Network N+ Guide Notes

Prepared by
IANT Udaipur

Network Indexing

CCNA Indexing

Network Types :

Personal Area Network (PAN)

The smallest and most basic type of network, a PAN is made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building. These types of networks are typically found in small offices or residences, and are managed by one person or organization from a single device.

Local Area Network (LAN)

We’re confident that you’ve heard of these types of networks before – LANs are the most frequently discussed networks, one of the most common, one of the most original and one of the simplest types of networks. LANs connect groups of computers and low-voltage devices together across short distances (within a building or between a group of two or three buildings in close proximity to each other) to share information and resources. Enterprises typically manage and maintain LANs.

Using routers, LANs can connect to wide area networks (WANs, explained below) to rapidly and safely transfer data.

Campus Area Network (CAN)

Larger than LANs, but smaller than metropolitan area networks (MANs, explained below), these types of networks are typically seen in universities, large K-12 school districts or small businesses. They can be spread across several buildings that are fairly close to each other so users can share resources.

Metropolitan Area Network (MAN)

These types of networks are larger than LANs but smaller than WANs – and incorporate elements from both types of networks. MANs span an entire geographic area (typically a town or city, but sometimes a campus). Ownership and maintenance is handled by either a single person or company (a local council, a large company, etc.).

Wide Area Network (WAN)

Slightly more complex than a LAN, a WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other over one large network to communicate even when they're miles apart.

The Internet is the most basic example of a WAN, connecting all computers together around the world. Because of a WAN's vast reach, it is typically owned and maintained by multiple administrators or the public.

Virtual Private Network (VPN)

By extending a private network across the Internet, a VPN lets its users send and receive data as if their devices were connected to the private network – even if they're not. Through a virtual point-to-point connection, users can access a private network remotely.

Workstation :

A workstation is a special computer designed for technical or scientific applications. Intended primarily to be used by one person at a time, they are commonly connected to a local area network and run multi-user operating systems. Desktop management is a comprehensive approach to managing all the computers within an organization. Despite its name, desktop management includes overseeing laptops and other computing devices as well as desktop computers. Desktop management is a component of systems management, which is the administration of all components of an organization's information systems. Other components of systems management include network management and database management.

Host & Nodes :

A network host is a computer or other device connected to a computer network. A network host may offer information resources, services, and applications to users or other nodes on the network. A network host is a network node that is assigned a network layer host address.

Typically, the term is used when there are two computer systems connected by modems and telephone lines. The system that contains the data is called the host, while the computer at which the user sits is called the remote terminal. A computer that is connected to a TCP/IP network, including the Internet.

Server :

In computing, a server is a computer program or a device that provides functionality for other programs or devices, called "clients". This architecture is called the client–server model, and a single overall computation is distributed across multiple processes or devices. Servers can provide various functionalities, often called "services", such as sharing data or resources among multiple clients, or performing computation for a client. A single server can serve multiple clients, and a single client can use multiple servers. A client process may run on the same device or may connect over a network to a server on a different device.

A server is a type of computer or device on a network that manages network resources. Servers are often dedicated, meaning that they perform no other tasks besides their server tasks. On multiprocessing operating systems, however, a single computer can execute several programs at once. A server in this case could refer to the program that is managing resources rather than the entire computer.

Different Types of Servers

Different types servers do different jobs, from serving email and video to protecting internal networks and hosting websites. There are many different types of servers, for example:

File server: a computer and storage device dedicated to storing files. Any user on the network can store files on the server.

Print server: a computer that manages one or more printers, and a network server is a computer that manages network traffic.

Database server: a computer system that processes database queries.

Web server: Web servers are computers that deliver (or serve up) Web pages. Every Web server has an IP address and possibly a domain name.

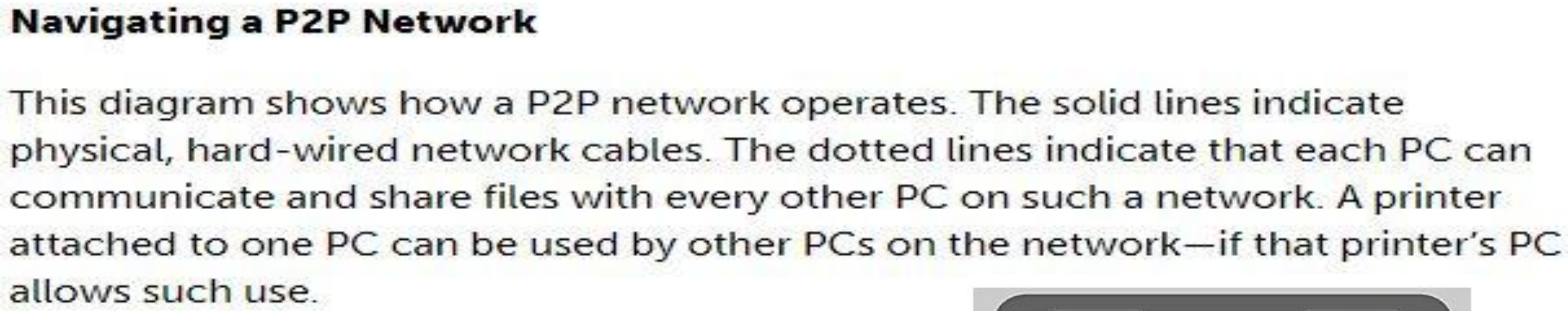
Proxy server: A proxy server is a server that sits between a client application, such as a Web browser, and a real server. Proxy servers have two main purposes: to improve performance and to filter requests.

Application server: An application server is a program that handles all application operations between users and an organization's back-end business applications or databases.

Cloud server: Cloud servers are services made available to customers on demand via the Internet. Rather than being provided by a single server or virtual server, cloud server hosting services are provided by multiple connected servers that comprise a cloud.

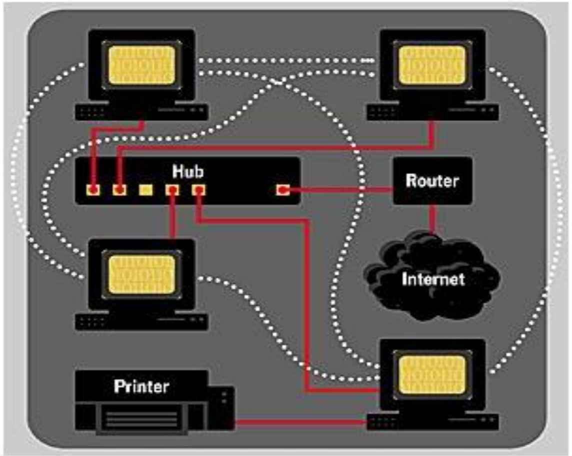
Peer to Peer Network (P2P) :

A peer-to-peer (P2P) network is created when two or more PCs are connected and share resources without going through a separate server computer. A P2P network can be an ad hoc connection - a couple of computers connected via a Universal Serial Bus to transfer files. A P2P network also can be a permanent infrastructure that links a half-dozen computers in a small office over copper wires. Or a P2P network can be a network on a much grander scale in which special protocols and applications set up direct relationships among users over the Internet.



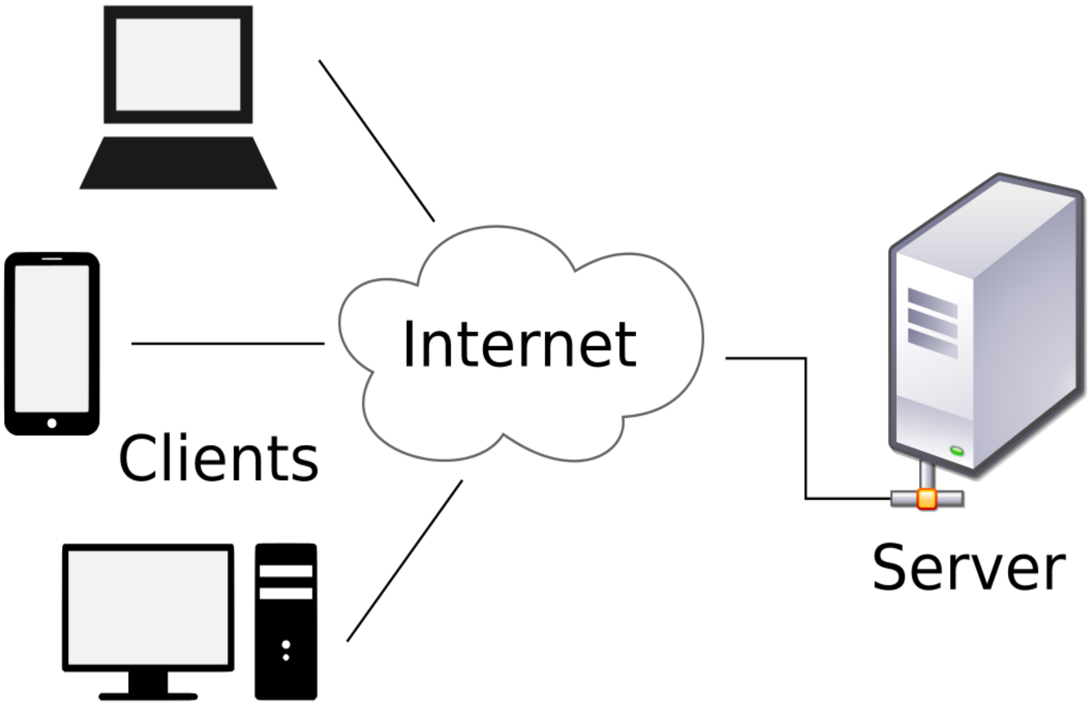
Navigating a P2P Network

This diagram shows how a P2P network operates. The solid lines indicate physical, hard-wired network cables. The dotted lines indicate that each PC can communicate and share files with every other PC on such a network. A printer attached to one PC can be used by other PCs on the network—if that printer's PC allows such use.



Client / Server Network :

A computer network in which one centralized, powerful computer (called the server) is a hub to which many less powerful personal computers or workstations (called clients) are connected. The clients run programs and access data that are stored on the server. Compare peer-to-peer network.

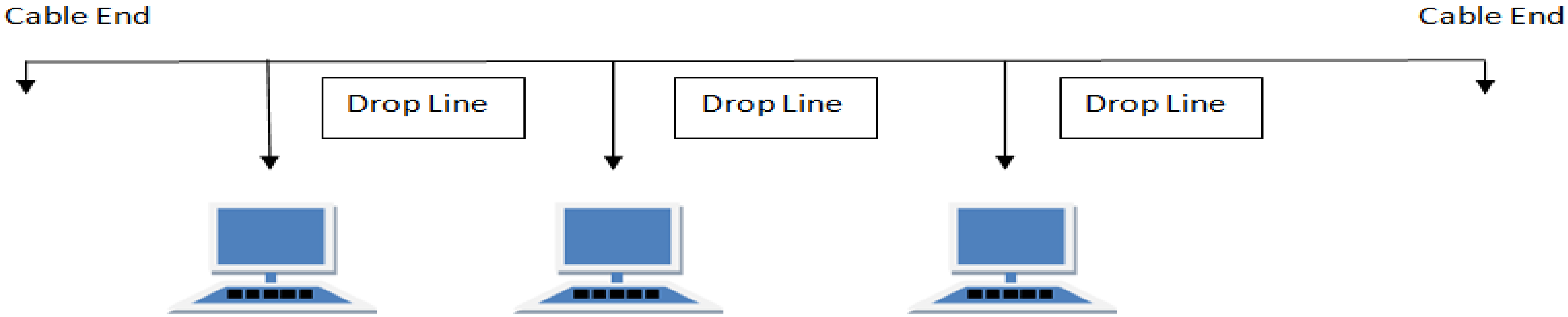


Network Topology :

Computers in a network have to be connected in some logical manner. The layout pattern of the interconnections between computers in a network is called network topology. You can think of topology as the virtual shape or structure of the network. Network topology is also referred to as 'network architecture.‘ Devices on the network are referred to as 'nodes.' The most common nodes are computers and peripheral devices. Network topology is illustrated by showing these nodes and their connections using cables. There are a number of different types of network topologies, including point-to-point, bus, star, ring, mesh, tree and hybrid. Let's review these main types.

BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called Linear Bus topology.



Features of Bus Topology

- It transmits data only in one direction.
- Every device is connected to a single cable

Advantages of Bus Topology

- It is cost effective.
- Cable required is least compared to other network topology.
- Used in small networks.
- It is easy to understand.
- Easy to expand joining two cables together.

Disadvantages of Bus Topology

- Cables fails then whole network fails.
- If network traffic is heavy or nodes are more the performance of the network decreases.
- Cable has a limited length.
- It is slower than the ring topology.

RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

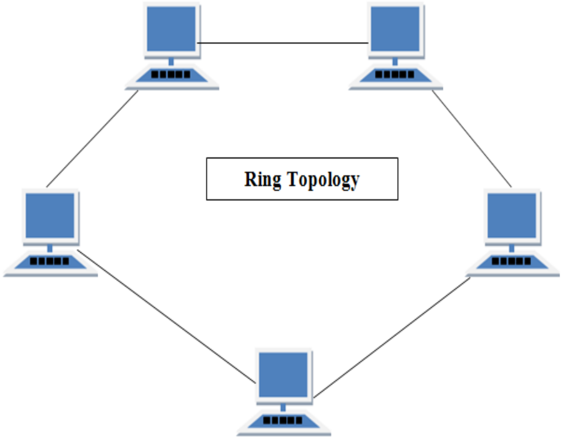
Features of Ring Topology

•A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

•The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.

•In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.

•Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.



Advantages of Ring Topology

•Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.

•Cheap to install and expand

Disadvantages of Ring Topology

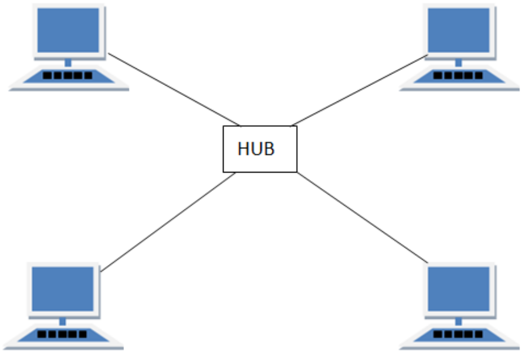
•Troubleshooting is difficult in ring topology.

•Adding or deleting the computers disturbs the network activity.

•Failure of one computer disturbs the whole network.

STAR Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features of Star Topology

- Every node has its own dedicated connection to the hub.
- Hub acts as a repeater for data flow.
- Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

- Fast performance with few nodes and low network traffic.
- Hub can be upgraded easily.
- Easy to troubleshoot.
- Easy to setup and modify.
- Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

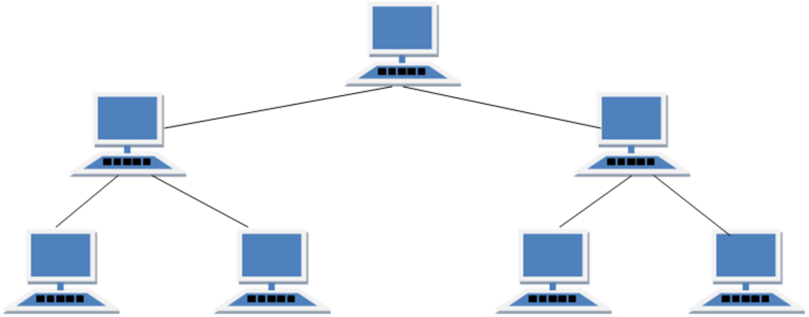
- Cost of installation is high.
- Expensive to use.
- If the hub fails then the whole network is stopped because all the nodes depend on the hub.
- Performance is based on the hub that is it depends on its capacity

TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

Features of Tree Topology

- Ideal if workstations are located in groups.
- Used in Wide Area Network.



Advantages of Tree Topology

- Extension of bus and star topologies.
- Expansion of nodes is possible and easy.
- Easily managed and maintained.
- Error detection is easily done.

Disadvantages of Tree Topology

- Heavily cabled.
- Costly.
- If more nodes are added maintenance is difficult.
- Central hub fails, network fails.

MESH Topology

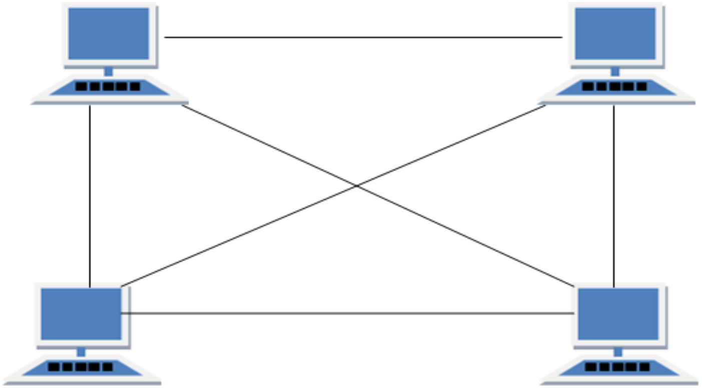
It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has **n(n-1)/2** physical channels to link **n** devices. There are two techniques to transmit data over the Mesh topology, they are : Routing & Flooding

Features of Mesh Topology

•Fully connected.

•Robust.

•Not flexible.



Advantages of Mesh Topology

•Each connection can carry its own data load.

•It is robust.

•Fault is diagnosed easily.

•Provides security and privacy.

Disadvantages of Mesh Topology

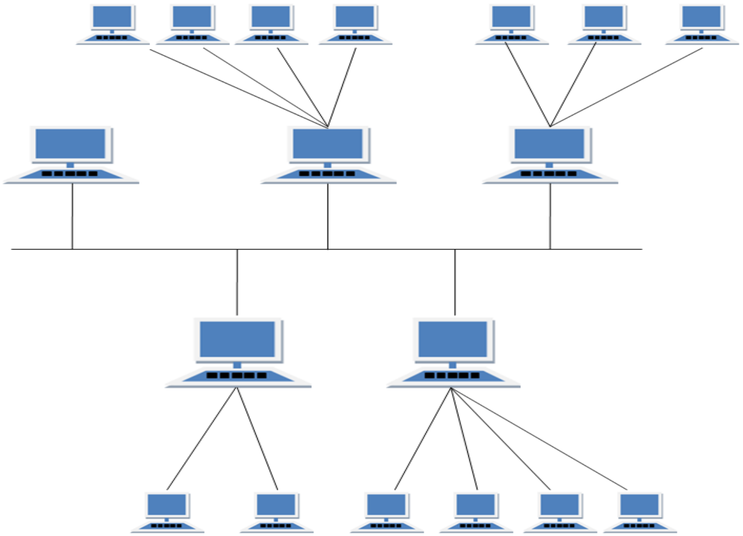
•Installation and configuration is difficult.

•Cabling cost is more.

•Bulk wiring is required.

HYBRID Topology

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



Features of Hybrid Topology

- It is a combination of two or topologies.
- Inherits the advantages and disadvantages of the topologies included.

Advantages of Hybrid Topology

- Reliable as Error detecting and trouble shooting is easy.
- Effective.
- Scalable as size can be increased easily.
- Flexible.

Disadvantages of Hybrid Topology

- Complex in design.
- Costly.

Backbone :

A backbone is a larger transmission line that carries data gathered from smaller lines that interconnect with it. At the local level, a backbone is a line or set of lines that local area networks connect to for a wide area network connection or within a local area network to span distances efficiently (for example, between buildings). On the Internet or other wide area network, a backbone is a set of paths that local or regional networks connect to for long-distance interconnection. The connection points are known as network nodes or telecommunication data switching exchanges (DSEs).

Network Segments :

Commonly refers to a specific connection between two computers, or between two pieces of hardware such as a bridge or router. In general, the term refers to a specific part of a network topology, which represents the way that the hardware system is set up.

Different kinds of topologies also have their own benefits and disadvantages. Some are better for security, whereas others provide a more redundant or fault-tolerant design. Some are more limiting in terms of access between individual computers and hardware stations, and some are easier to connect with cable. Network administrators look at all of these designs, as well as the issue of network segment engineering, to determine the best solutions for a given network.

Loopback Address :

Loopback address is a special IP number (127.0.0.1) that is designated for the software loopback interface of a machine. The loopback interface has no hardware associated with it, and it is not physically connected to a network. The loopback interface allows IT professionals to test IP software without worrying about broken or corrupted drivers or hardware. Every computer on a computer network has an IP address associated with it. This IP address includes four sets of numbers with a period between each set. The IP address assigned to your computer could be any of a number of combinations, but there is one IP address that is set aside specifically to connect back to your own computer. This is called the loopback address. The loopback address is usually the same for all computer networks.
The entire range from 127.0.0.0 to 127.255.255.255 is reserved for loopback purposes but you'll almost never see anything but 127.0.0.1 used in the real world.

Start >> Run >> ping 127.0.0.1 -t

Network Interface Card :

A network interface controller NIC, also known as a network interface card, network adapter, Ethernet card, LAN adapter onboard network card or physical network interface and by similar terms is a computer hardware component that connects a computer to a computer network using an Ethernet cable with an RJ-45 connector.

A network interface card provides the computer with a dedicated, full-time connection to a network. Personal computers and workstations on a local area network (LAN) typically contain a network interface card specifically designed for the LAN transmission technology.

Hub :

An Ethernet hub, active hub, network hub, repeater hub, multiport repeater, or simply hub is a network hardware device for connecting multiple Ethernet devices together and making them act as a single network segment. It has multiple input/output (I/O) ports, in which a signal introduced at the input of any port appears at the output of every port except the original incoming. A hub works at the physical layer (layer 1) of the OSI model. A repeater hub also participates in collision detection, forwarding a jam signal to all ports if it detects a collision. In addition to standard 8P8C ("RJ45") ports, some hubs may also come with a BNC or an Attachment Unit Interface (AUI) connector to allow connection to legacy 10BASE2 or 10BASE5 network segments.

A hub, also called a network hub, is a common connection point for devices in a network. Hubs are devices commonly used to connect segments of a LAN. The hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets. What Hubs DoHubs and switches serve as a central connection for all of your network equipment and handles a data type known as frames. Frames carry your data. When a frame is received, it is amplified and then transmitted on to the port of the destination PC.

Switch :

A network switch (also called switching hub, bridging hub, officially MAC bridge) is a computer networking device that connects devices together on a computer network by using packet switching to receive, process, and forward data to the destination device.

A network switch is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer (layer 2) of the OSI model. Some switches can also process data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

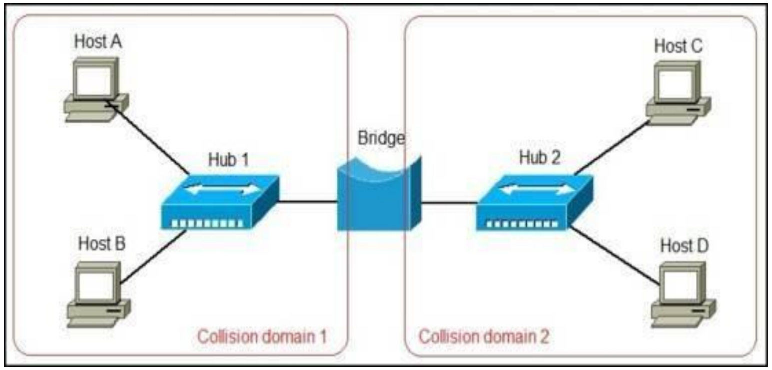
An ethernet switch is a device used to build a network connection between the attached computers (allows computers to talk to each other). It differs from an ethernet hub: While a hub will send incoming data packets to all ports, a switch understands the packets' addressing scheme and will send any data packet only to its destination port, thus limiting the number of collisions (data sent at the same time).

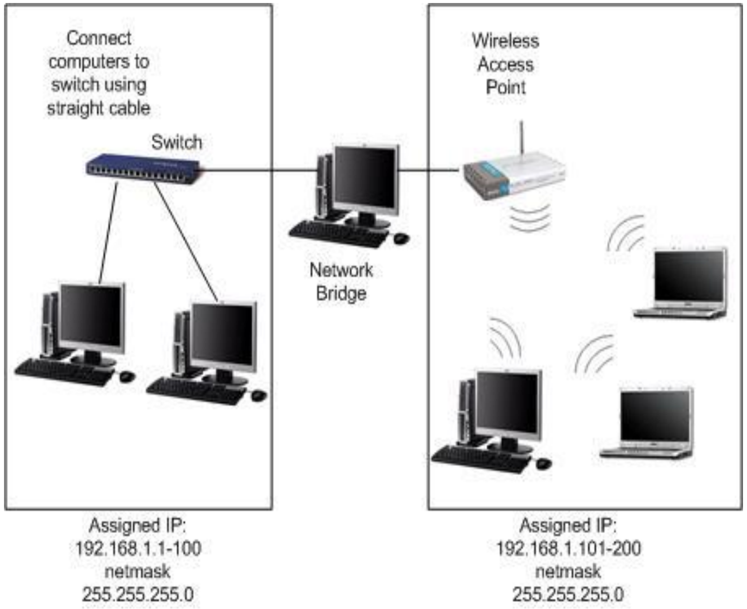
There are two types of switch: Unmanaged Switches & Managed Switches

Bridge :

A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments. This function is called network bridging. Bridging is distinct from routing, as routing allows multiple different networks to communicate independently while remaining separate bridging connects two separate networks as if they are only one network (hence the name "bridging"). In the OSI model, bridging is performed in the first two layers, the device is known as a wireless bridge and the function as wireless bridging.

An Ethernet network bridge is a device which connects two different local area networks together. Both networks must connect using the same Ethernet protocol. Bridges can also be used to add remote computers to a LAN. Many bridges can connect multiple computers or other compatible devices with or without wires.





Modem :

A modem (modulator–demodulator) is a network hardware device that allows a computer to send and receive data over a telephone line or a cable or satellite connection. In the case of transmission over an analog telephone line, which was once the most popular way to access the internet, the modem converts data between analog and digital formats in real time for two-way network communication. In the case of the high-speed digital modems popular today, the signal is much simpler and doesn't require the analog-to-digital conversion.

Router :

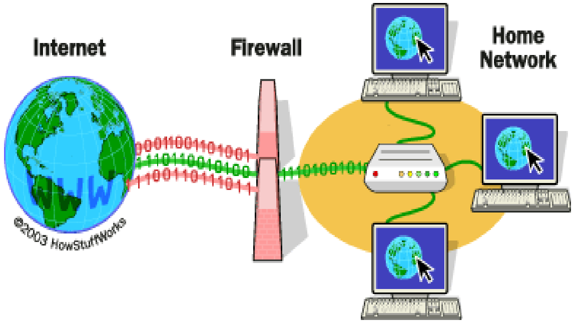
Routers are electronic devices that join multiple computer networks together via either wired or wireless connections. A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. A data packet is typically forwarded from one router to another router through the networks that constitute an internetwork until it reaches its destination node. A router is connected to two or more data lines from different networks.

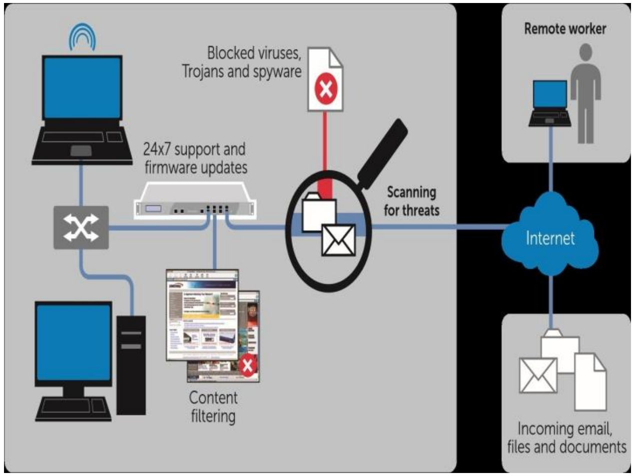
The most familiar type of routers are home and small office routers that simply pass IP packets between the home computers and the Internet. An example of a router would be the owner's cable or DSL router, which connects to the Internet through an Internet service provider (ISP). More sophisticated routers, such as enterprise routers, connect large business or ISP networks up to the powerful core routers that forward data at high speed along the optical fiber lines of the Internet backbone. Though routers are typically dedicated hardware devices, software-based routers also exist.

Firewall :

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

A firewall can be hardware, software, or both. In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.[1] A firewall typically establishes a barrier between a trusted internal network and untrusted outside network, such as the Internet. Firewall's are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks; they are either software appliances running on general-purpose hardware, or hardware-based firewall computer appliances. Firewall appliances may also offer other functionality to the internal network they protect.




Blocked viruses, Trojans and spyware
24x7 support and firmware updates
Scanning for threats
Content filtering
Remote worker
Internet
Incoming email, files and documents

IDS/IPS/HIDS :

Intrusion Detection System - A device or application that analyzes whole packets, both header and payload, looking for known events. When a known event is detected a log message is generated detailing the event. similar to IPS but does not affect flows in any way - only logs or alerts on malicious traffic.

Intrusion Prevention System - A device or application that analyzes whole packets, both header and payload, looking for known events. When a known event is detected the packet is rejected. inspects traffic flowing through a network and is capable of blocking or otherwise remediating flows that it determines are malicious. Usually uses a combination of traffic and file signatures and heuristic analysis of flows.

Host intrusion detection systems (HIDS) - And network intrusion detection systems (NIDS) are methods of security management for computers and networks. In HIDS, anti-threat applications such as firewalls, antivirus software and spyware-detection programs are installed on every network computer that has two-way access to the outside environment such as the Internet. In NIDS, anti-threat software is installed only at specific points such as servers that interface between the outside environment and the network segment to be protected.

OSI Layers :

OSI (Open Systems Interconnection) is reference model for how applications can communicate over a network. A reference model is a conceptual framework for understanding relationships. The main concept of OSI is that the process of communication between two endpoints in a telecommunication network can be divided into seven distinct groups of related functions, or layers. Each communicating user or program is at a computer that can provide those seven layers of function. So in a given message between users, there will be a flow of data down through the layers in the source computer, across the network and then up through the layers in the receiving computer. The seven layers of function are provided by a combination of applications, operating systems, network card device drivers and networking hardware that enable a system to put a signal on a network cable or out over Wi-Fi or other wireless protocol.

Trick to remember the OSI layer

Bottom to Top	**Top to Bottom**
[Application] Away	[Application] All
[Presentation] Pizza	[Presentation] People
[Session] Sausage	[Session] Should
[Transport] Throw	[Transport] Try
[Network] Not	[Network] New
[Data Link] Do	[Data Link] Dr
[Physical] Please	[Physical] Pepper

Physical (Layer 1)

OSI Model, Layer 1 conveys the bit stream - electrical impulse, light or radio signal - through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.
Layer 1 Physical examples include Ethernet, RJ45.

At Layer 1, the Physical layer of the OSI model is responsible for ultimate transmission of digital data bits from the Physical layer of the sending (source) device over network communications media to the Physical layer of the receiving (destination) device. Examples of Layer 1 technologies include Ethernet cables and Token Ring networks. Additionally, hubs and other repeaters are standard network devices that function at the Physical layer, as are cable connectors.

At the Physical layer, data are transmitted using the type of signaling supported by the physical medium: electric voltages, radio frequencies, or pulses of infrared or ordinary light.

Physical Layer (Bit & Binary)
This involves media, move bits between devices
MAC Address: Information Delivered
IP Address: Carrier of Information

Data Link (Layer 2)

At OSI Model, Layer 2, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.
Layer 2 Data Link examples include PPP, FDDI, ATM, IEEE 802.5/ 802.2, IEEE 802.3/802.2, HDLC, Frame Relay.

When obtaining data from the Physical layer, the Data Link layer checks for physical transmission errors and packages bits into data "frames". The Data Link layer also manages physical addressing schemes such as MAC addresses for Ethernet networks, controlling access of any various network devices to the physical medium. Because the Data Link layer is the single most complex layer in the OSI model, it is often divided into two parts, the "Media Access Control" sublayer and the "Logical Link Control" sublayer.

Data Link Layer (Frame)
Function of this layers: Error Detection and Control of Data
Uniqueness of this layer: MAC address
Protocols of this layer: PPP, HDLC, ATM, Frame Relay, SLIP, Ethernet

Network (Layer 3)

Layer 3 provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing. Layer 3 Network examples include AppleTalk DDP, IP, IPX.

The Network layer adds the concept of routing above the Data Link layer. When data arrives at the Network layer, the source and destination addresses contained inside each frame are examined to determine if the data has reached its final destination. If the data has reached the final destination, this Layer 3 formats the data into packets delivered up to the Transport layer. Otherwise, the Network layer updates the destination address and pushes the frame back down to the lower layers. To support routing, the Network layer maintains logical addresses such as IP addresses for devices on the network. The Network layer also manages the mapping between these logical addresses and physical addresses. In IP networking, this mapping is accomplished through the Address Resolution Protocol (ARP).

Network Layer (Packet)
This layer is used for communication to remote networks.
Functions of this layer: Sorting, Filtering and Distribution
Protocols of this layer: Routed Protocol: IP/IPX/Apple talk
Routing Protocol: IGP, EGP, BGP, EBGP, IBGP, RIP, IGRP, RIP, OSPF, IS-IS

Transport (Layer 4)

OSI Model, Layer 4, provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.
Layer 4 Transport examples include SPX, TCP, UDP.

The Transport Layer delivers data across network connections. TCP is the most common example of a Transport Layer 4 network protocol. Different transport protocols may support a range of optional capabilities including error recovery, flow control, and support for re-transmission.

Transport Layer (Segment)
This layer is responsible for Control of Data flow and, if an error occurs, reconnect the data and re-transmit.
Functions of this layer: Handshaking, Acknowledgement and Sequencing
Protocols of this layer: TCP, UDP, SPX

Session (Layer 5)

This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.
Layer 5 Session examples include NFS, NetBios names, RPC, SQL.

The Session Layer manages the sequence and flow of events that initiate and tear down network connections. At Layer 5, it is built to support multiple types of connections that can be created dynamically and run over individual networks.

Session Layer (Data)
This layer provides virtual agreement between two end communication devices.
Functions of this layer: Establishment, Management & Termination
The best example to explain this layer is telephone call in which first you established the connection, then exchange a message and finally terminate the session.
Protocols of this layer: SIP, NFS, SQL, ASP, RDBMS
The above three layers are known as the software layer.

Presentation (Layer 6)

This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.
Layer 6 Presentation examples include encryption, ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG, MIDI.

The Presentation layer is the simplest in function of any piece of the OSI model. At Layer 6, it handles syntax processing of message data such as format conversions and encryption / decryption needed to support the Application layer above it.

Presentation Layer (Data)
This layer facilitates the presentation of Data to the upper layer. Mainly, Provide Encoding Scheme & Encryption formation.
Protocols of this layer: JPEG, BMP, GIF, TIF, PNG, MP3, MIDI, ASCII & ANSI etc.

Application (Layer 7)

OSI Model, Layer 7, supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.
Layer 7 Application examples include WWW browsers, NFS, SNMP, Telnet, HTTP, FTP

The Application layer supplies network services to end-user applications. Network services are typically protocols that work with user's data. For example, in a Web browser application, the Application layer protocol HTTP packages the data needed to send and receive Web page content. This Layer 7 provides data to (and obtains data from) the Presentation layer.

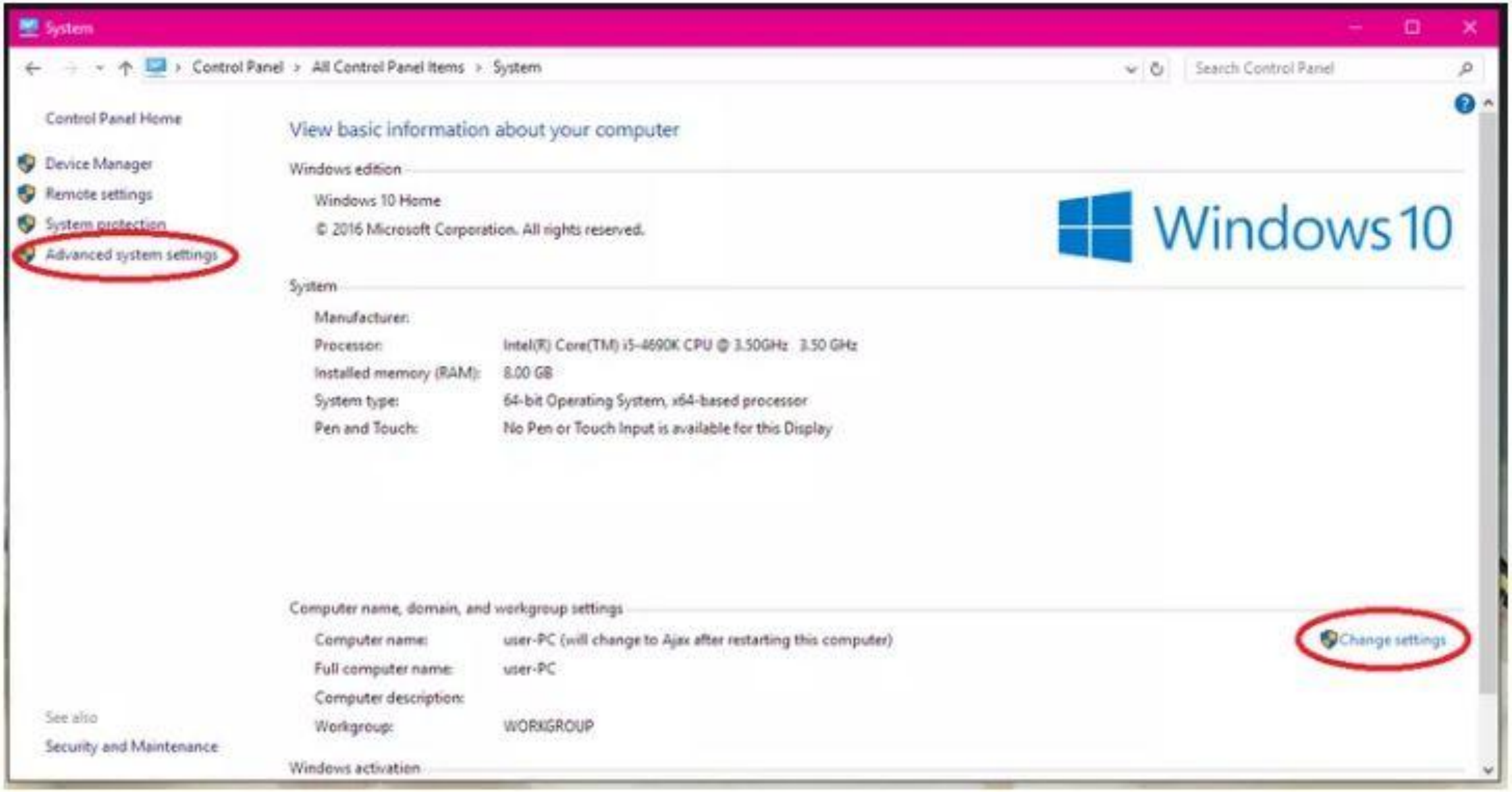
Application Layer (Data)
Application Layer provides Interface between users and machines.
Protocols of this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SNMP, DNS, Rlogin, SMTP, POP3, IMAP, and LDAP.

Lab # 1

Computer Name & Workgroup Change :

Step 1

Right-click on the Start button and click Control Panel.



View basic information about your computer

Windows edition

Windows 10 Home

© 2016 Microsoft Corporation. All rights reserved.

System

Manufacturer:	
Processor:	Intel(R) Core(TM) i5-4690K CPU @ 3.50GHz 3.50 GHz
Installed memory (RAM):	8.00 GB
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	No Pen or Touch Input is available for this Display

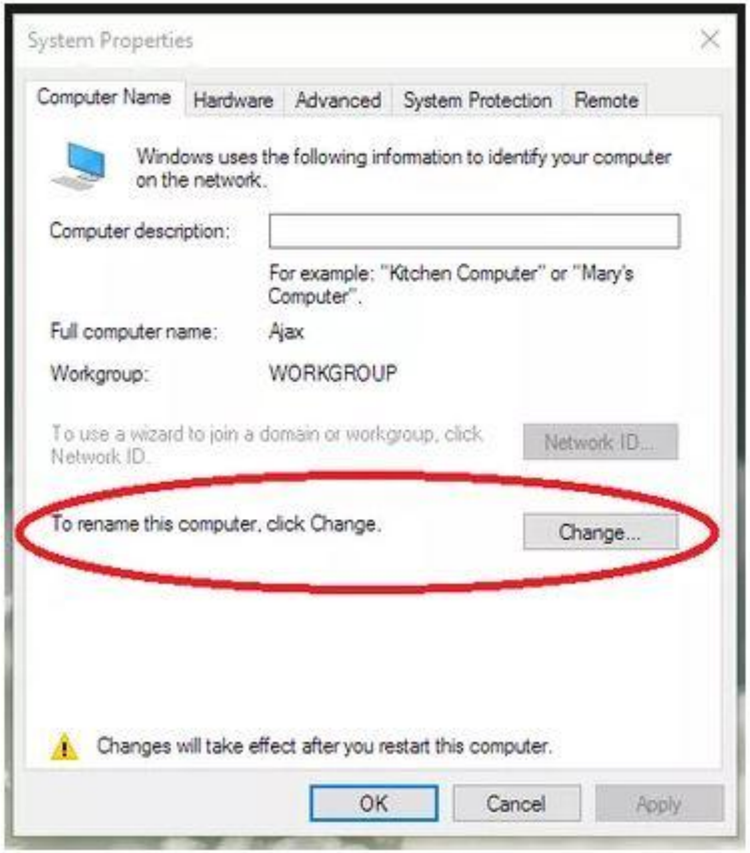
Computer name, domain, and workgroup settings

Computer name:	user-PC (will change to Ajax after restarting this computer)
Full computer name:	user-PC
Computer description:	
Workgroup:	WORKGROUP

Windows activation

Step 2

Navigate to System and either click Advanced system settings in the left-hand menu or click Change settings under Computer name, domain, and workgroup settings. This will open the System Properties window.



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: Ajax

Workgroup: WORKGROUP

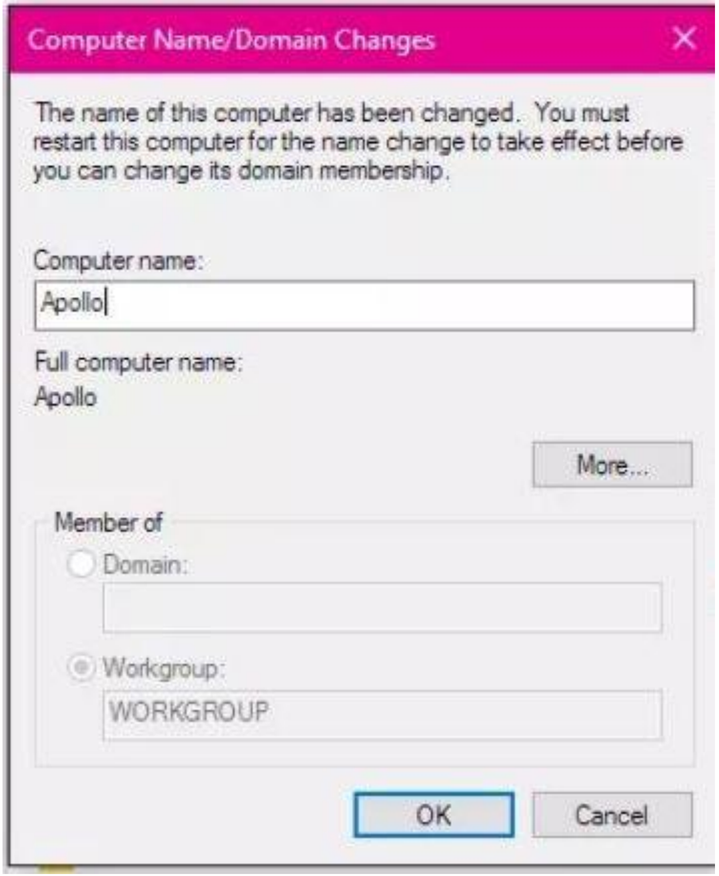
To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer, click Change.

Changes will take effect after you restart this computer.

Step 3

In the System Properties window, click the Computer Name tab. You'll see the message, "To rename this computer, click Change." Click Change...



The name of this computer has been changed. You must restart this computer for the name change to take effect before you can change its domain membership.

Computer name: Apollo

Full computer name: Apollo

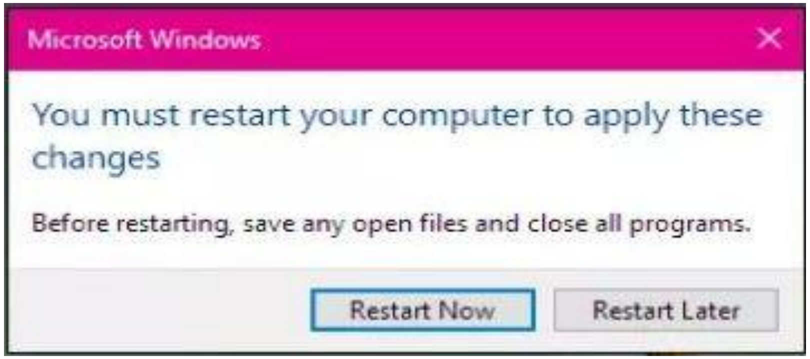
Member of

○ Domain:

● Workgroup: WORKGROUP

Step 4

Type the new name for your computer and click OK. A window will pop up telling you that you must restart your computer before the changes can be applied. Click OK. This will not restart your computer.



Microsoft Windows

You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

Lab # 2

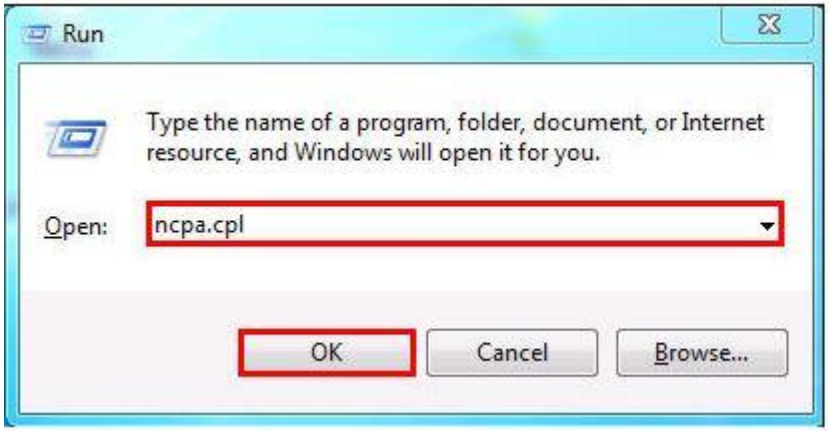
Configure TCP/IP Address :

Step 1

Click on windows key+ R key on the keyboard at the same time

Step 2

Type ncpa.cpl in the box, then press OK.



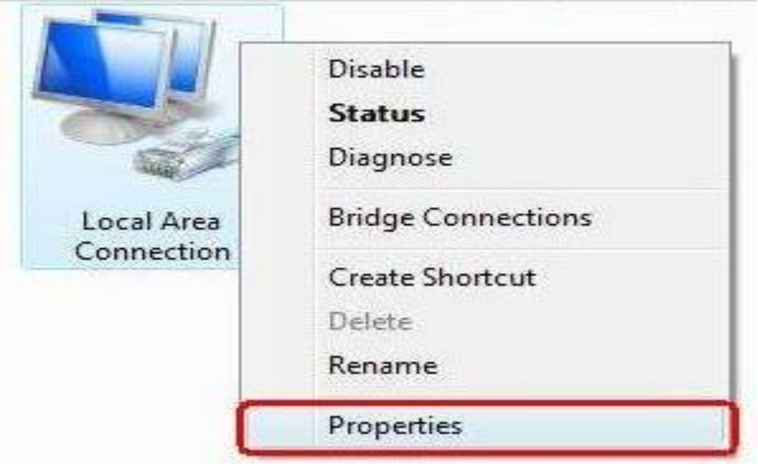
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: ncpa.cpl

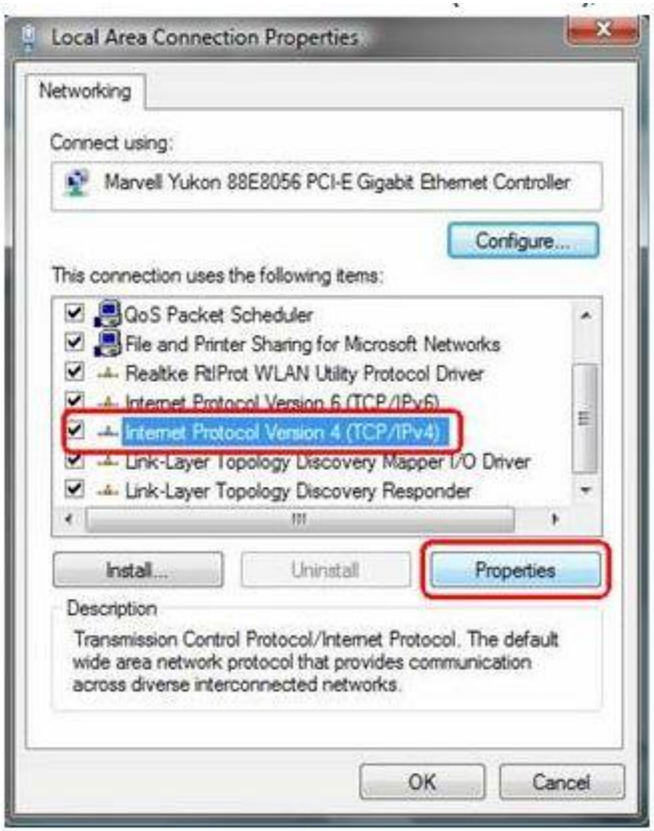
Step 3

Select the local area connection, right click it and select Properties.



Step 4

Select Internet Protocol Version 4(TCP/IPv4), double click it or click Properties.



Local Area Connection Properties

Networking

Connect using:

Marvell Yukon 88E8056 PCI-E Gigabit Ethernet Controller

Configure...

This connection uses the following items:

☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Realtke RtlProt WLAN Utility Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Install... Uninstall Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

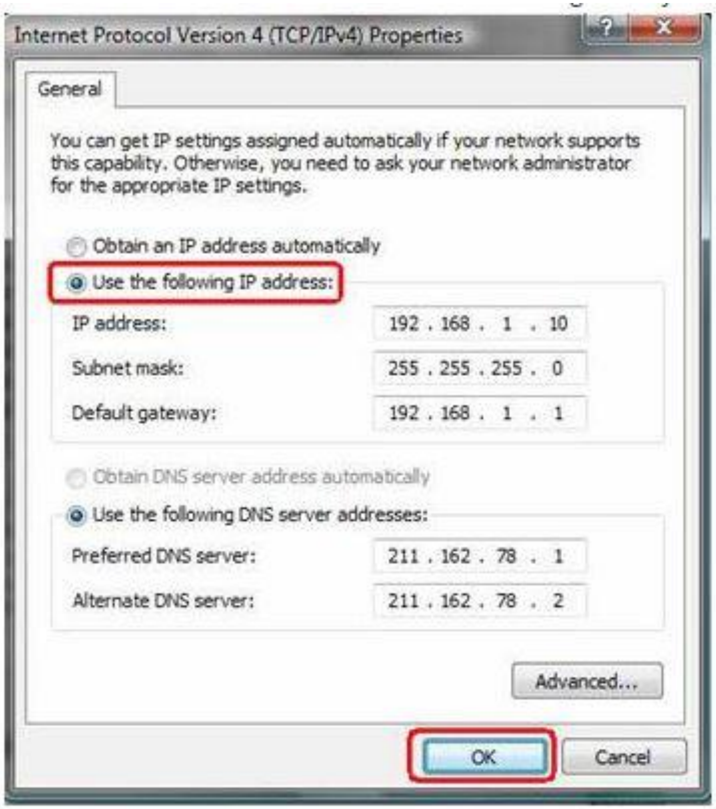
OK Cancel

Step 5

There are two ways to configure the TCP/IP Properties, Assigned by DHCP server automatically or manually.

1. Assigned by DHCP server

Select Obtain an IP address automatically and Obtain DNS server address automatically. If necessary, then click OK to save the settings.



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 . 10
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: 211 . 162 . 78 . 1
Alternate DNS server: 211 . 162 . 78 . 2

Advanced...

OK Cancel

Step 6

Click OK to save and apply your settings.

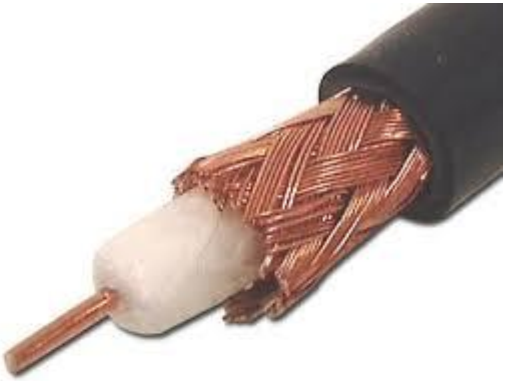
Network Cables :

Networking cables are networking hardware used to connect one network device to other network devices or to connect two or more computers to share printers, scanners etc. Different types of network cables, such as coaxial cable, twisted pair cables and optical fiber cable are used depending on the network's physical layer topology.

Coaxial Cables

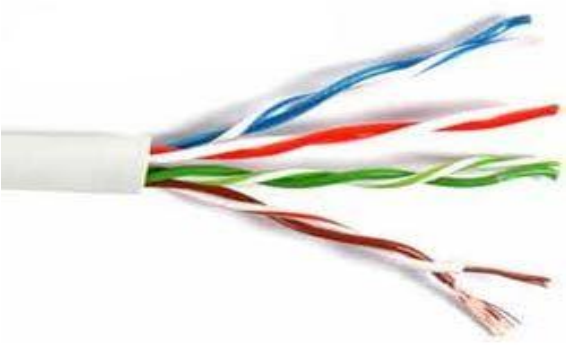
Invented in the 1880s, "coax" was best known as the kind of cable that connected television sets to home antennas. Coaxial cable is also a standard for 10 Mbps Ethernet cables.

When 10 Mbps Ethernet was most popular, during the 1980s and early 1990s, networks typically utilized one of two kinds of coax cable - thinnet (10BASE2 standard) or thicknet (10BASE5). These cables consist of an inner copper wire of varying thickness surrounded by insulation and another shielding. Their stiffness caused network administrators difficulty in installing and maintaining thinnet and thicknet.

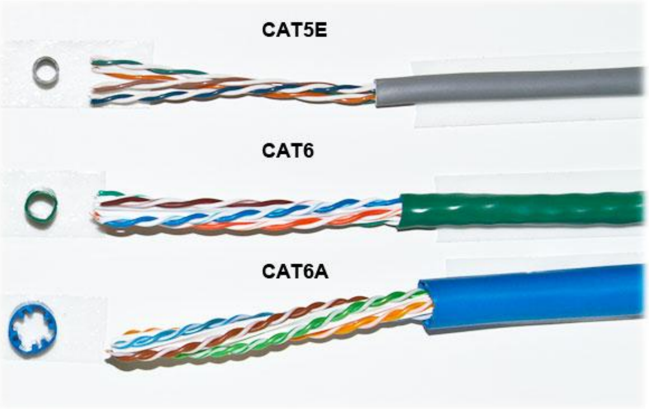


Twisted Pair Cables

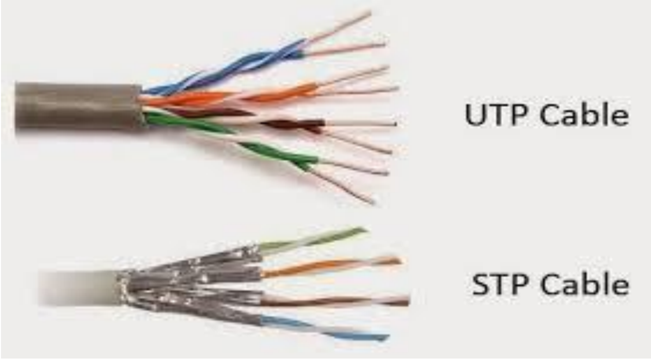
Twisted pair eventually emerged during the 1990s as the leading cabling standard for Ethernet, starting with 10 Mbps (10BASE-T, also known as Category 3 or Cat3), later followed by improved versions for 100 Mbps (100BASE-TX, Cat5, and Cat5e) and successively higher speeds up to 10 Gbps (10GBASE-T). Ethernet twisted pair cables contain up to eight (8) wires wound together in pairs to minimize electromagnetic interference.



Two primary types of twisted pair cable industry standards have been defined: Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP).

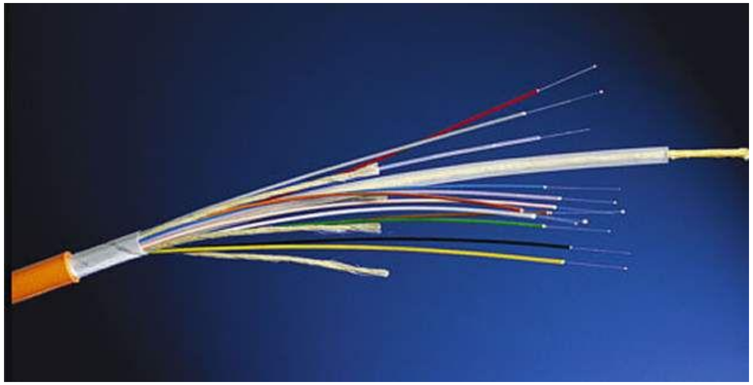


Modern Ethernet cables use UTP wiring due to its lower cost, while STP cabling can be found in some other types of networks such as Fiber Distributed Data Interface (FDDI).



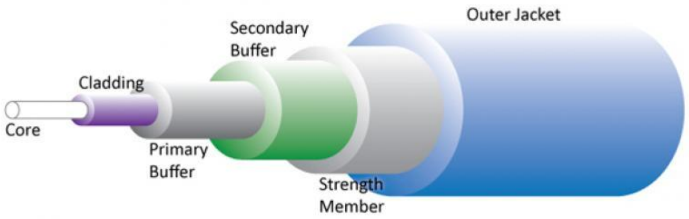
Optical Fiber Cables

Instead of insulated metal wires transmitting electrical signals, fiber optic network cables work using strands of glass and pulses of light.

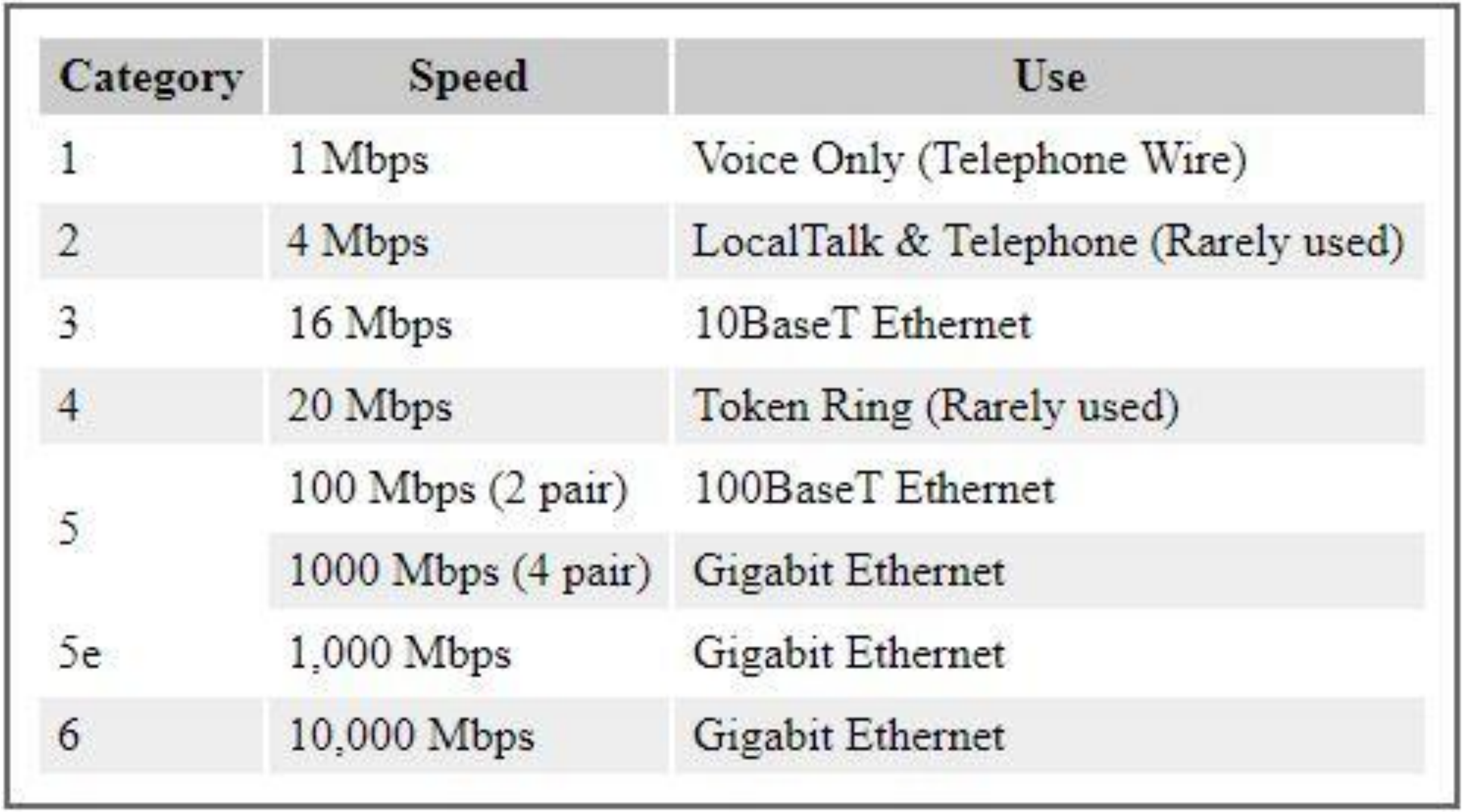


These network cables are bendable despite being made of glass. They have proven especially useful in wide area network (WAN) installations where long distance underground or outdoor cable runs are required and also in office buildings where a high volume of communication traffic is common.

Two primary types of fiber optic cable industry standards are defined – single-mode (100BaseBX standard) and multimode (100BaseSX standard). Long-distance telecommunications networks more commonly use single-mode for its relatively higher bandwidth capacity, while local networks typically use multimode instead due to its lower cost.



Categories of Unshielded Twisted Pair

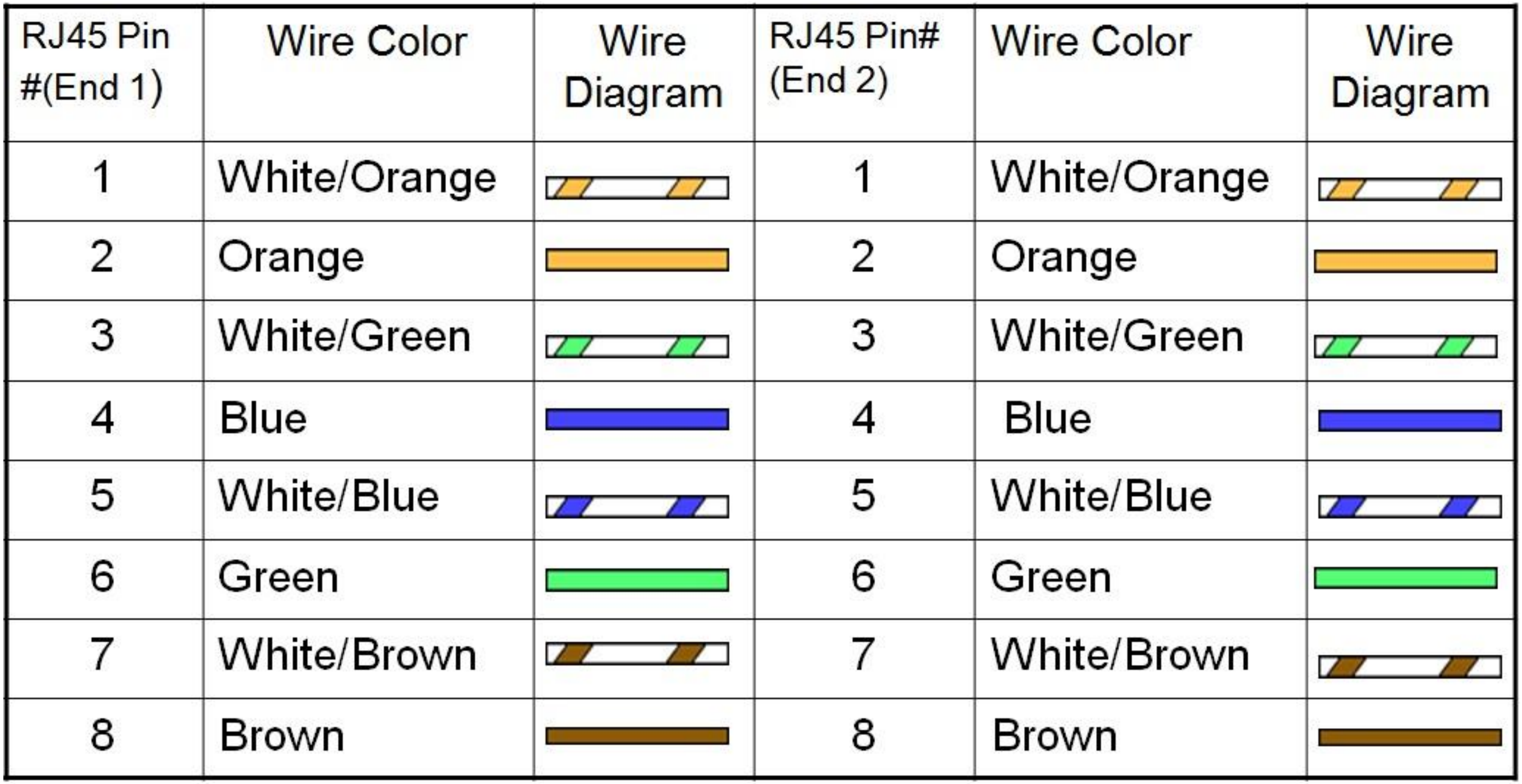


Category	Speed	Use
1	1 Mbps	Voice Only (Telephone Wire)
2	4 Mbps	LocalTalk & Telephone (Rarely used)
3	16 Mbps	10BaseT Ethernet
4	20 Mbps	Token Ring (Rarely used)
5	100 Mbps (2 pair)	100BaseT Ethernet
	1000 Mbps (4 pair)	Gigabit Ethernet
5e	1,000 Mbps	Gigabit Ethernet
6	10,000 Mbps	Gigabit Ethernet

Lab # 3

Straight Cable Coding :

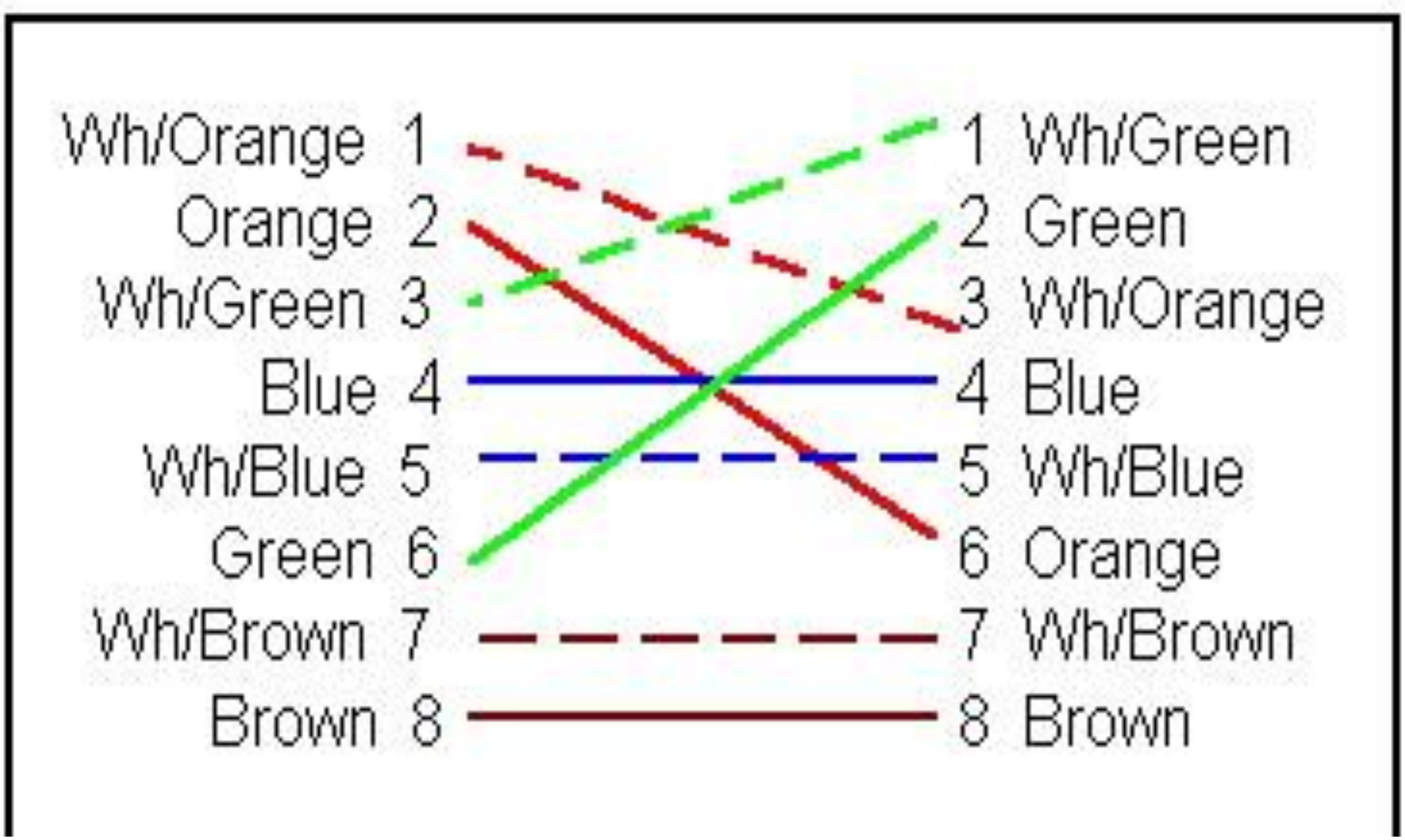
T568A **T568B**



RJ45 Pin #(End 1)	Wire Color	Wire Diagram	RJ45 Pin# (End 2)	Wire Color	Wire Diagram
1	White/Orange	⬜🟧	1	White/Orange	⬜🟧
2	Orange	🟧	2	Orange	🟧
3	White/Green	⬜🟩	3	White/Green	⬜🟩
4	Blue	🟦	4	Blue	🟦
5	White/Blue	⬜🟦	5	White/Blue	⬜🟦
6	Green	🟩	6	Green	🟩
7	White/Brown	⬜🟫	7	White/Brown	⬜🟫
8	Brown	🟫	8	Brown	🟫

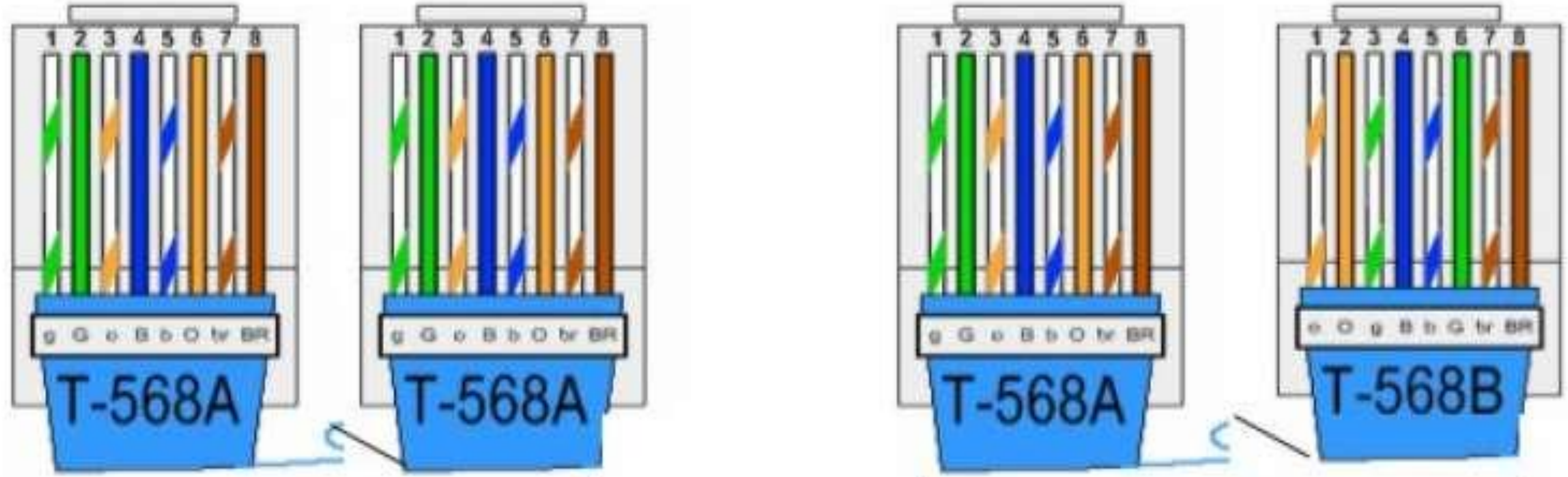
Lab # 4

Cross Cable Coding :



Cable Use :

Ethernet Cable Color Coding



Uses of Straight-Thru Cable

1. To Connect PC to Switch, Switch to Router, and Router to PC.

Uses of Cross-Over Cable

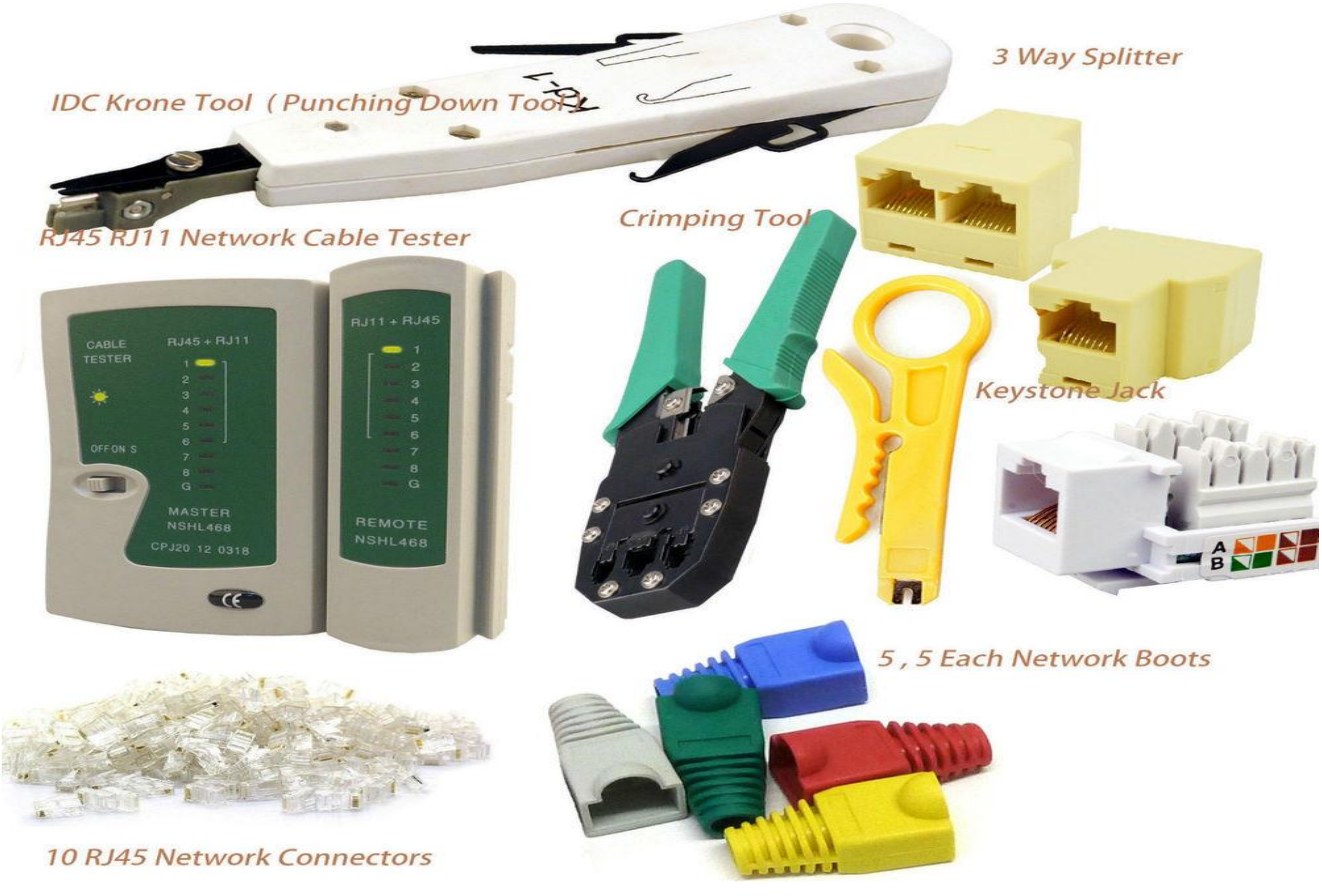
1. To Connect PC to PC, Switch to switch, and Router to router.

RJ 45
Connector

BNC
Connector

Fiber Optic
Cable

Tools :


IDC Krone Tool (Punching Down Tool)
KD-1
3 Way Splitter
RJ45 RJ11 Network Cable Tester
CABLE TESTER
RJ45 + RJ11
OFF ON S
MASTER
NSHL468
CPJ20 12 0318
RJ11 + RJ45
REMOTE
NSHL468
Crimping Tool
Keystone Jack
5 , 5 Each Network Boots
10 RJ45 Network Connectors

Collision Domain :

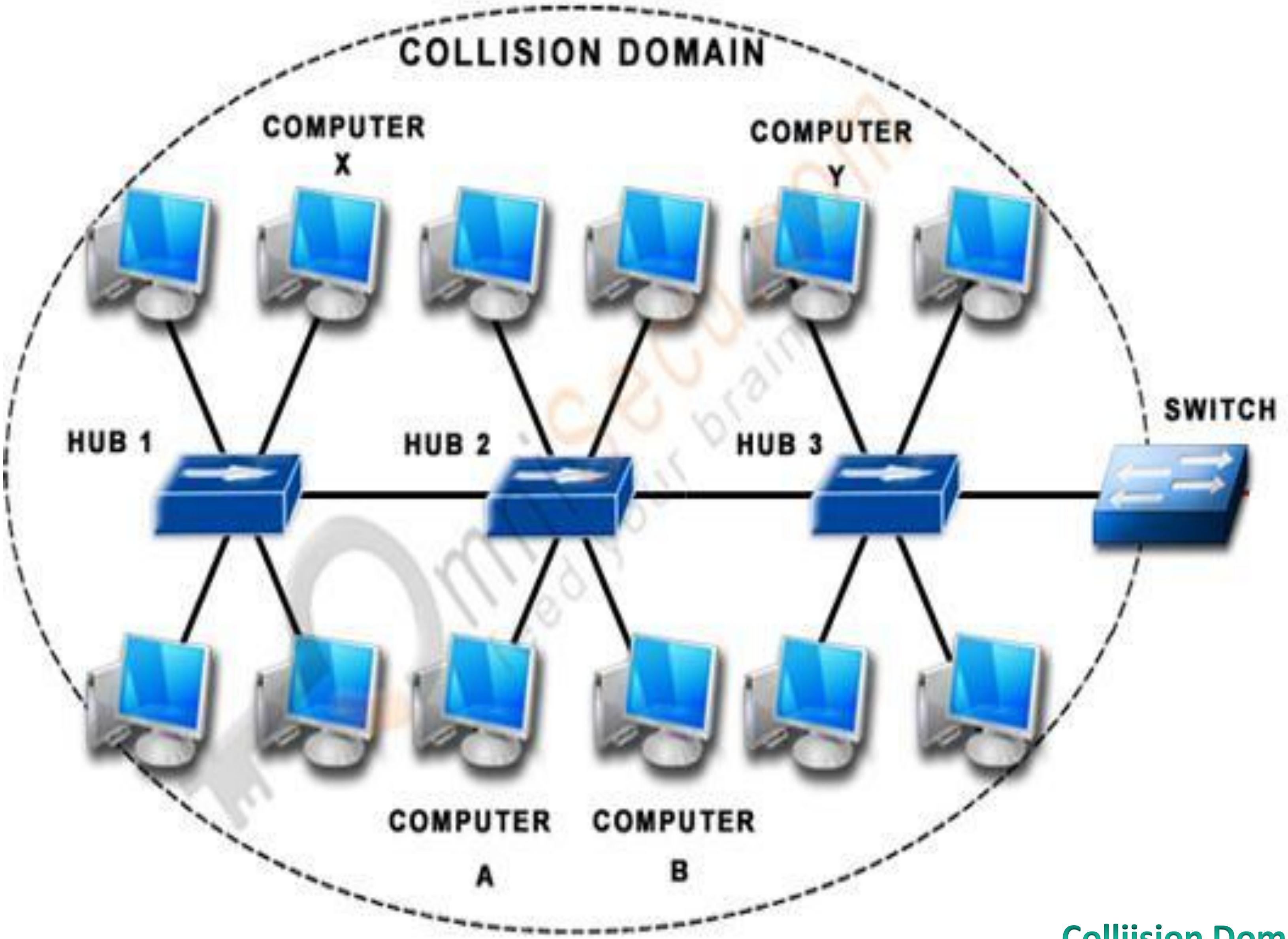
A collision domain is a network segment connected by a shared medium or through repeaters where data packets may collide with one another while being sent. The collision domain applies particularly in wireless networks, but also affected early versions of Ethernet. A network collision occurs when more than one device attempts to send a packet on a network segment at the same time. Members of a collision domain may be involved in collisions with one another. Devices outside the collision domain do not have collisions with those inside.

Only one device in the collision domain may transmit at any one time, and the other devices in the domain listen to the network and refrain from transmitting while others are already transmitting in order to avoid collisions. Because only one device may be transmitting at any one time, total network bandwidth is shared among all devices on the collision domain. Collisions also decrease network efficiency on a collision domain as collisions require devices to abort transmission and retransmit at a later time.

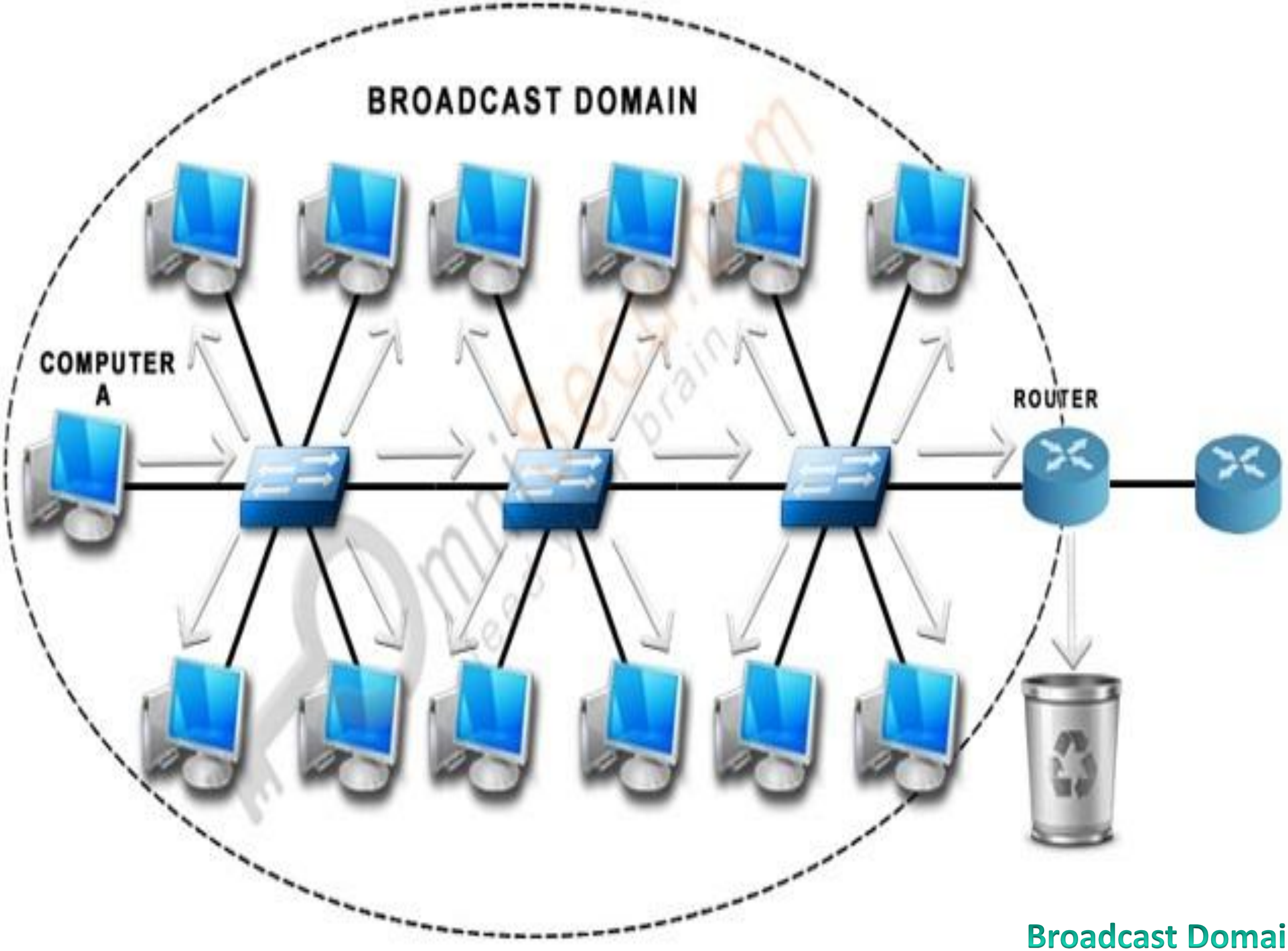
In a half duplex Ethernet network, a collision is the result of two devices on the same Ethernet network attempting to transmit data at exactly the same time. The network detects the "collision" of the two transmitted packets and discards them both. Collisions are a natural occurrence on Ethernets. Ethernet uses Carrier Sense Multiple Access/ Collision Detect (CSMA/CD) as its method of allowing devices to "take turns" using the signal carrier line. When a device wants to transmit, it checks the signal level of the line to determine whether someone else is already using it. If it is already in use, the device waits and retries, perhaps in a few seconds. If it isn't in use, the device transmits. However, two devices can transmit at the same time in which case a collision occurs and both devices detect it. Each device then waits a random amount of time and retries until successful in getting the transmission sent.

Broadcast Domain :

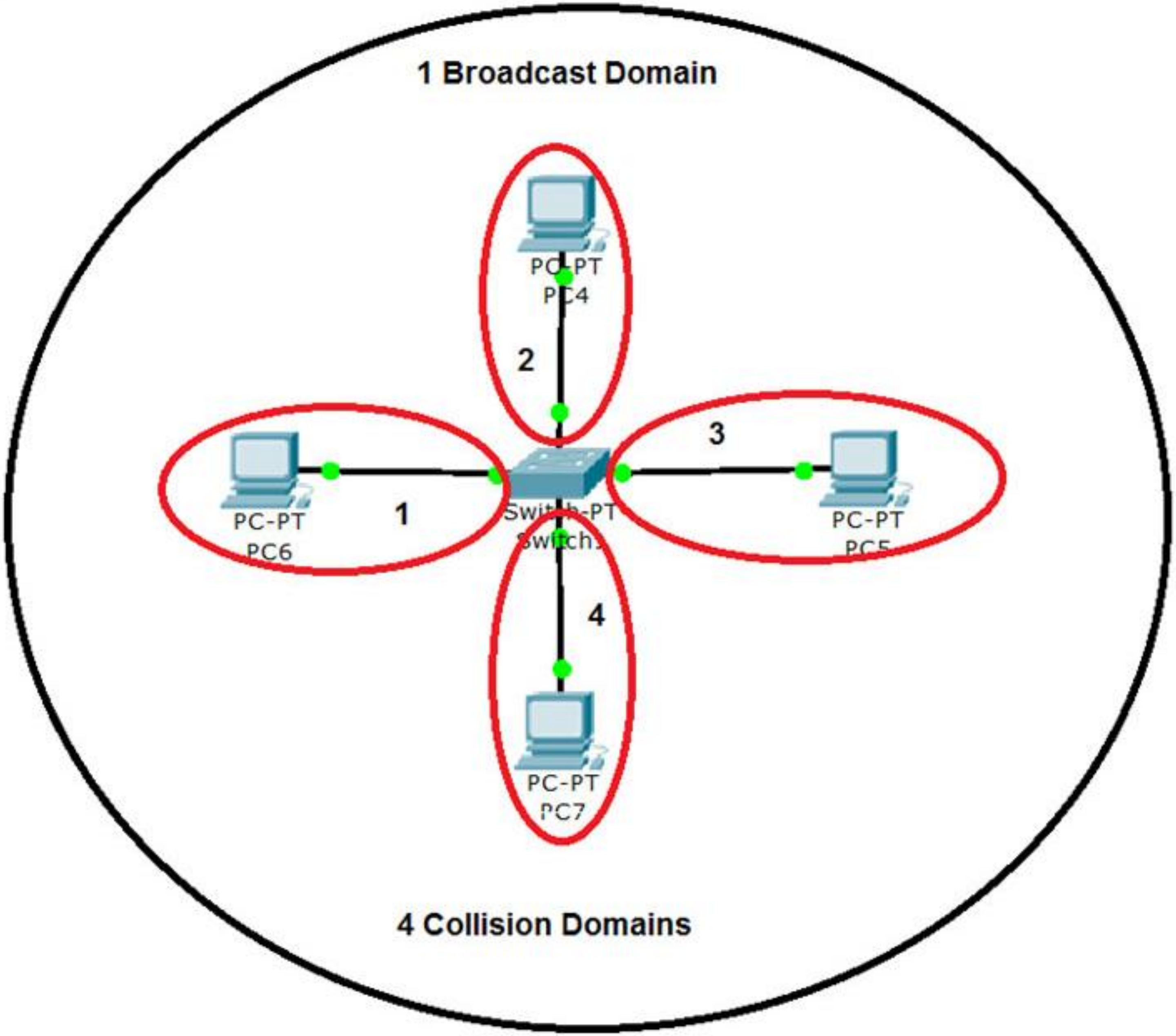
A broadcast domain is a logical division of a computer network, in which all nodes can reach each other by broadcast at the data link layer. A broadcast domain can be within the same LAN segment or it can be bridged to other LAN segments. In terms of current popular technologies: Any computer connected to the same Ethernet repeater or switch is a member of the same broadcast domain. Further, any computer connected to the same set of inter-connected switches/repeaters is a member of the same broadcast domain. Routers and other higher-layer devices form boundaries between broadcast domains. This is as compared to a collision domain, which would be all nodes on the same set of inter-connected repeaters, divided by switches and learning bridges. Collision domains are generally smaller than, and contained within, broadcast domains. A broadcast domain is a logical part or division of a computer network. In a broadcast domain, all the nodes can be reached via broadcast at the data link layer. Broadcast domains are located within a network or multi-network segment. Multi-network segments require a bridge, such as the networking device. A broadcast domain member can also be any device or computer that is directly connected to the same switch or repeater. Networking devices, such as routers, are used to separate the boundaries of broadcast domains. A broadcast domain provides high-level communication and reliability via a simple Ethernet connection. An assigned broadcast domain or destination receives addressed and transmitted data frames, which are detected by each node. However, data frames are only received by addressed nodes. The best broadcast domain example is the virtual local area network (VLAN) in which multiple computers establish a broadcast domain via a virtual connection, they are not physically connected. A broadcast domain provides fast and reliable communication for offices in different locations. One broadcast domain disadvantage is its tendency to drop Web data signals after reaching network router interface borders. Additionally, issues occur when a router links two or more broadcast domain networks, as described in the following example: Let networks A and B be connected via a router. Network A, which has a Dynamic Host Configuration Protocol (DHCP) server, broadcasts Internet Protocol (IP) addresses to all attached computers. The DHCP service also tries to broadcast IP addresses to all computers attached to network B. However, the router drops incoming messages and network B’s computers do not get configured properly. Such issues occur in broadcast domains. Current routers are manufactured with enhanced features, such as the no DHCP request blocking.

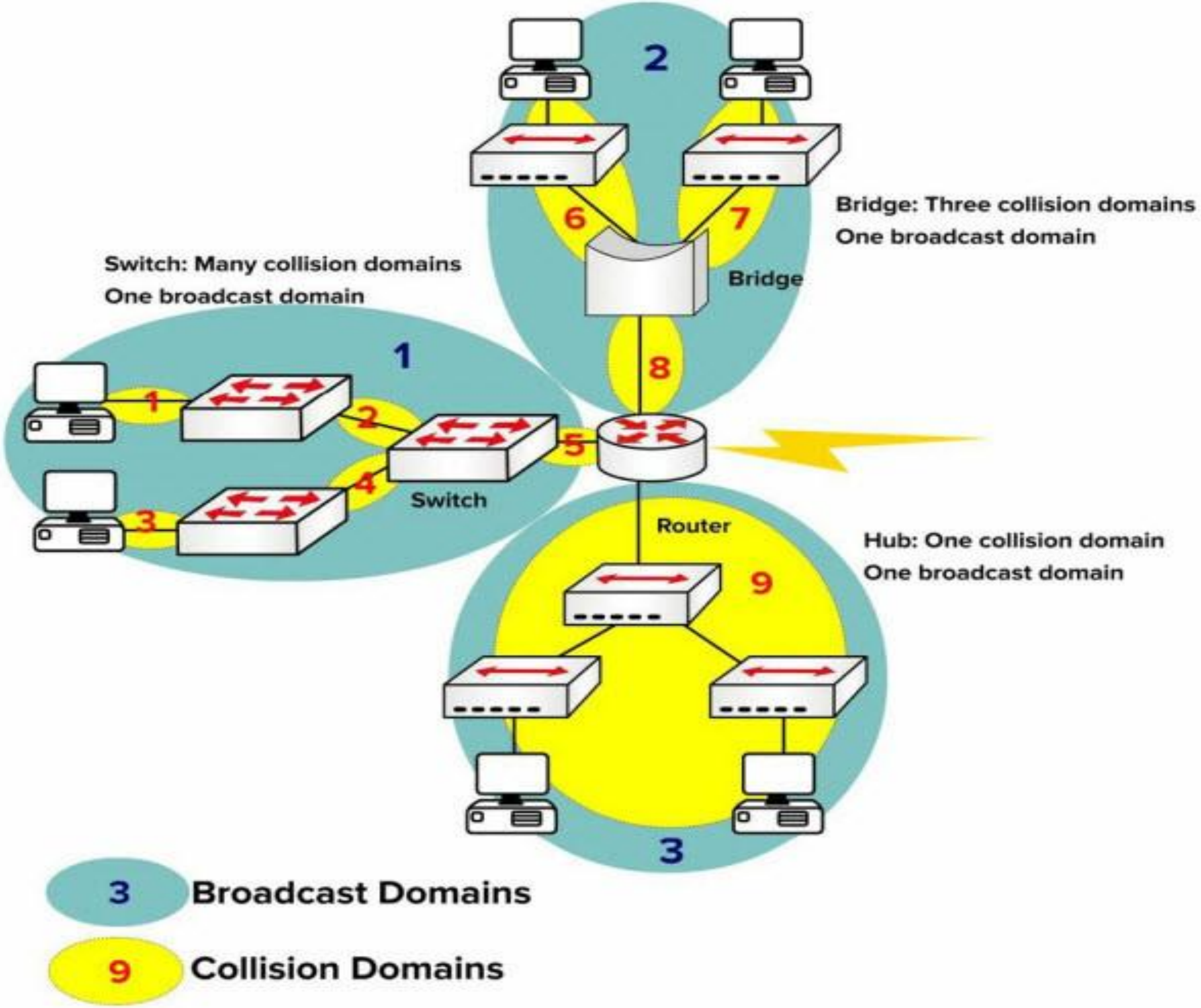


Colliision Domain



Broadcast Domain


1 Broadcast Domain
PC-PT
PC4
2
3
PC-PT
PC6
1
Switch-PT
Switch1
PC-PT
PC5
4
PC-PT
PC7
4 Collision Domains


2
6
7
Bridge: Three collision domains
One broadcast domain
Switch: Many collision domains
One broadcast domain
Bridge
1
8
1
2
5
4
3
Switch
Router
Hub: One collision domain
One broadcast domain
9
3
3 Broadcast Domains
9 Collision Domains

Transmission Mode :

Simplex, Half Duplex and Full Duplex

Simplex, half duplex and full duplex are three kinds of communication channels in telecommunications and computer networking. These communication channels provide pathways to convey information. A communication channel can be either a physical transmission medium or a logical connection over a multiplexed medium. The physical transmission medium refers to the material substance that can propagate energy waves, such as wires in data communication. And the logical connection usually refers to the circuit switched connection or packet-mode virtual circuit connection, such as a radio channel. Thanks to the help of communication channels, information can be transmitted without obstruction. A brief introduction about three communication channel types will be given in this article.

Three Types of Communication Channel -

1) Simplex

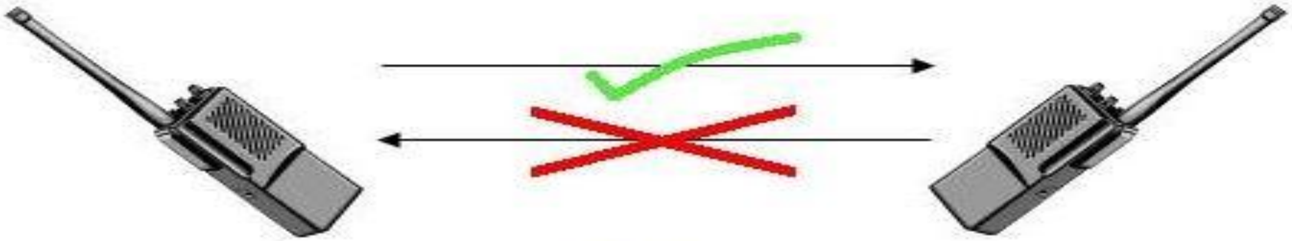
A simplex communication channel only sends information in one direction. For example, a radio station usually sends signals to the audience but never receives signals from them, thus a radio station is a simplex channel. It is also common to use simplex channel in fiber optic communication. One strand is used for transmitting signals and the other is for receiving signals. But this might not be obvious because the pair of fiber strands are often combined to one cable. The good part of simplex mode is that its entire bandwidth can be used during the transmission.

2) Half duplex

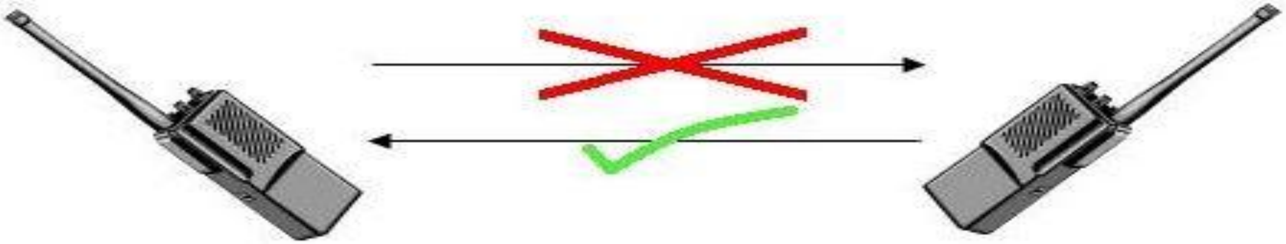
In half duplex mode, data can be transmitted in both directions on a signal carrier except not at the same time. At a certain point, it is actually a simplex channel whose transmission direction can be switched. Walkie-talkie is a typical half duplex device. It has a “push-to-talk” button which can be used to turn on the transmitter but turn off the receiver. Therefore, once you push the button, you cannot hear the person you are talking to but your partner can hear you. An advantage of half-duplex is that the single track is cheaper than the double tracks. Half-duplex is used to describe communication where only... one side can talk at a time. Once one side has finished transmitting its data, the other side can respond. Only one node can talk at a time. If both try to talk at the same time, a collision will occur on the network. As you can understand, this method of communication is not very efficient and requires more time to send/receive larger amounts of data. Older networks used to work in half-duplex mode, due to the constraints of the network medium (coax cable) and hardware equipment (hubs). In half-duplex systems, the transmission and reception of information must happen alternately. While one point is transmitting, the other must only receive. Walkie-talkie radio communication is a half-duplex system, this is characterised by saying “over” at the end of a transmission to signify that the party is ready to receive information.

3) Full duplex

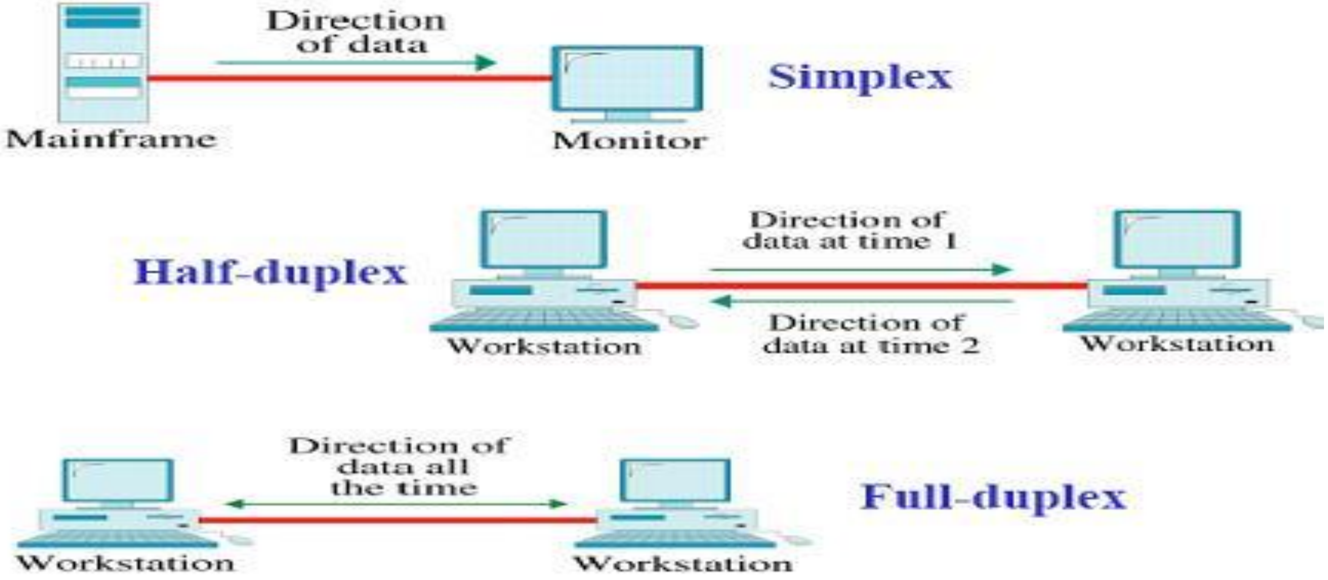
A full duplex communication channel is able to transmit data in both directions on a signal carrier at the same time. It is constructed as a pair of simplex links that allows bidirectional simultaneous transmission. Take telephone as an example, people at both ends of a call can speak and be heard by each other at the same time because there are two communication paths between them. Thus, using the full duplex mode can greatly increase the efficiency of communication. On the other hand, full-duplex is used to describe communication where both sides are able to send and receive data at the same time. In these cases, there is no danger of a collision and therefore the transfer of data is completed much faster. Today, all networks make use of switches (rather than hubs) and UTP Ethernet cabling, which allow full-duplex communication between all connected hosts. Full-duplex communication between two components means that both can transmit and receive information between each other simultaneously. Telephones are full-duplex systems so both parties on the phone can talk and listen at the same time.



OR



Transmission Mode



Direction of data

Mainframe

Monitor

Simplex

Half-duplex

Direction of data at time 1

Direction of data at time 2

Workstation

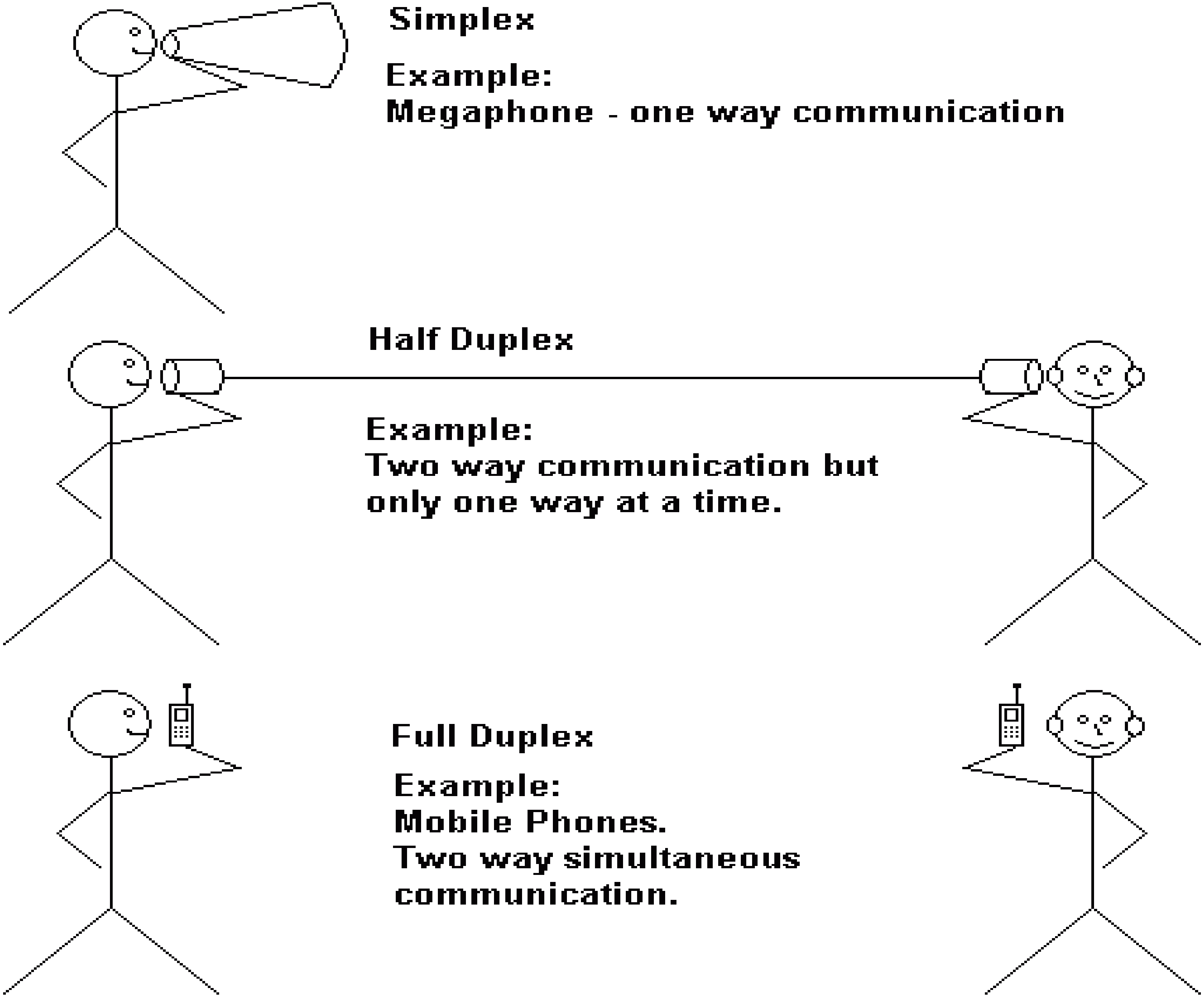
Workstation

Direction of data all the time

Workstation

Workstation

Full-duplex



Simplex

Example:
Megaphone - one way communication

Half Duplex

Example:
Two way communication but
only one way at a time.

Full Duplex

Example:
Mobile Phones.
Two way simultaneous
communication.

TCP/IP Layers :

TCP/IP protocols map to a four-layer conceptual model known as the DARPA model , named after the U.S. government agency that initially developed TCP/IP. The four layers of the DARPA model are: Application, Transport, Internet, and Network Interface. Each layer in the DARPA model corresponds to one or more layers of the seven-layer Open Systems Interconnection (OSI) model. Each layer of the TCP/IP has a particular function to perform and each layer is completely separate from the layer(s) next to it. The communication process that takes place, at its simplest between two computers, is that the data moves from layer 4 to 3 to 2 then to 1 and the information sent arrives at the second system and moves from 1 to 2 to 3 and then finally to layer 4.

Application Layer

The application layer is concerned with providing network services to applications. There are many application network processes and protocols that work at this layer, including HyperText Transfer Protocol (HTTP), Simple Mail Transport Protocol (SMTP) and File Transfer Protocol (FTP). At this layer sockets and port numbers are used to differentiate the path and sessions which applications operate. Most application layer protocols, especially on the server side, have specially allocated port numbers, e.g. HTTP = 80 and SMTP = 25, and FTP = 20 (Control), 21 (Data).

Transport Layer

This layer is concerned with the transmission of the data. The two main protocols that operate at this layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). TCP is regarded as being the reliable transmission protocol and it guarantees that the proper data transfer will take place. UDP is not as complex as TCP and as such is not designed to be reliable or guarantee data delivery. UDP is generally thought of as being a best effort data delivery, i.e. once the data is sent, UDP will not carry out any checks to see that it has safely arrived.

The Internet Layer

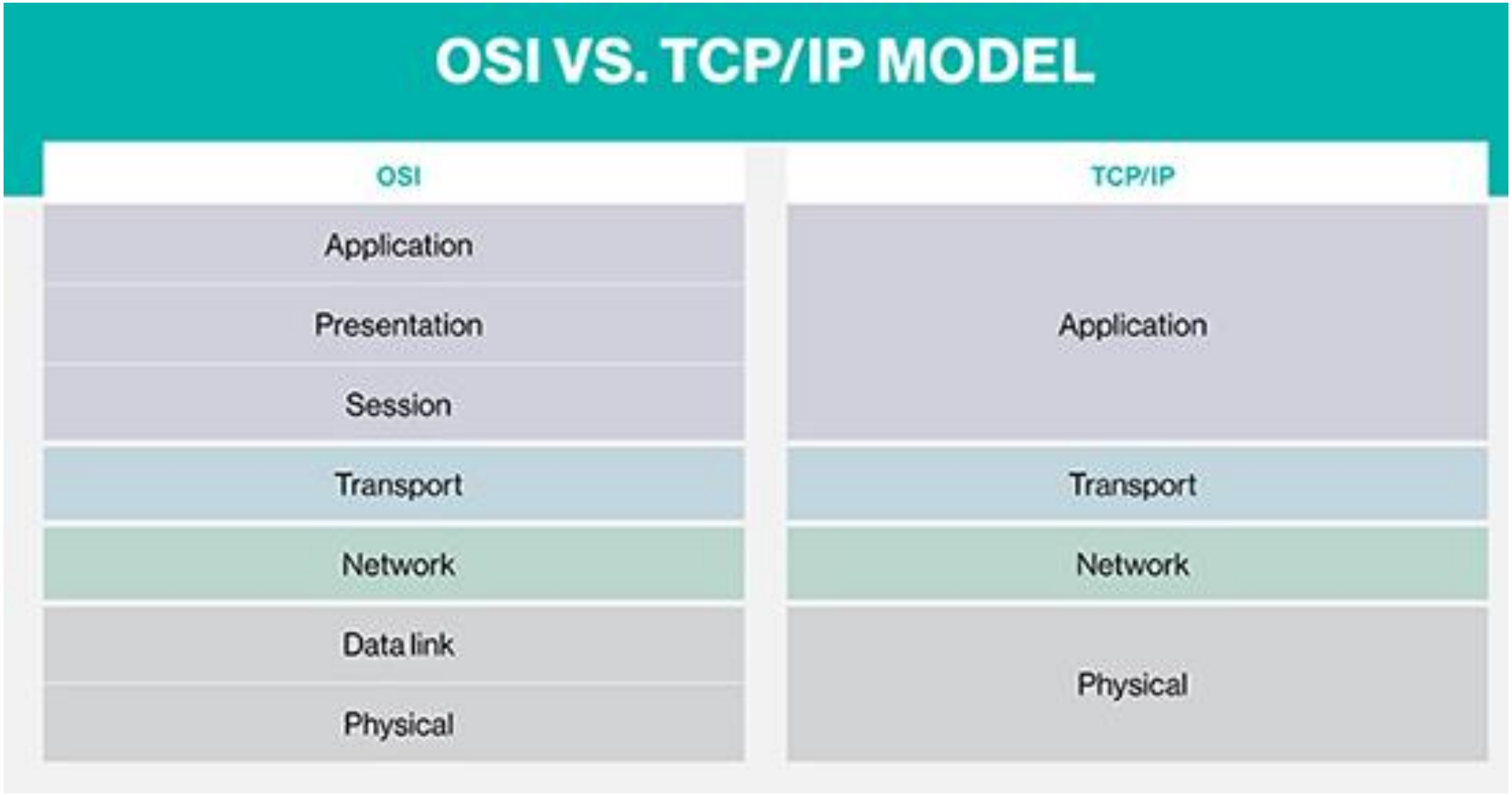
This is the layer that contains the packet construct that will be transmitted. This takes the form of the Internet Protocol (IP) which describes a packet that contains a source IP Address, destination IP Address and the actual data to be delivered.

Network Access Layer

This is the lowest level of the TCP/IP protocol stack and functions carried out here include encapsulation of IP packets into frames for transmission, mapping IP addresses to physical hardware addresses (MAC Addresses) and the use of protocols for the physical transmission of data.

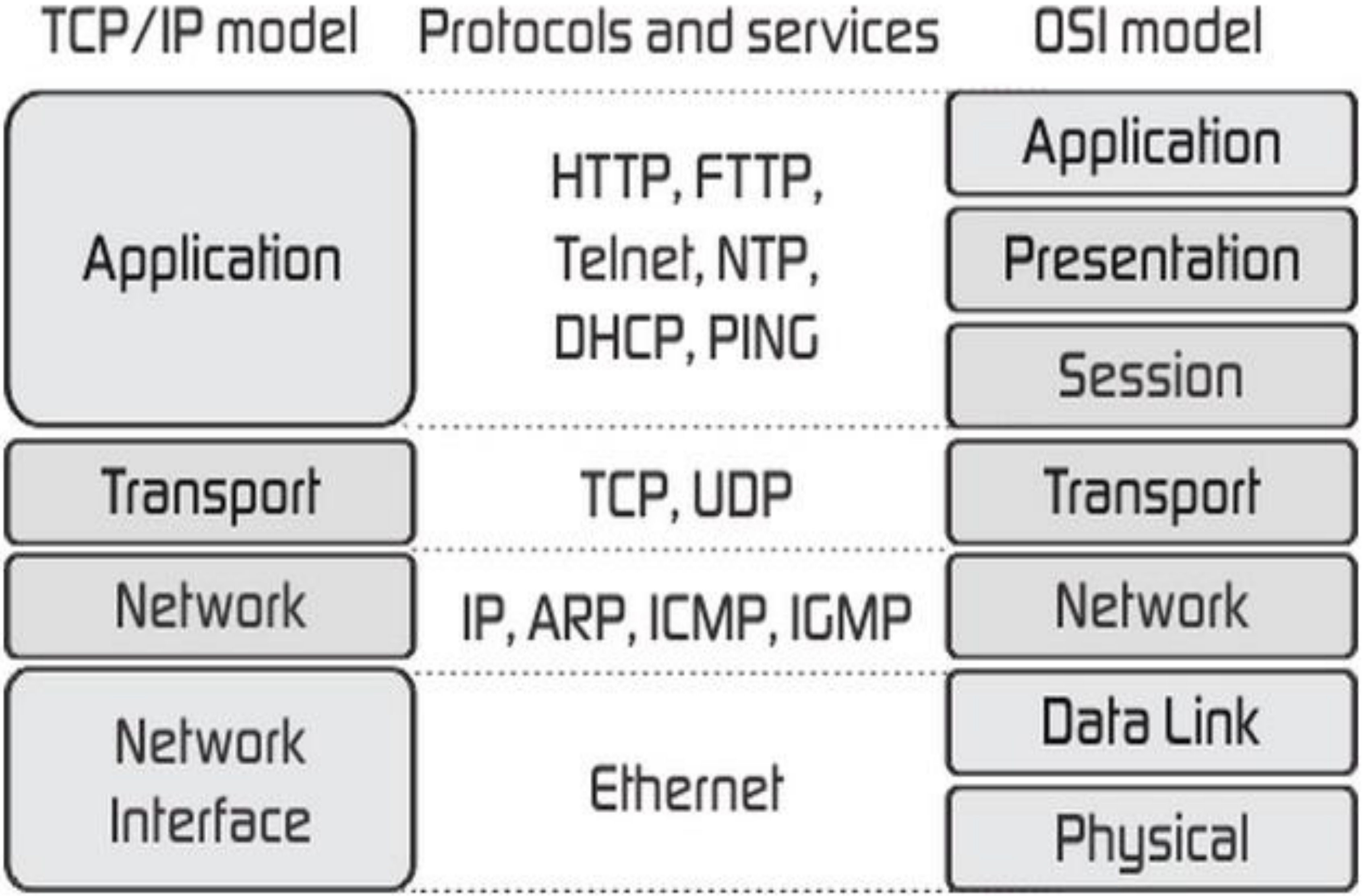
Note: TCP/IP is actually a suite of protocols sometimes referred to as the Internet Protocol Suite.

TCP/IP Protocol Architecture :

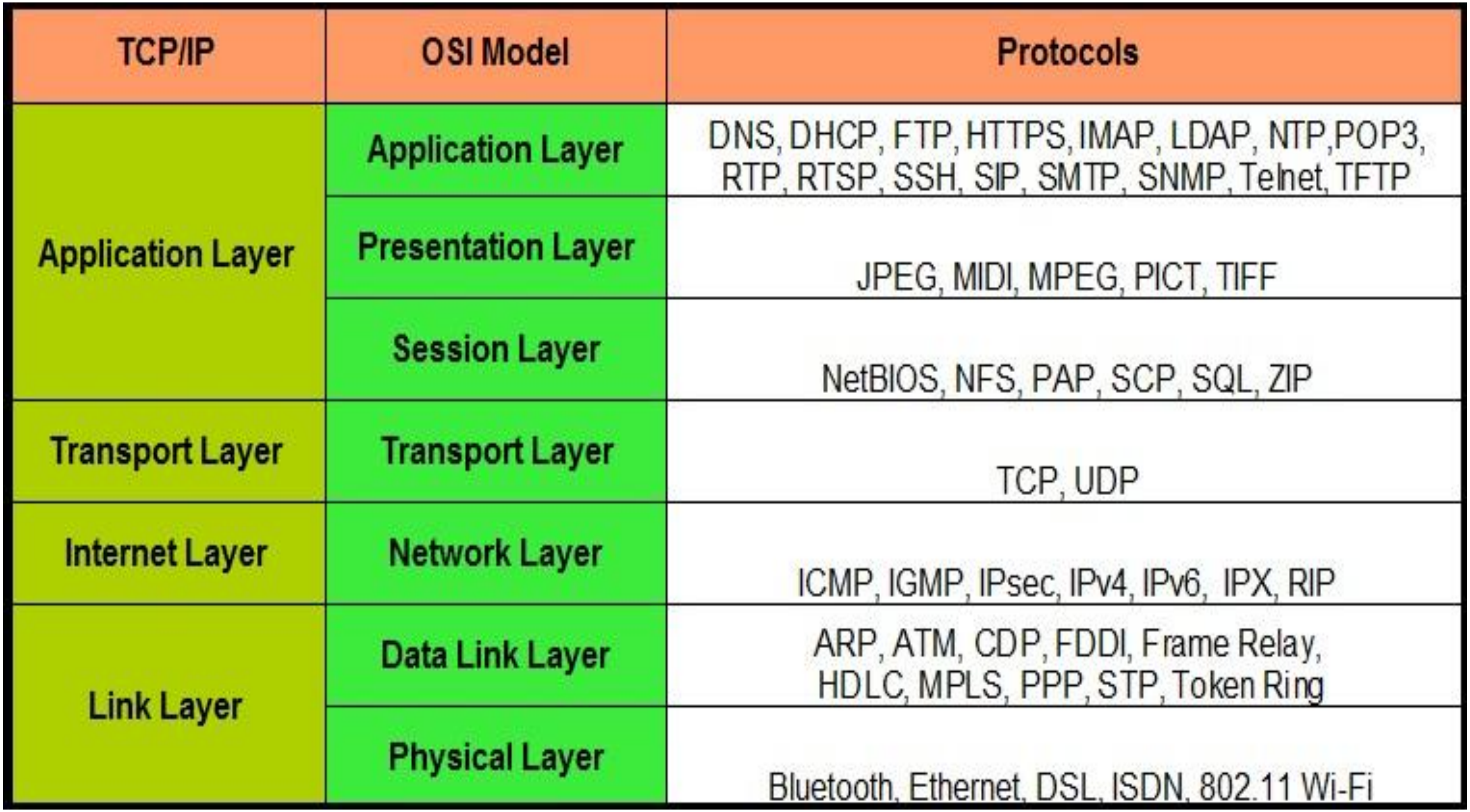


OSI VS. TCP/IP MODEL

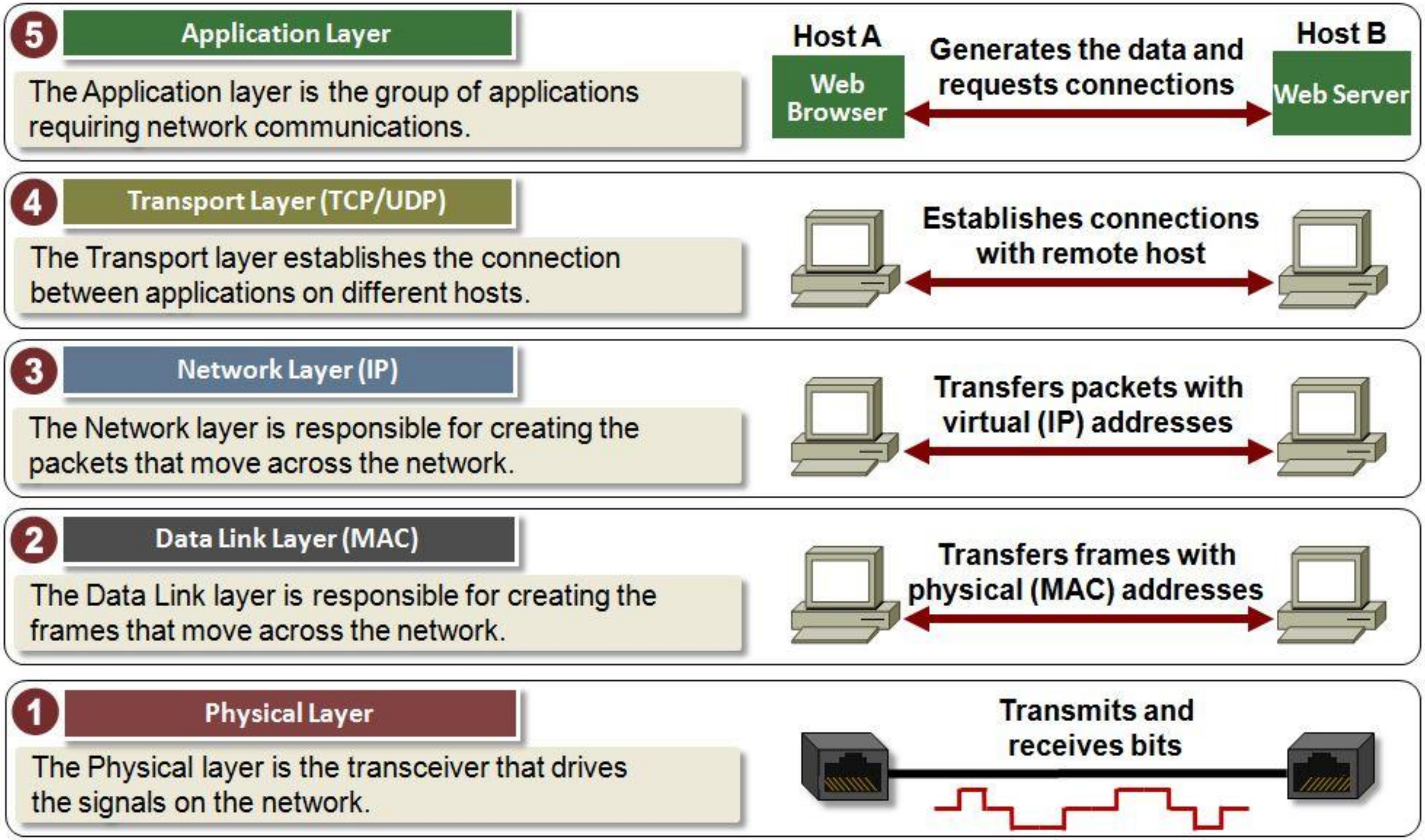
OSI	TCP/IP
Application	Application
Presentation	
Session	
Transport	Transport
Network	Network
Data link	Physical
Physical	



TCP/IP model	Protocols and services	OSI model
Application	HTTP, FTTP, Telnet, NTP, DHCP, PING	Application
		Presentation
		Session
Transport	TCP, UDP	Transport
Network	IP, ARP, ICMP, IGMP	Network
Network Interface	Ethernet	Data Link
		Physical



TCP/IP	OSI Model	Protocols
Application Layer	Application Layer	DNS, DHCP, FTP, HTTPS, IMAP, LDAP, NTP,POP3, RTP, RTSP, SSH, SIP, SMTP, SNMP, Telnet, TFTP
	Presentation Layer	JPEG, MIDI, MPEG, PICT, TIFF
	Session Layer	NetBIOS, NFS, PAP, SCP, SQL, ZIP
Transport Layer	Transport Layer	TCP, UDP
Internet Layer	Network Layer	ICMP, IGMP, IPsec, IPv4, IPv6, IPX, RIP
Link Layer	Data Link Layer	ARP, ATM, CDP, FDDI, Frame Relay, HDLC, MPLS, PPP, STP, Token Ring
	Physical Layer	Bluetooth, Ethernet, DSL, ISDN, 802.11 Wi-Fi



5 Application Layer

The Application layer is the group of applications requiring network communications.

Host A

Web Browser

Generates the data and requests connections

Host B

Web Server

4 Transport Layer (TCP/UDP)

The Transport layer establishes the connection between applications on different hosts.

Establishes connections with remote host

3 Network Layer (IP)

The Network layer is responsible for creating the packets that move across the network.

Transfers packets with virtual (IP) addresses

2 Data Link Layer (MAC)

The Data Link layer is responsible for creating the frames that move across the network.

Transfers frames with physical (MAC) addresses

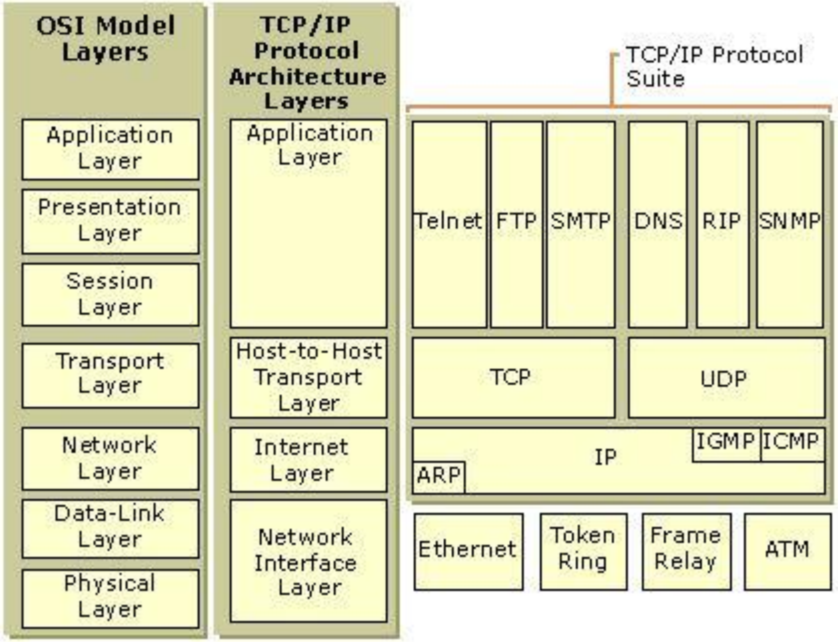
1 Physical Layer

The Physical layer is the transceiver that drives the signals on the network.

Transmits and receives bits

COMPARISON

OSI Model	TCP/IP Model
OSI stands for Open System Interconnection because it allows any two different systems to communicate regardless of their architecture.	TP/IP stands for Transmission Control Protocol/Internet Protocol. It is named after these protocols, being part of this model.
OSI model has seven layers.	TCP/IP has four layers..
This model provides clear distinction between services, interfaces and protocols	It does not clearly distinguish between services, interfaces & protocols.
In this model, Protocols do not fit well into the model.	TCP and IP protocols fit well in the model.



TCP/IP Address :

Short for Transmission Control Protocol/Internet Protocol, TCP/IP is a set of rules (protocols) governing communications among all computers on the Internet. More specifically, TCP/IP dictates how information should be packaged (turned into bundles of information called packets), sent, and received, as well as how to get to its destination. TCP/IP was developed in 1978 and driven by Bob Kahn and Vint Cerf.

IP addresses: Networks and hosts
An IP address is a 32-bit number that uniquely identifies a host (computer or other device, such as a printer or router) on a TCP/IP network.

IP addresses are normally expressed in dotted-decimal format, with four numbers separated by periods, such as 192.168.123.132. To understand how subnet masks are used to distinguish between hosts, networks, and sub networks, examine an IP address in binary notation.

For example, the dotted-decimal IP address 192.168.123.132 is (in binary notation) the 32 bit number 110000000101000111101110000100. This number may be hard to make sense of, so divide it into four parts of eight binary digits.

These eight bit sections are known as octets. The example IP address, then, becomes 11000000.10101000.01111011.10000100. This number only makes a little more sense, so for most uses, convert the binary address into dotted-decimal format (192.168.123.132). The decimal numbers separated by periods are the octets converted from binary to decimal notation.

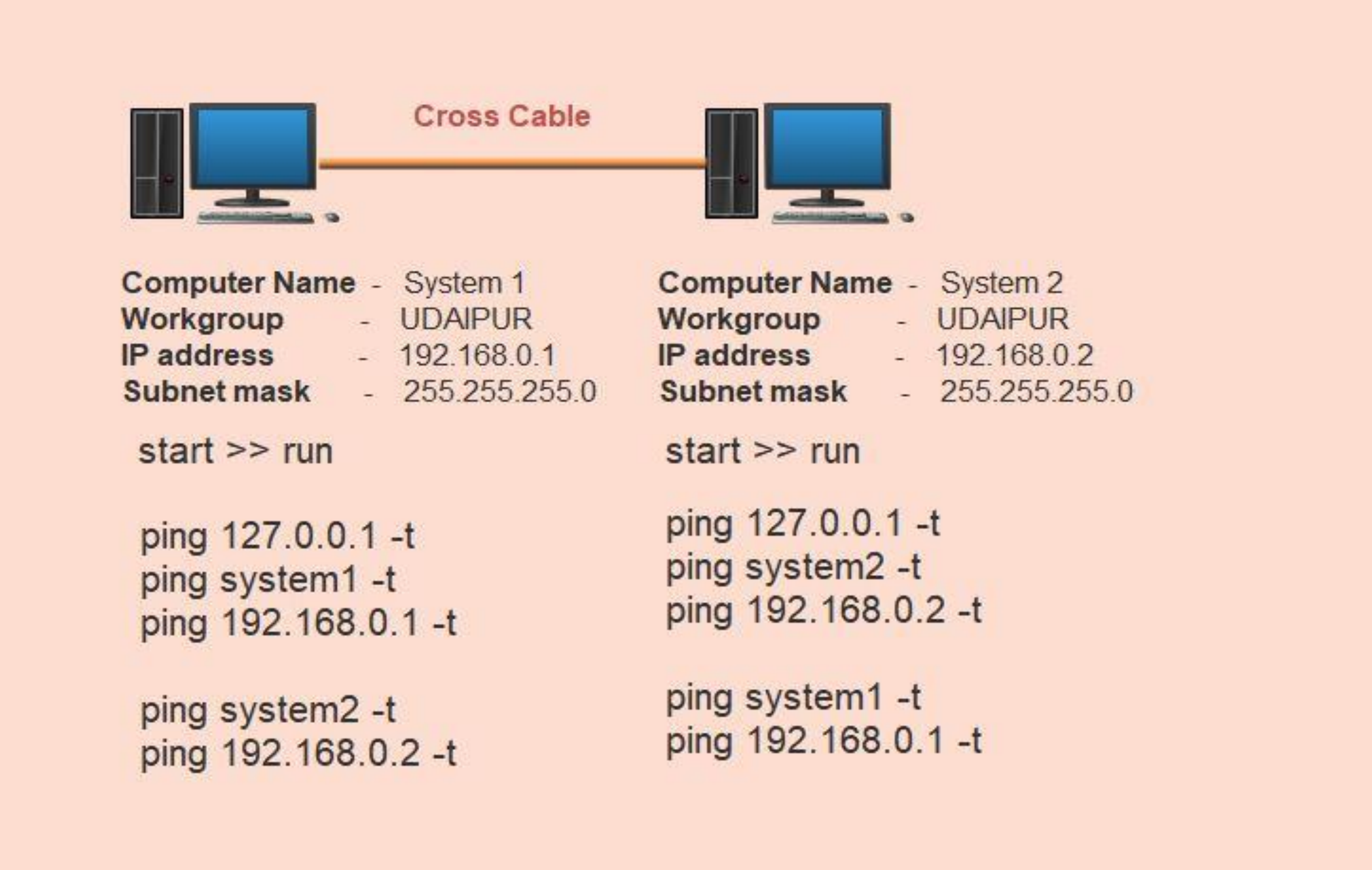
For a TCP/IP wide area network (WAN) to work efficiently as a collection of networks, the routers that pass packets of data between networks do not know the exact location of a host for which a packet of information is destined. Routers only know what network the host is a member of and use information stored in their route table to determine how to get the packet to the destination host's network. After the packet is delivered to the destination's network, the packet is delivered to the appropriate host.

For this process to work, an IP address has two parts. The first part of an IP address is used as a network address, the last part as a host address. If you take the example 192.168.123.132 and divide it into these two parts you get the following:

192.168.123.	Network
.132	Host

Lab # 6

Two system connect from cross cable



Computer Name - System 1
Workgroup - UDAIPUR
IP address - 192.168.0.1
Subnet mask - 255.255.255.0

start >> run

```
ping 127.0.0.1 -t
ping system1 -t
ping 192.168.0.1 -t

ping system2 -t
ping 192.168.0.2 -t
```

Computer Name - System 2
Workgroup - UDAIPUR
IP address - 192.168.0.2
Subnet mask - 255.255.255.0

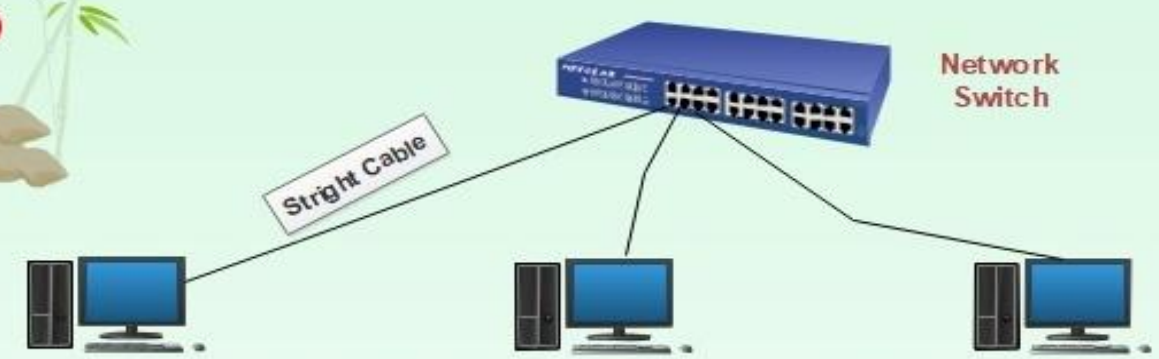
start >> run

```
ping 127.0.0.1 -t
ping system2 -t
ping 192.168.0.2 -t

ping system1 -t
ping 192.168.0.1 -t
```

Lab # 7

System connected from Network Switch



Computer Name	-	System 1
Workgroup	-	UDAIPUR
IP address	-	192.168.0.1
Subnet mask	-	255.255.255.0

start >> run

```
ping 127.0.0.1 -t
ping system1 -t
ping 192.168.0.1 -t

ping system2 -t
ping 192.168.0.2 -t
ping system3 -t
ping 192.168.0.3 -t
```

Computer Name	-	System 2
Workgroup	-	UDAIPUR
IP address	-	192.168.0.2
Subnet mask	-	255.255.255.0

start >> run

```
ping 127.0.0.1 -t
ping system2 -t
ping 192.168.0.2 -t

ping system1 -t
ping 192.168.0.1 -t
ping system3 -t
ping 192.168.0.3 -t
```

Computer Name	-	System 3
Workgroup	-	UDAIPUR
IP address	-	192.168.0.3
Subnet mask	-	255.255.255.0

start >> run

```
ping 127.0.0.1 -t
ping system3 -t
ping 192.168.0.3 -t

ping system1 -t
ping 192.168.0.1 -t
ping system2 -t
ping 192.168.0.2 -t
```

Lab # 8

IP Address to Binary Conversion

192	168	10	20
11000000	10101000	00001010	00010100

172	168	160	123
10101100	10101000	10100000	01111011

123	158	162	20
01111011	10011110	10100010	00010100

154	126	172	18
10011010	01111110	10101100	00010010

10	198	152	132
00001010	11000110	10011000	10000100

Lab # 9

Binary to IP Address Conversion

10110101	10101111	10101010	11100101
181	175	170	229

10101011	10011011	00101001	10001110
171	155	41	142

11010101	11001010	11001111	00000010
213	202	207	2

11010110	11110010	11101010	11110010
214	242	234	242

11110101	10101101	10110101	11100010
245	173	181	226

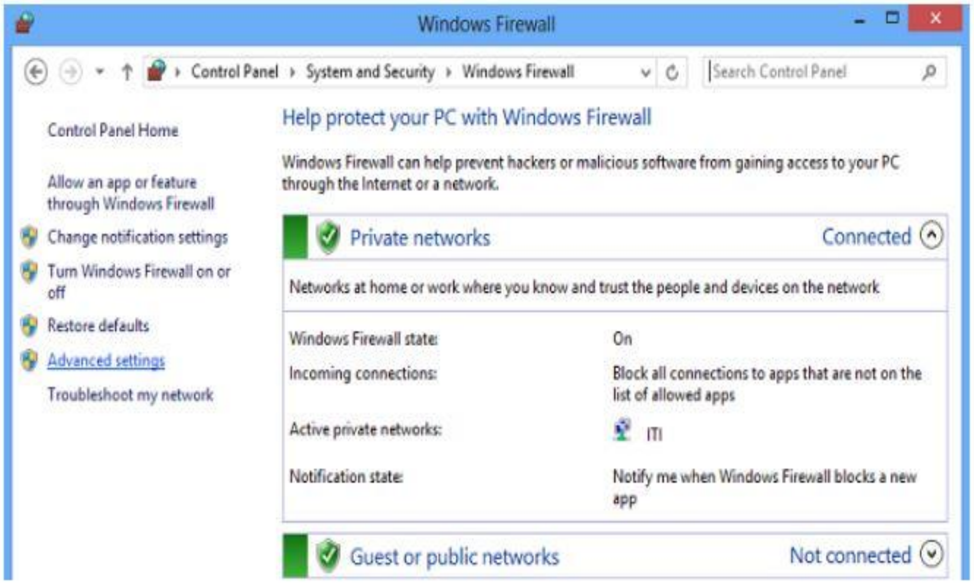
Allow or Block a Port in Windows Firewall :

Step 1

Open Windows Firewall in control panel & click ‘Advanced Settings’ of Windows 7/8/10 firewall, click the Advanced settings link in the left-hand pane of the main firewall dialog. This will bring up the Windows Firewall with Advanced Security window.

Step 2

Now, if you see the firewall window shows a list of rules on the left side. From the list, select Inbound Rules to display the inbound rules section.


Windows Firewall
Control Panel › System and Security › Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

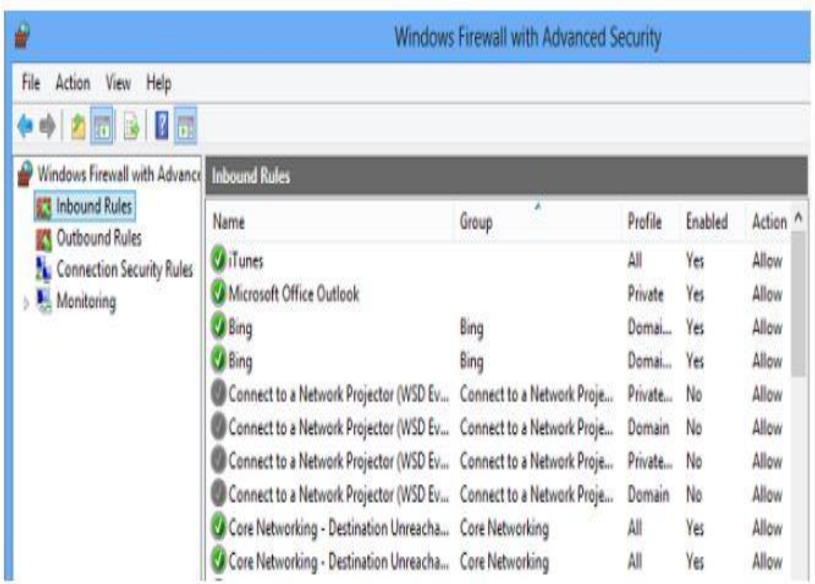
Windows Firewall state: On

Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active private networks: ITI

Notification state: Notify me when Windows Firewall blocks a new app

Guest or public networks — Not connected

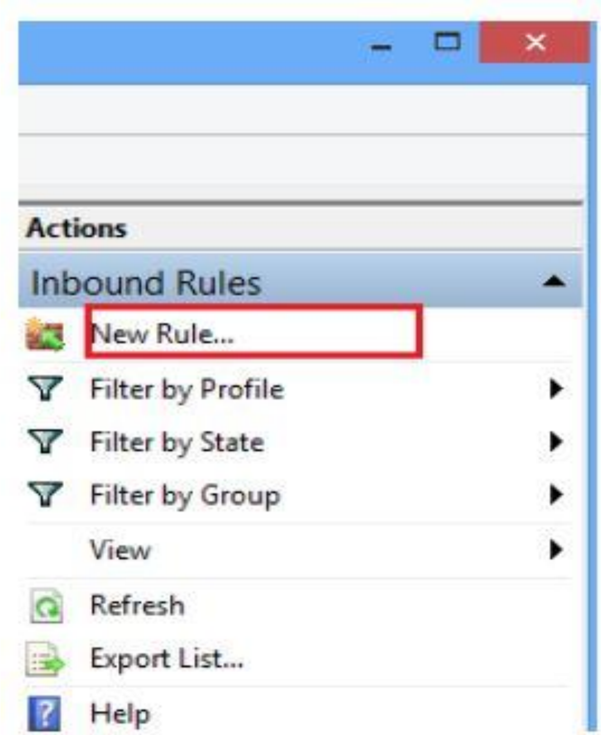

Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

Inbound Rules

Name	Group	Profile	Enabled	Action
iTunes		All	Yes	Allow
Microsoft Office Outlook		Private	Yes	Allow
Bing	Bing	Domai...	Yes	Allow
Bing	Bing	Domai...	Yes	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow

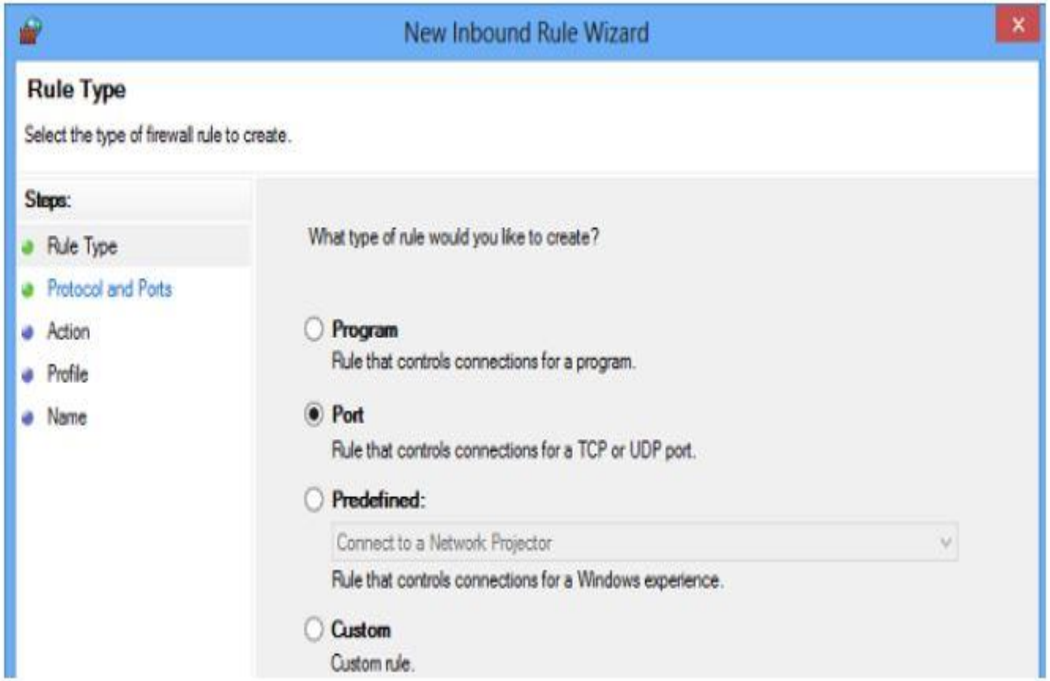
Step 3

Then, from the right pane select the ‘New Rule’ option.



Step 4

Doing so will open the ‘New Inbound Rule Wizard’ window. From it, select ‘Port’ as the new Rule Type and click Next. For safety purposes


New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

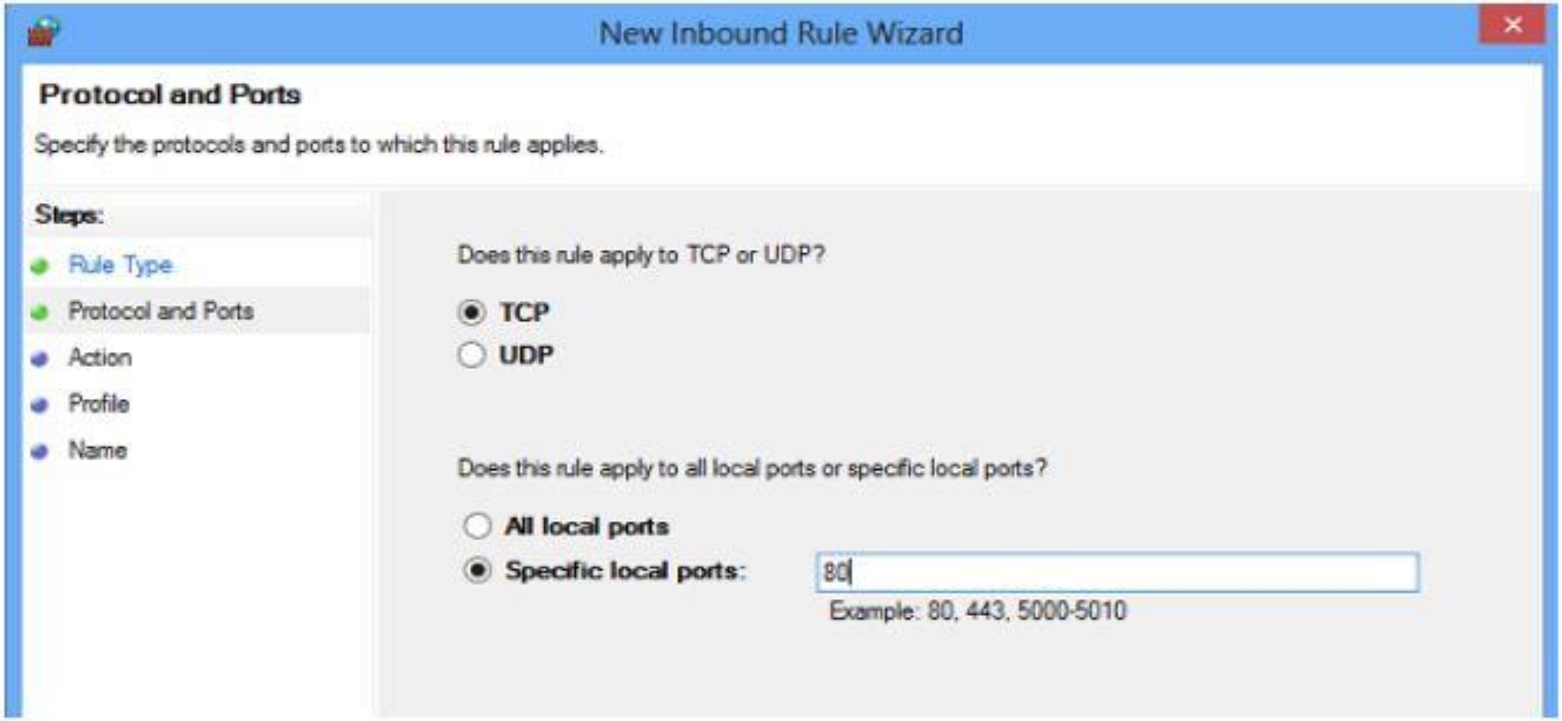
● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
Connect to a Network Projector
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Step 5

I tried allowing TCP port. Click on Specific local ports. Then choose one port like 80 as shown in the screenshot below.



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

● TCP
○ UDP

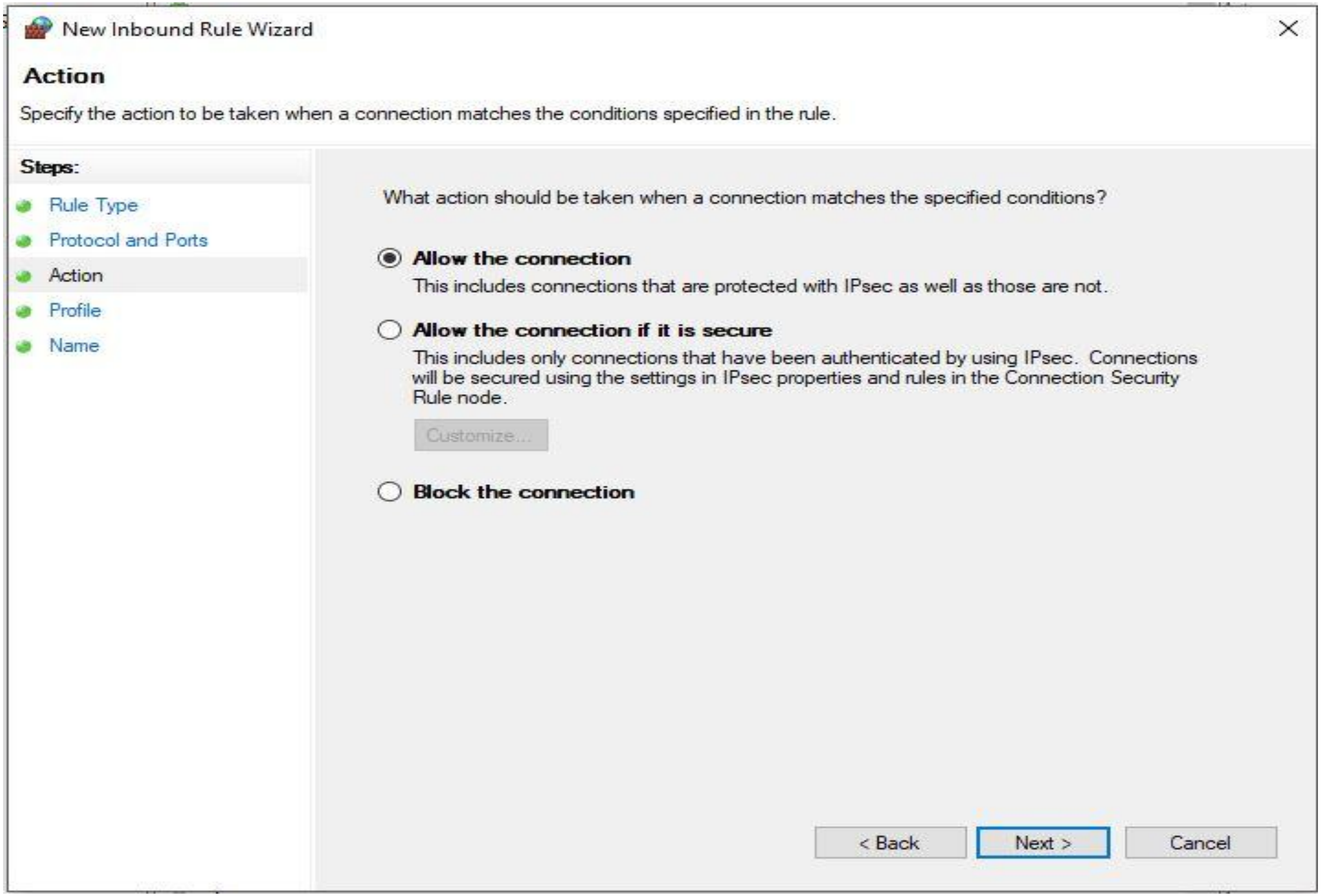
Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 80

Example: 80, 443, 5000-5010

Step 6

Next, select ‘Allow the connection’ as the Action and click Next.



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

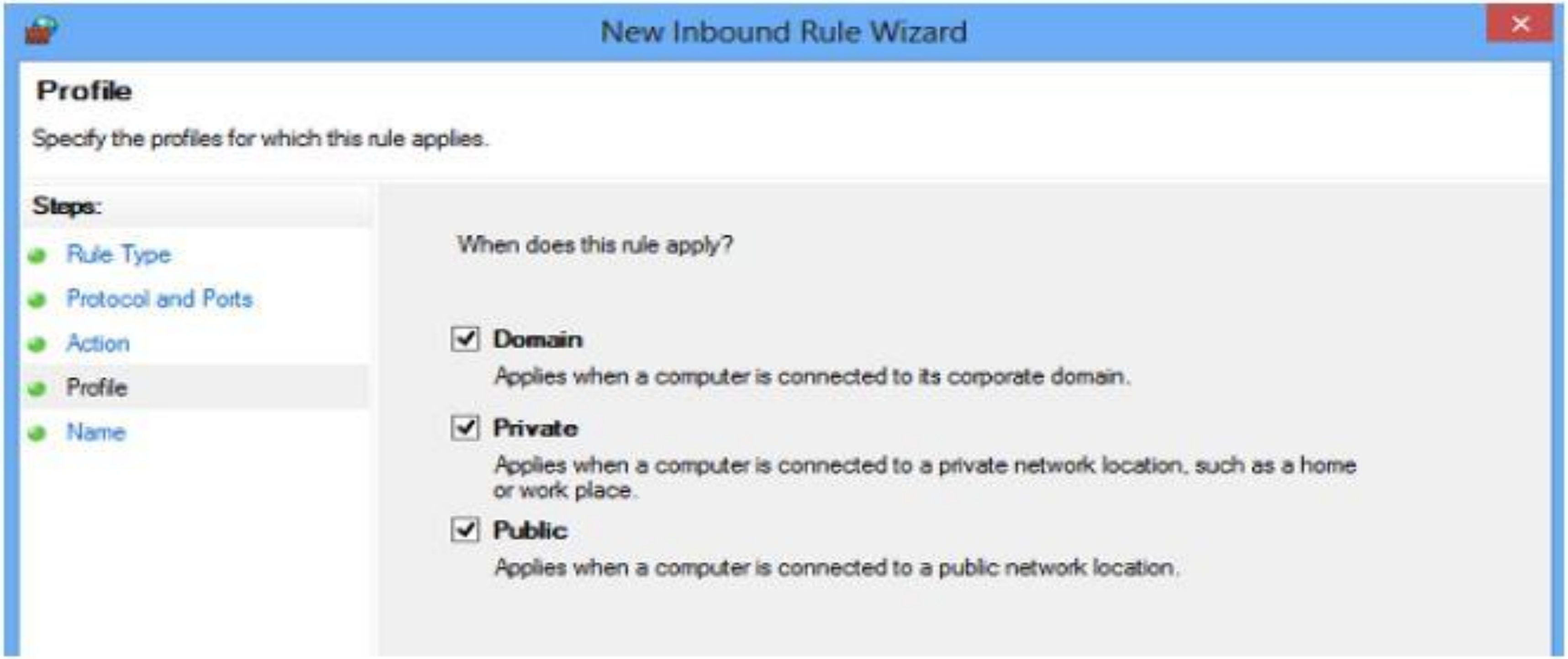
● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**

Step 7

Later, select all the profiles available for different type of connections (Domain, Private and Public) and Click Next to continue.



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

When does this rule apply?

☑ **Domain**

Applies when a computer is connected to its corporate domain.

☑ **Private**

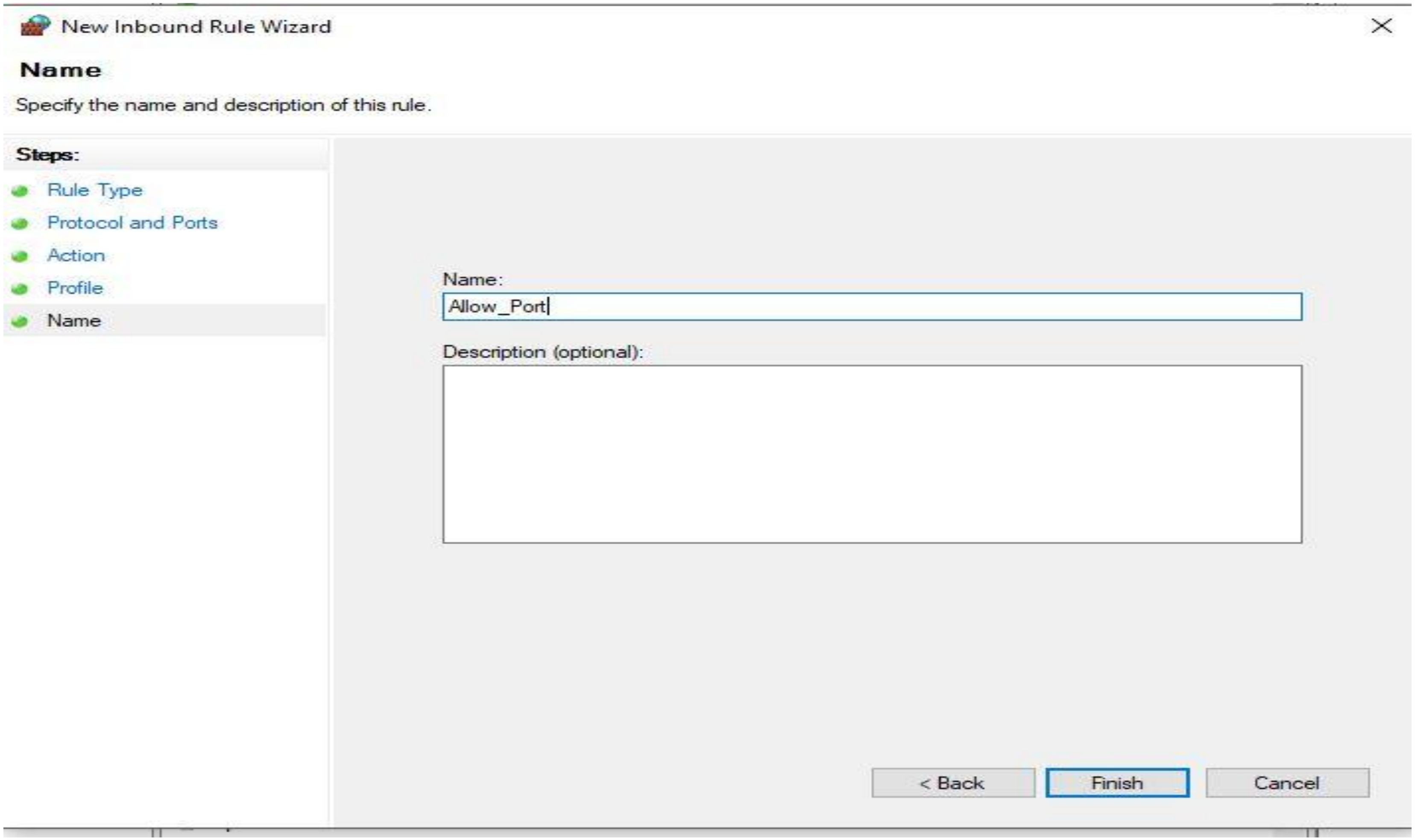
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**

Applies when a computer is connected to a public network location.

Step 8

Give a name of your choice to the new rule. I used ‘allow ports’. If you want, you can add the description to the new rule. This step is however optional.



New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name: Allow_Port

Description (optional):

Finally, click the Finish button to configure the settings.

ipconfig command :

#ipconfig

#ipconfig /all
This option displays the same IP addressing information for each adapter as the default option. Additionally, it displays DNS and WINS settings for each adapter.

#ipconfig /release
This option terminates any active TCP/IP connections on all network adapters and releases those IP addresses for use by other applications. "pconfig /release" can be used with specific Windows connection names.

#ipconfig /renew
This option re-establishes TCP/IP connections on all network adapters.

Network Command’s :

1. Traceroute is a command which can show you the path a packet of information takes from your computer to one you specify. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded. In addition to this, it will tell you how long each 'hop' from router to router takes.

In Windows, select Start > Programs > Accessories > Command Prompt(run as administrator).

#tracert

```
#tracert google.co.in
```

2. The netstat command is a Command Prompt command used to display very detailed information about how your computer is communicating with other computers or network devices. Specifically, the netstat command can show details about individual network connections, overall and protocol-specific networking statistics, and much more, all of which could help troubleshoot certain kinds of networking issues.

#netstat

```
A. #netstat -a
B. #netstat -o
C. #netstat -s -p tcp -f
D. #netstat -e -t 5
```

3. The net user command is used to add, remove, and make changes to the user accounts on a computer, all from the Command Prompt.

The net user command is one of many net commands.

#net user

```
A. #net user /add user_name
B. #net user user_name
```

4. The telnet commands allow you to communicate with a remote computer that is using the Telnet protocol. You can run telnet without parameters in order to enter the telnet context, indicated by the Telnet prompt (telnet>). From the Telnet prompt, use the following commands to manage a computer running Telnet Client.

```
#telnet IP_Address
```

5. The pathping displays the degree of packet loss at any given router or link, you can determine which routers or subnets might be having network problems. Pathping performs the equivalent of the tracert command by identifying which routers are on the path.

```
#pathping www.google.com
```

6.

```
#call "C:\Program Files\Microsoft Office\Office12\winword.exe"
```

7.

```
#whoami
```

8.

```
#getmac
```

Port & Protocols :

Well Known Ports: 0 through 1023
Registered Ports: 1024 through 49151
Dynamic/Private : 49152 through 65535

TCP ports use the Transmission Control Protocol. TCP is the most commonly used protocol on the Internet and any TCP/IP network. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and that packets will be delivered in the same order in which they were sent. Guaranteed communication/delivery is the key difference between TCP and UDP.

UDP ports use the Datagram Protocol, a communications protocol for the Internet network, transport, and session layers. Like TCP (Transmission Control Protocol), UDP is used with IP (the Internet Protocol) and makes possible the transmission of datagrams from one computer to applications on another computer, but unlike TCP, UDP is connectionless and does not guarantee reliable communication; it's up to the application that received the message to process any errors and verify correct delivery. UDP is often used with time-sensitive applications, such as audio/video streaming, where dropping some packets is preferable to waiting for delayed data.

When troubleshooting unknown open ports, it is useful to find exactly what services/processes are listening to them. This can be accomplished in both Windows command prompt and Linux variants using the "netstat -aon" command. We also recommend runnig multiple anti-virus/anti-malware scans to rule out the possibility of active malicious software. For more detailed and personalized help please use our forums.

Port & Protocols :

20 & 21	FTP
22	SSH
23 & 992	Telnet
25, 465 & 587	SMTP
37	Time Protocol
53	DNS
67 & 68	DHCP
69	TFTP
80,443 & 8080	HTTP
110 & 995	POP3
115	SFTP
118	SQL
123	NTP
137	NetBIOS
143	IMAP
389 & 636	LDAP
1512	WINS
3389	RDP
5931	Ammyy Admin
5938	Team Viewer

IP Address :

The IP address is a familiar term for most computer users. An IP address is the unique numerical address of a device in a computer network that uses Internet Protocol for communication. The IP address allows you to pinpoint a particular device from the billions of devices on the Internet. To send you a letter, someone needs your mailing address. In the same sense, one computer needs the IP address of another computer to communicate with it. An IP address consists of four numbers; each can contain one to three digits. These numbers are separated with a single dot (.). These four numbers can range from 0 to 255.

Types of IP addresses

The IP addresses can be classified into two. They are listed below.

1) Static IP addresses
2) Dynamic IP addresses

Static IP Addresses -

As the name indicates, the static IP addresses usually never change but they may be changed as a result of network administration. They serve as a permanent Internet address and provide a simple and reliable way for the communication. From the static IP address of a system, we can get many details such as the continent, country, region and city in which a computer is located, The Internet Service Provider (ISP) that serves that particular computer and non-technical information such as precise latitude and longitude of the country, and the locale of the computer.

Dynamic IP Addresses -

Dynamic IP address are the second category. These are temporary IP addresses. These IP addresses are assigned to a computer when they get connected to the Internet each time. They are actually borrowed from a pool of IP addresses, shared over various computers. Since limited number of static IP addresses are available, ISPs usually reserve the portion of their assigned addresses for sharing among their subscribers in this way.

Static IP addresses are considered as less secure than dynamic IP addresses because they are easier to track.

IP Version 4 and IP Version 6

The two versions of IP addresses currently running are IP versions 4 (IPv4) and IP versions 6 (IPv6). There are many features with these two versions.

IP Version 4 :

IP Version 4 (IPv4) was defined in 1981. It has not undergone much changes from that time. Unfortunately, there is a need of IP addresses more than IPv4 could supply.

IPv4 uses 32-bit IP address. So the maximum number of IP address is 232—or 4,294,967,296.

This is a little more than four billion IP addresses. An IPv4 address is typically formatted as four 8-bit fields. Each 8-bit field represents a byte of the IPv4 address. As we have seen earlier, each fields will be separated with dots. This method of representing the byte of an IPv4 address is referred to as the dotted-decimal format. The bytes of the IPv4 is further classified into two parts. The network part and the host part.

Network Part -

This part specifies the unique number assigned to your network. It also identifies the class of network assigned. The network part takes two bytes of the IPv4 address.

Host Part -

This is the part of the IPv4 address that you can assign to each host. It uniquely identifies this machine on your network. For all hosts on your network, the network part of the IP address will be the same and host part will be changing.

IP Version 6 :

The IPv6 is the most recent version of Internet Protocol. As the Internet is growing rapidly, there is a global shortage for IPv4. IPv6 was developed by the Internet Engineering Task Force (IETF). IPv6 is intended to replace the IPv4. IPv6 uses a 128-bit address and it allows 2128 i.e. approximately 3.4×1038 addresses. The actual number is slightly smaller as some ranges are reserved for special use or not used. The IPv6 addresses are represented by 8 groups of four hexadecimal digits with the groups being supported by colons. An example is given below:

Eg: 2001:0db8:0000:0042:0000:8a2e:0370:7334

The features of IPv6 -

The main features of the IPv6 are listed below.

1) IPv6 provides better end-to-end connectivity than IPv4.

2) Comparatively faster routing.

3) IPv6 offers ease of administration than IPv4.

4) More security for applications and networks.

5) It provides better Multicast and Anycast abilities.

6) Better mobility features than IPv4.

7) IPv6 follows the key design principles of IPv4 and so that the transition from IPv4 to IPv6 is smoother.

These are the key features of the IPv6 when compared to the IPv4. However, IPv6 has not become popular as IPv4.

IP Address and Classes :

The IP hierarchy contains many classes of the IP addresses. Broadly, the IPv4 addressing system is divided into five classes of IP address. All the five classes are identified by the first octet of the IP address. The Internet community originally defined five address classes to accommodate networks of varying sizes. Microsoft TCP/IP supports class A, B, and C addresses assigned to hosts. The class of address defines which bits are used for the network ID and which bits are used for the host ID. It also defines the possible number of networks and the number of hosts per network.

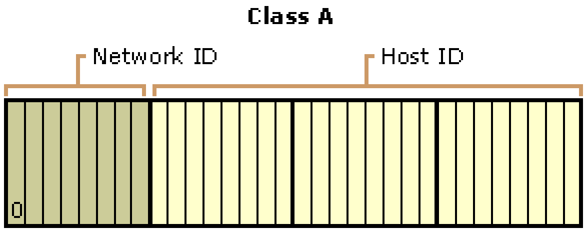
The classes of IPv4 addresses

The different classes of the IPv4 address are the following:

1) Class A address
2) Class B address
3) Class C address
4) Class D address
5) Class E address

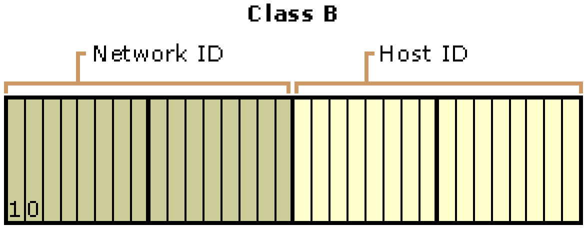
Class A Address -

Class A addresses are assigned to networks with a very large number of hosts. The high-order bit in a class A address is always set to zero. The next seven bits (completing the first octet) complete the network ID. The remaining 24 bits (the last three octets) represent the host ID. This allows for 126 networks and 16,777,214 hosts per network. The first bit of the first octet is always set to zero. So that the first octet ranges from 1 – 127. The class A address only include IP starting from 1.x.x.x to 126.x.x.x. The IP range 127.x.x.x is reserved for loop back IP addresses. The default subnet mask for class A IP address is 255.0.0.0. This means it can have 126 networks (27-2) and 16777214 hosts (224-2). Class A IP address format is thus: 0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH.



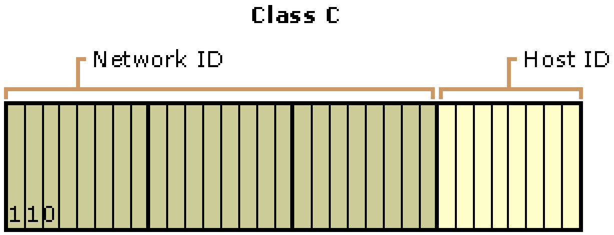
Class B Address -

Class B addresses are assigned to medium-sized to large-sized networks. The two high-order bits in a class B address are always set to binary 1 0. The next 14 bits (completing the first two octets) complete the network ID. The remaining 16 bits (last two octets) represent the host ID. This allows for 16,384 networks and 65,534 hosts per network. Here the first two bits in the first two bits is set to zero. Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x. Class B has 16384 (214) Network addresses and 65534 (216-2) Host addresses. Class B IP address format is: 10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH



Class C Address -

Class C addresses are used for small networks. The three high-order bits in a class C address are always set to binary 1 1 0. The next 21 bits (completing the first three octets) complete the network ID. The remaining 8 bits (last octet) represent the host ID. This allows for 2,097,152 networks and 254 hosts per network. The first octet of this class has its first 3 bits set to 110. Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x. Class C gives 2097152 (221) Network addresses and 254 (28-2) Host addresses. Class C IP address format is: 110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH



Class D Address -

Class D addresses are reserved for IP multicast addresses. The four high-order bits in a class D address are always set to binary 1 1 1 0. The remaining bits are for the address that interested hosts recognize. Microsoft supports class D addresses for applications to multicast data to multicast-capable hosts on an internetwork.

Class E Address -

Class E is an experimental address that is reserved for future use. The high-order bits in a class E address are set to 1111.
Below Table is a summary of address classes A, B, and C that can be used for host IP addresses.

IP Address Classes

Class	1st Octet Decimal Range	1st Octet High Order Bits	Network/Host ID (N=Network, H=Host)	Default Subnet Mask / CIDR Notation	Number of Networks	Hosts per Network (Usable Addresses)
A	1 – 126	0	N.H.H.H	255.0.0.0 /8	128 (2^7)	16,777,214 (2^{24} – 2)
B	128 – 191	10	N.N.H.H	255.255.0.0 /16	16,384 (2^{14})	65,534 (2^{16} – 2)
C	192 – 223	110	N.N.N.H	255.255.255.0 /24	2,097,152 (2^{21})	254 (2^8 – 2)
D	224 – 239	1110	Reserved for Multicasting			
E	240 – 254	1111	Experimental; used for research			

Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback and diagnostic functions.

IP Class	IP Address Range	No. of hosts and net-works each Class provides
Class A	1.0.0.1 to 126.255.255.254	Sup-ports 16.7 mil-lion hosts on each of 126 networks.
Class B	128.1.0.1 to 191.255.255.254	Sup-ports 65,534 hosts on each of 16,382 networks.
Class C	192.0.1.1 to 223.255.254.254	Sup-ports 254 hosts on each of 2 mil-lion networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or Research and Development Purposes.

Private IP Addresses :

Class	Private Networks	Subnet Mask / CIDR Value	Address Range
A	10.0.0.0-10.255.255.255	255.0.0.0 /8	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.255.255	255.240.0.0 /12	172.16.0.0 - 172.31.255.255
C	192.168.0.0-192.168.255.255	255.255.0.0 /16	192.168.0.0 - 192.168.255.255

Note* - Another range of private IP addresses is 169.254.0.0 to 169.254.255.255, but those addresses are for Automatic Private IP Addressing (APIPA) use only.