Above and beyond for task 5.2D

I have included the task 4.1c at the end of this task 5.2d

Going above and beyond for the Application Layer (Module 2)

Application layer protocols used in video streaming

The application layer protocols facilitate the smooth transmission and reception of video content over the internet. Key protocols include:

- **Hypertext Transfer Protocol (HTTP)**
- **Real-Time Protocol (RTP)**
- **Real-Time Streaming Protocol (RTSP)**
- **Dynamic Adaptive Streaming over HTTP (DASH)**
- **HTTP Live Streaming (HLS)**

HTTP

Web communication, including streaming videos, is based on HTTP. It transfers data reliably since it is stateless and uses TCP. The following are the main benefits of video streaming:

Caching: HTTP's ability to integrate with Content Delivery Networks (CDNs) improves video streaming by using edge caching to lower latency and buffering.

Security: HTTPS enables encryption over HTTP, guaranteeing safe delivery of video content.

On the other hand, because it was intended for document transfers rather than continuous data flows, standard HTTP is not optimized for live streaming.

RTP

Particularly for real-time data, such audio and video, RTP was created. It reduces latency using UDP, which is essential for live streaming:

RTP timestamps aid in the synchronization of audio and visual streams.

Identification of Payload Type: Enables one to determine the format of the data being transmitted.

Quality of Service (QoS): To preserve streaming quality in the face of fluctuating network conditions, RTP can cooperate with QoS techniques.

Network issues like as packet loss and jitter can affect RTP's performance and require extra protocols for control and reporting.

RTSP

A network control protocol called RTSP is used in communications and entertainment systems to manage streaming media servers. Media sessions between endpoints are established and managed via RTSP:

Commands: Play, pause, and stop are among the VCR-like commands supported, allowing for interactive streaming.

Session management is the process of overseeing and directing the flow of media during streaming sessions.

For the actual data transport, RTSP frequently collaborates with RTP, handling control commands.

DASH

Using standard HTTP web servers, DASH is an adjustable bitrate streaming technology that allows for high-quality media streaming over the internet. Important characteristics consist of:

Segmented Content: To enable adaptive streaming, media files are divided into smaller chunks.

Manifest File: The client is guided on which parts to download and play by a manifest file, also known as an MPD (Media Presentation Description).

Adaptive bitrate: Depending on the state of the network, clients can transition between various quality levels (bitrates), resulting in the best possible viewing experience with the least amount of buffering.

DASH can simply connect with current infrastructure and take use of HTTP-based content delivery because it uses conventional HTTP servers.

HLS

Apple developed the HLS media streaming protocol, which is comparable to DASH but differs in a few significant ways:

Chunked Transfer: HLS splits material into smaller HTTP-based file parts, just like DASH does.

M3U8 Playlist: Directs the client during streaming by listing accessible media segments from an M3U8 file.

Compatibility: It is a popular option for content providers targeting Apple ecosystems because it is widely supported across Apple devices and browsers.

Additionally, HLS allows adjustable bitrate streaming, which improves user experience on a range of network situations.

Protocol Interaction and Integration

In actuality, a combination of these protocols is frequently used for video streaming:

For real-time, interactive applications like live sports broadcasting, RTSP and RTP are frequently combined.

Because of their adaptive streaming features and dependency on HTTP, which enables them to take advantage of CDNs, DASH and HLS are frequently chosen for Video on Demand (VoD) services.

In order to distribute media assets more effectively and closer to end users, CDNs use HTTP/HTTPS, which lowers latency and speeds up load times.

Emerging Trends and Protocols

Advancements continue to evolve video streaming protocols:

WebRTC, or Web Real-Time Communication, is used in applications such as video conferencing and allows peer-to-peer streaming directly between browsers, eliminating the need for middle servers.

Google created QUIC (Quick UDP Internet Connections), which decreases connection establishment time and enhances congestion control to address TCP's inadequacies, especially for streaming.

A thorough understanding of video streaming application layer protocols reveals a complex environment in which several protocols frequently cooperate to deliver fluid, high-quality video content. This interaction highlights the crucial role that application layer protocols play in the current digital media ecosystem by ensuring reliable, flexible, and effective video distribution over a wide range of network circumstances and devices.

Additional resources I referred to

1. *The Application Layer: Video Streaming*. (n.d.). Srinivas Narayana.

   https://people.cs.rutgers.edu/~sn624/352-S22/lectures/08-video-streaming.pdf

2. Ruether, T. (2023, June 8). *Streaming protocols: Everything you need to know (Update)*. Wowza.

   https://www.wowza.com/blog/streaming-protocols

3. R, E. (2022, September 15). *Video streaming protocols: What are they & how to choose the best one*.

   https://getstream.io/blog/streaming-protocols/

Active class 7: Who is Instructing What (Module 5)

Identify three different widely used routing protocols.

3 Widely Used Routing Protocols

- **Routing Information Protocol (RIP)**
- **Open Shortest Path First (OSPF)**
- **Border Gateway Protocol (BGP)**

Feature	RIP	OSPF	BGP
Protocol Type	Distance-vector	Link-state	Path-vector
Metric	Hop Count	Cost (bandwidth delay)	Path attributes
Algorithm	Bellman-Ford	Dijkstra	Path vector algorithm
Max Hop Count	15	Unlimited	Not applicable
Convergence Speed	Slow	Fast	Slow
Scalability	Low	High	Very high
Resource Usage	Low	Moderate to high	Moderate to high
Configuration	Simple	Complex	Very Complex
Use case	Small networks	Large enterprise networks	Internet and large-scale inter-AS routing

Explanation on each protocol

RIP

RIP functions similarly to a basic messenger, assisting computers within a network to figure out the most effective ways of exchanging data. It keeps track of how many "hops"—or steps—there are between two computers. Consider hops as roadside checkpoints. If a message has to transit through more than 15 checkpoints, it won't go through because RIP thinks that's too far.

Benefits: RIP is well-suited for smaller, more straightforward networks because to its ease of configuration and comprehension. Because of its limited resource consumption, it works well in settings with limited memory and computing power.

Drawbacks: The largest network size that RIP can support is limited by its maximum hop count of 15, which is one of its main drawbacks. Furthermore, brief routing loops and inefficient routing may result from its slow convergence time.

OSPF

Like GPS mapping roads, OSPF is like a more advanced messenger that covers the entire network. Not only does it know the total number of steps (or hops), but it also understands the quality of those steps (taking into account things like speed limits on roadways). It determines the quickest and most cost-effective route for messages to travel using a technique known as Dijkstra's algorithm.

Benefits: Because OSPF is link-state based and uses the Dijkstra algorithm, it is very scalable and offers quick convergence. It enables more effective and dependable routing decisions by supporting a variety of indicators for identifying the optimal path. With the idea of regions, OSPF also facilitates hierarchical network design, improving management and scalability.

Drawbacks: Maintaining entire network topology information can lead to resource use issues and complexity in OSPF configuration. Compared to RIP, it takes more CPU power and memory, which makes it less appropriate for tiny, basic networks.

BGP

BGP is comparable to the internet's international travel guide. It facilitates communication and route sharing between many big networks, often known as autonomous systems, or ASes. To select the optimal way, BGP considers a number of factors in addition to hops and speed, such as customs regulations, tolls, and aircraft connections.

Benefits: BGP manages huge amounts of routing data between several autonomous systems, making it crucial for internet routing. Administrators can create intricate routing policies based on a variety of criteria thanks to its sophisticated policy-based routing capabilities. The internet's backbone, BGP is unparalleled in its scalability and durability.

Drawbacks: BGP requires extensive knowledge and experience due to its complex configuration and operation. Compared to OSPF, it has a slower convergence time, which might be problematic in situations when quick network changes are necessary.

Extra resources I referred to

1. GeeksforGeeks. (2024, January 29). *Border Gateway Protocol (BGP)*. GeeksforGeeks. https://www.geeksforgeeks.org/border-gateway-protocol-bgp/
2. GeeksforGeeks. (2023a, February 22). *Open Shortest Path First (OSPF) Protocol fundamentals*. GeeksforGeeks. https://www.geeksforgeeks.org/open-shortest-path-first-ospf-protocol-fundamentals/
3. GeeksforGeeks. (2023b, May 9). *Routing Information Protocol (RIP)*. GeeksforGeeks. https://www.geeksforgeeks.org/routing-information-protocol-rip/

Active class 8: Internet is full of Network Protocols (Module 5)

1.

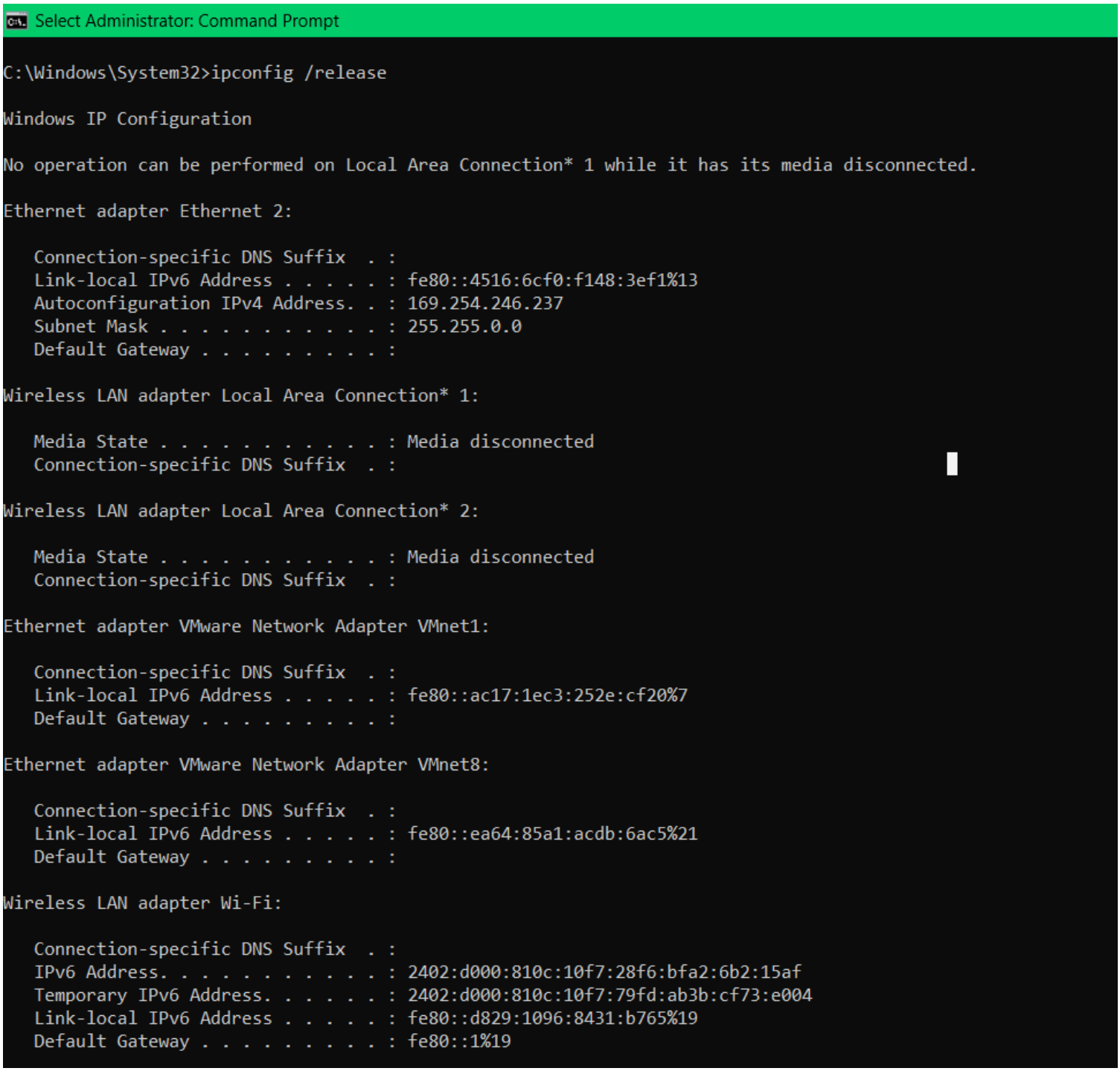
Steps to Capture DHCP Packets in Wireshark

Open Wireshark: Launch Wireshark on my PC.

Select the Network Interface: I Chose the network interface that I want to capture packets on (e.g., Wi-Fi or Ethernet adapter).

Start Capturing: Then I clicked on the start capture button (the shark fin icon).

Command Line: Then I entered the commands **ipconfig /release** to release the IP addresses of my computer, then entered the commands **ipconfig /renew** to get new IP adderesses, then to confirm I typed the ipconfig /all.

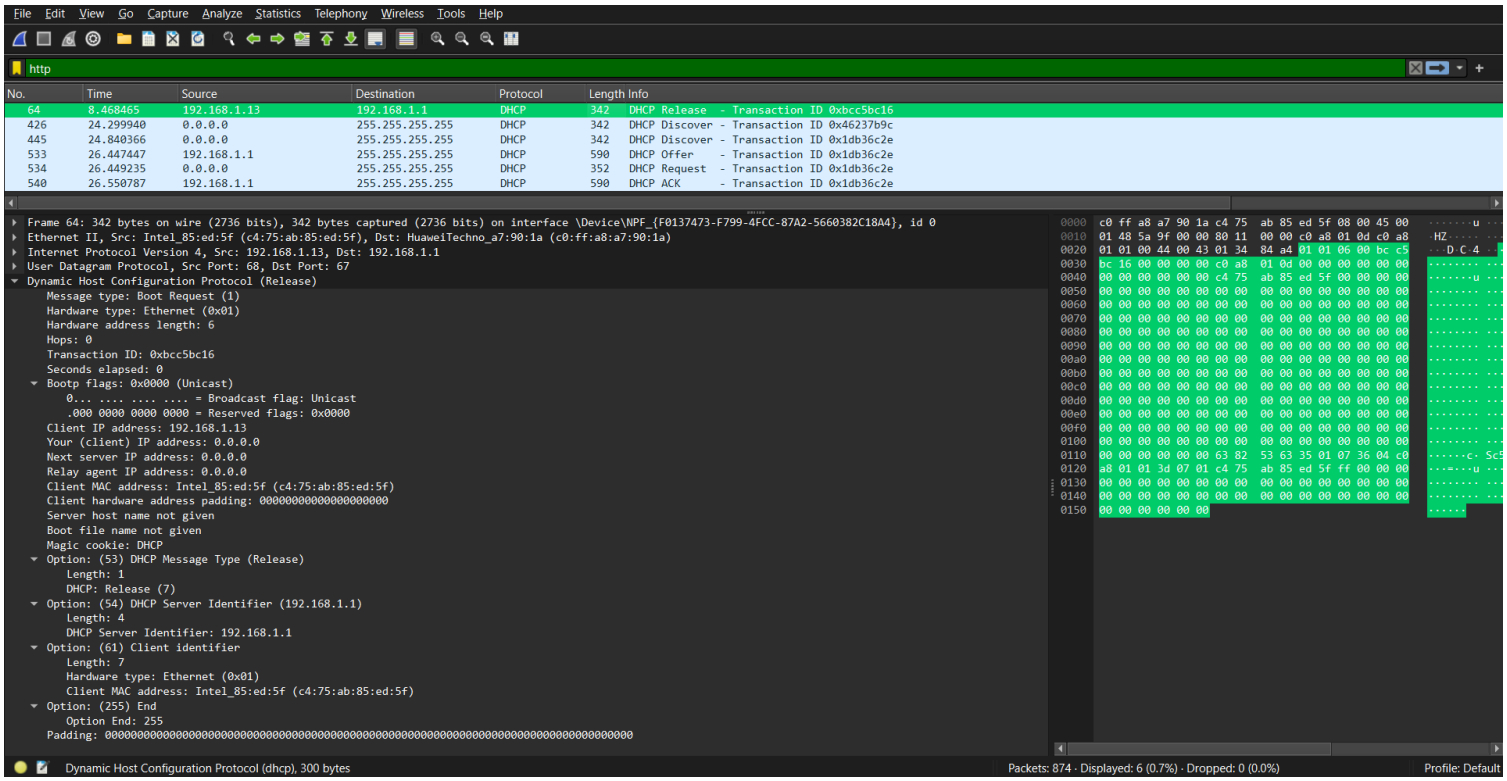


```
C:\Windows\System32>ipconfig /renew

Windows IP Configuration

No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.
An error occurred while renewing interface Wi-Fi : The operation was canceled by the user.


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4516:6cf0:f148:3ef1%13
   Autoconfiguration IPv4 Address. . : 169.254.246.237
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ac17:1ec3:252e:cf20%7
   IPv4 Address. . . . . . . . . . . : 192.168.125.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ea64:85a1:acdb:6ac5%21
   IPv4 Address. . . . . . . . . . . : 192.168.177.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2402:d000:810c:10f7:28f6:bfa2:6b2:15af
   Temporary IPv6 Address. . . . . . : 2402:d000:810c:10f7:79fd:ab3b:cf73:e004
```

Going back to Wireshark: Now I stop the capture and enter the filter dhcp to find out the following sequence of DHCP messages

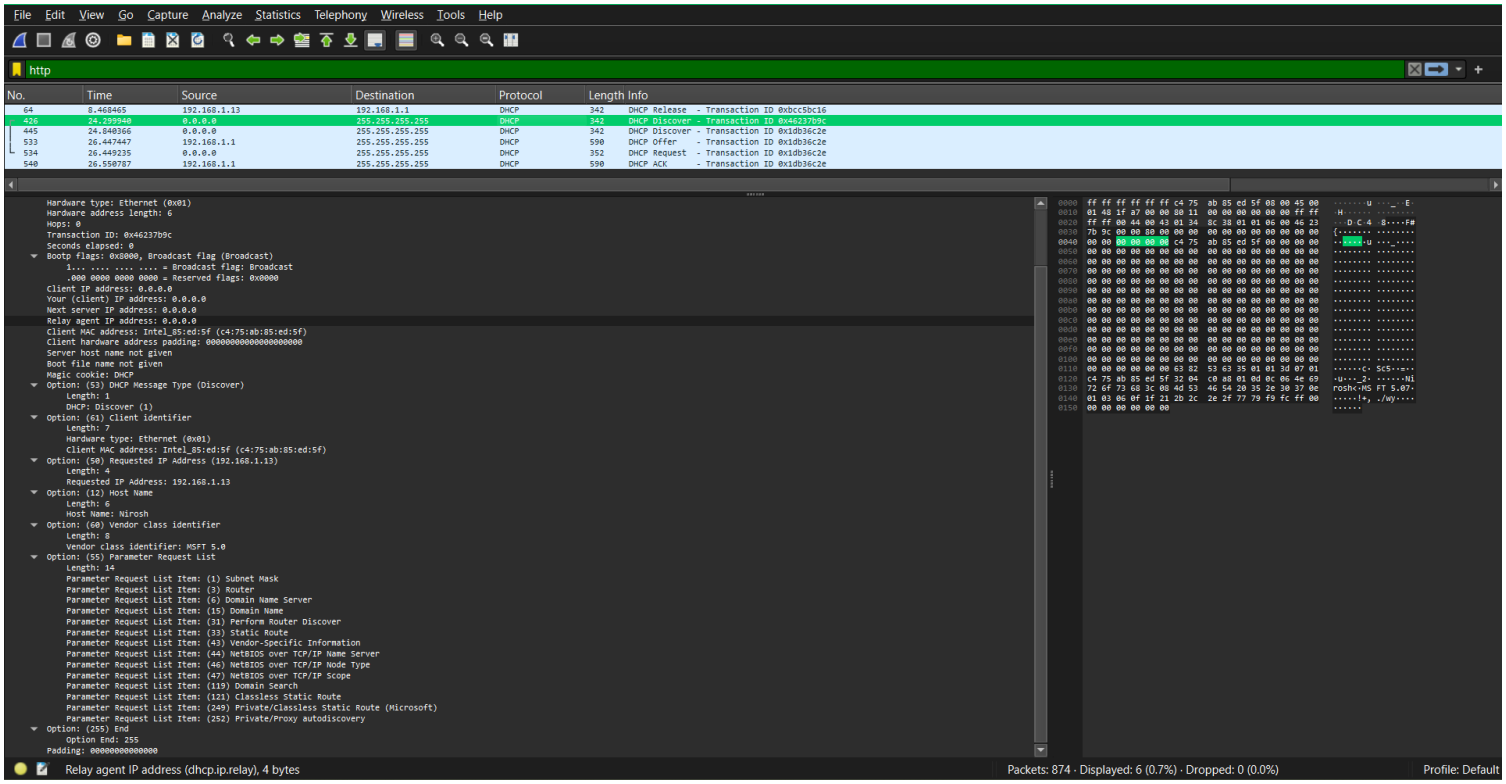
DHCP Release:

This was the message that indicates that the old address is released



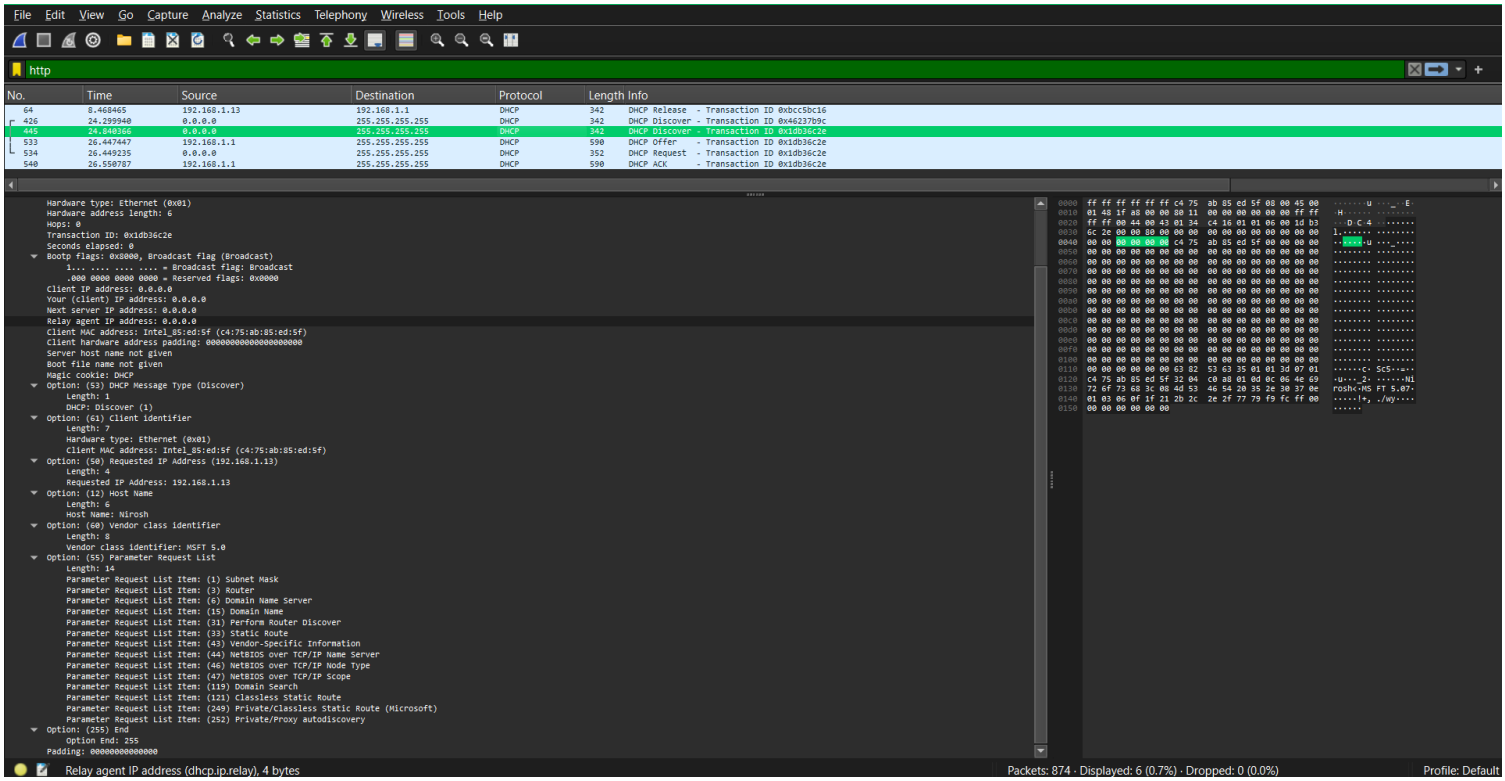
DHCP Discover:

A device must send and receive a sequence of DHCP (Dynamic Host Configuration Protocol) signals in order to connect to a network and obtain an IP address. The DHCP Discover message initiates the procedure. Here, the device looks for any DHCP servers that can provide it with an IP address by broadcasting a message. Because the device does not yet have an IP address, this message does not have a defined destination.



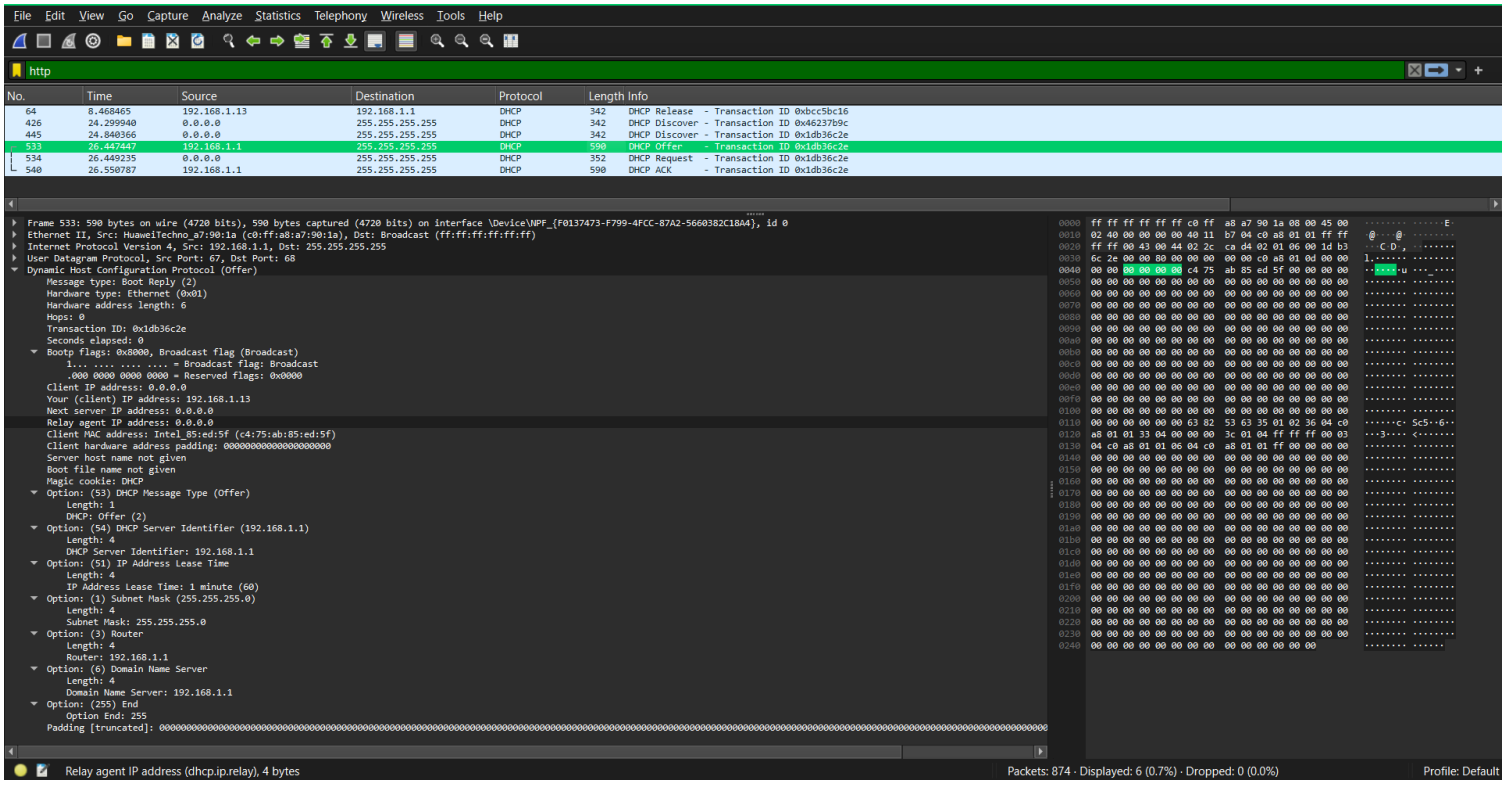
DHCP Offer:

A DHCP server that received the Discover message then sends the DHCP Offer message. The IP address for the device is proposed by the server in response, along with some other details like the subnet mask and the lease length (the amount of time the device can use this IP address).



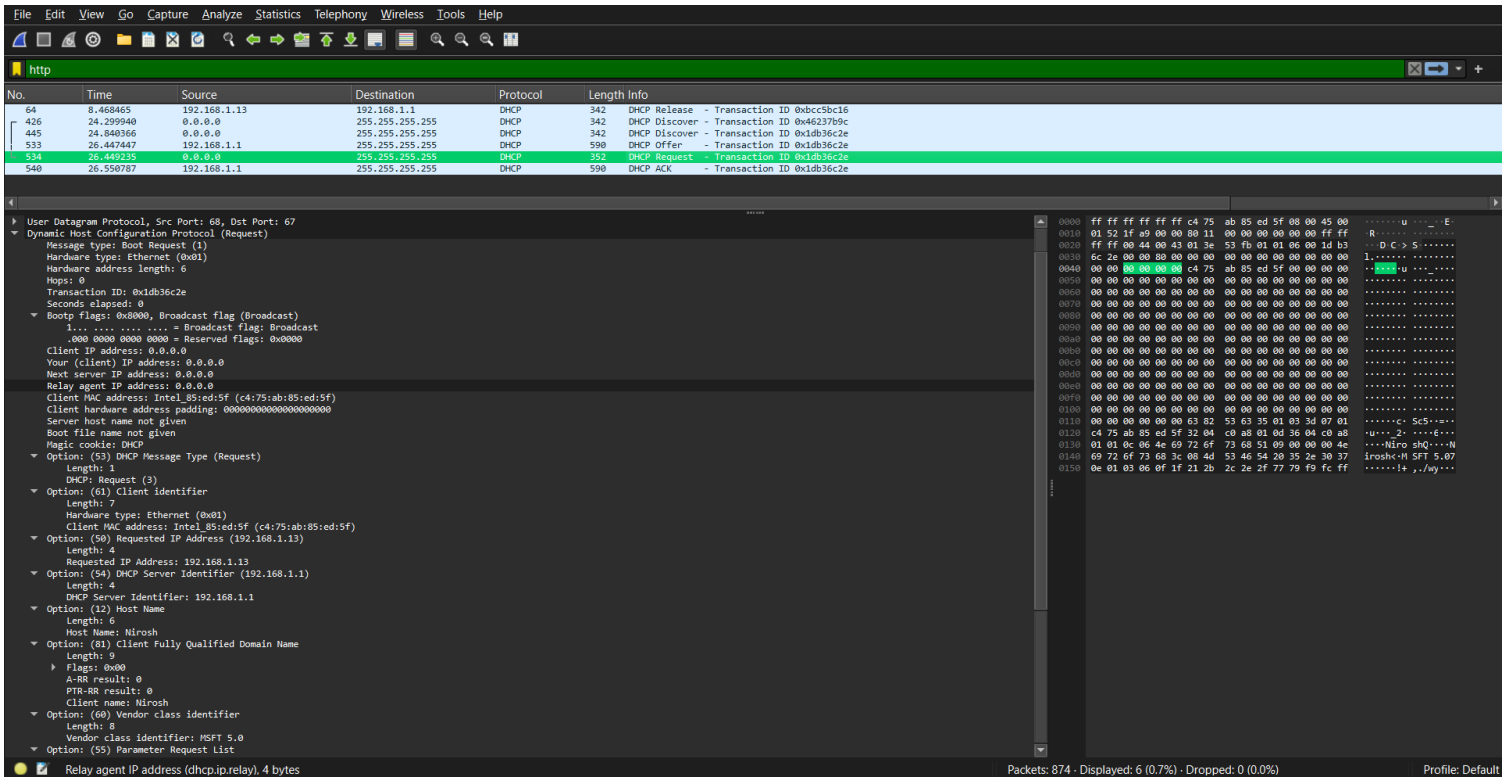
DHCP Request:

After that, the device sends back a DHCP Request message. To make sure that every DHCP server sees it, this message is also broadcast. According to the Request message, the device is notifying other servers that it is accepting an offer from a specific server and is requesting the IP address that server is offering.



DHCP Acknowledgment (ACK):

Finally, a DHCP Acknowledgment (ACK) message from the DHCP server verifies the lease. The IP address, subnet mask, default gateway, and lease duration are among the last assignment parameters included in this message. With the IP address provided, the device can now connect to the network and exchange messages.



To sum up, the device searches for a server by sending out a Discover message; the server responds with an Offer; the device asks the IP address that is offered; and the server verifies by sending out an ACK. This process makes sure the device is assigned the correct IP address and configuration when it connects to the network.

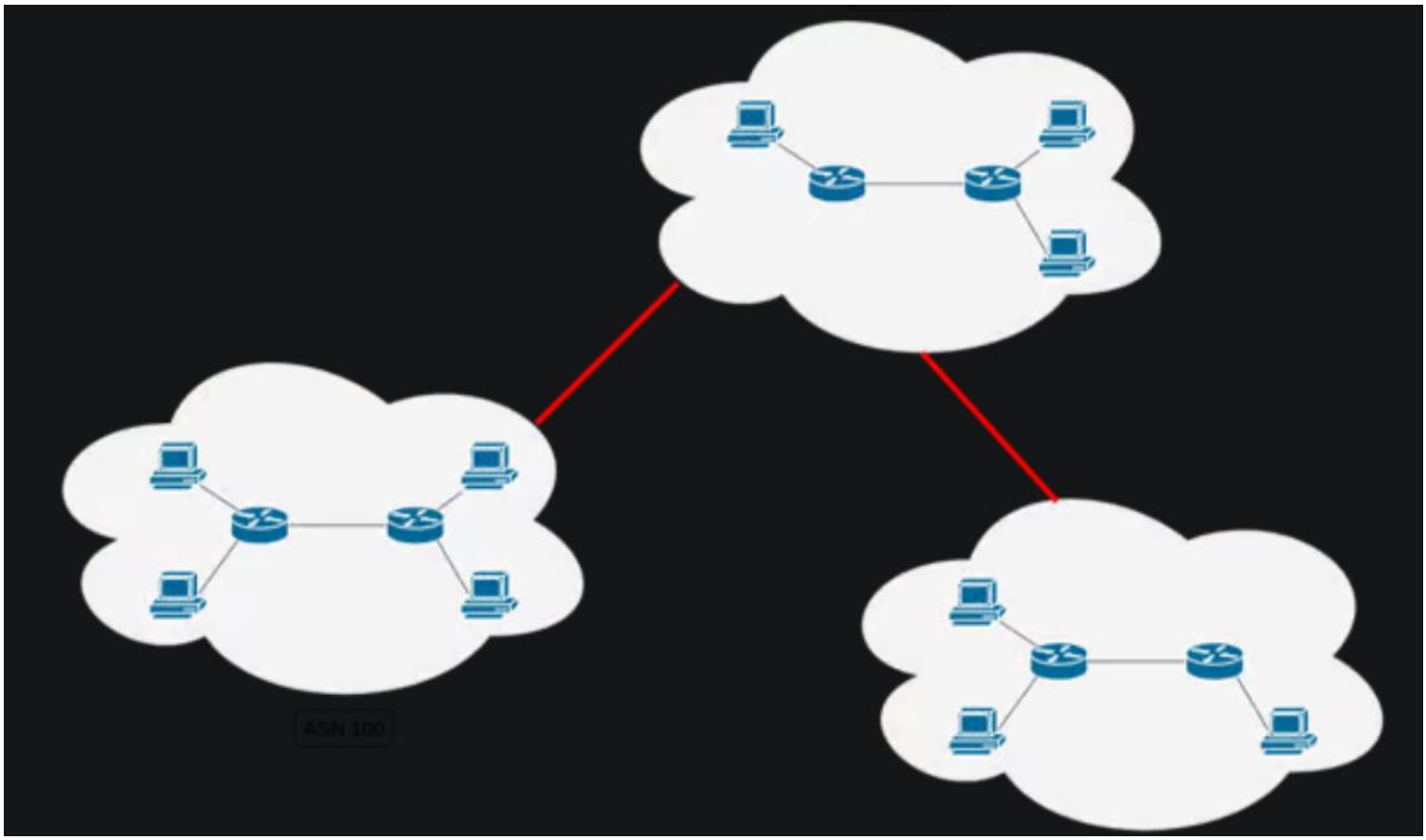
2.

Inter-AS Protocols

These protocols are used to route traffic between different autonomous systems (ASes), which are large networks or groups of networks under a common administration. They operate between independent networks, often with different policies and management. They also provide mechanisms for complex routing policies and agreements between autonomous systems.

Example:

Border Gateway Protocol (BGP): The standard protocol for inter-AS routing on the Internet is called BGP. In order to govern packet routing across several autonomous systems on the internet, BGP takes into account path properties, policies, and the avoidance of routing loops.



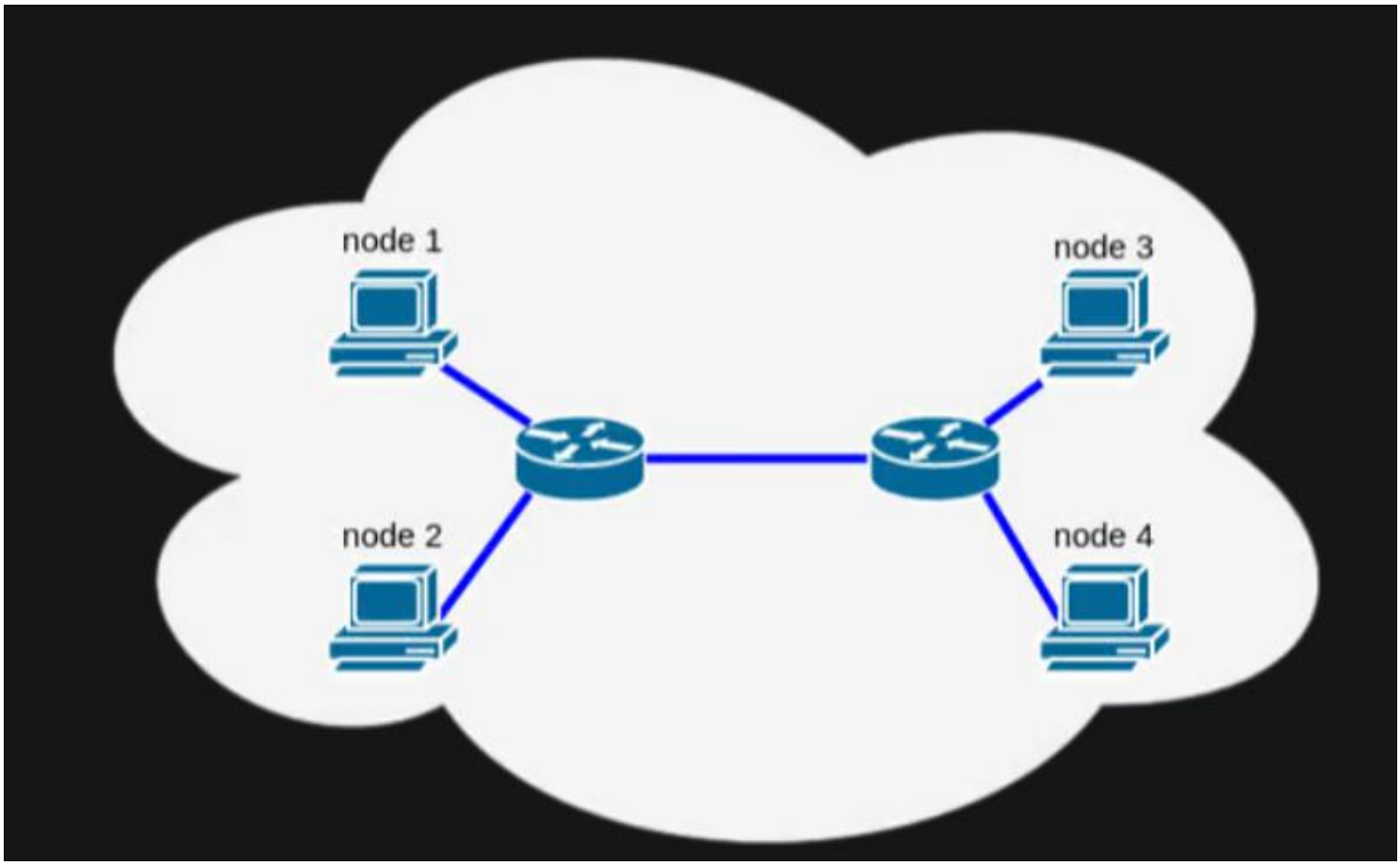
Intra-AS Protocols

These protocols are used to route traffic within a single autonomous system. They operate within a single, cohesive network under a single administrative domain. They focus on efficient routing within the AS, often prioritizing metrics like shortest path, bandwidth, or delay.

Example:

Open Shortest Path First (OSPF): Dijkstra's method is used by this link-state routing protocol to determine the shortest path within an AS. It is appropriate for large enterprise networks since it is rapidly convergent and extremely scalable.

Enhanced Interior Gateway Routing Protocol (EIGRP): Cisco-only protocol called EIGRP combines elements of distance-vector and link-state protocols. It is renowned for being effective and converging quickly.



Large-scale, autonomous network routing is managed using inter-AS protocols like BGP, which also provide complex policy control. With the use of metrics to guarantee the best possible path selection, intra-AS protocols such as OSPF and EIGRP concentrate on effective routing within a single network. Comprehending these protocols helps the efficient design and management of internal network operations as well as large-scale internet routing by network managers.

Some external resources I referred to

1. Educative. (n.d.). *What is the difference between inter-AS and intra-AS routing?* https://www.educative.io/answers/what-is-the-difference-between-inter-as-and-intra-as-routing
2. GeeksforGeeks. (2023b, May 3). *Differences between Intradomain and Interdomain Routing*. GeeksforGeeks. https://www.geeksforgeeks.org/differences-between-intradomain-and-interdomain-routing/
3. *Differences between InterDomain Routing and IntraDomain*. (n.d.). https://www.tutorialspoint.com/differences-between-interdomain-routing-and-intradomain

Summary and Reflection for Above and Beyond Tasks in Class 7 and 8

Summary

In summary, the above-and-beyond assignments in Classes 7 and 8 concentrated on complex subjects related to network protocols and routing. In Class 7, we investigated contemporary routing algorithms and contrasted static and dynamic routing protocols, going over each one's benefits and drawbacks. In class, we used Wireshark to investigate DHCP by recording and going over the series of DHCP messages that are sent back and forth as IP addresses are being assigned. Furthermore, we discussed the differences and use cases of the two types of routing protocols—intra-AS and inter-AS (Autonomous System)—giving instances of each.

reflection

These assignments gave me a thorough grasp of intricate networking principles. In Class 7, the advantages of automated routing decisions in dynamic protocols—like better scalability and less manual configuration—were emphasized through a comparison of the two types of routing protocols. At the same time, the benefits of static routing in small networks were recognized. Examining current routing algorithms made clear how crucial effective routing techniques are to maintaining network performance and reliability.

In Class 8, I learned how to analyze DHCP packets in Wireshark, which improved my understanding of the dynamic IP allocation process and helped me address network connectivity difficulties. My perspective on routing in large-scale networks has been widened by my understanding of the distinctions between intra-AS and inter-AS routing protocols, which emphasize the necessity of employing distinct strategies to handle internal and exterior network traffic.

My understanding of network management and diagnostics has been enhanced by these advanced exercises, which highlight the vital role that effective routing and IP address management play in the dependability and performance of networks.

Active class 9: Data-link Layer (Module 6)

Security issues associated with ARP

On a local network, IP addresses are mapped to MAC addresses via the Address Resolution Protocol (ARP). Even while ARP is necessary for network communication, attackers can take advantage of a number of security flaws in it.

The fact that ARP lacks any internal security mechanisms to confirm the legitimacy of ARP messages is one of its main problems. Because of this, it is open to different kinds of attacks:

ARP Poisoning (ARP Spoofing):

An attacker uses ARP spoofing to trick the network by sending fake ARP messages. These communications link an authorized device's IP address (such a gateway or another computer) to the attacker's MAC address. The attacker can then use this information to intercept, alter, or stop data meant for the authorized device. In the end, the attacker deceives the network into sending information to their device rather than the right one.

prevention:

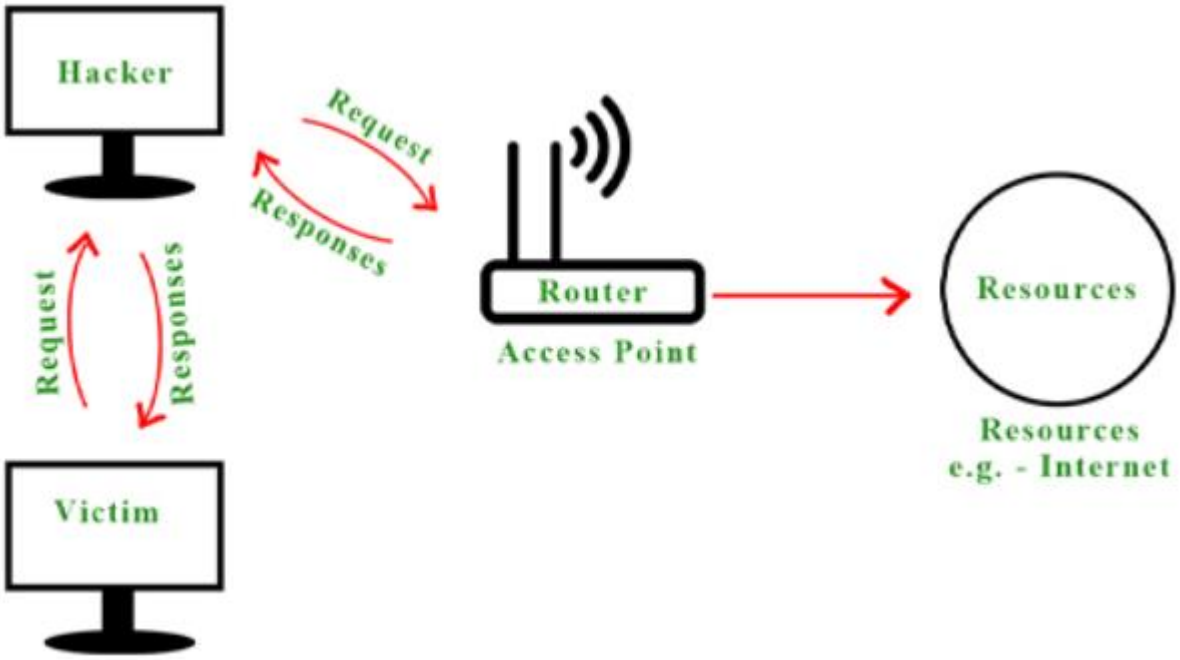
Static ARP Entries: Manually configuring ARP entries on critical devices can prevent unauthorized changes.

Man-in-the-Middle Attack:

An attack by a man-in-the-middle (MITM) can result from ARP spoofing. Here, the attacker secretly positions themself between two communication devices. This gives the attacker the ability to intercept and maybe manipulate the data being transferred. For example, during an MITM attack, private data such as financial information or passwords may be taken.

prevention:

Encryption: Using secure communication protocols like HTTPS and VPNs can help protect data even if ARP spoofing occurs.

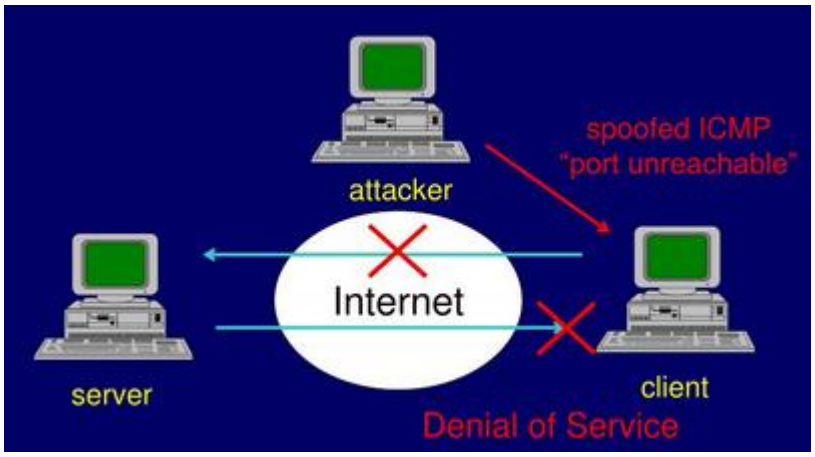


Denial of Service (DoS) Attack:

DoS attacks can also be launched by attackers via ARP spoofing. The attacker can overload the network by flooding it with fake ARP messages, which will lead to legitimate devices receiving inaccurate ARP information. This may interfere with regular communication and cause the network to lag or become unusable for authorized users.

prevention:

ARP Inspection: Some advanced network switches offer dynamic ARP inspection, which validates ARP packets before they are processed.



Some external resources I referred to

1. Molenaar, R. (2022, January 12). *DAI (Dynamic ARP Inspection)*. NetworkLessons.com. https://networklessons.com/switching/dai-dynamic-arp-inspection
2. *Denial of Service - OWASP Cheat Sheet series*. (n.d.). https://cheatsheetseries.owasp.org/cheatsheets/Denial_of_Service_Cheat_Sheet.html
3. GeeksforGeeks. (2021a, April 15). *MITM (Man in The Middle) Attack using ARP Poisoning*. GeeksforGeeks. https://www.geeksforgeeks.org/mitm-man-in-the-middle-attack-using-arp-poisoning/
4. Grimmick, R. (2022, August 4). ARP Poisoning: What it is & How to Prevent ARP Spoofing Attacks. *ARP Poisoning*. https://www.varonis.com/blog/arp-poisoning

Summary and Reflection for Above and Beyond Tasks in Class 9

Summary:

The objectives in Class 9 that went above and beyond focused on recognizing and comprehending security flaws in the Address Resolution Protocol (ARP). We talked about and looked at the effects of ARP attacks on network security, including ARP spoofing and ARP poisoning. We also looked into possible mitigation techniques to shield networks from these security flaws.

reflection

This task played a vital role in drawing attention to the security vulnerabilities related to the data link layer. I was able to obtain a better grasp of how attackers can use ARP vulnerabilities to intercept or modify network traffic by recognizing the many forms of ARP attacks. In order to protect networks from these types of attacks, the implementation of strong security measures—such as static ARP entries, dynamic ARP inspection, and ARP spoofing detection tools—was highlighted in the discussion of mitigation options.

This exercise emphasized how important it is to remain vigilant and take preventative action when it comes to network security, especially at the data link layer where even seemingly straightforward protocols can become targets of sophisticated assaults. It underlined how crucial it is for cybersecurity professionals to always be learning and adapting in order to successfully defend network infrastructure against changing threats.

Active class 10: Physical Connections and Protocols (Module 7)

What is an Ethernet cable

A high-speed wired network connection between two devices is made possible via an Ethernet cable. Twisted pair conductors make up the four pairs that make up this network cable. The RJ45 connection is used for data transfer at both ends of the wire.

Cat 5, Cat 5e, Cat 6, and UTP cables are the different types of Ethernet cables. While Cat 5e and Cat 6 cables can support Ethernet networks operating at 10/100/1000 Mbps, Cat 5 cable can only support networks operating at 10/100 Mbps.

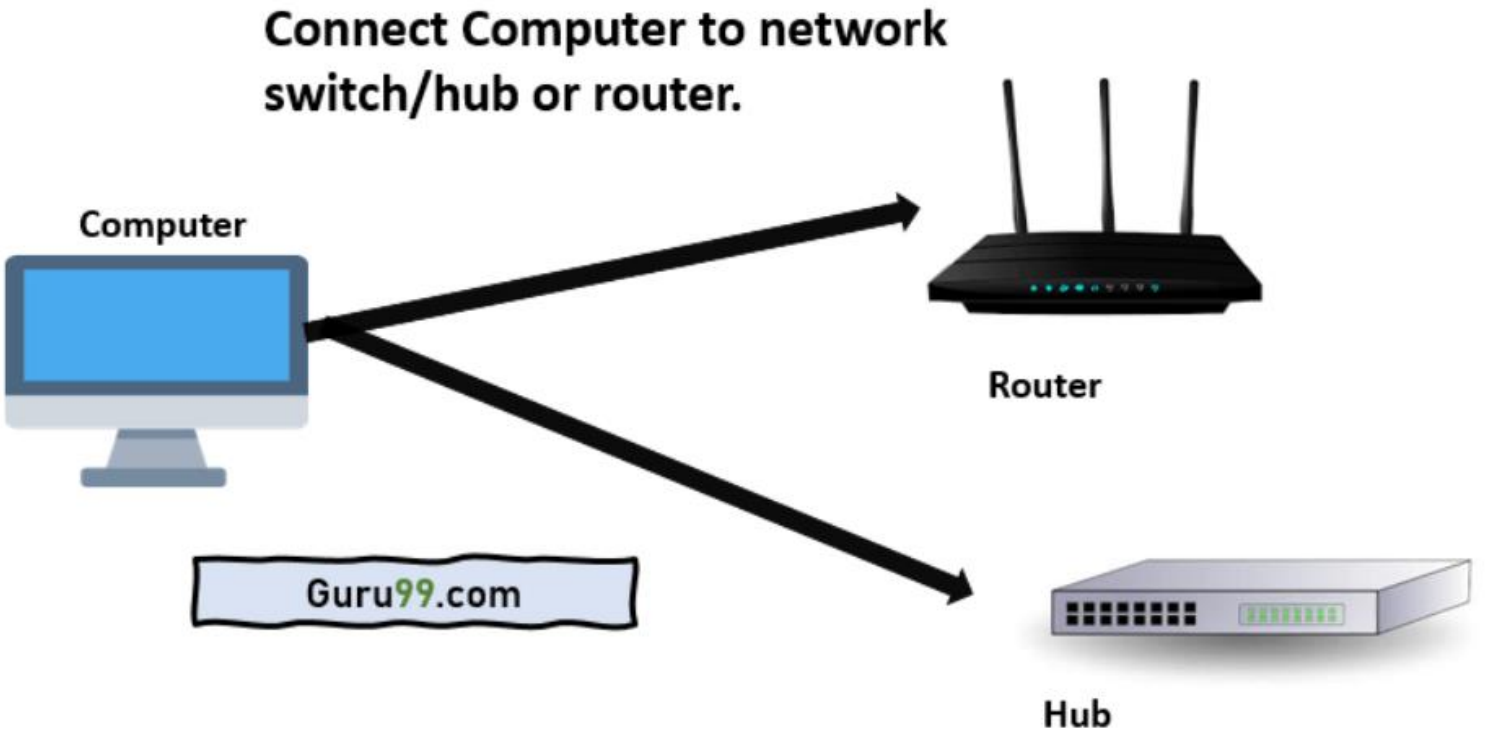
Straight through cables

The most popular kind of Ethernet cable is a straight through cable. The wires inside the cable are linked in the same sequence at both ends since it has the same wiring on both ends. To link various devices to one another, such as a computer to a switch or router, or a switch to a router, we use straight through cables.

For E.g., a straight through cable would be used to link a desktop computer to the internet if it were connected to a router.

We use straight through cables to connect different types of devices to each other. For example:

- Connecting a computer to a switch or router.
- Connecting a switch to a router.



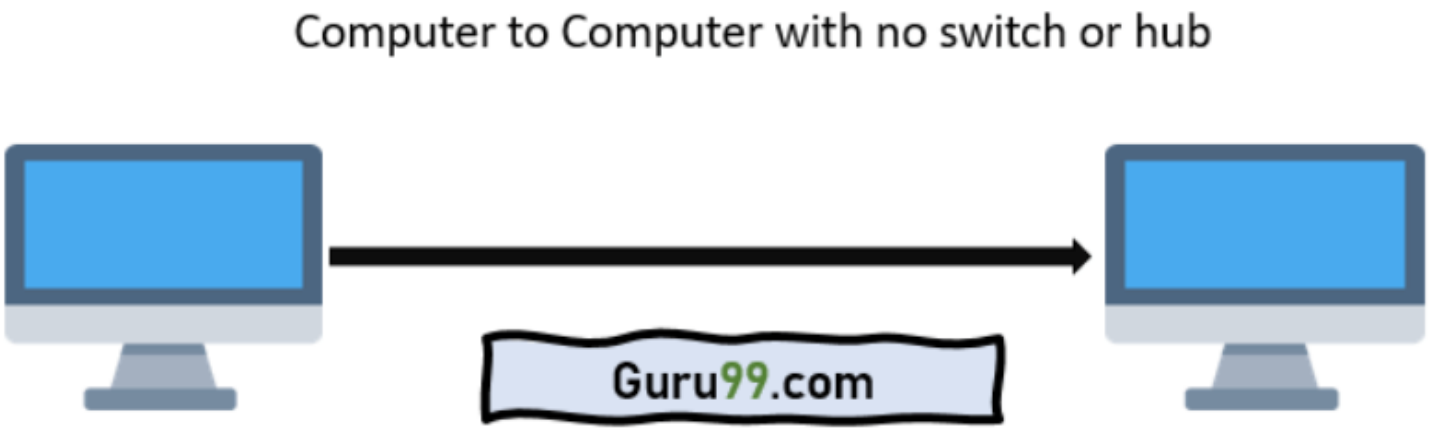
Crossover cables

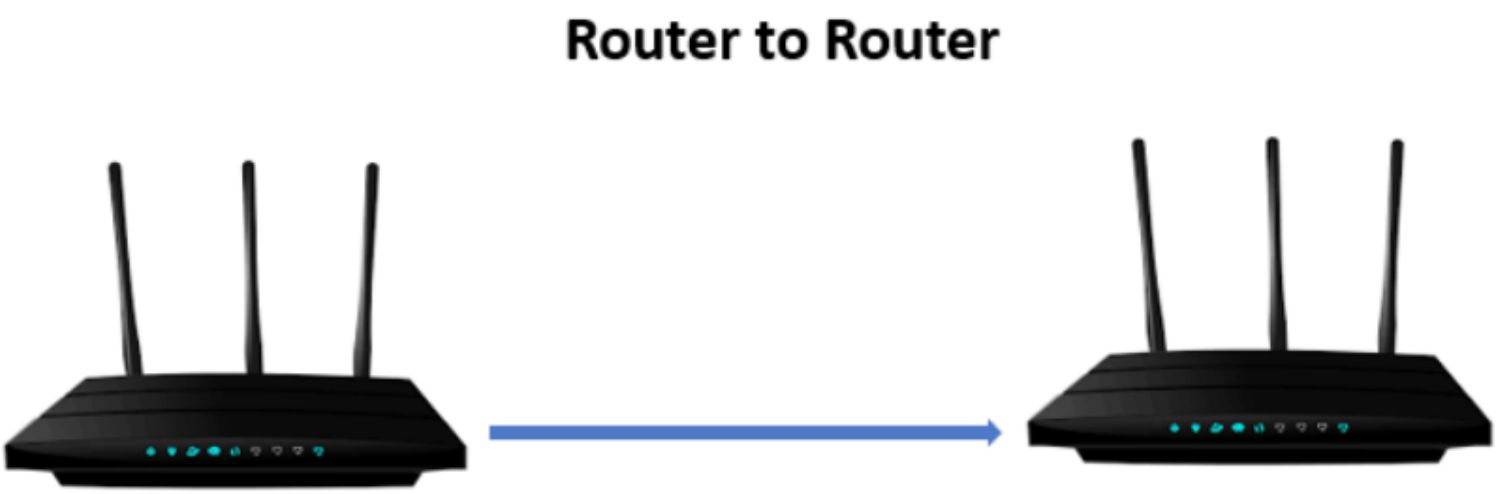
An Ethernet cable that is crossover has separate wiring on each end, with the wires crossed, resulting in a different wire order at either end of the cable. Crossover cables are used to link similar kinds of equipment directly to one another, such as a switch to another switch or a computer to another computer without the need for a router in between.

A crossover cable would be used, for E.g., if you had two computers and wanted to move files directly between them without utilizing the internet.

We use crossover cables to connect similar types of devices directly to each other. For e.g.:

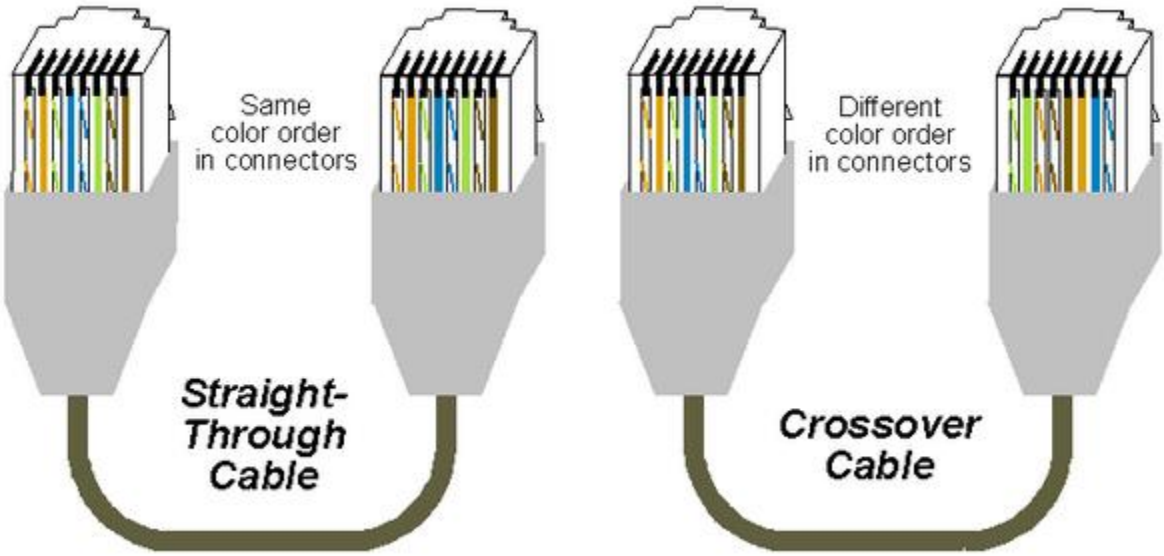
- Connecting one computer directly to another computer.
- Connecting one switch directly to another switch without a router in between.





How to identify these 2 cables

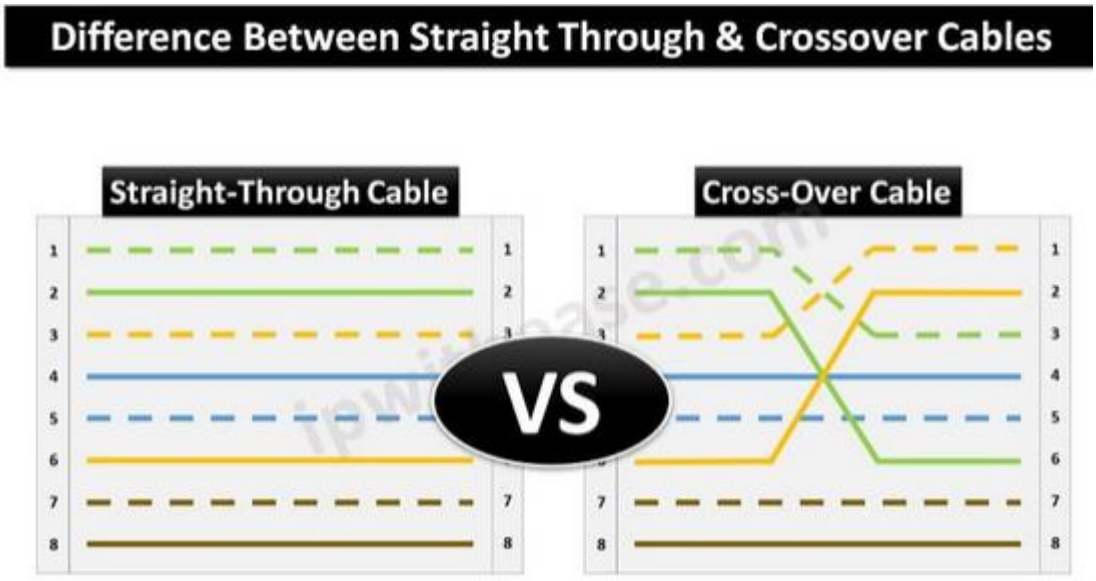
You may look at the ends of an Ethernet cable to determine if it is a crossover or straight through cable. Examine the colored wires inside the connectors by holding the two ends of the cable side by side (RJ45 connectors). The colors of a straight through cable will be in the same arrangement on both ends. The colors on either end of a crossover cable will be in a different order.



Another way to identify the cable type is by checking the pin configuration:

- **Straight Through Cable:** The pins are configured as 1-1, 2-2, 3-3, 4-4, 5-5, 6-6, 7-7, 8-8.

- **Crossover Cable:** The pins are configured as 1-3, 2-6, 3-1, 6-2 (the most important pins for crossing), while the remaining pins may stay in their original positions or also be crossed depending on the specific wiring standard used.



Some external resources I referred to

1. Grace, G. (n.d.). *Wiring diagram*. Wiring Digital and Schematic. https://www.organised-sound.com/
2. Bhardwaj, R. (2020, November 23). Difference between straight through and crossover cables - IP with ease. *IP With Ease*. https://ipwithease.com/difference-between-straight-through-and-crossover-cables/
3. *Ethernet Cables: Straight-Through vs Crossover*. (n.d.). melco.zendesk.com. Retrieved May 28, 2024, from https://melco.zendesk.com/hc/en-us/articles/203779335-Ethernet-Cables-Straight-Through-vs-Crossover
4. S, A. (2024, March 4). *Straight-Through vs. Crossover Cables: What's the Difference?* Uprite IT Services. https://www.uprite.com/straight-through-vs-crossover-cables/
5. Williams, L. (2023, December 30). *Straight Through Cables vs Crossover Cables*. Guru99. https://www.guru99.com/difference-between-straight-through-crossover-cables.html

Summary and Reflection for class 10

Summary:

Through this task, I investigated the straight through and crossover cables—the two primary types of Ethernet connections used in computer networks. I started by defining a straight through Ethernet wire and its applications. Usually, this kind of cable is used to link various devices together, like a computer and a switch or router. I then went over what a crossover Ethernet cable is and why you would need one. When connecting comparable equipment together, such two switches or a computer directly to another, a crossover cable is utilized. In the end, I explained how to determine the type of Ethernet cable by looking at the wiring sequence on both ends. I pointed out that crossover cables have different wiring patterns on both ends, but straight through cables have the same pattern on both ends.

reflection

Knowing the distinctions between crossover and straight through Ethernet connections is crucial for appropriate network configuration and troubleshooting. I now understand how crucial it is to choose the proper kind of cable to guarantee efficient network device communication thanks to this exercise. Network efficiency is increased and frequent connectivity problems are avoided by knowing when to use each type of cable. Furthermore, mastering the ability to recognize cables based on their wiring patterns gave me a vital skill for setting up new networks and troubleshooting already-existing ones. Since it establishes the foundation for more complex networking concepts and procedures, this understanding is essential for anyone working in network management.