Introduction to Networking

Course Incharge: **Yahya Batla**

Course Instructor: **Instructor_Name**

Topics Covered

Introduction to Networking

Networking Concepts

IP Addressing

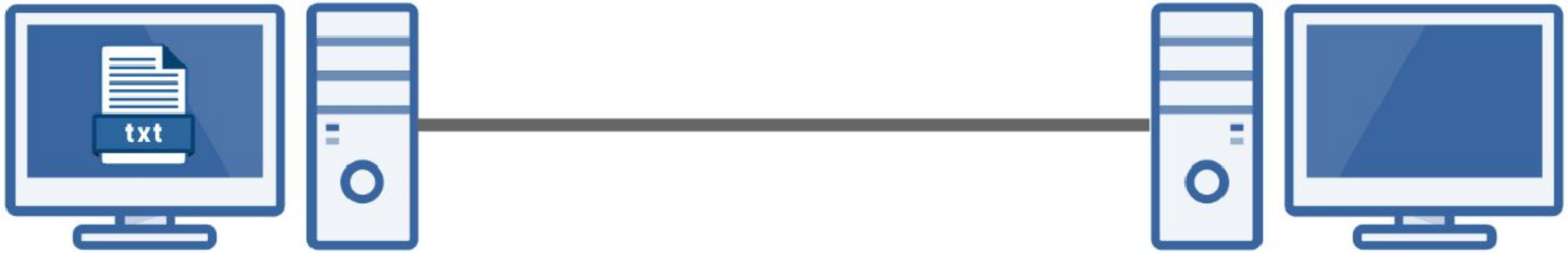
Networking Protocols

Network Security

Firewall, IDS, and IPS

VPN

What is a Network?



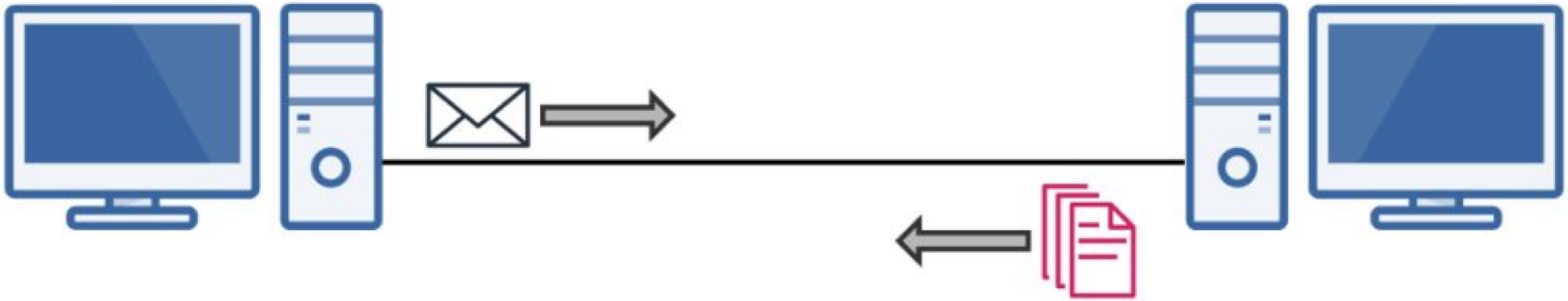
In its simplest form, a network is nothing more than “two connected computers sharing resources with one another.”

It is composed of two main aspects:

1. Physical Connection (wires, cables, wireless media)
2. Logical Connection (data transporting across the physical media)

Basic Networking Rules

1. The computers in a network must use the same procedures for sending and receiving data. We call these **communication protocols.**
2. Data must be delivered uncorrupted. If it is corrupted, it’s useless. (There are Exceptions)
3. Computers in a network must be capable of determining the origin and destination of a piece of information, i.e., its IP and Mac Address.



Basic Networking Rules

Protocols are rules governing how machines exchange data and enable effective communication. Some Everyday Examples

1. When you call somebody, you pick up the phone, ensure there is a dial tone, and if there is, you dial the number.
2. When you drive your car, you obey the rules of the road.

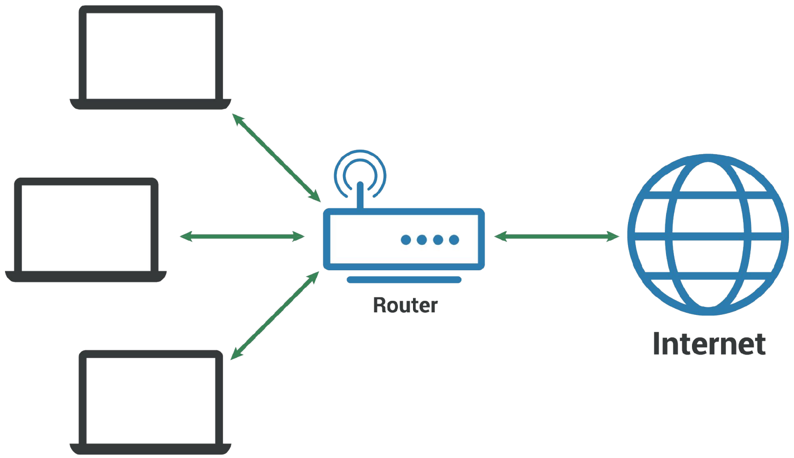
Physical Protocols: describe the medium (wiring), the connections, and the signal (voltage level on a wire).

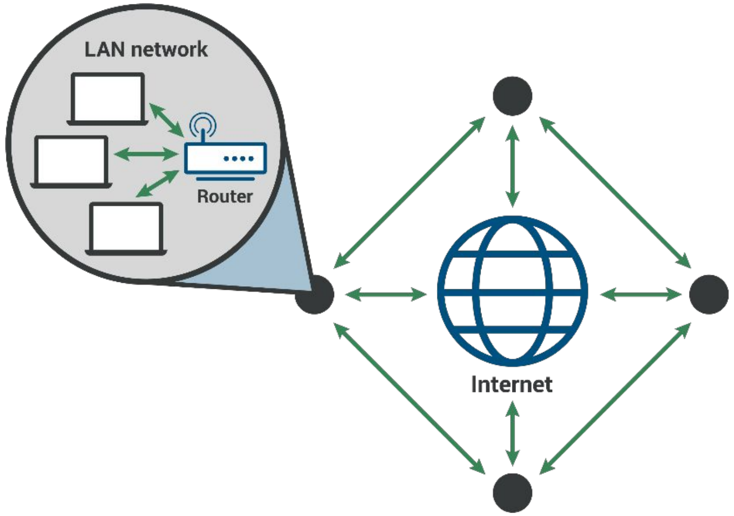
Logical Protocols: software controlling how and when data is sent and received to computers, supporting physical protocols.

Types of Networks

A **Local Area Network (LAN)** is a network that connects computers and devices within a limited geographic area, such as a home, office, or campus, allowing them to share resources like files and printers. Typically, LANs are privately owned and managed

A **Wide Area Network (WAN)** spans a larger geographic area, connecting LANs across cities, countries, or even continents, using technologies like routers and leased lines.

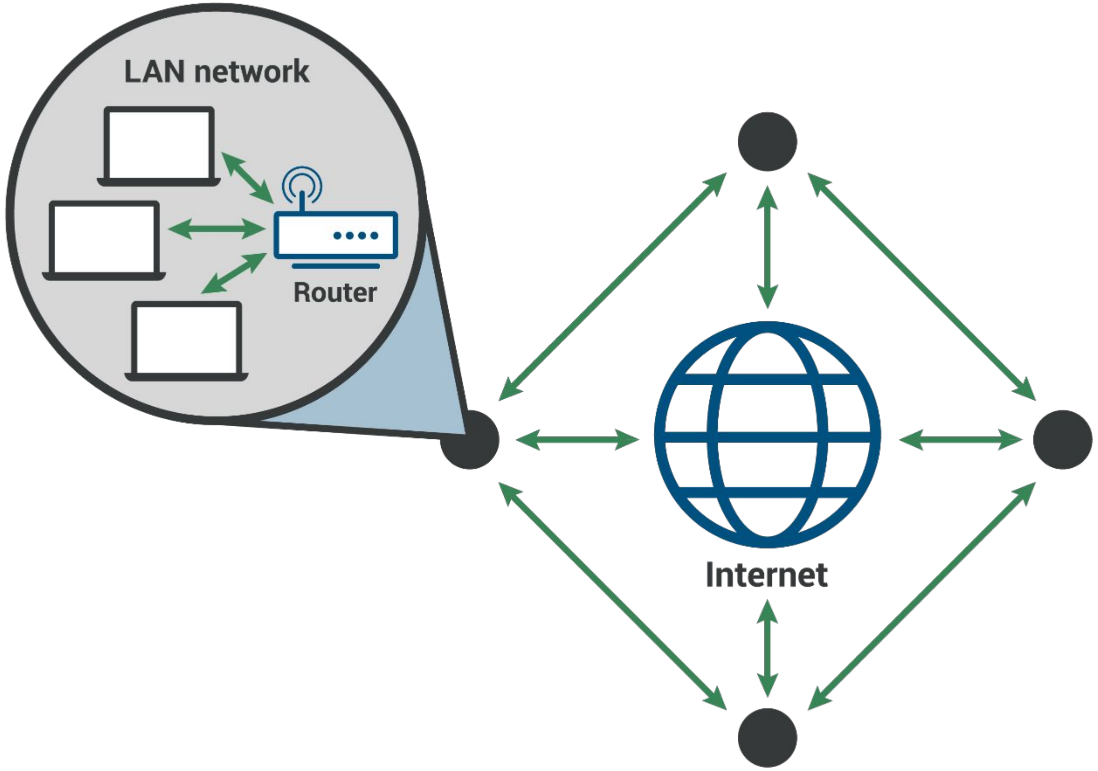




Types of Networks

A **Metropolitan Area Network (MAN)** is a network that covers a larger geographic area than a LAN but is smaller than a WAN, typically serving a city or a large campus. It connects multiple LANs within its range.

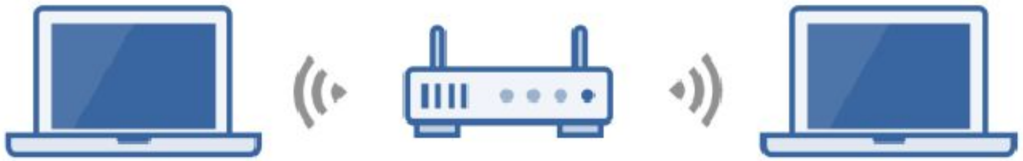
There are other types of networks as well, but the above mentioned are basic ones.



Basic Network Architectures

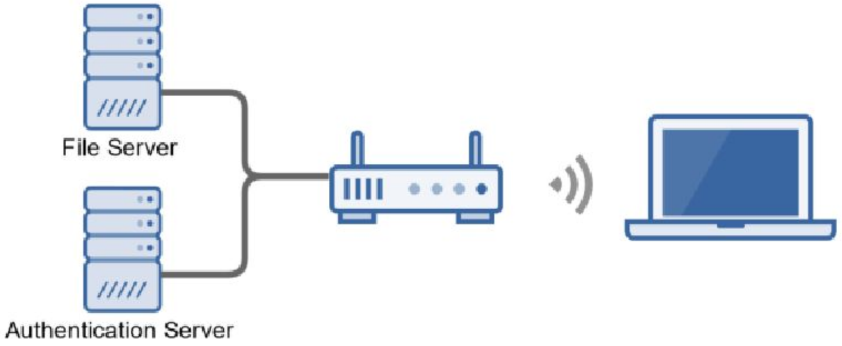
Peer-to-Peer

- All computers on the network are peers
- No dedicated servers
- There’s no centralized control over shared resources
- Any device can share its resources as it pleases
- All computers can act as either a client or a server
- Easy to set-up, and common in homes and small businesses

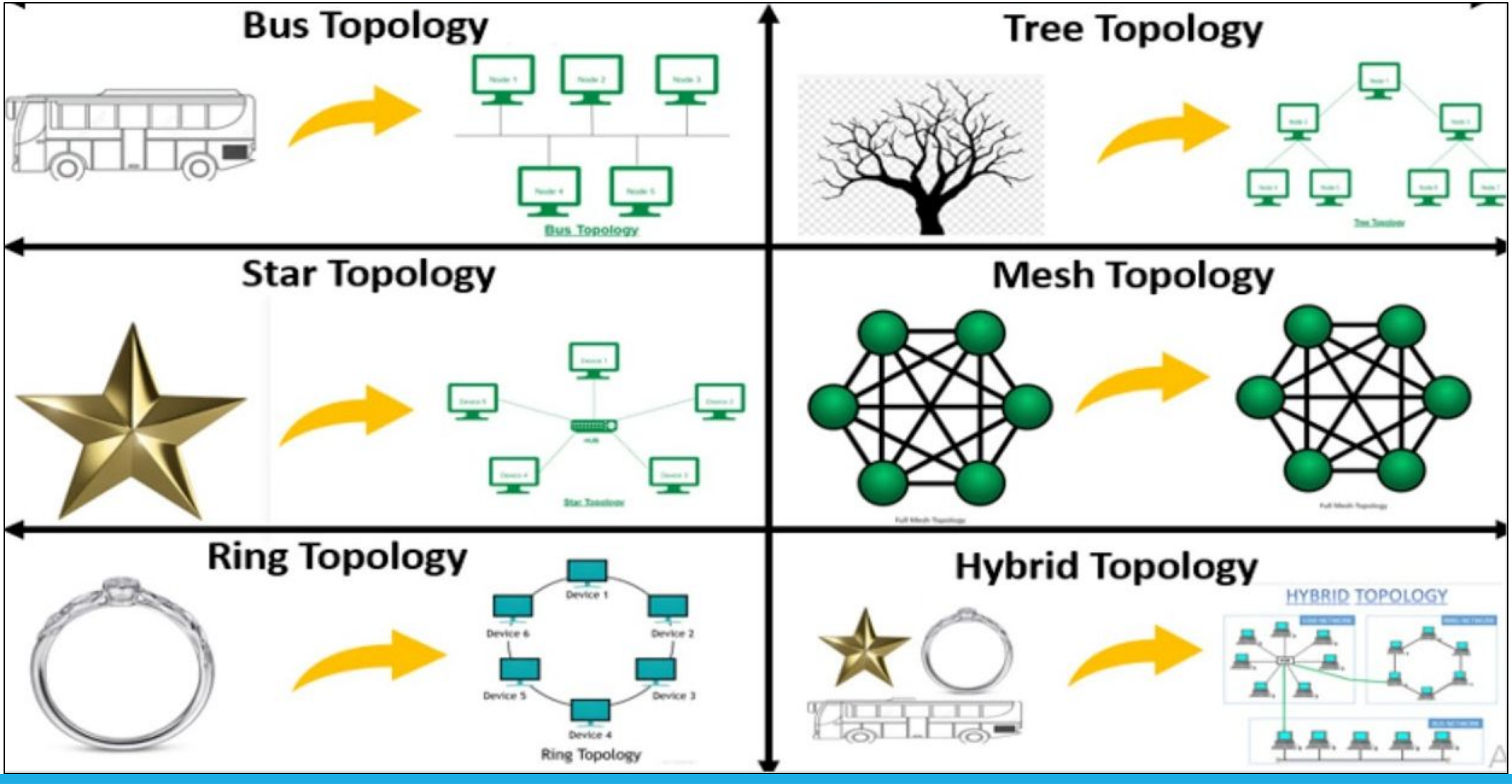


Client-Server

- The network is composed of client and servers
- Servers provide resources
- Clients receive resources
- Servers provide centralized control over network resources (files, printers, etc.)
- Centralizes user accounts, security, and access controls to simplify network administration
- More difficult to setup and requires an IT administrator

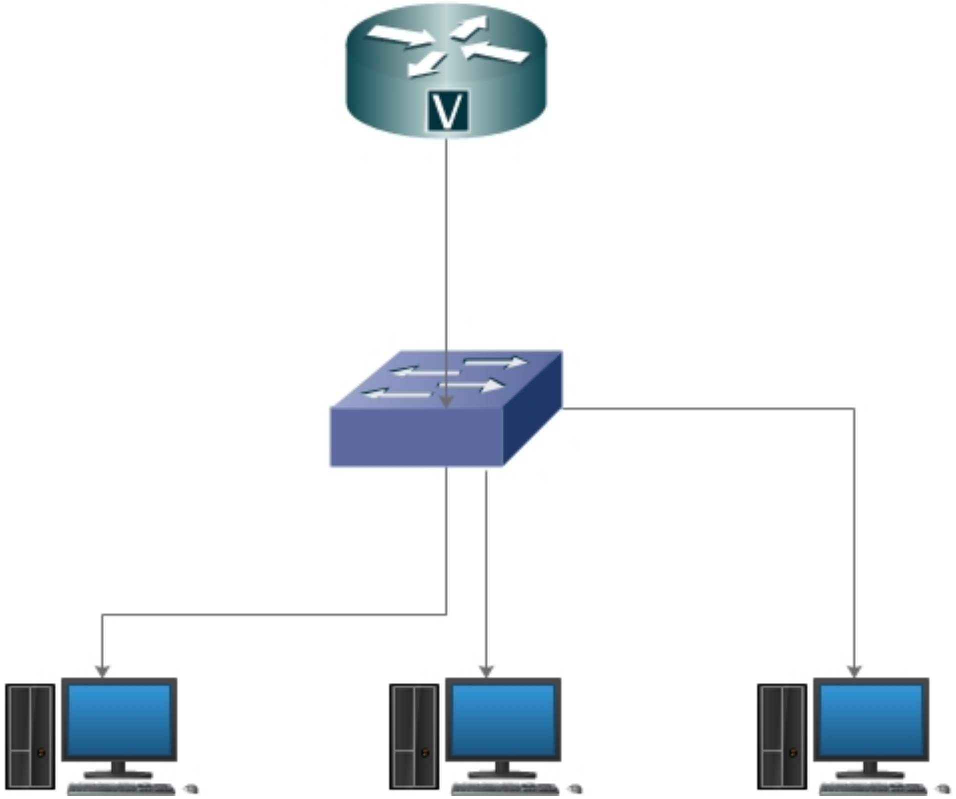


Network Topologies



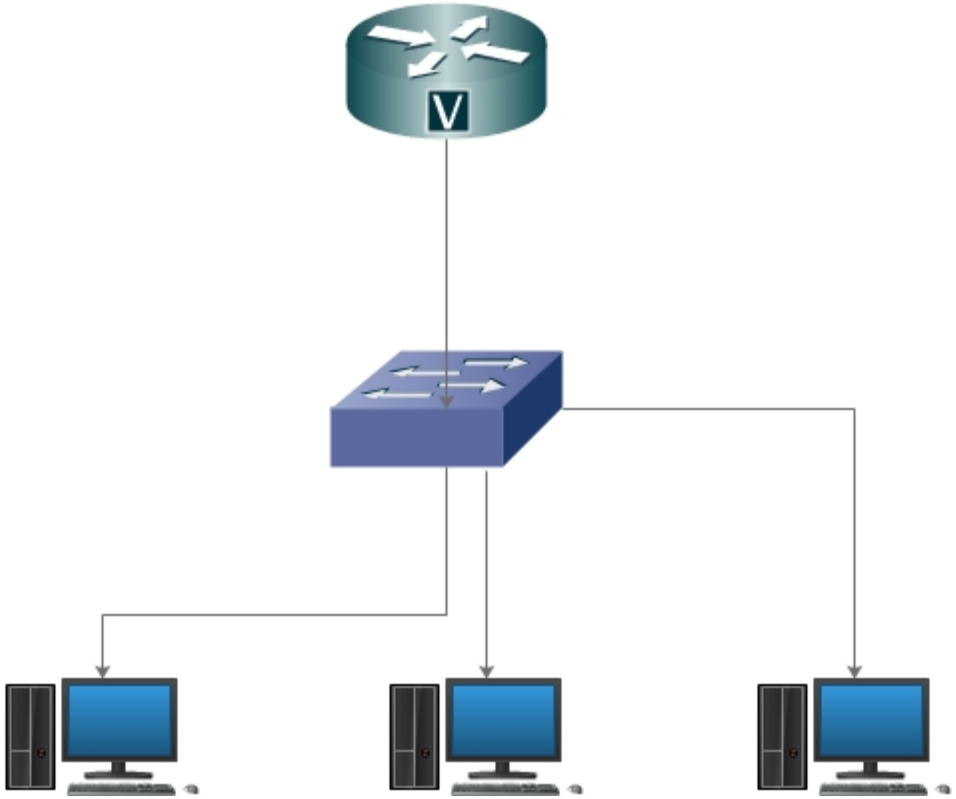
Basic Networking Components

A **switch** enables multiple devices to share a network while preventing each device's traffic from interfering with other devices' traffic. The switch acts as a traffic cop at a busy intersection. When a data packet arrives at one of its ports, the switch determines which direction the packet is headed. It then forwards the packet through the correct port for its destination.

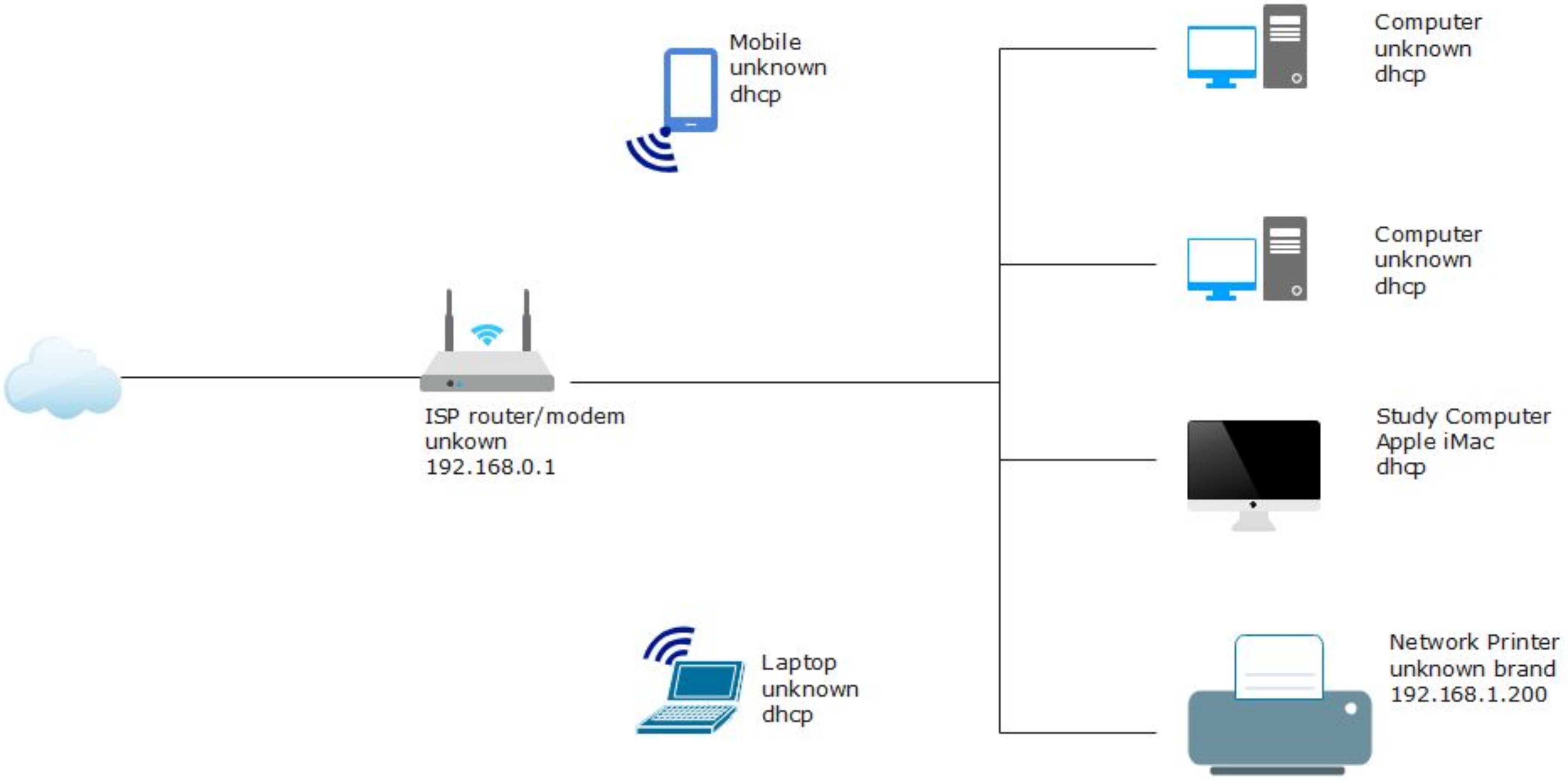


Basic Networking Components

A **router** directs data traffic between devices on different networks, determining the most efficient path for data to reach its destination. It connects local networks, assigns unique IP addresses, and serves as a gateway for devices to access the internet. A router Uses Intelligent Decisions (Routing Protocols) to Find the Best Way to Get a Packet of Information from One Network to Another.



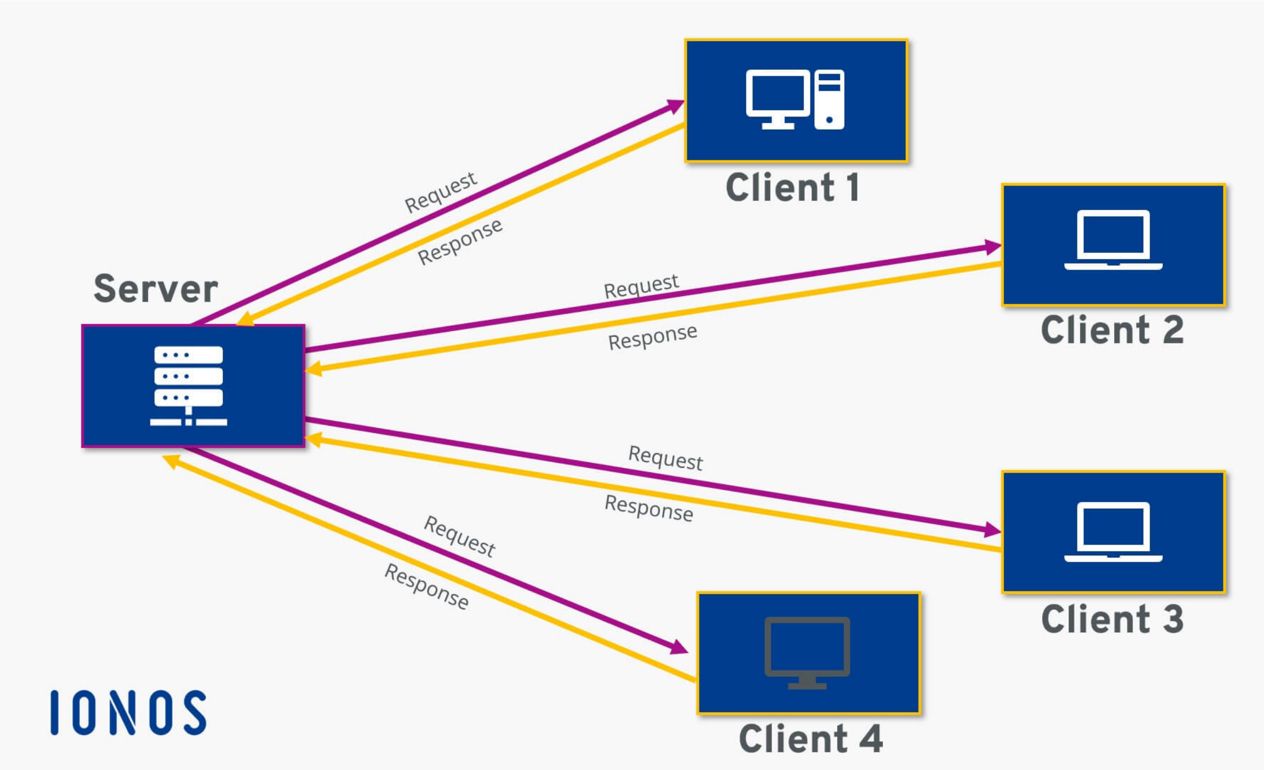
Basic Network Diagram



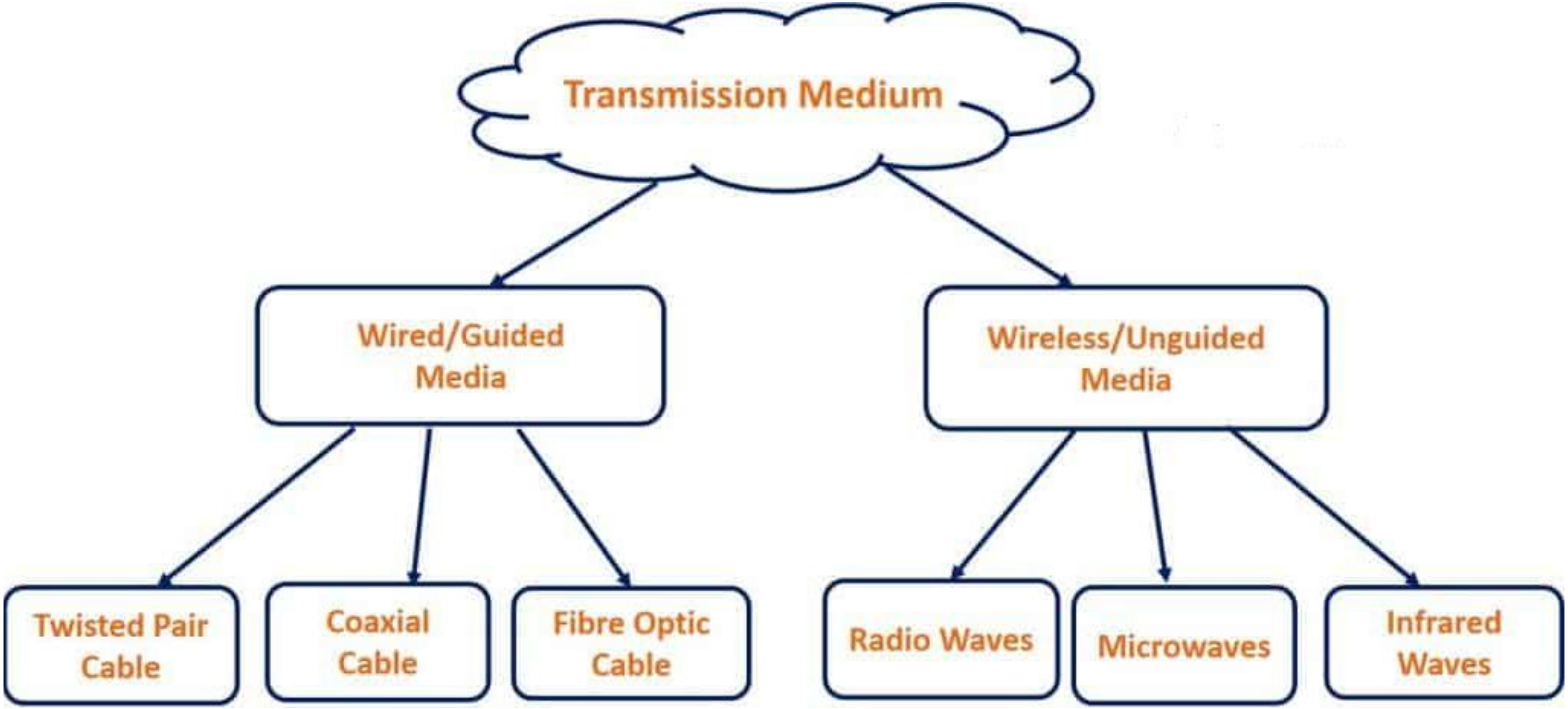
Basic Networking Components

A **server** is a specialized computer or software system designed to provide services, data, or resources to other computers, known as clients, over a network.

These services can range from delivering web pages and email to storing and managing files or running applications. These machines run on a client-server model, where clients request specific services or resources, and the server fulfills these requests.



Transmission Media



Practice:

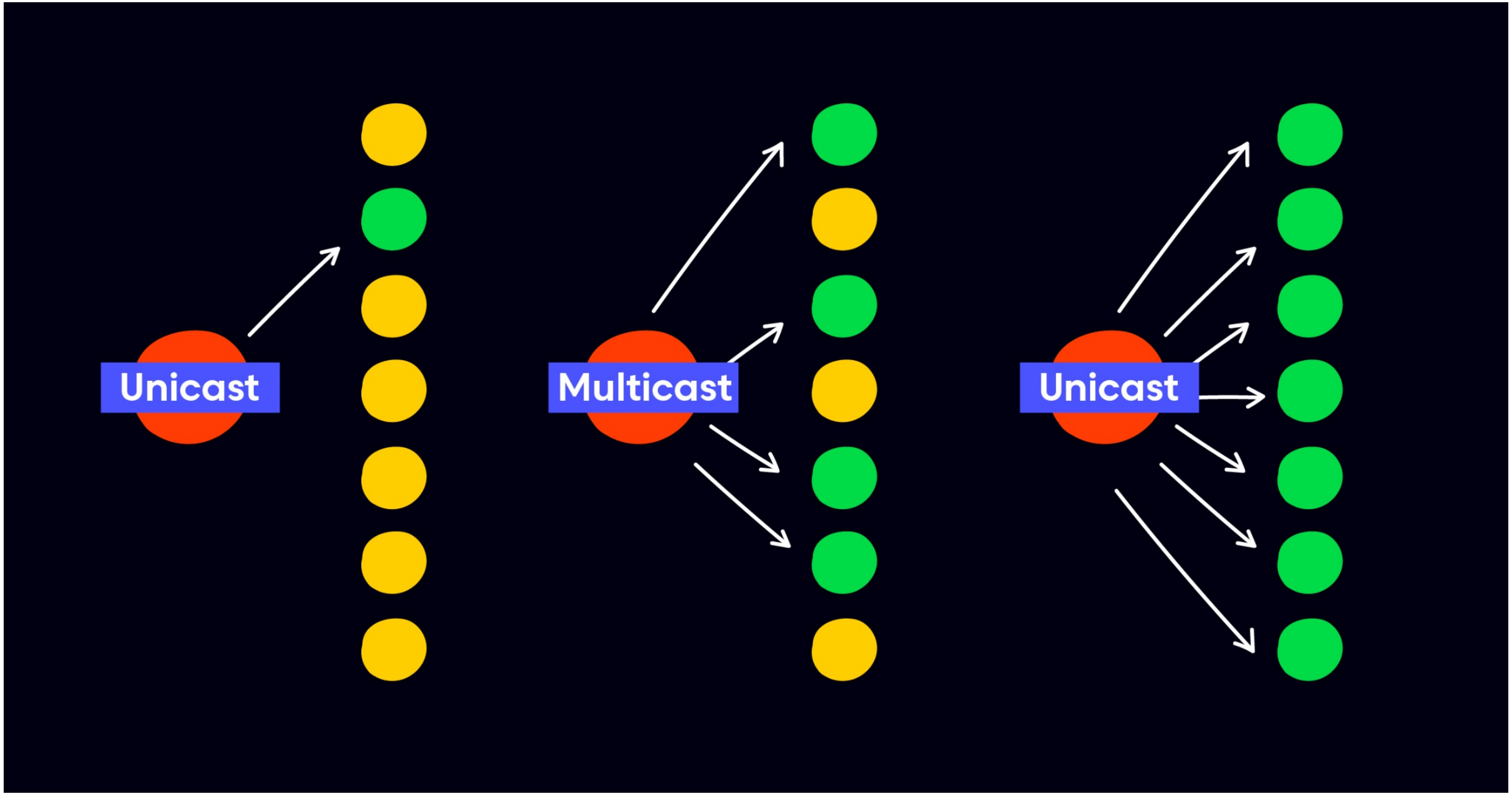
https://tryhackme.com/room/whatisnetworking

Students are advised to complete this room from their own THM account.

MAC Address

1. A MAC address is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment.
2. MAC addresses are primarily assigned by device manufacturers, and are therefore often referred to as the burned-in address, or as an Ethernet hardware address, hardware address, or physical address.
3. As typically represented, MAC addresses are recognizable as six groups of two hexadecimal digits, separated by hyphens, colons, or without a separator.

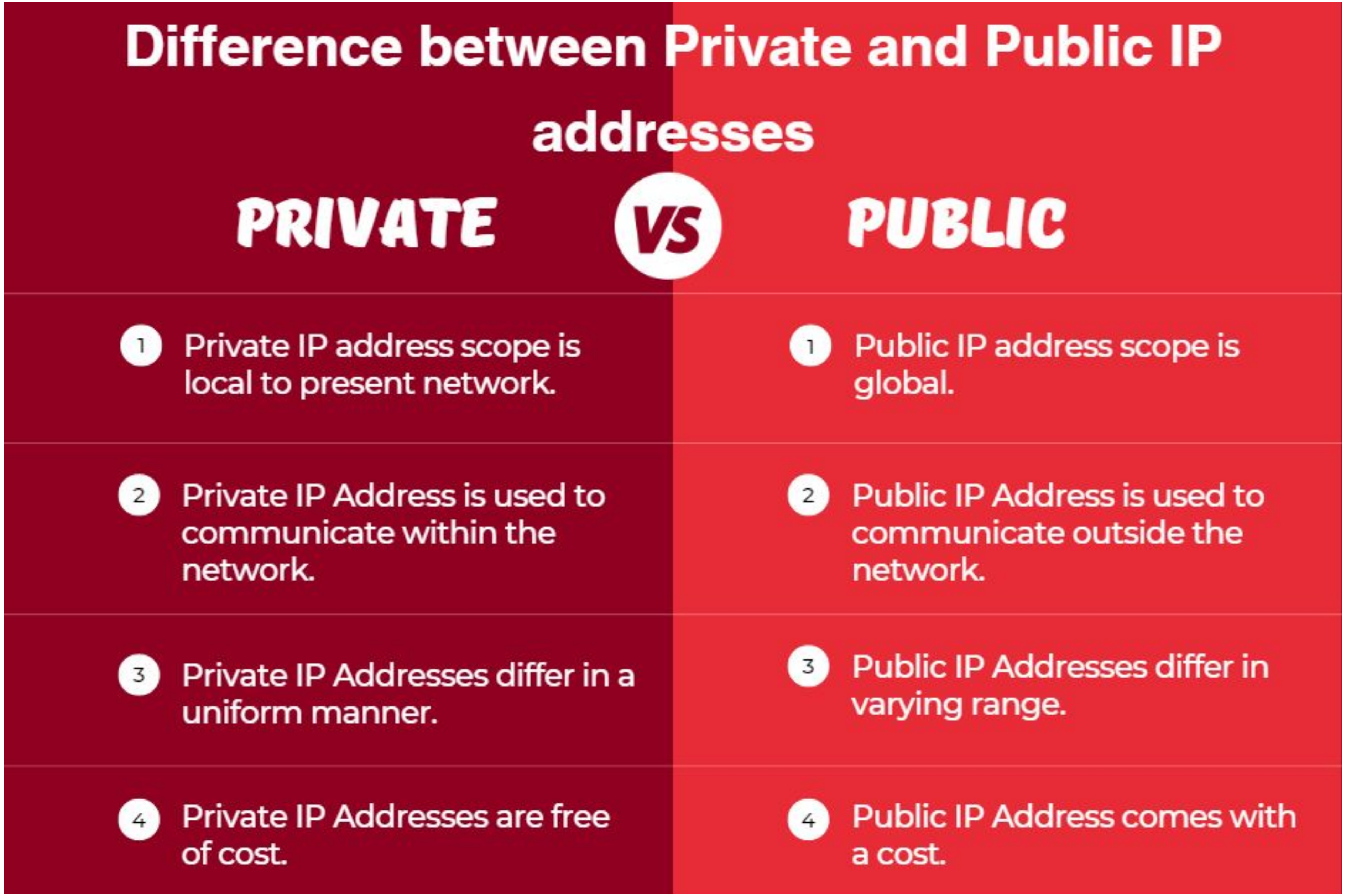
Types of Communication



IP Address

1. An Internet Protocol (IP) address is the unique identifying number assigned to every device connected to the internet. An IP address definition is a numeric label assigned to devices that use the internet to communicate.
2. The Internet Assigned Numbers Authority (IANA) allocates the IP address and its creation. The full range of IP addresses can go from 0.0.0.0 to 255.255.255.255.
3. A public IP address is a unique IP address assigned to your network router by your internet service provider and can be accessed directly over the internet. A private IP address is a unique address that your network router assigns to your device.

Types of IP Addresses



Difference between Private and Public IP addresses

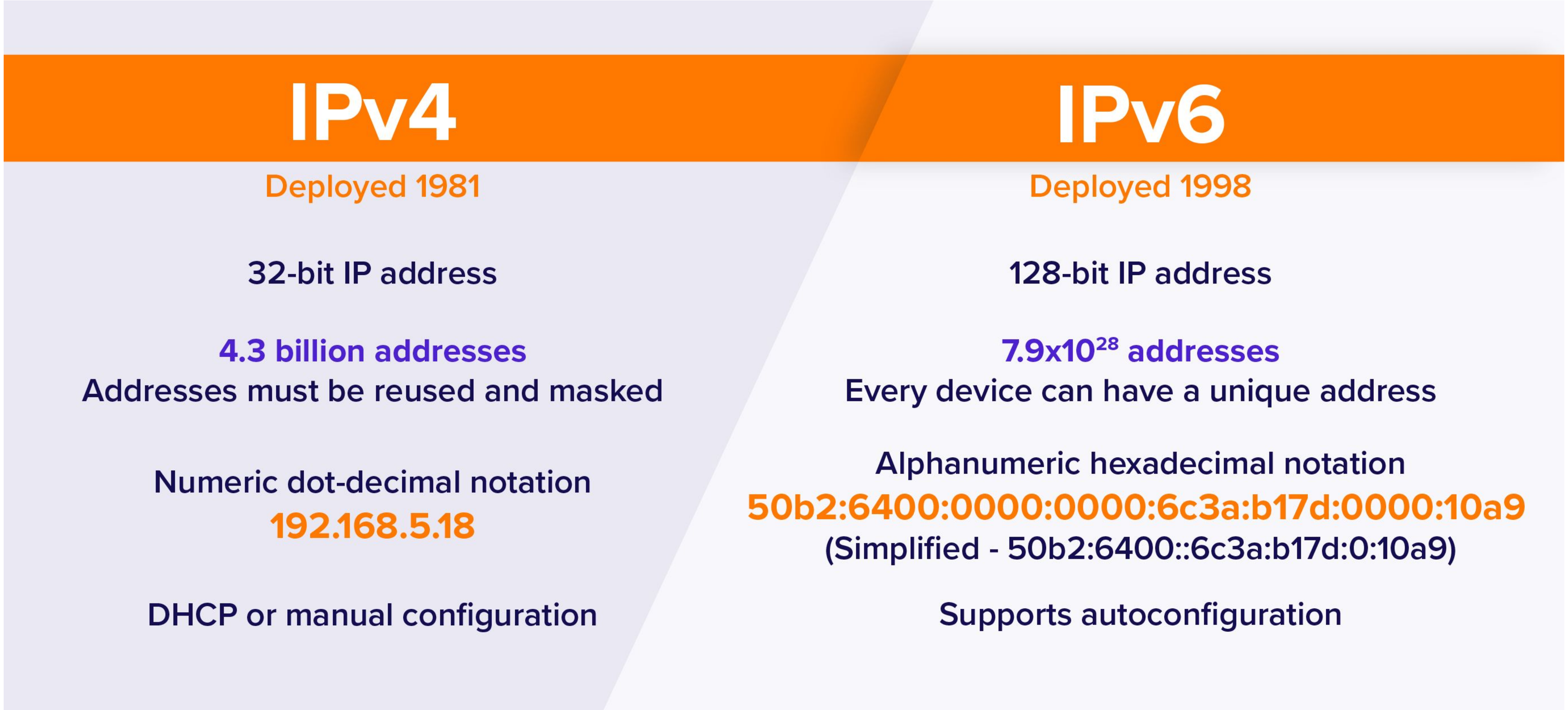
PRIVATE	PUBLIC
1 Private IP address scope is local to present network.	1 Public IP address scope is global.
2 Private IP Address is used to communicate within the network.	2 Public IP Address is used to communicate outside the network.
3 Private IP Addresses differ in a uniform manner.	3 Public IP Addresses differ in varying range.
4 Private IP Addresses are free of cost.	4 Public IP Address comes with a cost.

Task

Demonstrate how to find private and public IP Addresses of one's system.

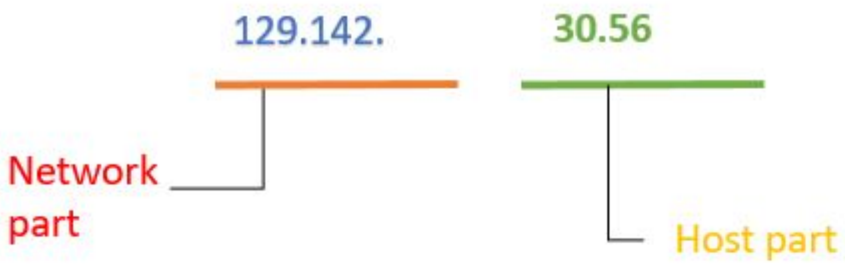
Use 'ipconfig' command and 'whatismyip' website

Types of IP Addresses



IPv4	IPv6
Deployed 1981	Deployed 1998
32-bit IP address	128-bit IP address
4.3 billion addresses Addresses must be reused and masked	$7.9x10^{28}$ addresses Every device can have a unique address
Numeric dot-decimal notation 192.168.5.18	Alphanumeric hexadecimal notation 50b2:6400:0000:0000:6c3a:b17d:0000:10a9 (Simplified - 50b2:6400::6c3a:b17d:0:10a9)
DHCP or manual configuration	Supports autoconfiguration

IPv4 Address Classification



IP Address is divided into two parts:

Prefix: The prefix part of IP address identifies the physical network to which the computer is attached. Prefix is also known as a **network address.**

Suffix: The suffix part identifies the individual computer on the network. The suffix is also called the **host address.**

IPv4 Address Classes

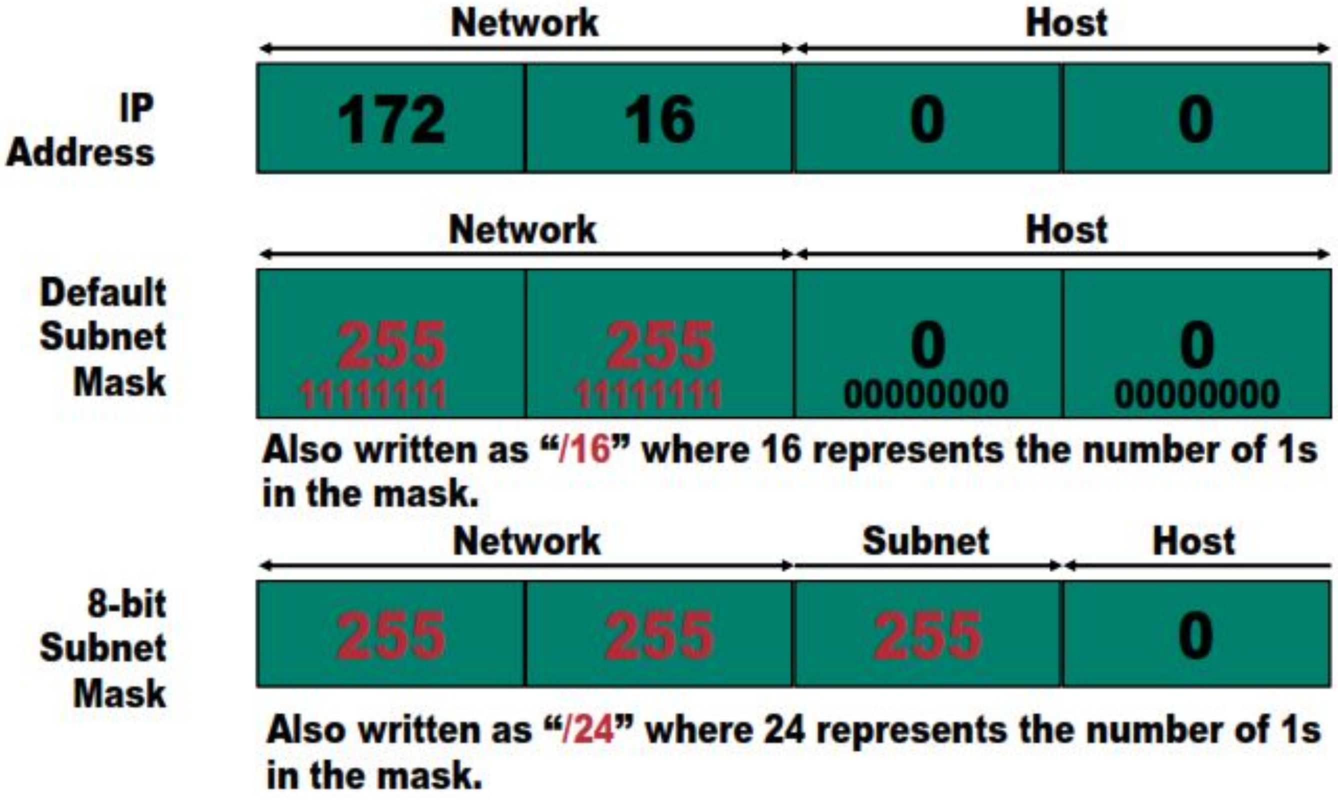
CLASS	1st Octet of IP Address	Default Subnet Mask	Network / Host	No. of Networks	Max. Nodes in a Network
A	1- 126	255.0.0.0	N. H. H. H	126	16,777,214
B	128 - 191	255.255.0.0	N.N.H.H	16,384	65,534
C	192 - 223	255.255.255.0	N.N.N.H	2,097,152	254
D*	224 – 239				
E**	240 - 254				

* Reserve for multi-tasking.

** This class is reserved for research and Development Purposes.

What Is Sub-Netting

- Sub-netting in networking is like dividing a large neighborhood into smaller blocks. It's a technique used to break down a single IP network into smaller, more manageable segments, called subnets. Sub-netting helps in efficient IP address management, network organization, and routing by grouping devices based on their location or function.



Also written as "/16" where 16 represents the number of 1s in the mask.

Also written as "/24" where 24 represents the number of 1s in the mask.

Protocols, Ports, & Sockets

Protocols

- Computers communicate with each other with network protocols.
- Protocols are rules governing how machines exchange data and enable effective communication.
- In an operating system (OS), a protocol runs as a process or service.

Ports

- Ports are logical constructs that bind a unique port number to a protocol process or service.
- A port address is like a door number on a building. It helps data packets know which service or application on a computer to go to.

Sockets

- Sockets are a combination of an IP address and a port number, for example, 192.168.1.1:80

Protocols, Ports, & Sockets

Protocols

- Computers communicate with each other with network protocols.
- Protocols are rules governing how machines exchange data and enable effective communication.
- In an operating system (OS), a protocol runs as a process or service.

Ports

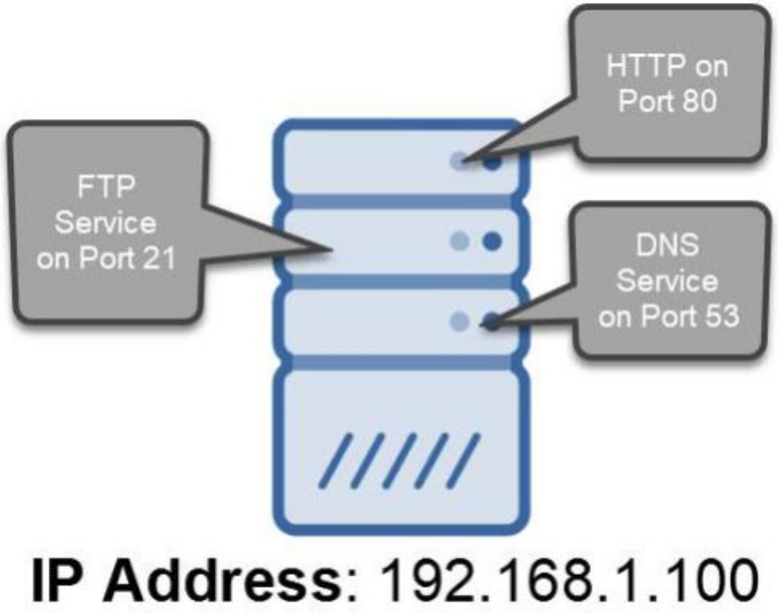
- Ports are logical constructs that bind a unique port number to a protocol process or service.
- A port address is like a door number on a building. It helps data packets know which service or application on a computer to go to.

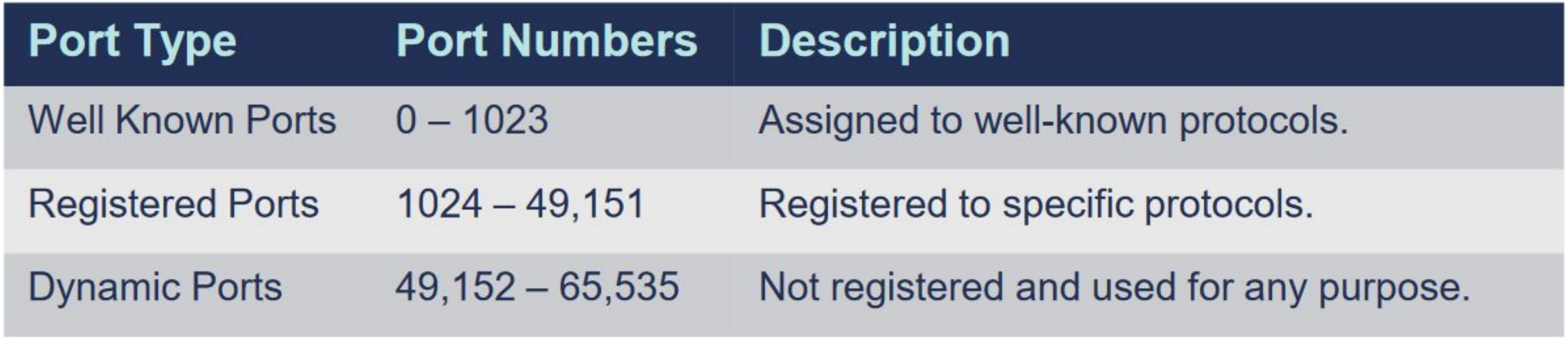
Sockets

- Sockets are a combination of an IP address and a port number, for example, 192.168.1.1:80

Protocols, Ports, & Sockets

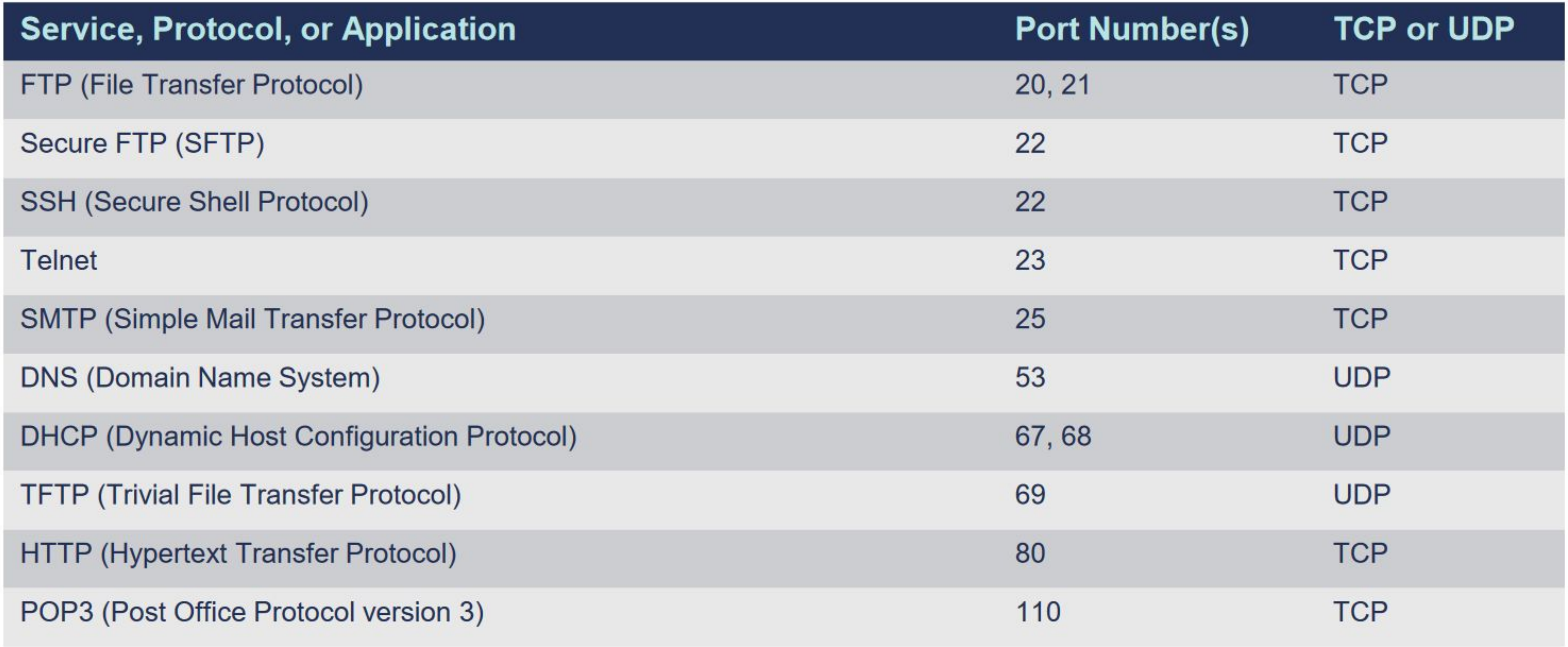
- Computers require ports because of network application multitasking.
- Because a computer may have only one IP address, it needs ports to differentiate network protocols and services running on it.
- There are 65,536 ports available





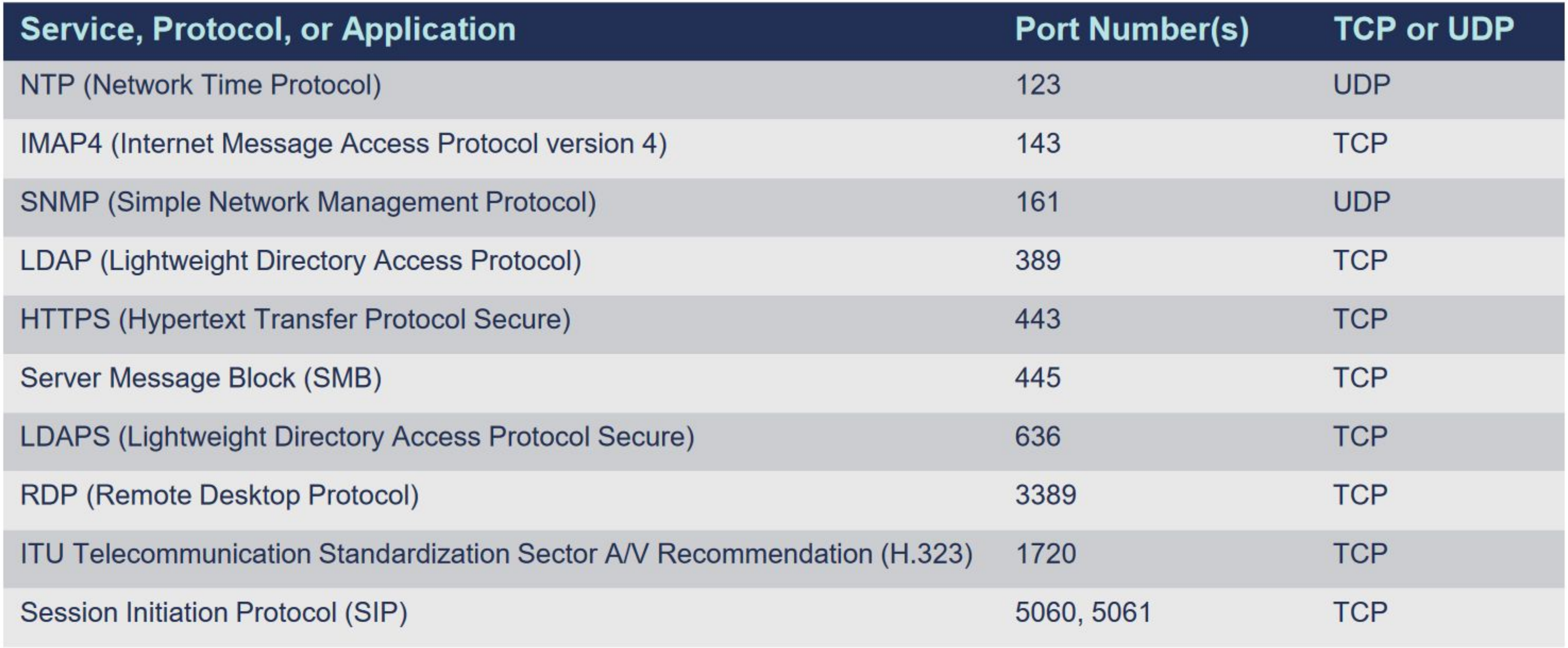
Port Type	Port Numbers	Description
Well Known Ports	0 – 1023	Assigned to well-known protocols.
Registered Ports	1024 – 49,151	Registered to specific protocols.
Dynamic Ports	49,152 – 65,535	Not registered and used for any purpose.

Some Well Known Ports



Service, Protocol, or Application	Port Number(s)	TCP or UDP
FTP (File Transfer Protocol)	20, 21	TCP
Secure FTP (SFTP)	22	TCP
SSH (Secure Shell Protocol)	22	TCP
Telnet	23	TCP
SMTP (Simple Mail Transfer Protocol)	25	TCP
DNS (Domain Name System)	53	UDP
DHCP (Dynamic Host Configuration Protocol)	67, 68	UDP
TFTP (Trivial File Transfer Protocol)	69	UDP
HTTP (Hypertext Transfer Protocol)	80	TCP
POP3 (Post Office Protocol version 3)	110	TCP

Some Well Known Ports



Service, Protocol, or Application	Port Number(s)	TCP or UDP
NTP (Network Time Protocol)	123	UDP
IMAP4 (Internet Message Access Protocol version 4)	143	TCP
SNMP (Simple Network Management Protocol)	161	UDP
LDAP (Lightweight Directory Access Protocol)	389	TCP
HTTPS (Hypertext Transfer Protocol Secure)	443	TCP
Server Message Block (SMB)	445	TCP
LDAPS (Lightweight Directory Access Protocol Secure)	636	TCP
RDP (Remote Desktop Protocol)	3389	TCP
ITU Telecommunication Standardization Sector A/V Recommendation (H.323)	1720	TCP
Session Initiation Protocol (SIP)	5060, 5061	TCP

Practice:

https://tryhackme.com/room/introtonetworking

This module covers OSI and TCP/IP in detail

Students are advised to complete this room from their own THM account.

THANK YOU