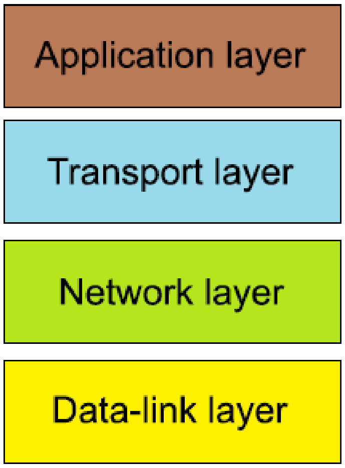
Exercise 1



TCP/IP Model

Application Layer: Interfaces with user applications and provides network services (HTTP, FTP, SMTP).

Transport Layer: Ensures reliable data transfer with error checking and flow control (TCP, UDP).

Network Layer: Manages logical addressing and routing packets (IP, ICMP, IGMP).

Data-Link Layer: Handles physical addressing, error detection, and correction (Ethernet, PPP, ARP).

Exercise 2

IP address 192.168.1.0/24

a) Network Address, Broadcast Address, and Range of Usable IP Addresses

1. **Network Address:**
   - It is the first address in the subnet.
   - Network Address: 192.168.1.0

2. **Broadcast Address:**

- It is the last in the subnet.
- Broadcast Address: 192.168.1.255

3. **Range of Usable IP Addresses:**

- Range from the first address after the network address to the address before the broadcast address.
- Range of Usable IP Addresses: 192.168.1.1 to 192.168.1.254

b) Subdivide the Network into 4 Smaller Subnets

To subdivide the 192.168.1.0/24 network into 4 smaller subnets, we need to borrow 2 bits from the host part of the address. This will give us 4 subnets, each with 64 addresses. The new subnet mask will be /26 (since 24 + 2 = 26).

Each /26 subnet will have 64 addresses, where 62 are usable.

- **Subnet 1:**
  - **Network Address:** 192.168.1.0/26
  - **Broadcast Address:** 192.168.1.63
  - **Range of Usable IP Addresses:** 192.168.1.1 to 192.168.1.62

- **Subnet 2:**
  - **Network Address:** 192.168.1.64/26
  - **Broadcast Address:** 192.168.1.127
  - **Range of Usable IP Addresses:** 192.168.1.65 to 192.168.1.126

- **Subnet 3:**
  - **Network Address:** 192.168.1.128/26
  - **Broadcast Address:** 192.168.1.191
  - **Range of Usable IP Addresses:** 192.168.1.129 to 192.168.1.190

- **Subnet 4:**

- **Network Address:** 192.168.1.192/26
- **Broadcast Address:** 192.168.1.255
- **Range of Usable IP Addresses:** 192.168.1.193 to 192.168.1.254

Exercise 3

TCP Three-Way Handshake Process

- **SYN (Synchronize):**
- The client sends a SYN packet to the server to initiate a connection.
- The packet includes an initial sequence number (ISN) chosen by the client.
- **SYN-ACK (Synchronize-Acknowledge):**
- The server responds with a SYN-ACK packet.
- The packet includes the server's own ISN and an acknowledgment number, which is the client's ISN + 1.
- **ACK (Acknowledge):**
- The client sends an ACK packet back to the server.
- The packet includes an acknowledgment number, which is the server's ISN + 1

Importance of the Three-Way Handshake

- **Connection Establishment:** Ensures both the client and server agree on the initial sequence numbers, establishing a synchronized state for communication.
- **Reliability:** Confirms that both parties are ready to transmit data, preventing data loss or miscommunication.
- **Flow Control:** Sets the stage for managing data flow and ensuring orderly and error-checked delivery of data packets.

Exercise 4

Comparison of TCP and UDP

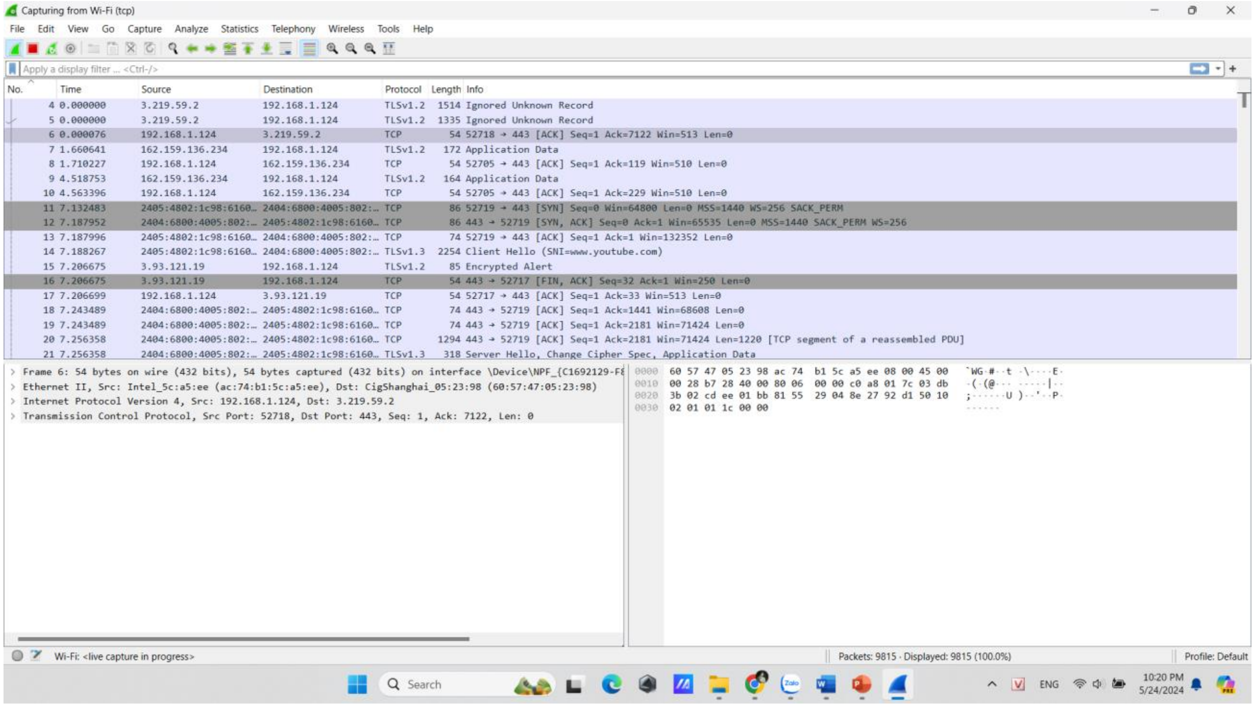
- **Transmission Control Protocol (TCP):**

  - Connection-Oriented: Establishes a connection through a three-way handshake before data transmission.
  - Reliable: Ensures data delivery with error checking, acknowledgments, and retransmissions.
  - Ordered: Guarantees that packets arrive in the same order they were sent.
  - Flow Control: Manages data flow to prevent congestion.
  - Overhead: Higher due to additional features like error correction and flow control.
- **User Datagram Protocol (UDP):**
  - Connectionless: Sends data without establishing a connection.
  - Unreliable: No guarantee of delivery, no error checking, or retransmissions.
  - Unordered: Packets may arrive out of order.
  - No Flow Control: Does not manage data flow, potentially leading to packet loss.
  - Low Overhead: Minimal protocol mechanisms, making it faster and more efficient for certain applications.

➢ TCP: Best for applications requiring reliable, ordered, and error-checked delivery (e.g., web browsing, email, file transfer).

➢ UDP: Ideal for applications needing speed and efficiency over reliability (e.g., video streaming, online gaming, VoIP).

Exercise 5


Capturing from Wi-Fi (tcp)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Search
ENG
10:20 PM
5/24/2024

```
No.  Time      Source              Destination          Protocol Length Info
   4 0.000000  3.219.59.2          192.168.1.124        TLSv1.2  1514 Ignored Unknown Record
   5 0.000000  3.219.59.2          192.168.1.124        TLSv1.2  1335 Ignored Unknown Record
   6 0.000076  192.168.1.124       3.219.59.2           TCP        54 52718 → 443 [ACK] Seq=1 Ack=7122 Win=513 Len=0
   7 1.660641  162.159.136.234     192.168.1.124        TLSv1.2   172 Application Data
   8 1.710227  192.168.1.124       162.159.136.234      TCP        54 52705 → 443 [ACK] Seq=1 Ack=119 Win=510 Len=0
   9 4.518753  162.159.136.234     192.168.1.124        TLSv1.2   164 Application Data
  10 4.563396  192.168.1.124       162.159.136.234      TCP        54 52705 → 443 [ACK] Seq=1 Ack=229 Win=510 Len=0
  11 7.132483  2405:4802:1c98:6160… 2404:6800:4005:802:… TCP      86 52719 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
  12 7.187952  2404:6800:4005:802:… 2405:4802:1c98:6160… TCP      86 443 → 52719 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM WS=256
  13 7.187996  2405:4802:1c98:6160… 2404:6800:4005:802:… TCP      74 52719 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
  14 7.188267  2405:4802:1c98:6160… 2404:6800:4005:802:… TLSv1.3 2254 Client Hello (SNI=www.youtube.com)
  15 7.206675  3.93.121.19         192.168.1.124        TLSv1.2    85 Encrypted Alert
  16 7.206675  3.93.121.19         192.168.1.124        TCP        54 443 → 52717 [FIN, ACK] Seq=32 Ack=1 Win=250 Len=0
  17 7.206699  192.168.1.124       3.93.121.19          TCP        54 52717 → 443 [ACK] Seq=1 Ack=33 Win=513 Len=0
  18 7.243489  2404:6800:4005:802:… 2405:4802:1c98:6160… TCP      74 443 → 52719 [ACK] Seq=1 Ack=1441 Win=68608 Len=0
  19 7.243489  2404:6800:4005:802:… 2405:4802:1c98:6160… TCP      74 443 → 52719 [ACK] Seq=1 Ack=2181 Win=71424 Len=0
  20 7.256358  2404:6800:4005:802:… 2405:4802:1c98:6160… TCP    1294 443 → 52719 [ACK] Seq=1 Ack=2181 Win=71424 Len=1220 [TCP segment of a reassembled PDU]
  21 7.256358  2404:6800:4005:802:… 2405:4802:1c98:6160… TLSv1.3  318 Server Hello, Change Cipher Spec, Application Data
```

```
> Frame 6: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{C1692129-F8
> Ethernet II, Src: Intel_5c:a5:ee (ac:74:b1:5c:a5:ee), Dst: CigShanghai_05:23:98 (60:57:47:05:23:98)
> Internet Protocol Version 4, Src: 192.168.1.124, Dst: 3.219.59.2
> Transmission Control Protocol, Src Port: 52718, Dst Port: 443, Seq: 1, Ack: 7122, Len: 0
```

```
0000  60 57 47 05 23 98 ac 74  b1 5c a5 ee 08 00 45 00   `WG·#··t ·\····E·
0010  00 28 b7 28 40 00 80 06  00 00 c0 a8 01 7c 03 db   ·(·(@··· ·····|··
0020  3b 02 cd ee 01 bb 81 55  29 04 8e 27 92 d1 50 10   ;······U )··'··P·
0030  02 01 01 1c 00 00                                  ······
```

```
Wi-Fi: <live capture in progress>    Packets: 9815 · Displayed: 9815 (100.0%)    Profile: Default
```

In the TCP packet No.6

- **Source IP address:** 192.168.1.124
- **Destination IP address:** 3.219.59.2
- **Source port number:** 52718
- **Destination port number:** 443
- **TCP control flags:** ACK

Exercise 6

- **Role of the ARP Protocol in a TCP/IP Network**
- Address Resolution Protocol (ARP) is used to map an IP address to a physical machine address (MAC address) in a local network. This is essential for communication within a local network segment.

- **ARP Works to Find a MAC Address**
- **ARP Request:**
- Broadcast: The device sends an ARP request packet to all devices on the local network.

- Content: The request contains the IP address of the target device and asks, "Who has this IP address?"

- **ARP Response:**
- Unicast Response: The device with the matching IP address replies with an ARP response.
- Content: The response includes its own MAC address.

- **MAC Address Mapping:**
  - Update ARP Cache: The requesting device updates its ARP cache with the IP-to-MAC address mapping for future use.

Exercise 7

Network Address Translation (NAT) work:

- Function: Translates private IP addresses to public IP addresses and vice versa.
- Purpose: Allows devices on a private network to access resources on the Internet using a single public IP address.

NAT is Necessary for TCP/IP Networks

- **Address Scarcity:**
  - Public IPv4 addresses are limited and expensive.
  - NAT conserves public IP addresses by allowing multiple devices on a private network to share a single public IP address.
- **Security:**
- Acts as a barrier between the public Internet and private networks.
- Hides internal IP addresses, providing an additional layer of security.

Example of NAT in Use

- **Outbound Traffic:**

Port Number: The router keeps track of the outgoing requests by assigning unique port numbers.

Exercise 8

DNS Works in a TCP/IP Network

1. **User Enters Domain Name:**
   - A user types a domain name (e.g., www.example.com) into a web browser.
2. **DNS Query Initiation:**
   - The browser sends a DNS query to the local DNS resolver, usually managed by the user's ISP.
3. **Resolver Checks Cache:**
   - The DNS resolver checks its cache to see if it has a recent record for the domain name.
4. **Recursive Query:**
   - If not found in the cache, the resolver sends a query to a root DNS server.
5. **Root Server Response:**
   - The root server responds with a referral to the appropriate Top-Level Domain (TLD) server (e.g., .com).
6. **TLD Server Query:**
   - The resolver queries the TLD server.
7. **TLD Server Response:**
   - The TLD server responds with a referral to the authoritative DNS server for the domain (e.g., example.com).
8. **Authoritative Server Query:**
   - The resolver queries the authoritative DNS server.
9. **IP Address Resolution:**
   - The authoritative DNS server responds with the IP address for the domain.
10. **Response to Browser:**
    - The DNS resolver returns the IP address to the browser.
11. **Connection Establishment:**
    - The browser uses the IP address to establish a connection to the web server and loads the website.

Exercise 9

- **Functions of the Transport Layer**

Transport Layer (Layer 4):

- End-to-End Communication: Facilitates communication between processes running on different hosts.
- Reliability: Ensures data delivery, error detection, and retransmission if necessary.
- Flow Control: Manages the rate of data transmission to prevent congestion.
- Multiplexing/Demultiplexing: Allows multiple applications to use the network simultaneously by assigning unique identifiers to data streams.

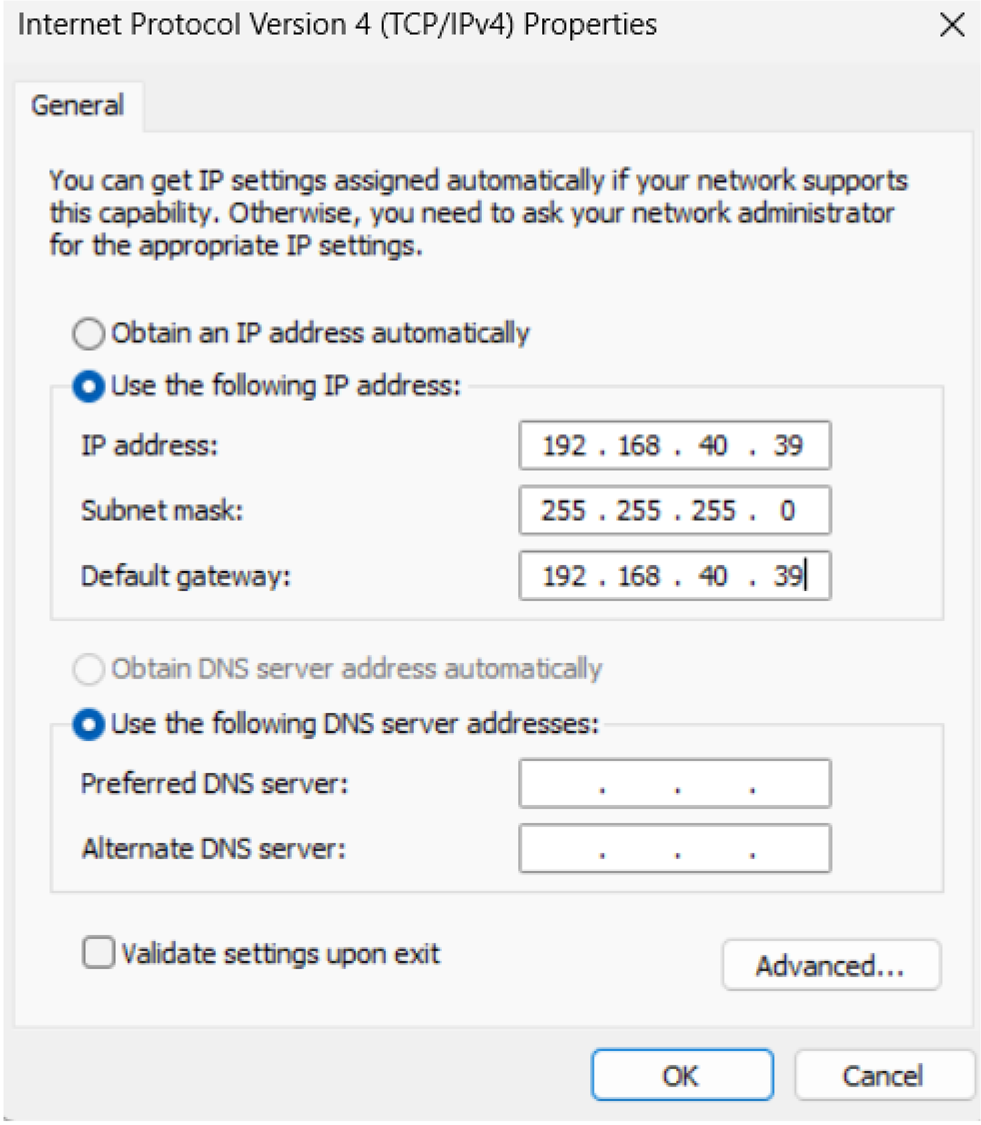
Comparison of TCP and UDP

- **Transmission Control Protocol (TCP):**
- Reliable: Provides reliable, connection-oriented communication.
- Error Detection and Correction: Includes mechanisms for error detection, acknowledgment, and retransmission.
- Ordered Delivery: Ensures data packets arrive in the correct order.
- Examples: Web browsing (HTTP), file transfer (FTP), email (SMTP).

- **User Datagram Protocol (UDP):**
- Unreliable: Provides connectionless, best-effort communication.
- No Error Handling: Does not include error detection, acknowledgment, or retransmission mechanisms.
- Low Overhead: Minimal protocol overhead, making it faster than TCP.
- Examples: Real-time applications (VoIP, video streaming), online gaming, DNS.

Exercise 10

a,



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 40 . 39

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 40 . 39

○ Obtain DNS server address automatically

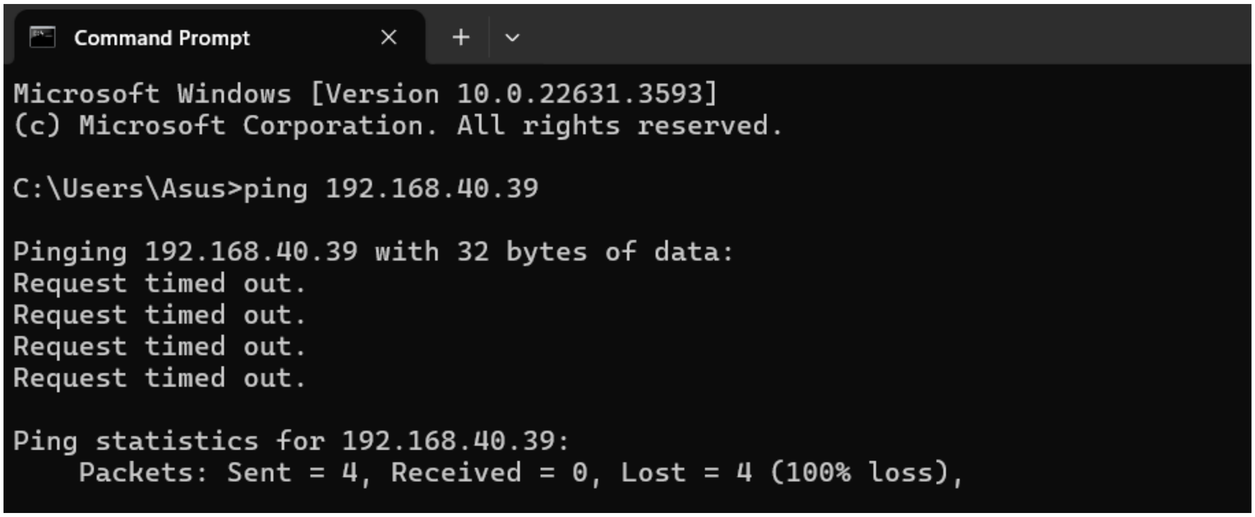
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

b,



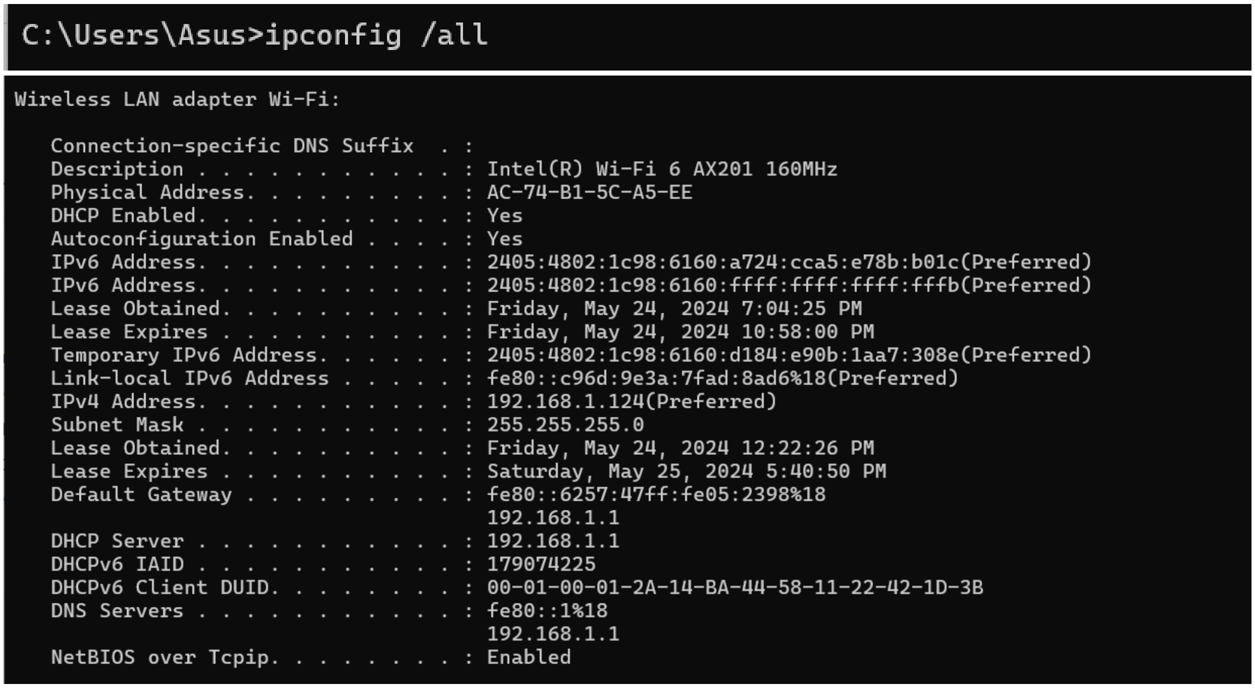
```
Microsoft Windows [Version 10.0.22631.3593]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Asus>ping 192.168.40.39

Pinging 192.168.40.39 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.40.39:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

c,



```
C:\Users\Asus>ipconfig /all
```

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   Physical Address. . . . . . . . . : AC-74-B1-5C-A5-EE
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2405:4802:1c98:6160:a724:cca5:e78b:b01c(Preferred)
   IPv6 Address. . . . . . . . . . . : 2405:4802:1c98:6160:ffff:ffff:ffff:fffb(Preferred)
   Lease Obtained. . . . . . . . . . : Friday, May 24, 2024 7:04:25 PM
   Lease Expires . . . . . . . . . . : Friday, May 24, 2024 10:58:00 PM
   Temporary IPv6 Address. . . . . . : 2405:4802:1c98:6160:d184:e90b:1aa7:308e(Preferred)
   Link-local IPv6 Address . . . . . : fe80::c96d:9e3a:7fad:8ad6%18(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.124(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, May 24, 2024 12:22:26 PM
   Lease Expires . . . . . . . . . . : Saturday, May 25, 2024 5:40:50 PM
   Default Gateway . . . . . . . . . : fe80::6257:47ff:fe05:2398%18
                                       192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 179074225
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-14-BA-44-58-11-22-42-1D-3B
   DNS Servers . . . . . . . . . . . : fe80::1%18
                                       192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

- **IPv4 Address:** The current IP address assigned to this device within the local network. In this case, it’s 192.168.1.2.
- **Subnet Mask:** Defines which portion of an IP address is allocated to the network and which part is available for host use within that network. The subnet mask 255.255.255.0 indicates a /24 subnet.

- **Default Gateway:** The IP address of the routing device used to send traffic to other networks if a specific route does not exist on the local network. In this case, it’s 192.168.1.1.