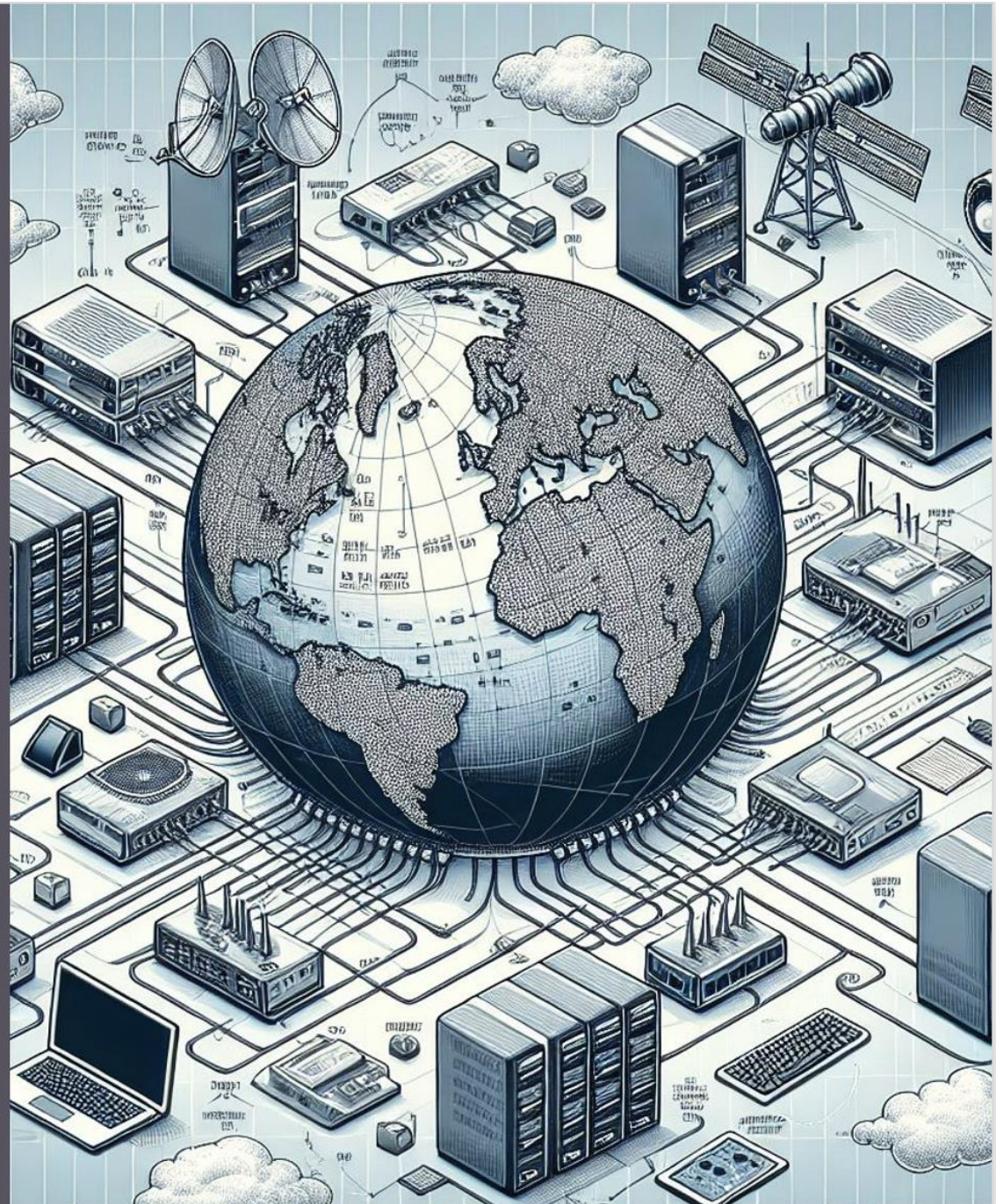
UAB COLLEGE OF ARTS AND SCIENCES
The University of Alabama at Birmingham
Department of Computer Science

CS 334/534 NETWORKING

Dr. Ragib Hasan

Lecture 2.1:
Network Topology and Traffic Management



Lecture goals

- Introduce topologies
- Optimizing Network Performance
- IP Address
- DNS Servers
- Networking Tools

- Book reference: Chapter 1, section 1.5 to 1.14

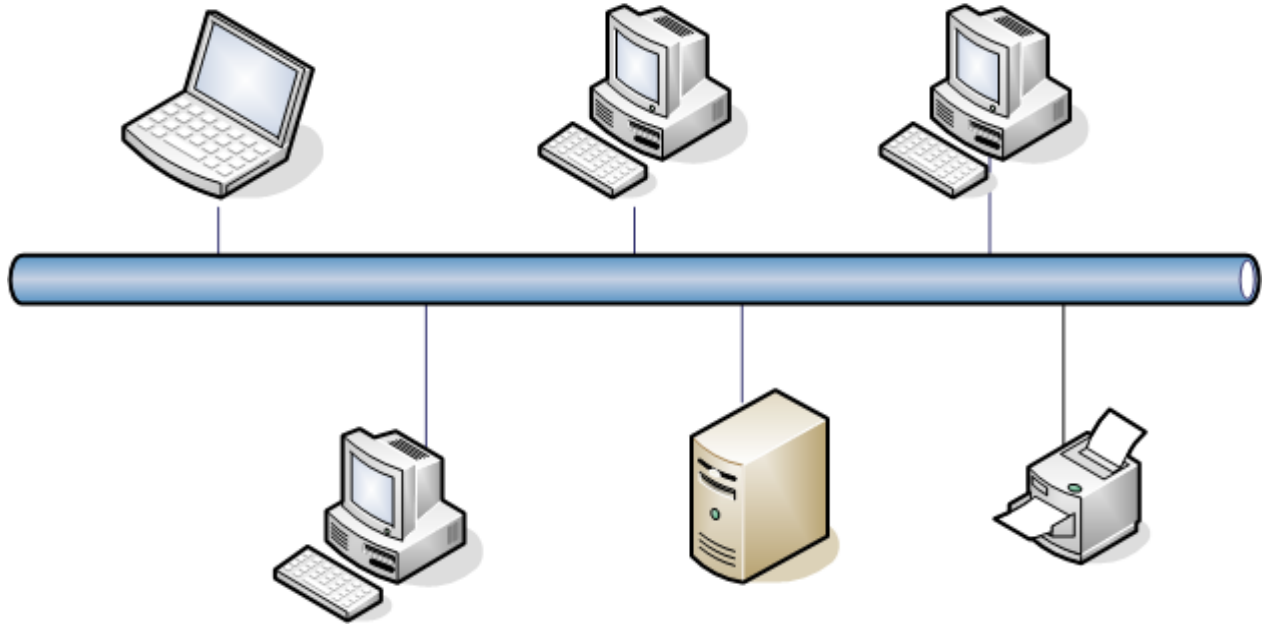
What is Network Topology?

- Topology in networking refers to the **arrangement or layout** of elements (such as devices, nodes, and connections) in a network.
- It defines how devices are **interconnected and communicate** with each other, either physically or logically.
- It describes the actual physical layout of the network, including the arrangement of cables, devices, and nodes. Also refers to how **data flows** within the network, regardless of the physical layout.

Bus Topology

All devices are connected to a single central cable (the bus)

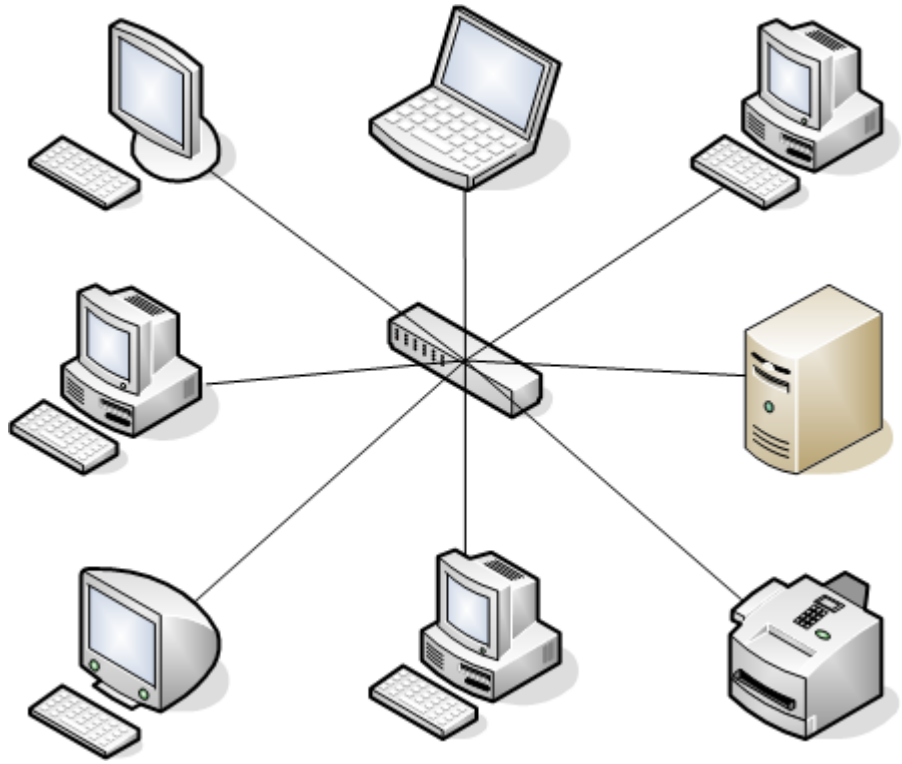
- Advantages
  - Simple
  - Cost-effective
  - Easy to connect or remove devices
- Disadvantages
  - Single point of failure
  - Not good for large networks.
  - Very slow
  - High packet loss



Star Topology

All devices are connected to a central hub or switch

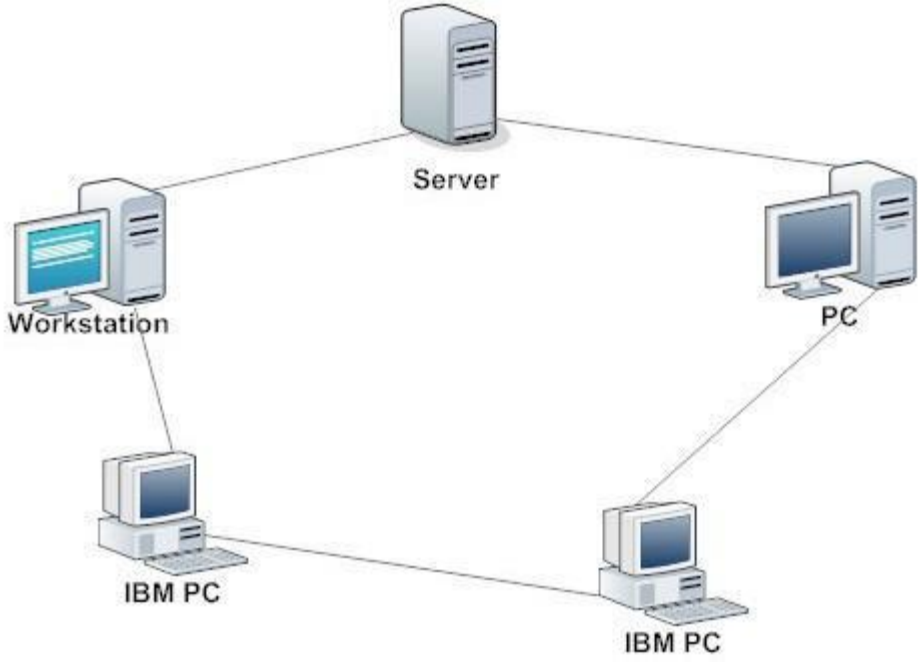
- Advantages
  - Reliable connections
  - Easy troubleshooting
  - Smooth data transfer
- Disadvantages
  - Expensive
  - Hub failure disrupts the entire network.



Ring Topology

Devices are connected in a circular fashion, and data travels in one or both directions around the ring.

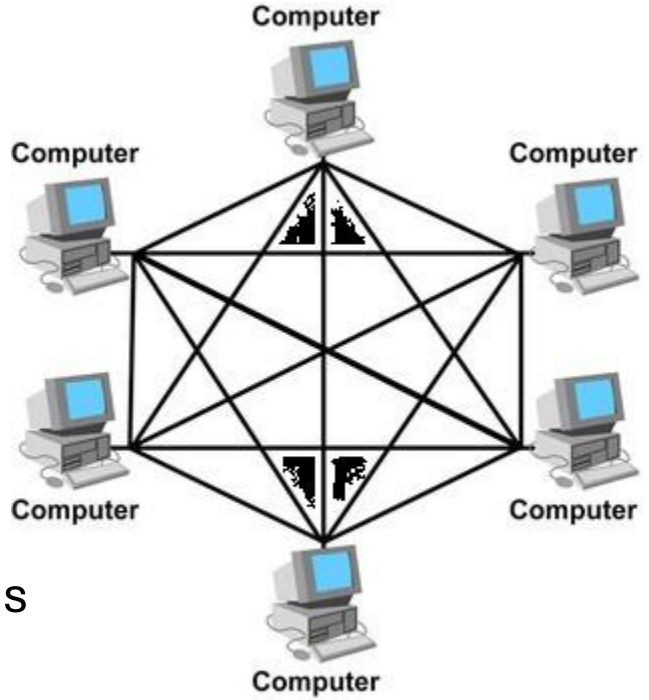
- Advantages
  - Efficient data transfer
  - Low Cost
  - Easier to identify bottlenecks
- Disadvantages
  - A single failure can disrupt the entire network.
  - Adding new devices in the network is complex



Mesh Topology

Each device is connected to every other device, providing multiple paths for data

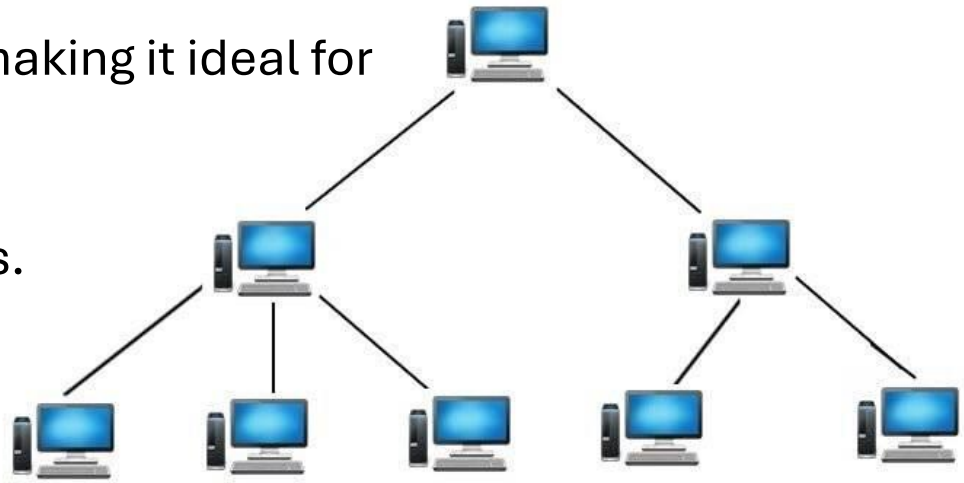
- Advantages
  - Extremely reliable and fault-tolerant
  - Suitable where downtime is not acceptable.
  - High performance
- Disadvantages
  - Complex to design, configure, and maintain.
  - Expensive due to the high number of connections and cables required.
  - Requires substantial resources for setup and scalability.



Tree Topology

Devices are connected in a hierarchical manner.

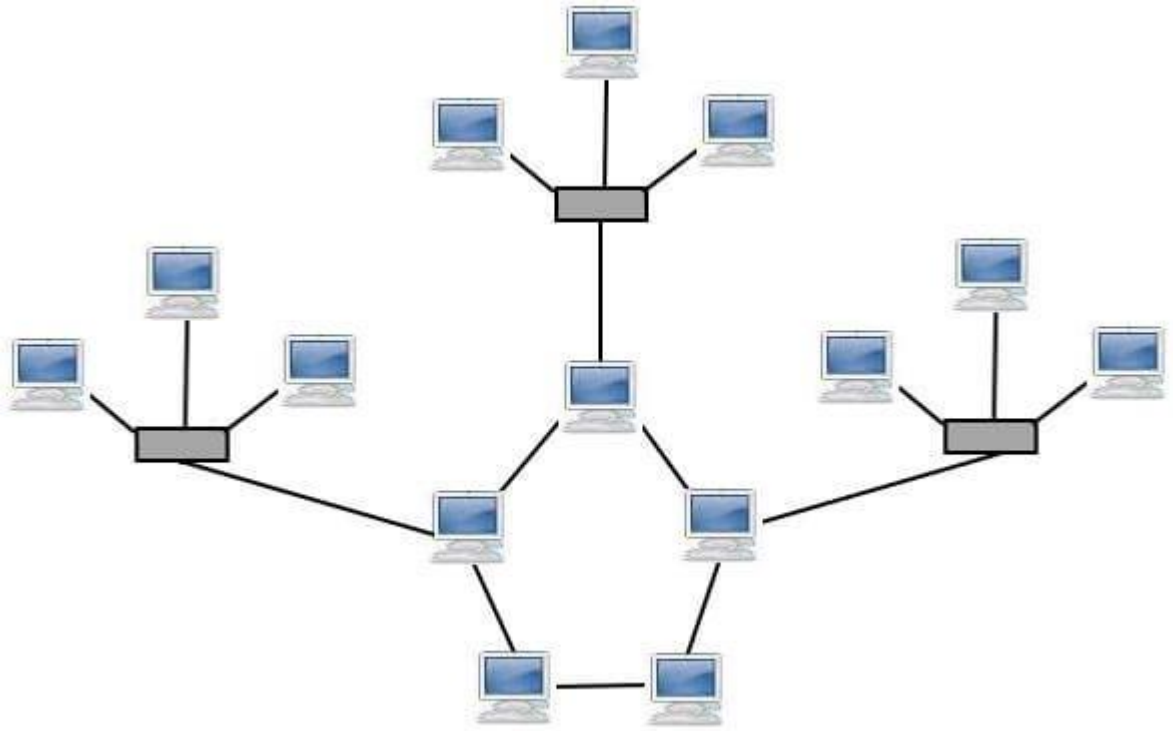
- Advantages
  - Scalable and supports hierarchical structuring, making it ideal for large networks.
  - Easier to troubleshoot due to clear organization.
  - Supports future expansion by adding new devices.
- Disadvantages
  - The root node is a single point of failure, impacting the entire network if it fails.
  - Maintenance and configuration become challenging
  - Requires more cabling and hardware.



Hybrid Topology

Combines two or more basic topologies.

- Advantages
  - Flexible as it combines the strengths of multiple topologies.
  - Scalable.
  - Fault tolerance can be enhanced
- Disadvantages
  - Highly complex to design and manage.
  - Expensive
  - Requires expertise for maintenance and troubleshooting.



Traffic Engineering

- Traffic engineering involves intentionally **selecting specific routes** or **prioritizing traffic** classes to optimize network performance.
- At LAN layers, packet paths are determined solely by their destinations focuses on selecting between alternative paths.

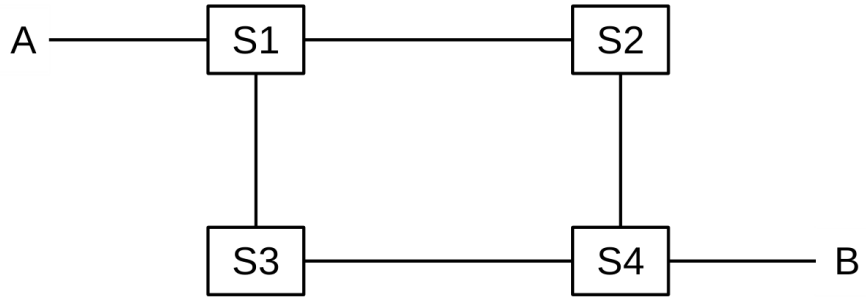
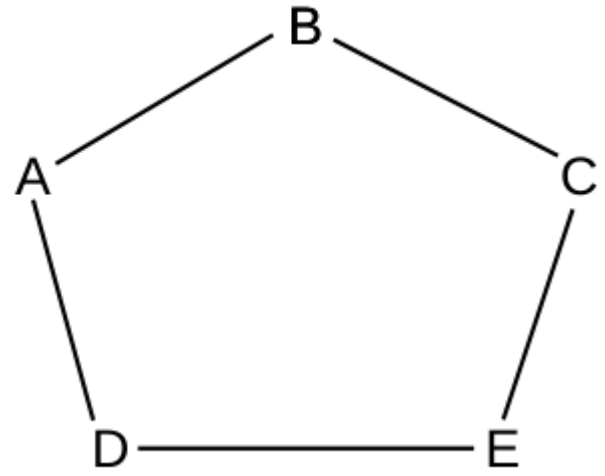


Fig. 4:: A network with more than one path from A to B

Routing Loops

- Routing loops occur when packets **circulate endlessly within a network**, typically due to misconfigured routing tables or incorrect forwarding decisions
- Example: D might feel that the best path to B is D–E–C–B (perhaps because it believes the A–D link is to be avoided). If E similarly decides the best path to B is E–D–A–B, and if D and E both choose their next_hop for B based on these best paths, then a linear routing loop is formed.

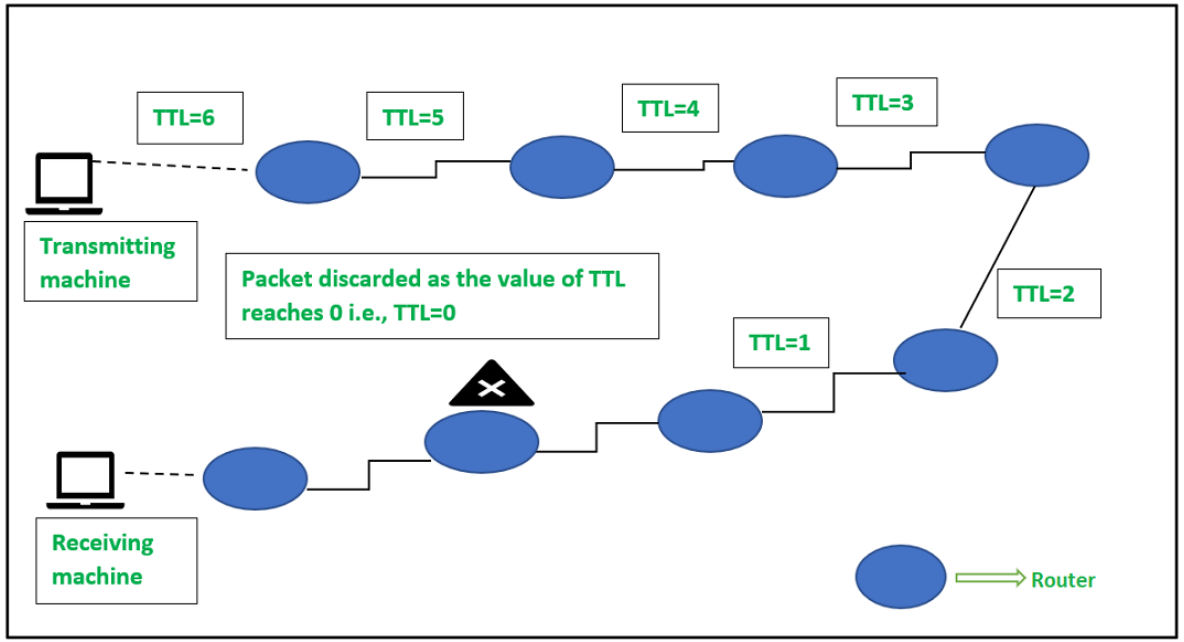


Routing Loops (Cont.)

- These loops can severely impact network **performance**, **consuming bandwidth** and preventing packets from reaching their destination.
- How Ethernet Avoids Routing Loops:
  - Nonlinear Routing Loops: Ethernet prevents these by **disallowing loops in** the network topology
  - Linear Routing Loops: Ethernet addresses these by ensuring switches **do not forward packets back** through the interface from which they arrived.

Routing Loops (Cont.)

- **How IP Handles Routing Loops:**
- The Time to Live (TTL) field in the IP header is initialized by the sender (commonly set to 64).
- Each router along the path decrements the TTL by 1.
- When the TTL reaches 0, the packet is discarded, effectively breaking any potential routing loop by limiting the number of hops a packet can take.



Congestion

Load on the network is higher than capacity.

- Capacity is not uniform across networks
  - Modem vs. Cellular vs. Cable vs. Fiber optics
- There are multiple flows competing for bandwidth
  - Residential cable modem vs. corporate data center
- Load is not uniform over time
  - 10 PM, Sunday night ⇒ BitTorrent latest Game of Thrones

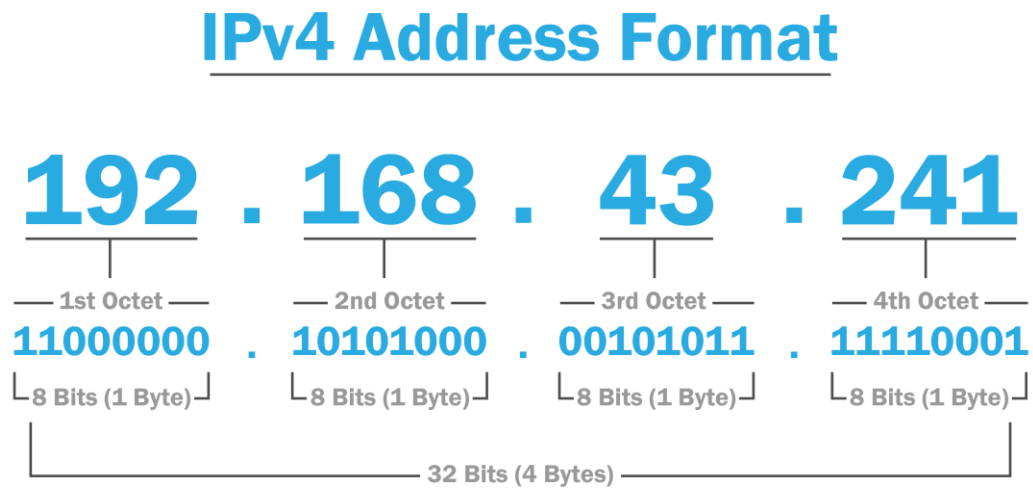
IP Address

An Internet Protocol (IP) address is the **unique identifying number** assigned to every device connected to the internet.

- Initially, IP was designed to **interconnect LANs** (internetworking) as faced **scalability issues**.
- IP enables **packet delivery** from any host to any other host globally, ensuring all **nodes can connect to one another.**

IPv4

- An IPv4 address consists of 32 bit (binary digit), grouped into four section of known as **octets or bytes.**
- **Each octet** has 8 bits and this bits can be represented only in 0 or 1 form, and when they grouped together, they form a binary number.
- Since each octet has 8 bits, it can represent 256 numbers ranging from o to 255. These four octets are represented as decimal numbers, separated by periods known as **dotted decimal notation**.

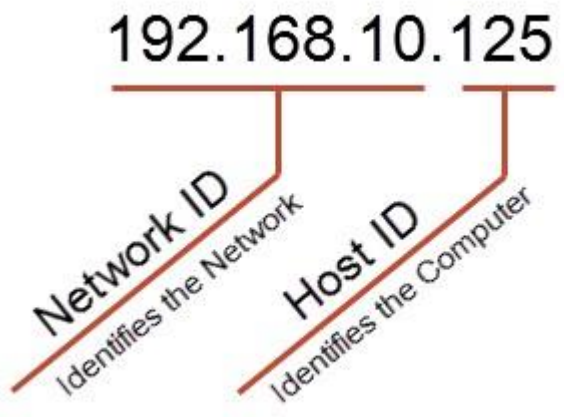


IPv4 Parts

IPv4 addresses consist of two parts:

•**Network Part**: The network part or prefix of an IP address is the portion that identifies a **specific network within** the IP addressing hierarchy. This part is used by routers to determine the appropriate route to the destination network.

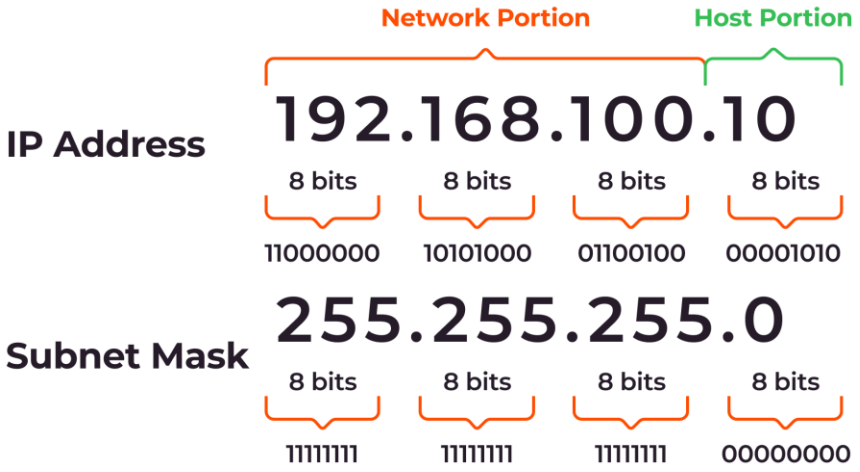
•**Host Part**: The host part is the portion of the IP address that identifies a **specific device (host)** within a given network. The host part is used by devices on the same network to communicate with each other. Routers do not use this part to route packets between networks.



Subnet Mask

- The **subnet mask** is a 32-bit number used to specify **which portion of the IP address** refers to the network part and which part refers to the host. It works by performing a bitwise AND operation between the IP address and the subnet mask.

- For 192.168.100.10/24, the subnet mask would be **255.255.255.0**. This means that the **first 24 bits are used for the network part**, and the remaining **8 bits are used for the host part.**



IPv4 Class

IPv4 Address Classes and Ranges						
Address Class	**Type**	**Range**	**Default Subnet Mask**	**Number of Networks**	**No of Hosts Per Network**	**Use**
A	Public	1.0.0.0 to 127.0.0.0	255.0.0.0	126	16,777,214	Governments and Large Number of Hosts
	Private	10.0.0.0 to 10.255.255.255				
B	Public	128.0.0.0 to 191.255.255.255	255.255.0.0	16,382	65,534	Medium Companies
	Private	172.16.0.0 to 172.31.255.255				
C	Public	192.0.0.0 to 223.255.255.255	255.255.255.0	2,097,150	254	Small Companies and LANs
	Private	192.168.0.0 to 192.168.255.255				
D	N/A	224.0.0.0 to 239.255.255.255	Not Applicable	N/A	N/A	Reserved for Multicasting
E	N/A	240.0.0.0 to 254.255.255.255	Not Applicable	N/A	N/A	Expermential
Special	Special	127.0.0.1 to 127.255.255.255	N/A	N/A	N/A	Loopback Testing

Note:
- Addesses 127.0.0.1 to 127.255.255.255 cannot be used and are reserved for loopback testing

- APIPA address range is 169.254.0.1 to 169.254.255.254 and has 65, 534 usable IP addresses, with the subnet mask of 255.255.0.0.

Thoughts?

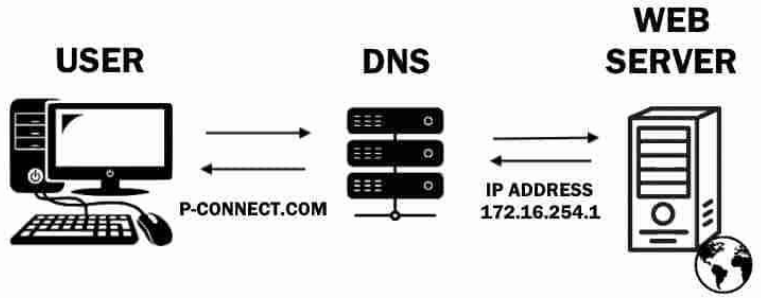
How many devices can be assigned with IPv4?

IPv4 addresses are 32-bit numbers, which means there 2^{32} (4.3 billion) possible addresses.

Is it enough in current world??

Domain Name System

- A system that translates domain names into IP addresses
- This allows users to access websites by typing in a domain name, like "www.example.com", instead of having to remember and enter a long IP address.
- Hostname-to-IP-address translation
- Host aliasing
  - Canonical, alias names
- Mail server aliasing
- Load distribution
  - Replicated Web servers: Many IP addresses correspond to one name



DNS (Cont.)

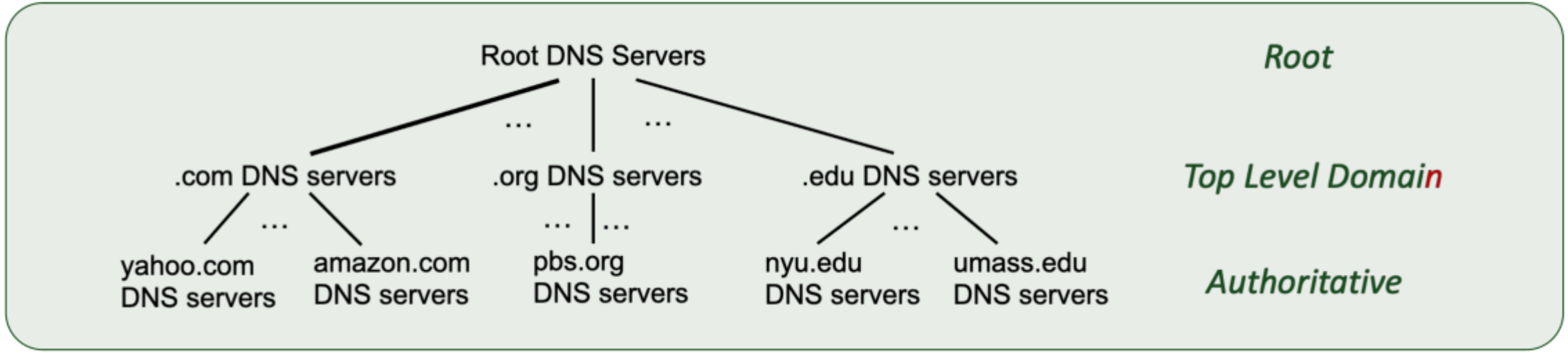
Q: Why not centralize DNS?

- Single point of failure
- Traffic volume
- Distant centralized database
- Maintenance

A: Doesn‘t Scale!

- Comcast DNS servers alone: 600B DNS queries/day
- Akamai DNS servers alone: 2.2T DNS queries/day

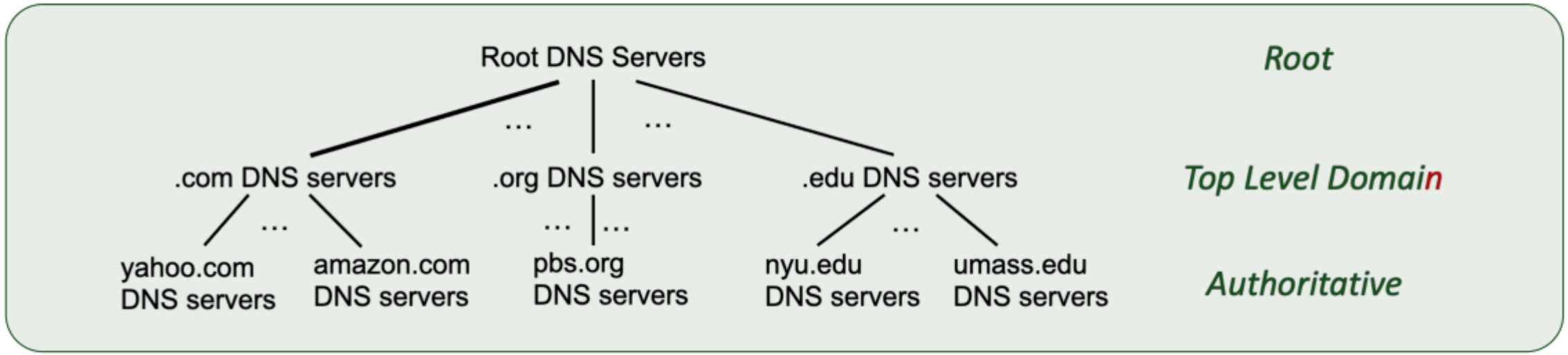
DNS (Cont.)



Top-Level Domain (TLD) Servers: responsible for .com, .org, .net, .edu, .aero, .jobs, .museums, .cn, .uk, .fr, .ca, .jp, .gov, etc.

Authoritative DNS servers: organization's own DNS server(s), providing authoritative hostname to IP mappings for organization's named hosts. can be maintained by organization or service provider

DNS (Cont.)



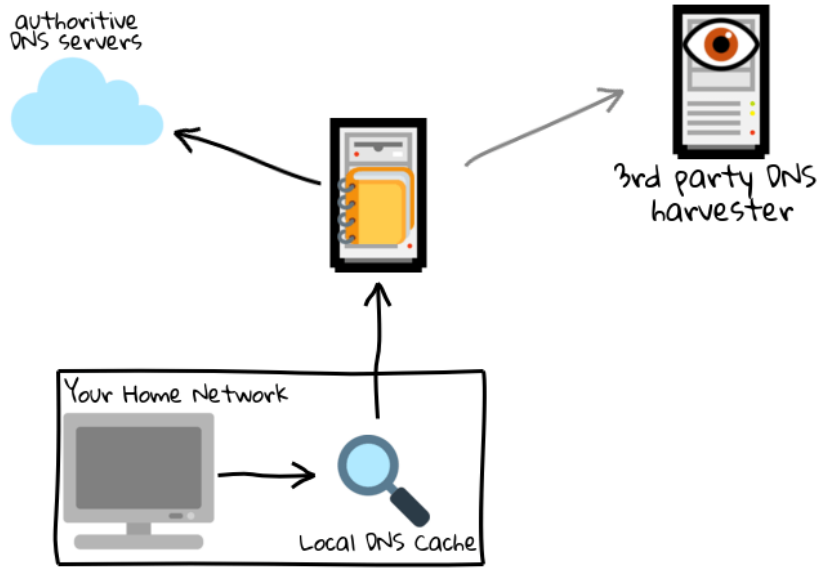
Client Wants IP Address for www.amazon.com:

- Client queries root server to find .com DNS server
- Client queries .com DNS server to get amazon.com DNS server
- Client queries amazon.com DNS server to get IP address for www.amazon.com

DNS (Cont.)

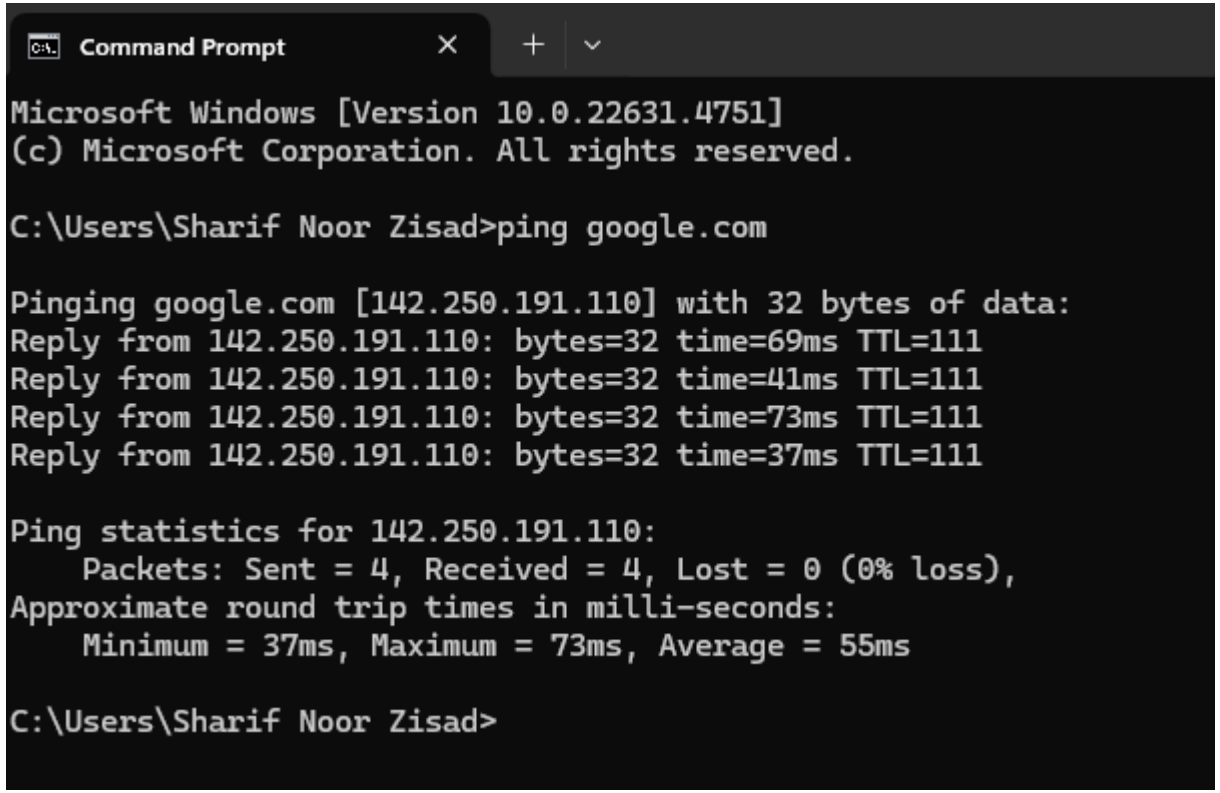
When host makes DNS query, it is sent to its local DNS server:

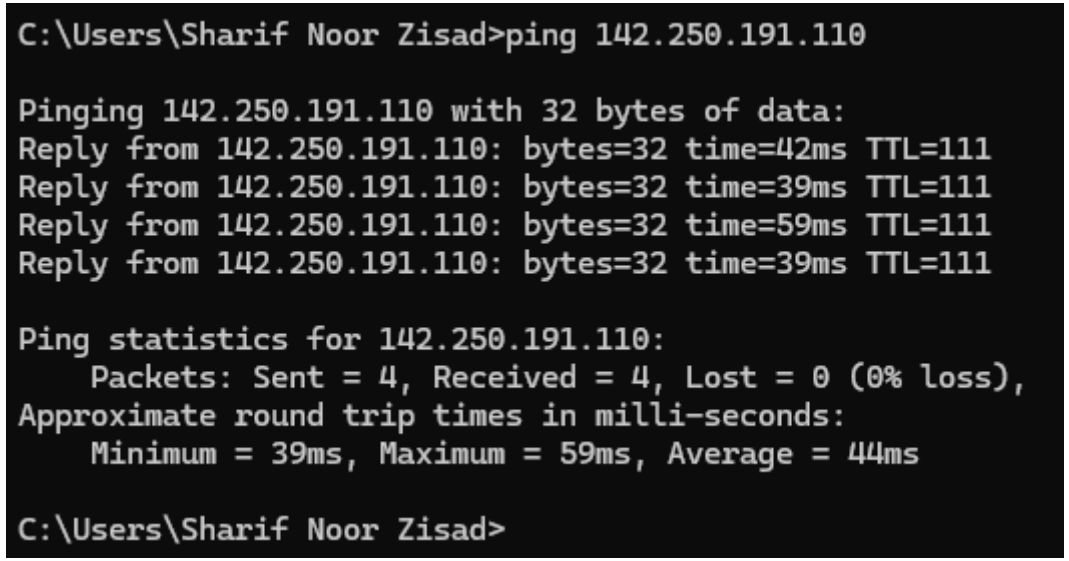
- Local DNS server returns reply, answering:
  - From its local cache of recent name-to-address translation pairs (possibly out of date!)
  - Forwarding request into DNS hierarchy for resolution
- each ISP has local DNS name server; to find yours:
  - MacOS: % scutil --dns
  - Windows: ipconfig /all



Network Utilities: Ping

Ping is useful to determine if another machine is **accessible** or not.





Network Utilities: ifconfig, ipconfig, ip

To find your own IP address you can use **ipconfig** on Windows, **ifconfig** on Linux and Mac.

```
C:\Users\Sharif Noor Zisad>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::19b4:e833:ed3f:1564%12
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VirtualBox Host-Only Network #4:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e96d:ff6f:310c:9230%10
   IPv4 Address. . . . . . . . . . . : 192.168.176.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

Network Utilities: traceroute

This lists the route from you to a remote host.

Command: traceroute or tracert

```
C:\Users\Sharif Noor Zisad>tracert google.com

Tracing route to google.com [142.250.191.110]
over a maximum of 30 hops:

  1    22 ms     6 ms   709 ms  192.168.1.1
  2    36 ms    22 ms     5 ms  syn-016-098-116-060.res.spectrum.com [16.98.116.60]
  3   222 ms    47 ms    31 ms  syn-016-098-116-060.res.spectrum.com [16.98.116.60]
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7    26 ms    35 ms    48 ms  syn-016-098-116-060.res.spectrum.com [16.98.116.60]
  8    20 ms    24 ms    20 ms  169.254.250.250
  9    80 ms    25 ms    23 ms  lag-63.bham01-cbr1.netops.charter.com [71.46.164.86]
 10    33 ms    20 ms    30 ms  lag-800-10.bcr01nsvntnjy.netops.charter.com [66.109.6.86]
 11    79 ms    43 ms    35 ms  lag-402.chcgildt87w-bcr00.netops.charter.com [107.14.19.197]
 12    35 ms    36 ms    58 ms  72.14.212.162
 13    48 ms   228 ms    38 ms  142.251.64.199
 14    41 ms    34 ms    42 ms  142.251.60.3
 15    40 ms    42 ms    37 ms  ord38s28-in-f14.1e100.net [142.250.191.110]

Trace complete.

C:\Users\Sharif Noor Zisad>
```

Network Utilities: route

The commands route, route print (Windows), ip route show (Linux), and netstat -r (all systems) display the host's local IP forwarding table.

For workstations not acting as routers, this includes the route to the default router and, usually, not much else.

The default route is sometimes listed as destination 0.0.0.0 with netmask 0.0.0.0 (equivalent to 0.0.0.0/0).

```
C:\Users\Sharif Noor Zisad>route print
===========================================================================
Interface List
 13...00 ff 81 33 2b f2 ......TAP-Surfshark Windows Adapter V9
 12...0a 00 27 00 00 0c ......VirtualBox Host-Only Ethernet Adapter
 10...0a 00 27 00 00 0a ......VirtualBox Host-Only Ethernet Adapter #4
  3...0a 00 27 00 00 03 ......VirtualBox Host-Only Ethernet Adapter #2
 24.........................OpenVPN Data Channel Offload
 20...f0 77 c3 5d 25 dd ......Microsoft Wi-Fi Direct Virtual Adapter
 15...f2 77 c3 5d 25 dc ......Microsoft Wi-Fi Direct Virtual Adapter #2
  9...f0 77 c3 5d 25 dc ......Intel(R) Wi-Fi 6 AX200 160MHz
 23...f0 77 c3 5d 25 e0 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.177     50
        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
      192.168.1.0    255.255.255.0         On-link     192.168.1.177    306
    192.168.1.177  255.255.255.255         On-link     192.168.1.177    306
    192.168.1.255  255.255.255.255         On-link     192.168.1.177    306
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
     192.168.68.0    255.255.255.0         On-link      192.168.68.1    281
     192.168.68.1  255.255.255.255         On-link      192.168.68.1    281
   192.168.68.255  255.255.255.255         On-link      192.168.68.1    281
    192.168.176.0    255.255.255.0         On-link     192.168.176.2    281
    192.168.176.2  255.255.255.255         On-link     192.168.176.2    281
  192.168.176.255  255.255.255.255         On-link     192.168.176.2    281
        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      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link     192.168.176.2    281
        224.0.0.0        240.0.0.0         On-link      192.168.68.1    281
        224.0.0.0        240.0.0.0         On-link     192.168.1.177    306
  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      192.168.56.1    281
  255.255.255.255  255.255.255.255         On-link     192.168.176.2    281
  255.255.255.255  255.255.255.255         On-link      192.168.68.1    281
  255.255.255.255  255.255.255.255         On-link     192.168.1.177    306
===========================================================================
```

Network Utilities: WireShark

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.