ITC212 – Assessment 2

# Question 1

Part 1

Public IP address:

These are globally unique and are used for communication over the internet. Any device with a public IP can be accessed directly from the internet. These addresses are assigned by the Internet Assigned Numbers Authority (IANA) and regional internet registries.

Private IP address:

These are used within private networks (e.g., home, office networks) and are not routable on the public internet. Private IP addresses are used for internal communications and require Network Address Translation (NAT) to communicate with public IP addresses.

Examples:

Public IP: 138.74.161.89 (used by a web server accessible globally)

Private IP: 192.168.1.10 (used by a device in a home network)

Part 2

To obtain IPv4 address space for your ISP, you would need to contact one of the regional internet registries (RIRs) such as ARIN (North America), RIPE (Europe), or APNIC (Asia-Pacific) based on your geographical location. You would then apply for address blocks based on your requirements and justification.

Part 3

Student ID is 221, therefore X = 1. The address space assigned to my ISP is 138.74.161.89/21.

Subnetting and Calculations for a /21 Prefix

Address Block:

The /21 subnet mask means that the first 21 bits are network bits, and the remaining 11 bits are available for hosts.

The total address block contains 2^11 = 2048 IP addresses, with the first IP address as the network address and the last as the broadcast address.

The range of IP addresses is from 138.74.160.0 to 138.74.167.255.

1. We divide the /21 block into smaller subnets. Let's create /22 subnets (since /22 uses one additional bit for subnetting). This gives two subnets.

First subnet: 138.74.160.0/22 (IP range: 138.74.160.0 to 138.74.163.255)

Second subnet: 138.74.164.0/22 (IP range: 138.74.164.0 to 138.74.167.255)

So, the second subnet number is 138.74.164.0/22.

1. The first IP address in the second subnet is reserved for the network address (138.74.161.128), so the first usable host IP address will be 138.74.161.129.
2. The last IP address in the second subnet is reserved for the broadcast address. For the second subnet (138.74.161.128/25), the broadcast address is 138.74.161.255.

# Question 2

Part 1

Subnet 1:

The first subnet of 138.74.161.89/21 is 138.74.160.0/22.

Range: 138.74.160.0 – 138.74.163.255

Subnet 2:

The second subnet of 138.74.161.89/21 is 138.74.164.0/22.

Range: 138.74.164.0 – 138.74.167.255

Subnet 3:

The third subnet of 138.74.161.89/21 is 138.74.168.0/22.

Range: 138.74.168.0 – 138.74.171.255

Subnet 1: 138.74.160.0/22

Computer A: 138.74.160.1/22

Computer B: 138.74.160.2/22

Router 1 Interface (R1-S1): 138.74.160.254/22

Subnet 2: 138.74.164.0/22

Computer C: 138.74.164.1/22

Computer D: 138.74.164.2/22

Router 1 Interface (R1-S2): 138.74.164.254/22

Router 2 Interface (R2-S2): 138.74.164.253/22

Subnet 3: 138.74.168.0/22

Computer E: 138.74.168.1/22

Computer F: 138.74.168.2/22

Router 2 Interface (R2-S3): 138.74.168.254/22

Part 2

Subnet 1:

A MAC: 00:1A:11:AA:BB:01

B MAC: 00:1A:11:AA:BB:02

R1-S1 (Router 1 interface for Subnet 1) MAC: 00:1A:11:AA:BB

Subnet 2:

C MAC: 00:1A:22:BB:CC:01

D MAC: 00:1A:22:BB:CC:02

R1-S2 (Router 1 interface for Subnet 2) MAC: 00:1A:22:BB:CC

R2-S2 (Router 2 interface for Subnet 2) MAC: 00:1A:22:BB:CC

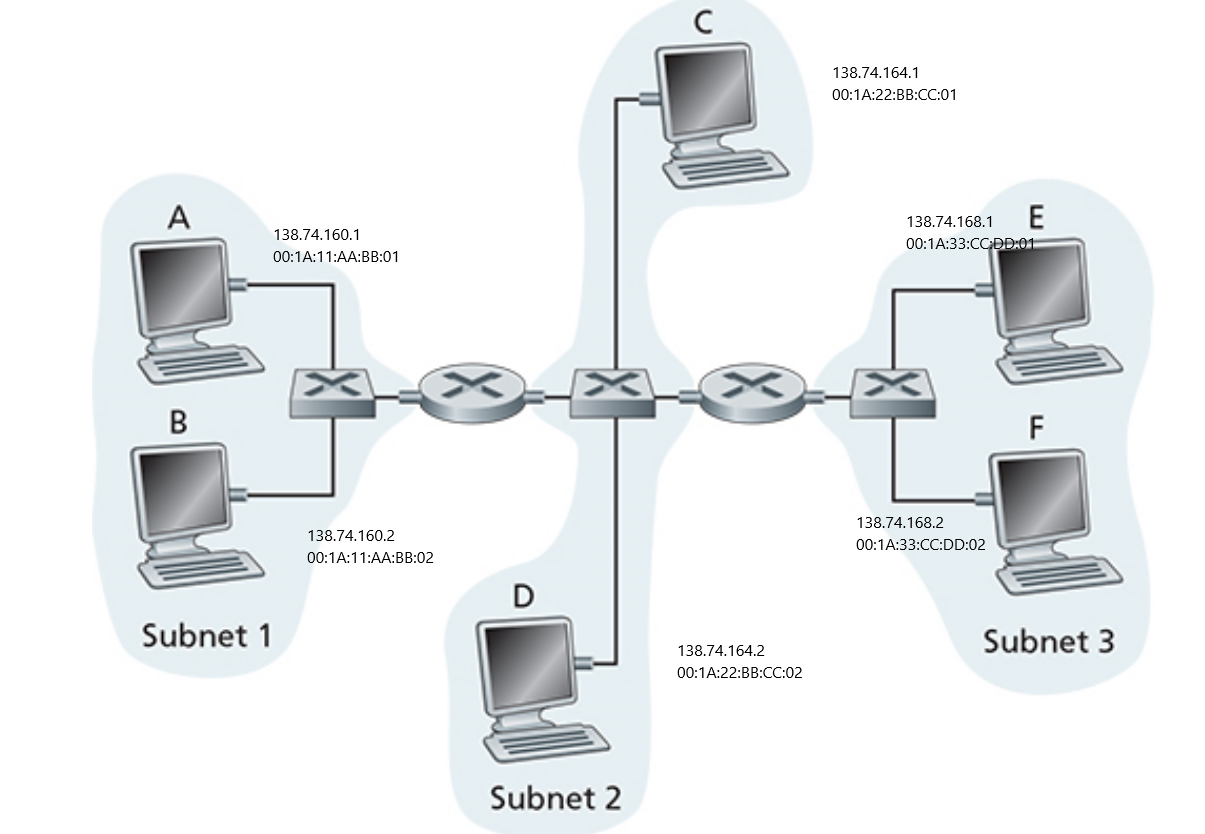
Subnet 3:

E MAC: 00:1A:33:CC:DD:01

F MAC: 00:1A:33:CC:DD:02

R2-S3 (Router 2 interface for Subnet 3) MAC: 00:1A:33:CC:DD

Part 3



Part 4

When sending an IP datagram from Host A (on Subnet 1) to Host F (on Subnet 3), several key steps occur in the communication process, involving both Layer 3 (IP) and Layer 2 (Ethernet) functions.

Host A → R1 (Router 1): Host A sends an Ethernet frame to R1 using its MAC address for Subnet 1.

R1 → R2 (Router 2): R1 forwards the packet to R2 via Subnet 2, using their respective MAC addresses for that subnet.

R2 → Host F: R2 sends the packet to Host F on Subnet 3 using the MAC address of Host F.

Part 5

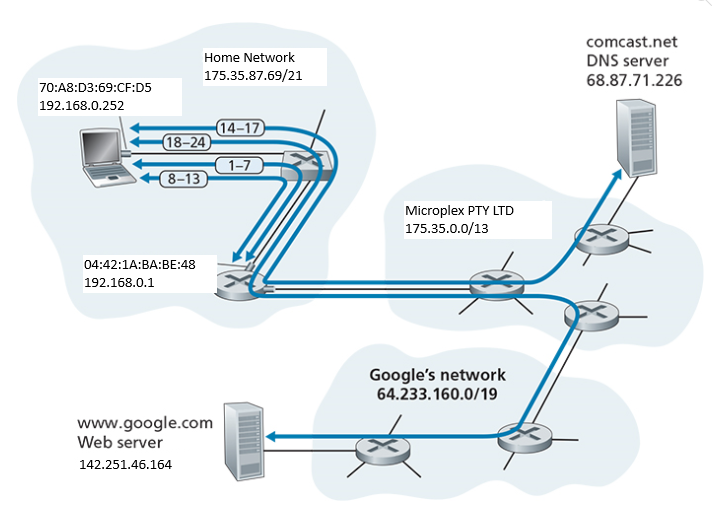
Switches, especially Layer 2 switches, traditionally operate by forwarding Ethernet frames based on MAC addresses and do not require IP addresses for basic switching operations. However, there are certain situations where assigning an IP address to a switch is necessary or beneficial.

One of the most common reasons for assigning an IP address to a switch is to enable remote management and monitoring. This allows network administrators to configure and manage the switch over the network using protocols like SSH, Telnet, or HTTP/HTTPS through the switch's management interface. E.g. A network administrator wants to remotely configure a switch or check its performance from a central location. Assigning an IP address allows the administrator to access the switch’s web interface or use CLI tools like SSH.

Switches often require time synchronization for logging and tracking network events. To synchronize with an NTP server, the switch must have an IP address so it can communicate with the NTP server and maintain accurate time. E.g. A switch needs to synchronize with an NTP server at 192.168.1.100 to ensure that logs are time-stamped correctly.

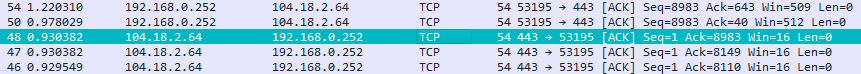
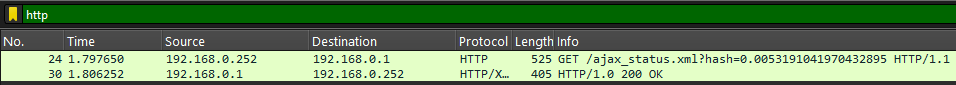
# Question 3

Part 1



1. 192.168.0.252
2. 192.168.0.1
3. 192.168.0.1
4. 142.261.46.164
5. Servers often require more than one IP address for various technical reasons, particularly when hosting multiple websites, managing load balancing, enhancing security, or running different services. For instance, in virtual hosting, a server might host multiple websites, and while many can share the same IP, some configurations, like SSL/TLS for older clients, demand a unique IP per site. Similarly, in load-balanced environments, multiple IP addresses allow traffic distribution across servers, improving performance and ensuring redundancy. Additionally, servers often connect to different network zones, such as internal and public networks, and multiple IPs help secure and segment this traffic. Finally, when running different services, such as a web server and mail server, separate IP addresses enable fine-tuned control over traffic, firewall rules, and port forwarding configurations.
6. 175.35.87.69

Part 2

1. The pairs of numbers refer to port ranges used by network communication processes. In networking, ports are essential for differentiating services on a computer.
2. 
3. 
4. The Time to Live (TTL) number is a field in the header of an IP packet that specifies the maximum number of hops (routers or network nodes) the packet is allowed to pass through before being discarded. Each time the packet passes through a router, the TTL value is decremented by one. When the TTL reaches zero, the packet is dropped, and the sender may receive a notification that the packet was not delivered.
5. The HTTP request provided is a GET request, which is one of the most common methods used in the HTTP protocol. The client (using HTTP/1.1) is making a GET request to the host www.bright.com, asking for the resource /weather.pdf. The client prefers the response in English as indicated by the Accept-Language: en field.