Network Configuration & Troubleshooting: Technical Report

1. Overview

understanding and utilizing core network troubleshooting tools is critical in ensuring secure and reliable communication across systems. This document provides a professional breakdown of essential networking concepts and commands used for diagnostics and troubleshooting techniques.

---

2. IP Addressing and Subnetting

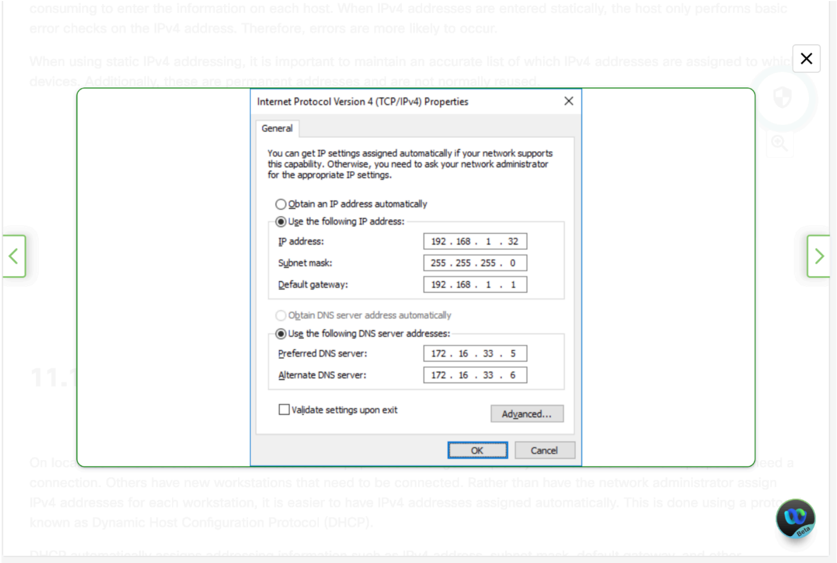
2.1 IP Addressing

An IP address is a numerical label assigned to each device connected to a network that uses the Internet Protocol. There are two types:

- **IPv4**: 32-bit address written as four octets (e.g., 192.168.1.1).
- **IPv6**: 128-bit address written in hexadecimal.

2.2 Static vs. Dynamic IP Addressing

- **Static IP**: Manually assigned; best for servers.
- **taDynamic IP**: Assigned via DHCP; commonly used for clients.



consuming to enter the information on each host. When IPv4 addresses are entered statically, the host only performs basic error checks on the IPv4 address. Therefore, errors are more likely to occur.

When using static IPv4 addressing, it is important to maintain an accurate list of which IPv4 addresses are assigned to whic devices. Additionally, these are permanent addresses and are not normally reused.

Internet Protocol Version 4 (TCP/IPv4) Properties

General

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 . 1 . 32
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 172 . 16 . 33 . 5
Alternate DNS server: 172 . 16 . 33 . 6

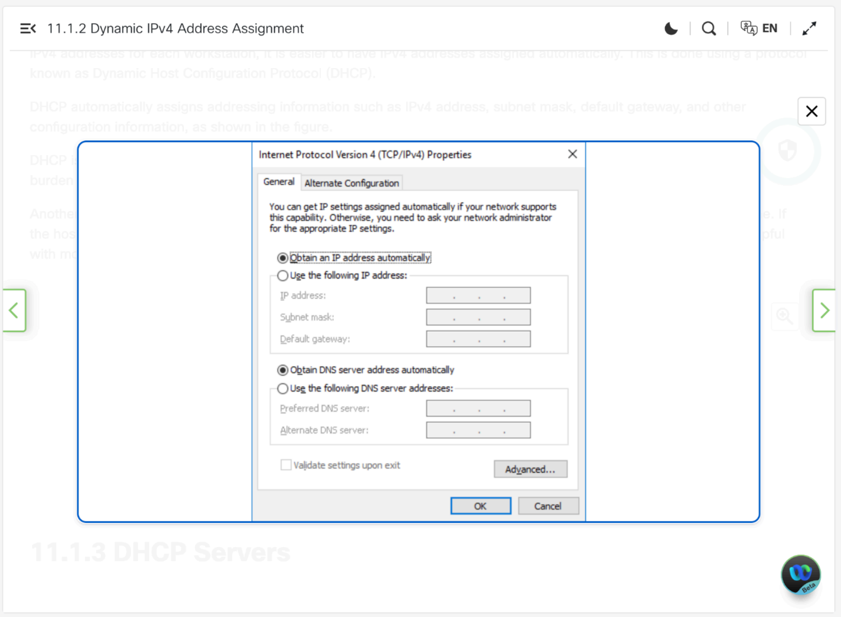
□ Validate settings upon exit

connection. Others have new workstations that need to be connected. Rather than have the network administrator assign IPv4 addresses for each workstation, it is easier to have IPv4 addresses assigned automatically. This is done using a proto known as Dynamic Host Configuration Protocol (DHCP).

Fig: Static IP Addressing

Steps to Assign Static IP on Windows:

1. Open Control Panel > Network and Sharing Center.
2. Click on "Change adapter settings."
3. Right-click on your network adapter > Properties.
4. Select "Internet Protocol Version 4 (TCP/IPv4)."
5. Click on "Use the following IP address."
6. Enter IP, Subnet Mask, Default Gateway, and DNS.



11.1.2 Dynamic IPv4 Address Assignment

Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

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: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

Fig: DHCP Assigning

Steps to Configure DHCP:

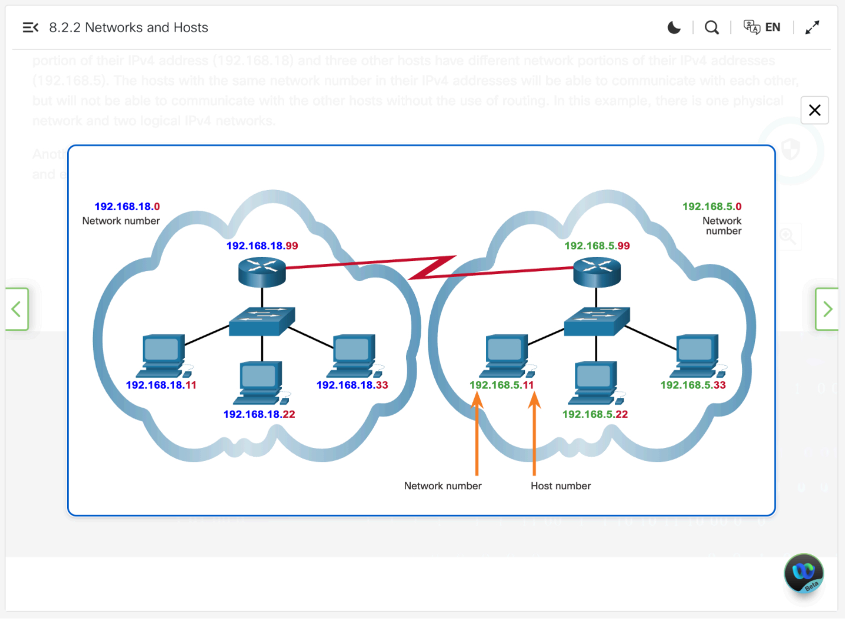
1. Ensure DHCP server is available (usually the router).
2. Set your client IP settings to “Obtain an IP address automatically.”

2.3 Subnetting

Subnetting divides a larger network into smaller sub-networks. It helps in efficient IP management and enhances security and performance.

Steps to Perform Subnetting:

1. Identify the IP class (A, B, C).
2. Determine the number of required subnets or hosts.
3. Calculate the new subnet mask.
4. Determine the block size (256 - subnet mask).
5. List subnets: Network ID, first host, last host, and broadcast address.



portion of their IPv4 address (192.168.18) and three other hosts have different network portions of their IPv4 addresses (192.168.5). The hosts with the same network number in their IPv4 addresses will be able to communicate with each other, but will not be able to communicate with the other hosts without the use of routing. In this example, there is one physical network and two logical IPv4 networks.

Ano
and

Example:

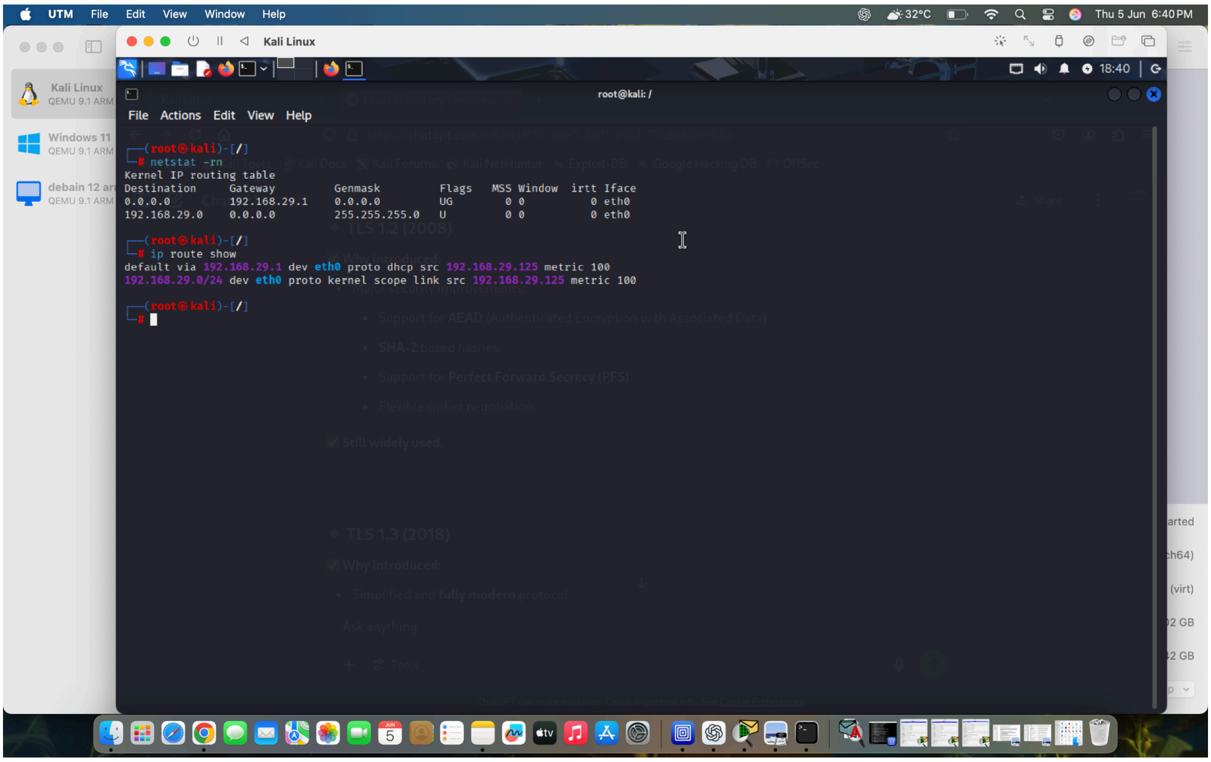
- IP: 192.168.10.0
- Need: 4 subnets
- Subnet Mask: 255.255.255.0(/24)
- Subnets:
  - 192.168.10.0/24
  - 192.168.10.64/24
  - 192.168.10.128/24
  - 192.168.10.192/24

3. Routing Table

The routing table maintains paths to network destinations. It helps routers and hosts determine the best path for outbound packets.

Command:

- Windows: `route print`
- Linux/macOS: `netstat -rn`

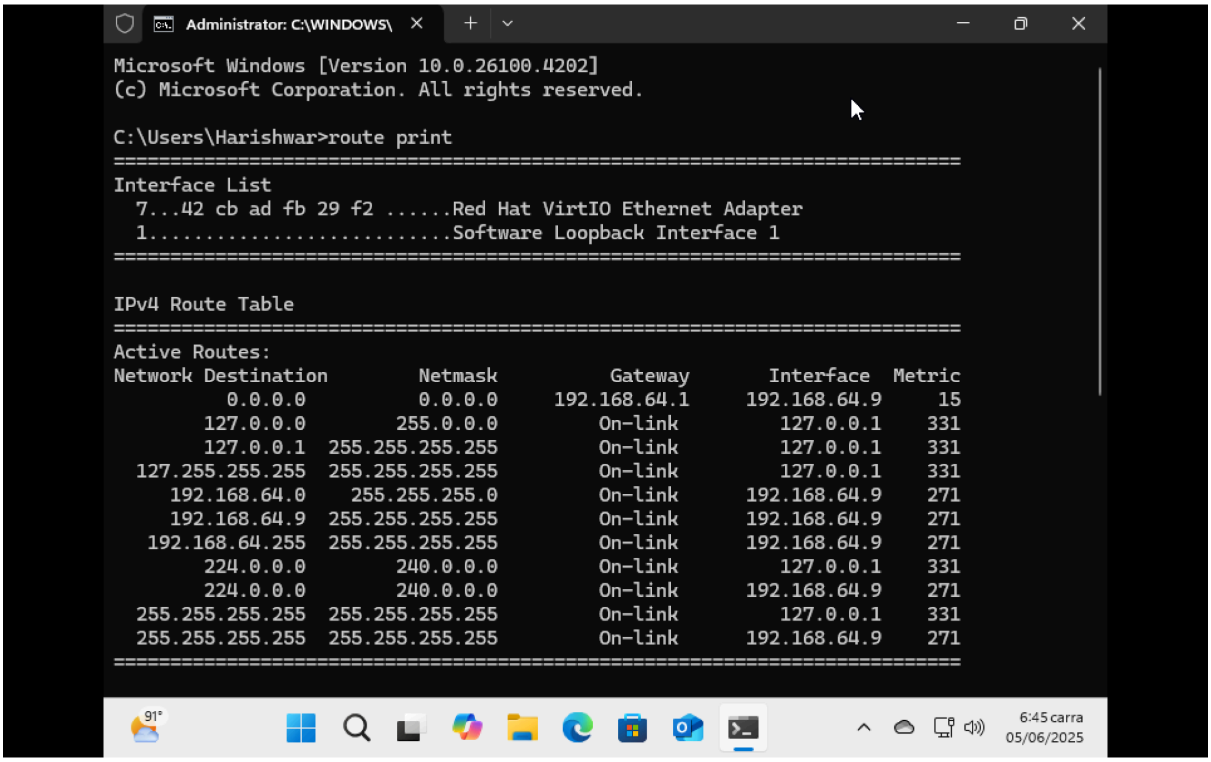


```
┌──(root㉿kali)-[/]
└─# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.29.1    0.0.0.0         UG        0 0          0 eth0
192.168.29.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0

┌──(root㉿kali)-[/]
└─# ip route show
default via 192.168.29.1 dev eth0 proto dhcp src 192.168.29.125 metric 100
192.168.29.0/24 dev eth0 proto kernel scope link src 192.168.29.125 metric 100

┌──(root㉿kali)-[/]
└─#
```

Fig: Routing Table Linux



```
Microsoft Windows [Version 10.0.26100.4202]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Harishwar>route print
===========================================================================
Interface List
  7...42 cb ad fb 29 f2 ......Red Hat VirtIO Ethernet Adapter
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.64.1     192.168.64.9     15
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     192.168.64.0    255.255.255.0         On-link      192.168.64.9    271
     192.168.64.9  255.255.255.255         On-link      192.168.64.9    271
   192.168.64.255  255.255.255.255         On-link      192.168.64.9    271
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.64.9    271
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.64.9    271
===========================================================================
```

Fig: Routing Table Windows

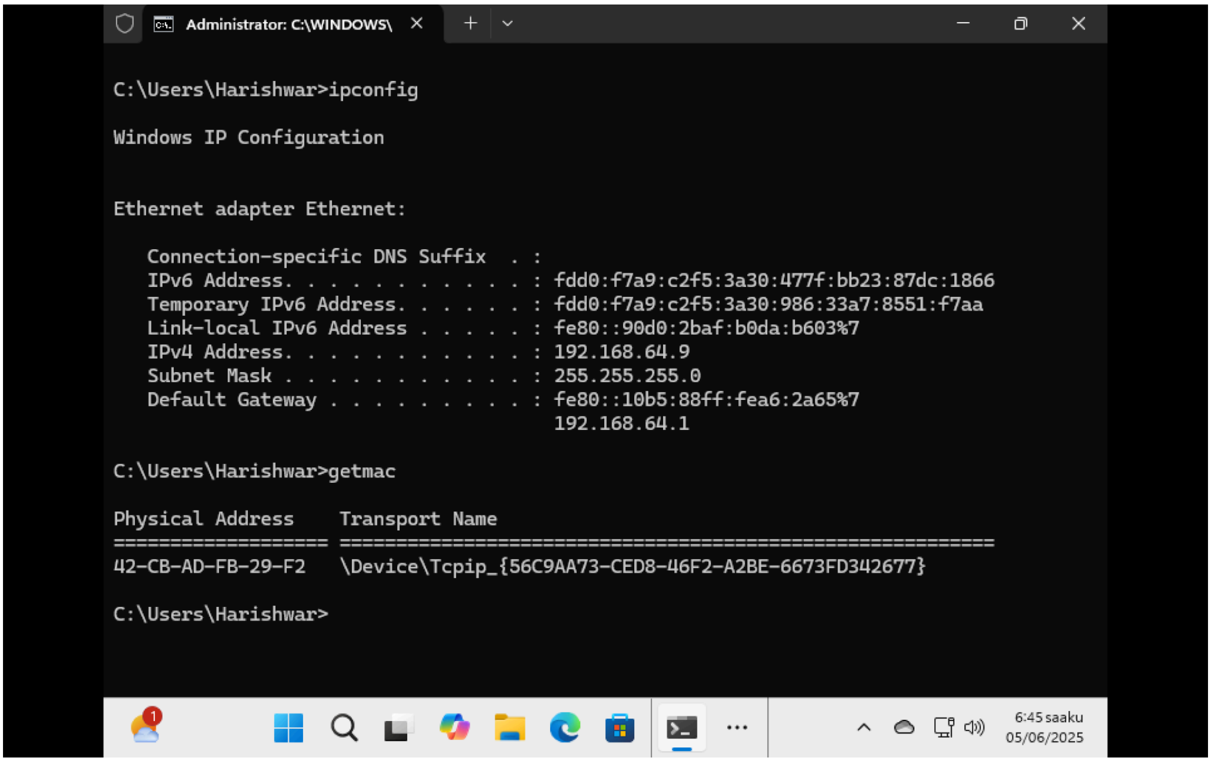
Purpose:

- Identify and verify routing paths.
- Detect routing issues or misconfigurations.

4. MAC Address

The **MAC (Media Access Control) address** is a hardware address assigned to a network interface card (NIC). It is unique to each device and operates at Layer 2 of the OSI model.

- **Format**: 6-byte (48-bit) address (e.g., 00:1A:2B:3C:4D:5E)
- **Use**: Device identification within a local network segment



```
C:\Users\Harishwar>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : fdd0:f7a9:c2f5:3a30:477f:bb23:87dc:1866
   Temporary IPv6 Address. . . . . . : fdd0:f7a9:c2f5:3a30:986:33a7:8551:f7aa
   Link-local IPv6 Address . . . . . : fe80::90d0:2baf:b0da:b603%7
   IPv4 Address. . . . . . . . . . . : 192.168.64.9
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::10b5:88ff:fea6:2a65%7
                                       192.168.64.1

C:\Users\Harishwar>getmac

Physical Address    Transport Name
=================== ==========================================================
42-CB-AD-FB-29-F2   \Device\Tcpip_{56C9AA73-CED8-46F2-A2BE-6673FD342677}

C:\Users\Harishwar>
```

Command to View MAC Address:

- Windows: `ipconfig /all`
- Linux/macOS: `ifconfig` or `ip a`

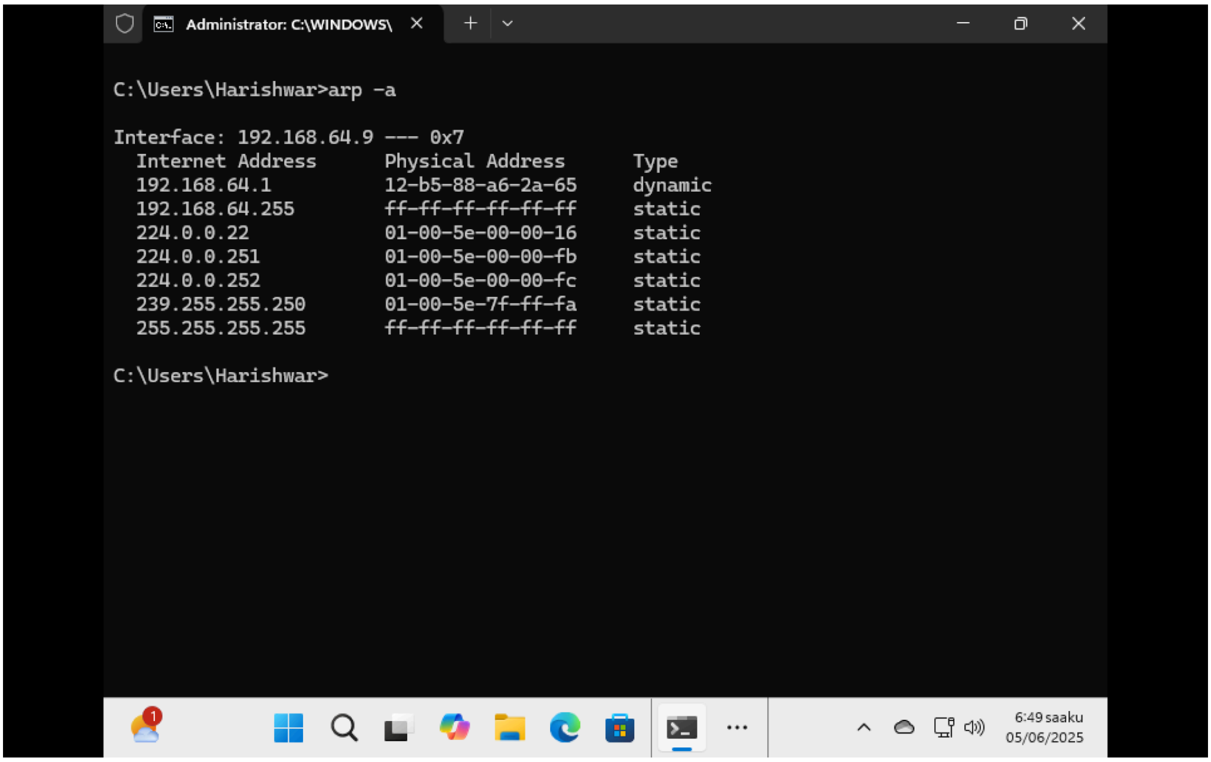
Purpose in Security:

- Track device access
- MAC filtering for network access control

5. ARP (Address Resolution Protocol)

ARP is used to map an IP address to a MAC address on a local area network.

- Works at Layer 2 (Data Link) and Layer 3 (Network)
- Broadcasts a request for a MAC address corresponding to a known IP



```
C:\Users\Harishwar>arp -a

Interface: 192.168.64.9 --- 0x7
  Internet Address      Physical Address      Type
  192.168.64.1          12-b5-88-a6-2a-65     dynamic
  192.168.64.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Harishwar>
```

Fig: ARP TABLE

Command to View ARP Table:

- Windows: `arp -a`
- Linux/macOS: `ip neighbour`

Security Concern:

- ARP Spoofing: An attacker sends fake ARP messages to associate their MAC address with the IP of another host

Mitigation:

- Use Dynamic ARP Inspection (DAI)
- Implement static ARP entries where applicable

6. DNS (Domain Name System)

DNS translates domain names (like www.google.com) into IP addresses.

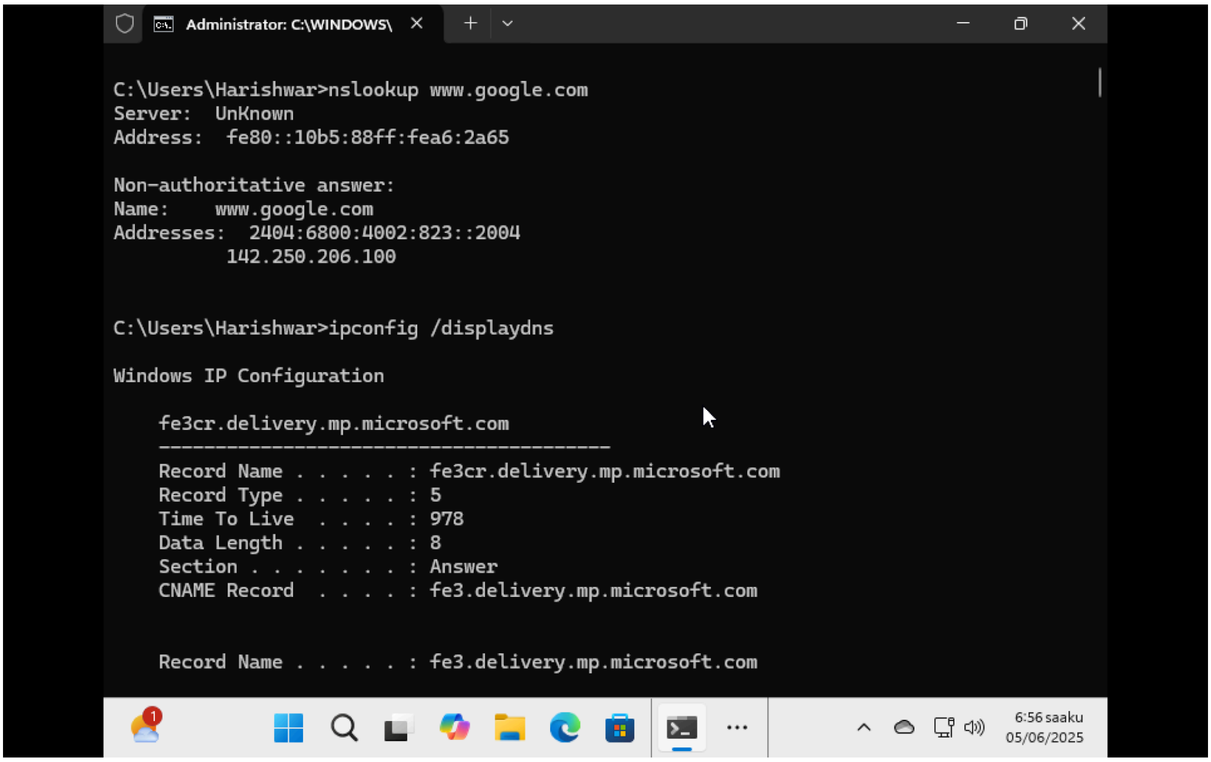
- Operates at Layer 7 (Application Layer)
- Essential for user-friendly web navigation

Process:

1. User types a domain name
2. Client sends DNS request to DNS server
3. Server returns IP address

Commands for DNS Testing:

- `nslookup` (Windows, Linux, macOS)
- `dig` (Linux/macOS)



```
C:\Users\Harishwar>nslookup www.google.com
Server:  UnKnown
Address:  fe80::10b5:88ff:fea6:2a65

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4002:823::2004
          142.250.206.100


C:\Users\Harishwar>ipconfig /displaydns

Windows IP Configuration

    fe3cr.delivery.mp.microsoft.com
    ----------------------------------------
    Record Name . . . . . : fe3cr.delivery.mp.microsoft.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 978
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : fe3.delivery.mp.microsoft.com


    Record Name . . . . . : fe3.delivery.mp.microsoft.com
```

Fig: DNS Query

Common Issues:

- DNS server unreachable
- Incorrect DNS configuration
- DNS cache poisoning

Troubleshooting:

- Flush DNS cache: `ipconfig /flushdns`
- Check server status with `nslookup <domain>`

7. Ping Command

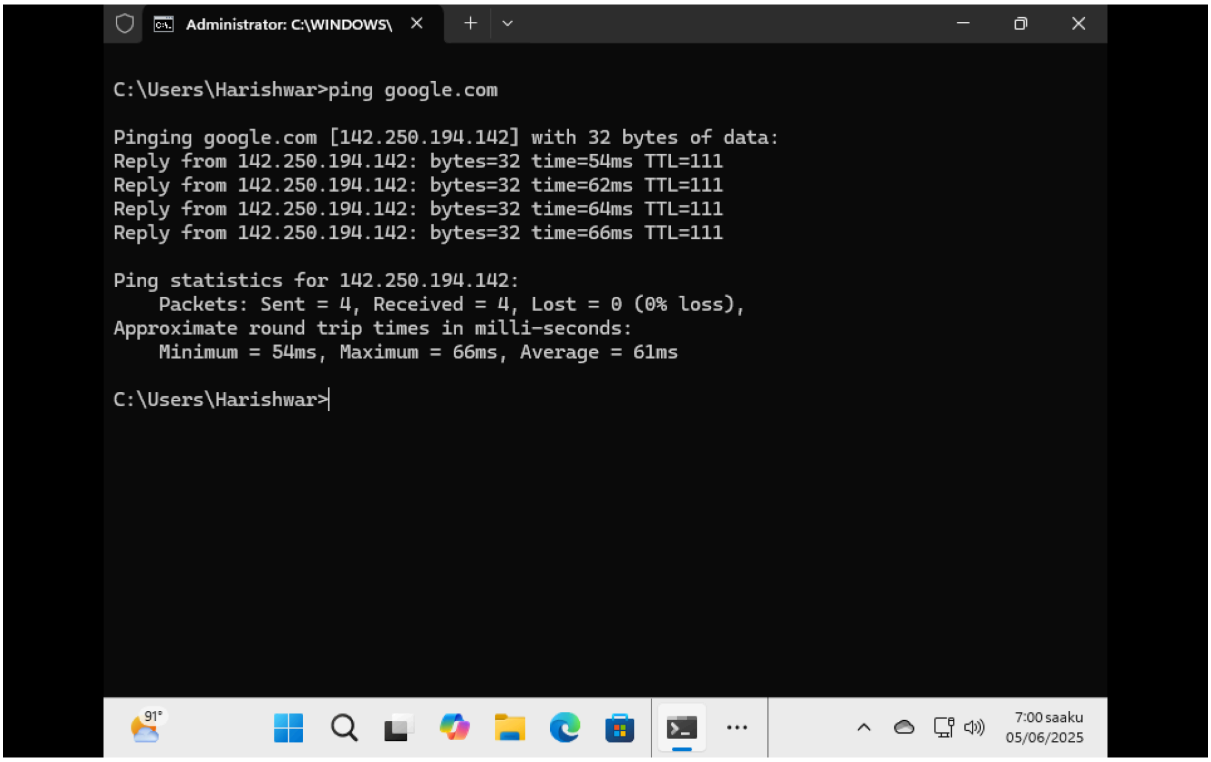
The `ping` command tests network connectivity by sending ICMP echo request packets and waiting for echo replies.

Use Cases:

- Test if a host is reachable.
- Measure latency and packet loss.

Command:

- `ping [IP address or domain name]`



```
C:\Users\Harishwar>ping google.com

Pinging google.com [142.250.194.142] with 32 bytes of data:
Reply from 142.250.194.142: bytes=32 time=54ms TTL=111
Reply from 142.250.194.142: bytes=32 time=62ms TTL=111
Reply from 142.250.194.142: bytes=32 time=64ms TTL=111
Reply from 142.250.194.142: bytes=32 time=66ms TTL=111

Ping statistics for 142.250.194.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 66ms, Average = 61ms

C:\Users\Harishwar>
```

Fig: Checking connectivity(Ping)

Output:

- Reply from [IP]: bytes=32 time=10ms TTL=128
- Errors: "Request timed out" or "Destination host unreachable"

8. Traceroute Command

The `traceroute` (or `tracert` in Windows) command maps the path packets take to a destination, showing all intermediate hops.

Purpose:

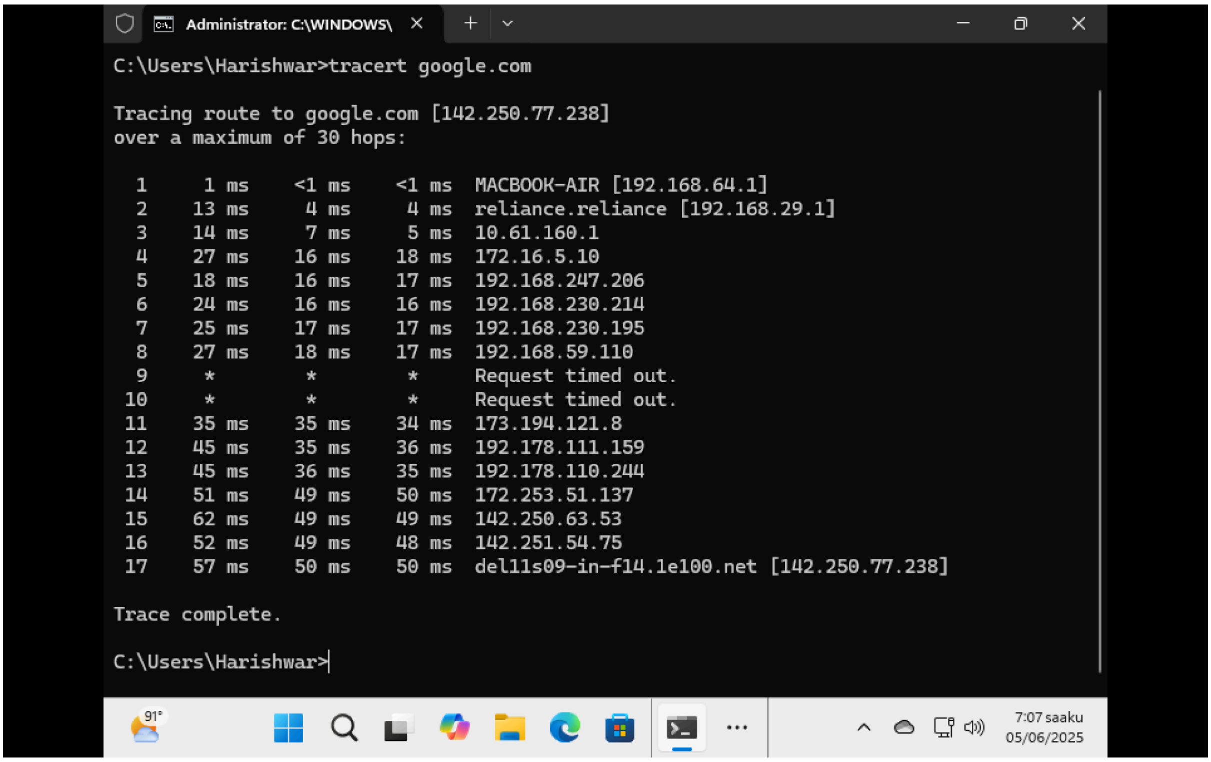
- Diagnose where the packet is being delayed or dropped.
- Identify routing issues or firewall filtering.

Command:

- Windows: `tracert [destination]`
- Linux/macOS: `traceroute [destination]`

Steps to Perform:

1. Open terminal or command prompt.
2. Type the traceroute command with a target domain/IP.
3. Analyze hop count, IPs, and response time at each step.



```
C:\Users\Harishwar>tracert google.com

Tracing route to google.com [142.250.77.238]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  MACBOOK-AIR [192.168.64.1]
  2    13 ms     4 ms     4 ms  reliance.reliance [192.168.29.1]
  3    14 ms     7 ms     5 ms  10.61.160.1
  4    27 ms    16 ms    18 ms  172.16.5.10
  5    18 ms    16 ms    17 ms  192.168.247.206
  6    24 ms    16 ms    16 ms  192.168.230.214
  7    25 ms    17 ms    17 ms  192.168.230.195
  8    27 ms    18 ms    17 ms  192.168.59.110
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11    35 ms    35 ms    34 ms  173.194.121.8
 12    45 ms    35 ms    36 ms  192.178.111.159
 13    45 ms    36 ms    35 ms  192.178.110.244
 14    51 ms    49 ms    50 ms  172.253.51.137
 15    62 ms    49 ms    49 ms  142.250.63.53
 16    52 ms    49 ms    48 ms  142.251.54.75
 17    57 ms    50 ms    50 ms  del11s09-in-f14.1e100.net [142.250.77.238]

Trace complete.

C:\Users\Harishwar>
```

Fig: Tracert (windows)

Output Includes:

- Hop count
- IP address or hostname of each router
- Response times from each hop

[Reference Section -https://www.netacad.com/courses/networking-basics?courseLang=en-US]

Note: This document is based on networking fundamentals and is referenced from Cisco Academy.