CSCI 5010 – Fundamentals of Data Communications

Lab 3

IP Addressing

University of Colorado Boulder

Department of Computer Science

Network Engineering

Professor Levi Perigo, Ph.D.

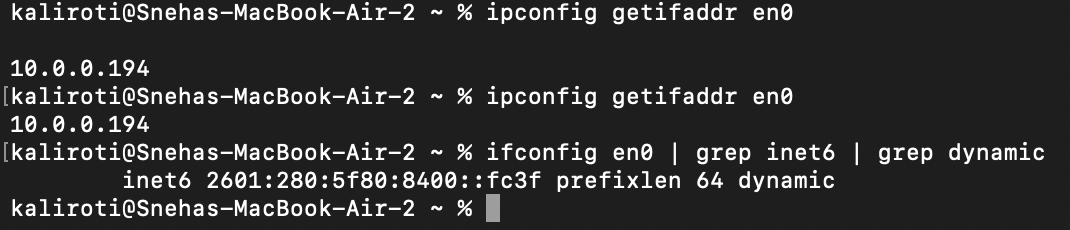
# Summary

This lab is intended to be an overview of IP addressing, the two formats in which IP addresses can be represented (IPv4 and IPv6) and the difference between public and private IP addresses. This lab will be a baseline for future exploration into these topics used throughout this course.

The questions in the lab are intentionally vague. The purpose of this is for you not only to research, investigate, and learn the technologies, but also become proficient at interpreting both non-technical and technical questions. Being able to research and discover answers on your own will be critical as you progress in your career.

# Note: Feel free to use your laptop or VMs provided for any objective.

# Objective 1: Public and Private IP addresses

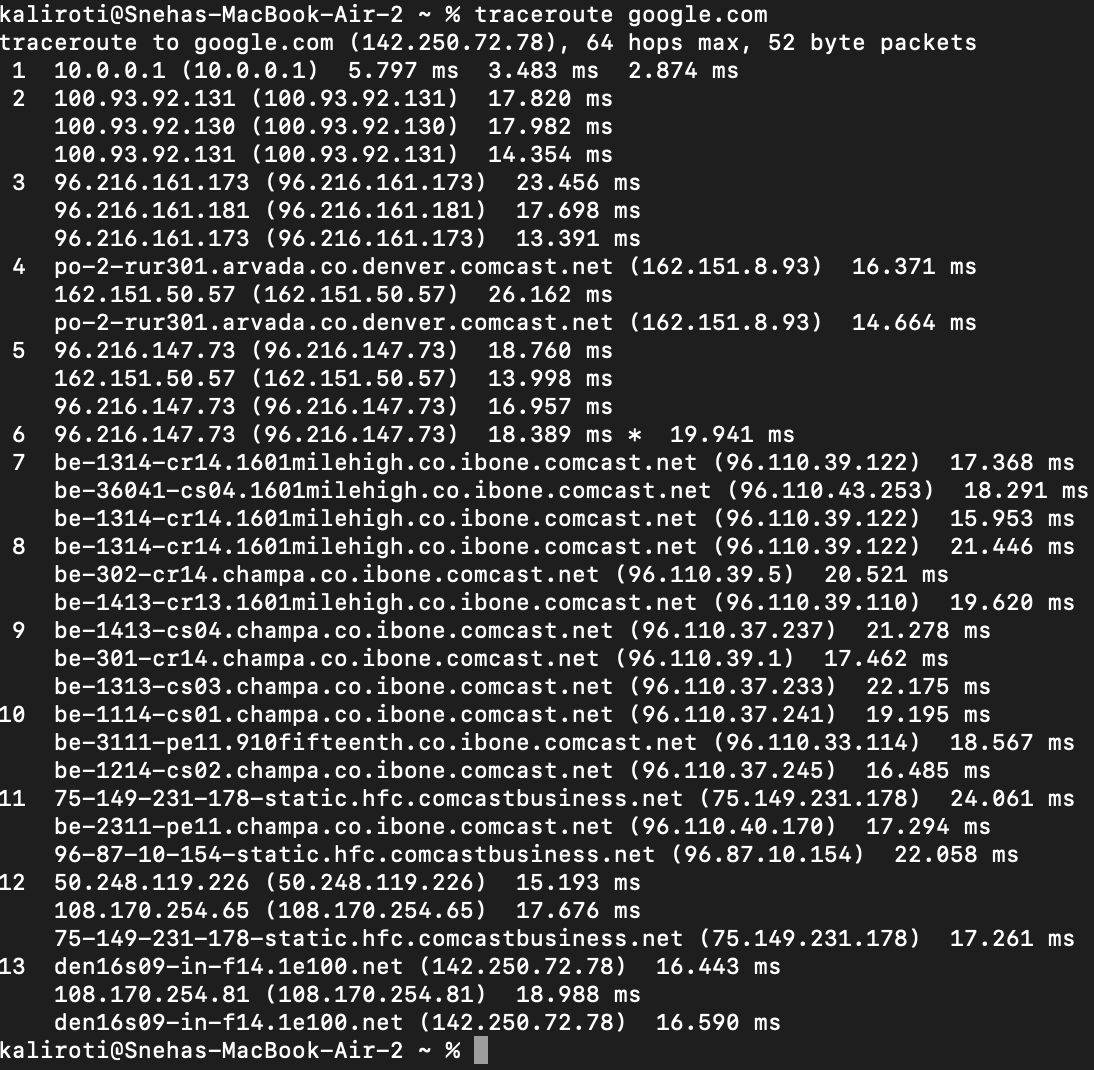
1. Using the command prompt, find your laptop’s IP address.
   1. Submit the IP address here (also note how the address was obtained (static/dynamic/etc.) [**1point**]

This IP address was dynamically assigned.

1. Navigate to the URL: [www.ipchicken.com](http://www.ipchicken.com). What IP address does it indicate? Is it different from the address above? Why or why not? [**2 points**]

The IP address I got from ipchicken.com is 67.173.225.54. This IP address is different from the IP address mentioned above as the IP address that I have is a private IP address and the IP address on ipchecken.com is a public IP address. My private IP address is “NAT”-ed from the ISP’s routers.

1. Execute a traceroute on your laptop to any URL. Provide a screenshot of the output [**1 point**].



* 1. Do all the IP addresses in the trace belong to the same network? What do these IP addresses represent? Is there any additional information you can obtain about these replies that you can gather? [**15 points**]

No, the IP addresses in the trace do not all belong to the same network. They represent various routers or switches or firewalls along the path from my computer to google.com. These devices are part of different networks and ISPs. The first hop, 10.0.0.1, is my default gateway. When my machine needs to communicate with anything that’s not on my network, it would always first go to my default gateway, which is, 10.0.0.1. The default gateway would then route the traffic to the appropriate routers to reach the destination. Each hop in the trace corresponds to a different networking device. As the traceroute progresses, it encounters routers belonging to various ISPs. The final hop (*142.250.72.78*) is the IP address of one of Google's servers, which is the google.com website. Additional information about the replies:

1. IP addresses: Each line in the traceroute represents a hop and displays the IP address of the router or device at that hop. These addresses help identify the specific routing path.
2. RTT: RTT or round-trip time is basically the time a packet takes to reach the next hop. This is measured in milliseconds. For example, it takes about 17.82 ms from my default gateway (*10.0.0.1*) to the next hop (*100.93.92.131*).
3. Hostnames: In some cases, the traceroute output also displays hostnames or network names for certain routers. This is because the traceroute command also does a DNS lookup for the IP address. If there’s a hostname associated with an IP address (i.e. an A record is present), the traceroute would show the hostname.
   1. Which of these are private IP addresses and which of these are public? How did you differentiate, and why would some be public and some private? [**10 points**]

10.0.0.1 (Hop 1): This IP address is in the private IPv4 address range 10.0.0.0 to 10.255.255.255. IP addresses in this range are reserved for private use within a closed network. Rest all the IP addresses in the traceroute are public IP addresses as they do not fall within the reserved private IP address ranges. 142.250.72.78 (Final Hop): This IP address belongs to Google, and it's the public IP address of google.com.

I differentiated the private vs public IP addresses as there is a reserved pool of private IP addresses. And anything that does not fall under this private IP address range, is a public IP address. These private IP address ranges are:

192.168.0.0 – 192.168.255.255 (65,536 IP addresses)

172.16.0.0 – 172.31.255.255 (1,048,576 IP addresses)

10.0.0.0 – 10.255.255.255 (16,777,216 IP addresses)

IP addresses outside these reserved ranges are considered public and are used for devices accessible over the public internet.

Private IP addresses are specifically used for utilization within the same Local Area Network (LAN), office, or similar closed network environments. Their primary purpose is to enable communication among devices within the same LAN without the necessity of reaching out to the broader internet. In the context of the traceroute output provided, the first hop is a private IP address, one that is not publicly advertised on the internet except to the ISP managing my network. In contrast, all subsequent hops involve public IP addresses, indicating that these network devices are engaged in communication across the global internet.

1. What are the IPv6 address that your system obtained? [ **1 point**]

::1 (Loopback Interface - lo0): This is the loopback address in IPv6, equivalent to 127.0.0.1 in IPv4.

fe80::1%lo0 (Loopback Interface - lo0): This is the link-local address for the loopback interface.

fe80::704c:dcff:fe77:1b98%anpi1 (Network Interface anpi1): This is the link-local address for the anpi1 network interface.

fe80::704c:dcff:fe77:1b97%anpi0 (Network Interface anpi0): Similar to the previous address, this is the link-local address for the anpi0 network interface.

fe80::1c77:5b9a:d9d4:26e2%en0 (Network Interface en0): This is the link-local address for the en0 network interface.

2601:280:5f80:8400:1490:2098:acd6:8302 (Network Interface en0): This is a global IPv6 address assigned to the en0 network interface. This is my WiFi’s IPv6 address.

2601:280:5f80:8400:a8a2:78ef:4035:2fef (Network Interface en0): This IPv6 address is also assigned to the en0 interface and is likely a temporary address generated for privacy.

2601:280:5f80:8400::fc3f (Network Interface en0): This is another global IPv6 address assigned to the en0 interface. It is likely dynamically assigned by my ISP.

2601:280:5f80:8400:fc41:3d62:3e8:e31e (Network Interface en0): Similar to the previous address, this is another temporary IPv6 address assigned to the en0 interface.

1. Repeat **Obj1.2** using any tool of your choice? What IPv6 address do you see on the public domain? Is it same as the seen above? Why or Why not?? [**10 points**]

I used whatismyip.com. The public IPv6 address is **2601:280:5f80:8400:a8a2:78ef:4035:2fef**. This IPv6 address is the same as mentioned in the ifconfig command under “temporary” IP addresses. This is assigned by my ISP dynamically and may change for security reasons, hence the “temporary” IPv6. The reason it is the same is that public IPv6 addresses remain consistent unless the ISP decides to change them. In my situation, both my IPv6 address (2601:280:5f80:8400:a8a2:78ef:40) and IPv4 address (67.173.225.54) are the same across both the websites, ipchicken.com and whatismyip.com. This suggests that my ISP likely has a Network Address Translation (NAT) rule in place. This rule specifies that any device or traffic originating from my network range is allowed to be NATed to the IPv4 address 67.173.225.54, or potentially to a range of these public IPv4 addresses. Hence, the public IP would mostly be the same as it is statically configured.

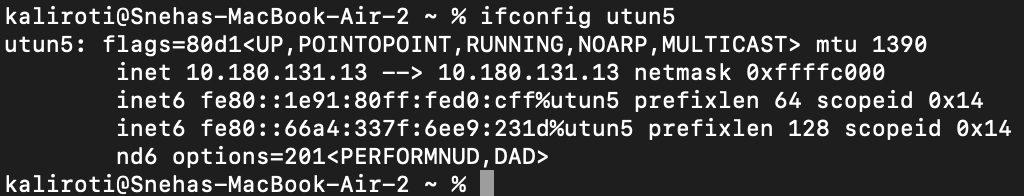
# Objective 2: IP Address Format

Note: Prefer using your own laptop instead of the VM, since assigning a static IP to VM might result in losing connection.

1. While connected to the CU campus network, run the command to find your laptop’s IP address from the command prompt again.
   1. How many IP addresses do you come across? Do you see both IPv4 and IPv6 addresses?

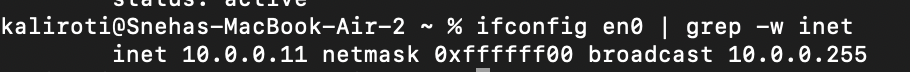
I see 3 IP addresses. 2 IPv6 and 1 IPv4.

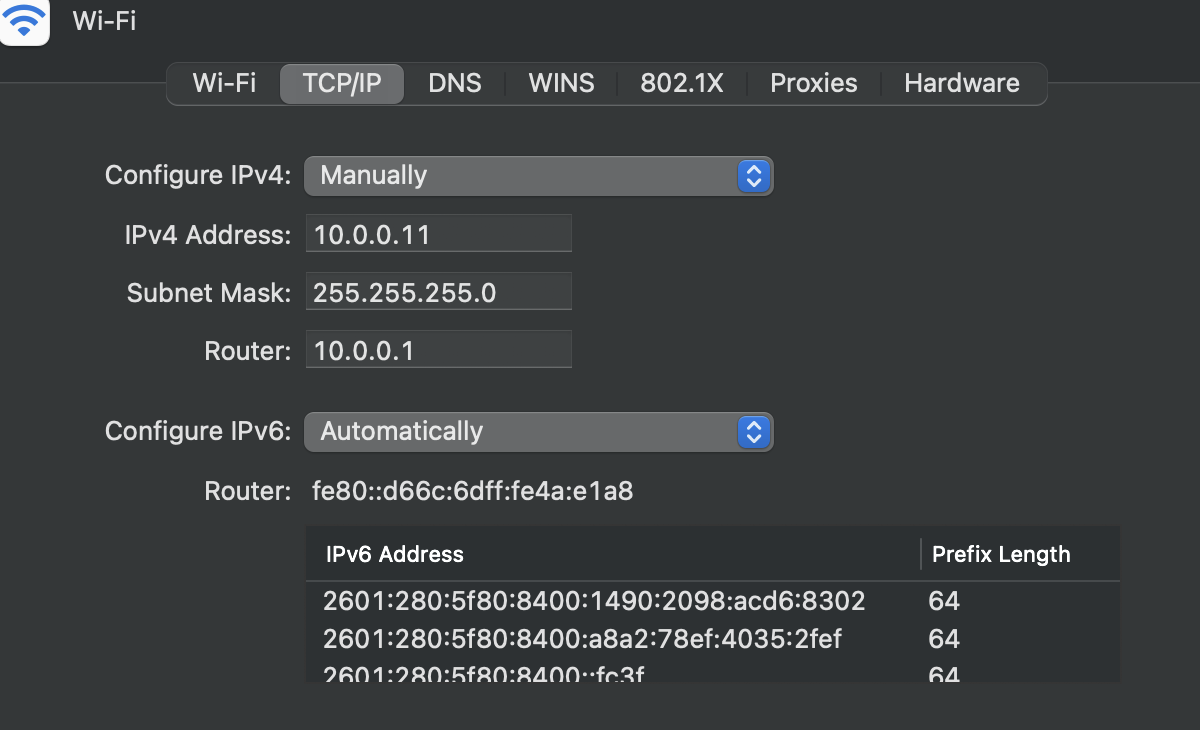
* 1. Indicate in screenshot [**5 points**]



1. Can you configure an IP address of your choice instead allowing the host to receive an IP address dynamically? If so, include a summary of how you can statically assign an IPv4 address, and provide the screenshot indicating that you have statically configured the IP address [**10 points**]

Yes, I can configure IPv4 address manually.





Here’s the summary of how I manually assigned the static IPv4 address:

Open System Preferences -> In the System Preferences window, click on "Network."

On the left side, select the active network interface you want to configure with a static IP address (*example: Wi-Fi*).

Click on the "Advanced" button in the bottom-right corner.

In the Advanced settings window, go to the "TCP/IP" tab. You should see the "Configure IPv4" dropdown menu.

From the "Configure IPv4" dropdown menu, select "Manually."

Now, enter the static IP address, subnet mask, default gateway, and DNS server information manually. And then click “Apply”.

1. Explain the formatting of IPv4 and IPv6 addresses. [**2 points**]

IPv4 addresses are 32-bit addresses represented in a dotted-decimal format, which means they are divided into four 8-bit octets and displayed in decimal form, separated by dots. Each octet can have values ranging from 0 to 255. Example: 192.168.22.1

The IPv4 address is divided into two parts: the network portion (*leftmost bits*) and the host portion (*rightmost bits*), with a subnet mask. The first IP address of a network is called the network address, the last IP address is called the broadcast address. The first usable IP address starts with 1 IP address after the network address and the last usable IP address is 1 IP address before the broadcast address.

IPv6 addresses are 128-bit addresses. IPv6 addresses are represented in hexadecimal format and are separated by colons (:). Example: 2601:280:5f80:8400:a8a2:78ef:4035:2fef. Leading zeros within each group can be omitted, and consecutive groups of zeros can be represented by a double colon (::), but only once in an address. Example: 29b1:1db9:34a1::0819:7e06.

References:

Windows: [How to Assign a Static IP Address in Windows 10 or Windows 11 (howtogeek.com)](https://www.howtogeek.com/19249/how-to-assign-a-static-ip-address-in-windows/#:~:text=To%20set%20a%20static%20IP%20address%20in%20Windows%2010%20or,IP%20details%2C%20and%20click%20Save.)

Mac: [Use DHCP or a manual IP address on Mac - Apple Support](https://support.apple.com/guide/mac-help/use-dhcp-or-a-manual-ip-address-on-mac-mchlp2718/mac)

Note: At any time if you are having issues, revert to DHCP.

# Objective 3:

Using what you have learned from the in class lectures, and from Objective 1 and Objective 2 of this lab, describe the difference between private and public addresses and the need for ipv6 addressing. [**10 points**]

**Private Addresses:** Private IP addresses are designed for use within private networks such as homes or within organizations. The private IP address ranges in IPv4 include 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255. Private IP addresses are usually not routable on the public internet. Private IP addresses also are not usually unique in the world but are unique in the same organization. For example a machine in Amazon can have 10.0.0.2/24 and a machine in Google can have the same IP address, however, 2 machines in Amazon cannot have 10.0.0.2/24 as the IP address.

**Public Addresses:** Public IP addresses are globally unique and used to identify devices on the public internet. They are essential for devices that need to communicate across the global network. Public IPv4 addresses include ranges like 8.8.8.8 (Google's public DNS server) or 208.67.222.222 (OpenDNS). Anything that does not belong in the private IP addresses range is a public IP address. Public IP addresses are routable on the public internet, allowing devices to communicate with one another globally. For example, amazon.com’s public IP address cannot be the same as google.com’s IP address.

**The Need for IPv6**:

* IPv4, which uses 32-bit addresses, has a limited address space of approximately 4.3 billion unique addresses. The rapid growth of the internet and devices have nearly exhausted this address pool.
* IPv6, has 128-bit address space. Hence, it provides numerous unique addresses (*approximately 340 undecillion*). This allows every device to have a globally unique identifier.
* With the enormous amount of IPv6 address ranges, it promotes end-to-end connectivity by providing a public address to **every** device, eliminating the need for NAT.

# Objective 4: IPv4 subnetting

1. What is the difference between classful and classless IPv4 addressing? Why do we need classless addressing and subnetting? [**5 points]**

In classful addressing, the IPv4 address space is divided into three classes: Class A, Class B, and Class C. Each class has a fixed portion of the network and host.

**Class A:** 1.0.0.0 to 126.0.0.0. Subnet Mask: 255.0.0.0

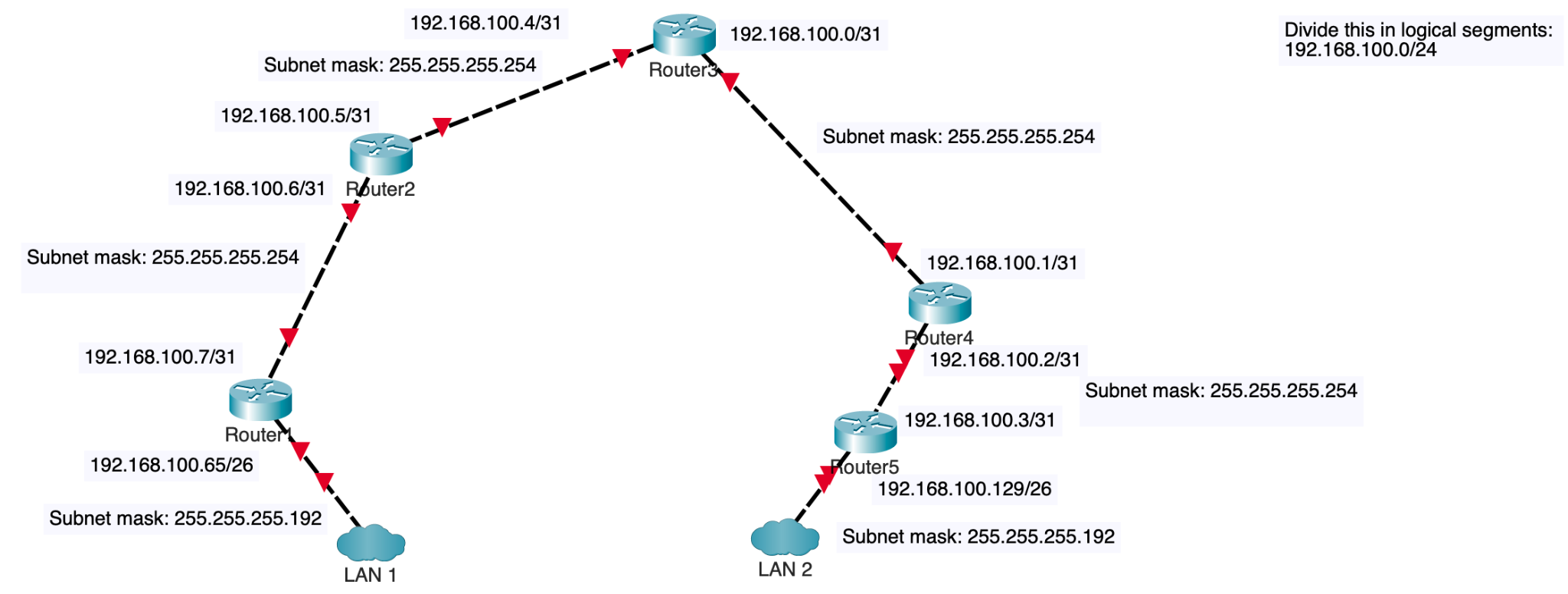
**Class B:** 128.0.0.0 to 191.255.0.0. Subnet Mask: 255.255.0.0

**Class C:** 192.0.0.0 to 223.255.255.0. Subnet Mask: 255.255.255.0

Classful addressing inefficiently uses address space which often leads to IP address space wastage. For example, if you only needed 300 IP addresses, a Class C would not suffice, so you would end up with a Class B and around 60,000 IP addresses would be wasted. To address this IP address wastage, classless addressing or Classless inter-domain routing (CIDR) was introduced. In CIDR notation, an IP address is represented as a prefix followed by a slash and a subnet mask length. For example, "192.168.1.0/24" indicates a Class C network with a 24-bit subnet mask.

We need classless addressing and subnetting to efficiently utilize IP addresses. Classless addressing allows for efficient utilization of the limited IPv4 address space, which is essential as IPv4 addresses are becoming scarce. Subnetting within a network enables better organization, security, and management. Different subnets can be allocated to different departments or functions within an organization.

1. Use the CPT file uploaded on canvas and configure the topology using the subnet 192.168.100.0/24 efficiently. Write down the Interface IPs and subnet details in the space provided on the CPT. [**25 points**]



1. List 2 points to be noted for efficient subnetting? [ **3 points**]

-> **Subnet mask length**: Subnet sizes should align with the current number of hosts, while also leaving space for potential expansion. Subnets that are excessively large result in address space wastage, whereas overly small subnets might necessitate frequent reconfiguration.

-> **Hierarchical Structure**: Create subnets hierarchically and grouping similar subnets together. This helps in network management and also helps in routing and aggregation.

Report Questions:

1. The network graph is shown in Figure. 2.
2. Host H1 sends a packet to the destination 128.96.34.126. Explain how this packet traverses in the network described below. You need to describe who received the packet and what their reactions are. Also trace the return path that is taken. [**2 point**]

Since both H1 and 128.96.34.126 are on the same network, H1 first generates a packet destined for 128.96.34.126 and then performs an ARP lookup to find the MAC address.

H1 forwards the packet to its default gateway, R1. R1 then looks up in its ARP table and then since 128.96.34.126 does not exist, R1 would typically respond with an ICMP "Destination Host Unreachable" message back to H1, indicating that the destination is unreachable.

1. Host H3 sends a packet to the destination H1 (128.96.34.15). Explain how this packet traverses in the network. [**3 point**]

* H3 generates a packet destined for H1 with the IP address 128.96.34.15.
* H3 checks its local routing table and realizes that the destination IP address is not within its local subnet (*128.96.33.0/24*).
* H3 forwards the packet to its default gateway, which is R2 (*128.96.33.1*).
* R2 realizes that the destination IP address is not within its directly connected subnet (128.96.33.0/24).
* R2 forwards the packet to its next hop router, which is R1 (128.96.34.1) assuming R1 is advertising its connected networks to R2 appropriately.
* R1 realizes that the destination IP address is within its directly connected subnet (*128.96.34.0/25*).
* R1 performs an ARP lookup to find the MAC address of H1 (*128.96.34.15*) within the same subnet.
* Once R1 has the MAC address, it encapsulates the packet in an Ethernet frame with the destination MAC address of H1 and forwards it directly to H1 within the same subnet.
* H1 receives the packet, as it is the intended destination.

1. The subnet of H1 has now two different teams and would like to split it into two subnets. Please add one more subnet and add R3 and change the network configurations as you need. Note that you are allowed to modify the network as least disruptive as possible. [**3 point**]

**Existing Configuration**:

* H1 (128.96.34.0/25) is in the same subnet.
* R1 (128.96.34.1) is the gateway for this subnet.
* R2 (128.96.34.129) connects to R1 (128.96.34.130).
* H2 (128.96.34.139) is connected to R2.
* H3 (128.96.33.14/24) is connected to R2.

**Modified Configuration**:

* We'll introduce a new subnet for H1, creating two subnets (128.96.34.0/26 and 128.96.34.64/26).
* We'll add R3 (128.96.34.130) to handle the new subnet for H1.
* The new subnet’s machines would have 128.96.34.130 as their default gateway, whereas the existing machines which are connected to R1, do not need any config changes.
* H1a: 128.96.34.0/26 (Range: 128.96.34.0 to 128.96.34.63)
* H1b: 128.96.34.64/26 (Range: 128.96.34.64 to 128.96.34.127)
* R1 (128.96.34.1): Remains the same and connects to R2.
* R2 (128.96.34.129): Connects to R1 and R3.
* R3 (128.96.34.130): Connects to H1b (128.96.34.64/26) and R2.

This way, each router is connected in a triangle. For redundancy, we can also connect R1 and R2 and use appropriate routing protocols.

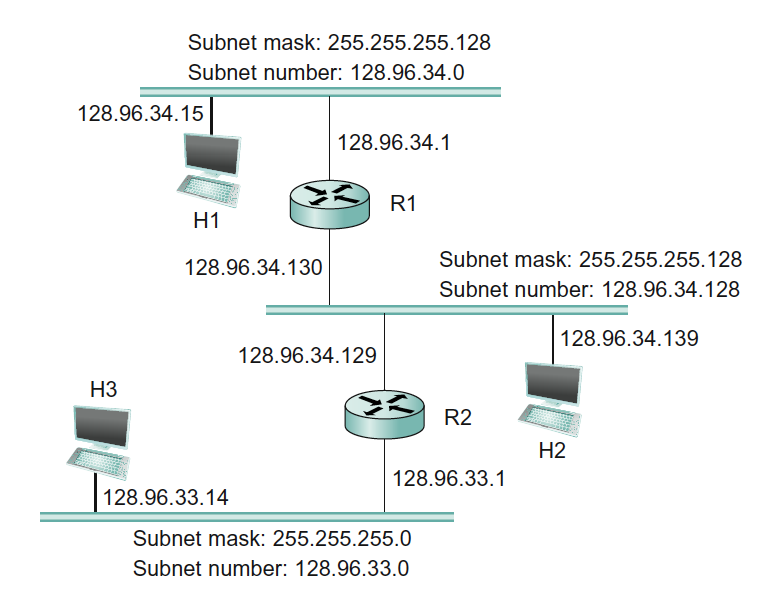


Figure 2.

1. Problem 2

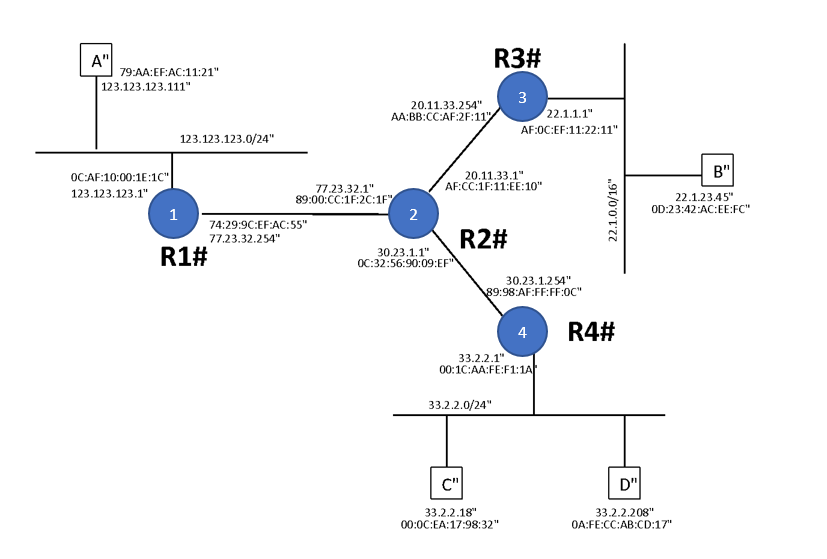


Figure. 3

Above in Figure 3 is the network graph with 4 routers (R1, R2, R3, R4) and 4 hosts (A, B, C, D). Each router interfaces and hosts are labeled with both IP and MAC address, Routing is enabled so that any two hosts can communicate with each other and also the default gateway of each host is set to its gateway router.

1. Suppose that A send an IP packet to B through R1, R2, R3. Write down the IP packet’s content (src MAC, dst MAC, src IP, dst IP) along the path in the Table given below: [**10 points**]

|  | src MAC | dst MAC | src IP | dst IP |
| --- | --- | --- | --- | --- |
| A -> R1 | 79:AA:EF:AC:11:21 | 0C:AF:10:00:1E:1C | 123.123.123.111 | 22.1.23.45 |
| R1 -> R2 | 74:29:9C:EF:AC:55 | 89:00:CC:1F:2C:1F | 123.123.123.111 | 22.1.23.45 |
| R2 -> R3 | AF:CC:1F:11:EE:10 | AA:BB:CC:AF:2F:11 | 123.123.123.111 | 22.1.23.45 |
| R3 -> B | AF:0C:EF:11:22:11 | 0D:23:42:AC:EE:FC | 123.123.123.111 | 22.1.23.45 |

Table. 1

1. When C sends out an ARP query for its default gateway, what is the reply to that query? [**2 points**]

Since Host C and the R4’s IP (default gateway) are in the same subnet, Host C will perform an ARP lookup Assuming this is the first time they are initiating the communication, Host C broadcasts asking “who has the IP 33.2.2.1?” to which R4 would respond with an ARP reply which provides the MAC address of R4. Host C would then update its ARP cache with default gateway’s (R4) MAC address.

# Total Score = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_120\_\_