MDNS 143 Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 192.168.43.1 AAAA fe80::d8ce:74ff:fe06:fc74
32 0.884995 192.168.43.1 192.168.43.181 DNS 233 Standard query response 0x2424 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a1961.g
33 0.886896 192.168.43.181 223.224.12.139 TCP 66 54353 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
34 0.919874 192.168.43.1 192.168.43.181 DNS 164 Standard query response 0xcb0e A skydrive.wns.windows.com CNAME client.wns.windows.com CNAME wns.notify.trafficmanager.net A 20.197.71.89
35 0.922103 192.168.43.181 20.197.71.89 TCP 66 54354 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
36 0.943785 192.168.43.1 224.0.0.251 MDNS 123 Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 192.168.43.1 AAAA fe80::d8ce:74ff:fe06:fc74
37 0.943785 fe80::d8ce:74ff:fe06:fc74 ff02::fb MDNS 143 Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 192.168.43.1 AAAA fe80::d8ce:74ff:fe06:fc74
38 0.953764 223.224.12.139 192.168.43.181 TCP 66 80 → 54353 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1370 SACK_PERM WS=128
Ethernet II, Src: Intel_85:ed:5f (c4:75:ab:85:ed:5f), Dst: da:ce:74:06:fc:74 (da:ce:74:06:fc:74)
Destination: da:ce:74:06:fc:74 (da:ce:74:06:fc:74)
Source: Intel_85:ed:5f (c4:75:ab:85:ed:5f)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.43.181, Dst: 20.197.71.89
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0x5f09 (24329)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.43.181
Destination Address: 20.197.71.89
Transmission Control Protocol, Src Port: 54354, Dst Port: 443, Seq: 0, Len: 0
Source Port: 54354
Destination Port: 443
[Stream index: 1]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 3845624404
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
Window: 64240
[Calculated window size: 64240]
Checksum: 0x48a2 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
[Timestamps]
0000 da ce 74 06 fc 74 c4 75 ab 85 ed 5f 08 00 45 00
0010 00 34 5f 09 40 00 80 06 00 00 c0 a8 2b b5 14 c5
0020 47 59 d4 52 01 bb e5 37 92 54 00 00 00 00 80 02
0030 fa f0 48 a2 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02
Ready to load or capture
Packets: 5915 · Displayed: 5915 (100.0%) · Dropped: 0 (0.0%)
Profile: Default



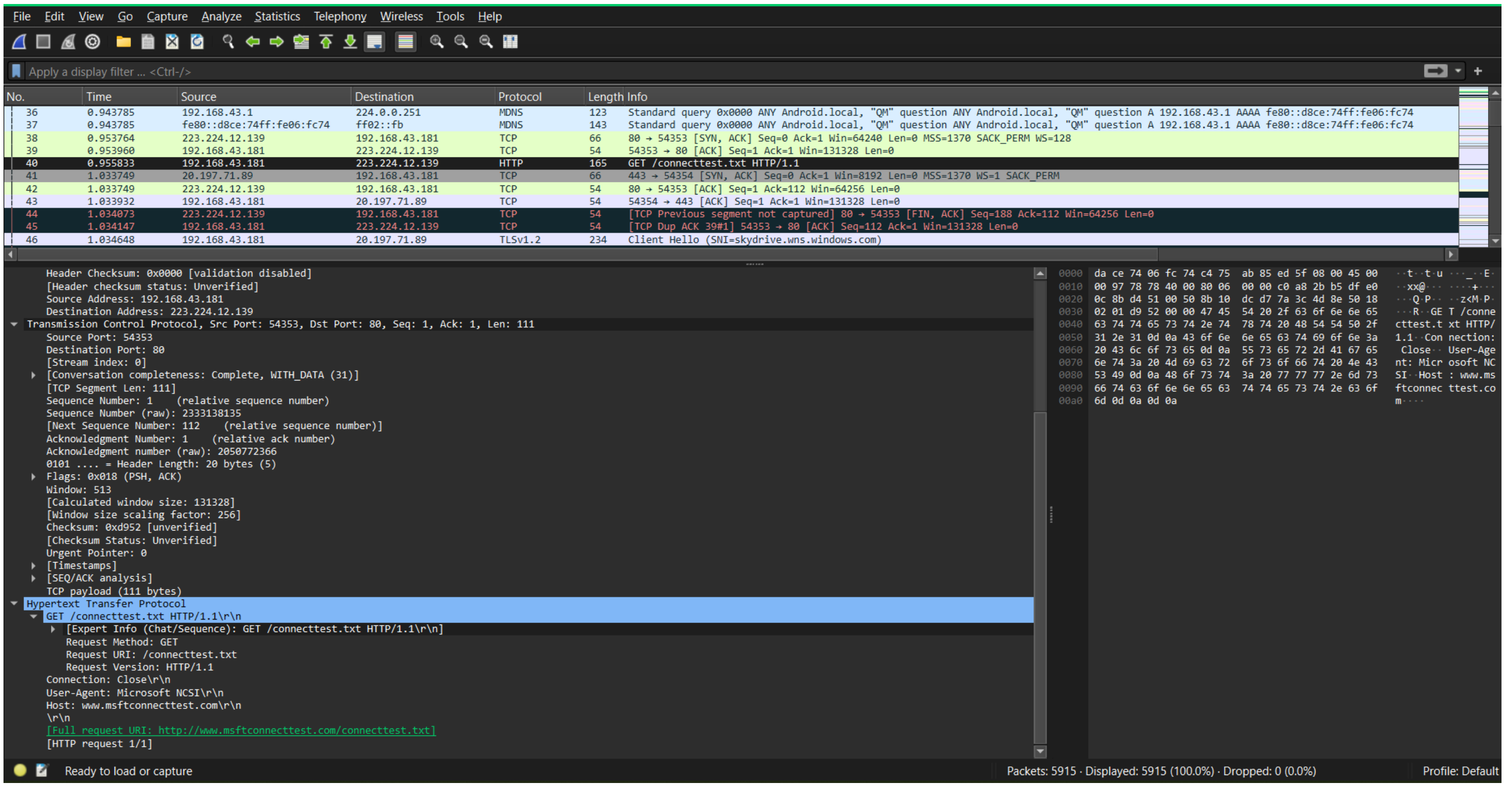
TCP (Transmission Control Protocol):

Layer: Transport Layer

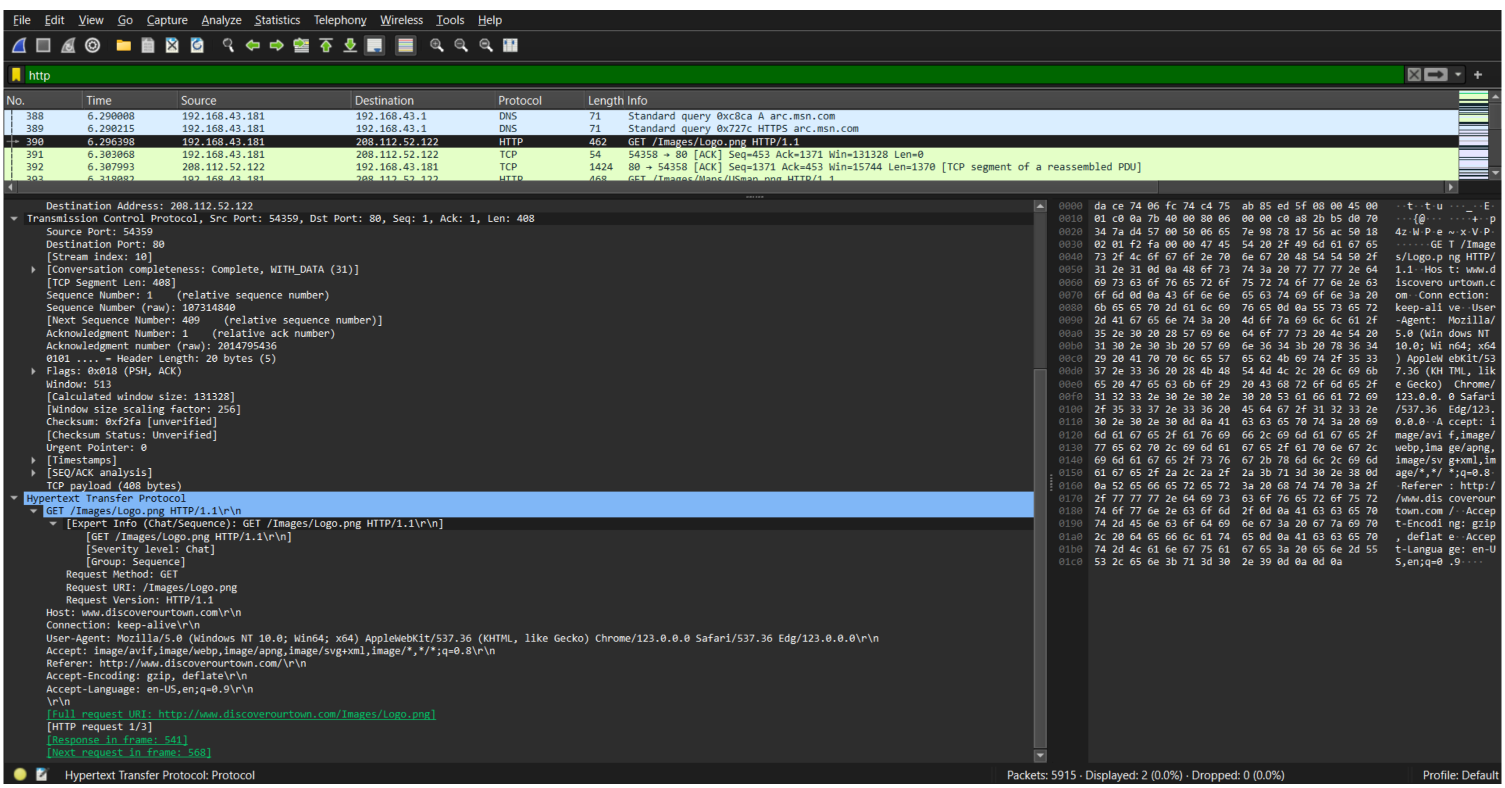
Use: Establishes a reliable connection between my laptop and the server. This involves the TCP three-way handshake (SYN, SYN-ACK, ACK) to ensure a stable connection for data transfer.

TCP: The three-way handshake ensures a reliable connection. My laptop sends a SYN packet to initiate the connection, the server responds with a SYN-ACK, and my laptop completes the handshake with an ACK.

Step 5



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
36 0.943785 192.168.43.1 224.0.0.251 MDNS 123 Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 192.168.43.1 AAAA fe80::d8ce:74ff:fe06:fc74
37 0.943785 fe80::d8ce:74ff:fe06:fc74 ff02::fb MDNS 143 Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 192.168.43.1 AAAA fe80::d8ce:74ff:fe06:fc74
38 0.953764 223.224.12.139 192.168.43.181 TCP 66 80 → 54353 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1370 SACK_PERM WS=128
39 0.953960 192.168.43.181 223.224.12.139 TCP 54 54353 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
40 0.955833 192.168.43.181 223.224.12.139 HTTP 165 GET /connecttest.txt HTTP/1.1
41 1.033749 20.197.71.89 192.168.43.181 TCP 66 443 → 54354 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1370 WS=1 SACK_PERM
42 1.033749 223.224.12.139 192.168.43.181 TCP 54 80 → 54353 [ACK] Seq=1 Ack=112 Win=64256 Len=0
43 1.033932 192.168.43.181 20.197.71.89 TCP 54 54354 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
44 1.034073 223.224.12.139 192.168.43.181 TCP 54 [TCP Previous segment not captured] 80 → 54353 [FIN, ACK] Seq=188 Ack=112 Win=64256 Len=0
45 1.034147 192.168.43.181 223.224.12.139 TCP 54 [TCP Dup ACK 39#1] 54353 → 80 [ACK] Seq=112 Ack=1 Win=131328 Len=0
46 1.034648 192.168.43.181 20.197.71.89 TLSv1.2 234 Client Hello (SNI=skydrive.wns.windows.com)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.43.181
Destination Address: 223.224.12.139
Transmission Control Protocol, Src Port: 54353, Dst Port: 80, Seq: 1, Ack: 1, Len: 111
Source Port: 54353
Destination Port: 80
[Stream index: 0]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 111]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2333138135
[Next Sequence Number: 112 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2050772366
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 513
[Calculated window size: 131328]
[Window size scaling factor: 256]
Checksum: 0xd952 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (111 bytes)
Hypertext Transfer Protocol
GET /connecttest.txt HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /connecttest.txt HTTP/1.1\r\n]
Request Method: GET
Request URI: /connecttest.txt
Request Version: HTTP/1.1
Connection: Close\r\n
User-Agent: Microsoft NCSI\r\n
Host: www.msftconnecttest.com\r\n
\r\n
[Full request URI: http://www.msftconnecttest.com/connecttest.txt]
[HTTP request 1/1]
Ready to load or capture
Packets: 5915 · Displayed: 5915 (100.0%) · Dropped: 0 (0.0%)
Profile: Default



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
388 6.290008 192.168.43.181 192.168.43.1 DNS 71 Standard query 0xc8ca A arc.msn.com
389 6.290215 192.168.43.181 192.168.43.1 DNS 71 Standard query 0x727c HTTPS arc.msn.com
390 6.296398 192.168.43.181 208.112.52.122 HTTP 462 GET /Images/Logo.png HTTP/1.1
391 6.303068 192.168.43.181 208.112.52.122 TCP 54 54358 → 80 [ACK] Seq=453 Ack=1371 Win=131328 Len=0
392 6.307993 208.112.52.122 192.168.43.181 TCP 1424 80 → 54358 [ACK] Seq=1371 Ack=453 Win=15744 Len=1370 [TCP segment of a reassembled PDU]
Destination Address: 208.112.52.122
Transmission Control Protocol, Src Port: 54359, Dst Port: 80, Seq: 1, Ack: 1, Len: 408
Source Port: 54359
Destination Port: 80
[Stream index: 10]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 408]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 107314840
[Next Sequence Number: 409 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2014795436
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 513
[Calculated window size: 131328]
[Window size scaling factor: 256]
Checksum: 0xf2fa [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (408 bytes)
Hypertext Transfer Protocol
GET /Images/Logo.png HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /Images/Logo.png HTTP/1.1\r\n]
[GET /Images/Logo.png HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /Images/Logo.png
Request Version: HTTP/1.1
Host: www.discoverourtown.com\r\n
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36 Edg/123.0.0.0\r\n
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
Referer: http://www.discoverourtown.com/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://www.discoverourtown.com/Images/Logo.png]
[HTTP request 1/3]
[Response in frame: 541]
[Next request in frame: 568]
Hypertext Transfer Protocol: Protocol
Packets: 5915 · Displayed: 2 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

HTTP (Hypertext Transfer Protocol):

Layer: Application Layer

Use: Governs the request and delivery of web content. My laptop sends an HTTP GET request to the server, which responds with the requested web page data.

HTTP: My laptop sends an HTTP GET request to retrieve the web page. The server processes the request and sends back the HTML content of the web page.

Now this is how the sequence goes.

Comparison with Activity 1:

The observed protocols and steps match the theoretical process described in Activity 1, confirming that the behind-the-scenes process involves these key protocols at their respective layers.

By using Wireshark to capture and analyze these packets, I could see the practical application of these protocols and how they work together to facilitate network communication and web page retrieval.

Activity 3: Wired vs. Wireless Networks - Understanding Traffic Flow

Okay, let's play around with wired and wireless networks in Cisco Packet Tracer!

It's like a virtual network lab where I can build networks and see how they work.

First, I'm going to send a test message, like a little package of information, in two ways:

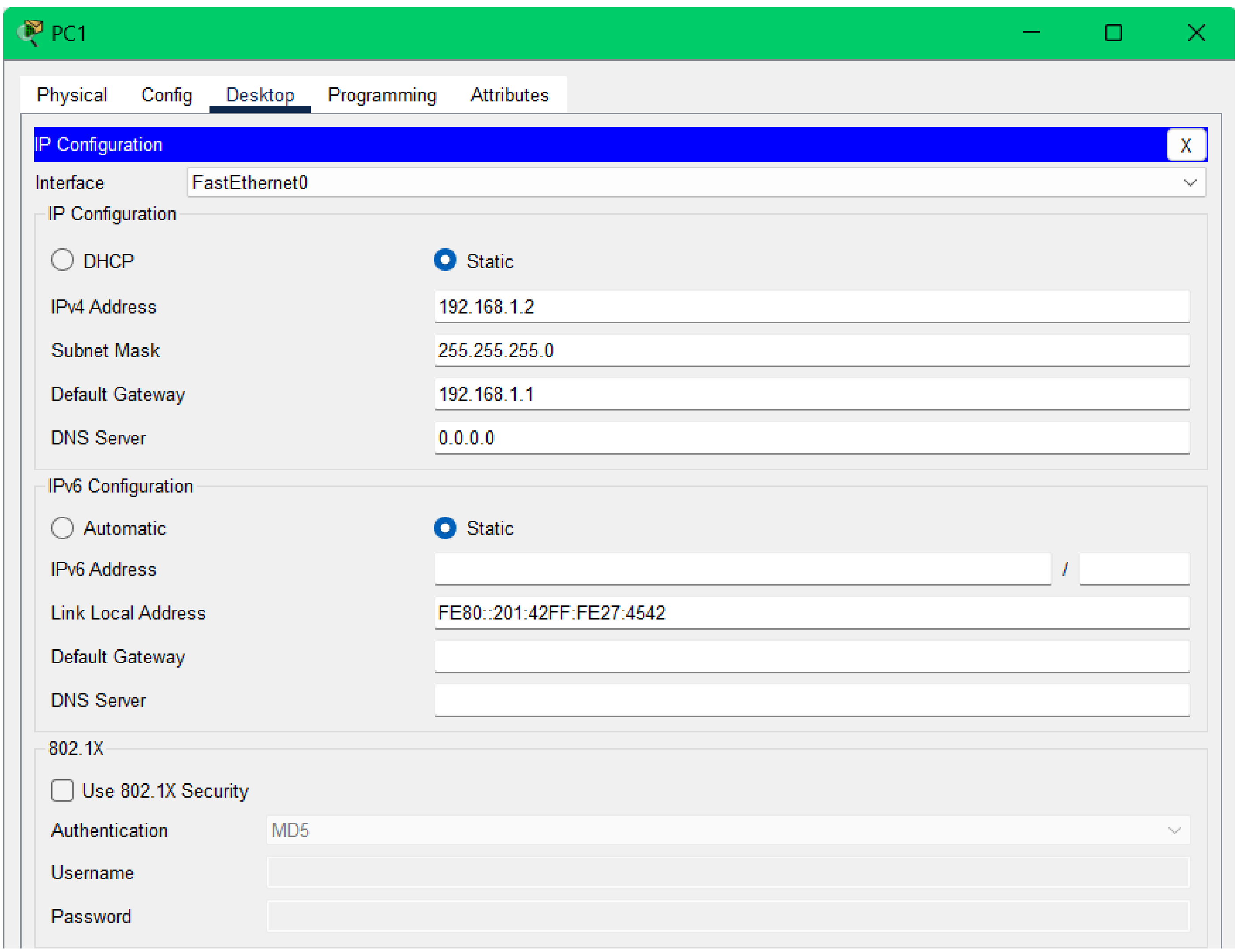
From my desktop computer to another one - Imagine this as shouting across the room to a friend. We're connected by a wire, just like the computers.

From my laptop to a tablet - Now picture whispering to someone across the room. We're not directly connected, but the message travels through the air.

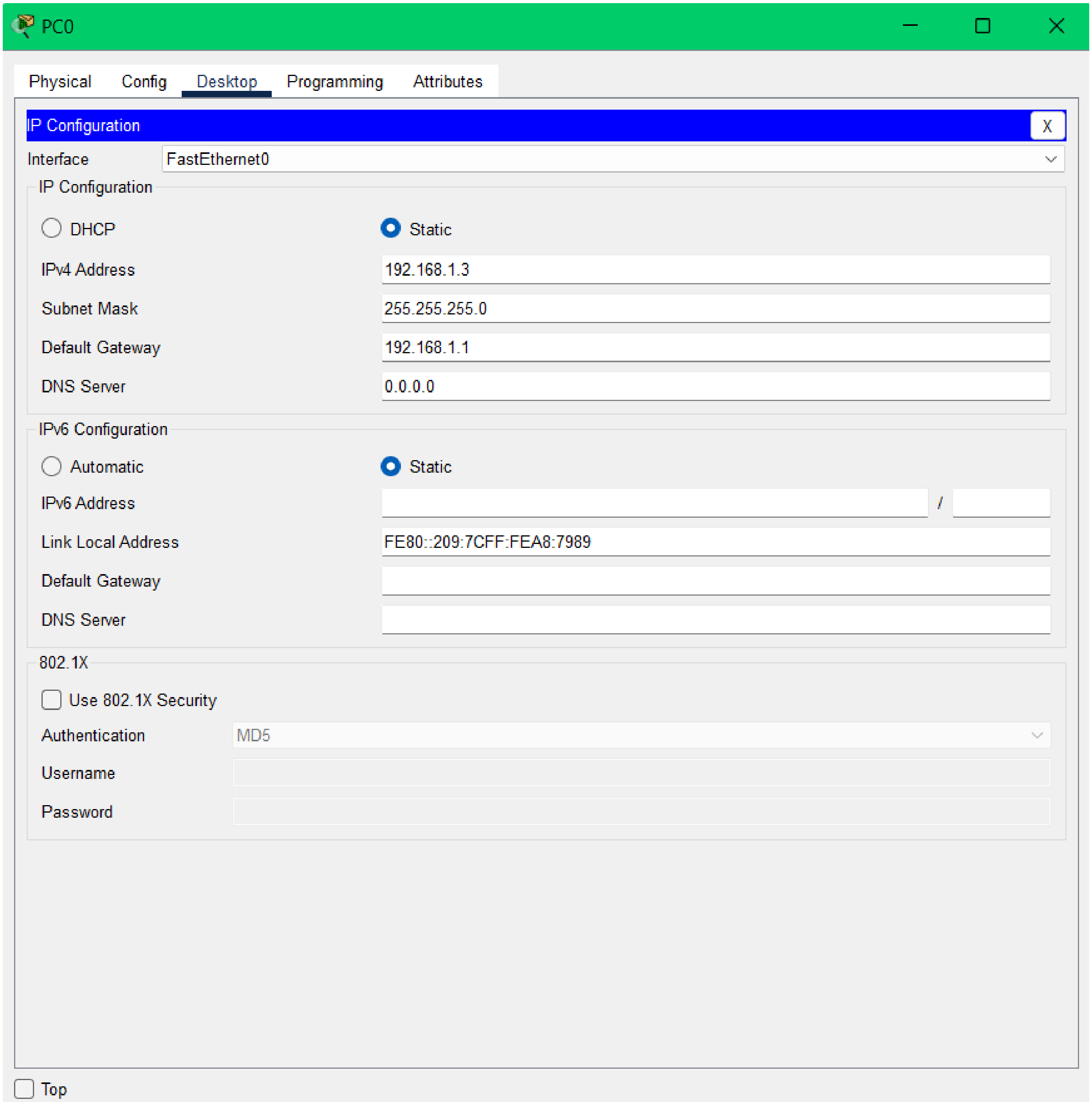
First, I'll provide how I statically configured the devices in both the wired and wireless networks

Wired network

PC1

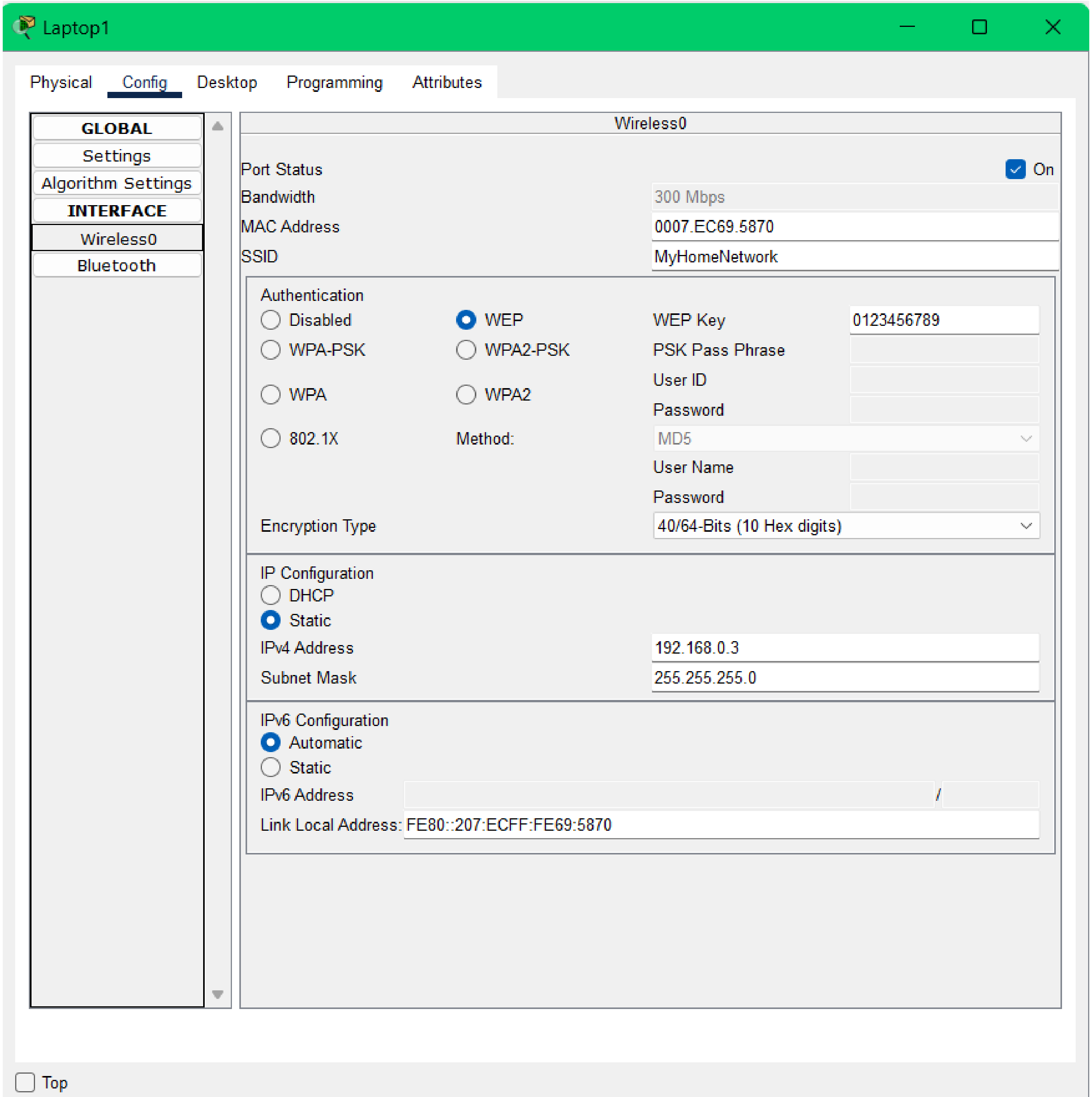


PC0

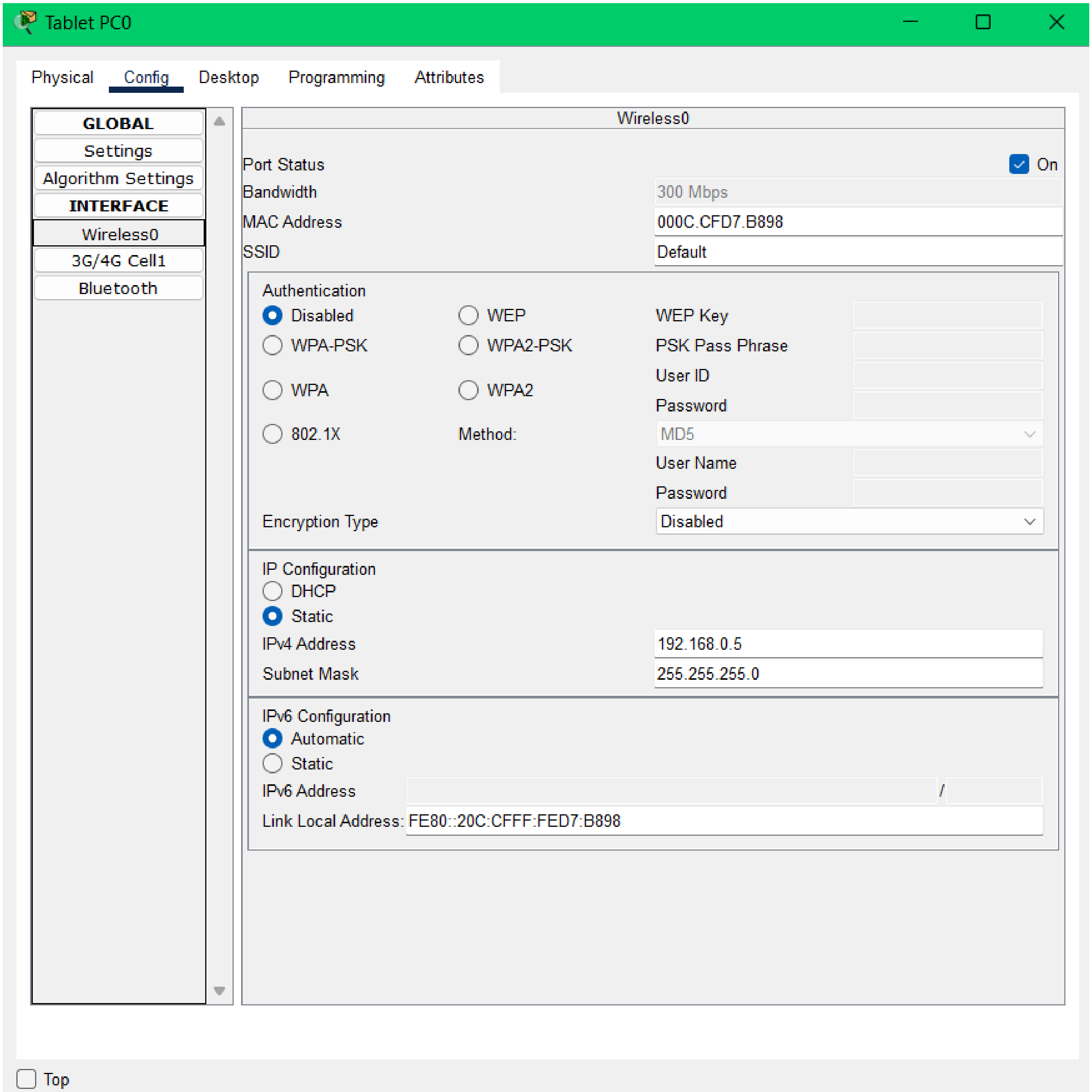

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::209:7CFF:FEA8:7989
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

Wireless Network

Laptop 1

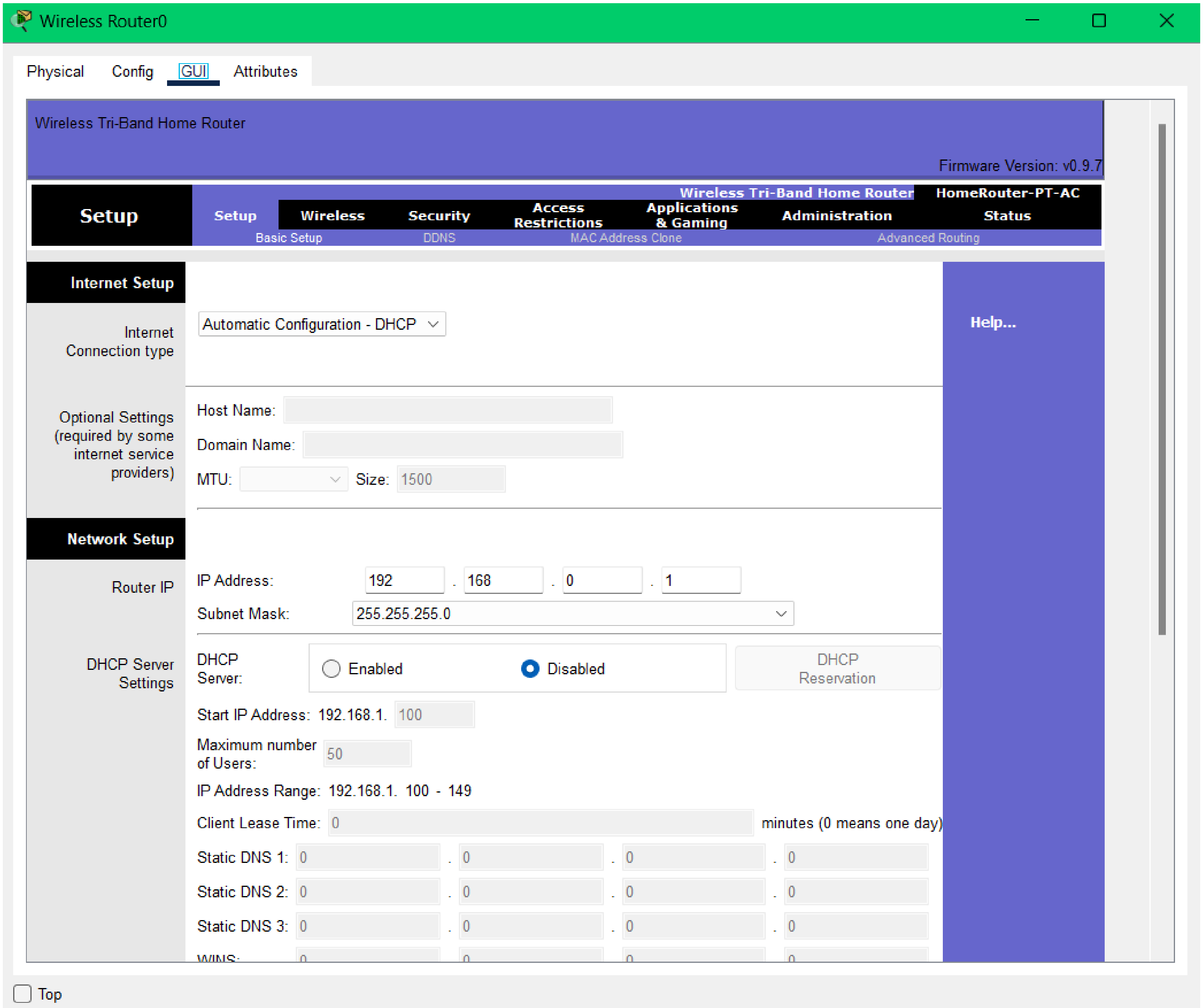


Tablet 0

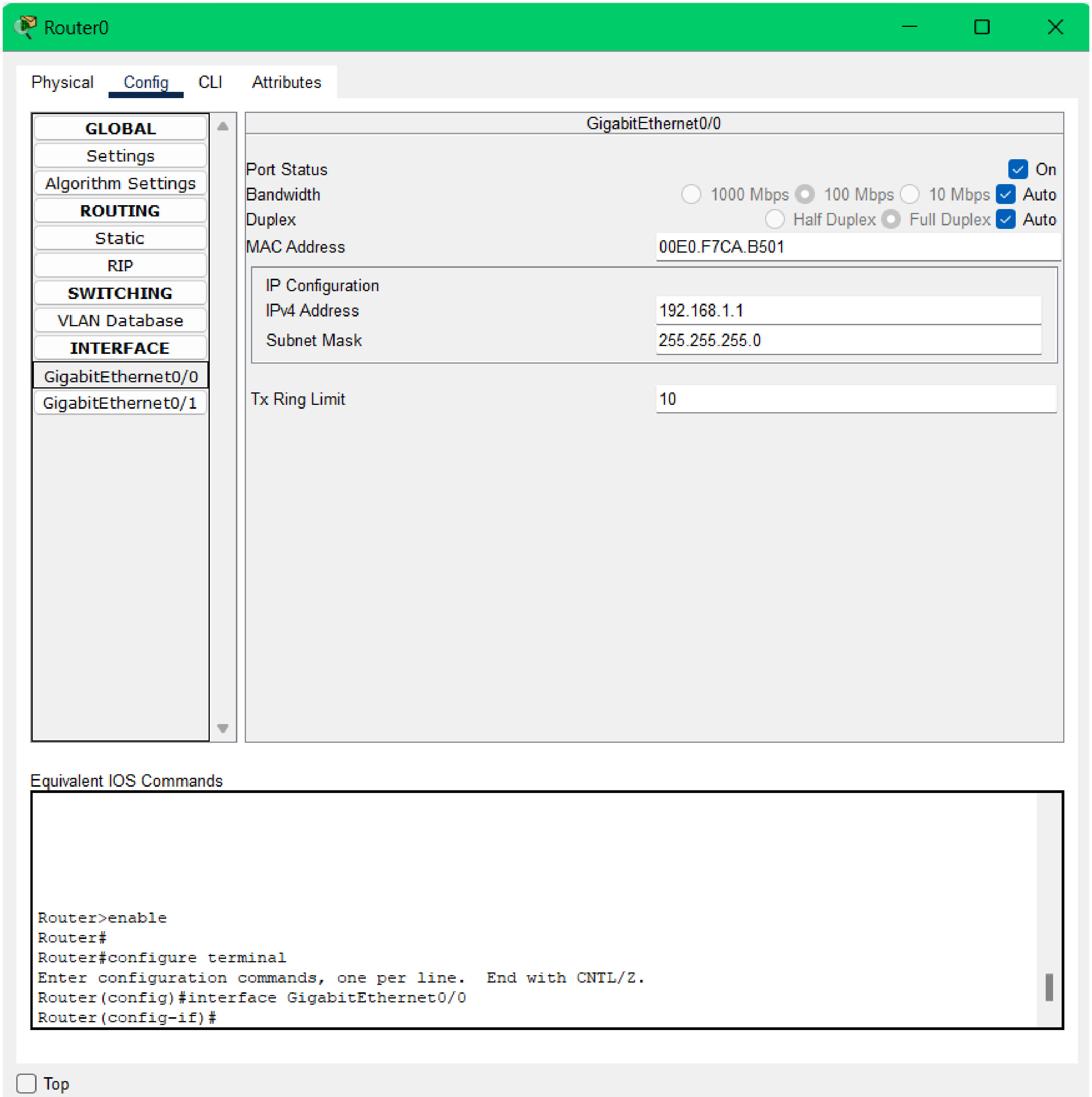


Tablet PC0
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
Wireless0
3G/4G Cell1
Bluetooth
Wireless0
Port Status
On
Bandwidth
300 Mbps
MAC Address
000C.CFD7.B898
SSID
Default
Authentication
Disabled
WEP
WEP Key
WPA-PSK
WPA2-PSK
PSK Pass Phrase
User ID
WPA
WPA2
Password
802.1X
Method:
MD5
User Name
Password
Encryption Type
Disabled
IP Configuration
DHCP
Static
IPv4 Address
192.168.0.5
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address:
FE80::20C:CFFF:FED7:B898
Top

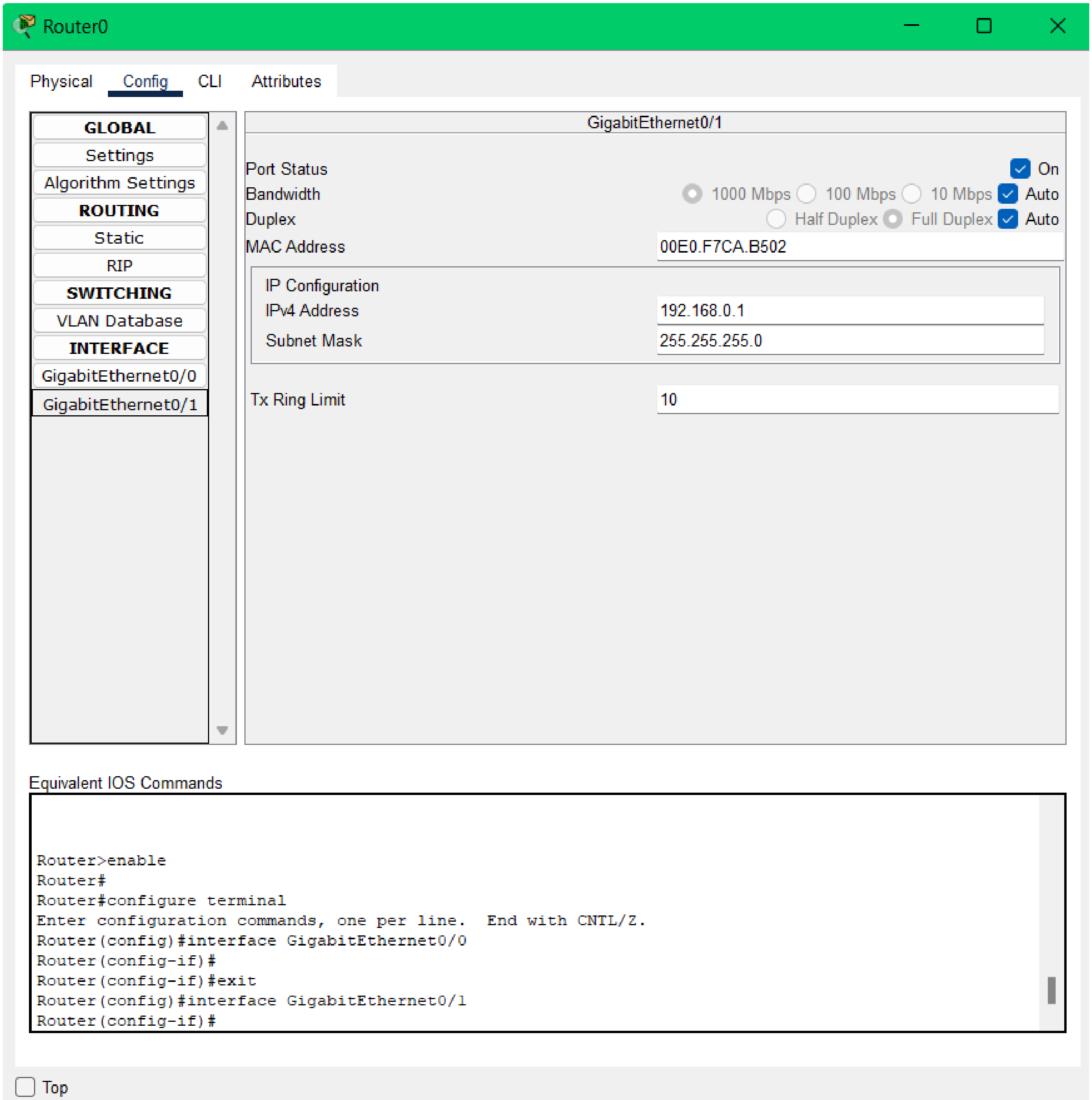
Wireless Home Router



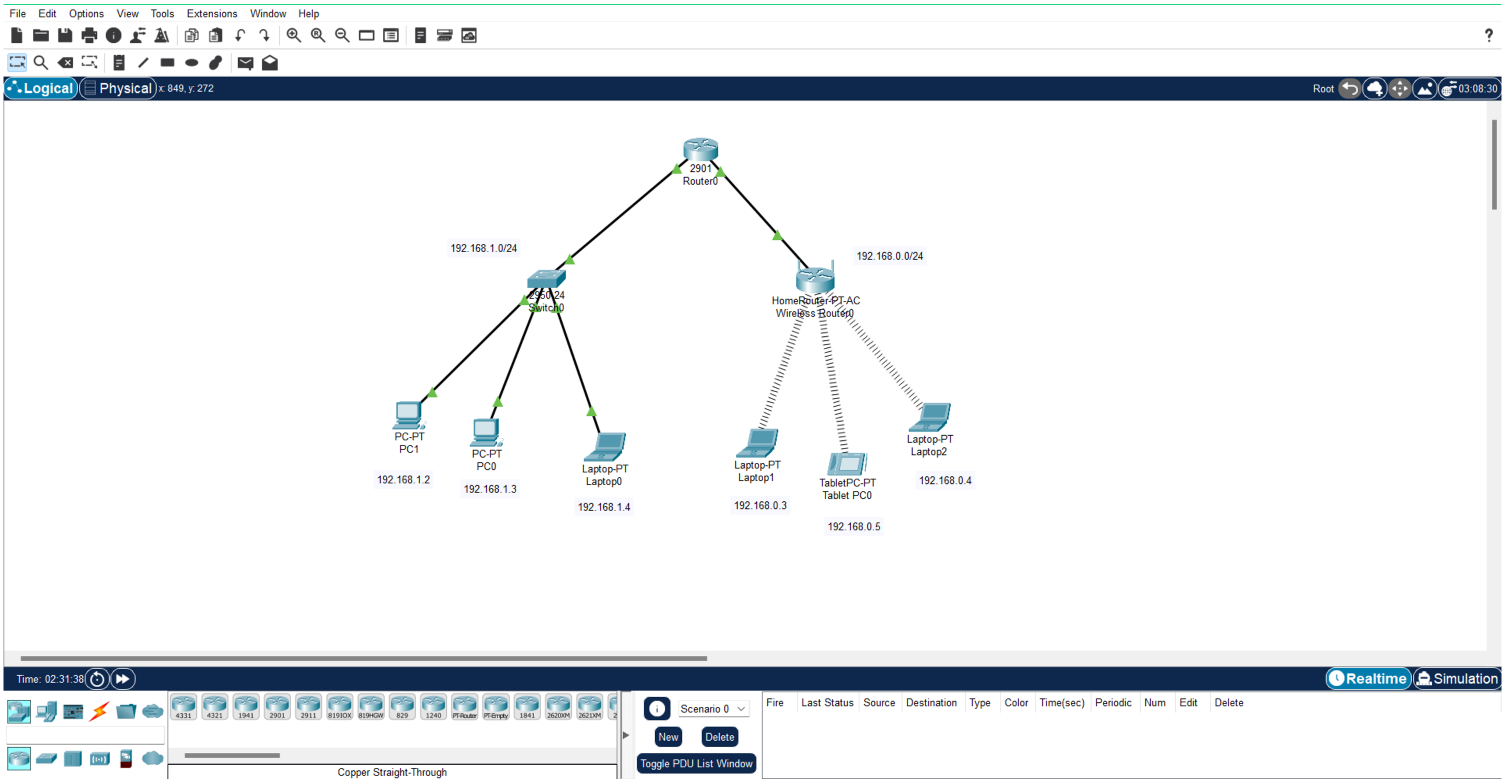
Router 0 gigabit ethernet 0



Router 0 gigabit ethernet 1



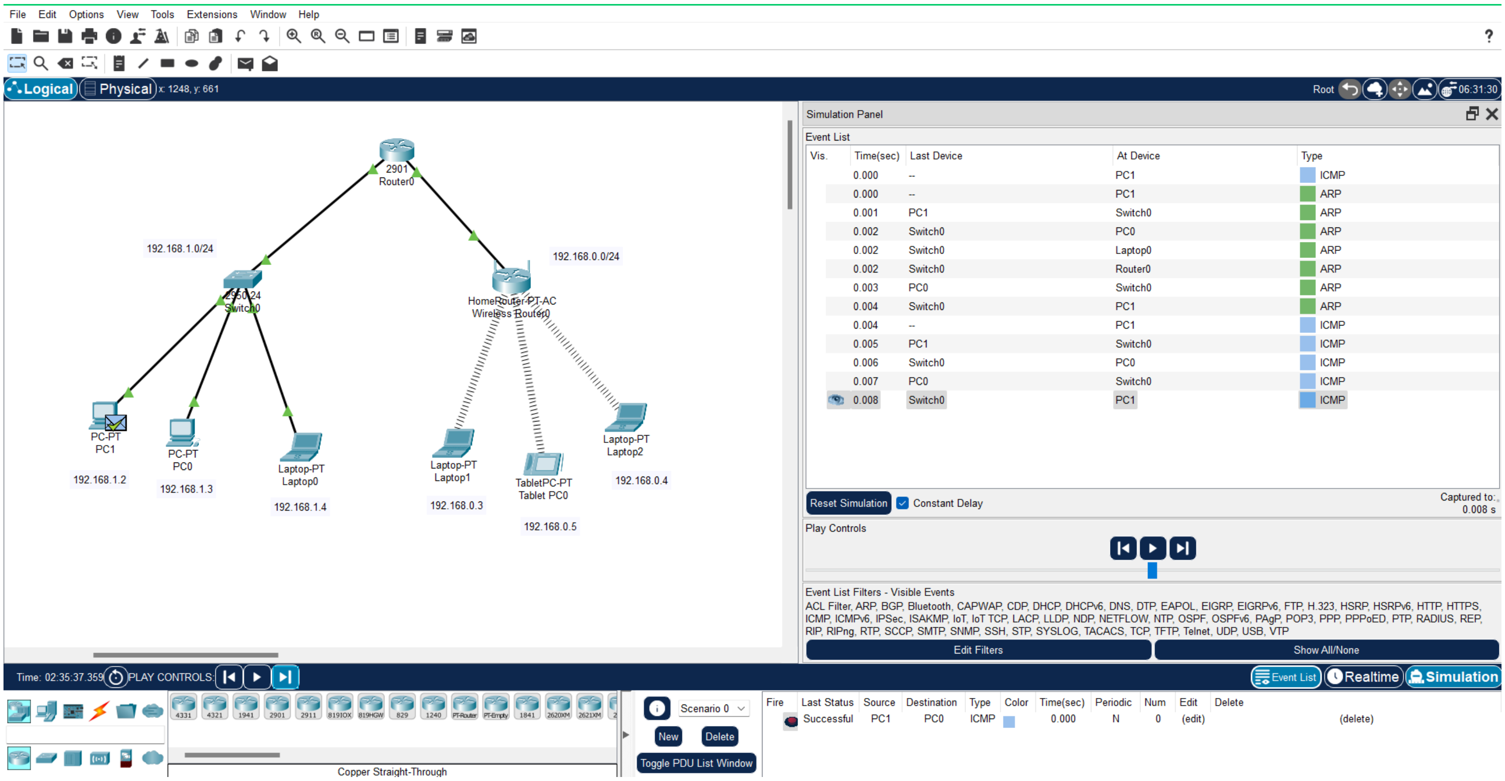
The Whole Network configurations are done



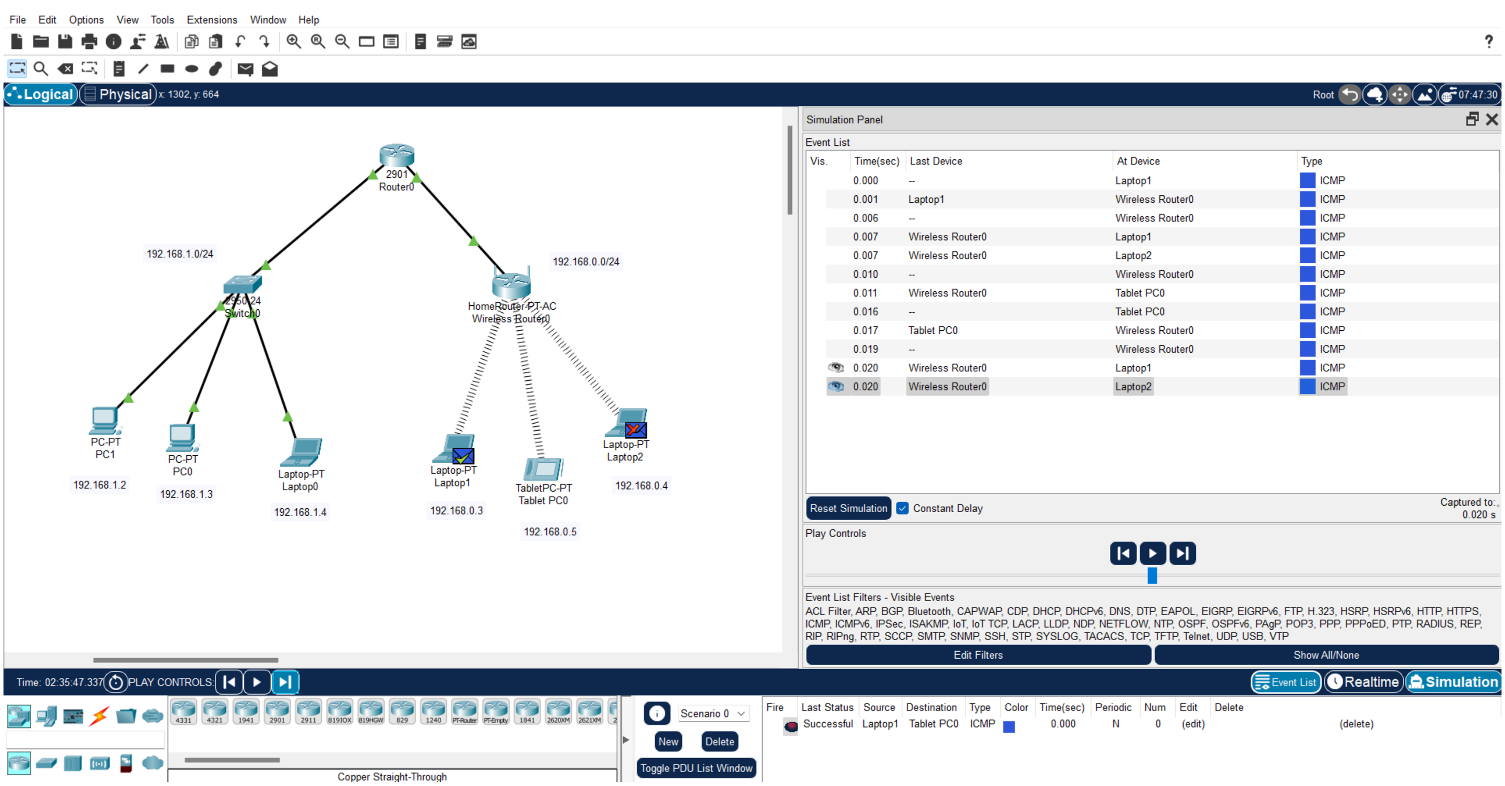
Then I'm going to peek at the messages themselves to see if there are any differences and similarities.

1.

a. **PC1 to PC0**

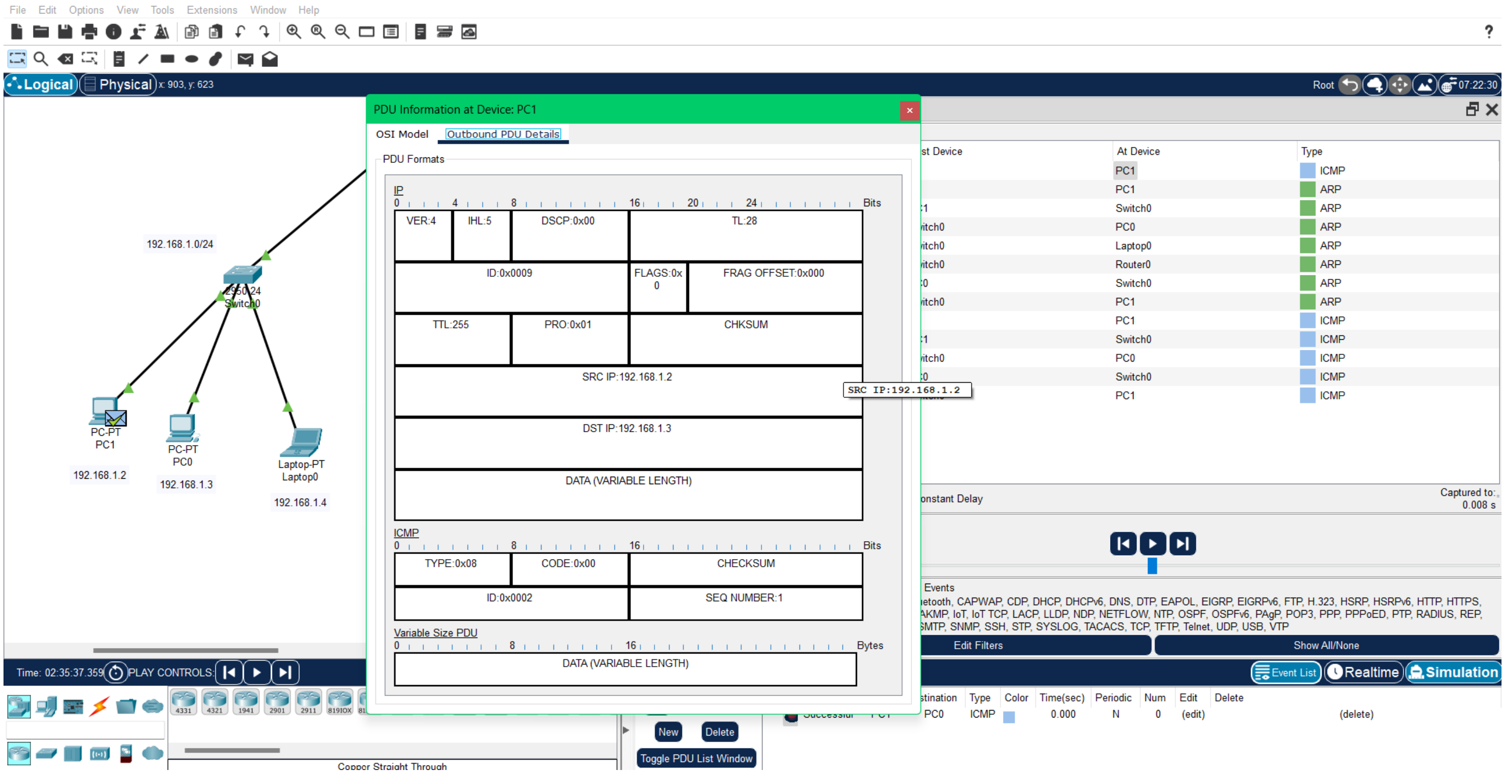


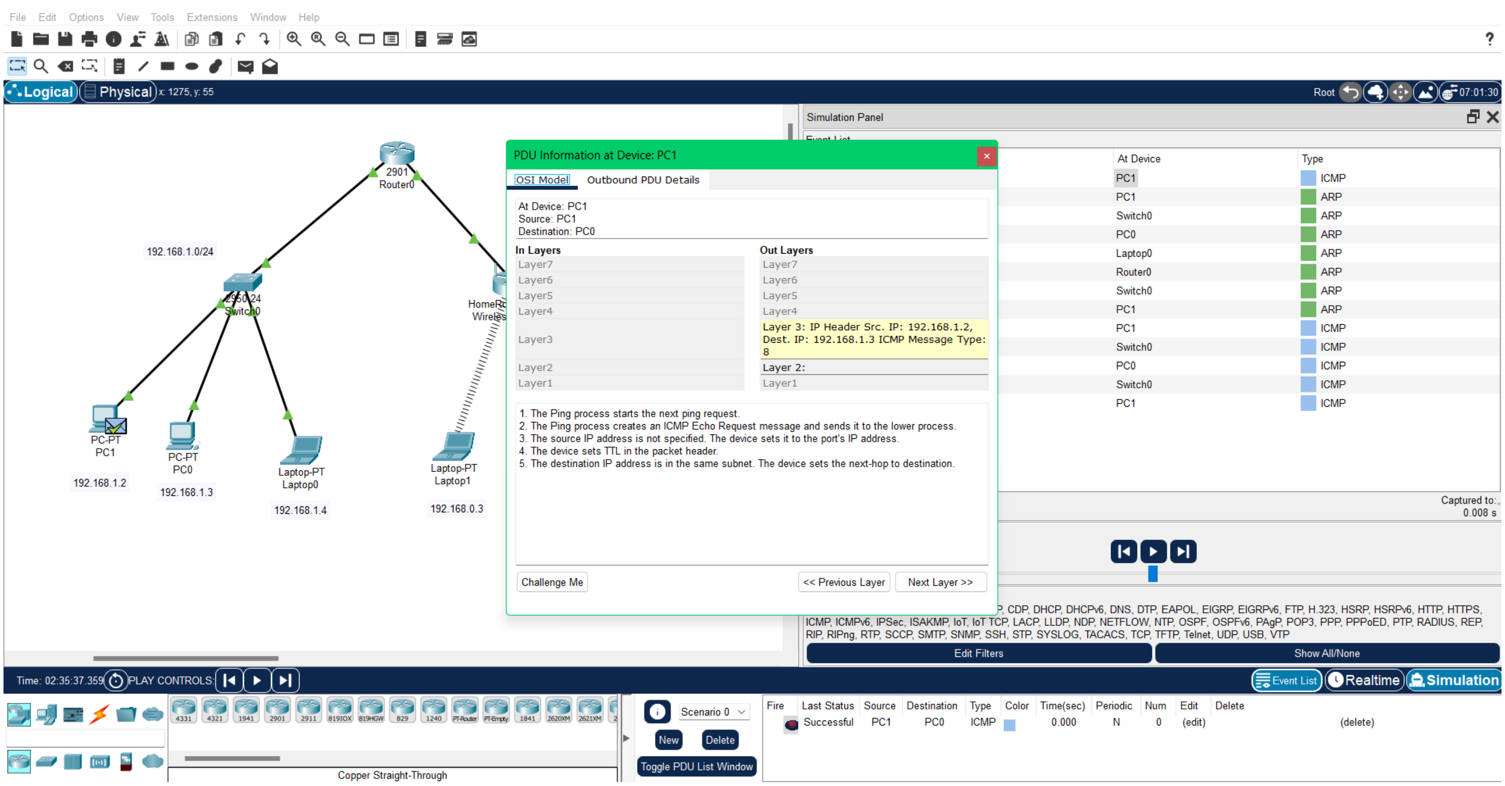
b. **Laptop 1 to tablet 0**



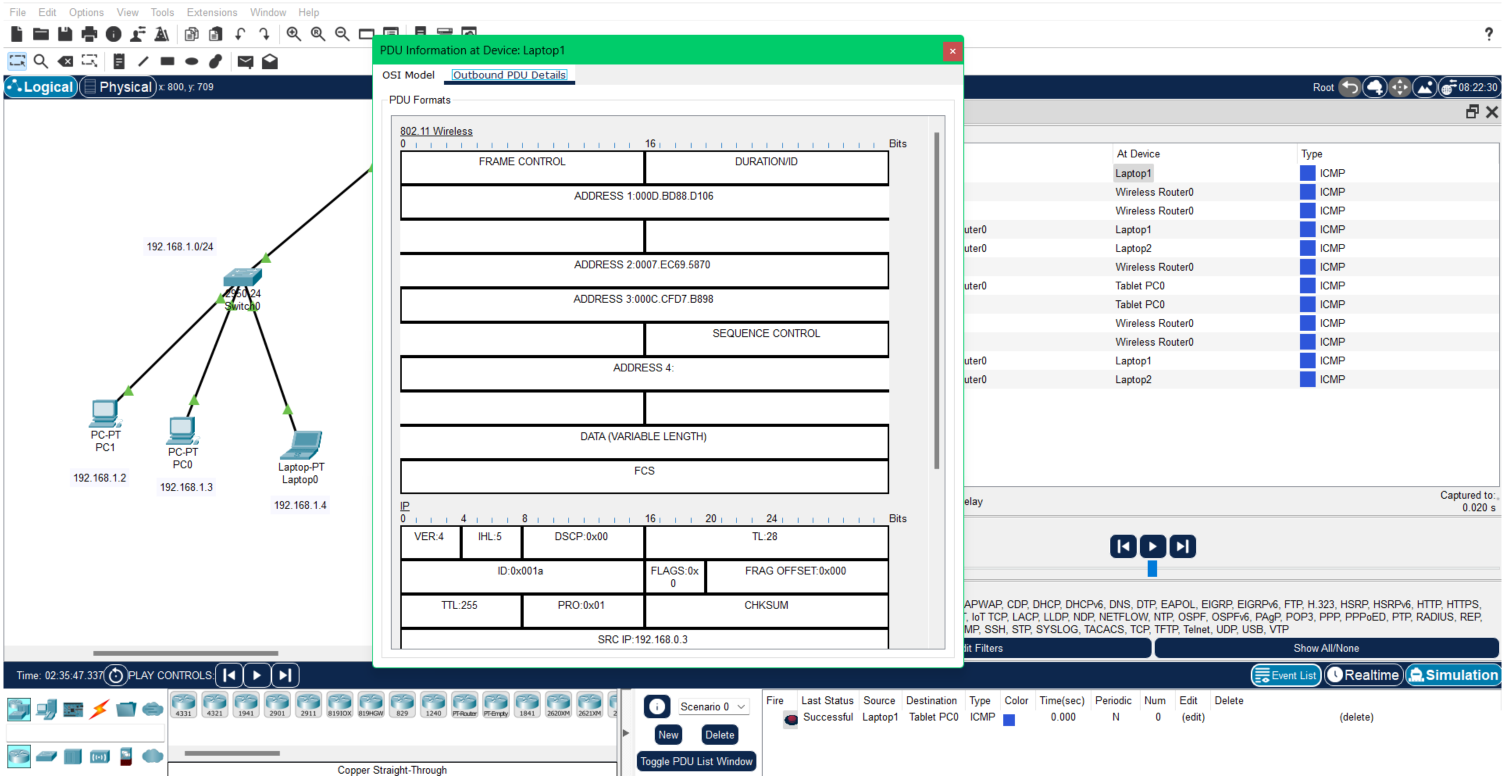
2. The differences and similarities

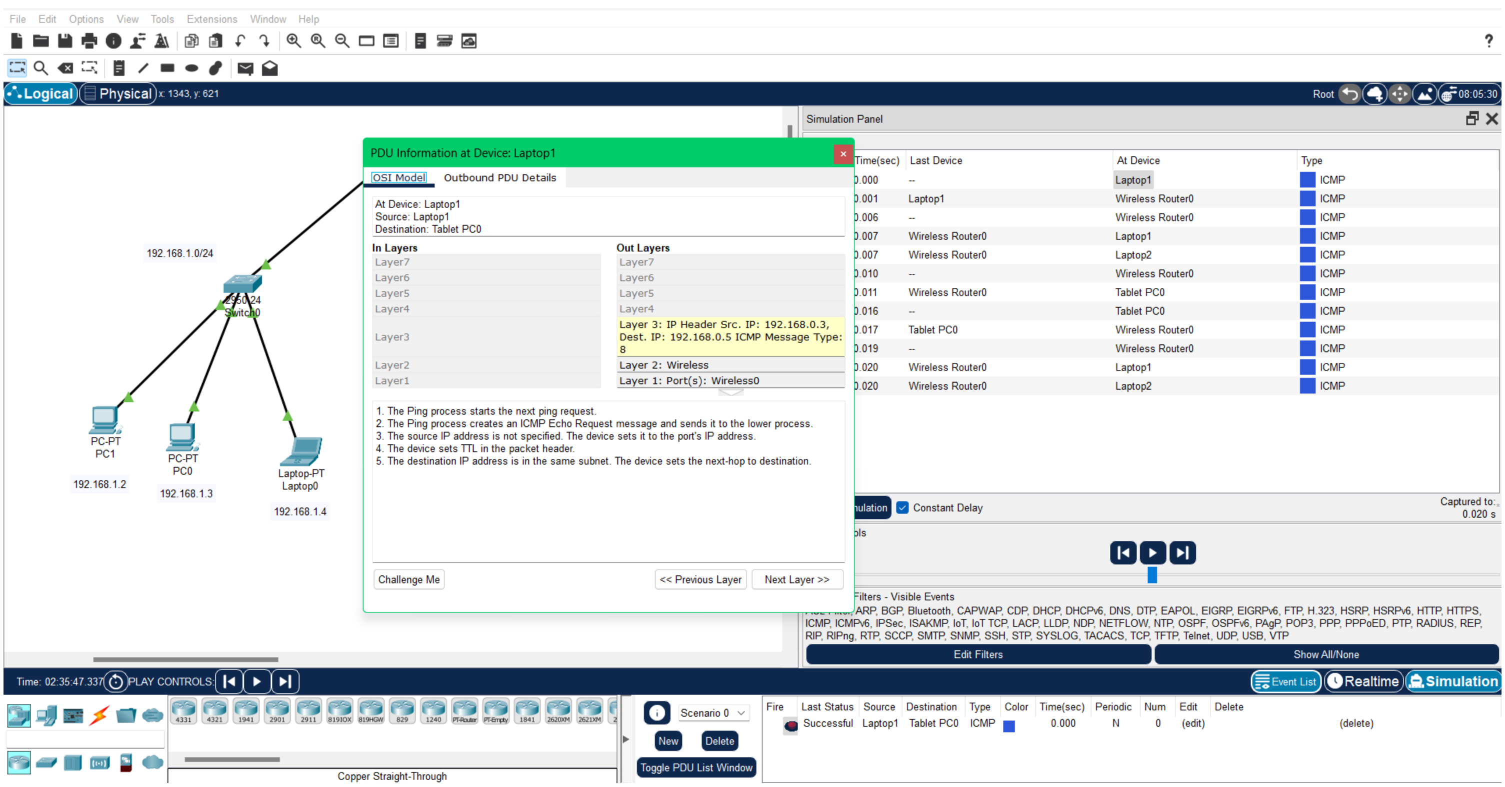
Wired PDU details





Wireless network PDU details





Similarities in both the networks

- Both the wired and wireless PDUs are intended to facilitate communication between network devices.
- Both types of connections rely on network protocols like Ethernet for wired and 802.11 for wireless, which function within the data link layer of the OSI model.
- Both types of networks transmit data in the form of frames. These frames encapsulate higher-level protocol data units, such as IP packets.
- Both networks might involve routing or switching to direct the frames from the source to the destination.
- In both cases, the PDUs are transferred from the source to the destination successfully.

Differences in both the networks

Wired LAN

When I sent a PDU from PC1 to PC0, I observed that the packet traveled directly between the two devices without any intermediate hops. The packet's path was straightforward and consisted of a single hop.

Wireless LAN

In contrast, when sending a PDU from Laptop 1 to Tablet 0, the packet first traveled to the wireless access point before reaching Tablet 0. This added an extra hop in the communication path, making it a two-hop journey.

Wired LAN

Upon inspecting the packet details, I noticed that the Ethernet frame contained only two MAC addresses: the source MAC address from PC1 and the destination MAC address to PC0.

Wireless LAN

When examining the packet details in the wireless LAN scenario, I found three MAC addresses listed in the 802.11 frame: the source MAC address from Laptop 1, the destination MAC address to Tablet 0, and the MAC address of the wireless access point.

Wired LAN

In the wired setup, there were no intermediary devices involved. The packet went straight from one device to the other.

Wireless LAN

The wireless setup involved an intermediary device, the wireless access point. This device played a crucial role in relaying the packet between Laptop 1 and Tablet 0.

Wired LAN

The transmission occurred over a physical Ethernet cable, which I could see visually represented in the Packet Tracer simulation.

Wireless LAN

The transmission happened wirelessly. In Packet Tracer, this was indicated by the packet's movement through the wireless signals to the access point and then to the destination device.

Wired LAN

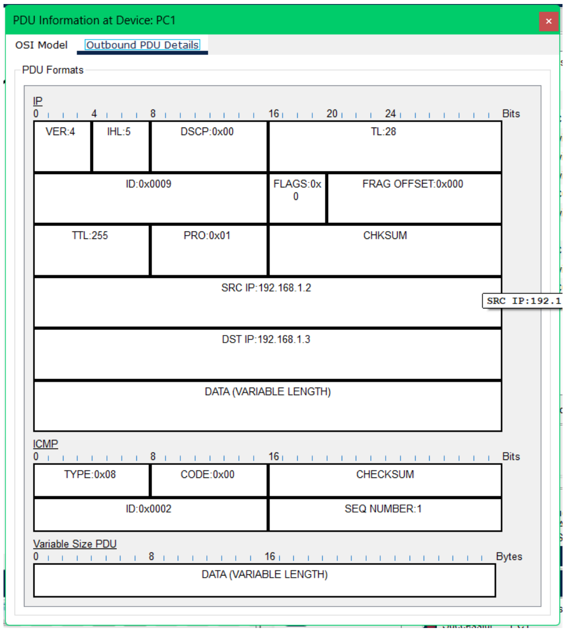
The network interface involved was an Ethernet interface, as shown by the Ethernet symbol in Packet Tracer.

Wireless LAN

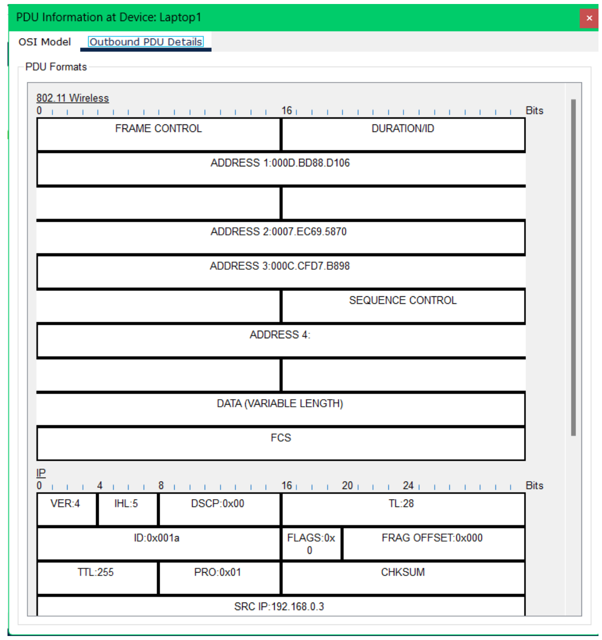
The network interface was a wireless NIC, evident from the wireless signal icon and the interaction with the access point in Packet Tracer.

4.

Wired LAN



Wireless LAN



In the PDUs of the wireless LAN, three MAC addresses were listed: the source MAC address (from Laptop 1), the destination MAC address (to Tablet 0), and an additional MAC address of the wireless access point. The wireless LAN PDU involved an additional step, passing through the wireless access point, resulting in three MAC addresses being listed.

- Source MAC Address: The MAC address of the device that originated the frame (e.g., Laptop 1).
- Destination MAC Address: The MAC address of the final recipient of the frame (e.g., Tablet 0).
- Access Point MAC Address: The MAC address of the wireless access point that bridges the communication between the source and destination devices.

These three MAC addresses facilitate proper routing of the frames in a wireless network, ensuring they reach their intended destination through the intermediary access point.