

# **The University of Jordan, Comp. Eng. Dept.**

## **Spring 2023: Networks laboratory: Handout:**

### **Experiment 1**

#### **Network Cabling and Devices and Packet Tracer (Theory and Practice)**

**Instructors: Prof. Khalid A. Darabkh and Eng. Muna Al-Akhras**

**Parts Included: Introduction to Networks, Transmission Media, Network Devices, Internal Components of Routers, Device Configuration, ARP and ICMP, Network Troubleshooting, and Packet Tracer.**

#### **Part I: Introduction to Networks**

Network is a small group of computers that share information, or they can be very complex, spanning large geographical areas that provide its users with unique capabilities, above and beyond what the individual machines and their software applications can provide.

Internetworking term in computer networking explains how computer networks connect with each other through Internetworking devices. Before we learn internetworking in details, let's understand what computer network is first. Computer networks are basically built from three components; End Devices, Networking Devices and Media.

- **End Devices:** End devices are used to access or transmit the data. Computer, laptop, data server and tablet are the example of end devices.
- **Networking Devices:** Networking devices are used to control the data flow. Switches, Routers, HUB, Bridges, firewalls and modems are the example of networking devices.
- **Media:** Media is used to transmit the data. Copper cables, fiber cable and wireless signals are the example of media.

Models are useful because they help us understand difficult concepts and complicated systems. When it comes to networking, there are several models that are used to explain the roles played by various technologies, and how they interact. Of these, the most popular and commonly used are the Open Systems Interconnection (OSI) Reference Model and TCP/IP Model. Both the TCP/IP and OSI model work in a very similar fashion. But they do have very subtle differences too. The most apparent difference is the number of layers. TCP/IP is a four-layered structure, while OSI is a seven-layered model. Figure 1 presents the OSI and TCP/IP networking models.

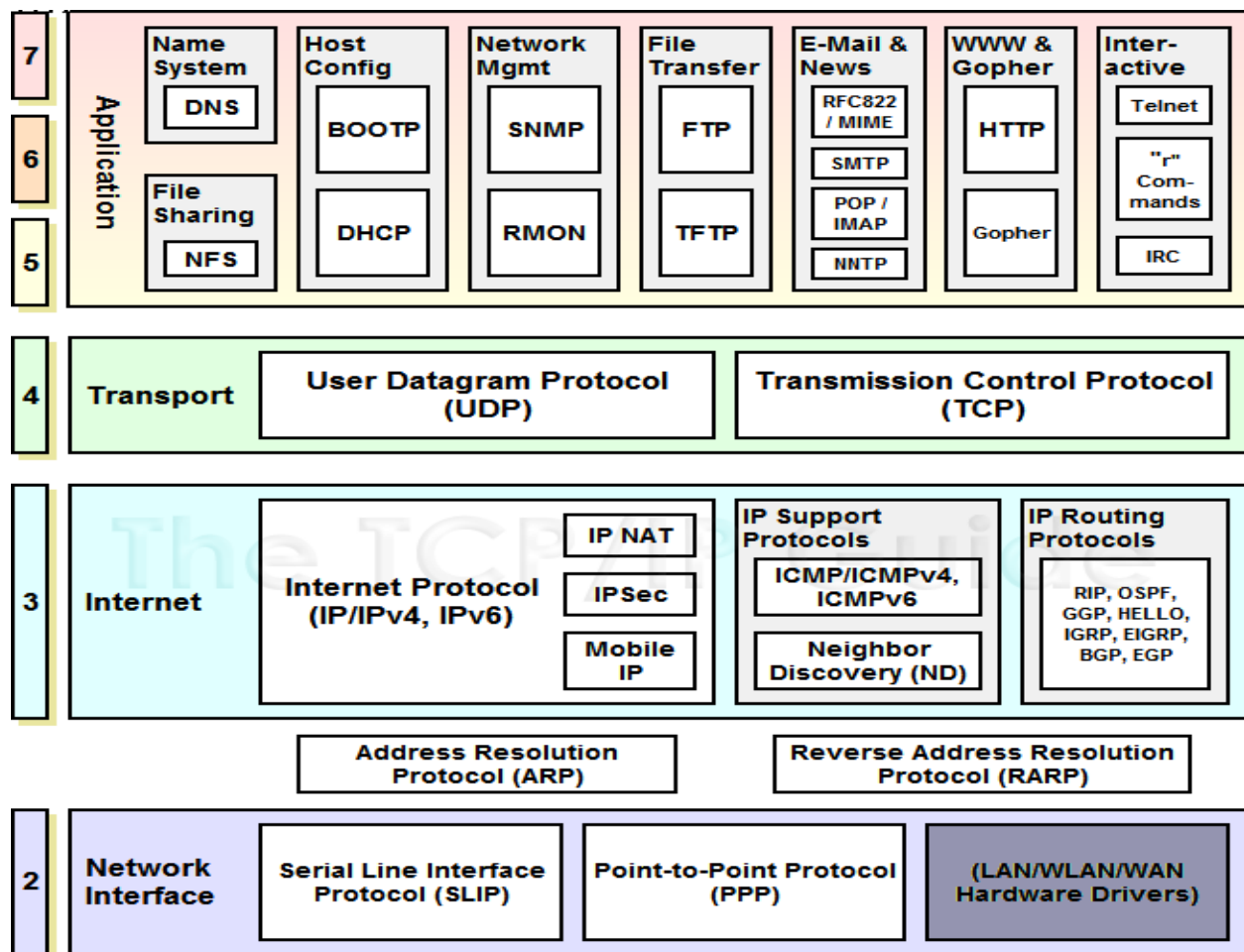


Figure 1: The OSI and TCP/IP networking models.

## Part II: Network Cabling System (Transmission Media)

In this section we talk about the physical layer, types of cables used for networking communication.

### A. The Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur. Figure 2 shows the position of the physical layer with respect to the transmission medium and the data link layer. On the sending computer, it converts digital signals received from the Data Link layer, into analog signals and loads them on the physical media. On the receiving computer, it picks analog signals from the media and converts them into digital signals, and transfers them to the Data Link layer for further processing.

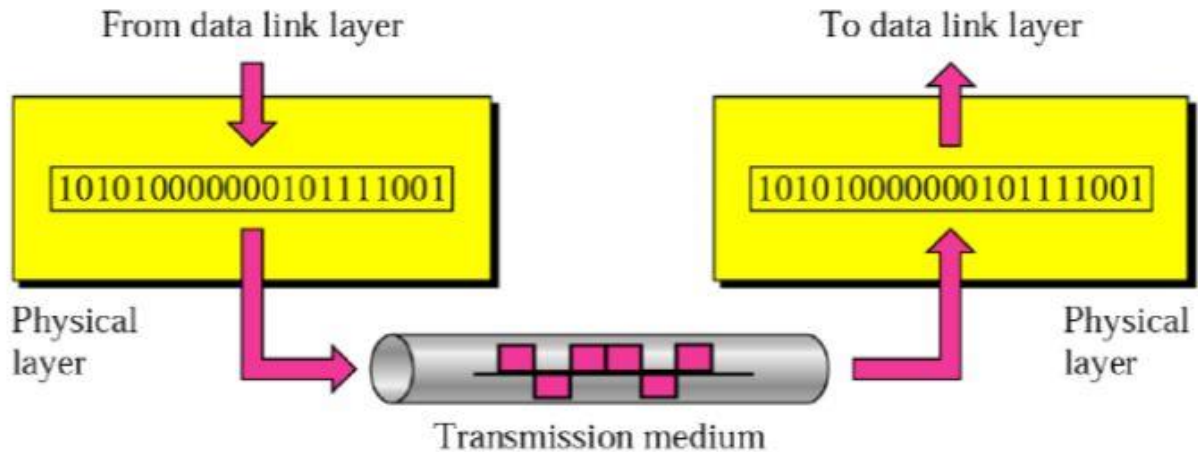


Figure 2: The position of the physical layer.

The Physical Layer is the first layer of the OSI model. This layer mainly defines standards for media devices, and technologies that are used to move data across the network, such as:

- Type of cable used in connecting the devices.
- Patterns of pins used in both sides of the cable.
- Type of interface-card used in the networking device.
- Type of connector used to connect the cable with the network interface.
- Encoding of digital signals received from the Data Link layer based on the attached media type such as electrical for copper, light for fiber, or a radio wave for wireless.
- 10BaseT, 10Base100, Channel Service Unit/Data Service Unit (CSU/DSU), Data Communications Equipment (DCE), and Data Terminal Equipment (DTE) are examples of the standards used in this layer.

## B. Transmission media

Transmission media are actually located below the physical layer and are directly controlled by the physical layer. **A transmission medium can be broadly defined as anything that can carry information from a source to a destination.** In data communications the definition of the information and the transmission medium is more specific. The transmission medium is usually free space, metallic cable, or fiber-optic cable. The information is usually a signal that is the result of a conversion of data from another form. Computers and other telecommunication devices use signals to represent data. These signals are transmitted from one device to another in the form of electromagnetic energy, which is propagated through transmission media. **In telecommunications, transmission media can be divided into two broad categories: guided and unguided. Guided media include twisted-pair cable, coaxial cable, and fiber-optic cable. Unguided medium is free space.** Figure 3 shows this taxonomy.

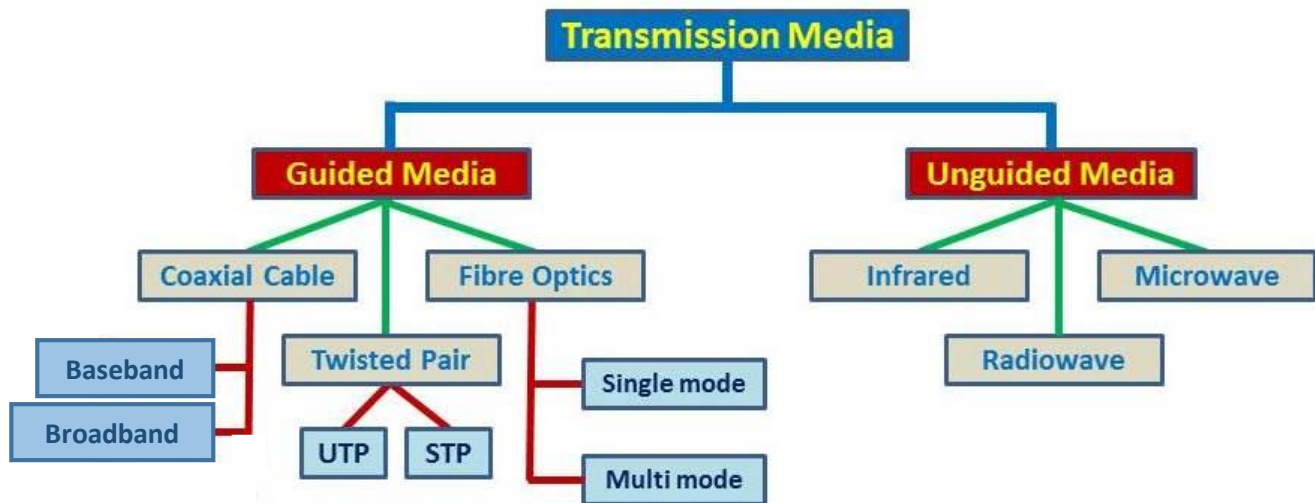


Figure 3: Types of transmission media.

### 1. Guided media:

Guided media which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable. A signal traveling along any of these media is directed and contained by the physical limits of the medium.

- Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current.
- Optical fiber is a cable that accepts and transports signals in the form of light.

#### a) Twisted-Pair Cable

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together, as shown in Figure 4. The twisting helps to reduce the electromagnetic interference (noise) and crosstalk. More twist, more quality. It is important to install cable away from sources of interference such as high voltage cables and the fluorescent lighting. Televisions, computers monitors and microwaves are other possible sources of interference. Cross talk is the leakage of signals between pairs. Crosstalk degrades the network performance and are often caused by untwisting too much cable when terminating. If high crosstalk values are detected, the best thing to do is check the cable terminations and re-terminate as necessary.

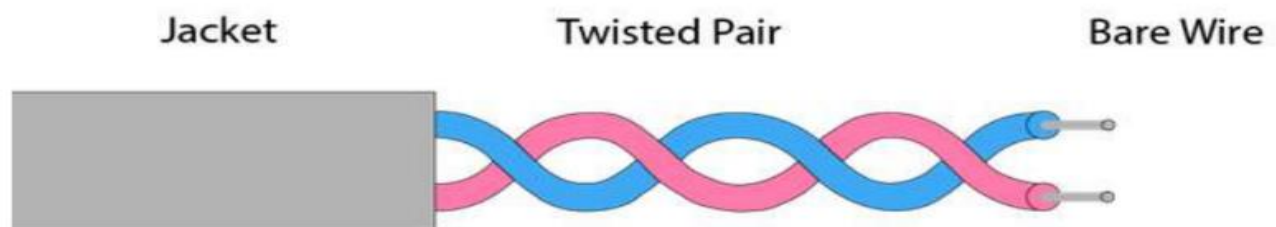


Figure 4: Twisted-Pair cable.

### i. Types of Twisted-Pair Cable

Twisted-pair cable has many advantages, such as being easy to install and less expensive when compared to other cable types; however, its low data rate and short range are the main drawbacks. Twisted-pair cable comes in two forms, as follows, as shown in Figure 5:

- **Unshielded Twisted-Pair (UTP)** cable is the most common type of telecommunication medium in use today. The advantages of UTP cable are: it is cheap, flexible, and easy to install.
- **Shielded Twisted-Pair (STP)** cable has a metal foil or braided- mesh covering that encases each pair of insulated conductors. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive. Table 1 shows the difference between UTP and STP.

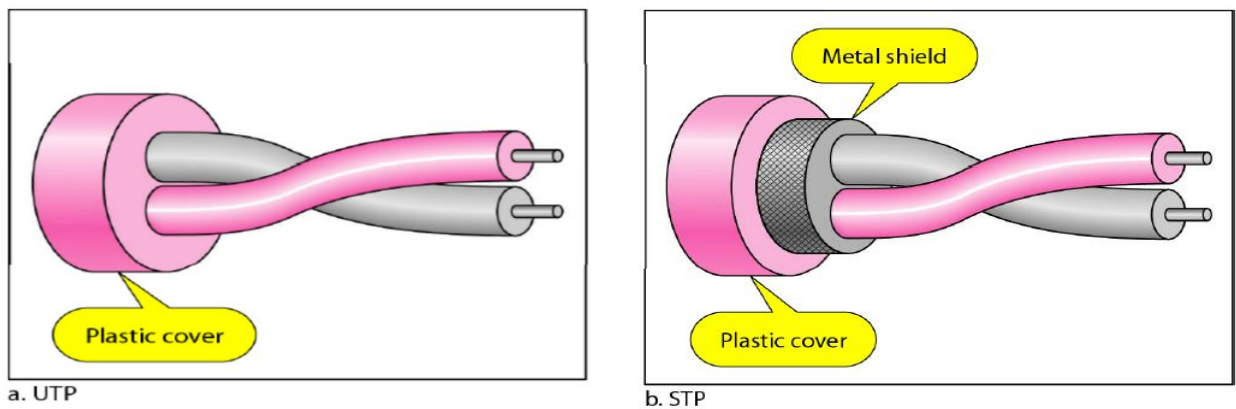


Figure 5: UTP and STP cables.

Table 1: The difference between UTP and STP cables.

Parameters	UTP	STP
Full Form	Unshielded Twisted Pair	Shielded Twisted Pair
Structure	cable with wires that are twisted together.	Twisted pair cable enclosed in foil / shield.
Cost	Cheaper than STP	Costlier than UTP
Weight	Lighter than STP	Heavier than UTP
Noise & interference	Prone to Noise and interference	Less prone to noise and interference
Data Speed	Supports slower speed than on STP	Support higher speed than UTP
Grounding of cable	Not required	Required
Target deployments	Locations less prone to interference like offices and homes.	Locations prone to interference like factories and airports

## ii. Categories

The Electronic Industries Association (EIA) has developed standards to classify UTP cable into eight categories. Categories are determined by cable quality, with 1 as the lowest and 8 as the highest. Each EIA category is suitable for specific uses. For example, CAT 5e is an UTP cable, which has maximum speed up to 10 Gbps, maximum length 100, frequency 100 MHz, and used for Ethernet, Fast Ethernet, and Giga Ethernet.

## iii. UTP Connectors

The most common UTP connector is RJ45 (RJ stands for registered jack). RJ-45 connector is the male component, crimped at the end of the cable. The socket is the female component of a network device, wall, cubicle partition outlet, or patch panel, as shown in Figure 6. The RJ45 is a keyed connector, meaning the connector can be inserted in only one way. RJ-45 connectors are used for interconnecting network hosts with intermediate networking devices, such as switches and routers. **RJ-45 connector is used for a range of physical layer specifications, one of which is Ethernet. The TIA/EIA-568 standard describes the wire color codes to pin assignments (pinouts) for Ethernet cables.**

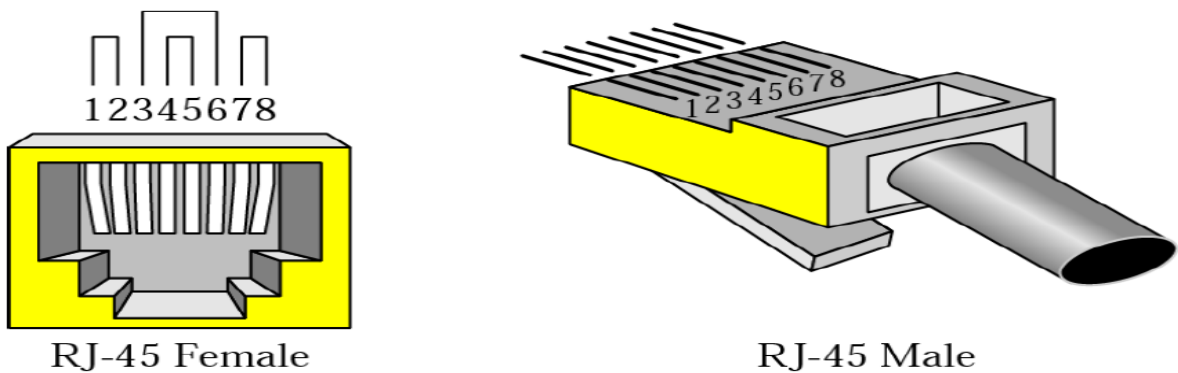


Figure 6: RJ-45 connector.

## iv. What is an Ethernet cable?

An Ethernet cable is a network cable used for high-speed wired network connections between two devices. **This network cable is made of four-pair cable, which consists of twisted pair conductors,** as shown in Figure 7. It is used for data transmission at both ends of the cable, which is called RJ45 connector.

The Ethernet cables are categorized as Cat 5, Cat 5e, Cat 6, and UTP cable. Cat 5 cable can support a 10/100 Mbps Ethernet network while Cat 5e and Cat 6 cable to support Ethernet network running at 10/100/1000 Mbps, which namely Ethernet, Fast Ethernet, and Giga Ethernet, respectively.



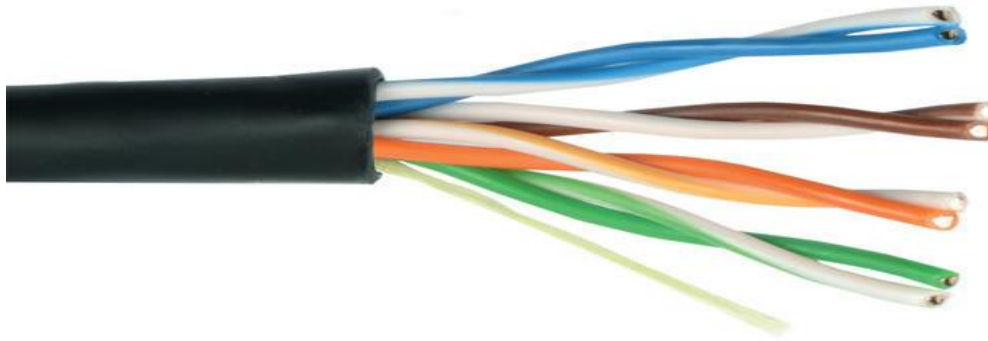


Figure 7: Ethernet UTP cable.

➤ **Color code for 4 cables pairs:**

- Wiring standards that defines the pinout (connection order) for terminating twisted pair network cable.
- EIA defines two different patterns, or wiring scheme, called T568A and T568B.
- The two schemes are similar except two of the four pairs are reversed in the termination order. Figure 8 shows this color-coding and how the two pairs are reversed.
- Different situations may require UTP cables to be wired according to different wiring schemes and one of the T568A or T568B should be chosen. This means that the individual wires in the cable have to be connected in different orders to different sets of pins in the RJ-45 connectors.

TIA 568A				TIA 568B			
Pin #	Wire Color Legend		Signal	Pin #	Wire Color Legend		Signal
1		White/Green	TX+	1		White/Orange	TX+
2		Green	TX-	2		Orange	TX-
3		White/Orange	RX+	3		White/Green	RX+
4		Blue	TRD2+	4		Blue	TRD2+
5		White/Blue	TRD2-	5		White/Blue	TRD2-
6		Orange	RX-	6		Green	RX-
7		White/Brown	TRS3+	7		White/Brown	TRS3+
8		Brown	TRD3-	8		Brown	TRD3-

Figure 8: T568A and T568B standards.

- **Types of interfaces:** In an Ethernet LAN, devices use one of two types of UTP interfaces:
  - ✓ **The Media-Dependent Interface (MDI):** MDIs are found in end devices; it uses the normal Ethernet pinouts. Pins 1 and 2 are used for transmitting data and pins 3 and 6 are used for receiving data. Examples of such devices are PCs, routers, and servers.
  - ✓ **The Media-Dependent Interface, crossover (MDIX):** The MDIX connection swaps the transmit pairs internally. It receives data on pins 1 and 2 and transmits data from the pin 3 and 6. Examples of such devices are: hubs and switches.
- Based on the type of end devices, a UTP cable can be made in two ways. The first type of cable, known as the straight-through cable, connects two different types of end devices; such as PC to Switch. The second type of cable, known as the cross-over cable, connects two same

type of end devices such as PC to PC or Switch to Switch. Figure 9 presents the difference between MDI and MDI-X interfaces in NIC and hub respectively.



Figure 9: The difference between MDI and MDI-X interfaces.

- The following are the main cable types that are obtained by using the T568A and T568B:
  - ✓ Ethernet Straight-through.
  - ✓ Ethernet Crossover.
  - ✓ Rollover.

Here is a more detailed illustration of the aforementioned cables:

### 1) Straight Through Cable:

- ❖ Straight-through cable is the most common network cable type. It is a type of CAT5 with RJ-45 connectors at each end, and each has the same pin out.
- ❖ In other words, if T568A is on one end of the cable, T568A is also on the other. If T568B is on one end of the cable, T568B is also on the other, as shown in Figure 10.
- ❖ This means that the order of connections for each color is the exact same on both ends.
- ❖ A straight-through cable is used to connect the following devices:
  - PC to Switch, PC to Hub, Router to Switch, Switch to Server, and Hub to Server

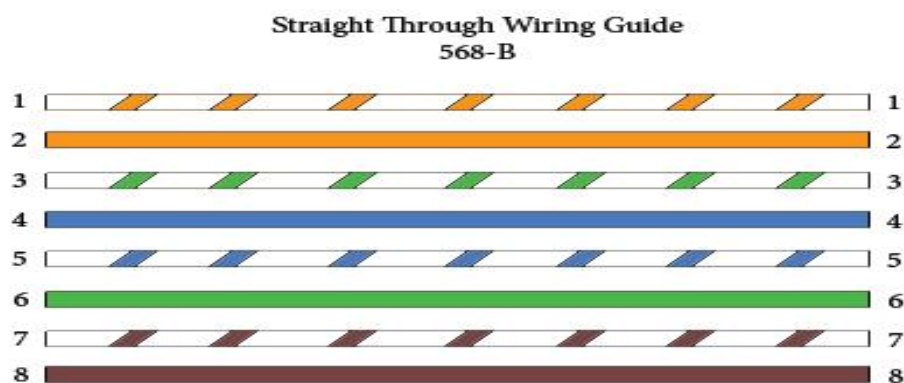


Figure 10: Straight through cable wiring..

### 2) Ethernet cross-over cable

- ❖ A Crossover cable is a type of CAT 5 where one end is T568A configuration and the other end as T568B configuration.



- ❖ In this cable, transmitting pins of one side connect with the receiving pins of the other side.
- ❖ In this type of cable connection, Pin 1 is crossed with Pin 3, and Pin 2 is crossed with Pin 6. Remaining wires connect in the same positions at both ends, as shown in Figure 11.
- ❖ It is widely used to connect two devices of the same type, such as:
  - Two computers, Two hubs, A hub to a switch, A cable modem to a router, and Two router interfaces.
- ❖ Figure 12 demonstrates an example of the physical connections using straight through and cross over, with PC-Hub and PC-PC, respectively.

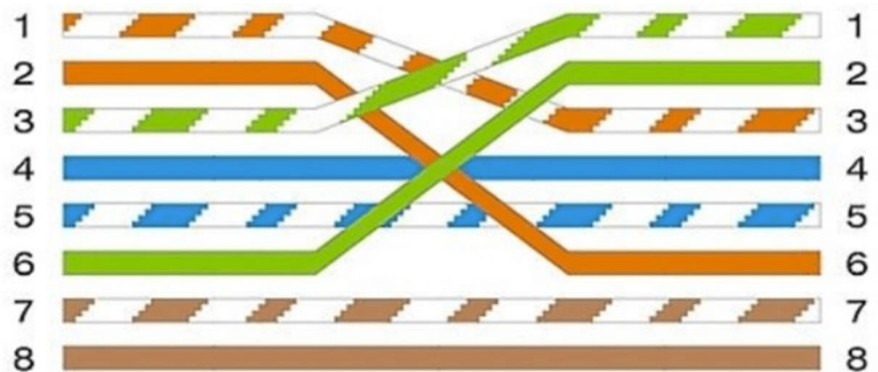


Figure 11: Cross-over cable wiring..

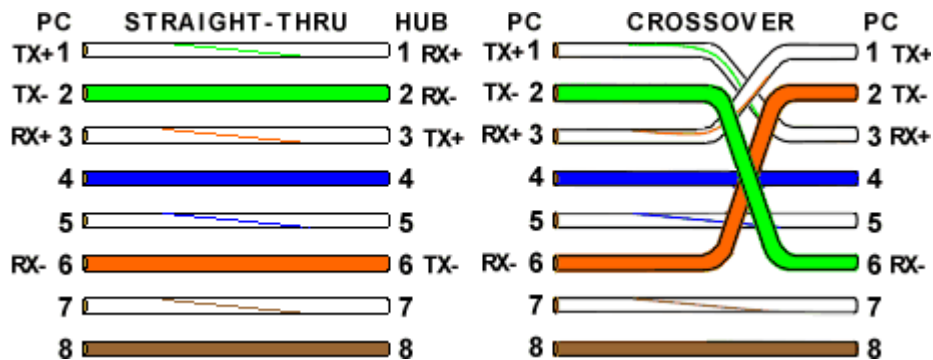


Figure 12: Straight through between PC and Hub, and Cross-over cable between PC and PC.

### 3) Rollover Cable

- ❖ A rollover cable is usually shipped with each Cisco device.
- ❖ It is called rollover because the wires on one end are rolled at the other end – the wire at pin 1 connects to the pin 8 on the other side, the wire at pin 2 to the pin 7, etc., as shown in Figure 13.
- ❖ This cable connects a serial port on your computer to the console port of the device and it is used for the device's initial configuration. The connection to the computer is made by plugging the DB-9 connector into an available EIA/TIA 232 serial port on the computer and the RJ-45 to the console interface on the router, as shown in Figure 14.

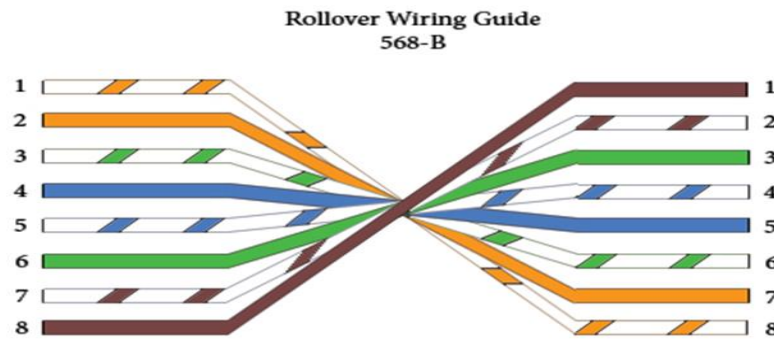


Figure 13: Rollover cable.

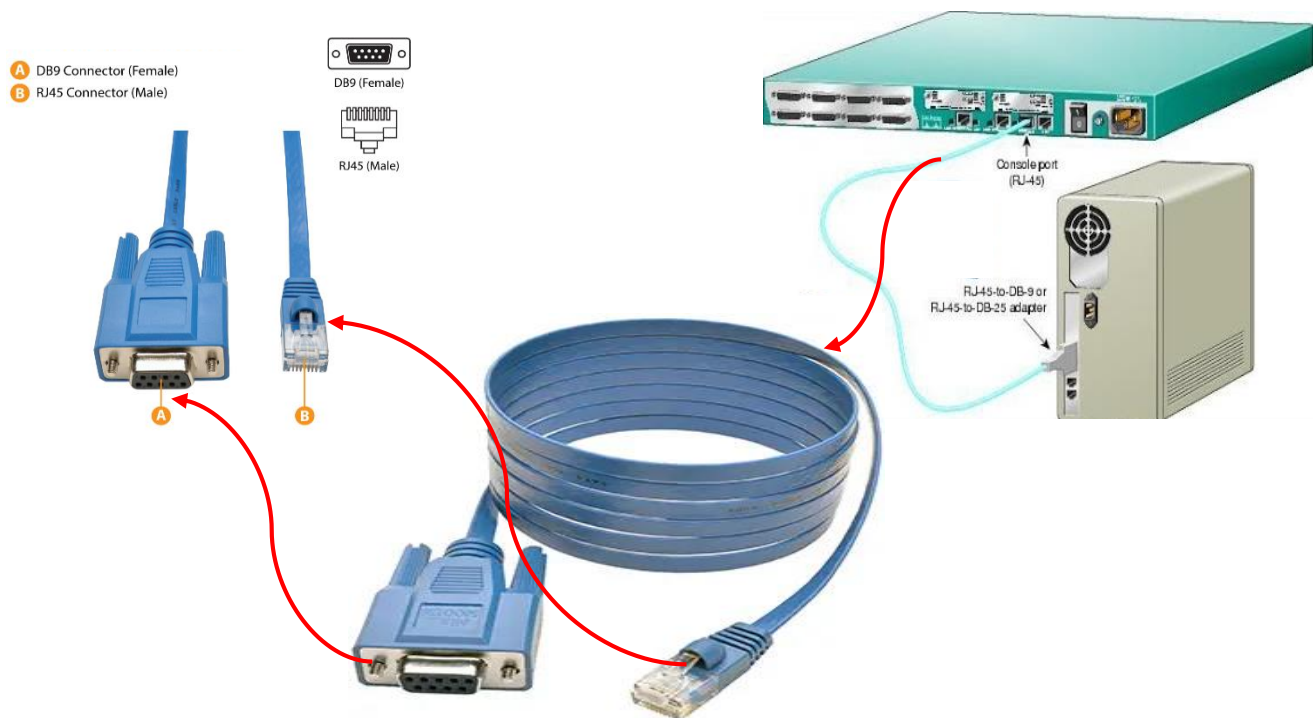


Figure 14: Rollover cable connection between PC and router.

#### v. Communication via a WAN connection (serial cable between two routers)

In the lab experiments, you may be using Cisco routers with one of two types of physical serial cables. Figure 15 shows the serial connection in the routers. Both cables use a large Winchester 15 Pin connector on the network end. This end of the cable is used as a V.35 connection to a Physical layer device such as a CSU/DSU. The first cable type has a male DB-60 connector on the Cisco end and a male Winchester connector on the network end. The second type is a more compact version of this

cable and has a Smart Serial connector on the Cisco device end. It is necessary to be able to identify the two different types in order to connect successfully to the router.

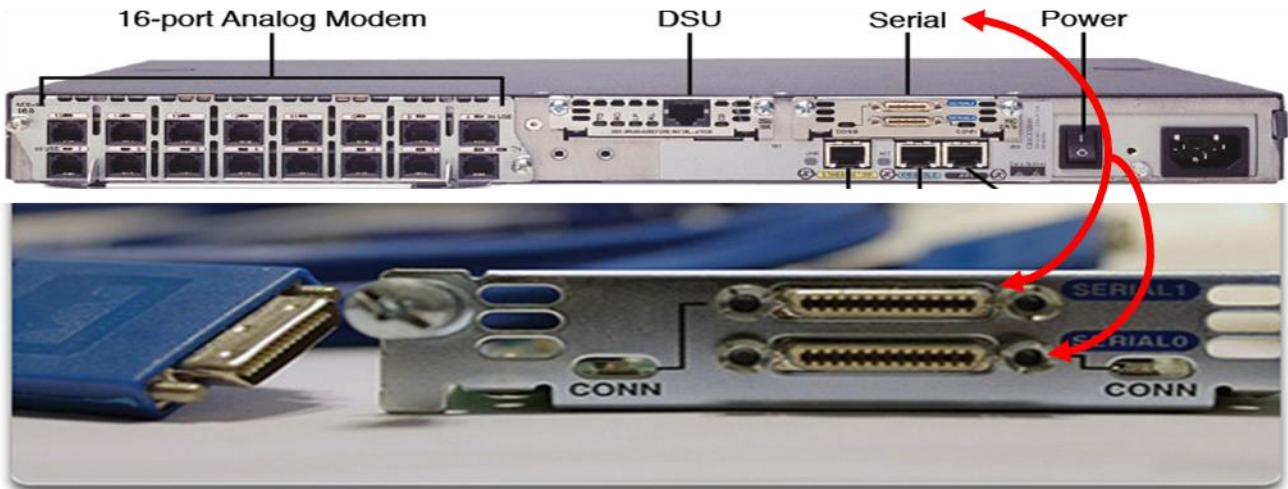


Figure 15: Serial connection in routers.

➤ **The main differences between DTE and DCE as a serial cable:**

- Recommended Standard 232 (RS-232) is a standard introduced for serial communication transmission of data. It formally defines signals connecting between a DTE such as a computer terminal and a DCE, such as a modem. Figure 16 represents a serial cable that contains DCE and DTE ends.



Figure 16: DCE and DTE ends on a serial cable.

- DCEs and DTEs are used in WAN connections. One side of the link (DCE) has to generate and transmit the clock signal, which controls the data rate, and the other side (DTE) receives the clock signal. In most cases, the ISP provides the clocking rate that synchronizes the transmitted signal.
- If a serial connection is made directly to a service provider or to a device that provides signal clocking such as a CSU/DSU, the router is considered to be DTE and will use a DTE serial cable.
- In the Packet Tracer simulator: the DCE cable, (red zigzag with clock) the side you click first will be the DCE, the second will be DTE. With the DTE cable (red zigzag no clock) the side you click first will be DTE, the second will be DCE, whichever way you do it, you'll see one side of the cable shows the clock symbol: this is the DCE, as shown in Figure 17.

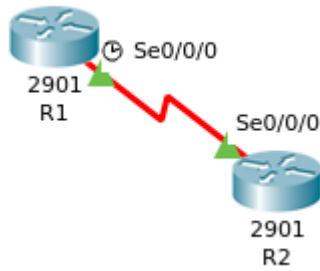


Figure 17: The representation of DCE and DTE ends for a serial cable on Packet Tracer.

## b) Coaxial Cable

Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted-pair cable, in part because the two media are constructed quite differently. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover (see Figure 18).

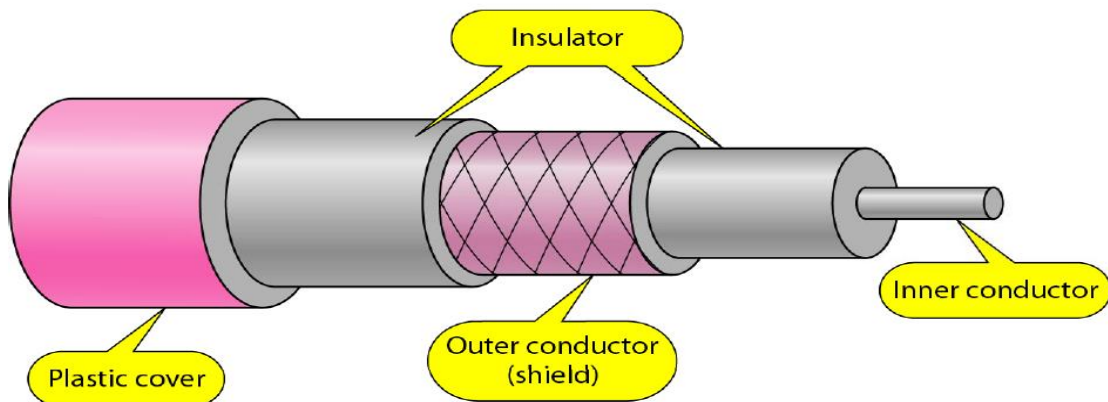


Figure 18: Coaxial cable.

Coaxial cables are used in many applications, such as: Television distribution (i.e., cable TV), long distance telephone transmission, which carry 10,000 voice calls simultaneously, but now this is being replaced by fiber optic, short distance computer system links (i.e., LANs).

## c) Fiber-Optic Cable

**A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.** To understand optical fiber, we first need to explore several aspects of the nature of light. Light travels in a straight line as long as it is moving through a single uniform substance. If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes direction.

### i. Optic fiber cable architecture.

Figure 19 shows the main components of fiber optic cable.

#### Optical Fiber → Architecture:

- Core
  - Glass or plastic with a higher index of refraction than the cladding
  - Carries the signal
- Cladding
  - Glass or plastic with a lower index of refraction than the core
- Buffer (one type of component made from plastic)
  - Protects the fiber from damage and moisture
- Jacket
  - Holds one or more fibers in a cable

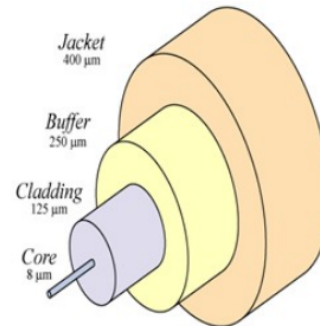


Figure 19: Optic fiber cable architecture.

### ii. Propagation Modes

Current technology supports two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics, which are Single mode and Multi-mode which can be implemented in two forms: step-index or graded-index (see Figures 20, 21)

There are two forms of fiber optic cable: multimode and single mode.

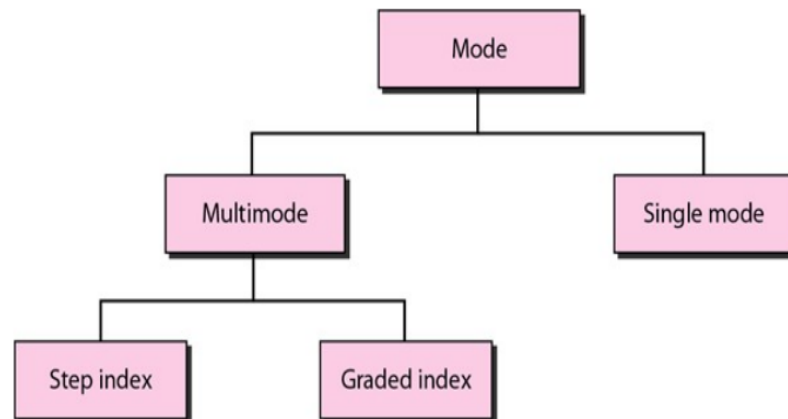


Figure 20: Optic fiber cable modes.

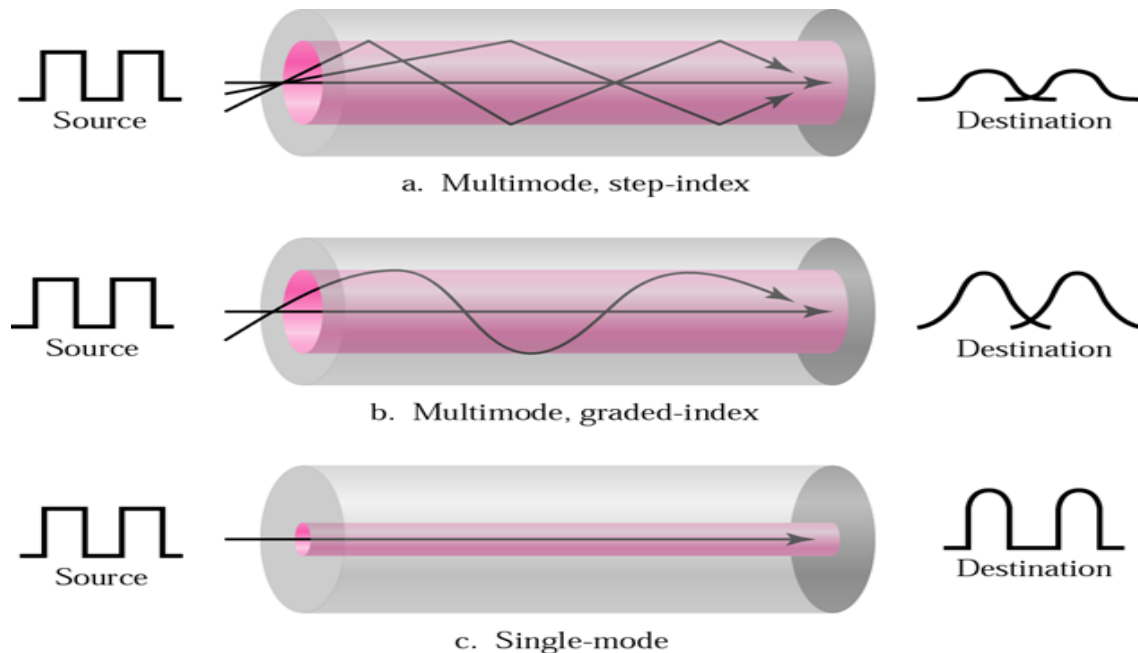


Figure 21: Optic fiber cable modes.

### iii. Advantages and disadvantages of Optical Fiber

The following is a summarization of the advantages and disadvantages of fiber optic:

- **The major advantages** offered by fiber-optic cable over twisted-pair and coaxial cable are:
  - **Noise Resistance:** Because fiber-optic transmission uses light rather than electricity, noise is not a factor. External light, the only possible interference, is blocked from the channel by the outer jacket.
  - **Less signal attenuation:** Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for miles without requiring regeneration.
  - **Higher bandwidth:** Currently, data rates and bandwidth utilization over fiber-optic cable are limited not by the medium but by the signal generation and reception technology available.
- **The main disadvantages of Optical Fiber:**
  - **Cost:** Fiber-optic cable is expensive. Also, a laser light source can cost thousands of dollars, compared to hundreds of dollars for electrical signal generators.
  - **Installation/maintenance:** Since it is a relatively new technology, its installation and maintenance require expertise that is not yet available everywhere.
  - **Fragility:** Glass fiber is more easily broken than wire, making it less useful for applications where hardware portability is required.



## **Part III: Network Devices**

A network device is a hardware device that is used to connect computers, laptop, smartphones, printers, scanners with one another. Several examples of these network devices: NIC, Repeater, Hub, Bridge, Switch, Router, and Gateway. Based on that, Figure 22 demonstrates that there are five categories of network devices which can be defined as:

- Those which operate below the physical layer such as a passive hub.
- Those which operate at the physical layer (a repeater or an active hub).
- Those which operate at the physical and data link layers (a bridge or a two-layer switch).
- Those which operate at the physical, data link, and network layers (a router or a three-layer switch).
- Those which can operate at all five layers (a gateway).

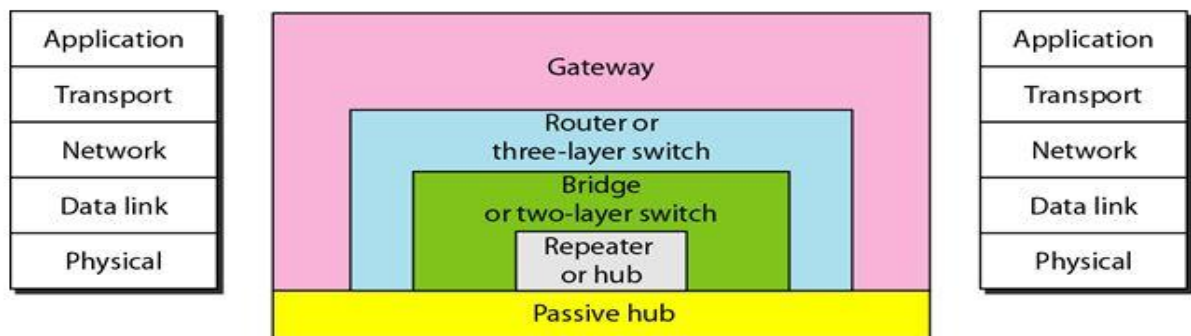


Figure 22: Network devices works on different layers.

### **A. Network Interface Card (NIC)**

- NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed on the mother board to establish a LAN (see Figure 23).
- Computer data is translated into electrical signals send to the network via NICs.
- It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and router or modem.
- NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model.



Figure 23: NIC components.

## B. Repeaters

- A repeater is a device that boosts/regenerate the data signals of the network. If a data signal travels a long distance, then it becomes weak or corrupted. To make the signal in its original shape we use the repeater. It is cheaper than other network devices (See Figure 24).
- The repeater is unable to connect dissimilar network.
- Repeater operates only on the physical layer. It has two ports. It forwards every frame without filtering.



Figure 24: Repeater.

## C. Hubs

- A hub is a physical layer device, serves as a central point to which all of the hosts in a network connect to (See Figure 25).
- A Hub has no concept of Ethernet frames or addressing (Hubs do not process or address packets; they only send data packets to all connected devices. It simply receives a signal from one port and sends it out to all other ports.
- Hubs are sometimes called multiport repeaters; it repeats what it receives on one ports to all other ports.
- There are two types of Hubs:
  - ✓ **Active Hub:** These are the hubs that have their own power supply and can clean, boost, and distribute the signal along with the network. It serves both as a repeater as well as a wiring center.
  - ✓ **Passive Hub:** It is just a connector. It connects the wires coming from different branches. These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs transmit signals onto the network without cleaning and boosting them.
- **Hubs have numerous disadvantages, such as:**
  - ✓ They are not aware of the traffic that passes through them, since it broadcast all data to all computers attached to the hub.
  - ✓ They create only **one large collision domain**, since the hub cannot filter the data. It has only **one broadcast domain**.
  - ✓ **A hub typically operates in half duplex** meaning that one computer either sends or receive a message at a time. Computers cannot send and receive data simultaneously.
  - ✓ There is also a security issue with hubs since the traffic is forwarded to all ports (except the source port), which makes it possible to capture all traffic on a network with a network sniffer!
  - ✓ If there occurs any problem in the hub, then the whole network stops working.



Figure 25: Hub.

## D. Bridges

- A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination (See Figure 26).
- It is also used for interconnecting two LANs working on the same protocol.
- It has a single input and single output port, thus making it a 2-port device.

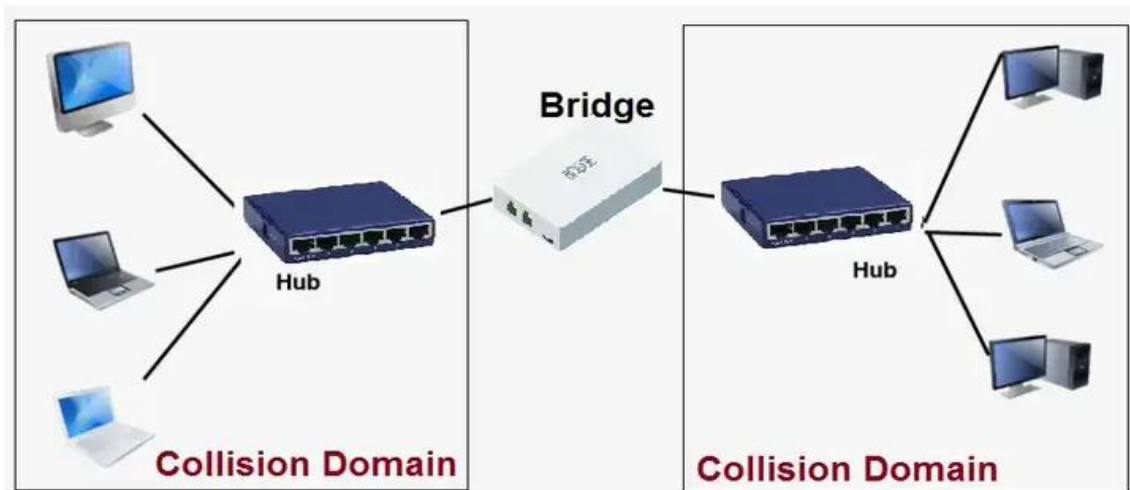


Figure 26: Bridge.

## E. Switches

- Switch is a multiport bridge with a buffer (See Figure 27). A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only.
- In other words, the switch divides the collision domain of hosts (**Each port on a switch is a separate collision domain**), but **broadcast domain remains the same**.
- **It stores the MAC address** of all the connected devices and upon receiving a message from the sender it first checks the MAC address of the message and then sends the message to the receiver that matches the MAC address.
- Switch do unicast meaning it sends a message to only one receiver and not a broadcast message. It has high security than a hub.
- **Also, the switch uses full-duplex** transmission mode meaning computers can send/receive a message simultaneously.

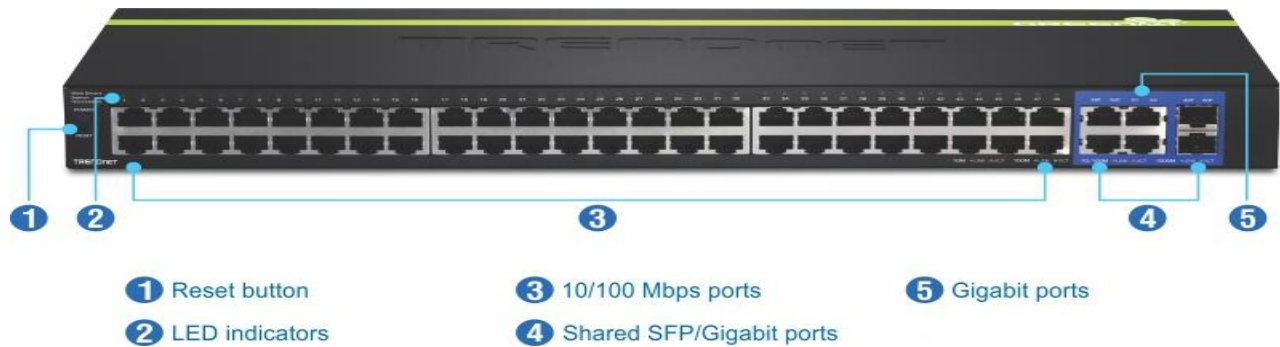


Figure 27: Switch and its physical ports.

## F. Routers

- A router is a three-layer device that routes data packets based on **their IP addresses** from one network to another (See Figure 28).
- Routers normally connect LANs and WANs together in the Internet and have a dynamically updating routing table based on which they make decisions on routing the data packets using routing protocols.
- **Router divide broadcast domains** of hosts connected through it and have traffic filtering capabilities.
- Table 2 summarizes the main differences of hubs, switches, and routers.

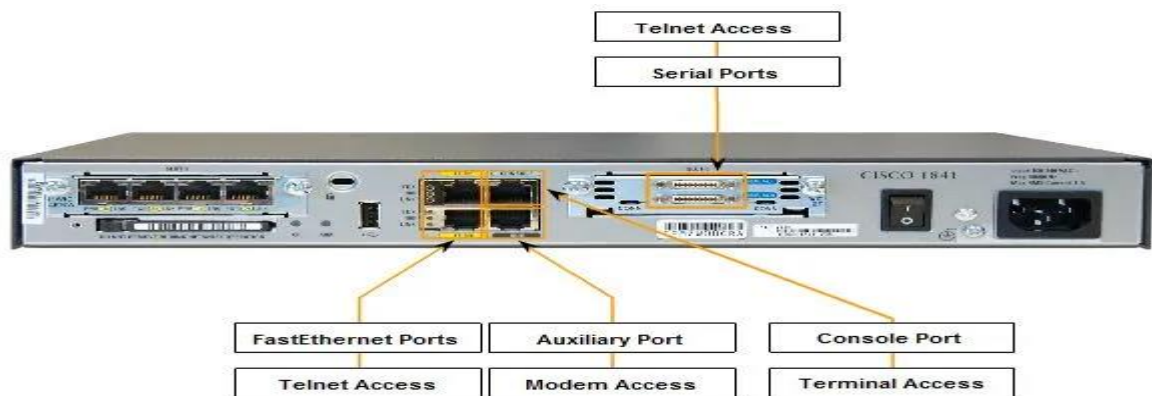


Figure 28: Router and its physical interfaces.

## G. Gateway

A gateway is normally a computer that operates in all five layers of the Internet or seven layers of OSI model. A gateway takes an application message, reads it, and interprets it. This means that it can be used as a connecting device between two internetworks that use different models. For example, a network designed to use the OSI model can be connected to another network using the Internet model. The gateway connecting the two systems can take a frame as it arrives from the first system, move it up to the OSI application layer, and remove the message.

Table 2: The difference between hub, switch, and routers.

Template	Hub	Switch	Router
Layer	Physical Layer	Data link layer	Network layer
Function	To connect a network of personal computer together through a central hub	Allow connections to multiple devices, manage ports and VLAN security	Direct data in a network
Data Transmission Form	Electrical Signal or bits	Frame & packet	Packet
Port	4/12 ports	Multi-port, usually between 4 and 48	2/4/5/8 ports
Transmission Type	Frame flooding, unicast, multicasts or Broadcast	First broadcast, then unicast and multicast	Ate initial level Broadcast then Uni- cast and Multicast
Device type	Non-intelligent device	Intelligent device	Intelligent device
Used in (LAN, MAN, WAN)	LAN	LAN	LAN, MAN, WAN
Transmission mode	Half duplex	Half/Full duplex	Full duplex
Speed	10Mbps	10/100 Mbps, 1Gbps	1-100Mbps(wireless) 1000Mbps-1Gbps (wired)
Address used for Data Transmission	MAC address	MAC address	IP address
Broadcast domain	Single	Single	Every interface has its own collision domain
Collision domain	Single	Every port has its own collision domain	Every interface has its own collision domain

## Part IV: The Internal Components of Router:

The router is an intelligent device; routers use routing algorithms such as Dijkstra's Algorithm to map the destination or to find the best route to a destination on the parameters like the number of hops. Below is the raw diagram (i.e., Figure 29) showing the internal components of the router, similar to a PC, a router also includes Central Processing Unit (CPU), Random-Access Memory (RAM), Read-Only Memory (ROM), flash memory, Nonvolatile RAM (NVRAM), and interfaces. The next subsections explain these components thoroughly.

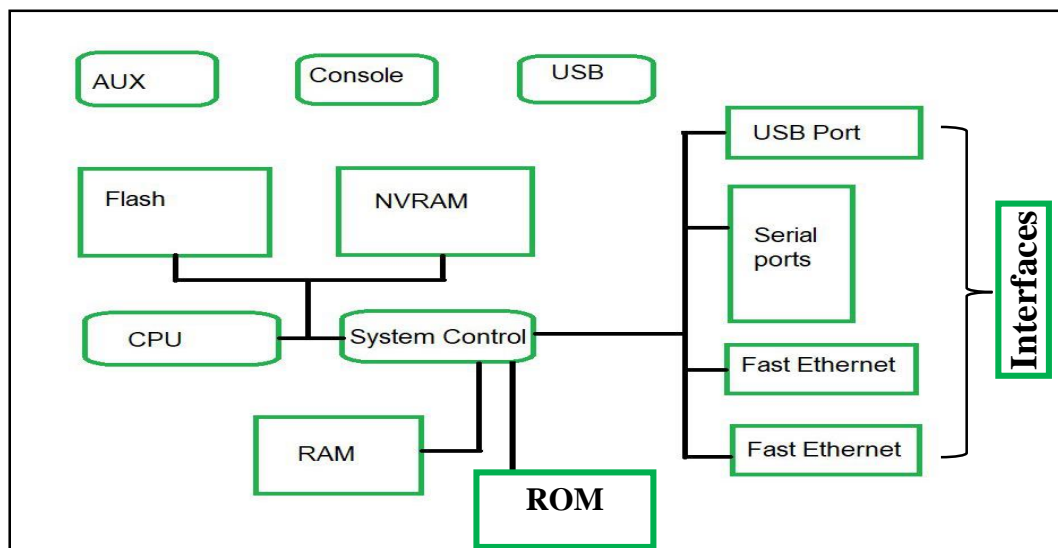


Figure 29: The internal components of router.



### A. CPU:

The CPU in the router executes the commands and processes the commands in the operating system. The flow of data on the interface is controlled by the CPU.

### B. ROM:

Read Only Memory in the router mainly works when the router boots up or is powered up. **It stores the bootstrap program needed when the router is turned on. Also, it stores Basic diagnostic software and Scaled-down version of IOS.** ROM does not lose its contents when the router power off or is restarted.

### C. RAM:

RAM in the router contains **the executable file and running file of the configuration file and** the contents are lost when the router's power is turned off.

### D. Flash Memory:

**It contains the operating system.** The data of the flash memory remain unchanged when the router is rebooted or powered off. So, **whenever the router is powered on the OS is loaded into RAM from flash memory.**

### E. NVRAM:

It is **a backup copy of the running configuration file.** Its functioning basically helps when the router loses power and the router needs to establish the configuration and load it again. The content of NVRAM is changeable. **When the router is powered on it searches the startup-config file in NVRAM only.**

### F. Interfaces / Ports:

If we want to connect the router with wire or we want a wired connection, there are multiple interfaces that are used to connect the network. i.e., Fast Ethernet, Gigabit Ethernet, and Serial, as shown in Figure 30. Additionally, Table 3 summarizes the ports of routers and their functions.

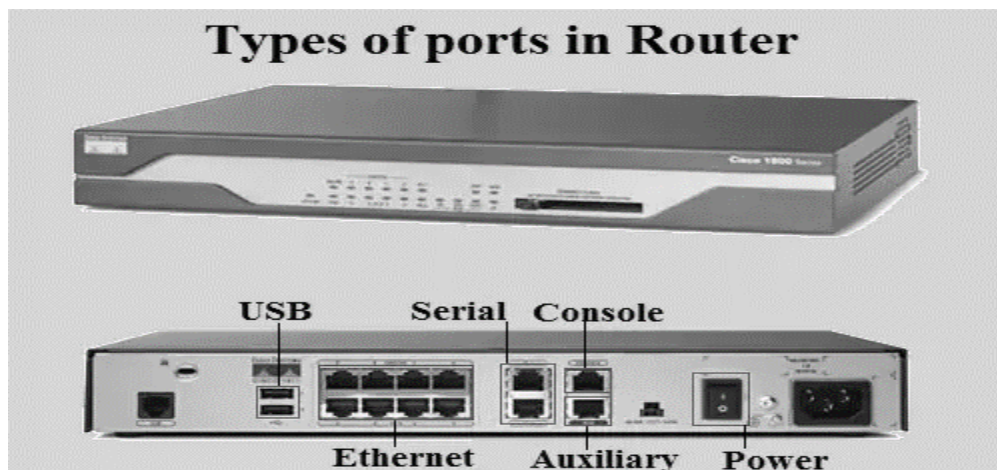


Figure 30: Types of ports in router.



Table 3: The router ports and their corresponding function.

Router Port	Function
Power Port	To provide Electricity.
Console Port	It provides to use to configure the router.
Ethernet Port	It is used to connect different network segment or LAN. It is 4 type – <ul style="list-style-type: none"> <li>• Ethernet Port (10 Mbps)</li> <li>• Fast Ethernet Port (100 Mbps)</li> <li>• Gigabit Ethernet Port (1 Gbps)</li> <li>• 10 Gigabit Ethernet Port (10 Gbps)</li> </ul>
Serial Port	It is used to connect another Router. It is 2 type – <ul style="list-style-type: none"> <li>• Serial Interface: - It has 60 pins to connect in fixed Router. Its speed is low.</li> <li>• Smart Serial Interface: - It has 26 pins to connect in modular Router. Its speed is Higher.</li> </ul>
Aux Port	It is used to connect modem.
USB Port	It is used to connect any USB devices.
BRI Port	To connect ISDN devices.

Technically speaking, these ports can be divided into:

### 1. Management ports

Routers have physical connectors that are used for router management. These connectors are known as management ports. **The most common management port is the console port.** The console port is used to connect a terminal, or most often a PC running terminal emulator software, to configure the router without the need for network access to that router. **The console port must be used during initial configuration of the router. Another management port is the auxiliary port.** Not all routers have auxiliary ports. The auxiliary port can be used in similar manner of the console port. **It can also be used to attach a modem.**

### 2. Network Interfaces

The term interface refers to a physical connector on the router whose main purpose is to receive and forward packets. Routers have multiple interfaces that are used to connect to multiple networks. Typically, the interfaces connect to various types of networks, which means that different types of media and connectors are required.

- **Ethernet interface:** Ethernet is typically IEEE 802.3 standard based physical interface of the router. The operating speed of the port is 10 Mbps. The media standard for this interface is 10BaseT.
- **Fast Ethernet interface:** The Fast Ethernet also is known is the FE interface. It is IEEE 802.3u standard based physical interface. The operating speed of Fast Ethernet is 100 Mbps. The media standard used for Fast Ethernet interface is 100BaseT.
- **Gigabit Ethernet interface:** Gigabit Ethernet is also known as GE interface. This ports standard is Ethernet IEEE 802.3ab. Gigabit Ethernet can connect at the remarkable speed of 1000mb/s. The media standard used is 1000BaseT.

- **Serial interfaces:** A serial interface is a communication interface between two digital systems that transmit data as a series of voltage pulses down a wire. Serial interfaces typically used for WAN connections from ISP to host. the serial interface provides connectivity types like Frame Relay, T1, T3, etc.

## **Part V: Device Configuration**

The basic user levels and modes for Cisco IOS are clarified in this section.

### **A. Overview of user levels and modes:**

As a security feature, Cisco IOS Software separates EXEC sessions into two different access levels: user EXEC level and privileged EXEC level. User EXEC level allows you to access only basic monitoring commands; privileged EXEC level allows you to access all router commands. Privileged EXEC level can be password protected to allow only authorized users the ability to configure or manage the router. From privileged EXEC level, you can access all the command modes. There are five command modes: global configuration mode, interface configuration mode, sub-interface configuration mode, router configuration mode, and line configuration mode.

### **B. Cisco IOS commands hierarchy**

After an EXEC session is established, commands within Cisco IOS Software are hierarchically structured. Understanding this hierarchy is important for successfully configuring a router. The following figure (i.e. Figure 31) illustrates a simple high-level schematic diagram of some Cisco IOS commands. This figure summarizes the different modes you will explore in the Network Labs in a later section.

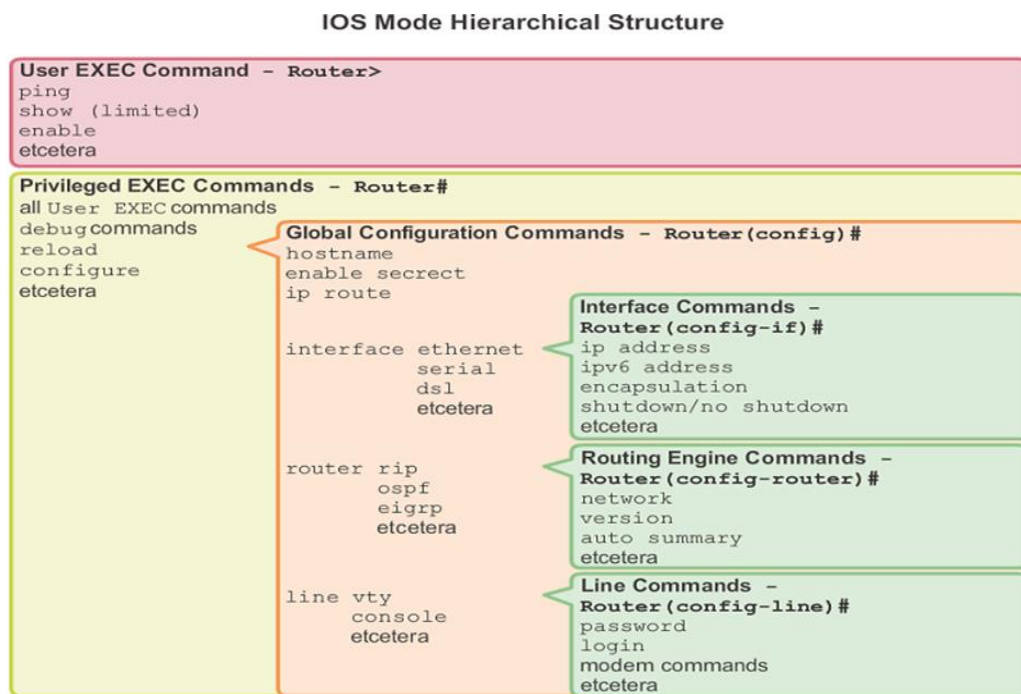


Figure 31: IOS mode hierarchical structure.

Figure 32 represents how do the Command options and applications vary, depending on your position within this hierarchy. Configuration command options are not available until you have navigated to the configuration branch of the Cisco IOS command-line interface (CLI) structure. When you are in the configuration branch, you may enter system-level configuration commands that apply to the entire router at the global configuration level. Interface-specific configuration commands are available when you switch to the interface configuration level.

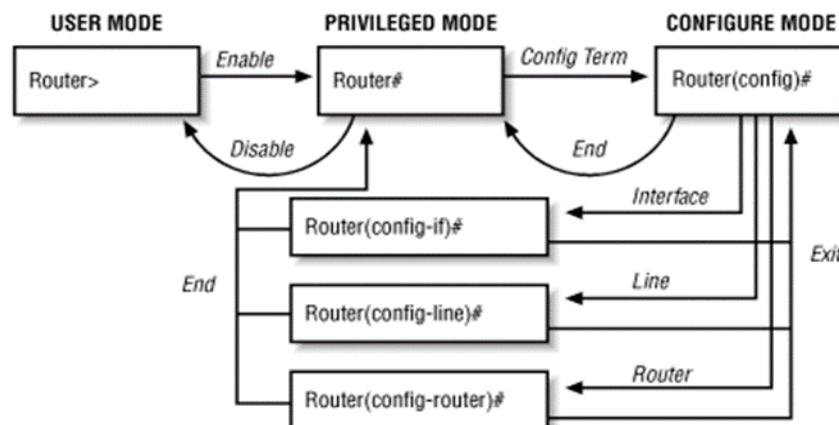


Figure 32: Command options and applications variation.

To assist you in navigation through the Cisco IOS CLI, the command prompt changes to reflect your position within the command hierarchy. This setup allows you to easily identify where within the command structure you are at any given moment. The following table (i.e., Table 4) is a summary of command prompts and the corresponding location within the command structure.

Table 4: Navigation through the Cisco IOS CLI.

<b>Router&gt;</b>	- User EXEC mode
<b>Router#</b>	- Privileged EXEC mode
<b>Router(config)#</b>	- Configuration mode (notice the # sign indicates this is accessible only at privileged EXEC mode)
<b>Router(config-if)#</b>	- Interface level within configuration mode
<b>Router(config-router)#</b>	- Routing engine level within configuration mode
<b>Router(config-line)#</b>	- Line level (vty, tty, async) within configuration mode

Here, many hot key commands are available while using the Cisco IOS CLI. A comprehensive list of hot keys is shown below in Table 5, outlining the function of each hot key.

Table 5: Cisco IOS CLI hot key commands

Hot Key	Function	Hot Key	Function
<b>Delete</b>	- Removes one character to the right of the cursor.	<b>Ctrl-U</b>	- Erases a line.
<b>Backspace</b>	- Removes one character to the left of the cursor.	<b>Ctrl-W</b>	- Erases a word.
<b>Tab</b>	- Finishes a partial command.	<b>Ctrl-Z</b>	- Ends configuration mode and returns to the EXEC mode.
<b>Ctrl-A</b>	- Moves the cursor to the beginning of the current line.	<b>Up Arrow</b>	- Allows user to scroll forward through former commands.
<b>Ctrl-E</b>	- Moves the cursor to the end of the line.	<b>Down Arrow</b>	- Allows user to scroll backward through former commands.
<b>Ctrl-R</b>	- Redisplays current line.	<b>Ctrl-Shift-6</b>	- Allows user to interpret an IOS process.

As we mentioned previously, EXEC sessions for Cisco IOS Software are divided into two different access levels: user EXEC level and privileged EXEC level. From the privileged EXEC level, you can access all the command modes. There are five command modes: global configuration mode, interface configuration mode, sub-interface configuration mode, router configuration mode, and line configuration mode. The following sub-sections demonstrate each mode thoroughly.

### 1. User EXEC mode

- Logging in to the router places you in user EXEC command mode (unless the system is configured to take you immediately to privileged EXEC mode).
- The Exec commands available at the user level are a subset of those available at the privileged level. In general, the user EXEC commands allow you to connect to remote devices, change terminal line settings on a temporary basis, perform basic tests, and list system information.
- **Configuration parameters cannot be read or modified in this mode.**
- The user EXEC mode prompt consists of the hostname of the device followed by an angle bracket (>), as shown in the following example: `Router>`
- To list the commands available in user EXEC mode, enter a question mark (?).

### 2. Privileged EXEC Mode

- The privileged EXEC command set includes those commands contained in user EXEC mode. Privileged EXEC mode also provides access to configuration modes through the `configure` command, and includes advanced testing commands, such as `debug`.
- To access privileged EXEC mode, use the following command: `Router> enable`
- After typing `enable`, you enter the privileged EXEC mode prompt, which consists of the hostname of the device followed by a pound sign (#), as shown in the following example: `Router#`
- **The privileged EXEC mode is used to read configuration files, reboot the router, and set operating parameters.**
- To exit from privileged EXEC mode to user EXEC mode, type: `Router1#disable`
- To list the commands available in privileged EXEC mode, issue the (?) command at the prompt.
- From privileged EXEC mode you can access global configuration mode, which is described in the following section.

### 3. Global Configuration Mode

- The term "global" is used to indicate characteristics or features that affect the system as a whole.
- Global configuration mode is used to configure your system globally, or to enter specific configuration modes to configure specific elements such as interfaces or protocols.
- To access global configuration mode, use the following command in privileged EXEC mode:

```
Router# configure terminal
```

- Note that the system prompt changes to indicate that you are now in global configuration mode. The prompt for global configuration mode consists of the hostname of the device followed by (config) and the pound sign (#). The following example shows the process of entering global configuration mode from privileged EXEC mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

- To list the commands available in privileged EXEC mode, issue the (?) command at the prompt.
- Commands entered in global configuration mode update the running configuration file as soon as they are entered. In other words, changes to the configuration take effect each time you press the Enter or Return key at the end of a valid command. However, these changes are not saved into the startup configuration file until you issue the `copy running-config startup-config` command in EXEC mode. This behavior is explained in more detail later in this lab.
- From global configuration mode, you can enter a number of protocol-specific, platform-specific, and feature-specific configuration modes. Information about specific modes is given in task-specific contexts throughout the Cisco IOS software documentation set.
- Interface configuration mode, described in the following section, is an example of a configuration mode you can enter from global configuration mode.

#### 4. Interface Configuration Mode

- One example of a specific configuration mode you enter from global configuration mode is interface configuration mode.
- Many features are enabled on a per-interface basis. Interface configuration commands modify the operation of an interface such as an Ethernet, FDDI, or serial port.
- Interface configuration commands always follow an interface command in global configuration mode, which defines the interface type.
- Bandwidth or clock rate are examples of interface configuration commands that affect general interface parameters.
- To access and list the interface configuration commands, use the following command:

```
Router(config)# interface type number
```

- In the following example, the user enters interface configuration mode for serial interface 0/1. The new prompt, `hostname(config-if)#`, indicates interface configuration mode.

```
Router(config)# interface serial 0/1
Router(config-if)#
```

- To exit interface configuration mode and return to global configuration mode, enter the exit command.
- **To Configure the router interface with IP address and subnet mask, and activate it, use the following commands.**

```
Router1(config)# interface s0/1
Router1(config-if)# ip address [insert ip address]
[insert subnet mask]
Router1(config-if)# no shutdown
Router1(config-if)# end
Router1#
```

## **Part VI: Address Resolution Protocol (ARP) and Internet Control Message Protocol (ICMP)**

In this section, we'll go over addressing, including IPv4, IPv6, and MAC addresses, as well as why we need supporting protocols for Network layer protocol (i.e., IP). Then later, in separate sub-sections, we cover the two types of supporting protocols, namely, ARP and ICMP.

### **A. Addressing**

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical (MAC) addresses, IP addresses, port addresses, and specific addresses. The hosts and routers are recognized **at the network level by their logical (IP) addresses**. However, packets pass through physical networks to reach these hosts and routers. **At the physical level, the hosts and routers are recognized by their physical addresses.**

**MAC Addresses:** is the address of a node as defined by its LAN or WAN. It is included in the frame used by the data link layer. The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC). Most local-area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below:

MAC address: 07:01:02:01:2C:4B

**An IPv4 address:** is a 32-bit address (4-bytes) that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet. The address space of IPv4 is ( $2^{32}$ ) or 4,294,967,296. To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. The following is the dotted decimal notation:

IPv4 address: 117.149.29.2

**An IPv6 address** is 128 bits long and is arranged in eight groups, each of which is 16 bits. Each group is expressed as four hexadecimal digits and the groups are separated by colons. The address space of IPv6 is ( $2^{128}$ ). An example of a full IPv6 address could be:

IPv6 address: FE80:CD00:0000:0CDE:1257:0000:211E:729C

### **B. Why we need supporting protocols?**

At the network layer, TCP/IP supports the Internetworking Protocol (IP), in turn, uses four supporting protocols: **ARP**, **RARP**, **ICMP**, and **IGMP**, as shown in Figure 33. IP is the transmission mechanism used by the TCP/IP protocols. **It is an unreliable and connectionless protocol (a best-effort delivery service).** Interestingly, the term best effort means that IP provides **no error checking or tracking**. Thus, IP lacks some features such as **flow control and error control**. Additionally, IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees. To resolve these issues, two supporting protocols were introduced, which are:

- **ARP:** We need ARP to create a mapping between physical and logical addresses. IP packets use logical addresses. These packets, however, need to be encapsulated in a frame, which needs physical addresses.



- **ICMP:** Lack of flow and error control in the IP has resulted in using ICMP that provides alerts. It reports congestion and some types of errors in the network or destination host.

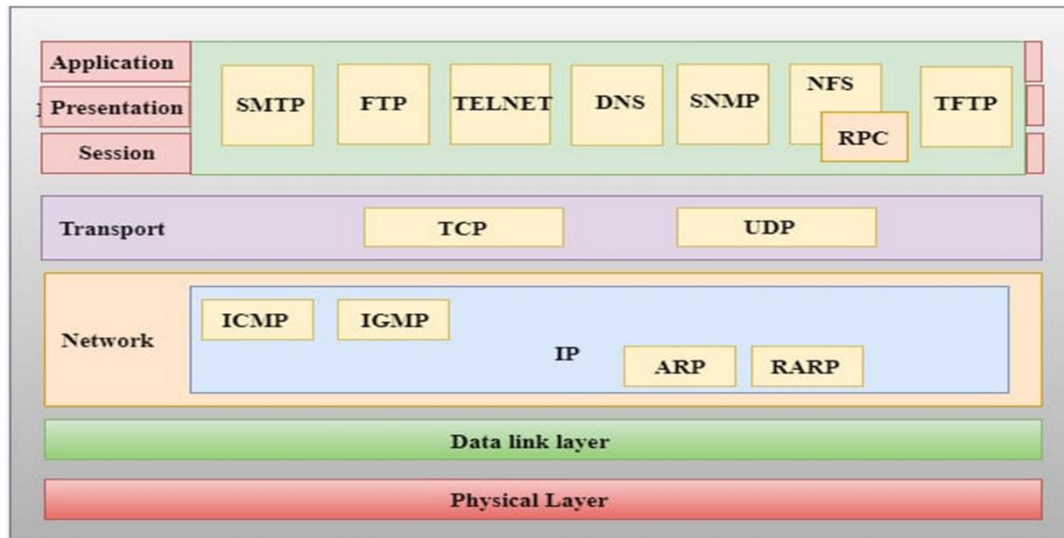


Figure 33: The position of ARP and ICMP protocols in the OSI layers model.

## C. ARP

In this section we review the major aspects of ARP, including ARP definition, ARP functions, Types of ARP messages, how ARP works, and removing ARP table cache.

### 1. ARP definition and its types:

The network that uses ARP to map IPv4 addresses to MAC addresses. This section explains how ARP works.

- Every IP device on an Ethernet network has a unique Ethernet MAC address. When a device sends an Ethernet Layer 2 frame, it contains these two addresses:
  - **Destination MAC address:** MAC address of the target device on the same local network segment. If the target host is on a different network, the frame's destination address is that of the default gateway (i.e., router).
  - **Source MAC address:** The MAC address of the source host's Ethernet NIC.
- To transmit a packet to another host on the same local IPv4 network, the host must know the target device's IPv4 address as well as its MAC address. Device destination IPv4 addresses are either known or resolved by device name. Nevertheless, MAC addresses must be determined.
- When a device knows its IPv4 address, it may utilize ARP to discover the target MAC address of a local device. Thus, **ARP is used to find the physical address of the node when its IP address is known.**
- **ARP performs two basic functions:** Resolving IPv4 addresses to MAC addresses and keeping a table of IPv4 to MAC address mappings.
- Mapping an IP address to its corresponding MAC address and vice versa can be done by using either **static or dynamic mapping.**

- **Static mapping:** It is a map where **someone manually** enters the IP to MAC address association by using the ARP command utility. This table is stored in each machine on the network. Each machine that knows, for example, the IP address of another machine but not its physical address, can look it up in the table.
- **Dynamic mapping:** It is a map which is **created automatically** when the sender broadcast its message to the entire network. **Dynamic entries are not permanent, and they are removed periodically.** Each time a machine knows one of the two addresses (logical or physical), it can use a protocol to find the other one.

## 2. Types of ARP messages:

There are two types of ARP messages, which are classified as follow:

### a) ARP Request:

When a device wants to discover the MAC address associated with an IPv4 address but does not have an entry for the IPv4 address in its ARP table, **it sends an ARP request.** ARP messages are directly wrapped within an Ethernet frame. There is no IPv4 header included. The following header information is used to encapsulate the ARP request in an Ethernet frame:

- **The destination MAC address:** is FF-FF-FF-FF-FF-FF, and all Ethernet NICs on the LAN must accept and process the ARP request.
- **The source MAC address:** is the MAC address of the user who sent the ARP request.
- **Type:** The type field in ARP messages is 0x806. This notifies the receiving NIC that the data portion of the frame must be forwarded to the ARP process.

**Because ARP requests are broadcasts, the switch floods all ports except the receiving port.** All Ethernet NICs on the LAN process broadcasts and must forward ARP requests to their respective operating systems for processing. Every device must analyze the ARP request to determine whether the destination IPv4 address is the same as its own. Broadcasts will not be forwarded to other interfaces by a router. Just one device on the Network will have an IPv4 address that corresponds to the IPv4 address specified in the ARP request. Other devices will not respond.

### b) ARP Reply:

Basically, **only the device with the corresponding target IPv4 address will respond with an ARP reply.** The following header information is used to encapsulate the ARP reply in an Ethernet frame:

- **The MAC address of the destination** is the same as the MAC address of the sender of the ARP request.
- **The source MAC address** is the MAC address of the user who sent the ARP reply.
- **The type field** in ARP messages is 0x806. This notifies the receiving NIC that the data component of the frame must be forwarded to the ARP process.

Accordingly, just the device that initiated the initial ARP request will get the unicast ARP response. After receiving the ARP response, the device will add the IPv4 address and accompanying MAC address to its ARP database. Packets destined for that IPv4 address can now be wrapped in frames using the MAC address associated with it. **If no device replies to the ARP request, the packet is discarded due to the inability to generate a frame.**

Kindly note that, ICMPv6 Neighbor Discovery (ND) is a technique equivalent to ARP for IPv4. Similar to IPv4 ARP requests and ARP replies, IPv6 employs neighbor solicitation and neighbor advertising messages, this topic will be explained and covered comprehensively in the coming experiments.

### 3. ARP functions

Anytime a host or a router has an IP datagram to send to another host or router, it has the IP address of the receiver. The IP address is obtained from the Domain Name Service (DNS) if the sender is the host, or it is found in a routing table if the sender is a router.

When a packet is transferred to the data link layer to be encapsulated into an Ethernet frame, the sender device looks for the MAC address of the receiver that is mapped to the IPv4 address in a table in its memory. **This information is called the ARP table or the ARP cache and is temporarily saved in RAM memory.**

The transmitting device will check in its ARP database for a destination IPv4 address and its corresponding MAC address. If the packet's destination IPv4 address is on the same network as the source IPv4 address, the device will look up the destination IPv4 address in the ARP table.

On the other hand, if the destination IPv4 address is not on the same network as the source IPv4 address, the sender device will look up the default gateway's IPv4 address in the ARP table. The search in both situations is for an IPv4 address and a MAC address for the device.

Each ARP table entry, or row, associates an IPv4 address with a MAC address. The relationship between the two values is called a map. Basically, this implies that you can look up an IPv4 address in the table and find the MAC address associated with it. The ARP table stores (caches) the mapping for the LAN devices momentarily. If the device finds the IPv4 address, the accompanying MAC address is utilized as the frame's destination MAC address. **If no entries are found, the device sends an ARP request.** We can check this empty ARP cache using a `arp -a` command, as shown in Figure 34(a). The packet includes the physical and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the physical address of the receiver, **the query is broadcast over the network.** Every device on the network receives and processes the ARP request packet, **but only the intended recipient recognizes its IP address and sends back an ARP reply packet.** The reply packet contains the recipient's IP and physical addresses. The packet is **unicast** directly to the inquirer by using the physical address received in the request packet and then the MAC address gets stored in the ARP cache.



Figure 34 (a): Case 1: ARP cache is empty.

Figure 34 (b) and Figure 34 (c) shows the ARP cache after receiving the MAC addresses. We can check the ARP cache using the two commands:

- For windows' command prompt, the `arp -a` command is used to display the ARP table, as shown in the Figure 34 (b).

- On a Cisco router's CLI, the `show ip arp` command is used to display the ARP table, as shown in the Figure 34 (c).

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

Interface: 192.168.1.10 --- 0x3
Internet Address      Physical Address      Type
192.168.1.1          74-da-da-db-f7-67    dynamic
192.168.1.11         fc-aa-14-ee-cc-c2    dynamic
192.168.1.14         18-60-24-bd-3d-1d    dynamic
192.168.1.32         1c-1b-0d-bd-d2-7e    dynamic
192.168.1.41         58-20-b1-40-b7-74    dynamic
192.168.1.55         fc-aa-14-a5-67-7a    dynamic
192.168.1.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250      01-00-5e-7f-ff-fa    static
255.255.255.255      ff-ff-ff-ff-ff-ff    static
```

Figure 34 (b): Case 2: ARP cache is filled on Windows' command prompt.

```
Router#sho ip arp
Protocol Address      Age (min)  Hardware Addr  Type   Interface
Internet 192.168.10.1    -          001b.10ae.7d00 ARPA   GigabitEthernet0/0.10
Internet 192.168.10.2    33         0050.7966.6800 ARPA   GigabitEthernet0/0.10
Internet 192.168.10.3    33         0050.7966.6801 ARPA   GigabitEthernet0/0.10
Internet 192.168.20.1    -          001b.10ae.7d00 ARPA   GigabitEthernet0/0.20
Internet 192.168.20.2    0          001b.10a0.2500 ARPA   GigabitEthernet0/0.20
Internet 192.168.20.3    33         0050.7966.6802 ARPA   GigabitEthernet0/0.20
Internet 192.168.30.1    -          001b.10ae.7d00 ARPA   GigabitEthernet0/0.30
Internet 192.168.30.2    2          001b.108c.8700 ARPA   GigabitEthernet0/0.30
Internet 192.168.30.3    11         0050.7966.6803 ARPA   GigabitEthernet0/0.30
Router#
```

Figure 34 (c): Case 3: ARP cache is filled on Cisco router' CLI.

The following example illustrates the operations of ARP (ARP request and reply) for a local network destination IPv4 address, where PC A needs to send a packet for PC C, as shown in Figures 35 (a) to 34 (h):

- PC A with IP address 192.168.1.110 prepares a packet for PC C which has an IP address 192.168.1.50 and needs to know the MAC address.

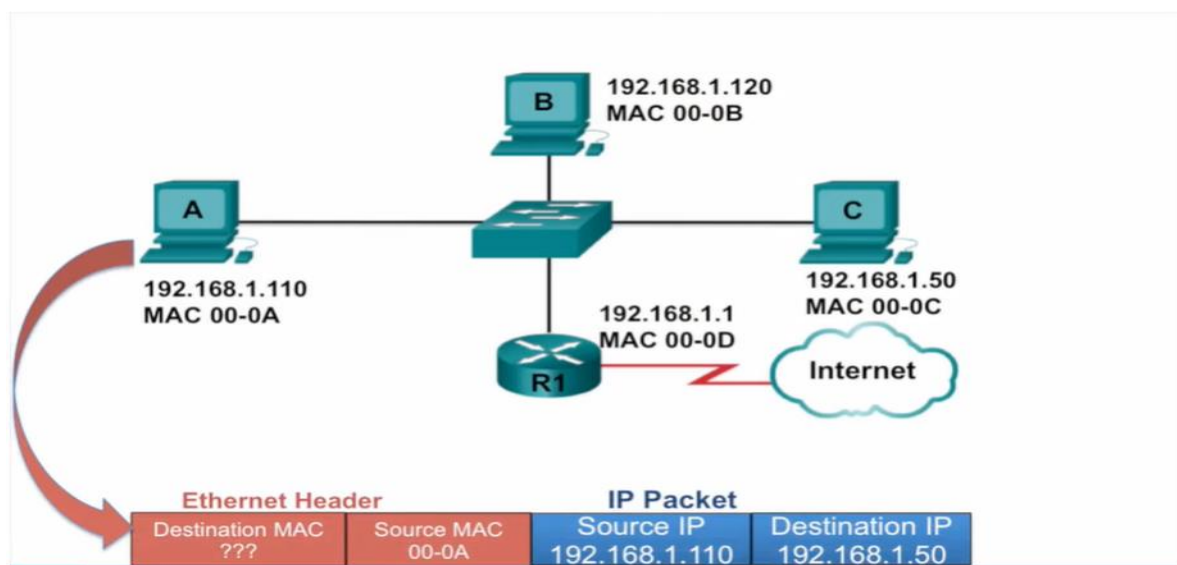


Figure 35 (a): The operations of ARP (ARP request and reply).



- 2) PC A checks its ARP cache to find the MAC address for IP address 192.168.1.50.

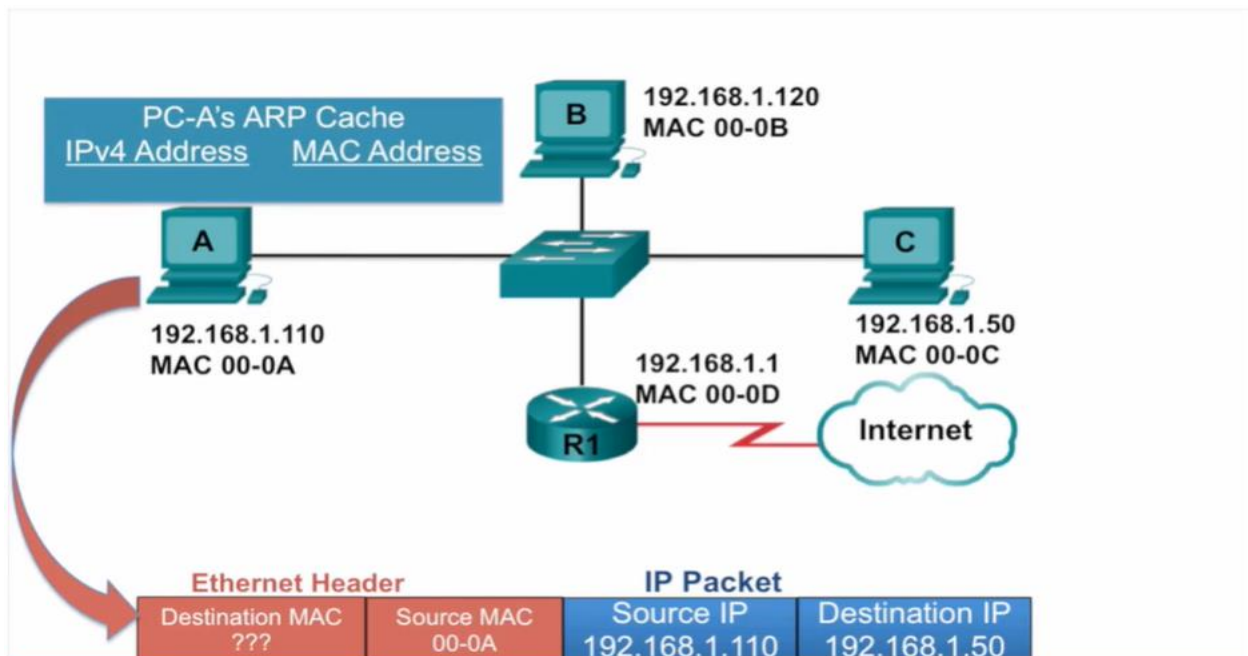


Figure 35 (b): The operations of ARP (ARP request and reply).

- 3) Because it is not in its ARP cache, it will put the packet on hold and **send an ARP request**. The **switch floods or broadcasts the ARP request** to all ports except the one from where the packet comes (i.e., sender).

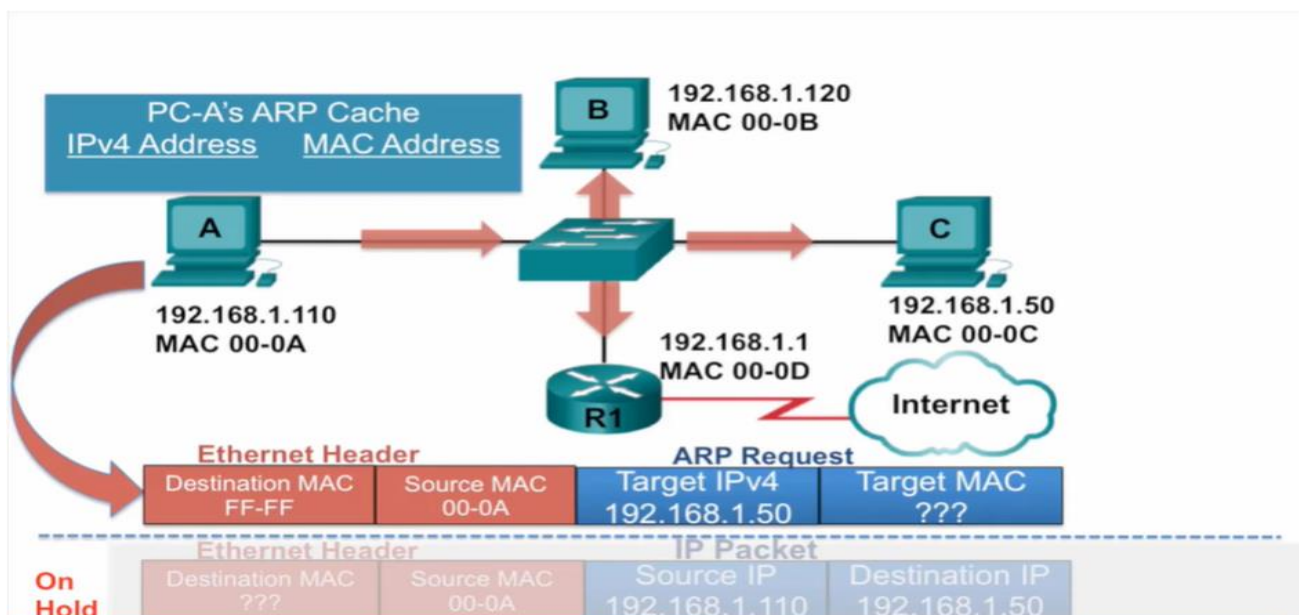


Figure 35 (c): The operations of ARP (ARP request and reply).

- 4) All PCs that received the ARP request will process the packet, compare their IPv4 with the target IP address, and realize that **this is not their IP address (no need to send an ARP reply).**

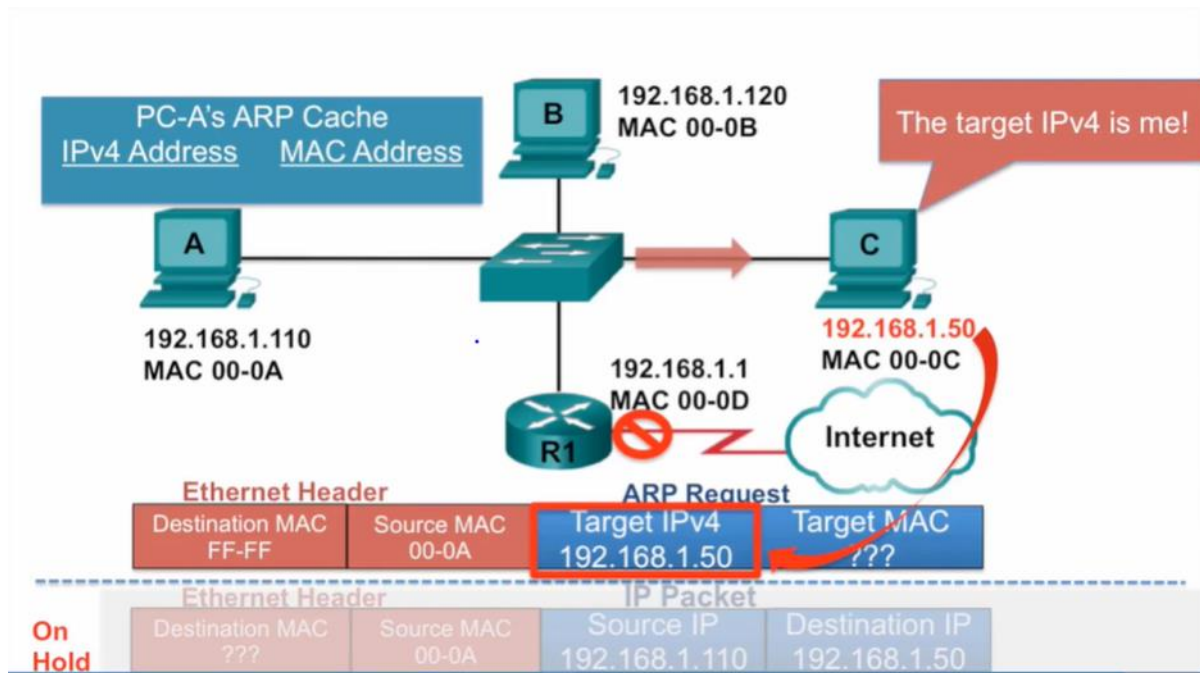


Figure 35 (d): The operations of ARP (ARP request and reply).

- 5) PC C receives the packet, compares its IPv4 address versus the target IP address in the packet, then realizes that its own IPv4 address, **so PC C needs to send an ARP reply.**

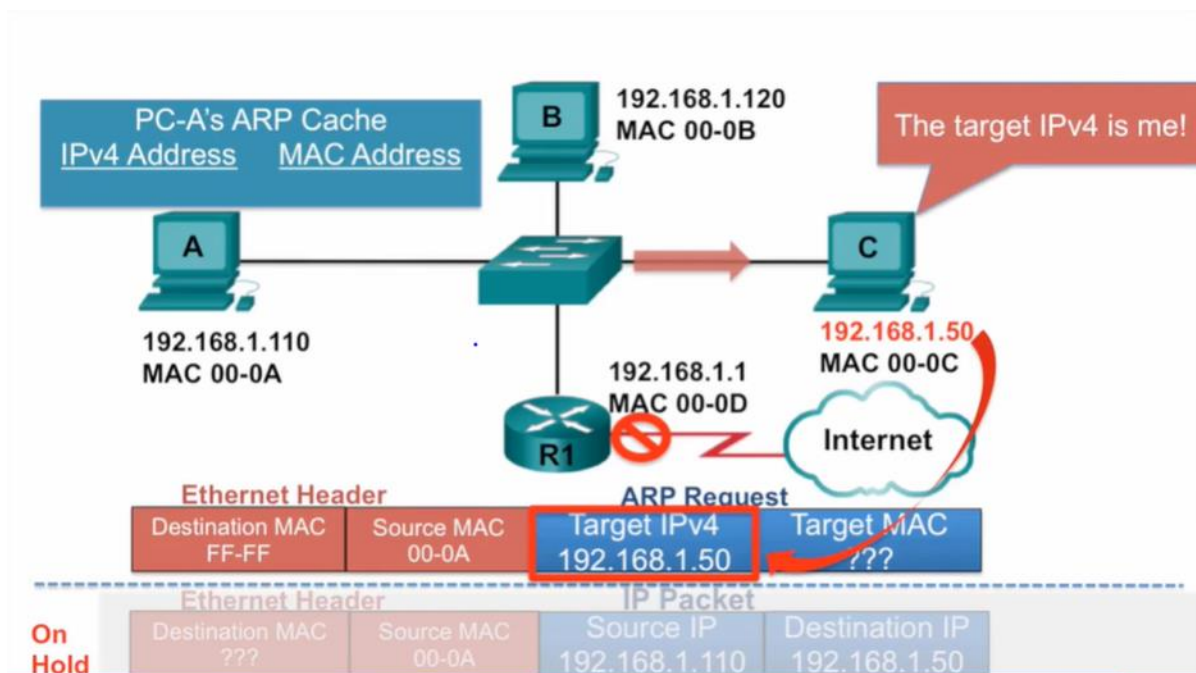


Figure 35 (e): The operations of ARP (ARP request and reply).



- 6) PC C creates **an ARP reply** that includes its MAC address, it is a unicast message send to **PC A**.

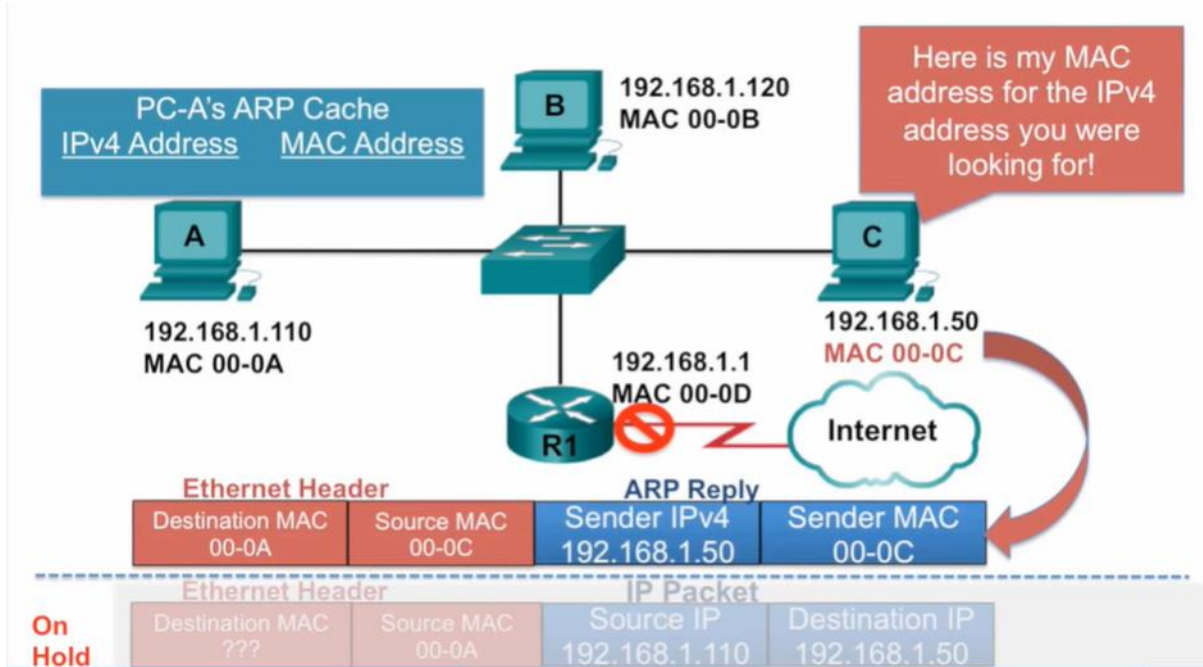


Figure 35 (f): The operations of ARP (ARP request and reply).

- 7) **PC A takes the sender IP and MAC addresses from the ARP reply** and adds them to its **ARP cache**, off hold the original packet to be sent to the destination.

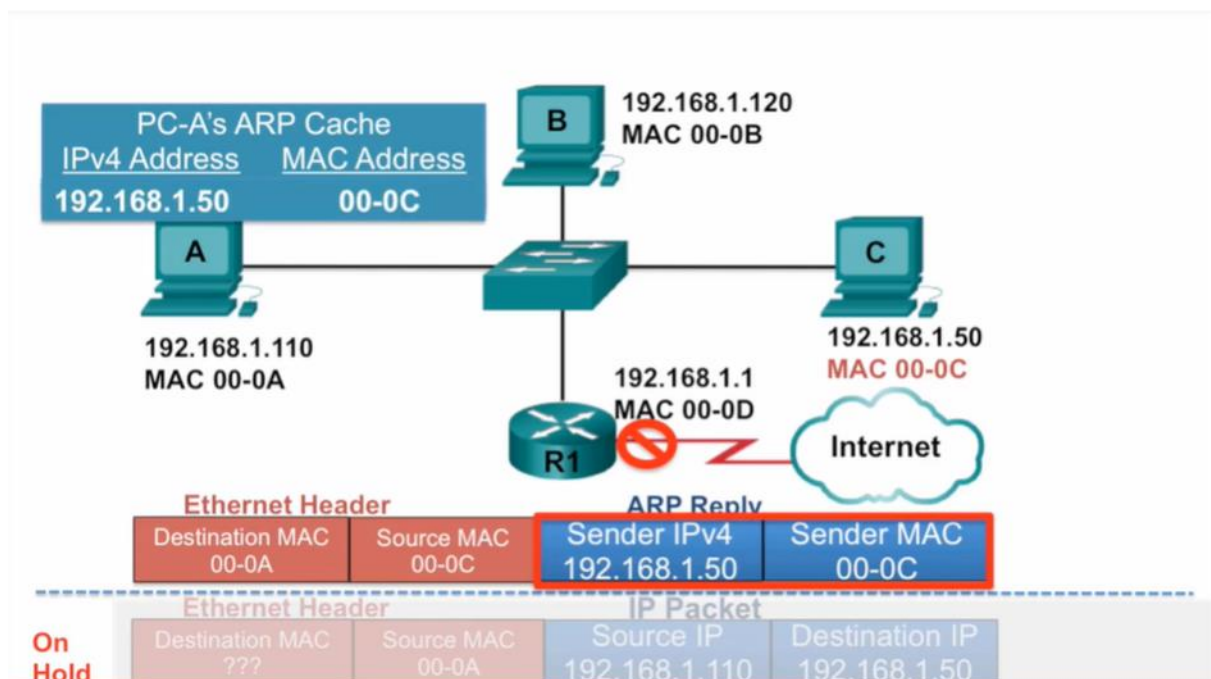


Figure 35 (g): The operations of ARP (ARP request and reply).

8) Finally, PC A adds the MAC address from its ARP cache to the Ethernet frame.

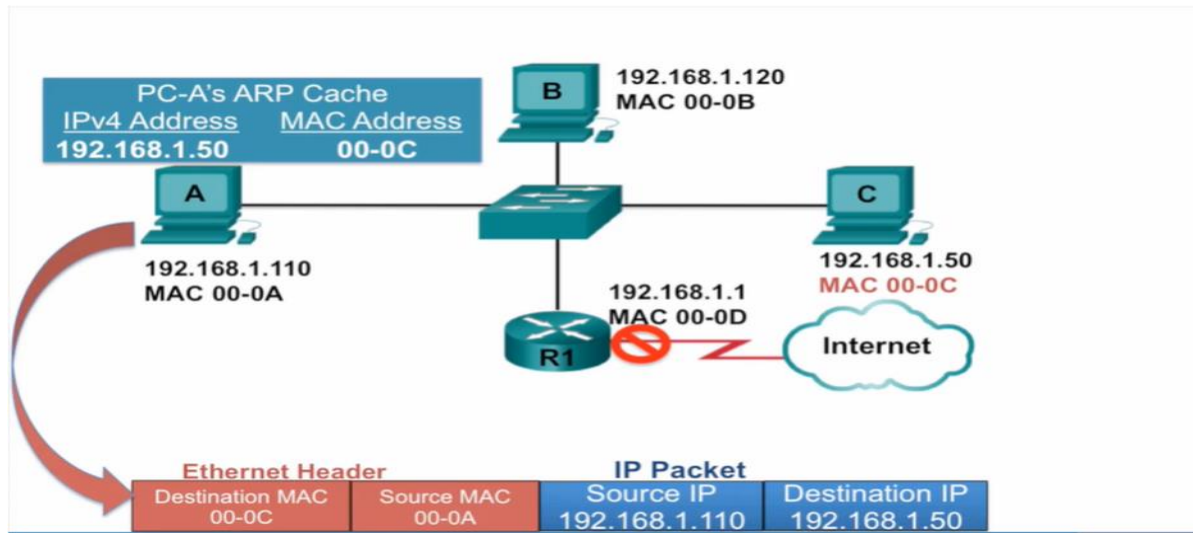


Figure 35 (h): The operations of ARP (ARP request and reply).

#### 4. Removing Entries from an ARP Table:

The ARP table entries are time stamped. If a device does not receive a frame from a specific device before the date expires, the device's record in the ARP table is deleted. Static map entries can also be stored in an ARP table, but this is rarely done. **Static ARP table entries do not expire and must be deleted manually.** An ARP cache timer for each device delete ARP entries that have not been utilized for a predetermined period of time. The times vary based on the device's operating system. As seen in the Figure 36, recent Windows operating systems save ARP table entries between 15 and 45 seconds.

The command `arp -d` can also be used to delete part or all of the entries from the ARP table manually. After removing an entry, the procedure of making an ARP request and getting an ARP reply must be repeated in order to put the map into the ARP table.

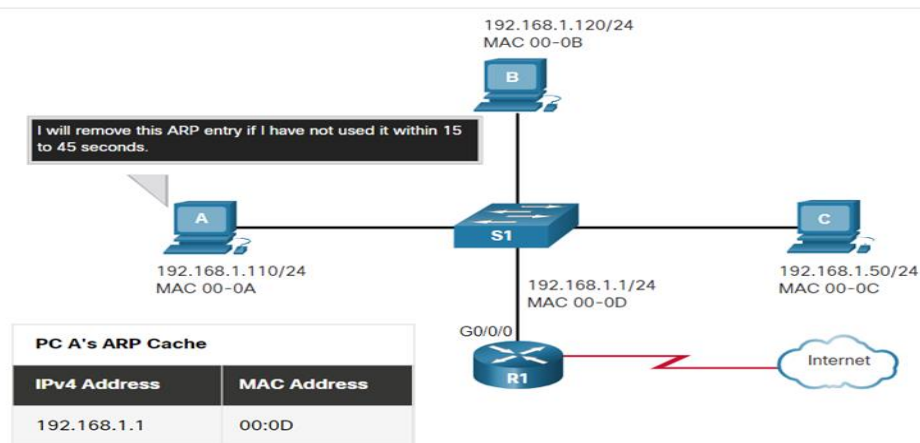


Figure 36: Delete ARP cache.

## D. ICMP

In this section, we illustrate the ICMP definition, the basic types of its messages, which are error reporting and query messages.

### 1. ICMP definition and its types:

The ICMP is a network layer protocol used by hosts and routers to send the notifications of IP datagram problems back to the sender (error control and flow control). Importantly, ICMP sends query and error reporting messages, as shown in Figure 37.

- **The error-reporting messages** report problems that a router or a host (destination) may encounter when it processes an IP packet (does not correct the error).
- **The query messages**, which occur in pairs, help a host or a network manager get specific information from a router or another host (diagnostic tool).

The next sub-sections discuss the two types of ICMP briefly.

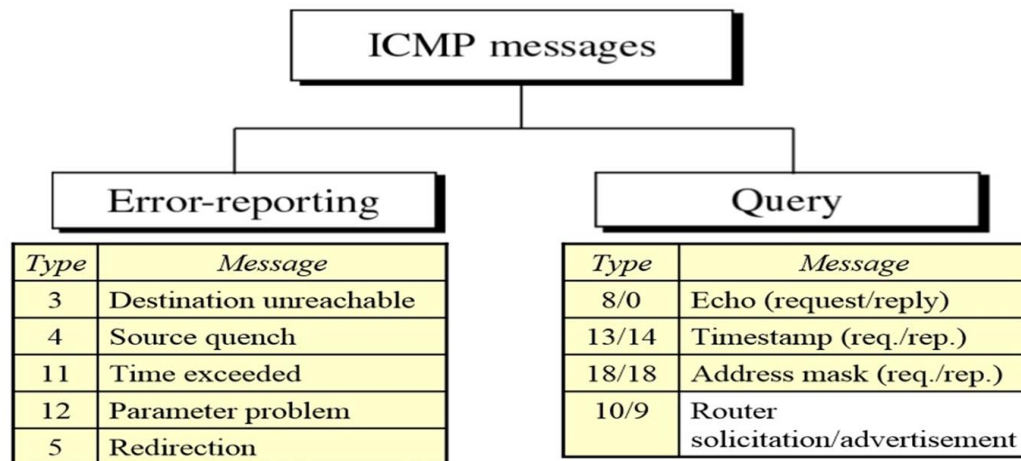


Figure 37: Types of ICMP messages.

### 2. ICMP: Error Reporting Messages

**Error messages are always sent to the original source** because the only information available in the datagram about the route is the source and destination IP addresses. The following are the most used error-reporting messages:

- **Destination Unreachable:** The message of "Destination Unreachable" is sent from receiver to the sender when destination cannot be reached, or packet is discarded when the destination is not reachable or when a router cannot route a datagram or host can't deliver a datagram, then the datagram is discarded and the "destination unreachable message" is sent.
- **Source Quench:** This message is a kind of flow control. The purpose of the source quench message is **congestion control**. The message sent from the congested router to the source host to reduce the transmission rate. ICMP will take the IP of the discarded packet and then add the source quench message to the IP datagram to inform the source host to reduce its transmission rate. The source host will reduce the transmission rate (slow down or quench) so that the router will be free from congestion.

- **Parameter problems:** When a router or host discovers any missing value in the IP datagram, the router discards the datagram, and the "parameter problem" message is sent back to the source host.
- **Time Exceeded:** Time Exceeded is also known as "Time-To-Live". **It is a parameter that defines how long a packet should live before it would be discarded.** There are two ways when Time Exceeded message can be generated:
  - Sometimes packet discarded due to some bad routing implementation, and this causes the looping issue and network congestion. **Due to the looping issue, the value of TTL keeps on decrementing, and when it reaches zero, the router discards the datagram.** However, when the datagram is discarded by the router, the time exceeded message will be sent by the router to the source host.
  - When destination host does not receive all the fragments in a certain time limit, then the received fragments are also discarded, and the destination host sends time Exceeded message to the source host.

### 3. ICMP: Query Messages

In addition to error reporting, ICMP can diagnose some network problems. This is accomplished through the query messages, a group of four different pairs of messages. In this document we only just mention one type of them since it the most one related to our practical experiments, which is **Echo Request and Reply messages.**

**The echo-request and echo-reply messages** are designed for diagnostic purposes. Network managers and users utilize this pair of messages to identify network problems and to determine if there is communication at the IP level. The combination of echo-request and echo-reply messages determines whether two systems (hosts or routers) can communicate with each other. Today, most systems provide a version of the **ping command, which we will explain shortly** that can create a series (instead of just one) of echo-request and echo-reply messages, providing statistical information.

## Part VII: Network Troubleshooting

For network troubleshooting, we used tools and commands to test the network connectivity using ping and traceroute tools. Moreover, we can investigate the network settings on your device using a variety of command prompt commands. This section addresses these topics professionally.

### A. Debugging tools to test TCP/IP network connectivity.

There are several tools that can be used on the Internet for debugging, such as **ping and traceroute**. We can determine the feasibility of a host or router and we trace the route of a packet.

**Before we get started with the discussion of the ping and traceroute tools, two concepts must be understood because these tools depend on them and they are highly related to the statistical output results of the ping and traceroute, which are:**

- **Round Trip Time (RTT)**
  - **The RTT is the time a packet takes to reach the remote host and for the response from the host to return. An asterisk (\*) is used to indicate a lost packet.**

- Using **traceroute provides RTT for each hop** along the path and indicates if a hop fails to respond.
- This information can be used to locate a problematic router in the path. If we get high response times or data losses from a particular hop, this is an indication that the resources of the router or its connections may be stressed.

#### ➤ **Time to Live (TTL)**

- A datagram has a limited lifetime in its travel through an internet. Today, this field is used mostly to control the maximum number of hops (routers) visited by the datagram.
- A datagram may travel between two or more routers for a long time without ever getting delivered to the destination host. This field limits the lifetime of a datagram.
- Another use of this field is to limit the journey of the packet. For example, if the source wants to limit the packet to the local network, it can store 1 in this field. When the packet arrives at the first router, this value is decremented to 0, and the datagram is discarded.
- **When a packet enters a router, the TTL field is decremented by 1. When the TTL reaches zero, a router will not forward the packet and the packet is dropped and sends ICMP “Time Exceeded Message” to the originating source host.**

**Here, the explanation of the two tools that use ICMP for debugging, namely, ping and traceroute.**

#### **1) Packet Internet Group (Ping) tool**

- **Ping** is an application program that uses the services of ICMP to test the reachability of a host (IP connectivity).
- **The source host sends ICMP echo-request messages (type: 8, code: 0); the destination, if alive, responds with ICMP echo-reply messages.**
- Note that ping can calculate the RTT. How? It inserts the sending time in the data section of the message. When the packet arrives, it subtracts the arrival time from the departure time to get the RTT.
- The TTL field in the IP datagram that encapsulates an ICMP message. If we set to 62, this means that the packet cannot travel more than 62 hops.
- The Ping results have four ICMP packets have been sent and four received. This result indicates you that the host is alive at the ICMP level.
- The ping program also continues to send messages, if we do not stop it by using the interrupt key (ctrl + c, for example). After it is interrupted, it prints the statistics summary of the responses. **It tells us the number of packets sent, the number of packets received, the total time, and the RTT minimum, maximum, and average.**
- Ping has a timeout value for the response. If a response is not received within that timeout, ping gives up and provides a message indicating that a response was not received.
- Type of connectivity tests performed with ping include the following:
  - Pinging the local loopback (127.0.0.1 for IPv4 and ::1 for IPv6), Pinging the default gateway, and Pinging the remote host.



- You can ping an IP address, as shown in Figure 38:

```
C:\>ping 172.16.1.100

Pinging 172.16.1.100 with 32 bytes of data:

Reply from 172.16.1.100: bytes=32 time<1ms TTL=127
Reply from 172.16.1.100: bytes=32 time<1ms TTL=127
Reply from 172.16.1.100: bytes=32 time<1ms TTL=127
Reply from 172.16.1.100: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figure 38: The result of pinging an IP address.

- You can ping website, as shown in Figure 39, as you can see from the below figure, we can observe that, the first output line shows the Fully Qualified Domain Name (FQDN) followed by the IP address.

```
C:\Users\hp>ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [23.79.160.81] with 32 bytes of data:
Reply from 23.79.160.81: bytes=32 time=63ms TTL=50
Reply from 23.79.160.81: bytes=32 time=62ms TTL=50
Reply from 23.79.160.81: bytes=32 time=62ms TTL=50
Reply from 23.79.160.81: bytes=32 time=62ms TTL=50

Ping statistics for 23.79.160.81:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 62ms, Maximum = 63ms, Average = 62ms

C:\Users\hp>
```

Figure 39: The result of pinging cisco web site.

- A DNS server is responsible to resolve the domain name to an IP address. DNS servers resolve domain names, not hostnames, to IP addresses. Without this name resolution, the ping would have failed because TCP/IP only understands valid IP addresses. It would not be possible to use the web browser without this name resolution.
- With DNS, connectivity to computers on the Internet can be verified using a familiar web address, or domain name, without having to know the actual IP address. If the nearest DNS server does not know the IP address, the server asks a DNS server higher in the Internet structure.
- On a Cisco device (e.g., switch and router), a ping from the IOS will yield to one of several indications for each ICMP echo that was sent. The most common indicators are:



- (!): indicates receipt of an ICMP echo reply. Ping completed successfully and verifies layer 3 connectivity.
- (.): indicates a timed out while waiting for a reply. A connectivity problem occurred somewhere along the path, a router along the path did not have a route to the destination and did not send an ICMP destination unreachable message, or ping was blocked by device security.
- (U): indicates an ICMP unreachable message was received. A router along the path did not have a route to the destination address and responded with an ICMP unreachable message.

## 2) Trace route

- The tracert utility, available on Windows, (a similar utility, traceroute, is available on Linux and Cisco IOS). Tracert program in Windows can be used to trace the route of a packet from the source to the destination. It is used to simulate the loose source route and strict source route options of an IP datagram. We use this program in conjunction with ICMP packets, as shown in Figure 40.
- **Traceroute makes use of a function of the TTL field in the Layer 3 header and ICMP Time Exceeded Message and destination unreachable message.**

```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.16299.309]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>tracert www.google.com

Tracing route to www.google.com [172.217.14.164]
over a maximum of 30 hops:

  0  0 ms  0 ms  0 ms  PRAMATAROV.mshome.net [192.168.137.1]
  1  *  *  *  Request timed out.
  2  49 ms 18 ms 10 ms 192.168.0.1
  3  9 ms 12 ms 10 ms 192.168.15.1
  4  31 ms 31 ms 268 ms 187-162-16-10.static.axtel.net [187.162.16.10]
  5  344 ms 90 ms 54 ms 189-209-118-1.static.axtel.net [189.209.118.1]
  6  12 ms 11 ms 13 ms 187-177-98-185.dynamic.axtel.net [187.177.98.185]
  7  506 ms 104 ms 47 ms dial-148-240-205-26.zone-1.ip.static-ftth.axtel.net.mx [148.240.205.26]
  8  36 ms 39 ms 77 ms tenge4-4.br01.mca01.pccwbtn.net [63.218.161.105]
  9  44 ms 31 ms 40 ms HundredGE0-3-0-0.br04.dal01.pccwbtn.net [63.223.32.66]
 10  *  994 ms 237 ms 63-218-23-190.static.pccwglobal.net [63.218.23.190]
 11  *  32 ms 37 ms 108.170.252.129
 12  33 ms 33 ms 41 ms 72.14.236.241
 13  56 ms 31 ms 32 ms dfw28s22-in-f4.1e100.net [172.217.14.164]

Trace complete.

C:\WINDOWS\system32>

```

Figure 40: The result of tracert command for Google web site.

- Given the topology, shown in Figure 41, we know that a packet from host A to host B travels through routers R1, R2, and R2. However, most of the time, we are not aware of this topology. There could be several routes from A to B. The traceroute program uses the ICMP messages and the TTL field in the IP packet to find the route. But the question arises here, How Trace route works.

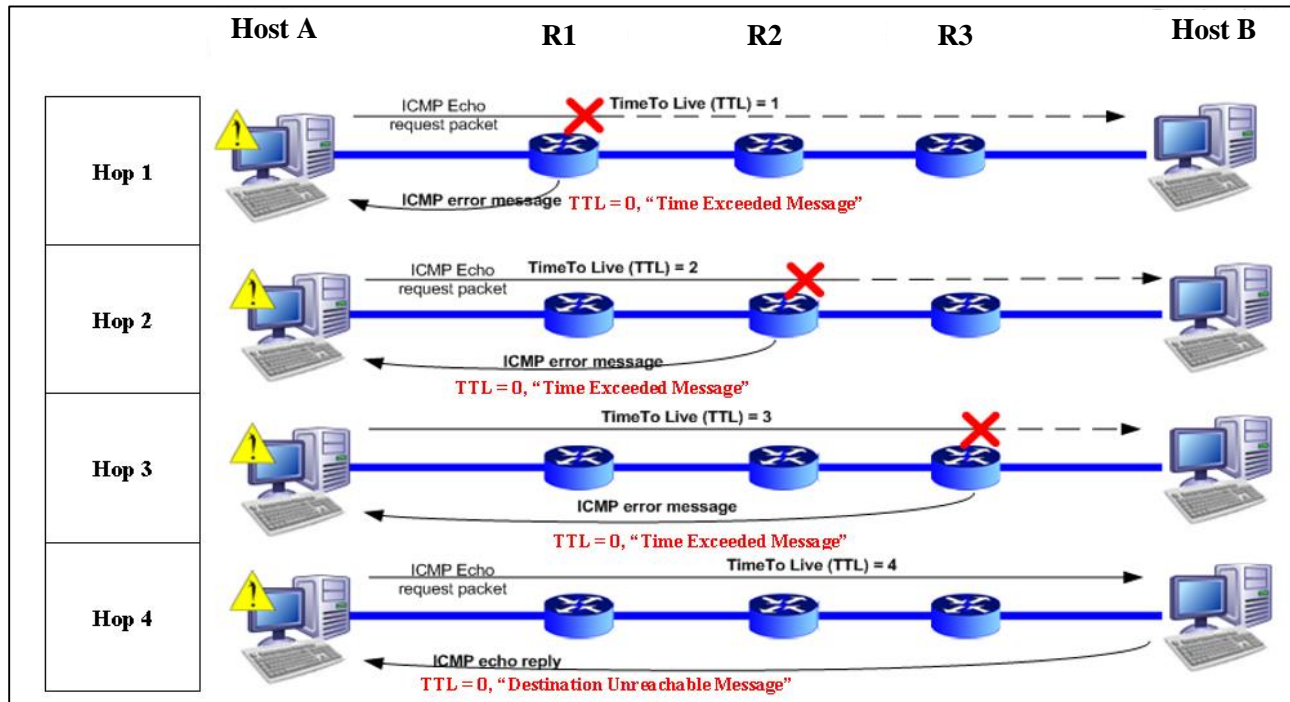


Figure 41: Trace route process.

The trace route adheres to the steps below to trace the journey of packets:

- 1) The traceroute program uses the following steps to find the address of the router R1 and the RTT between host A and router R1.
  - 1.1. The traceroute application at hostA sends a packet to destination B using UDP; the message is encapsulated in an IP packet with a TTL value of 1. The program notes the time the packet is sent.
  - 1.2. Router R1 receives the packet and decrements the value of TTL to 0. It then discards the packet (because TTL is 0). The router, however, sends a time exceeded ICMP message to show that the TTL value is 0 and the packet was discarded.
  - 1.3. The traceroute program receives the ICMP messages and uses the destination address of the IP packet encapsulating ICMP to find the IP address of router R1. The program also makes note of the time the packet has arrived. The difference between this time and the time at step 1.1 is the RTT.
  - 1.4. The traceroute program repeats steps 1.1-1.3 three times to get a better average RTT. The first trip time may be much longer than the second or third because it takes time for the ARP program to find the physical address of router R1. For the second and third trips, ARP has the address in its cache.
- 2) The traceroute program repeats the previous steps to find the address of router R2 and the RTT between host A and router R2. However, in this step, the value of TTL is set to 2. So, router R1 forwards the message, while router R2 discards it and sends a time exceeded ICMP message.
- 3) The traceroute program repeats the previous steps to find the address of router R3 and the RTT between host A and router R3. However, in this step, the value of TTL is set to 3. So, router R1 forwards the message and router R2 forwards the message, while router R3 discards it and sends a time exceeded ICMP message.

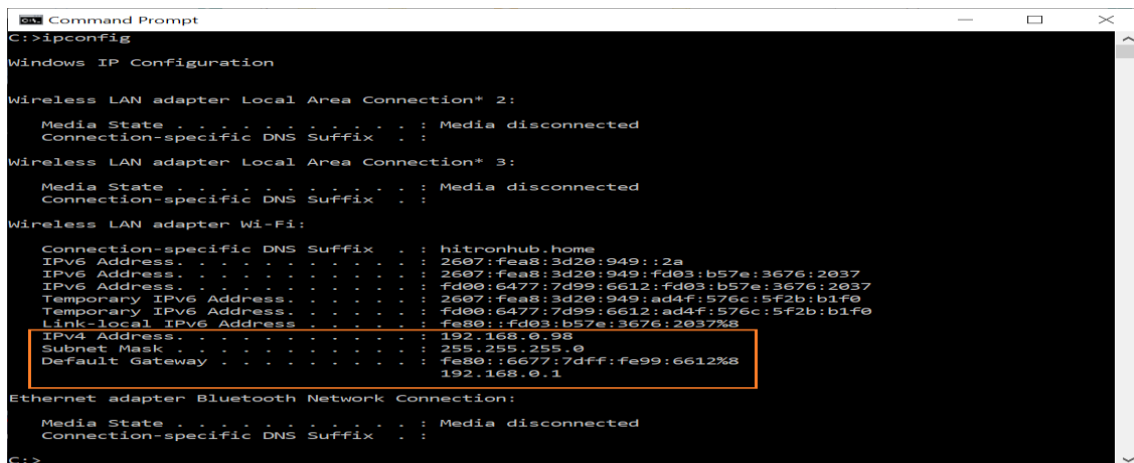
- 4) The traceroute program repeats step 2 to find the address of host B and the RTT between host A and host B. When host B receives the packet, it decrements the value of TTL, but it does not discard the message since it has reached its final destination.
- 5) Now, how can an ICMP message be sent back to host A?

**Answer:** The traceroute program uses a different strategy here. The destination port of the UDP packet is set to one that is not supported by the UDP protocol. **When host B receives the packet, it cannot find an application program to accept the delivery. It discards the packet and sends an ICMP destination unreachable message to host A. Note that this situation does not happen at router R1, R2, or R3 because a router does not check the UDP header. The traceroute program records the destination address of the arrived IP datagram and makes note of the RTT.** Receiving the destination unreachable message is an indication that the whole route has been found and there is no need to send more packets.

## B. Examining Network Properties Settings:

This section reviews the basic commands used to investigate the network setting in your device, which are categorized as follows:

- 1) **C:>ipconfig** command displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and DNS settings. If we used this command without parameters, ipconfig displays the IP address, subnet mask, and default gateway for all adapters, as shown in Figure 42.



```
Command Prompt
C:>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 2:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
Wireless LAN adapter Local Area Connection* 3:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
Wireless LAN adapter Wi-Fi:
    Connection-specific DNS Suffix  . : hitronhub.home
    IPv6 Address . . . . . : 2607:fea8:3d20:949::2a
    IPv6 Address . . . . . : 2607:fea8:3d20:949:fd03:b57e:3676:2037
    IPv6 Address . . . . . : fd00:6477:7d99:6612:fd03:b57e:3676:2037
    Temporary IPv6 Address. . . . . : 2607:fea8:3d20:949:ad4f:576c:5f2b:b1f0
    Temporary IPv6 Address. . . . . : fd00:6477:7d99:6612:ad4f:576c:5f2b:b1f0
    Link-local IPv6 Address . . . . . : fe80::fd03:b57e:3676:2037%8
    IPv4 Address . . . . . : 192.168.0.98
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::6677:7d99:fe99:6612%8
                                192.168.0.1

Ethernet adapter Bluetooth Network Connection:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
C:>
```

Figure 42: The results of ipconfig command.

- 2) **C:>ipconfig /all** command displays detailed configuration information about your TCP/IP connection including, host name, physical address, IPv4 address, subnet mask, default Gateway, DNS servers, DHCP, and type of Ethernet adapter in your system. Figure 43 show the results of this command.

```
Administrator: Command Prompt
C:\WINDOWS\system32>ipconfig /all

Windows IP Configuration

Host Name . . . . . : SOMOISJ00KS7N
Primary Dns Suffix . . . . . : ad.unc.edu
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : ad.unc.edu
                                  med.unc.edu

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) Ethernet Connection I217-LM
Physical Address. . . . . : 00-23-24-65-F6-A3
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 152.19.95.83(Preferred)
Subnet Mask . . . . . : 255.255.255.224
Default Gateway . . . . . : 152.19.95.92
                              152.19.95.65
DNS Servers . . . . . : 152.19.4.1
                              152.19.4.2
Primary WINS Server . . . . . : 152.2.247.14
Secondary WINS Server . . . . . : 152.2.247.15
NetBIOS over Tcpip. . . . . : Disabled
```

Figure 43: The results of ipconfig/all command.

- 3) **C:>ipconfig / release** command: This command terminates any active TCP/IP connections on all network adapters and releases those IP addresses from the DHCP server.
- 4) **C:>ipconfig /renew** command: This command re-establishes TCP/IP connections on all network adapters, but this command does not work if you have been configured with a static IP address.
- 5) **C:>netstat** command displays a variety of statistics about computers active TCP/IP connections. This tool is most useful when you are having trouble with TCP/IP applications such as HTTP and FTP.
- 6) **C:>arp -a** command displays current ARP cache tables for all interfaces.
- 7) **C:>nslookup** command is used for diagnosing DNS problems.
- 8) On Cisco routers, **show ip route** (in privileged EXEC mode) is a common IOS command used to view the routing table of a router.

**There are many troubleshooting commands, but until now we only just mentioned the essential ones that are required to deal with the first experiment, bearing in mind that we will add new troubleshooting commands whenever the need arises in the later experiments.**

## **Part VIII:Packet Tracer**

Packet Tracer is a useful network simulation tool from Cisco. It's a great software designed to guide beginners about networking certifications, such as CCNA. The program allows students to experiment with a system's network behavior. Due to this, students are able to contemplate various questions and explore multiple scenarios.

Cisco Packet Tracer download is a popular choice among developers and IT students around the world. The program has been developed by Cisco Systems as a core part of the Networking Academy

and proves to be quite useful for running network configuration simulations. This multi-faceted, comprehensive software uses simulation to confirm theories, concepts, practical knowledge, and ideas.

Since this network simulation tool is easy to install, it's a good choice for beginners without much experience working with network simulations and configurations. In order to use the software, you only need to sign up for the Networking Academy. After successfully signing up, you can conveniently download the installation file, confirm your email address, and start using multiple functionalities.

- You can download Packet Tracer from this link (Packet Tracer 8.2.0 (Latest Version)):  
<https://www.computernetworkingnotes.com/ccna-study-guide/download-packet-tracer-for-windows-and-linux.html>
- Open the link bellow, and follow the instructions step by step to install the Packet Tracer.  
<https://www.computernetworkingnotes.com/ccna-study-guide/how-to-install-and-activate-packet-tracer-in-windows.html>
- After installing the Packet Tracer, you must activate it by signing up and registering in the Network Academy: When you start Packet Tracer, it presents a login box The guest account offers limited features. This account allows you to save only 3 practice labs. To remove this restriction, you must log in to Packet Tracer from a Cisco Academy account. To create a free Cisco Academy account, visit the following web pages: [jitl.jp/packet-tracer](http://jitl.jp/packet-tracer) or <https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer>.

**Important Note:** Some parts of this handout have been collected from several trustable sites, books, and published slides and the other parts have been prepared and written by the instructors. As a matter of fact, this handout is made to be so straight forward, understandable, and so attractive whereas the students can do the required activities and solve the problems in a systematic and easy way, but still the instructors are expected to discuss some important material during the labs' sessions.