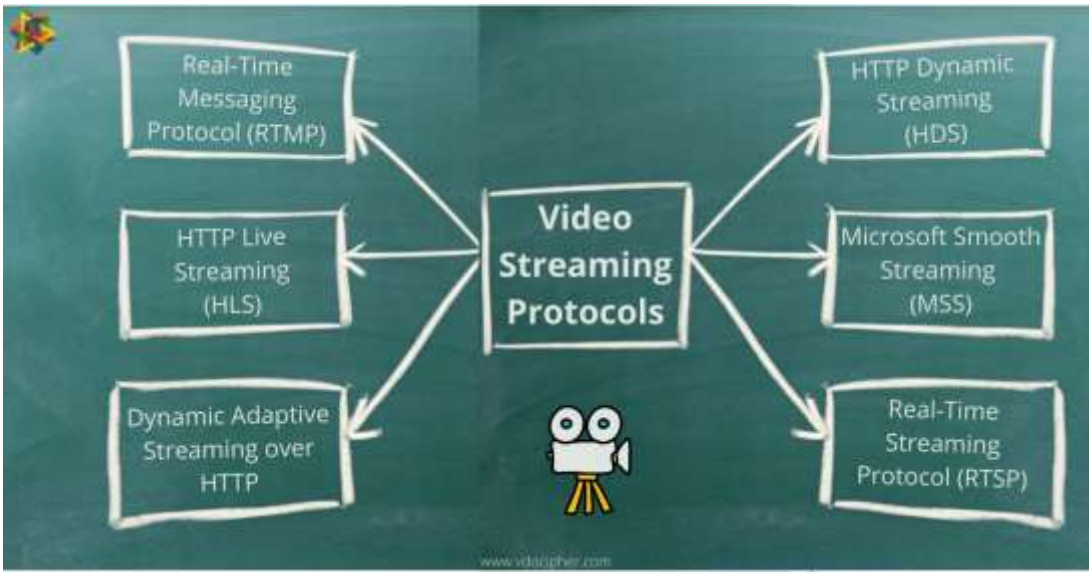
Task 5.2D Above and Beyond Credit

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

- In my case, this challenge was useful for developing my overall Python programming, particularly in networks. It also extended my skills of critical thinking when designing and launching the network services that correspond to the defined protocols. It has been a quite useful project that has helped me build a clear understanding of DNS, which will be beneficial for more complex networking topics in future work.

RTP

- RTP was developed specifically for real-time data, like audio and video. It uses UDP to lower latency, which is necessary for live streaming: The synchronization of audio and visual streams is facilitated by RTP timestamps. Determining the Payload Type: Facilitates ascertaining the structure of the data being conveyed. QoS, or quality of service, RTP can interact with QoS strategies to maintain streaming quality in the face of varying network conditions.
  RTP's performance can be impacted by network problems like packet loss and jitter, which call for additional protocols for reporting and control.

RTSP

- Systems for communications and entertainment employ a network control protocol called RTSP to control streaming media servers. RTSP is used to create and manage media sessions between endpoints: Commands: Supported VCR-like commands include play, pause, and stop, enabling interactive streaming. The technique of controlling and guiding the material flow during streaming sessions is known as session management.
  RTSP often works alongside RTP to handle control commands during the actual data transport.

DASH

- DASH is an adjustable bitrate streaming system that enables high-quality media streaming over the internet using regular HTTP web servers. Crucial attributes include: Segmented Content: Media files are split up into smaller pieces to allow for adaptive streaming. Manifest File: Also referred to as an MPD (Media Presentation Description), a manifest file instructs the client on which segments to download and play. Adaptive bitrate: Clients can switch between several qualities levels (bitrates) based on the network's condition, providing the optimal viewing experience with the least amount of buffering. Using standard HTTP servers, DASH may easily integrate with existing infrastructure and leverage HTTP-based content delivery.

HLS

- The HLS media streaming protocol, created by Apple, is similar to DASH but has a few key differences: Chunked Transfer: Similar to DASH, HLS divides content into smaller HTTP-based file segments. M3U8 Playlist: During streaming, this list of accessible media segments from an M3U8 file directs the client. Compatibility: Due to its broad support across Apple devices and browsers, it is a popular choice for content creators aiming to reach Apple ecosystems. HLS also provides flexible bitrate streaming, which enhances the user experience across a variety of network conditions.

Protocol Interaction and Integration

- In reality, video streaming typically makes use of a combination of these protocols: RTSP and RTP are often used for real-time interactive applications such as live sports broadcasting. DASH and HLS are commonly used for Video on Demand (VoD) services due to their adaptive streaming capabilities and reliance on HTTP, which allows them to benefit from CDNs. Through the use of HTTP/HTTPS, which reduces latency and speeds up load times, content delivery networks (CDNs) may more efficiently and locally distribute media assets.

Emerging Trends and Protocols

- Video streaming methods are continually evolving due to advancements.
  Peer-to-peer streaming between browsers is made possible via WebRTC, or Web Real-Time Communication, which is utilized in applications like video conferencing and does away with the need for intermediate servers.
  Google introduced QUIC (Quick UDP Internet Connections), which minimizes connection establishment time and boosts congestion control to address TCP's limitations, notably for streaming.

- A deep comprehension of the application layer protocols for video streaming exposes a complex ecosystem in which multiple protocols frequently work together to offer smooth, high-quality video content. This exchange demonstrates the vital role that application layer protocols play in the modern digital media ecosystem by guaranteeing efficient, adaptable, and dependable video delivery across a variety of devices and network conditions.

Active class 7: Who is Instructing (Module 5)

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 algorithms
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

A description of every protocol

RIP

- RIP helps computers inside a network choose the most efficient means of data exchange, much like a simple messenger. It counts the number of "hops" or steps that separate two computers. Think of hops as rest stops along the way. A message will not be allowed to pass via RIP if it must pass through more than 15 checkpoints.
  - ✓ Because RIP is simple to understand and configure, it works well for smaller, more basic networks. Owing to its little resource usage, it functions effectively in environments with constrained memory and processing capacity.
  - ✓ One of the main disadvantages of RIP is that it can only support networks up to a maximum of 15 hop counts, which limits the size of networks it can support. Furthermore, its slow convergence time may lead to short routing loops and wasteful routing.

OSPF

- OSPF is similar to a more sophisticated messenger that covers the whole network, much like GPS maps roads. It understands the quality of those steps as well as their overall number (or hops), accounting for factors like speed limitations on public roads. It uses a method called Dijkstra's algorithm to figure out the fastest and most economical path for messages to take.

    - ✓ OSPF is highly scalable and provides rapid convergence since it is link-state based and employs the Dijkstra algorithm. It supports multiple indicators to choose the best way, making routing decisions more reliable and efficient. OSPF also makes hierarchical network design easier using the concept of regions, which enhances scalability and management.
    - ✓ Keeping track of the complete network topology might cause problems with resource usage and complicate the OSPF configuration. It is less suitable for small, simple networks than RIP since it requires more CPU power and memory.

BGP

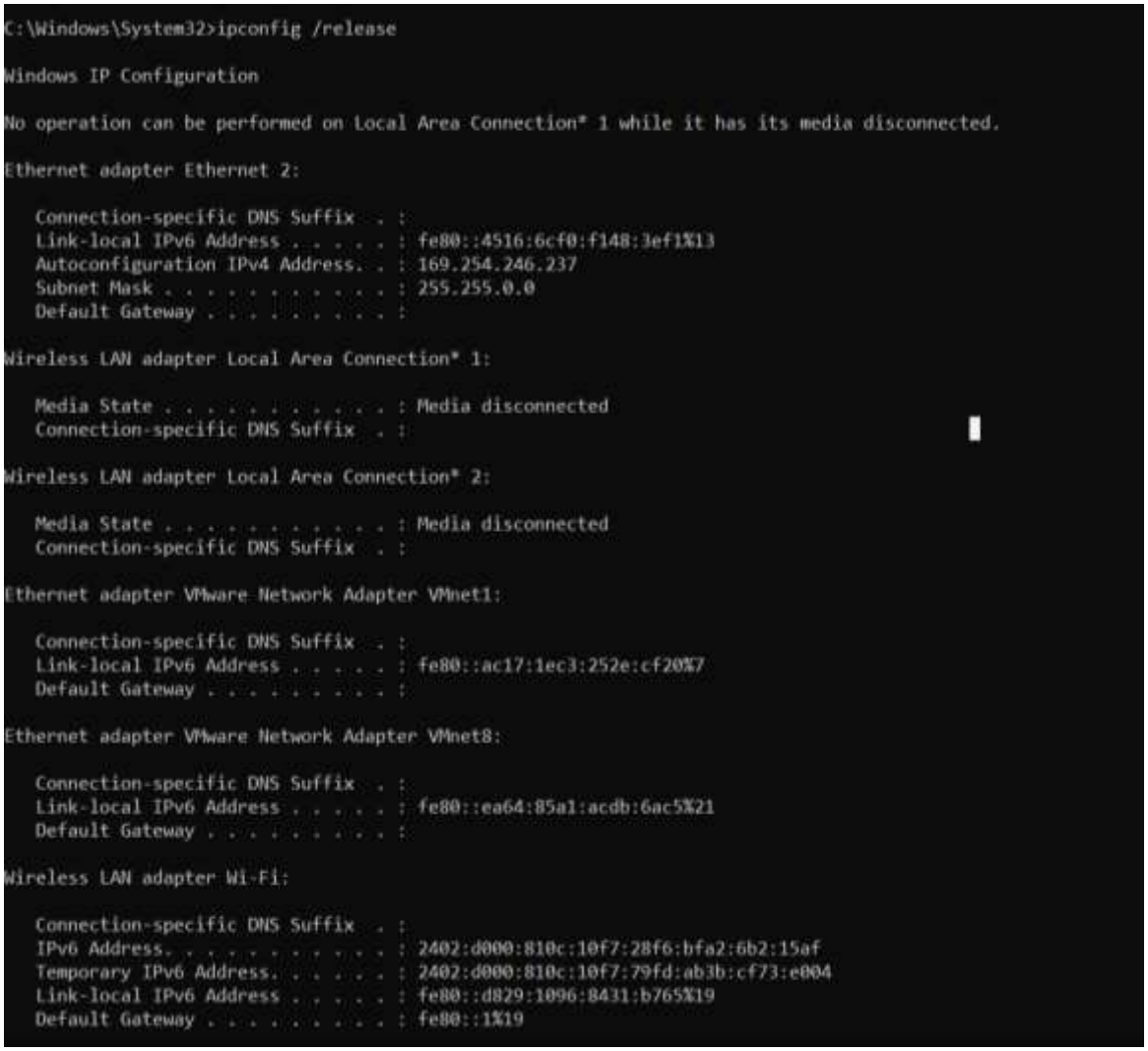
- BGP is similar to the international travel guide on the internet. It makes it easier for numerous large networks—often referred to as autonomous systems, or ASes—to communicate and share routes. In addition to hops and speed, BGP takes into account other variables like customs laws, tolls, and airline connections to determine the best route.

    - ✓ BGP is essential for internet routing because it handles enormous volumes of routing data between multiple autonomous systems. Its powerful policy-based routing capabilities allow administrators to design complex routing policies based on a range of parameters. BGP, the backbone of the internet, is unmatched in terms of scalability and endurance.
    - ✓ Because of its intricate setup and functioning, BGP demands a high level of expertise.
      Its slower convergence time when compared to OSPF could be a concern when rapid network modifications are required.

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

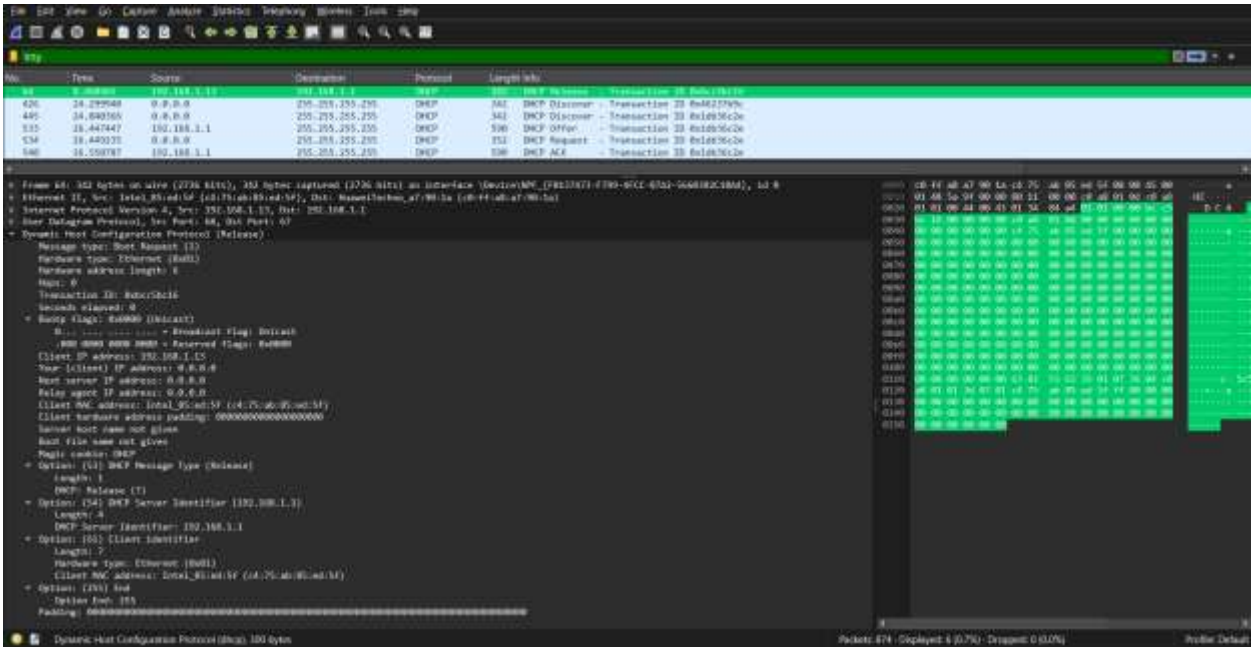
How to Use Wireshark to Capture DHCP Packets

- Start Wireshark: Turn on Wireshark on my computer
- Choose the Network Interface: I selected the network interface (such as an Ethernet adapter or Wi-Fi network) on which I wanted to record packets.
- Start Capturing: Next, I selected the shark fin-shaped button labeled "Start Capturing."
- Command Line: Next, I typed the commands ipconfig /release to release my computer's IP addresses, ipconfig /renew to obtain new IP addresses, and ipconfig /all to double-check.



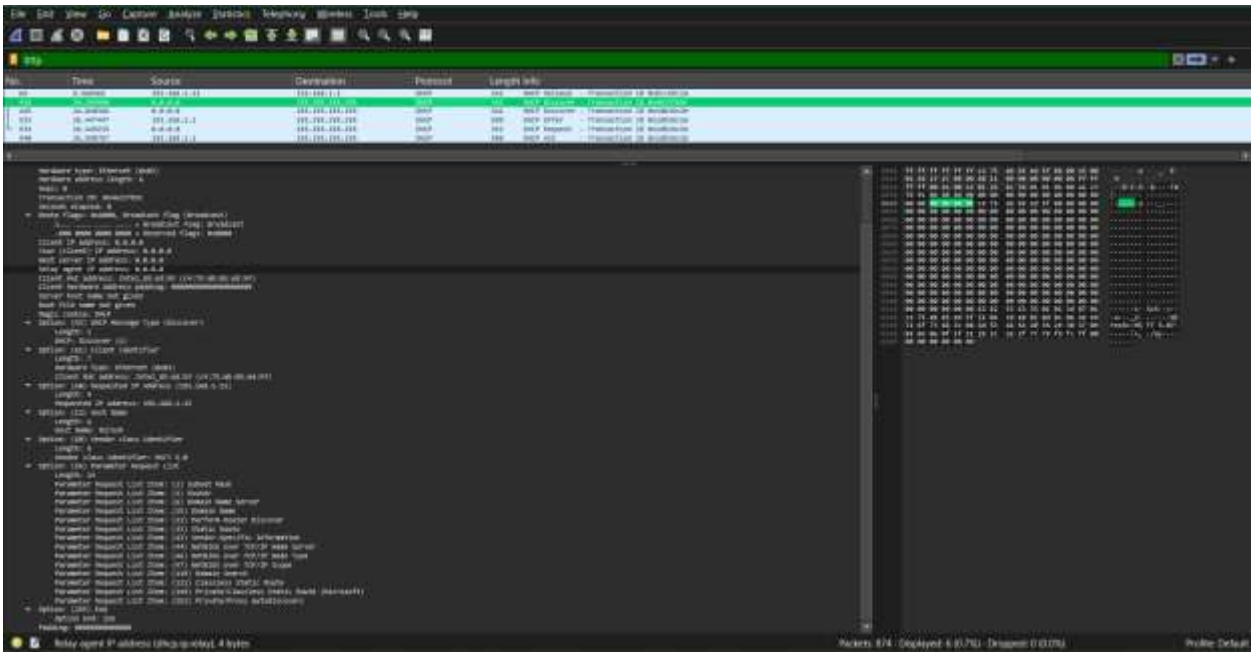
Returning to Wireshark I now halt the capture and enter the dhcp filter to discover the subsequent DHCP message sequence.

DHCP Release



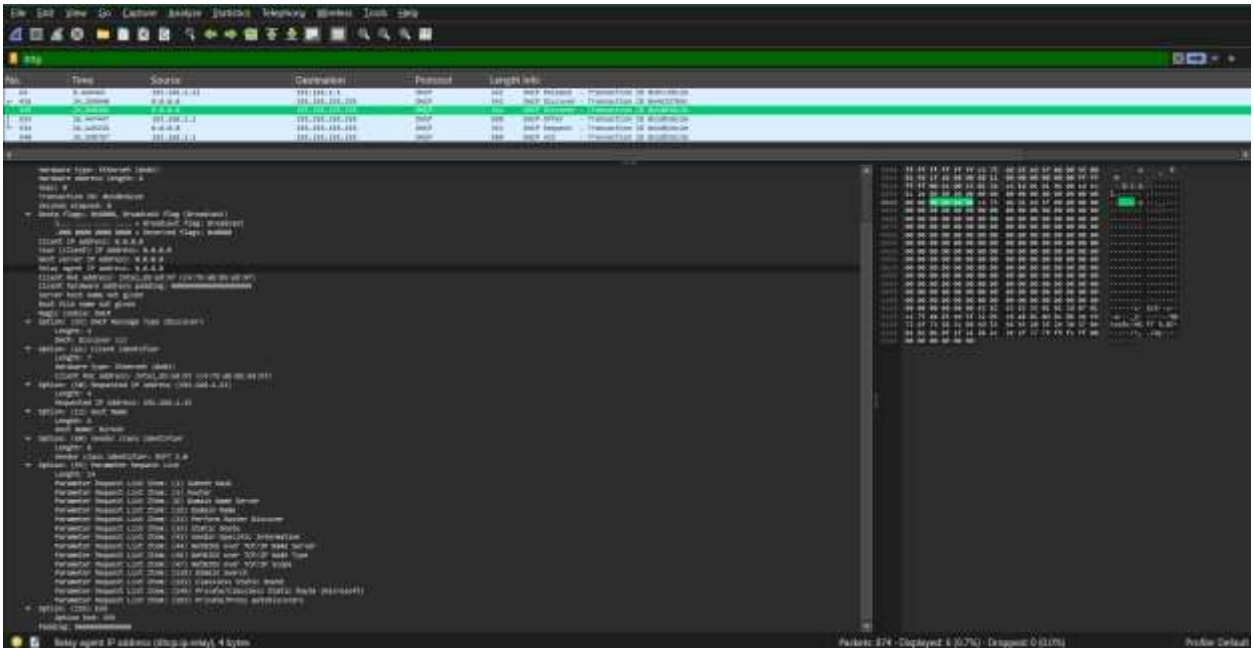
DHCP Discover

- To join a network and get an IP address, a device needs to transmit and receive a series of DHCP (Dynamic Host Configuration Protocol) signals. The process is started with the DHCP Discover message. Here, the device broadcasts a message to find any DHCP servers that can provide it an IP address. This message has no specified destination because the device does not yet have an IP address.



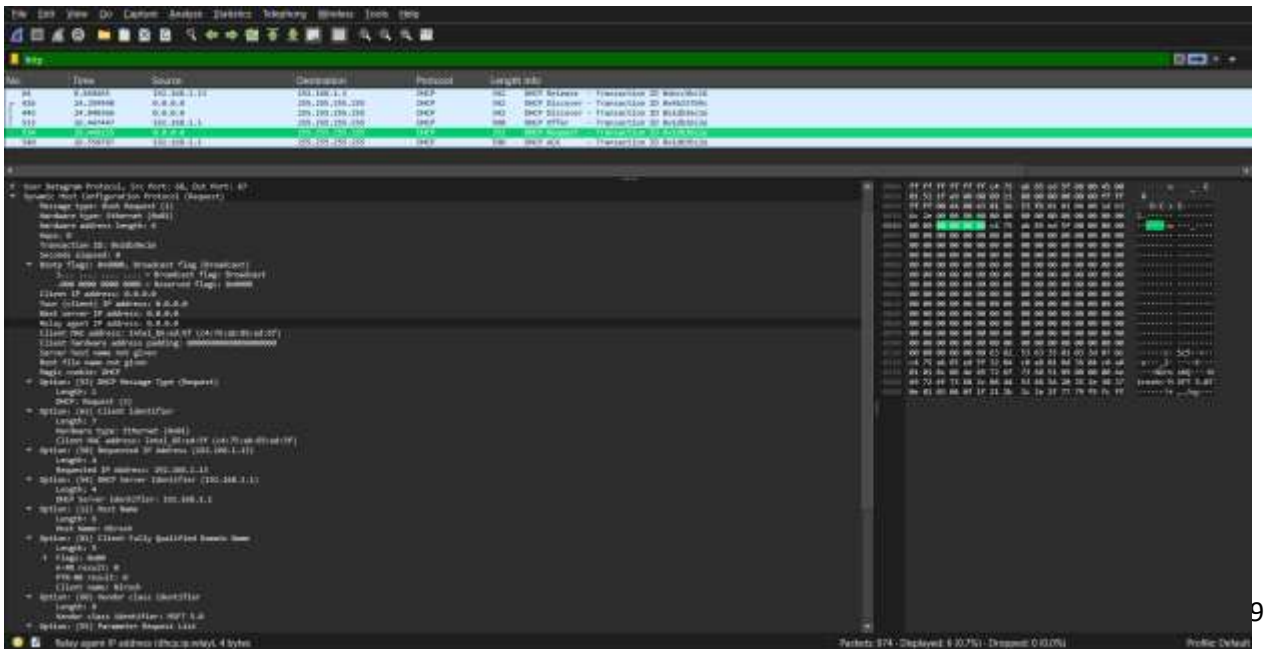
DHCP Offer

- The DHCP Offer message is subsequently sent by a DHCP server that has received the Discover message. The server responds with the device's IP address and some additional information, such as the subnet mask and the lease term (the duration for which the device is allowed to use this IP address).



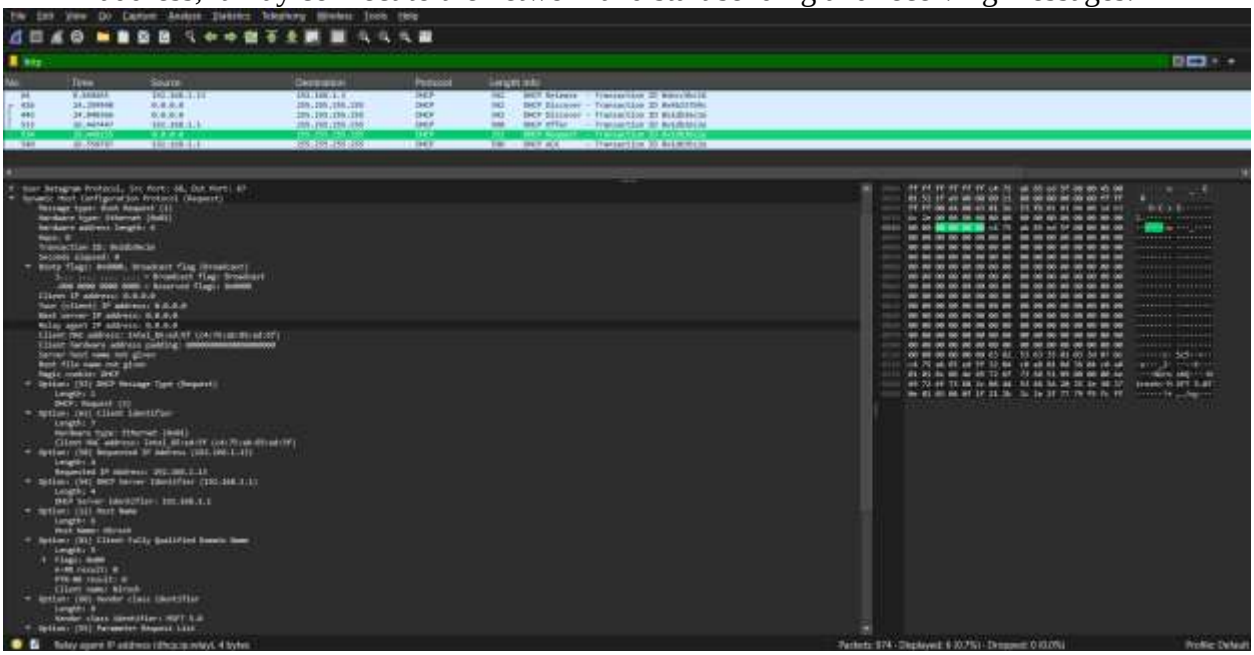
DHCP Request

- The device then responds with a DHCP Request message. This message is also broadcast so that it is seen by all DHCP servers. The device is informing other servers that it is accepting an offer from a particular server and is asking for the IP address that server is providing, based on the Request message.



DHCP Acknowledgment (ACK):

- Lastly, the DHCP server verifies the lease by sending out a DHCP Acknowledgment (ACK) message. Finally, this message includes the IP address, subnet mask, default gateway, and lease length as assignment parameters. Now that the device has the IP address, it may connect to the network and start sending and receiving messages.

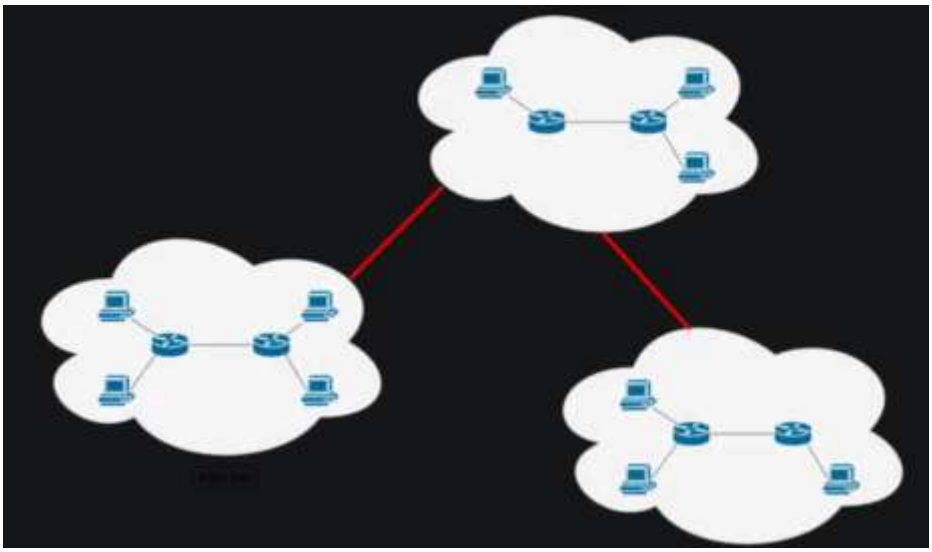


- In summary, the device sends out a Discover message to find a server; the server replies with an Offer; the device requests the IP address that is supplied; and the server confirms by sending out an ACK. Through this procedure, the device's IP address and configuration are guaranteed to be correct when it joins to the network.

Inter-AS Protocols

- ✓ Traffic between several autonomous systems (ASes), which are sizable networks or clusters of networks under a single management, is routed via these protocols. They function between separate networks, frequently with various management and policy setups. They also offer tools for intricate agreements and routing policies amongst autonomous systems.

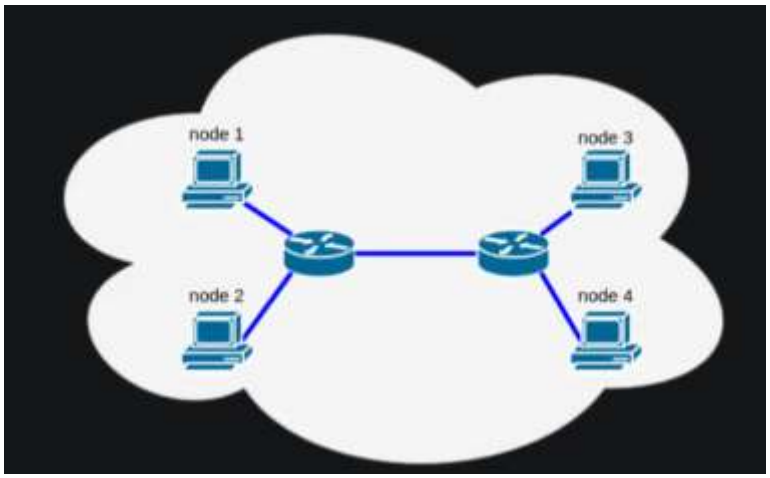
Eg : order Gateway Protocol (BGP)



Intra-AS Protocols

- ✓ Within a single autonomous system, traffic is routed via these protocols. Under a single administrative domain, they function as a single, unified network. They prioritize criteria like shortest path, bandwidth, and delay in order to concentrate on effective routing within the AS.

Eg: Open Shortest Path First (OSPF)
Enhanced Interior Gateway Routing Protocol (EIGRP)



- Inter-AS protocols like BGP are used to handle large-scale, autonomous network routing. They also offer sophisticated policy control. Effective routing within a single network is the focus of intra-AS protocols like OSPF and EIGRP, which use metrics to ensure the best possible path selection. Network administrators can more effectively design and manage internal network operations and large-scale internet routing by having a thorough understanding of these protocols.

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

Summary

- To summarize, the advanced topics pertaining to network protocols and routing were covered in the above-and-beyond assignments in Classes 7 and 8. In Class 7, we looked into modern routing algorithms and discussed the advantages and disadvantages of both static and dynamic routing protocols. In class, we recorded and examined the series of DHCP communications that are exchanged when IP addresses are assigned, using Wireshark to study DHCP. Additionally, we talked about the distinctions and applications of the two kinds of routing protocols—intra-AS and inter-AS (Autonomous System)—providing examples of both.

Reflection

- Through these exercises, I was able to fully understand complex networking concepts. In Class 7, the benefits of a comparison of the two kinds of routing protocols highlighted the advantages of automated routing decisions in dynamic protocols, such as greater scalability and fewer manual setting. The advantages of static routing in small networks were realized at the same time. It is evident from looking at current routing algorithms how important efficient routing methods are to preserving network dependability and performance.

- In Class 8, I gained a grasp of the dynamic IP allocation process and learned how to use Wireshark to analyze DHCP packets. This helped me solve issues with network connectivity. Understanding the differences between intra-AS and inter-AS routing protocols, which highlight the need of using different tactics to handle internal and external network traffic, has broadened my perspective on routing in large-scale networks. These advanced exercises have improved my understanding of network administration and diagnostics by highlighting the critical roles that efficient routing and IP address management play in the reliability and performance of networks.

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

Security issues associated with ARP

- The Address Resolution Protocol (ARP) maps IP addresses to MAC addresses on a local network. Although ARP is required for network communication, there are several security holes in it that attackers might exploit. One of ARP's primary issues is the absence of any internal security measures to verify the authenticity of ARP messages. It is hence vulnerable to several types of attacks.

ARP Poisoning (ARP Spoofing)

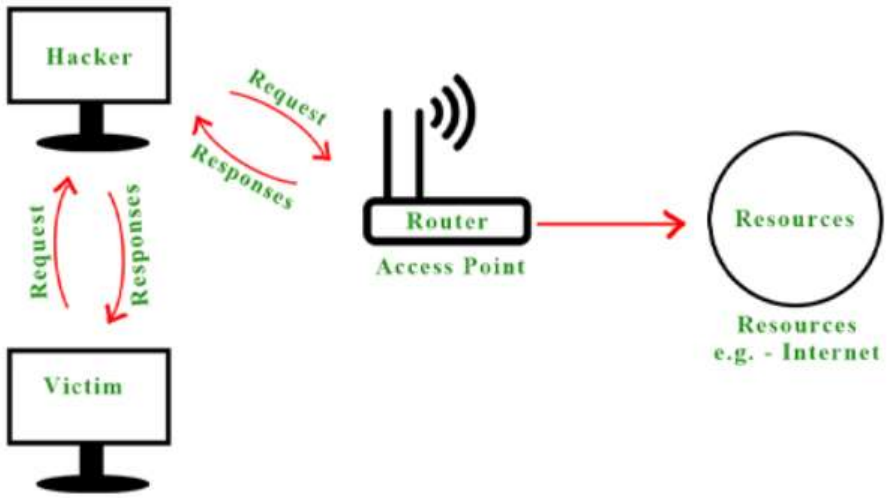
- By sending phony ARP messages, an attacker can fool the network through ARP spoofing. These connections connect the MAC address of the attacker to the IP address of an authorized device (such a gateway or another computer). With this knowledge, the attacker can then intercept, modify, or halt data intended for the approved device. Ultimately, the attacker tricks the network into transmitting data to their device instead of the correct one.

Static ARP Entries

Man-in-the-Middle Attack

- ARP spoofing may lead to a man-in-the-middle (MITM) attack. In this instance, the assailant inserts themselves covertly between two communication devices. This allows the attacker to potentially intercept and alter the data being sent. For instance, confidential information like passwords or financial information may be stolen during a Man-in-the-Middle attack.

Encryption



Denial of Service (DoS) Attack

- Attackers can also use ARP spoofing to perform DoS assaults. By sending a large number of bogus ARP packets, the attacker can overwhelm the network and cause legitimate devices to receive erroneous ARP information. This could impede normal communication, slow down the network, or render it unusable for authorized users.

ARP Inspection

Dynamic ARP inspection is a feature of some sophisticated network switches that verifies ARP packets prior to processing.

Summary and Reflection for Above and Beyond Tasks in Class 9

Summary

- The class's above-and-beyond goals centered on identifying and understanding Address Resolution Protocol (ARP) security vulnerabilities. We examined and discussed how ARP attacks, such as ARP spoofing and ARP poisoning, affect network security. We also investigated potential mitigation strategies to protect networks from these security vulnerabilities.

Reflection

- The security flaws pertaining to the data link layer were mostly brought to light by this assignment. I was able to identify the various ARP attack types and have a better understanding of how attackers can utilize ARP vulnerabilities to intercept or alter network communication. To safeguard networks against these kinds of intrusions, the application of robust security mechanisms, including ARP inspection, dynamic ARP inspection, and static ARP entries The topic of spoofing detection technologies was brought up during the mitigation alternatives discussion.

- This exercise highlighted the need of being proactive and on guard when it comes to network security, particularly at the data connection layer where even seemingly simple protocols can become the subject of sophisticated attacks. It emphasized how important it is for cybersecurity experts to continuously learn and adjust in order to successfully protect network infrastructure from evolving threats.

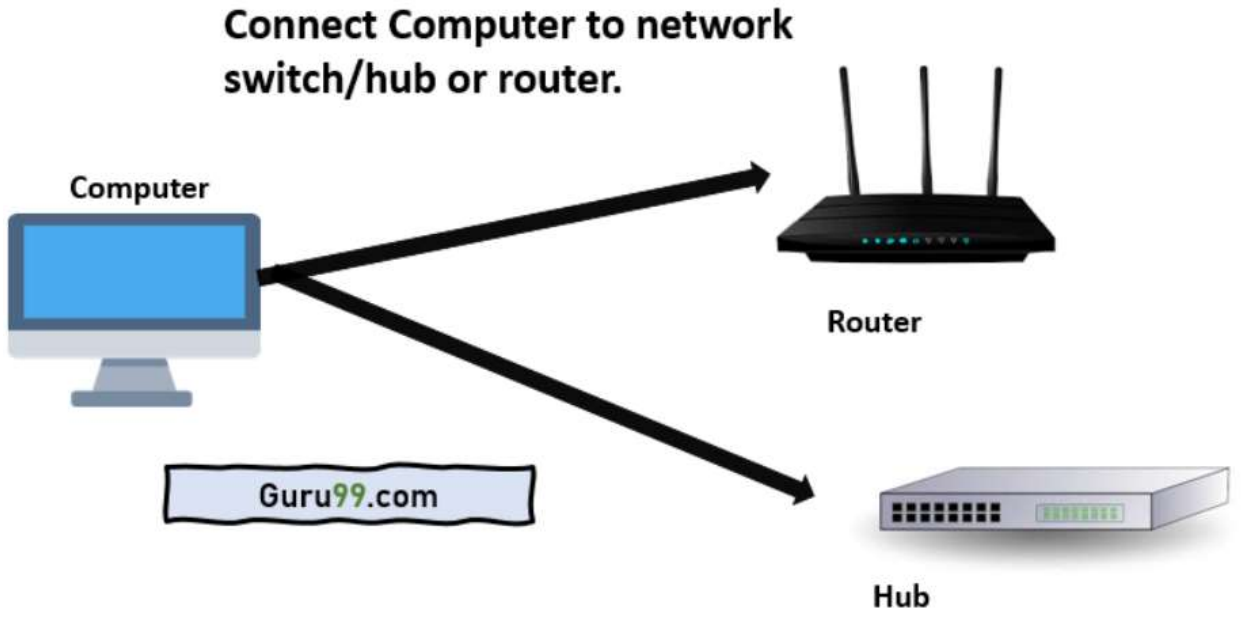
Active class 10: Physical Connections and Protocols (Module 7)

What is an Ethernet cable

- An Ethernet cable allows two devices to be connected to a wired network at a high speed. This network connection is composed of four pairs of twisted pair transistors. At both ends of the line, data transfer is accomplished via the RJ45 connector. He many kinds of Ethernet cables are Cat 5, Cat 5e, Cat 6, and UTP cables. Cat 5 cable can only handle networks operating at 10/100 Mbps, but Cat 5e and Cat 6 cables can support Ethernet networks operating at 10/100/1000 Mbps.

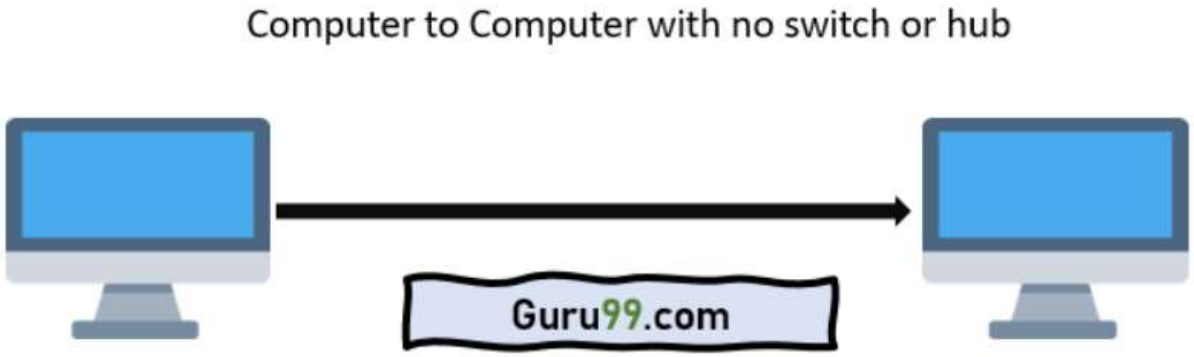
Straight through cables

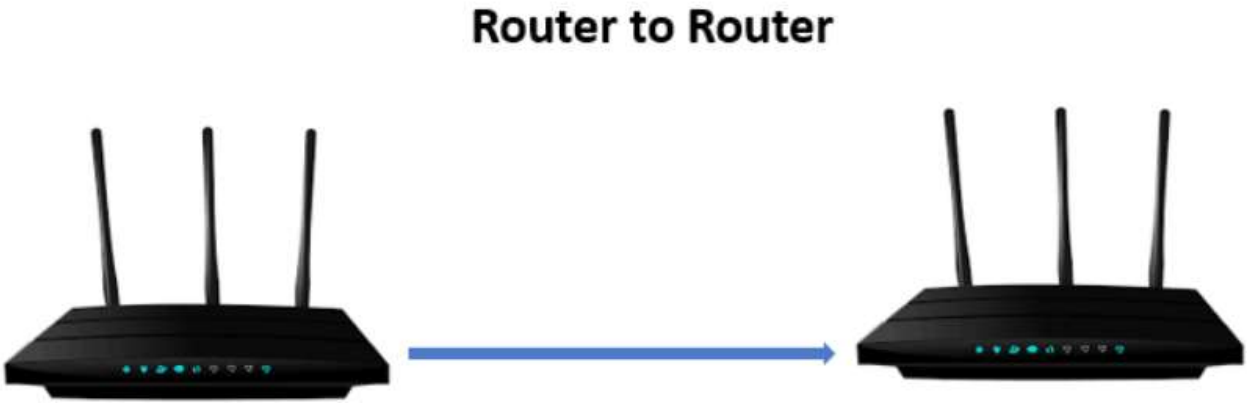
- A straight through Ethernet cable is the most often used type. Because the cable has the same wiring on both ends, the wires within are connected in the same order at both ends. Straight through cables are used to connect different devices to one another, such as a computer to a switch or router or a switch to a router. For instance, if a desktop computer were linked to a router, it would be connected to the internet using a straight through cable.



Crossover cables

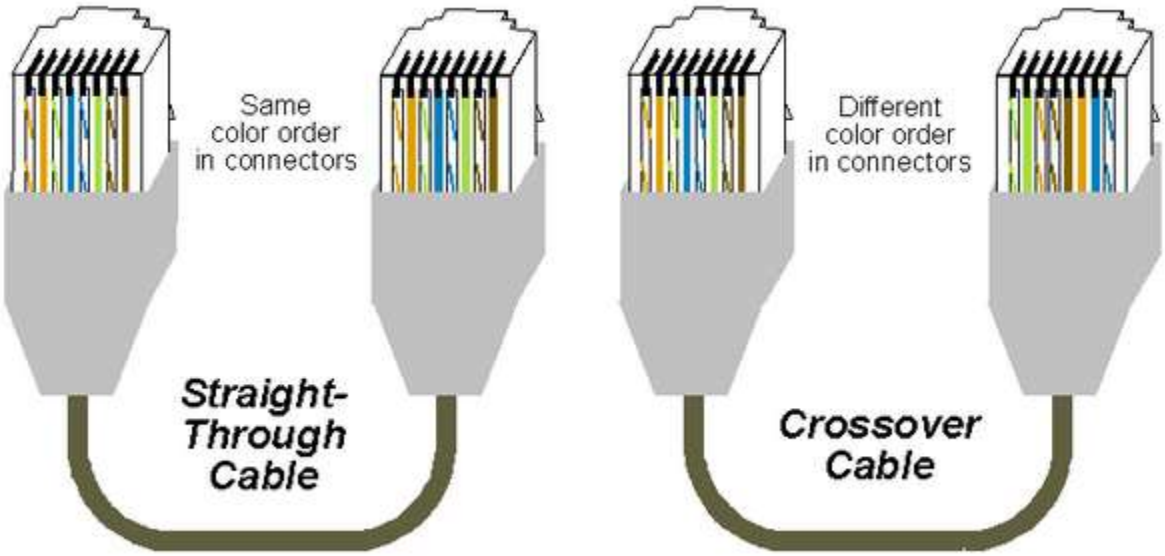
- A crossover Ethernet cable features distinct wiring on each ends, with the wires crossed, giving the cable a distinctive wire sequence at each end. Without the use of a router in between, crossover cables are used to connect comparable types of equipment directly to one another, such as a switch to another switch or a computer to another computer.
  If you wanted to transfer files directly between two computers without using the internet, for example, you would use a crossover connection.





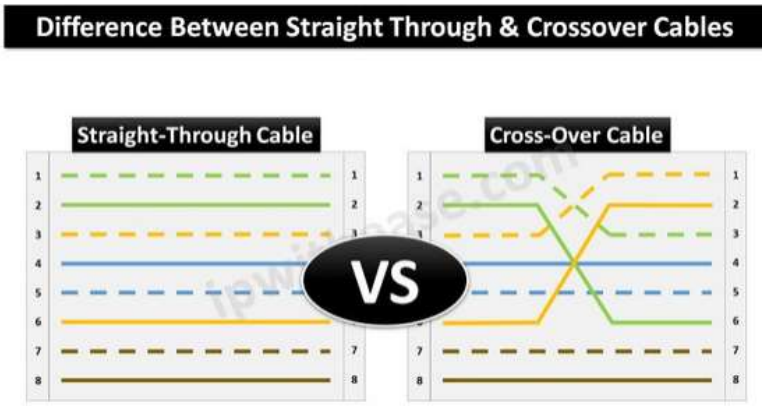
How to identify these 2 cables

- An Ethernet cable's ends can be used to identify if it is a straight through or crossover cable. Holding the two ends of the cable side by side, examine the colored wires inside the connectors (RJ45 connectors). In a straight through wire, the colors are arranged the same on both ends. A crossover cable's colors will appear in a different order on either end.



Straight Through Cable: 1-1, 2-2, 3-3, 4-4, 5-5, 6-6, 7-7, and 8-8 are the pin configurations.

Crossover Cable: Depending on the particular wiring standard being used, the remaining pins may remain in their original positions or may also be crossed. The pins that are most crucial for crossing are arranged as 1-3, 2-6, 3-1, and 6-2.



Summary and Reflection for class 10

Summary

- I looked into the two main kinds of Ethernet cables—straight through and crossover cables—during this assignment. The connections that make up computer networks. I began by outlining the uses for a straight through Ethernet line. This type of cable is typically used to connect multiple devices, such as a switch or router and a computer. Next, I discussed the use of crossover Ethernet cables and their definition. When establishing comparable A crossover cable is used to connect two pieces of equipment, such as switches or a computer, directly to one another. Lastly, I described how to look at the wiring sequence on both ends to identify the type of Ethernet cable. Straight through cables have the same wiring pattern on both ends, whereas crossover cables have distinct designs, as I mentioned.

Reflection

- It's essential to understand the differences between crossover and straight through Ethernet connections in order to configure and troubleshoot networks properly. I now realize how vital it is to choose the correct kind of cable to assure efficient network device communication thanks to this activity. By understanding when to use each type of cable, network efficiency is boosted and frequent connectivity issues are avoided. Furthermore, I gained a crucial skill for configuring new networks and repairing old ones when I mastered the ability to identify wires based on their wiring patterns. Since it sets the framework for more complicated networking concepts and procedures, this understanding is crucial for anyone working in network administration