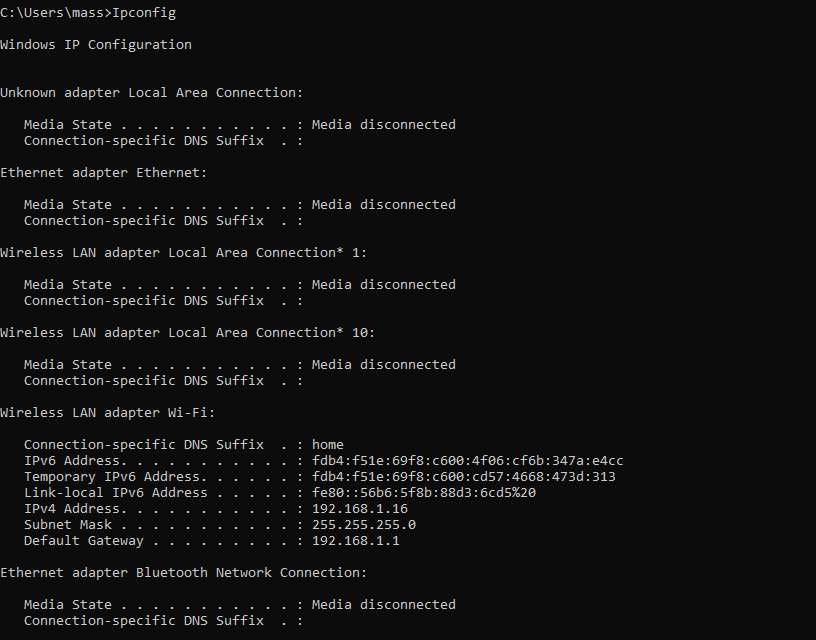
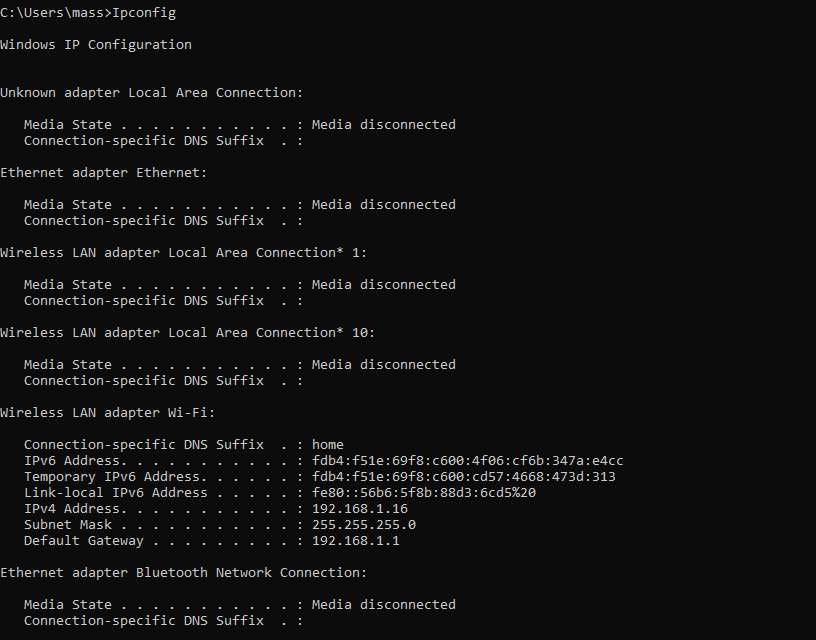
**Network LAB 1**

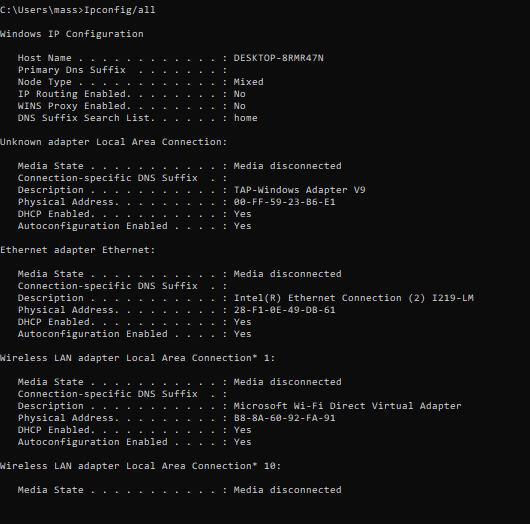
Q1: explain how to get the private IP?

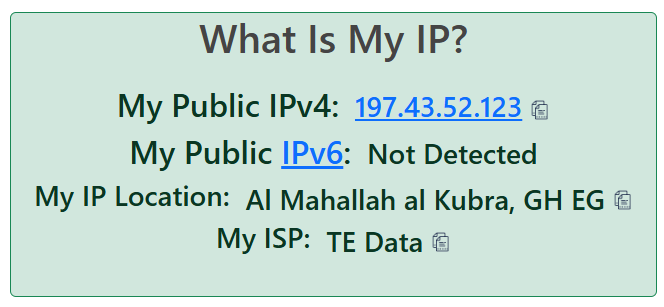


Q2: What is the difference between ipconfig & ipconfig/all?

|  |  |  |  |
| --- | --- | --- | --- |
|  | purpose | Details shown | usage |
| Ipconfig | Displays a **basic overview** of your network interfaces. | IP, Subnet Mask, Default Gateway | you need a quick glance at your IP address and gateway |
| Ipconfig/all | Displays **detailed and complete information** about all network interfaces. | Everything from ipconfig plus MAC, DHCP and DNS | when troubleshooting or configuring networks, as it provides comprehensive details. |





Q3: explain how to get the public IP?

Q4: What is the difference between public ip & private ip?

**Public IP:** Acts as the address for your entire network on the internet. Only one public IP is typically assigned to a network by an ISP.

**Private IP:** Used to uniquely identify devices within a local network. Devices behind a private IP connect to the internet through NAT, which translates private IPs to the public IP.

Q5: How does the device get its IP?

1. Dynamic IP Assignment (Most Common)

This method uses the Dynamic Host Configuration Protocol (DHCP), which is usually handled by the router or ISP.

Steps:

* Device Connection:

When a device connects to a network, it sends a DHCP Discover message to request an IP address.

* DHCP Server Responds:

The DHCP server (usually your router) assigns an available IP address from its pool and sends it to the device.

* Lease Time:

The IP address is assigned temporarily for a "lease time." Once the lease expires, the device must request a new IP.

* Network Details Provided:

Along with the IP, the DHCP server also sends information like:

Subnet mask

Default gateway (router's IP)

DNS server addresses

2. Static IP Assignment

In some cases, an IP address is manually assigned to a device.

Steps:

* A network administrator assigns a specific IP address to the device.
* The user enters the IP address, subnet mask, and gateway details manually in the device’s network settings.
* The device uses this static IP permanently unless changed.

Use Cases: Servers, printers, or devices needing consistent network access.

3. Public IP Address Assignment

For devices or networks connected to the internet, public IPs are assigned by the ISP.

Steps :

* The ISP assigns a dynamic public IP by default through their DHCP servers.
* If a static public IP is requested, the ISP manually assigns one to your router or modem.

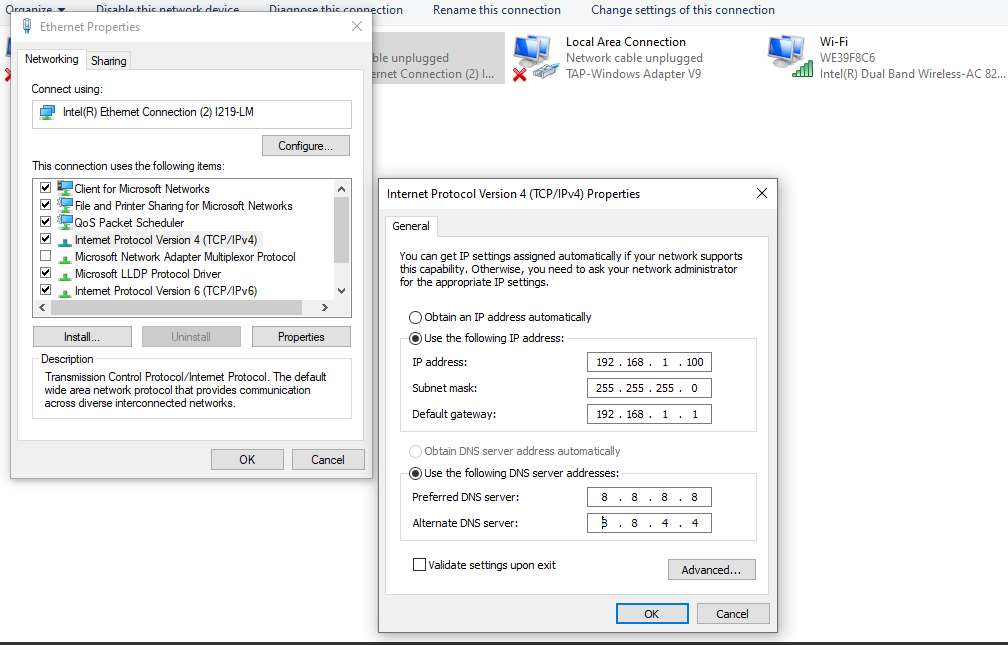
4. Automatic Private IP Assignment

If a device can't contact a DHCP server, it assigns itself an Automatic Private IP Address (APIPA).

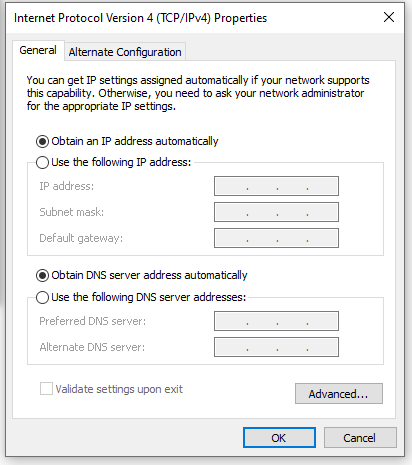
Key Points:

* This is a fallback mechanism.
* The IP range is 169.254.x.x.
* The device can only communicate with other devices in the same network but not access the internet.

Q6: Make your device get its private IP statically?



Q7: Reset your device to get its private IP automatically?



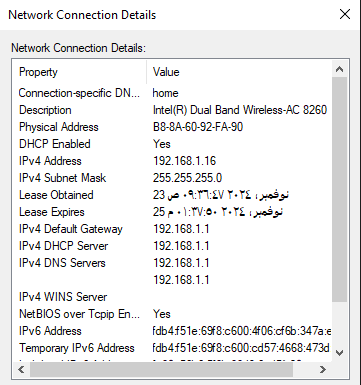
Q8: What do you know about APIPA Address ?

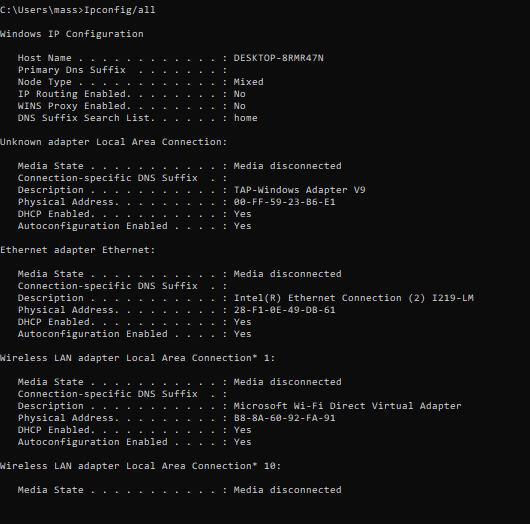
**APIPA (Automatic Private IP Addressing)** is a feature in operating systems (such as Windows, macOS, and Linux) that allows devices to assign themselves an IP address automatically when they are unable to obtain one from a **DHCP server**.

### ****Key Characteristics of APIPA****

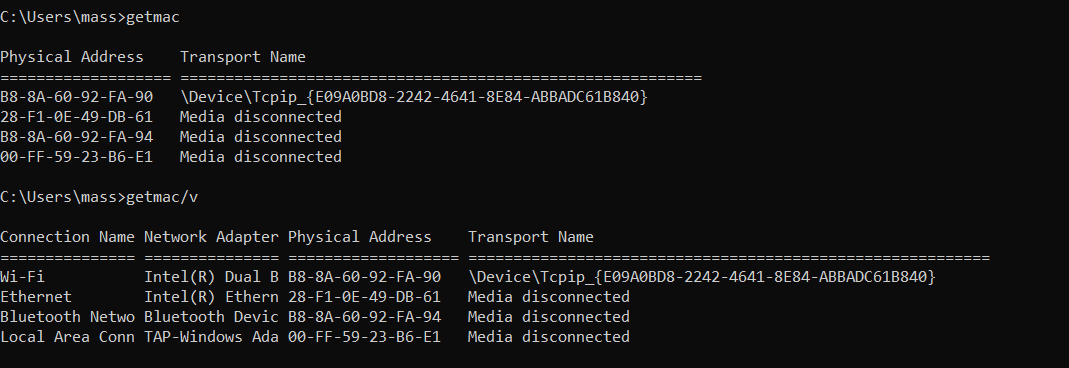
1. **IP Range**:
   * APIPA uses a specific reserved range of IP addresses:  
     **169.254.0.1 to 169.254.255.254**.
   * The subnet mask is always 255.255.0.0.
2. **Purpose**:
   * Provides a fallback mechanism for devices to communicate with each other on the same local network when no DHCP server is available.
3. **Local Network Only**:
   * APIPA allows communication only within the same subnet.
   * Devices using APIPA addresses cannot access the internet.
4. **Automatic Assignment**:
   * If a device cannot contact a DHCP server, it will automatically pick an address from the 169.254.x.x range.

Q9: Give me 2 ways to find out your device's MAC address.



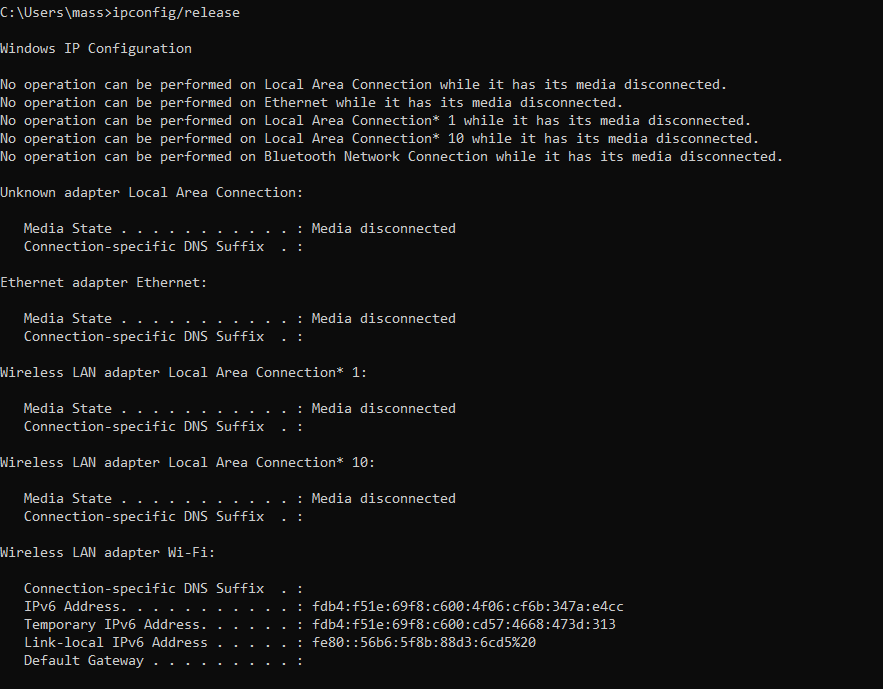


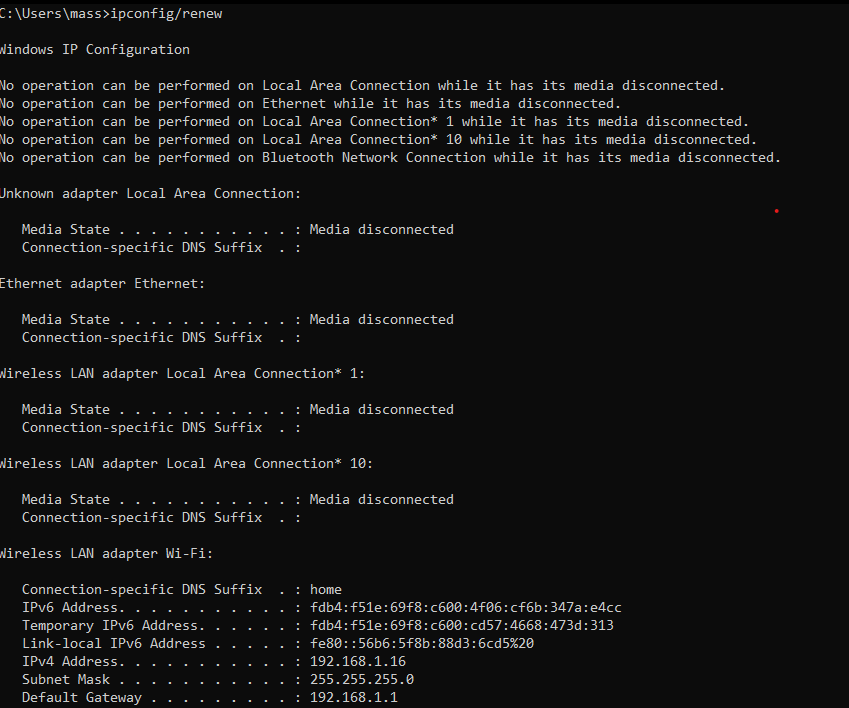
Q10: What is the difference between getmac & getmac/v ?



* getmac command: shows a basic list of the **MAC addresses** and the **transport names** of all network interfaces on your computer.
* Getmac/v It provides **more detailed information**, including the **connection status** of each network interface, and the **connection description**

Q11: How can you request a new IP from a DHCP server?

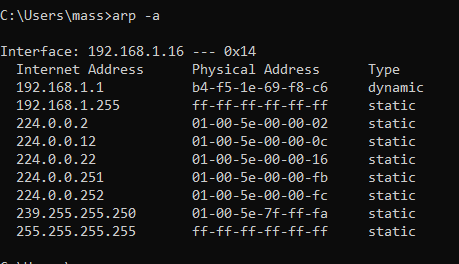




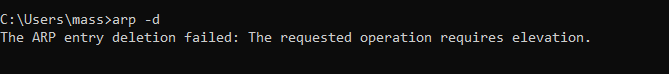
Q12: Explain what you understand about ARP protocol?

ARP plays a critical role in ensuring that devices on a local network can communicate with each other by resolving IP addresses to MAC addresses, allowing packets to be correctly directed within the network.

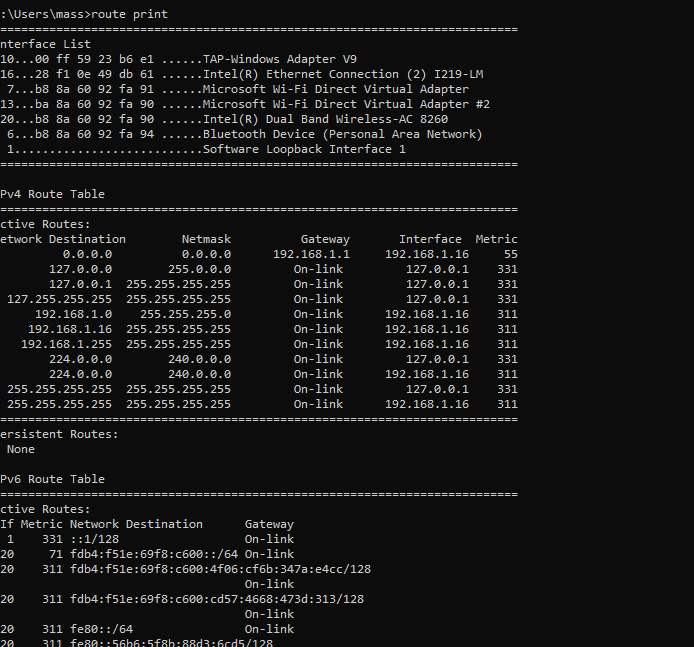
Q13. How do we view the contents of the ARP cache?



Q14. How do we delete the ARP cache?

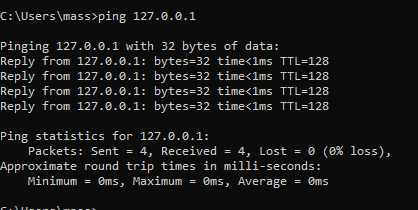


Q15. How do we view the local routing table?



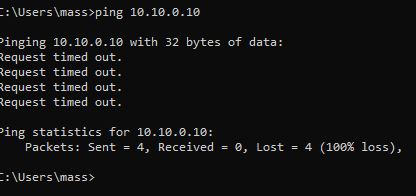
Q16. Can you tell me which command that could check connectivity between 2 devices?

Ping command



**2. Sent** equals the **Received** (Sent = 4, Received = 4), it means there is **no packet loss**, and the connectivity is functioning perfectly.

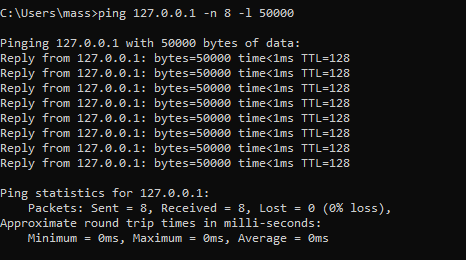
4.



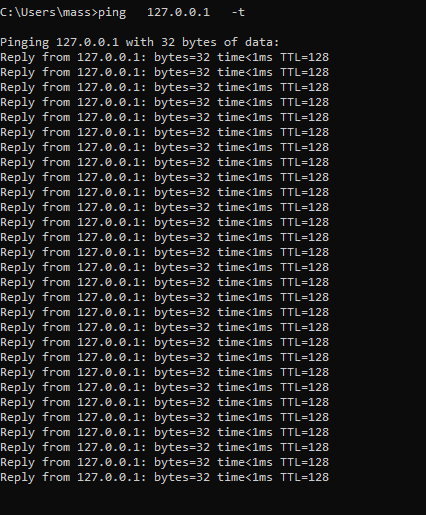
**Request Timed Out:** The packets were sent, but no response was received. Possible causes:

* The IP is not active.
* A firewall is blocking ICMP packets.

Q17. Verify the connectivity of the loopback IP address "127.0.0.1" by sending “8” packets which the size of each packet is "50000"?



Q18. Explain what is the meaning of this command: “ping 127.0.0.1 -t “?



**-t**: A flag specific to **Windows**, which means to send packets **continuously** without stopping

Q19. What is the meaning of “ DOS Attack” ?

A **DoS (Denial of Service) attack** is a cyberattack designed to make a system, server, or network unavailable by overwhelming it with excessive requests or exploiting vulnerabilities. This disrupts normal operations, preventing legitimate users from accessing the service.

Key points:

* **Single Source**: The attack originates from one source.
* **Techniques**: Includes flooding (e.g., SYN flood, ping flood) or crashing systems via vulnerabilities.
* **Impact**: Causes service downtime, financial losses, and reputational damage.
* **Mitigation**: Use firewalls, rate limiting, and network monitoring to detect and block malicious activity.

This contrasts with a **DDoS attack**, which uses multiple sources for greater disruption.

Esraa tark mohammed foda

Os