VET CERTIFICATE III in COMPUTER SYSTEM TECHNOLOGY

SMALL OFFCE HOME OFFICELAN SET UP

COSSL301

Setup Small office /Home office LAN

Competence

Credits: 4

Learning hours: 40

Sector: ICT

Sub-sector: Computer System Technology

Module Note Issue date: November, 2020

Purpose statement

This Specific module introduces set up Small office /Home office LAN (SOHO LAN).

The course materials will assist in developing the Knowledge, skills and attitude necessary to Plan and implement small and medium enterprise networks.

The leaner will be able to analyze facilities and existing network, Describe the purpose and functions of various network devices, SOHO LAN. Applications, SOHO LAN architecture, install and configure shared network devices, Select the appropriate media, cables, ports, and connectors to connect switches and router, Describe the technology and media access control method for Ethernet

networks, implement an IP addressing scheme and IP Services to meet network requirements in SOHO LAN, mounting network equipment.

Table of Contents

Total Number of Pages: 171

Learning Unit 1 – Apply basics of Computer networking and set up a LAN

LO 1.1 – Introduce Network

- Content/Topic 1 Introduction of common terms used in local area network:

A. Definition of LAN

Local area networks (LANs) are computer networks ranging in size from a few computers in a single office to hundreds or even thousands of devices spread across several buildings. They function to link computers together and provide shared access to printers, file servers, and other services

cables are connected to hubs, switches, and routers by rj45 ports.

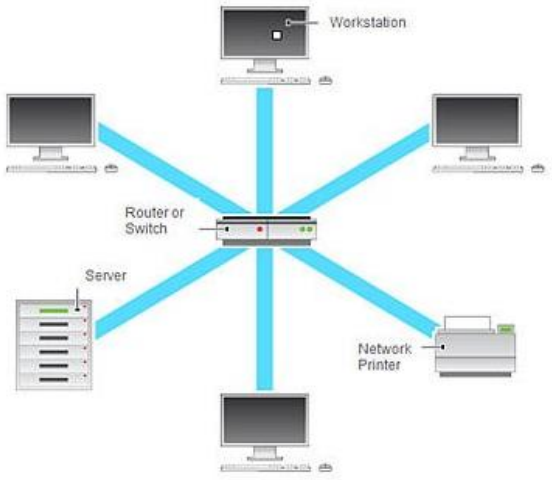


Figure: LAN devices

B. Common terms used in Local Area network

- ✓ **Computer network:** Computer network is a group of computers that shares information across wireless or wired technology likewise **network** is a collection of computers and devices connected together, often wirelessly, via communications devices and transmission media.
- ✓ **The internet: Internet** the term internet (dived into two word INTER and NET short for International Network) is a worldwide collection of networks linked together. It is also largest wide area network in the world.

The functions of internet

- Communication and Access information

- Downloading program, document and video
- Participate in discussion
- Online shopping
- Online advertising
- Money transfer

✓ **Internet service Provider (ISP):** Internet service provider is a company that supplies or provides internet services to the client and hosting. Some of the factors considered when choosing internet service provider: **Services offered, cost internet access, types of communication, security, speed and technical support.**

✓ **Firewall:** Firewall is a system designed to prevent unauthorized access to or from a private **network**. You can implement a **firewall** in either hardware or software form, or a combination of both differ to antivirus which is software detect, scan and prevent virus from computer.

Firewalls prevent unauthorized internet users from accessing private **networks** connected to the internet, especially intranets.

The difference between Firewall and Antivirus

FIREWALL	**ANTIVIRUS**
Firewall can be employed in software and hardware	Antivirus can be worked only in software
Firewall monitors and filters the incoming and outgoing packet via LAN home router	Antivirus perform scanning operations which involves: detection, identification and removal virus in computers,
Firewall deal with external attackers only	Deal with internal as well as internal attacks
In firewall inspection of the attacks is based on incoming packets by applying some set of rules	Antivirus the infected malicious software and files are inspected or scanned during scanning computer.

IP address: Internet Protocol address is 32 bits logical address assigned to network interface card that help computers to communicate.

- ✓ **TCP/IP:** is the language a computer uses to access the internet. It consists of a suite of protocols designed to establish a network of networks to provide a host with access to the internet.

The Benefits of using TCP/IP

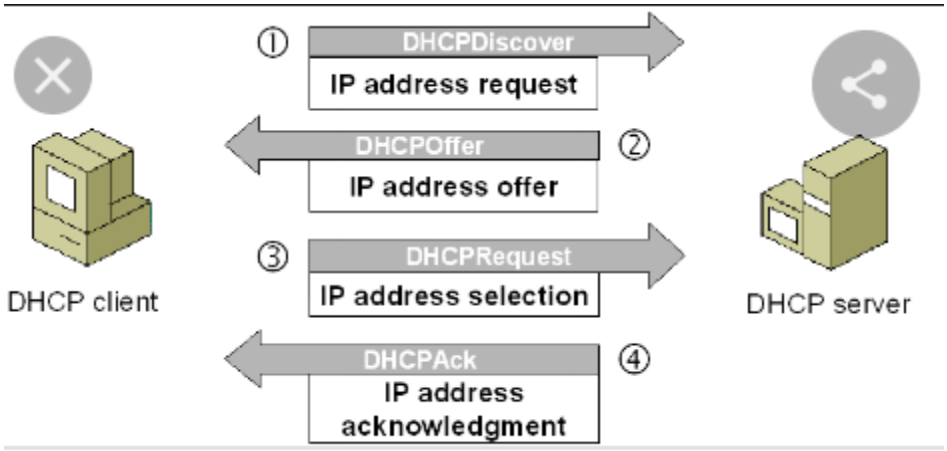
- Good failure recovery.
- The ability to add networks without interrupting existing services.
- High error-rate handling.
- Platform independence.
- Low data overhead.

- ✓ **DHCP:** is a protocol for assigning dynamic IP addresses to devices on a **network**. With dynamic addressing, a device can have a different IP address every time it connects to the **network means that** Dynamic IP changes each time when a user connects to a network**. While** The static IP address is fixed IP address which is manually assigned to a device for a long period of time. is a network management protocol used on Internet Protocol networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks. Dynamic Host Configuration Protocol (DHCP) is an application layer protocol used to distribute network configuration parameters, such as IP addresses, subnet masks, default gateways, etc. to hosts on a TCP/IP network. Assigning network parameters using DHCP reduces the amount of work of a network administrator, since there is no need to statically configure parameters on each device.

Advantages of Dynamic Host Configuration protocol

- Automatic management of IP addresses, including the prevention of duplicate IP address problems
- There is no need to manually configure each client with an IP address.
- You don't need to keep a record of the IP addresses that you have assigned
- You can automatically assign a new IP address if you move a client to a different subnet.
- Address duplication is eliminated as DHCP automatically tracks IP address assignments.
- The DHCP server can detect unauthorized DHCP servers on the network.

Four stapes of DHCP Communication



1. **DHCP DISCOVER:** IP Address request
2. **DHCPOFFER:** IP Address Offer
3. **DHCP Request:** IP address selection
4. **DHCPACK:** IP address Acknowledgement

DHCP Discovery: when we start a device, it checks whether a valid IP is available or not. If the valid IP configuration is not available, the device generate a special messages known as the DHCPDISCOVER message and Broadcasts this message on the local LAN segment.

To broadcast CHCPDISCOVER messages, the device uses the 0.0.0.0 and 255.255.255.0 as the source address and destination addresses, respectively. The 0.0.0.0 and 255.255.255.0 are two special addresses. Any device, whether it has a valid IP configuration or not, can use these addresses to send local broadcast messages. From these addresses, the 0.0.0.0 is used as the source address. If a device does not have the source address, it can use this address to send broadcast messages. 255.255.255.0 Is the local broadcast address. Any message sent on this address is received by all hosts of the local network.

DHCP Offer: since the client sends the DHCPDISCOVER Message to the local broadcast address, if a DHCP Server is configured on the local network, it will also receive the message. If multiple DHCP Servers are configured on the Local network, they all will receive the DHCPDISCOVER message. If multiple DHCP Servers are available, based on their configuration, one of them or all of them can reply to the DHCPDISCOVER message. In the reply to the DHCPDISCOVER message, a DHCP Server sends a DHCPOFFER message to the client.

Since the client does not have an IP address the DHCP Server can not send the DHCPOFFER message directly to the client. Because of this, the server sets the destination address to 255.255.255.255. In other words the server broadcast also broadcasts the DHCPOFFER message to the local network.
The DHCPOFFER message contains protocol specific information and an IP configuration. An IP configuration typically include the following important information: the IP address for the client, the subnet mask of the proposed IP address, the address of the default gateway, the DNS domain name, the DNS server address or addresses and the TFTP server address or addresses.
A part from these, the DHCPOFFER message also contains other protocol specific information such as the lease duration and client ID. This information is required by the core functions of DHCP.
DHCP Request all host in the local network receive the **DHCPOFFER** message. The host that sent the **DHCPDISCOVER** message accepts the **DHCPOFFER** message. Except the original host, all other hosts ignore the **DHCPOFFER**.
DHCPACK the DHCPACK indicates that the server "**Acknowledges**" the request and the **DHCPACK** message contains the field which indicates the IP address lease time, and network configuration parameters that the client is being configured with. The **DHCPACK** message is an acknowledgement to the client indicating that the DHCP server has received the **DHCP Request** message of the client, and the client can use the offered IP configuration.

- ✓ **Automatic Private IP Address (APIPA)** is the window **function that provides the DHCP auto configuration addressing.** APIPA assigns a class B IP address from 169.254.0.0 to 169.254.255.255 to the client when a DHCP server is either permanently or temporarily unavailable.
- ✓ **Mac Address:** MAC Address (Media access Control) address is 48bits hardware or physical address of LAN Card (NIC).MAC is usually stored in ROM on the network adapter card by manufacture and it unique. MAC address is also known as physical address, hardware address and burned-in address. MAC addresses are usually written in the form of 12 hexadecimal digits. For example, this is a valid MAC address: D8-D3-85-EA-1B-EE. Each hexadecimal character is 4 bits long, so the first six hexadecimal characters represent the vendor (in this case, Hewlett Packard).

C. The Purpose of Local Area Network

✓ **To share the files**

A network offers the facility of sharing a file so that it may be used by other users. The owner of the file may set permissions so that other users may be limited on the way they use that file. To those who are given read/write will be able to modify the content of the file.

✓ **To share information**

Computer networks provide communication possibilities faster than other facilities. Because of these optimal information and communication possibilities, computer networks may increase the organizational learning rate, which many authors declare as the only fundamental advantage in competition.

✓ **To share Printer**

If you have a printer attached to your computer, you can share it with anyone on the same network. It doesn't matter what type of printer it is, as long as the printer is installed on your computer and directly attached with a universal serial bus (USB) cable or other type of printer cable. Whoever you choose to share the printer with will be able to use it to print, provided they can locate your computer on the network.

✓ **To communicate (Sending and Receiving message)**

Communication begins with a message, or information, that must be sent from one individual or device to another. People exchange ideas using many different communication methods.

D. Disadvantages of Local Area Network

1. Cabling can be expensive to install and replace.
2. A fault with the server will prevent the whole network from working.
3. Security measures are needed to restrict access to the network (insecurity).
4. WANs are vulnerable to hackers and viruses.

LO 1.2 – Apply LAN Concepts and architectures

- **Content/Topic 1 Applications of LAN**

LAN applications: LAN networking comprises cables, switches, routers and other components that let users connect to internal servers, websites and other LANs via wide area networks. Ethernet and

Wi-Fi are the two primary ways to enable LAN connections. Ethernet is a specification that enables computers to communicate with each other.

1. **Personal computer LANS**

   A common LAN configuration is one that supports personal computers. With the relatively low cost of such systems, individual managers within organizations often independently procure personal computers for departmental applications, such as spreadsheet and project management tools, and for Internet access.

   Low cost: LAN that support very low cost attachment will not be suitable for meeting the overall requirement but it is cheap and easy to implement.

   Limited data rate: There is standard 100 Mbps Ethernet, which is what most people have at home. 100 Mbps is 100 megabits per second. That is translated into 12.5 megabytes per second (MBps or MB/s). It's much easier to convert to MBs since that is something we are all familiar with rather than bits.

   This means that if you don't have a gigabit router or switch and gigabit network card on your computers or NAS, the maximum speed you'll be able to transfer a file across your home network is 12.5 MBps. Also, in the real world, it's impossible to actually get that theoretical maximum. You'll probably end up somewhere around 4 to 8 MBps. If you are getting something really low like 1 MBps or less, there are reasons for that which I will mention below.

2. **Backend networks** are used to interconnect large systems such as mainframes, supercomputers, and mass storage devices. The key requirement for backend network is bulk data transfer with high reliability among a limited number of devices in a small area. These are some typical characteristics:

- High data rate. To satisfy the high-volume demand, data rates of 100 Mbps or more are required.
- High-speed interface. Data transfer operations between a large host system and a mass storage device are typically performed through high-speed parallel I/O interfaces, rather than slower communications interfaces. Thus, the physical link between station and network must be high speed.
- Distributed access. Some sort of distributed medium access control (MAC) technique is needed to enable a number of devices to share the medium with efficient and reliable access.
- Limited distance. Typically, a back-end network will be employed in a computer room or a small number of contiguous rooms.

- Limited number of devices. The number of expensive mainframes and mass storage devices found in the computer room generally numbers in the tens of devices.

3. **A Storage area networks** (SAN) is a specialized, high-speed network that provides block-level network access to storage. SANs are typically composed of hosts, switches, storage elements, and storage devices that are interconnected using a variety of technologies, topologies, and protocols. SANs may also span multiple sites SANs are primarily used to enhance storage devices, such as **disk arrays** and **tape libraries**, accessible to servers so that the devices appear to the **operating system** as **locally attached** devices.

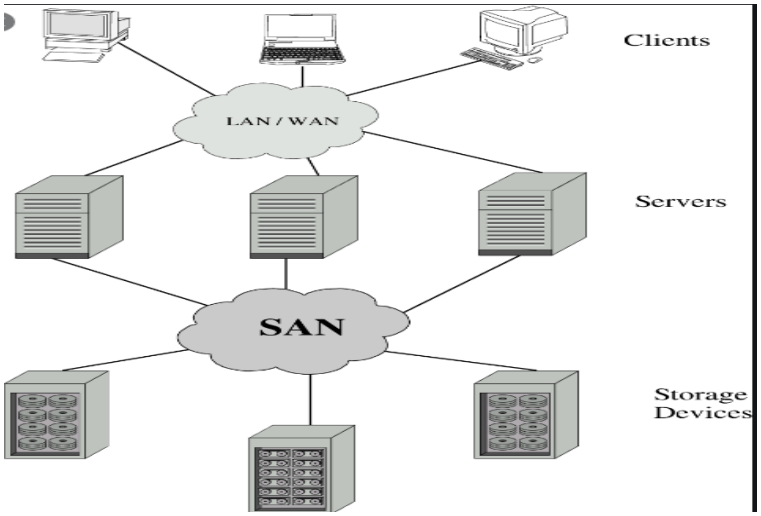


Figure: Storage Area Network (SAN)

Advantages of Storage Area network

- Separate network handling storage needs.
- Detaches storage tasks from specific servers
- Shared storage facility across high-speed network
- Hard disks, tape libraries, CD arrays
- Improved client-server storage access
- Direct storage to storage communication for backup

4. **High speed office networks:** the number of megabits per second(MBPS) determine the network speed: more Mbps means better performance and any businesses try to gets by with basic

consumer-level network using Ethernet to interconnect computers and device in a local area network for the following:

- Desktop image processing
- High capacity local storage

5. **Backbone LANs** An Internet backbone refers to one of the principal data routes between large, strategically interconnected networks and core routers on the Internet. Internet backbones are the largest data connections on the Internet.

   They require high-speed bandwidth connections and high-performance servers/routers.

   The backbone network usually consists of dedicated packet, message, or circuit switches connected by high-capacity trunk circuits, along with some special diagnostic and control equipment. Backbone networks must be extremely reliable.

✓ **Characteristic of backbone LAN**

- Interconnect low speed local LANs
- Reliability
- Capacity
- Cost

● **Content/Topic 2: Description of LAN Topologies**

1. **Topologies** is refers to the layout of connected devices. The shape of the cabling layout used to link devices is called the physical topology of the network. This refers to the layout of wiring, cables, the locations of nodes, and the interconnections between the nodes and the cabling or wiring system this is physical topology while The logical topology is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices.

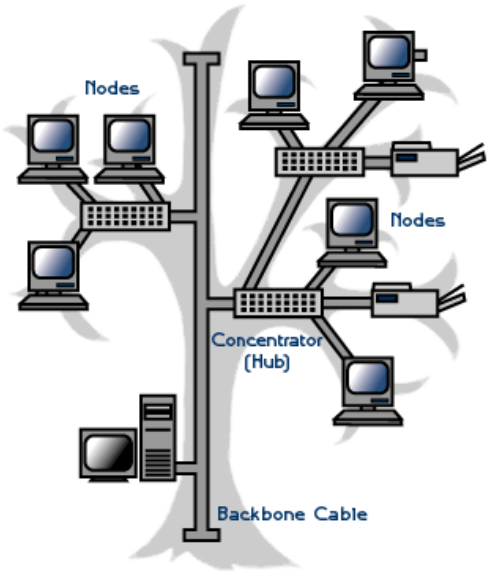
   Ethernet, token ring, FDDI are examples of logical topology

✓ **Types of physical topology**

a. Expanded Star or Tree Topology

   A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable.

Figure of Expanded Star Topology or Tree



Advantages of a Tree Topology

- Point-to-point wiring for individual segments.
- Supported by several hardware and software vendors.
- The tree topology is useful in cases where a star or bus cannot be implemented individually. It is most-suited in networking multiple departments of a university or corporation, where each unit (star segment) functions separately, and is also connected with the main node (root node).
- The advantages of centralization that are achieved in a star topology are inherited by the individual star segments in a tree network.
- Each star segment gets a dedicated link from the central bus. Thus, failing of one segment does not affect the rest of the network.
- Fault identification is easy.
- The network can be expanded by the addition of secondary nodes. Thus, scalability is achieved.

Disadvantages of a Tree Topology

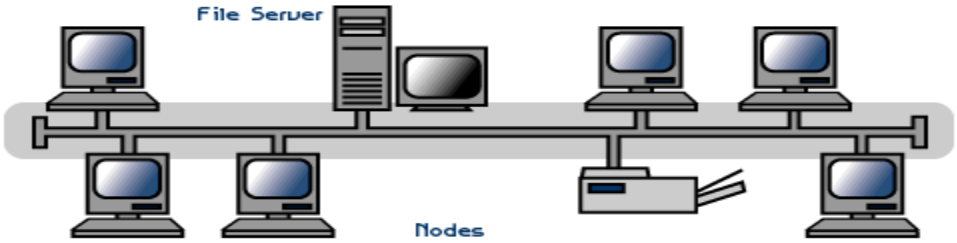
- As multiple segments are connected to a central bus, the network depends heavily on the bus. Its failure affects the entire network.
- Owing to its size and complexity, maintenance is not easy and costs are high. Also, configuration is difficult in comparison to that in other topologies.

- Though it is scalable, the number of nodes that can be added depends on the capacity of the central bus and on the cable type.

b. Bus Topology

Bus topology refers to a single cable that connects all the workstations, servers, printers and other devices on the network. A bus is usually referred to a cable that connects end to end and this is used to transmit the signals from one end to the other end.

Figure of Bus Topology



Advantages of Bus Topology

- The tree topology is useful in cases where a star or bus cannot be implemented individually. It is most-suited in networking multiple departments of a university or corporation, where each unit (star segment) functions separately, and is also connected with the main node (root node).
- The advantages of centralization that are achieved in a star topology are inherited by the individual star segments in a tree network.
- Each star segment gets a dedicated link from the central bus. Thus, failing of one segment does not affect the rest of the network.
- Fault identification is easy.
- The network can be expanded by the addition of secondary nodes. Thus, scalability is achieved.

Disadvantages of a Linear Bus Topology

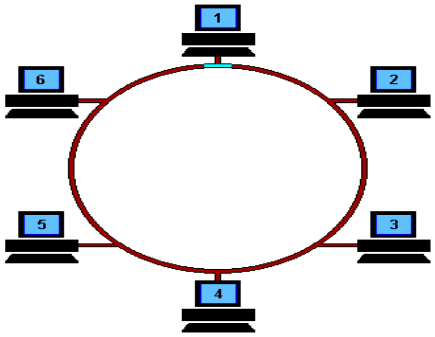
- The cable length is limited. This limits the number of network nodes that can be connected.
- This network topology can perform well only for a limited number of nodes. When the number of devices connected to the bus increases, the efficiency decreases.
- It is suitable for networks with low traffic. High traffic increases load on the bus, and the network efficiency drops.

- It is heavily dependent on the central bus. A fault in the bus leads to network failure.
- It is not easy to isolate faults in the network nodes.
- Each device on the network “sees” all the data being transmitted, thus posing a security risk.

c. Ring Topology

Ring topologies are used on token ring networks. Each device processes and retransmits the signal, so it is capable of supporting many devices. A token, or small data packet, is continuously passed around the network

Figure of Ring Topology



Advantages of Ring Topology

- Very orderly network where every device has access to the token and the opportunity to transmit
- Performs better than a star topology under heavy network load
- Can create much larger network using Token Ring

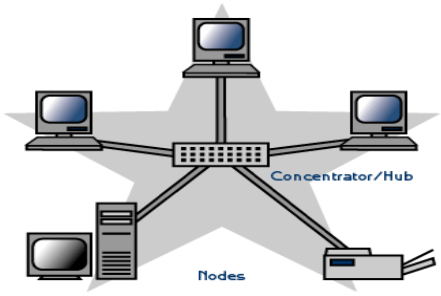
Disadvantages of Ring Topology

- One malfunctioning workstation or bad port in the MAU can create problems for the entire network
- Moves, adds and changes of devices can affect the network
- Network adapter cards and MAU's are much more expensive than Ethernet cards and hubs
- Much slower than an Ethernet network under normal load
- There is heavy dependency on the wire connecting the network nodes in the ring.

d. <u>STAR TOPOLOGY</u>

In a star topology, each network device has a home run of cabling back to a network hub or switch, giving each device a separate connection to the network.

Figure of Star Topology



Advantages of a Star Topology

- Easy to install and wire.
- No disruptions to the network when connecting or removing devices.
- Easy to detect faults and to remove parts.
- Due to its centralized nature, the topology offers simplicity of operation.
- It also achieves isolation of each device in the network.
- As the analysis of traffic is easy, the topology poses lesser security risk.
- Data packets do not have to pass through many nodes, like in the case of a ring network. Thus, with the use of a high-capacity central hub, traffic load can be handled at fairly decent speeds.

Disadvantages of a Star Topology

- Requires more cable length than a linear topology.
- If the hub or concentrator fails, nodes attached are disabled.
- More expensive than linear bus topologies because of the cost of the concentrators.
- The number of nodes that can be added depends on the capacity of the central hub.

Content/Topic 3: Description of medium

Network medium refers to the communication channels used to interconnect nodes on a computer network. Typical examples of network media include copper coaxial cable, copper twisted pair cables and optical fiber cables used in wired networks, and radio waves used in wireless data communications networks.

✓ **Cable Media**

There are a number of different cabling types that a network engineer/administrator sees over the course of their career. New individuals coming in to the field have to be familiar with a number of different cables and connectors to be prepared for their day-to-day activities. The following cabling media types will be most commonly seen in LAN environments.

Unshielded Twisted Pair (UTP)

Unshielded twisted pair (UTP) is a ubiquitous type of copper cabling used in telephone wiring and local area networks (LANs). There are five types of UTP cables -- identified with the prefix CAT, as in category -- each supporting a different amount of bandwidth.

Alternatives to UTP cable include coaxial cable and fiber optic cable. There are benefits and tradeoffs to each type of cabling, but broadly speaking, most enterprises favor UTP cable due to its low cost and ease of installation.

How UTP cables work: Twisted pair design

Inside a UTP cable is up to four twisted pairs of copper wires, enclosed in a protective plastic cover, with the greater number of pairs corresponding to more bandwidth. The two individual wires in a single pair are twisted around each other, and then the pairs are twisted around each other, as well. This is done to reduce crosstalk and electromagnetic interference, each of which can degrade network performance. Each signal on a twisted pair requires both wires.

Twisted pairs are color-coded to make it easy to identify each pair. In North America, one wire in a pair is identified by one of five colors: blue, orange, green, brown or slate (gray). This wire is paired with a wire from a different color group: white, red, black, yellow or violet. Typically, one wire in a pair is solid-colored, and the second is striped with the color of its mate -- e.g., a solid blue wire would be paired with a white-and-blue striped wire -- so they can be easily identified and matched.

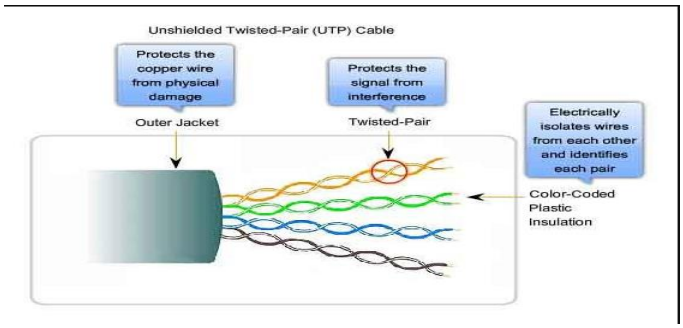


Figure: Unshielded Twisted Pair (UTP)

Unshielded Twisted Pair (UTP) cable is most certainly by far the most popular cable around the world. UTP cable is used not only for networking but also for the **traditional telephone** (**UTP-Cat 1**). There are **seven different types of UTP categories** and, depending on what you want to achieve, you would need the appropriate type of cable. **UTP-CAT5e** is the most popular UTP cable which

came to replace the old coaxial cable that was not able to keep up with the constant growing need for faster and more reliable networks.

Characteristics of UTP

The characteristics of UTP are very good and make it easy to work with, install, expand and troubleshoot and we are going to look at the different wiring schemes available for UTP, how to create a straight through UTP cable, rules for safe operation and a lot of other cool stuff !

So let's have a quick look at each of the UTP categories available today along with their specifications:

UTP Categories - Copper Cable

UTP Category	Data Rate	Max. Length	Cable Type	Application
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

Figure 1: UTP Categories

UTP cable applications

UTP cables are mostly used for LAN networks. They can be used for voice, low-speed data, high-speed data, audio and paging systems, and building automation and control systems. UTP cable can be used in both the horizontal and backbone cabling subsystems.

Shielded Twisted Pair (STP)

Shielded twisted pair (STP) cable was originally designed by IBM for token ring networks that include two individual wires covered with a foil shielding, which prevents electromagnetic interference, thereby transporting data faster.

STP is similar to unshielded twisted pair (UTP); however, it contains an extra foil wrapping or copper braid jacket to help shield the cable signals from interference. STP cables are costlier when compared to UTP, but has the advantage of being capable of supporting higher transmission rates across longer distances.

Following images show two different types of Shielded Twisted Pair cables (STP).

Figure: Shielded twisted-pair (STP)

Shielded twisted-pair (STP) cabling is more expensive than unshielded twisted-pair (UTP) cabling. It has an impedance of 150 ohms, has a maximum length of 90 meters, and is used primarily in networking environments with a high amount of EMI due to motors, air conditioners, power lines, or other noisy electrical components. STP cabling is the default type of cabling for IBM Token Ring networks.

STP cabling comes in various grades or categories defined by the EIA/TIA wiring standards, as shown in the following table.

Types of STP Cable (Shielded Twisted Pair Cable)

Category 5e: Defines a shielded cable that operates at 350 MHz and carries data up to 1000 Mbps. It carries high-quality signal while traveling across high voltage or power cables. Cat 5e cables are used in networking, data transfer, and telephone lines.

150 Ohm Shielded Cable: Defines a cable in which twisted pairs are individually covered in a foil shield and again enclosed in an outer braided wire shield. The shielding helps minimize EMI and crosstalk. The maximum signaling frequency is 16 MHz.

Characteristics of STP Cable

Characteristics	**Description**
Maximum cable length	**100 meters**
bandwidth	**100 Mbps**
Connector type	**RJ-45**
Cost	**Costlier than UTP but cheaper than FIBER OPTIC cable.**
Interference protection	**Better protection from crosstalk and external interference**
Signal transmission mode	**Baseband**
Resistance	**50 ohms**

Table 1: Characteristics of STP Cable

Fiber-optic cable

A fiber-optic cable, also known as an optical-fiber cable, is an assembly similar to an electrical cable, but containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example, long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Different types of fiber optic cables and their uses

Single-Mode Fiber Optic Cable

Businesses that need to enhance their network's capability to perform long distance communication need a single mode fiber optic cable. This cable has the smallest core and the thickest sheathing – specifically designed to carry a single signal source over great distances with a low chance of failure. Its small diametric core allows one mode of light to promulgate, causing the number of light reflections it creates to decrease. And as the light that passes through the core decreases, its attenuation lowers. Because of that, the signal this cable transmits is enabled to travel further, making it excellent for businesses that require long distance communication.

Figure: Single-Mode Fiber Optic Cable

Multimode Fiber Optic Cable

In contrast with the single-mode fiber optic cable, multimode fiber optic cables are capable of carrying multiple signals. Its large diametrical core is designed to enable multiple modes of light to promulgate. And, as it passes through the core, it creates more light reflections, unlike the single-mode cable. Although it can transfer data in a shorter distance, it enables the computer network to transfer more data at any given time. That being said, if your company needs to transmit more data, multimode fiber optic cable is what you need. Moreover, there are two types of multimode cable available in the market: the step-index multimode cables and graded-index multimode cables.

Figure 2: Multimode Fiber Optic Cable

Here is a general breakdown of the three different types of cable and what they are capable of:

Twisted Pair Cables:

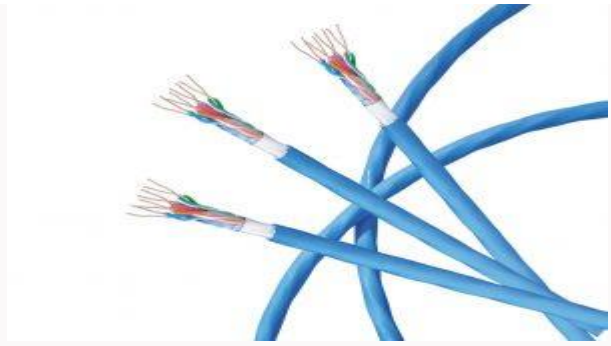


Figure: Twisted Pair Cables

Twisted pair cables are literally a pair of insulated wires that are twisted together. While this does help to reduce outside noise, these cables are still very susceptible to it. Twisted pair cables are the most cost-effective option of the three – mostly due to their lower bandwidth capacity and high attenuation. There are two types of twisted pair cables:

Unshielded twisted pair (UTP)

- 'Unshielded' meaning it does not rely on physical shielding to block interference
- Most commonly used cable of the two, often utilized for both residential and business use
- There are several UTP categories, which increase in bandwidth as you move up the scale, for example:
- **CAT1** = up to 1Mbps | **CAT2** = up to 4 Mbps | **CAT5e** = up to 1Gbps

Shielded twisted pair (STP)

- ‘Shielded’ with a foil jacket to cancel any external interference
- Used primarily for large-scale enterprises, high-end applications, and exterior cabling that will be exposed to environmental elements.

Coaxial Cables:

Figure: Coaxial Cables

Coaxial cables are high-frequency transmission cables made up of a single solid-copper core that transfers data electrically over the inner conductor. Coax has **80X more transmission capacity** than twisted pair cables.

This type of cable is commonly used to deliver TV signals (its higher bandwidth makes it more suitable for video applications) and to connect computers in a network. Along with stable transmission of data, coax also has anti-jamming capabilities and can effectively protect signals from being interfered. The cost is slightly higher than twisted pair but still more economical than fibre. There are also two types of coaxial cables:

75 Ohm

Most commonly used to transmit video signals

Often used to connect video signals between different components like DVDs, VCRs, or receivers commonly known as A/V cables

50 Ohm

Primarily utilized to transmit a data signal in a 2-way communication system

Most commonly used for computer Ethernet backbones, AM/FM radio receivers, GPS antenna, police scanners, and cell phone systems

Considerations of choosing medium

- Constrained by LAN topology
- Capacity
- Reliability
- Types of data supported
- Environmental scope

- **Content/Topic 3 : Description of Protocol architecture**

A **protocol architecture** is the layered structure of hardware and software that supports the exchange of data between systems and supports distributed applications, such as electronic mail and file transfer. Each protocol provides a set of rules.

Protocol Architectures and Networks

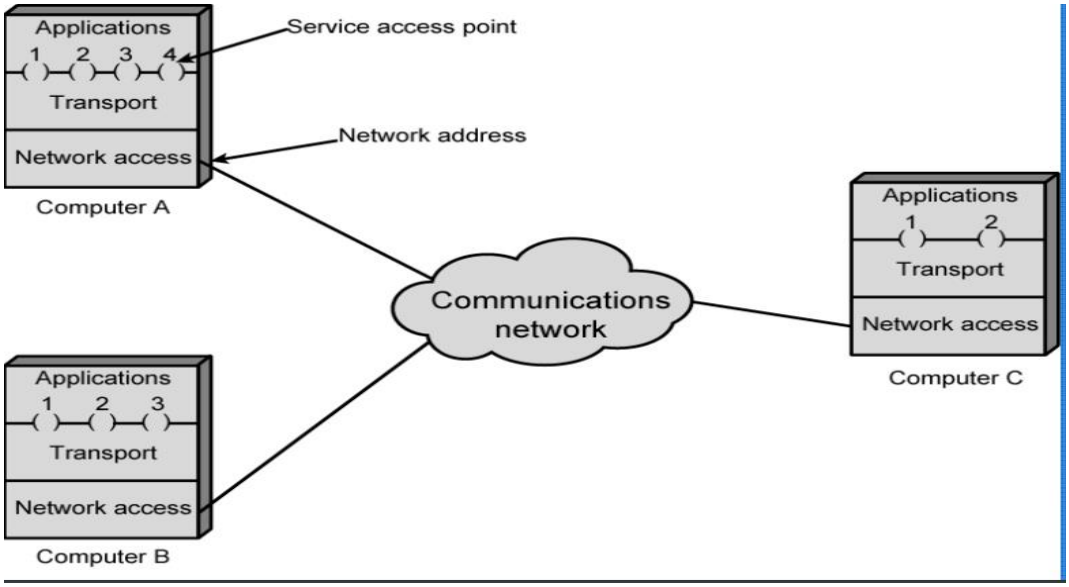


Figure 3: Protocol Architectures and Networks

- **Lower layers of OSI model**

OSI Model. It divides network communication into seven **layers**. **Layers** 1-4 are considered the **lower layers** and mostly are concerned with data around. **Layers** 5-7, the upper **layers**, contain application-level data.

LOWER AND UPPER LAYERS OF OSI MODEL

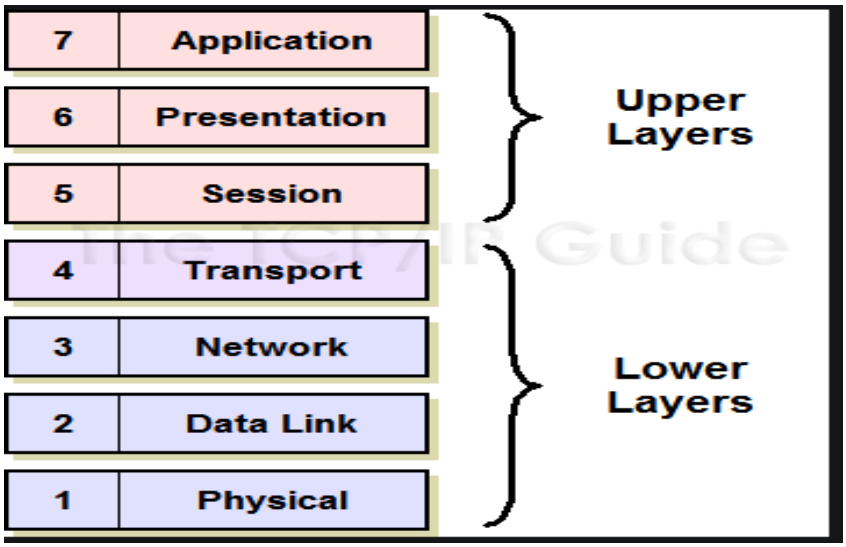


Table 2: LOWER AND UPPER LAYERS OF OSI MODEL

Lower layers of OSI model

Transport Provides reliable, transparent transfer of data between end points; provides end-to-end error recovery and flow control.
Network Provides upper layers with independence from the data transmission and switching technologies used to connect systems; responsible for establishing, maintaining, and terminating connections.
Data Link Provides for the reliable transfer of information across the physical link; sends blocks (frames) with the necessary synchronization, error control, and flow control.
Physical Concerned with transmission of unstructured bit stream over physical medium; deals with the mechanical, electrical, functional, and procedural characteristics to access the physical medium.

Table 3: Lower layers of OSI model:

- **IEEE 802 reference model**

- IEEE, pronounced "Eye-triple-E," stands for the Institute of Electrical and Electronics Engineers. The association is chartered under this name and it is the full legal name.
- **What is IEEE for?**

  The IEEE (Institute of Electrical and Electronics Engineers) describes itself as "the world's largest technical professional society -- promoting the development and application of electrotechnology and allied sciences for the benefit of humanity, the advancement of the profession, and the well-being of our members."

- The IEEE fosters the development of standards that often become national and international standards.

  The IEEE 802 reference model defines three layers:

- Logical link control (LLC),
- Medium access control (MAC),
- Physical (PHY).

  Bridging functions are considered a sublayer within the MAC layer. The LLC and MAC layers map to the OSI data-link layer. The PHY layer maps to the OSI physical layer.

  The IEEE 802.3 specification derives from Ethernet II. Today, nearly all Ethernet LANs are 802.3 compliant. A separate amendment, known as 802.3ae, specifies 10-Gbps operation. The frame format of Ethernet II has been merged into 802.3 by allowing the third field of the 802.3 header to be interpreted as either length or type, depending on the numeric value of the field. The 802.3ae specification uses the same frame format. When the third field is interpreted as length, the 802.3 header is followed by the 802.2 header in the PDU. (One notable exception to this rule is the 802.3 raw frame format used by Novell NetWare in the past.) Combined, 802.3 and 802.2 provide full OSI physical layer functionality plus all OSI data-link layer functionality except for bridging-related services. The 802.1D, 802.1G, 802.1H, and 802.1Q specifications provide OSI data-link layer bridging functionality. Alternately, when the third field of the 802.3 header is interpreted as type, the 802.2 header is omitted from the PDU. The 802.3 service then provides full OSI physical layer functionality plus limited OSI data-link layer functionality. The type field enables identification of the intended upper layer protocol at the destination host (also known as the destination EtherType). This is

important because it enables demultiplexing of OSI network layer protocols, which is a subset of the functionality provided by the 802.2 header. Figure 2-4 compares the IEEE 802 reference model to the OSI reference model and lists the relevant Ethernet specifications.

IEEE 802 Relative to OSI

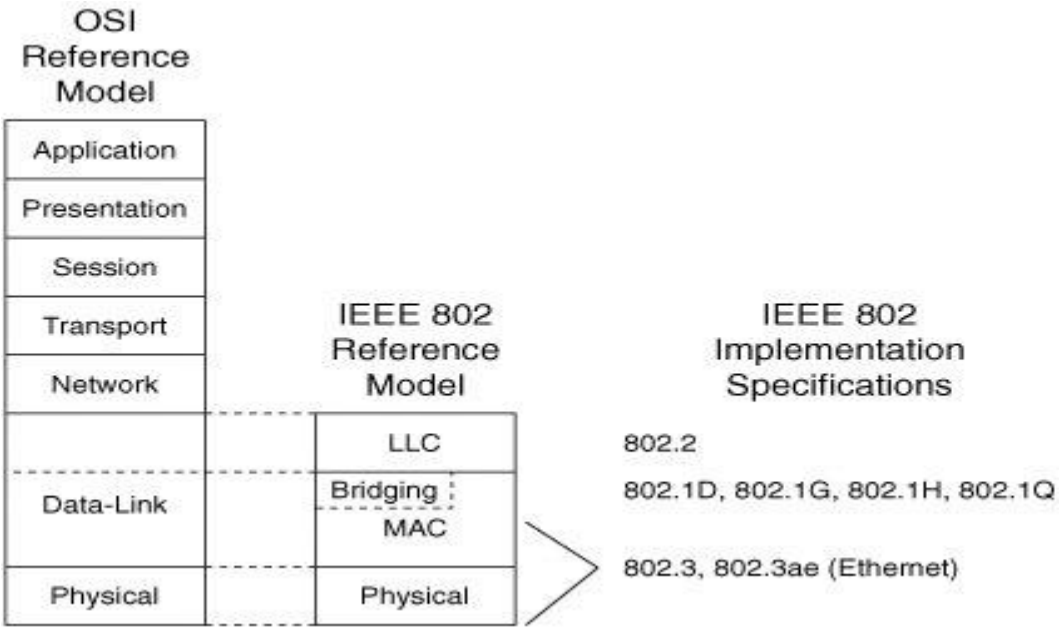


Figure: IEEE 802 Relative to OSI

IEEE specification names are case sensitive. For example, 802.1q is not the same as 802.1Q. Lower-case letters indicate an amendment to an existing standard, whereas upper-case letters indicate a full standard that might or might not incorporate various amendments.

- **Physical**

  A **PHY**, an abbreviation for "**physical** layer", is an electronic circuit, usually implemented as an integrated circuit, required to implement **physical** layer functions of the OSI model in a network interface controller.

- ✓ **What is the main function of physical layer?**

  Located at the lowest layer of the Open Systems Interconnection (OSI) communications model, the physical layer's function is to **transport** data using electrical, mechanical or procedural interfaces.

- **Logical link control (LLC)**

  In the **IEEE 802 reference model** of computer networking, the **logical link control** (**LLC**) data communication protocol **layer** is the upper sublayer of the data **link layer** (**layer** 2) of the seven-**layer OSI model**. The **LLC** sublayer acts as an interface between the **media access control** (MAC) sublayer and the network **layer**.

- ✓ **What is the main function of LLC?**

  The **function** of the **Logical Link Control** (LLC) is to manage and ensure the integrity of data transmissions. The LLC provides Data **Link Layer** links to services for the Network **Layer** protocols. This is accomplished by the LLC Service Access Points (SAPs) for the services residing on network computers.

- **Media access control (MAC)**

  What is media access control?

  A **media access control** is a network data transfer policy that determines how data is transmitted between two computer terminals through a network cable. The **media access control** policy involves sub-layers of the data link layer 2 in the OSI reference model.

- ✓ **Bridges**

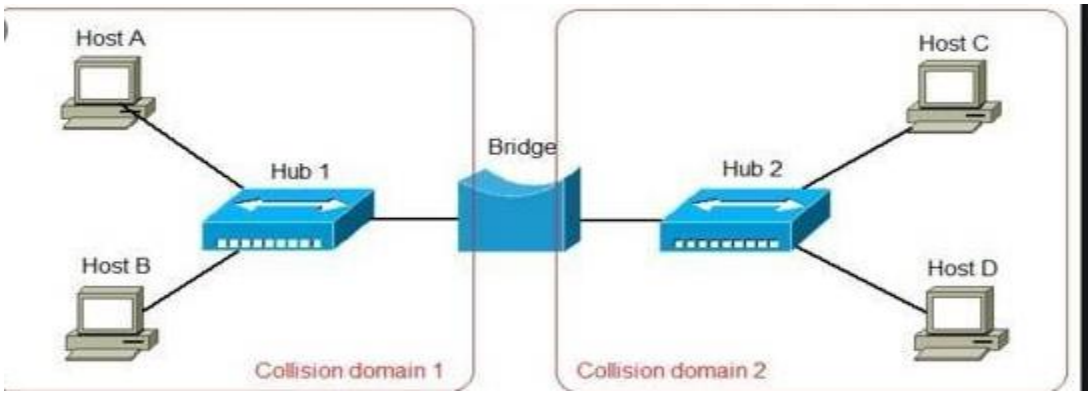


Figure: Network Bridge

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. Routing allows multiple networks to communicate independently and yet remain separate, whereas bridging connects two separate networks as if they were a single

network. In the OSI model, bridging is performed in the data link layer (layer 2). If one or more segments of the bridged network are wireless, the device is known as a **wireless bridge**.

- **Why bridge**

  A **bridge** is a device that connects and passes packets between two **network** segments that use the same communications protocol. **Bridges** operate at the data link layer (layer 2) of the OSI reference model. A **bridge** will filter, forward or flood an incoming frame based on the MAC address of that frame.

- **Reliability**

  Reliability is the measure of how often a network is useable. MTBF (Mean Time between Failures) is a measure of the average time a component is expected to operate between failures. Normally provided by the manufacturer. A network failure can be: hardware, data carrying medium and Network Operating System.

- **Performance**

  Performance is the defined as the rate of transferring error free data. It is measured by the Response Time. Response Time is the elasped time between the end of an inquiry and the beginning of a response. Request a file transfer and start the file transfer. Factors that affect Response Time are:

  - Number of Users: More users on a network - slower the network will run
  - Transmission Speed: speed that data will be transmitted measured in bits per second (bps)
  - Media Type: Type of physical connection used to connect nodes together
  - Hardware Type: Slow computers such as XT or fast such as Pentiums
  - Software Program: How well is the network operating system (NOS) written

- **Security**

  Security is the protection of Hardware, Software and Data from unauthorized access. Restricted physical access to computers, password protection, limiting user privileges and data encryption are common security methods. Anti-Virus monitoring programs to defend against computer viruses are a security measure.

- **Geography**

- **Functions of a bridge**

  What is the main function of bridge?

  A network bridge, also known as an Ethernet bridge, connects two segments of a network together. The segments are not independent entities, but are owned and managed by the same organization. The purpose of the bridge is to divide a network into manageable sections.

  - Read all frames transmitted on one LAN and only accept those address to any station on the other LAN
  - Using MAC protocol for second LAN, retransmit each frame
  - Creating a ***bridging table*** to keep track of devices on each segment.
  - **Filtering packets based on their MAC addresses**, i.e., forwarding packets whose destination MAC address is on a different segment of the network from their source and removing packets that do not need to be forwarded to other segments.
  - **Dividing a single network** into multiple collision domains, thereby reducing the number of collisions on each segment and effectively increasing its bandwidth.

- **Bridge operation**

  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. Routing allows multiple networks to communicate independently and yet remain separate, whereas bridging connects two separate networks as if they were a single network. In the OSI model, bridging is performed in the data link layer .If one or more segments of the bridged network are wireless, the device is known as a wireless bridg

- **Bridge design aspects**

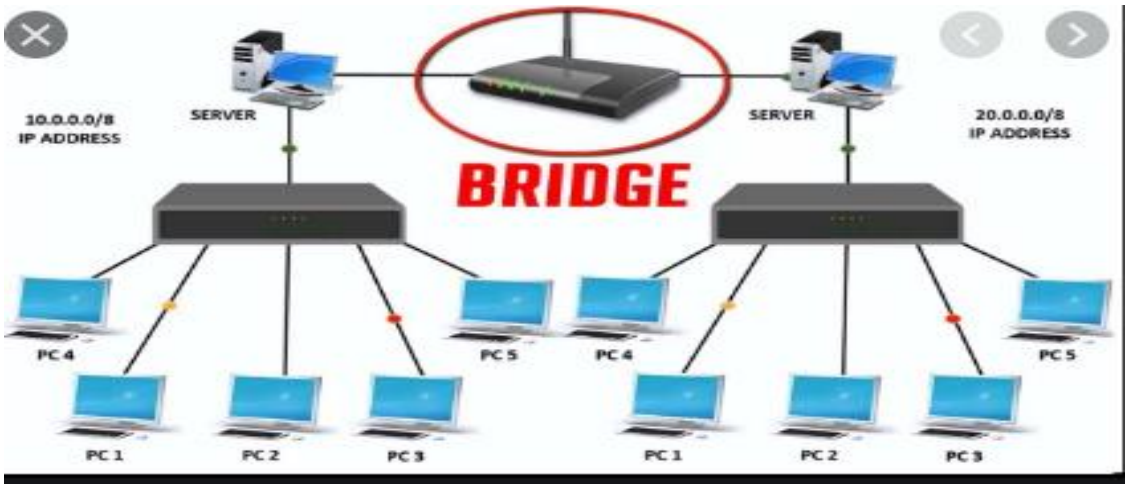


Figure: Bridge on network design

✓ **Bridge operation**

1. Bridge connects two or more different LANs that has a similar protocol and provide communication between the devices in them.
2. Joining multiple LANs
3. It helps in multiplying the network capacity of a single LAN.
4. It operates at data link layer and it transmit data as frames

✓ **Bridge design Aspect**

- No modification to content/format of frame
- Exact bitwise copy of frame
- Contains routing and address intelligence
- May connect more than two LANs:

1. Must be able to tell which frames to pass
2. May be more than one bridge to cross

- Bridging is transparent to stations

✓ **Bridge protocol architecture**

Bridging Protocols

Bridged networks use the following protocols:

Spanning Tree Protocol (STP)

STP is the default protocol that is used by the bridged networks. Bridging uses the STP mechanism to prevent network loops that potentially render the sub networks unusable. To forward packets to

their destinations, bridges must listen in promiscuous mode on every link that is attached to the bridge. Listening in promiscuous mode causes bridges to become vulnerable to the occurrences of forwarding loops, in which packets infinitely circle at full-line rate.

LO 1.3 – Apply Basics of computer networking

- **Content /Topic 1:Introduction to basic computer networking**

A computer network is a group of devices connected with each other through a transmission medium such as wires, cables etc. These devices can be computers, printers, scanners, Fax machines etc. The purpose of having computer network is to send and receive data stored in other devices over the network.

These devices are often referred as nodes.

A. Elements of network

There are five basic components **of a computer network**

Message: It is the data or information which needs to be transferred from one device to another device over a computer network.

Sender: Sender is the device that has the data and needs to send the data to other device connected to the network.

Receiver: A receiver is the device which is expecting the data from other device on the network.

Transmission media: In order to transfer data from one device to another device we need a transmission media such as wires, cables, radio waves etc.

Protocol: A protocol is a set of rules that are agreed by both sender and receiver, without a protocol two devices can be connected to each other but they cannot communicate. In order to establish a reliable communication or data sharing between two different devices we need set of rules that are called protocol. For example, http and https are the two protocols used by web browsers to get and post the data to internet, similarly smtp protocol is used by email services connected to the internet.

Features of a Computer Network

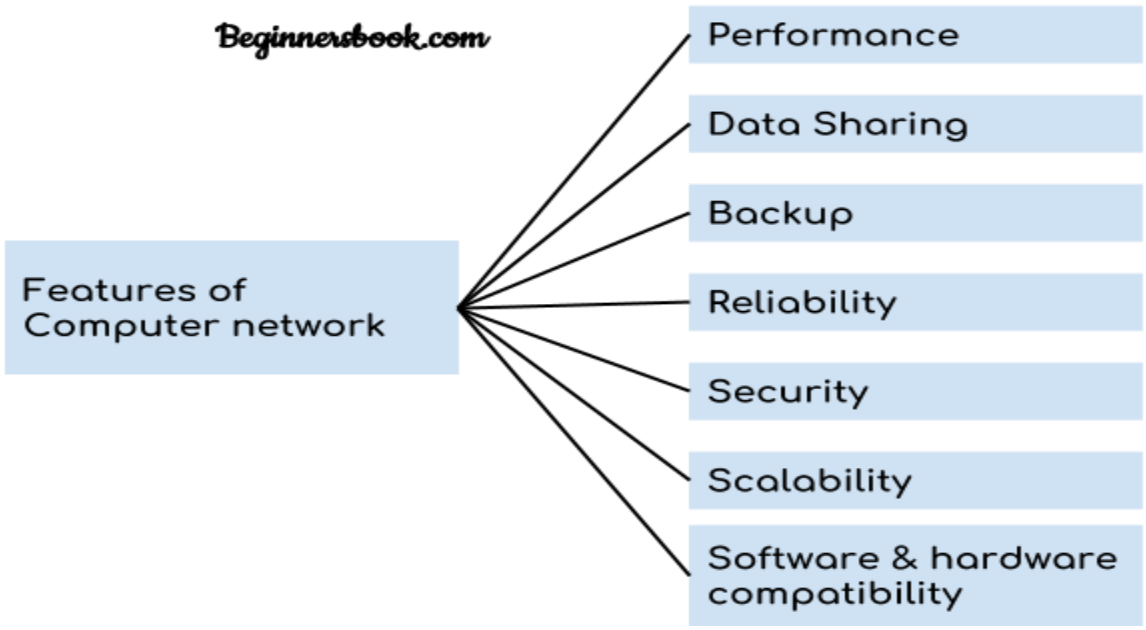


Figure: Features of computer network

B. Common used network components

Computer network components are the major parts which are needed to install the software. Some important network components are **NIC**, **switch**, **cable**, **hub**, **router**, and **modem**. Depending on the type of network that we need to install, some network components can also be removed. For example, the wireless network does not require a cable.

Following are the major components required to install a network:

✓ **Router**

A router is defined as a device that **connects two or more networks** and forwards data packets along **networks**

Figure: Different types of routers

- ✓ **Wireless routers**

Figure: Wireless router

Definition - What does Wireless Access Point (WAP) mean?

A wireless access point (WAP) is a hardware device or configured node on a local area network (LAN) that allows wireless capable devices and wired networks to connect through a wireless standard, including Wi-Fi or Bluetooth. WAPs feature radio transmitters and antennae, which facilitate connectivity between devices and the Internet or a network.A WAP is also known as a hotspot.

- ✓ **Switches :**

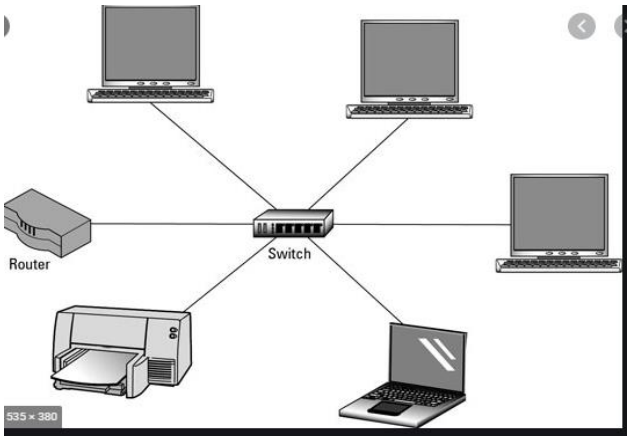


Figure: Switch

- A network switch is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer of the OSI model.
- A **switch** is a hardware device that connects multiple devices on a computer network. A Switch contains more advanced features than Hub. The Switch contains the updated table that decides where the data is transmitted or not. Switch delivers the message to the correct destination based on the physical address present in the incoming message. A Switch does not broadcast the message to the entire network like the Hub. It determines the device to whom the message is to be transmitted. Therefore, we can say that switch provides a direct connection between the source and destination. It increases the speed of the 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, optical fiber cable, and twisted pair cables, are used depending on the network's physical layer, topology, and size.

✓ **Adapter cards**

Figure: Adapter cards

An adapter card is any internal expansion card that allows the computer to communicate with another peripheral. A good example is a monitor or a video card.

✓ **Bridges**

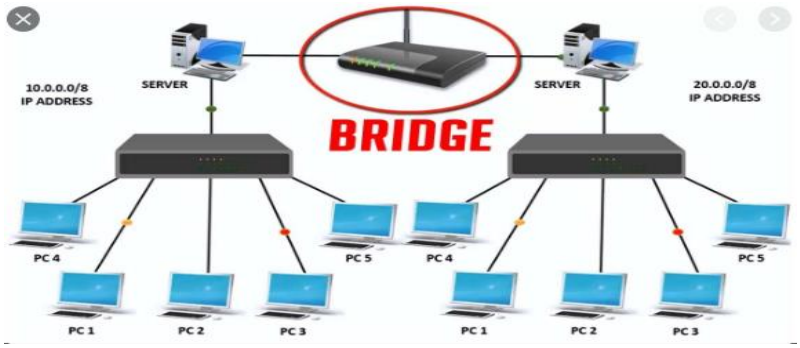


Figure: Bridges

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. Routing allows multiple networks to communicate independently and yet remain separate, whereas bridging connects two separate networks as if they were a single network. In the OSI model, bridging is performed in the data link layer (layer 2) If one or more segments of the bridged network are wireless, the device is known as a wireless bridge.

- **Servers: a** computer or computer program which manages access to a centralized resource or service in a network.
- In computing, a server is a piece of computer hardware or software that provides functionality for other programs or devices, called "clients". This architecture is called the client–server mode
- **What is server used for?**

Servers are used to manage network resources. For example, a user may set up a server to control access to a network, send/receive e-mail, manage print jobs, or host a website. They are also proficient at performing intense calculations

Figure: Server room

- ✓ **Repeater**

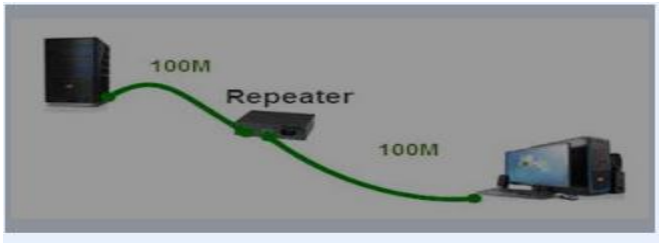


Figure: Repeater

Repeater: is device used to regenerate the signal over the same **network** before the signal becomes too weak or corrupted so as to extend the length to which the signal **can** be transmitted over the same network.

What is the difference between a WiFi extender and a wifi repeater?

What is a WiFi Extender? WiFi extenders connect directly to your home network through a wired connection. ... Another difference between a WiFi extender and a WiFi repeater is that a repeater will repeat the same WiFi signal, while an extender will create a new WiFi network.

- ✓ **Shared hardware:** hardware devices that can be easily accessed from a remote computer through a local area network (LAN) or enterprise intranet. Sharing hardware in a networked environment,

each computer on a network may access and use hardware resources on the network, such as printing a document on a shared network printer

- ✓ **Modem**
  - A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line.
  - It stands for Modulator/Demodulator. It converts the digital data into an analog signal over the telephone lines.

  Based on the differences in speed and transmission rate, a modem can be classified in the following categories:
  - Standard PC modem or Dial-up modem
  - Cellular Modem
  - Cable modem
- ✓ **PC (personal computer)**

Figure: PC (personal computer)

A personal computer (PC) is a multi-purpose computer whose size, capabilities, and price make it feasible for individual use. Personal computers are intended to be operated directly by an end user, rather than by a computer expert or technician. Unlike large,

costly minicomputers and mainframes, time-sharing by many people at the same time is not used with personal computers.

- ✓ **Rack mount**

Figure: Rack mount

What is rack mounted?

Rack-mounted describes a unit of electronic equipment that is housed in a metal framework called an equipment rack. Usually, an equipment rack contains multiple "bays," each designed to hold a unit of equipment such as a computer server.

- ✓ **Truncks**

  A trunk is a communications line or link designed to carry multiple signals simultaneously to provide network access between two points. It is a “link” that carries many signals at the same time, creating more efficient network access between two nodes Trunks typically connect switching centers in a communications system.

- ✓ **Patch panel**

  A patch panel in a local area network (LAN) is a mounted hardware assembly that contains ports used to connect and manage incoming and outgoing LAN cables. Patch panels are also referred to as patch bays, patch fields or jack fields and are also commonly used in radio and television.

Figure: patch panel

- **Cable manager**

Cable management refers to management of electrical or optical cable in a cabinet or an installation. The term is used for products, workmanship or planning. ... Cable management both supports and contains cables during installation, and makes subsequent maintenance or changes to the cable system easier.

Why is cable management important?

Cable management is essential to create a visually pleasing and clean work environment. Managing cables or wires helps to maintain basic functionality and also protect the devices from the clogged airflow due to unorganized and disordered wires. Tangled Wires or Cables are generally time-consuming to untangle

Figure: Cable manager

Shared hardware: Shared printers and other peripherals - Shared printers and peripherals are hardware resources provided to the users of the network by servers. Resources provided include data files, printers, software, or any other items used by clients on the network.

- **Content /Topic 2: Description of Network characteristics and Access Method**

A. Network Characteristics

The Network Architecture Characteristics are the followings:

1. Geographic Distribution

The main difference between the two types of networks is the way in which they are geographically distributed. A LAN is restricted to a limited geographic coverage of a few kilometers, but WAN spans greater distances and may extend over several thousand kilometers. Therefore LANs typically

provide communication facilities within a building or a campus, whereas WANs may nationwide or even worldwide.

2. Data rate

Data transmission rates are usually much higher in LANs than in WANP- transmission rates in LANs usually range from 0.2 megabit per second to 1 gigabit per second. On the other hand, transmission rates in WANs usually range from 1200 bits per second to slightly over 1 Mbps.

3. Error rate

Local area networks generally experience fewer data transmission errors than WANs do. Typically bit error rates are in the range of 10 to the power of -8 to 10 to the power of -10 with LANs as opposed to 10 to the power of -5 to 10 to the power of -7 with WANP-

4. Communication link

The most common communication links used in LANs are twisted pair, coaxial cable and fiber optics. On the other hand since the sites in a WAN are physically distributed over a large geographic area, the communication links used are by default relatively slow and unreliable. The communication links used in WANs are telephone lines, microwave links and satellite channels.

- **5. Ownership**

A LAN is owned by a single organization because of its limited geographic coverage. A WAN is usuall formed by interconnecting multiple LANs each of which may belong to a different organization. Therefore administrative and maintenance complexities and costs of LANs are usually much lower than for WANs.

6. Communication cost

The overall communication costs of a LAN is usually much lower than that of a WAN. The main reasons for this are lower error rates, simple routing algorithms and lower administrative and maintenance costs. The cost to transmit data in a LAN is negligible since the transmission medium is usually owned by the user organization. However with a WAN, this cost may be very high because the transmission media used are leased lines or public communication systems, such as telephone lines, microwave links and satellite channels.

7. Performance

Performance can be measured in many ways, including transit time and response time.

Transit time is the amount of time required for a message to travel from one device to another.

Response time is the elapsed time between an inquiry and a response.

The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

8. Reliability

In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

9. Security

Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

B. Network Access Method

- **CSMA/CD (Carrier Sense Multiple Access/Collision Detection)**

In CSMA/CD (Carrier Sense Multiple Access/Collision Detection) Access Method, every host has equal access to the wire and can place data on the wire when the wire is free from traffic. When a host want to place data on the wire, it will “sense” the wire to find whether there is a signal already on the wire. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted, to avoid collision again.

Advantages of CSMA/CD

- Reliable; Collisions are detected and packets are re-sent, so no data is lost.
- Relatively fast; A computer does not have to wait its "turn" to transmit data.

Disadvantages of CDMA/CD

- Limited to 2500 meters/11/2 mile; the collision detection mechanism restricts the length of cable segment that can be used.

- Inappropriate for large/active networks; Collisions slow the network and clog bandwidth with retransmissions.

➢ **CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)**

In CSMA/CA, before a host sends real data on the wire it will "sense" the wire to check if the wire is free. If the wire is free, it will send a piece of "dummy" data on the wire to see whether it collides with any other data. If it does not collide, the host will assume that the real data also will not collide.

Advantages of CSMA/CA

- Effective; Avoids data collisions.
- Reliable; Intent signals are sent until the cable is clear so that data will travel and reach its destination safely.

Disadvantages of CSMA/CA

- Relatively slow; A signal of intent must be sent *every* time a computer wants to transmit causing signal traffic.
- Inappropriate for large/active networks; The slowdown increases, as the network grows larger.
- Limited; suffers from same distance limitations as CSMA/CD since it must listen for the signals of intent.

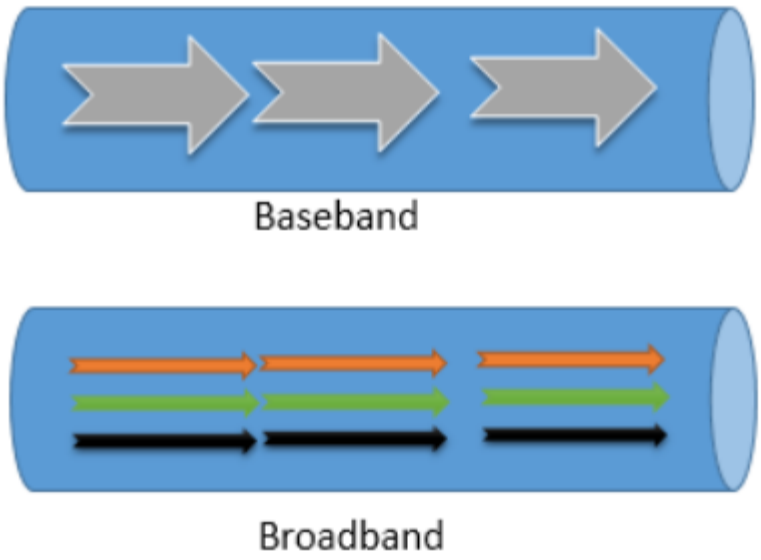
➢ **Token Passing**

In **CSMA/CD** and **CSMA/CA** the chances of collisions are there. As the number of hosts in the network increases, the chances of collisions also will become more. In token passing, when a host want to transmit data, it should hold the token, which is an empty packet. The token is circling the network in a very high speed. If any workstation wants to send data, it should wait for the token. When the token has reached the workstation, the workstation can take the token from the network, fill it with data, mark the token as being used and place the token back to the network. Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a modification of CSMA in which each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other node is already transmitting on the cable, the computer will wait and try again when the line is clear. Sometimes two computers attempt to transmit at the same instant. When

this happens, a collision occurs. Each computer then backs off and waits a random amount of time before attempting to retransmit.

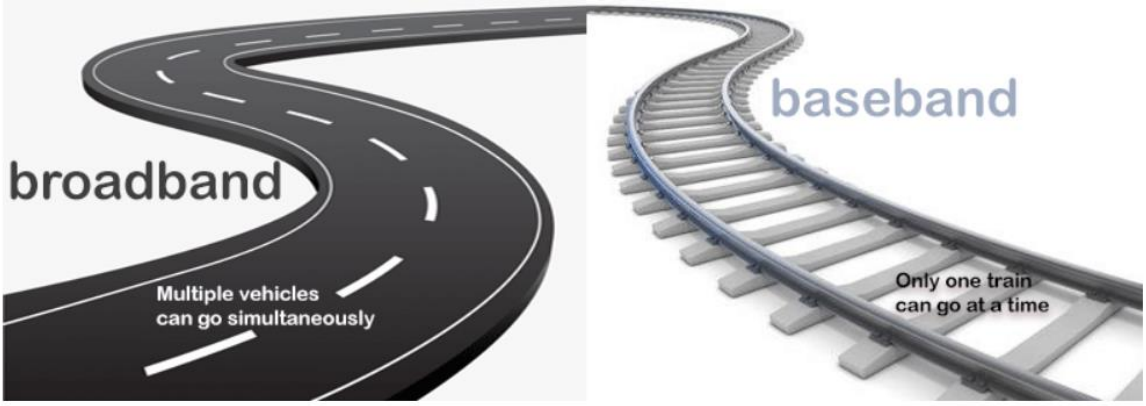
Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is similar to CSMA/CD except that a computer signals its intent to transmit before it actually does so. This removes the possibility for collisions to occur.

- **Content /Topic 3: Description of Network architecture**
- This tutorial explains give the differences between the baseband and broadband transmissions in detail. Learn what the baseband and broadband transmissions are and how they differ from each other. Both baseband and broadband describe how data is transmitted between two nodes. Baseband technology transmits a single data signal/stream/channel at a time while broadband technology transmits multiple data signals/streams/channels simultaneously at the same time. The following image shows an example of both technologies.



To understand the basic differences between both technologies, consider the baseband as a railway track and the broadband as a highway. Like, at a time, only one train can go on a railway track, in the baseband transmission only one data signal can be transmitted at a time.

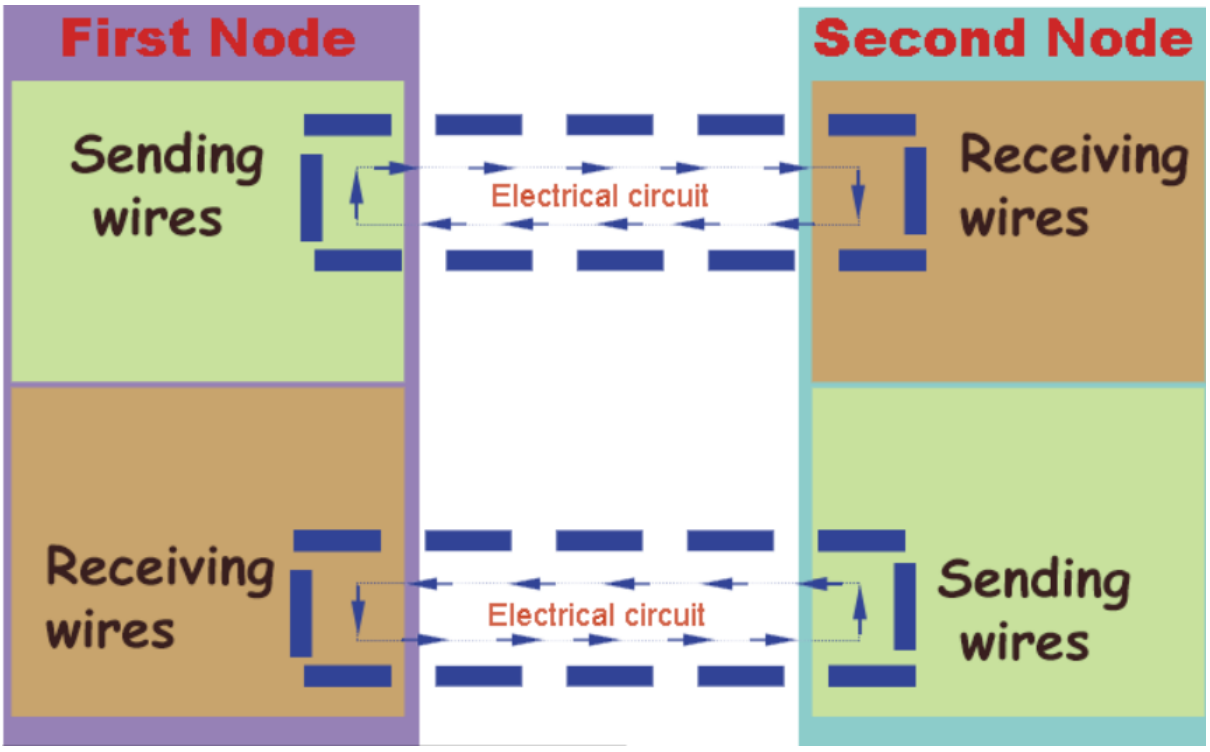
Unlike a railway track on a highway, multiple vehicles can go simultaneously. For example, on a 3 lanes highway, 3 vehicles can go at the same time. Same as a highway, in the broadband transmission, multiple data signals can be transmitted at the same time.



Baseband technology uses digital signals in data transmission. It sends binary values directly as pulses of different voltage levels. Digital signals can be regenerated using repeaters in order to travel longer distances before weakening and becoming unusable because of attenuation.

Baseband supports bidirectional communication. It means, this technology can send and receive data simultaneously. To support bidirectional communication, this technology uses two separate electric circuits together; one for sending and another for receiving.

The following image shows an example of this.



Although baseband transmits only a single data stream at a time, it is possible to transmit signals of multiple nodes simultaneously. This is done by combining all the signals into a single data stream.

To combine the signals of multiple nodes, a technology known as multiplexing is used. Baseband supports the Time Division Multiplexing (TDM).

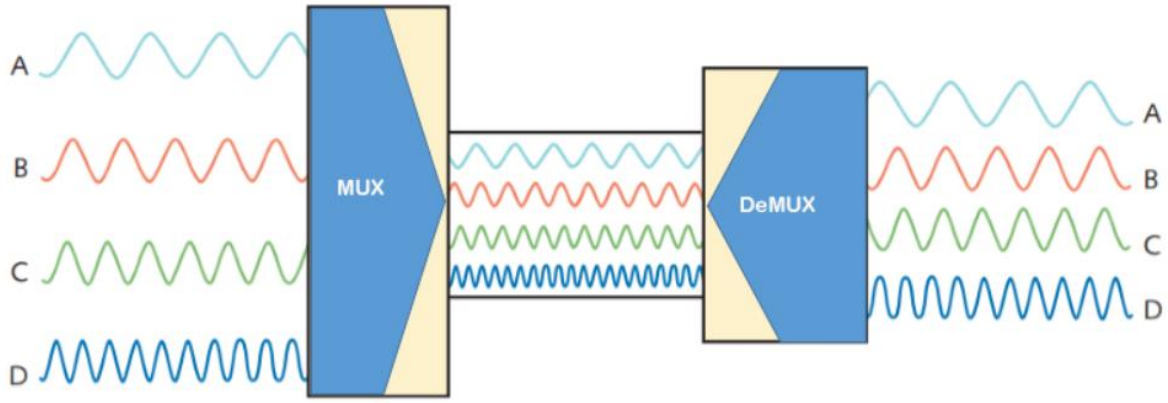
Baseband technology is mainly used in Ethernet networks to exchange data between nodes. This technology can be used on all three popular cable media types of Ethernet; coaxial, twisted-pair, fiber-optic.

Broadband transmission

Broadband technology uses analog signals in data transmission. This technology uses a special analog wave known as the **carrier wave**. A carrier wave does not contain any data but contains all properties of the analog signal. This technology mixes data/digital signal/binary values into the carrier wave and sends the carrier wave across the channel/medium.

To transmit data of multiple nodes simultaneously, this technology supports the Frequency Division Multiplexing. FDM (Frequency Division Multiplexing) divides the channel (medium or path) into several sub-channels and assigns a sub-channel to each node. Each sub-channel can carry a separate carrier wave.

The following image shows an example of this process.

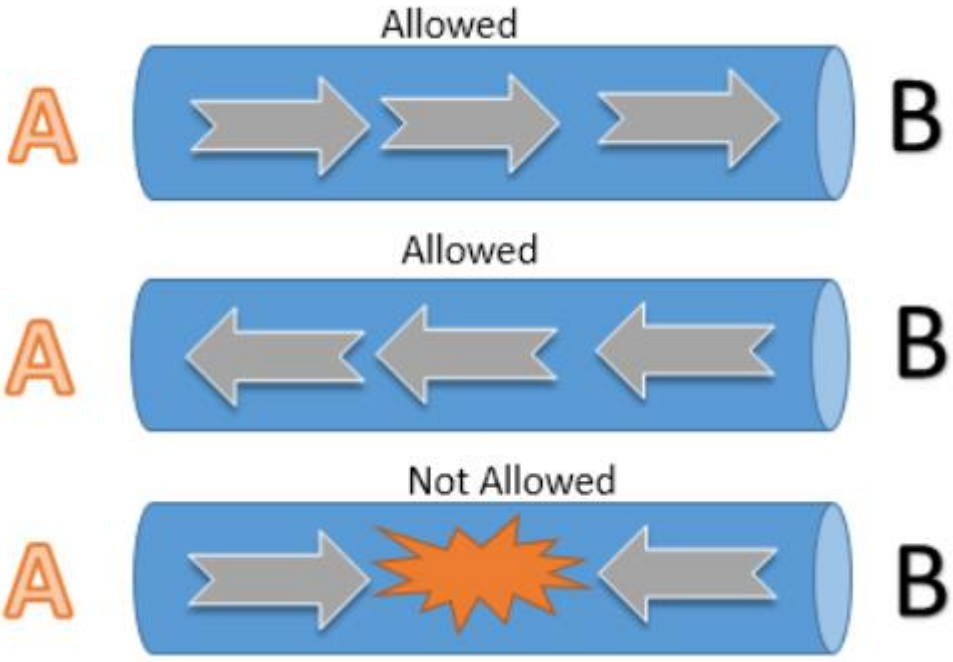


Analog signals can be regenerated using amplifiers in order to travel longer distances.

Broadband supports only unidirectional communication. It means, nodes connected at both ends of a medium can send or receive data but can't perform both actions simultaneously. Only one action is allowed at a time.

For example, two nodes A and B are connected through a cable that uses broadband technology to transmit signals. When node A transmits signals, node B receives the transmitted signals and when node B transmits signals, node A receives the transmitted signals.

The following image shows this example.



Broadband is typically used in an environment that transmits audio, video, and data simultaneously. For example, Cable TV Networks, Radio stations, and Telephone companies. Usually radio waves, coaxial, fiber-optic cables are used for broadband transmission.

Key differences between baseband and broadband transmissions

Baseband transmission	Broadband transmission
Transmit digital signals	Transmit analog signals
To boost signal strength, use repeaters	To boost signal strength, use amplifiers
Can transmit only a single data stream at a time	Can transmit multiple signal waves at a time
Support bidirectional communication simultaneously	Support unidirectional communication only
Support TDM based multiplexing	Support FDM based multiplexing
Use coaxial, twisted-pair, and fiber-optic cables	Use radio waves, coaxial cables, and fiber optic
Mainly used in Ethernet LAN networks	Mainly used in cable and telephone network

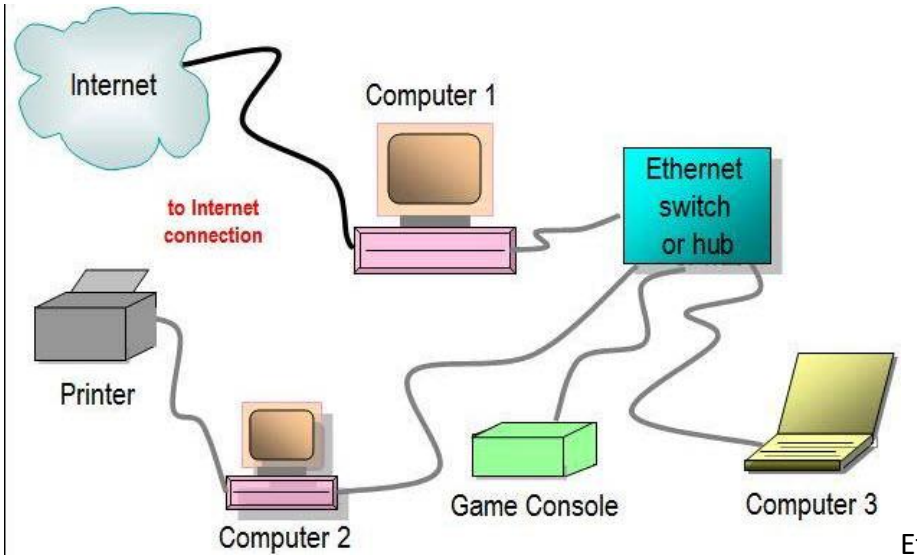
✓ Ethernet

Ethernet is a technology that connects wired local area networks (LANs) and enables the device to communicate with each other through a protocol which is the common network language.

The local area network is a computer network that interconnects a group of computers and shares the information through cables or wires.

Wired Ethernet Network

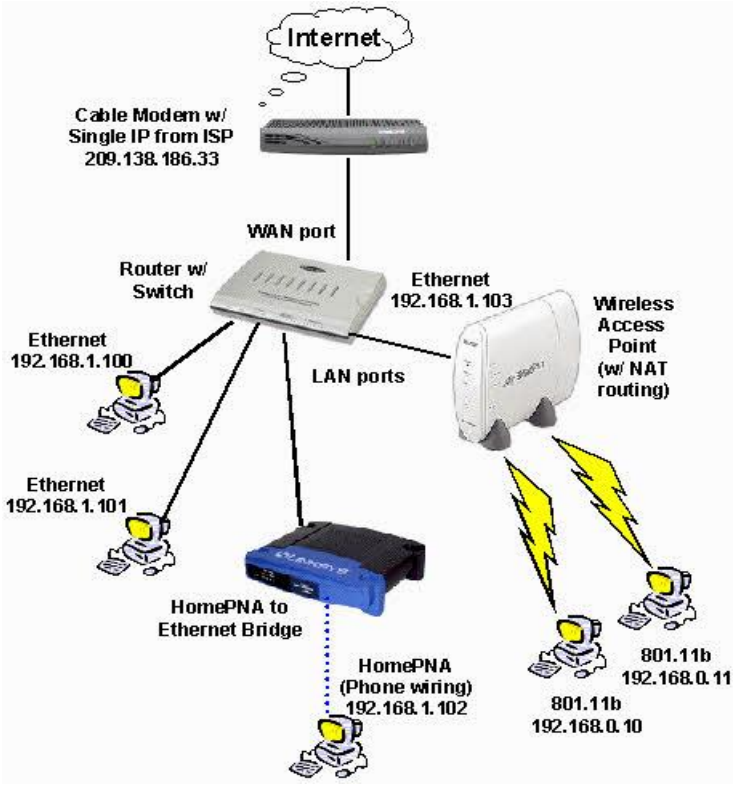
The Ethernet technology mainly works with the fiber optic cables that connect devices within a distance of 10 km. The Ethernet supports 10 Mbps.



Ethernet communication

A computer network interface card (NIC) is installed in each computer, and is assigned to a unique address. An Ethernet cable runs from each NIC to the central switch or hub. The switch and hub act as a relay though they have significant differences in the manner in which they handle network traffic – receiving and directing packets of data across the LAN. Thus, Ethernet networking creates a communications system that allows sharing of data and resources including printers, fax machines and scanners.

Wireless Ethernet



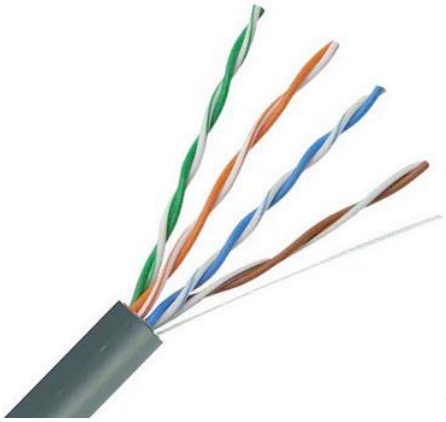
Wireless Network

Ethernet networks can also be wireless. Rather than using Ethernet cable to connect the computers, wireless NICs use radio waves for two-way communication with a wireless switch or hub. It consists of Ethernet ports, wireless NICs, switches and hubs. Wireless network technology can be more flexible to use, but also require extra care in configuring security.

Types of Ethernet Networks

There are several types of Ethernet networks, such as Fast Ethernet, Gigabit Ethernet, and Switch Ethernet. A network is a group of two or more computer systems connected together.

1. Fast Ethernet



Twisted pair cable

The fast Ethernet is a type of Ethernet network that can transfer data at a rate of 100 Mbps using a twisted-pair cable or a fiber-optic cable. The older 10 Mbps Ethernet is still used, but such networks do not provide necessary bandwidth for some network-based video applications.

Fast Ethernet is based on the proven CSMA/CD Media Access Control (MAC) protocol, and uses existing 10BaseT cabling. Data can move from 10 Mbps to 100 Mbps without any protocol translation or changes to the application and networking software.

What is Ethernet Port Speed?

When compare to a 10 mb port, a 100 Mb port is theoretically 10 times faster than the standard port. Therefore, with a 100 Mb port more information can stream to and from your server. This will be of great help to you if you really need to explore very high speed, but not if you are under DDOS attack because you will find yourself running out of traffic

100Mbit/s Ethernet port

If you are doing standard web hosting, the bigger 100 Mbps pipe will not offer true benefit to you because you may not even use more than 1 mbps at any given time. If you are hosting games or streaming media, then the bigger pipe of 100 Mbps would indeed be helpful to you. With a 10 mbps

pipe, you can transfer up to 1.25 Mbps, while a 100 mbps pipe, would allow you to transfer up to 12.5 Mbps.

However, if you leave your server unattended and running at full steam, a 10 Mbps pipe can consume about 3,240 GB a month and a 100 Mbps pipe can consume up to 32,400 GB a month. It would be really disgusting when you receive your bill.

1. **Gigabit Ethernet**

The Gigabit Ethernet is a type of Ethernet network capable of transferring data at a rate of 1000 Mbps based on a twisted-pair or fiber optic cable, and it is very popular. The type of twisted-pair cables that support Gigabit Ethernet is Cat 5e cable, where all the four pairs of twisted wires of the cable are used to achieve high data transfer rates. The 10 Gigabit Ethernet is a latest generation Ethernet capable of transferring data at a rate of 10 Gbps using twisted-pair or fiber optic cable.

Optic fiber cable

3. Switch Ethernet

Multiple network devices in a LAN require network equipments such as a network switch or hub. When using a network switch, a regular network cable is used instead of a crossover cable. The crossover cable consists of a transmission pair at one end and a receiving pair at the other end. The main function of a network switch is to forward data from one device to another device on the same network. Thus a network switch performs this task efficiently as the data is transferred from one device to another without affecting other devices on the same network.

Switch Ethernet

The network switch normally supports different data transfer rates. The most common data transfer rates include 10 Mbps – 100 Mbps for fast Ethernet, and 1000 Mbps – 10 Gbps for the latest Ethernet.

Switch Ethernet uses star topology, which is organized around a switch. The switch in a network uses a filtering and switching mechanism similar to the one used by the gateways, in which these techniques have been in use for a long time.

- 10Base2: The cable used is a thin coaxial cable: thin Ethernet.
- 10Base5: The cable used is a thick coaxial cable: thick Ethernet.
- 10Base-T: The cable used is a twisted-pair (T means twisted pair) and the speed achieved is around 10 Mbps.
- 100Base-FX: Makes it possible to achieve a speed of 100 Mbps by using multimode fiber optic (F stands for Fiber).
- 100Base-TX: Similar to 10Base-T, but with a speed 10 times greater (100 Mbps).
- 1000Base-T: Uses a double-twisted pair of category 5 cables and allows a speed up to one Gigabit per second.
- 1000Base-SX: Based on multimode fiber optic uses a short wavelength signal (S stands for short) of 850 nanometers (770 to 860 nm).
- 1000Base-LX: Based on multimode fiber optic uses a long wavelength signal (L stands for long) of 1350 nm (1270 to 1355 nm). Ethernet is a widely used network technology because the cost of such a network is not very high.

✓ **Making Ethernet Cables**

There are two kinds of Ethernet cables you can make, **Straight Through** and **Crossover**.

Straight through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router. This type of cable is used to connect the difference device such as

- Router to switch
- Computer to switch
- HUB to switch

How straight through UTP cable is built

In straight through UTP cable all Pins are matched on both sides. Pin-1 connects with pin-1; pin-2 connects pin-2; pin-3 connects pin-3; pin-4 connects pin-4; pin-5 connects pin-5 and pin-6 connects pin-6 on other side.

Required tools, material and components for Ethernet cable making

RJ-45 Registered jack-45 refers to a cable termination specification that specifies physical male and female **connectors** and the pin assignments of wires-in telephone cables and other networks that use **RJ45** connections.

Bulk RJ45 Crimpable Connectors for CAT-5e
or
Bulk RJ45 Crimpable Connectors for CAT-6

Crimping tool is a device used to conjoin two pieces of metal by deforming one or both of them in a way that causes them to hold each other.

RJ-45 Crimping tool

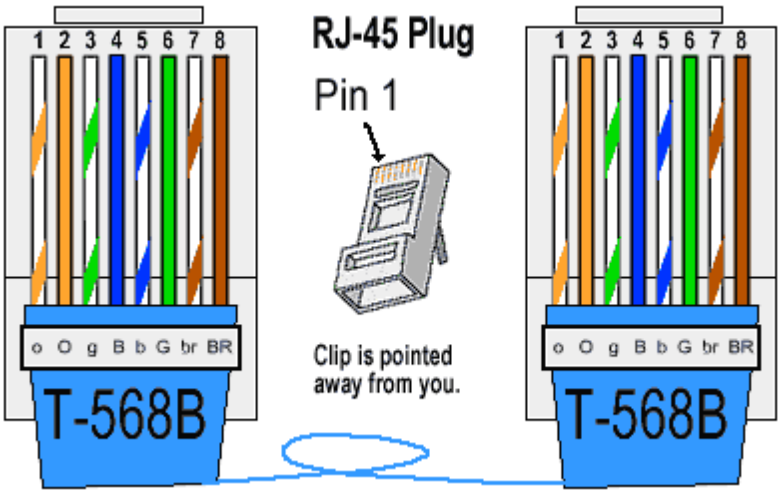
Cable tester is a **cable tester** is a device that is **used to test** the strength and connectivity of a particular type of **cable** or other wired assemblies.

Ethernet cable

Bulk Ethernet Cable - Category 5e or CAT5e

(You may also use Category 6 or CAT6 cabling which has higher performance specifications and is about 20% more expensive than CAT5e.)

Straight trough UTP cable color code



Connector1# connector2#

pins		pins	
1	White orange	1	White orange
2	orange	2	orange
3	White green	3	White green
4	blue	4	blue
5	Blue white	5	Blue white
6	green	6	green
7	White brown	7	White brown
8	brown	8	brown

In straight through cable the pins which send data from one computer connect with the pins which also send data on other computer.

Simple a computer will not be able to pick the data from sending pins. So the transmission will be failed if we directly connect the two systems through the straight UTP cable. To connect two systems directly we have to use the crossover cable which connects sending pins with receiving pins. That's why we cannot use straight through cable two connect two system directly.

CROSSOVER UTP Cable

An Ethernet crossover cable is a crossover cable for Ethernet used to connect computing devices together directly. It is most often used to connect two devices of the same type.

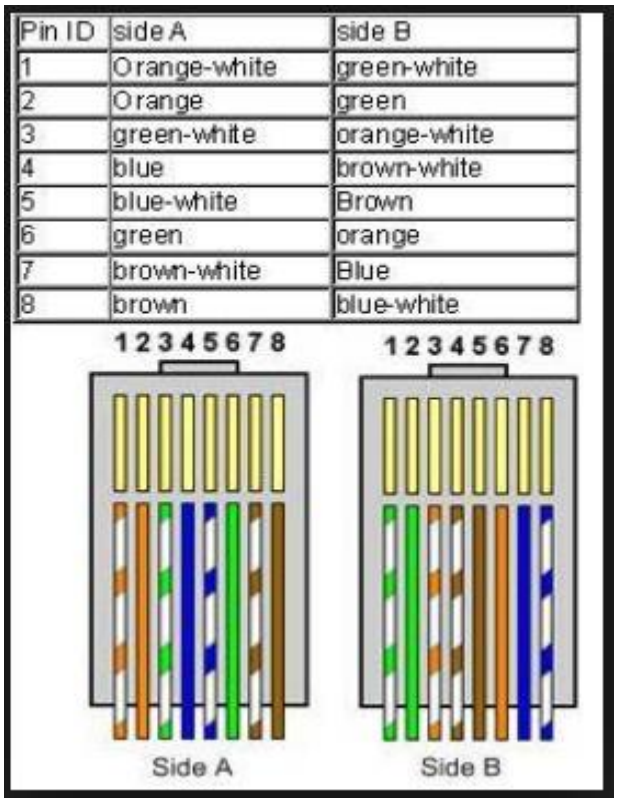
How crossover UTP cable is built and where do we use crossover?

In crossover cable the pins which send data from one end connect with the pins which received data on other end. Pin-1 connects with pin-3 while pin-2 connects with pin-6.

The crossover cable is used to connect the following:

- HUB/SWITCH to HUB/SWITCH
- Router to Router
- System to system

Crossover UTP cable color code



Steps Required To Make Ethernet Cable

Step 1: Strip the cable jacket about 1.5 inch down from the end.

Step 2: Spread the four pairs of twisted wire apart. For Cat 5e, you can use the pull string to strip the jacket farther down if you need to, then cut the pull string. Cat 6 cables have a spine that will also need to be cut.

Step 3: Untwist the wire pairs and neatly align them in the T568B orientation. Be sure not to untwist them any farther down the cable than where the jacket begins; we want to leave as much of the cable twisted as possible.

Step 4: Cut the wires as straight as possible, about 0.5 inches above the end of the jacket.

Step 5: Carefully insert the wires all the way into the modular connector, making sure that each wire passes through the appropriate guides inside the connector.

Step 6: Push the connector inside the crimping tool and squeeze the crimper all the way down.

Step 7: Repeat steps 1-6 for the other end of the cable.

Step 8: To make sure you've successfully terminated each end of the cable, use a cable tester to test each pin.

- ✓ **Token Ring** is a computer networking technology used to build local area networks. It uses a special three-byte frame called a **token** that travels around a logical **ring** of workstations or servers.

  How does a token ring work?

  A token ring network is a local area network (LAN) in which all computers are connected in a ring or star topology and pass one or more logical tokens from host to host. Only a host that holds a token can send data, and tokens are released when receipt of the data is confirmed.

- ✓ **Fiber Distributed Data Interface(FDDI)**

  FDDI stands for Fiber Distributed Data Interface. It is a high-speed, high-bandwidth network based on optical transmissions. It is most often used as a network backbone, for connecting high-end computers (mainframes, minicomputers, and peripherals), and for LANs connecting high-performance engineering, graphics, and other workstations that demand a rapid transfer of large amounts of data. It can transport data at a rate of 100 Megabits per second and can support up to 500 stations on a single network. FDDI was designed to run through fiber cables, transmitting light pulses to convey information between stations, but it can also run on copper using electrical signals. It is relatively expensive to implement, although the mixing of fiber-optic with copper cabling can hold down the cost.

LO 1.4 – Set up a LAN and shared devices

- **Content/Topic 1 Steps of Setting up a simple LAN**

  Gather your network hardware. To create a LAN, you'll need a router or switch, which will act as the hub of your network. These devices route information to the correct computers.

  A **router** will automatically handle assigning IP addresses to each device on the network, and is necessary if you intend to share your internet connection with all the connected devices. It is highly recommended that you build your network with a router, even if you're not sharing an internet connection.

A **network switch** is like a simpler version of a router. It will allow connected devices to talk to each other, but will not automatically assign IP addresses and will not share an internet connection. Switches are best used to expand the number of LAN ports available on the network, as they can be connected to the router.

Set up your router. You don't need to do much to set up a router for a basic LAN. Just plug it into a power source, preferably close to your modem if you plan on sharing the internet connection through it.

Connect your modem to your router (if necessary). If you're sharing the internet connection from your modem, connect the modem to the WAN/INTERNET port on the router. This is usually a different colors from the other ports.

Connect your switch to your router (if necessary). If you're using a switch to expand the number of ports available on the router, plug an Ethernet cable into any LAN port on the router and any LAN port on the switch. This will expand the network to the rest of the LAN ports on the switch.

Connect your computers to open LAN ports. Use Ethernet cables to connect each computer to an open LAN port on your router or switch. It doesn't matter what order the ports are connected in.

Setup one PC as a DHCP server if you're just using a switch. If you're only using a switch as your network hub, setting up one computer as a DHCP (Dynamic Host Configuration Protocol) server will allow all of the connected computers to easily obtain IP addresses.

You can quickly create a DHCP server on one of your computers.

The rest of the computers on the network will obtain IP addresses automatically once the server is running, as long as they are set to do so.

Verify the network connection on each computer. After each computer obtains an IP address, they'll be able to talk to each other on the network. If you're using a router to share your internet connection, each computer will be able to access the internet.

Set up file and printer sharing. Once your network is up, you won't see anything on other computers unless that computer has shared files.

Press “OK” and then “Close”.

Setup wireless computer to the router steps:

1. Select where to place the router

2. Connect router to the internet
3. Configure the wireless router to the gateway
4. Connect gateway to router
5. Use application or web dashboard
6. Create a username and password
7. Update the router firmware
8. Create WIFI password

Setup access point to the router connection steps

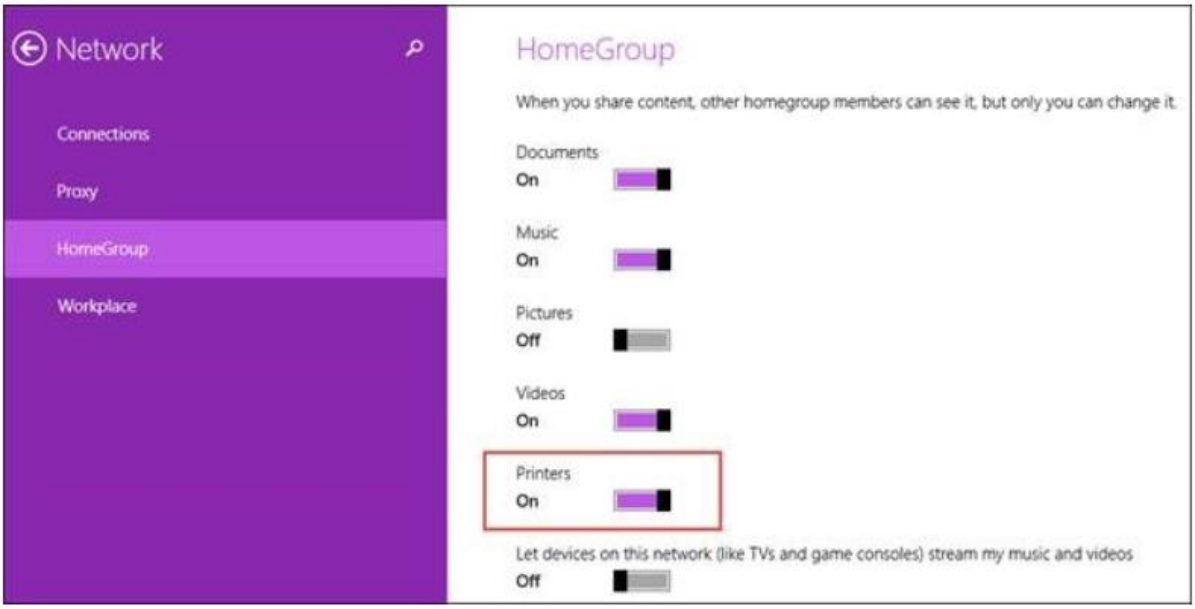
1. Connect router to your existing router via Ethernet cable
2. Attach the new router to be used AP
3. Attach the power cable to the rear electrical outlet and turn on them
4. Wait until the device initializes.
5. Enter the AP router's IP address in your browser bar and press enter. For example the ip address might be "192.168.1.1" when you press the enter ey, you will be prompted by the webpage to enter your AP router's username and password. By default username and password are "admin", "admin" or "admin", "password" in some AP routers you only need to enter "admin" in the field and leave the the username field lack. Click ok or login
6. Once the AP router's webpage loads, click the wireless tab
7. Enter your WI-FI password field and click save
8. You can connect your mobile devices to either the router or AP.

- **Content /Topic 2 Sharing network Devices on LAN**

How to Share Your Printer with the Homegroup

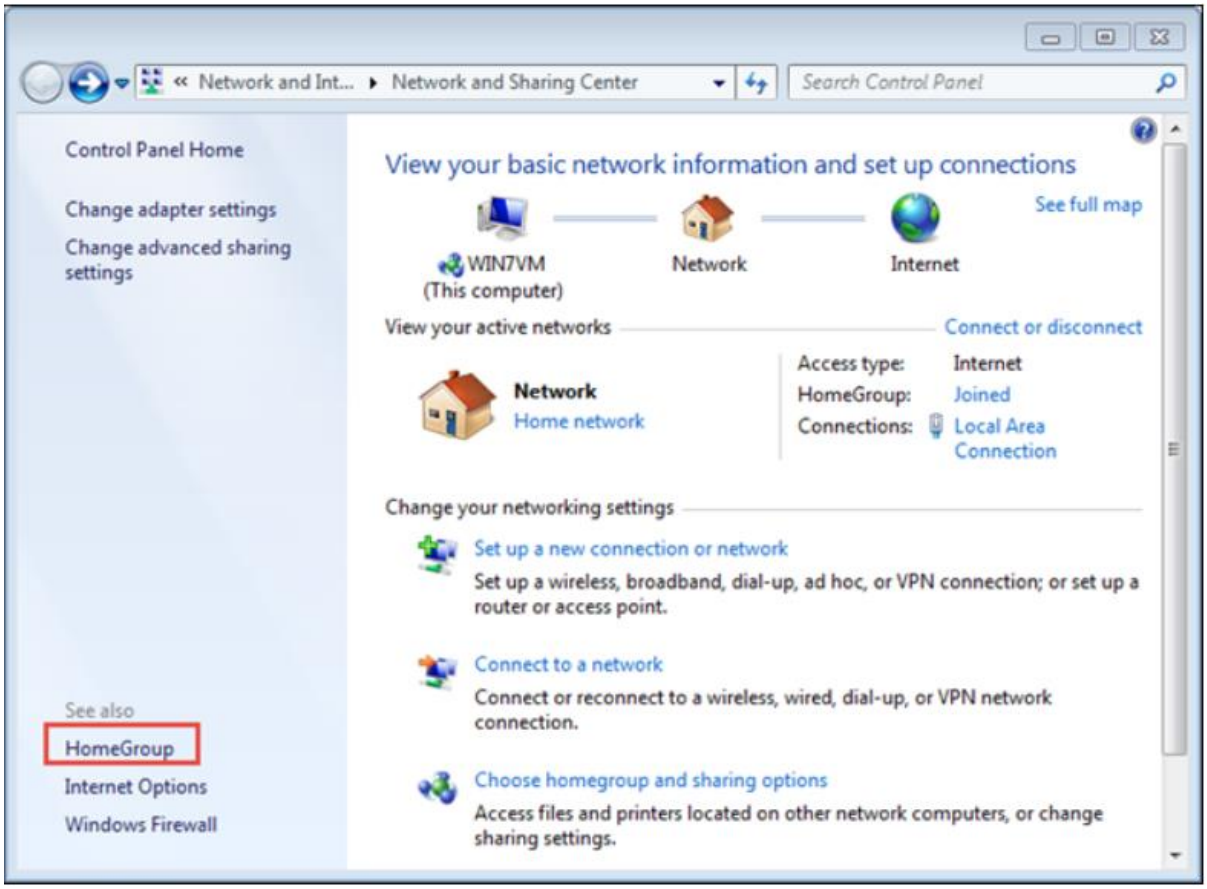
Sharing your local printer with the Homegroup is incredibly easy. In Windows 8.x, go to PC Settings and then to "Network > HomeGroup". There you will find several switches for sharing with the Homegroup.

Find the one named "Printers" and set it to "On".

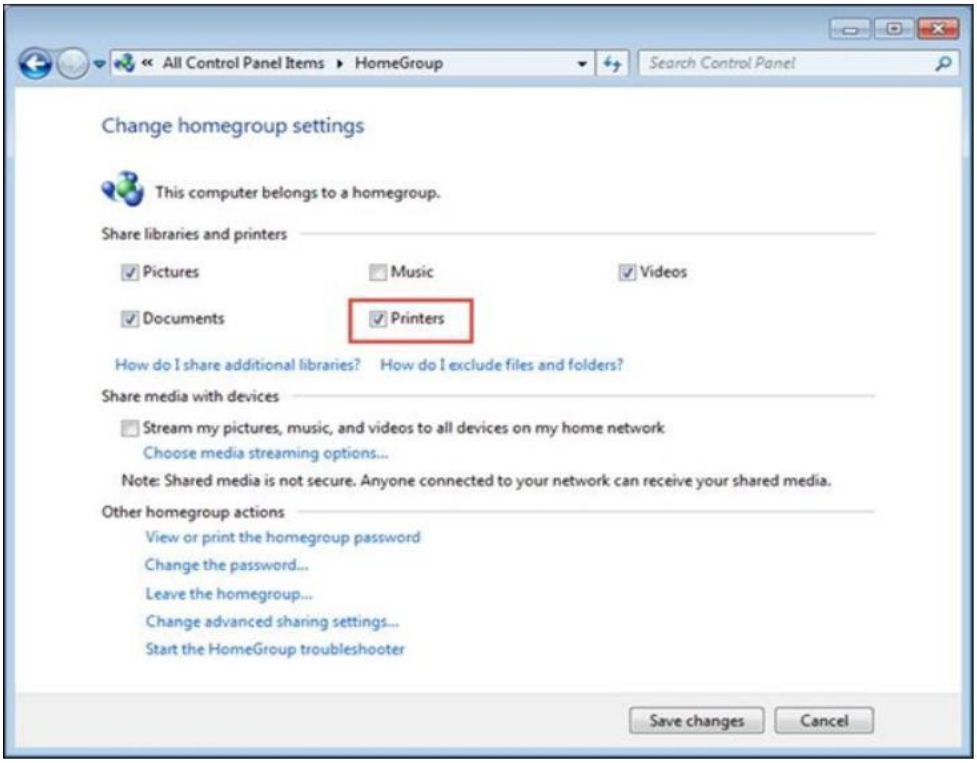


Any printer that is connected to your Windows 8.x PC or device is now shared with others on the Homegroup.

In Windows 7, go to the Control Panel and then to “Network and Internet > Network and Sharing Center”. In the column on the left, click “HomeGroup”.



In the HomeGroup window check the box for “Printers” and press “Save changes”.

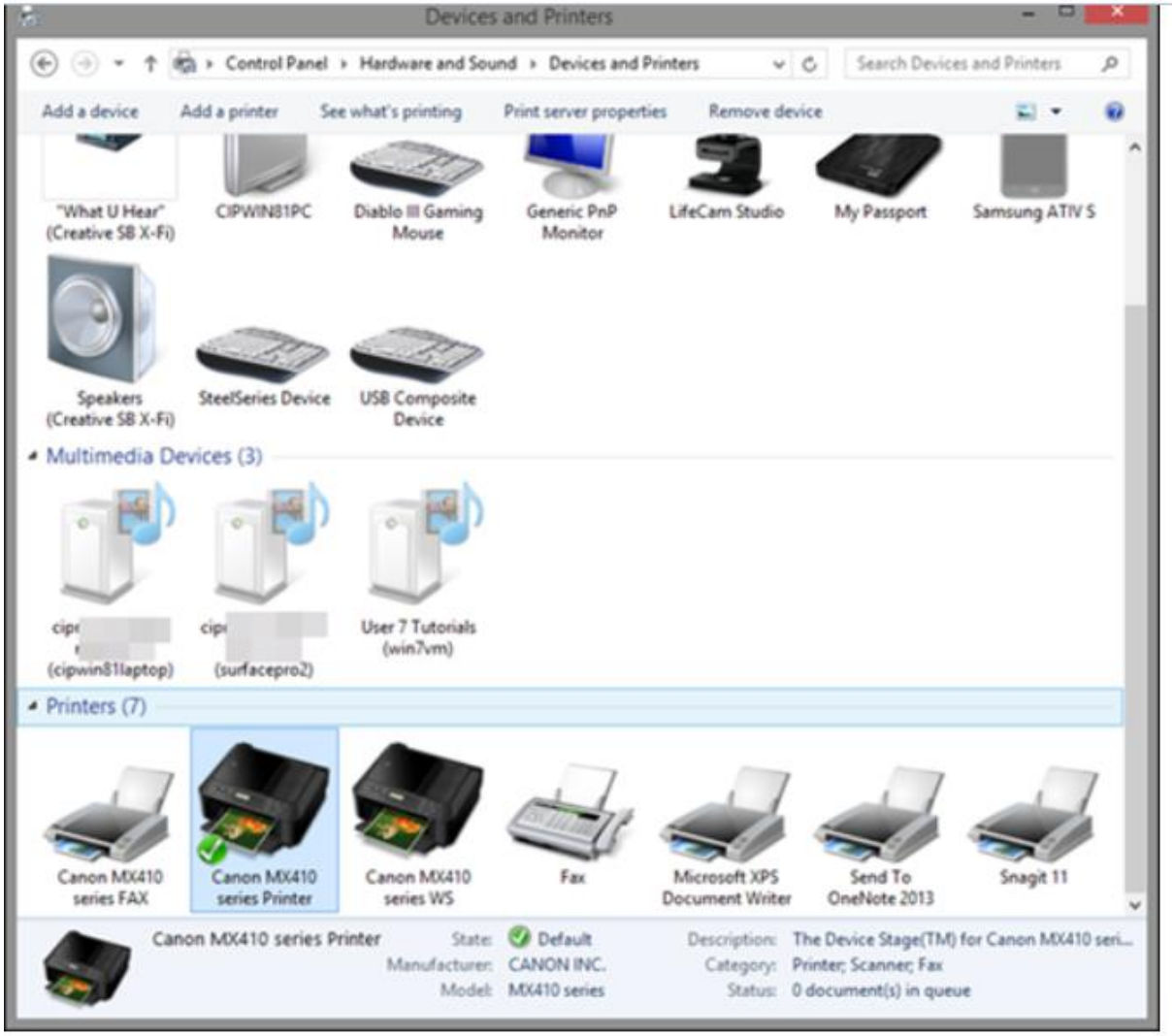


Any printer that is connected to your Windows 7 PC is now shared with others on the Homegroup. If you need a refresher about the Homegroup and how it can be used for network sharing, don't hesitate to read Lesson 5.

How to Share Your Printer with the Network

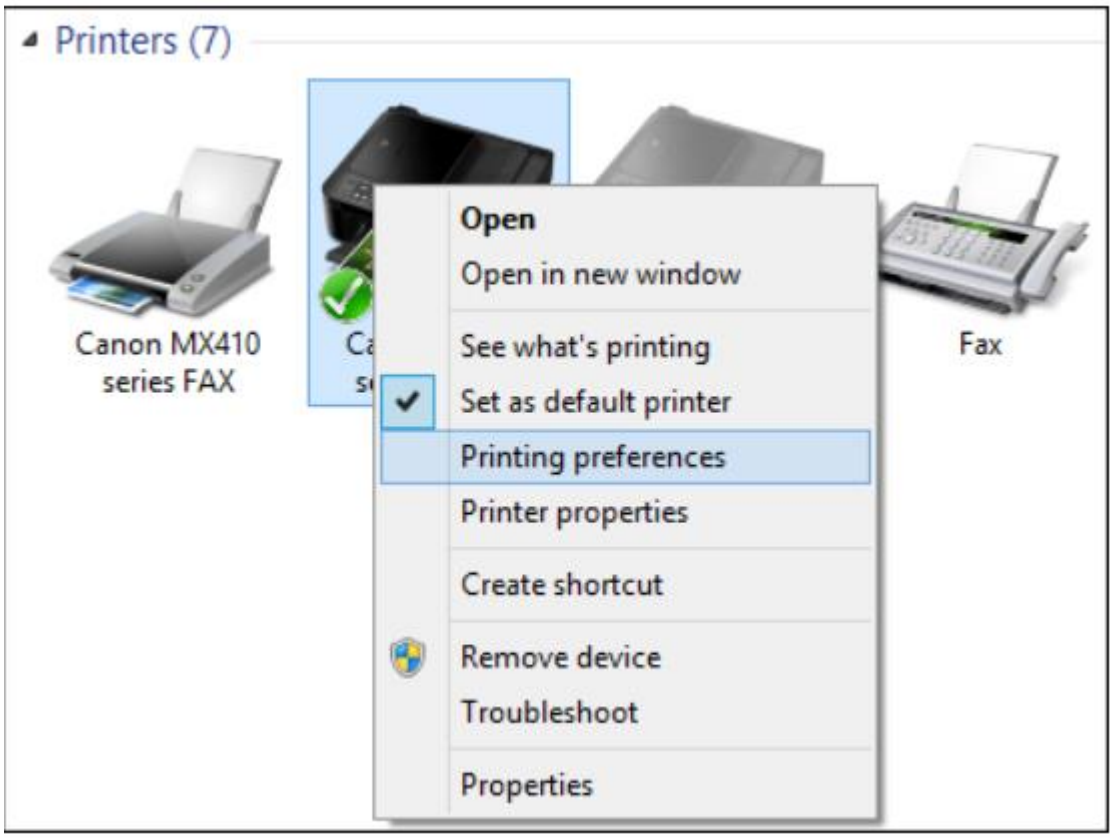
If you have a network with operating systems other than Windows 7 and Windows 8.x, you may want to share your local printer using a different method, so that the printer can be discovered by all the computers in the network.

First, open the Control Panel and then go to "Hardware and Sound > Devices and Printers". Here you will find all the external devices that are connected to your Windows PC or device. Things like webcams, keyboards, external hard drives, printers, etc.

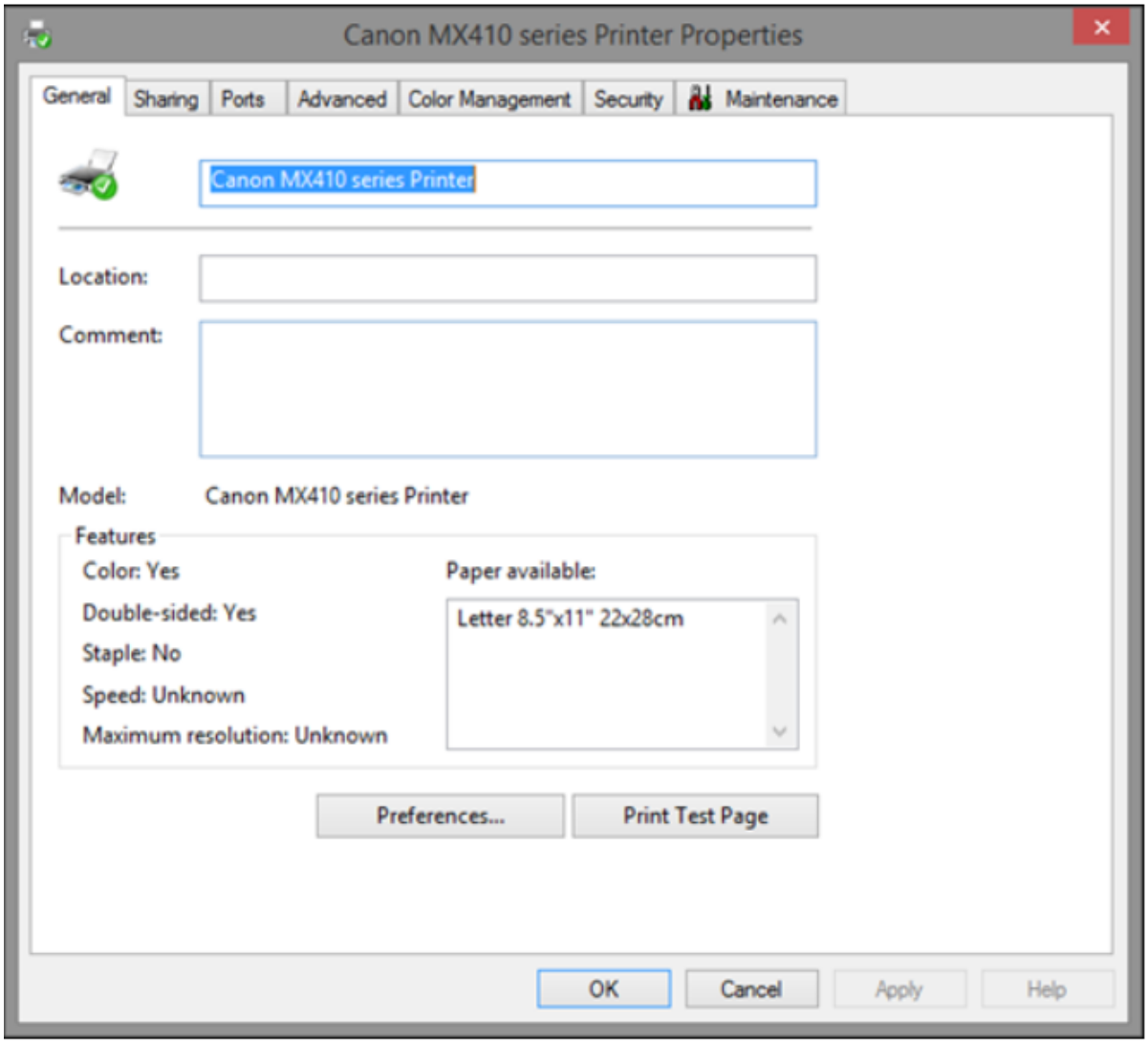


Your local printer is displayed in the “Printers” section alongside virtual printers installed by the software on your PC or device.

Right-click or press and hold the printer you want to share with the network, and select “Printing preferences”.

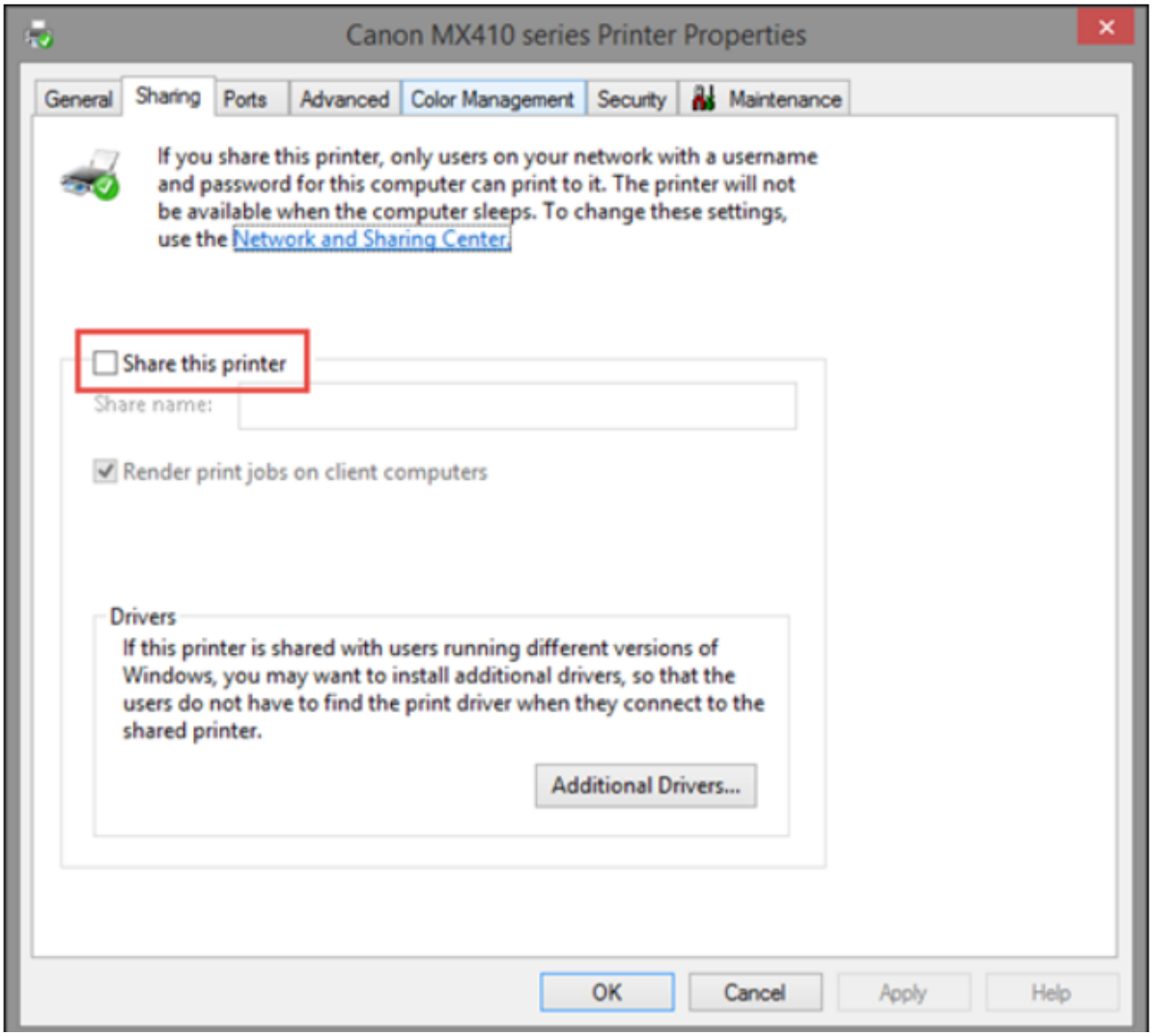


The “Printer Properties” window is shown. Here you can configure all the important aspects of your printer and you can also share it with the network.



Since we are interested in sharing it with others on the network, go to the “Sharing” tab. You are informed that the printer will not be available when your computer sleeps or it is shut down. Also, if you are using password protected sharing (see Lesson 3 for a refresher), you are informed that only users on your network with a username and password for this computer can print to it.

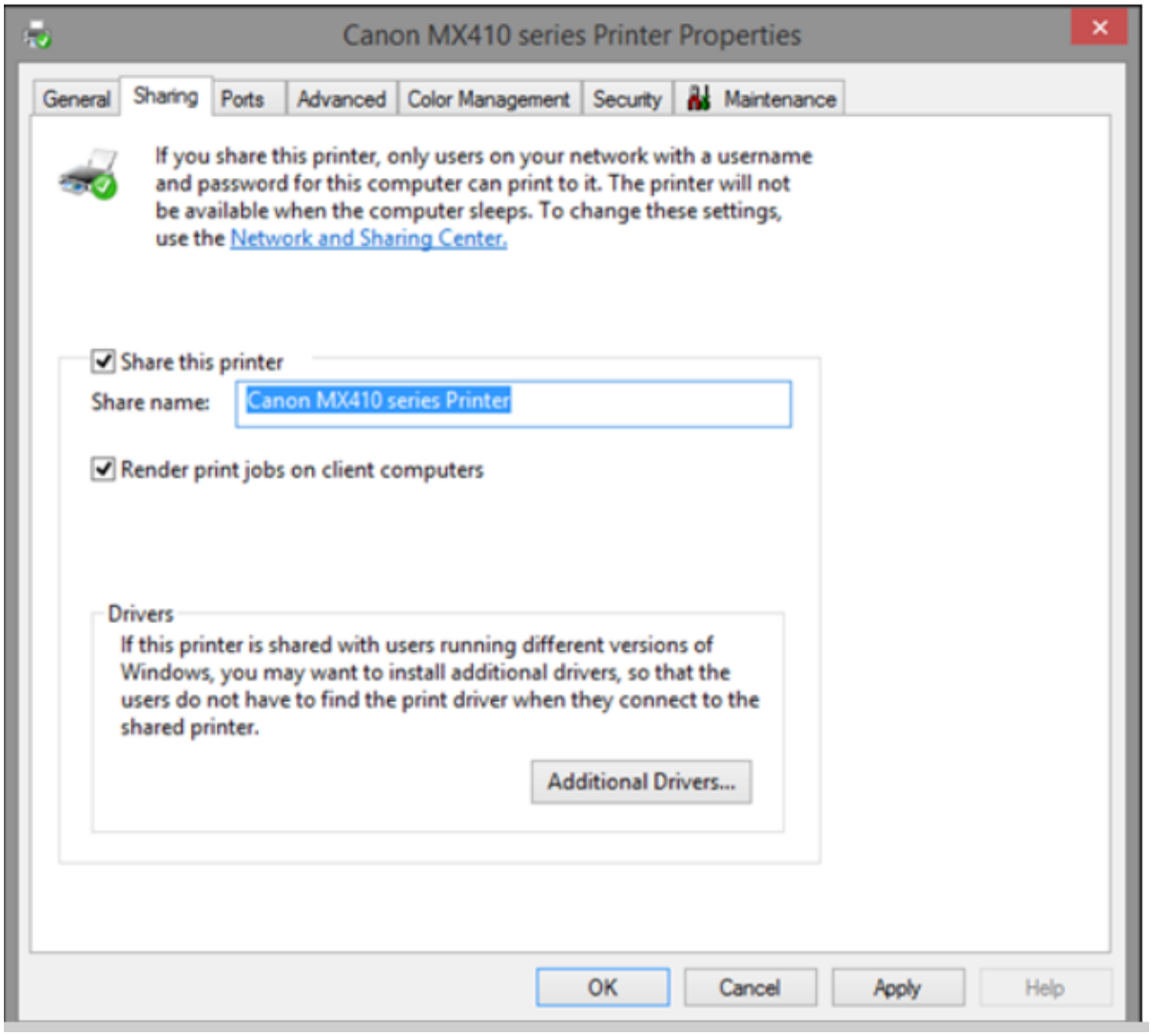
To share your printer, check the box that says “Share this printer”.



The printer will be shared using its default product name and version. You can customize its share name by typing something else. You can also set whether you would like to render print jobs on client computers.

If this setting is enabled, all the documents that will be printed are rendered on the computers that order the printing process. When this setting is disabled, the documents are rendered on the computer to which the printer is attached.

We recommend enabling this setting so that system performance is not impacted on the computer to which the printer is attached, every time something gets printed.



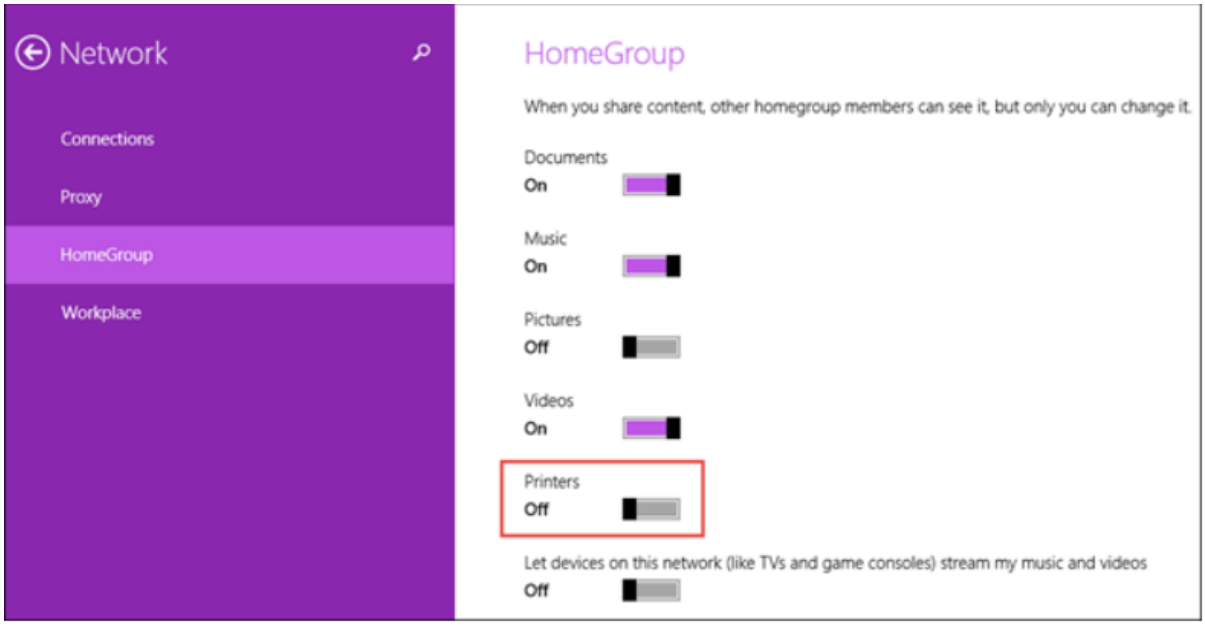
To share the printer with the network, press “OK”.

Other computers can install the printer you are sharing as a network printer and use it when they need to print something.

How to Stop Sharing the Printer with the Homegroup

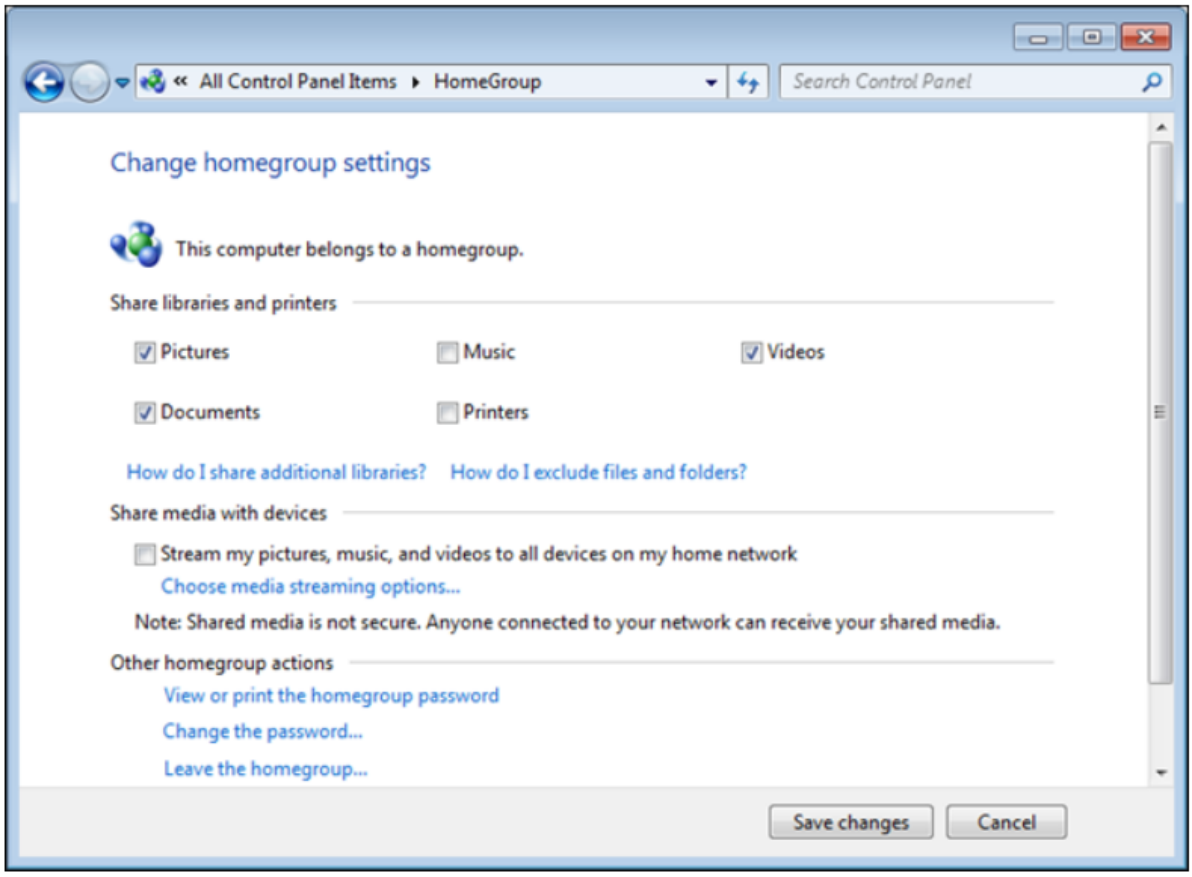
The steps involved when you want to stop sharing your printer with the Homegroup are the same as when you start sharing it.

In Windows 8.x, go to PC Settings and then to “Network > HomeGroup.” Set the switch for “Printers” to “Off”.



All the local printers attached to your PC or device are no longer shared with the Homegroup.

In Windows 7, go to the Control Panel and then to “Network and Internet > Network and Sharing Center”. In the “Network and Sharing Center” go to the column on the left and click “HomeGroup”. In the “HomeGroup” window clear the box for “Printers” and press “Save changes”.

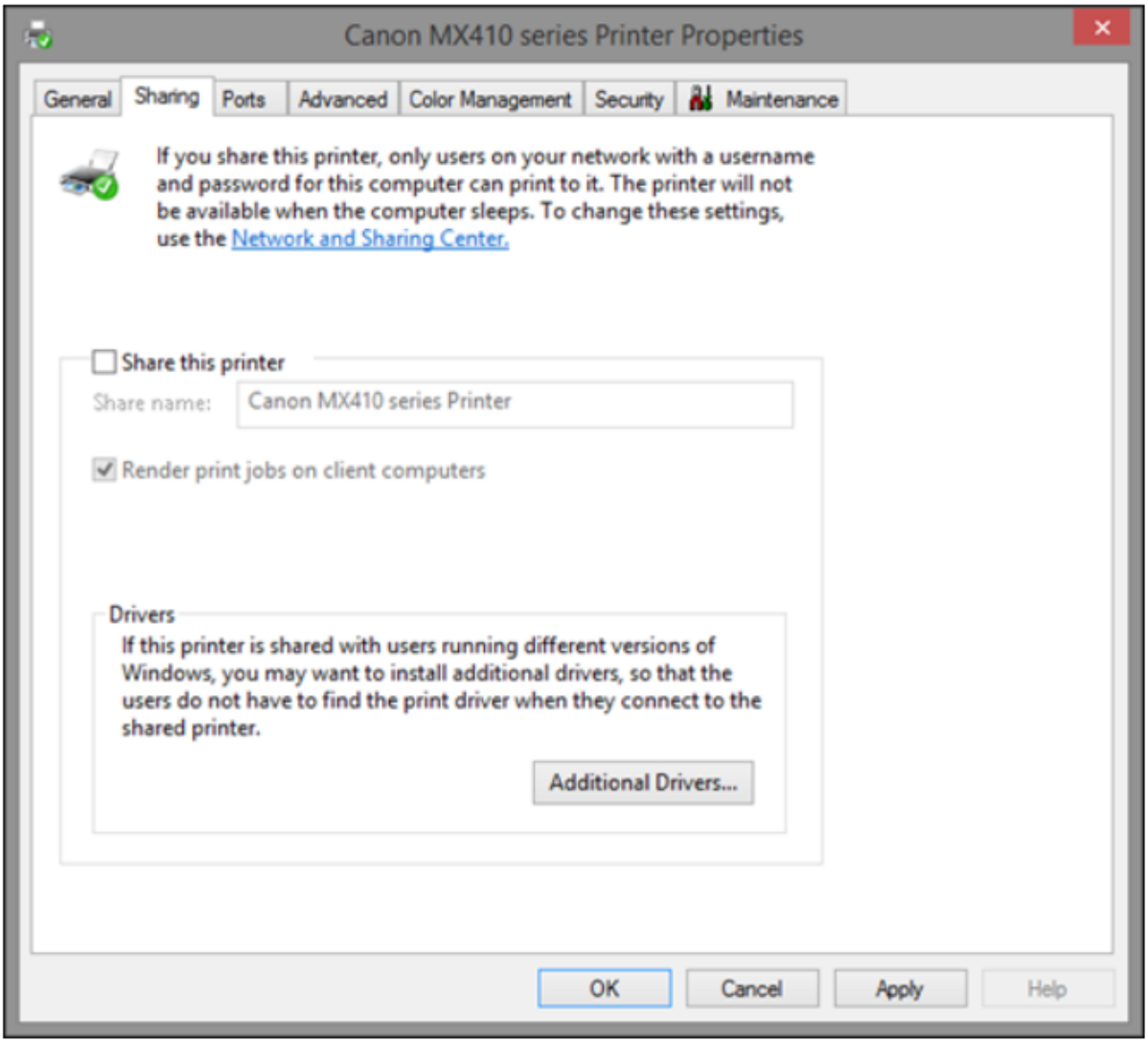


All the local printers attached to your PC are no longer shared with the Homegroup.

Keep Reading…

How to Stop Sharing the Printer with the Network

The steps involved when you no longer want to share a printer with the network are the same as when sharing it. Follow the instructions in the “How to Share Your Printer with the Network” section, found earlier in this article. Then, in the “Printer Properties” window, go to the “Sharing” tab, clear the box for “Share this printer” and press “OK”.



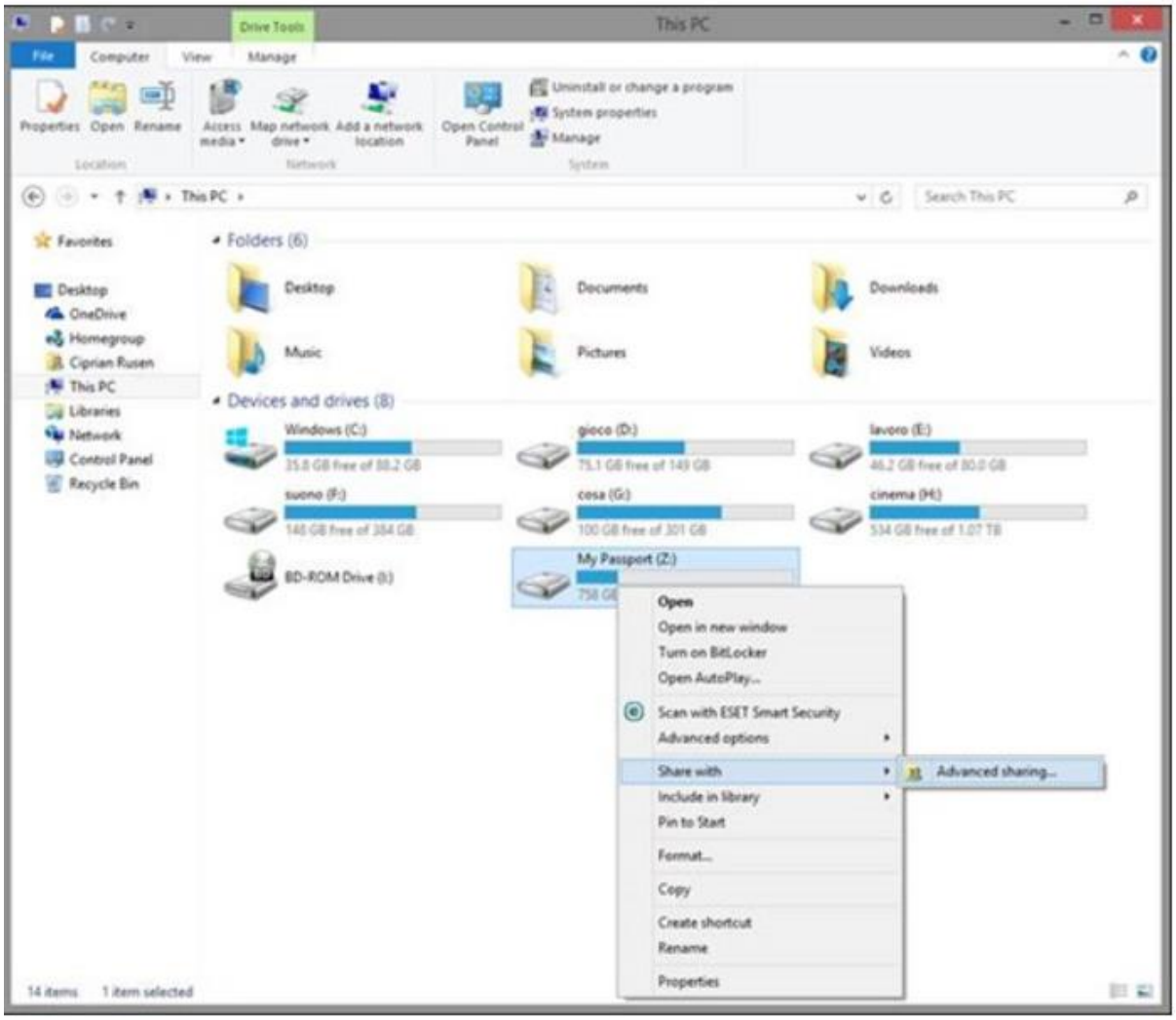
Your local printer is no longer shared with others on the network.

How to Share Partitions or External Hard Drives with the Network

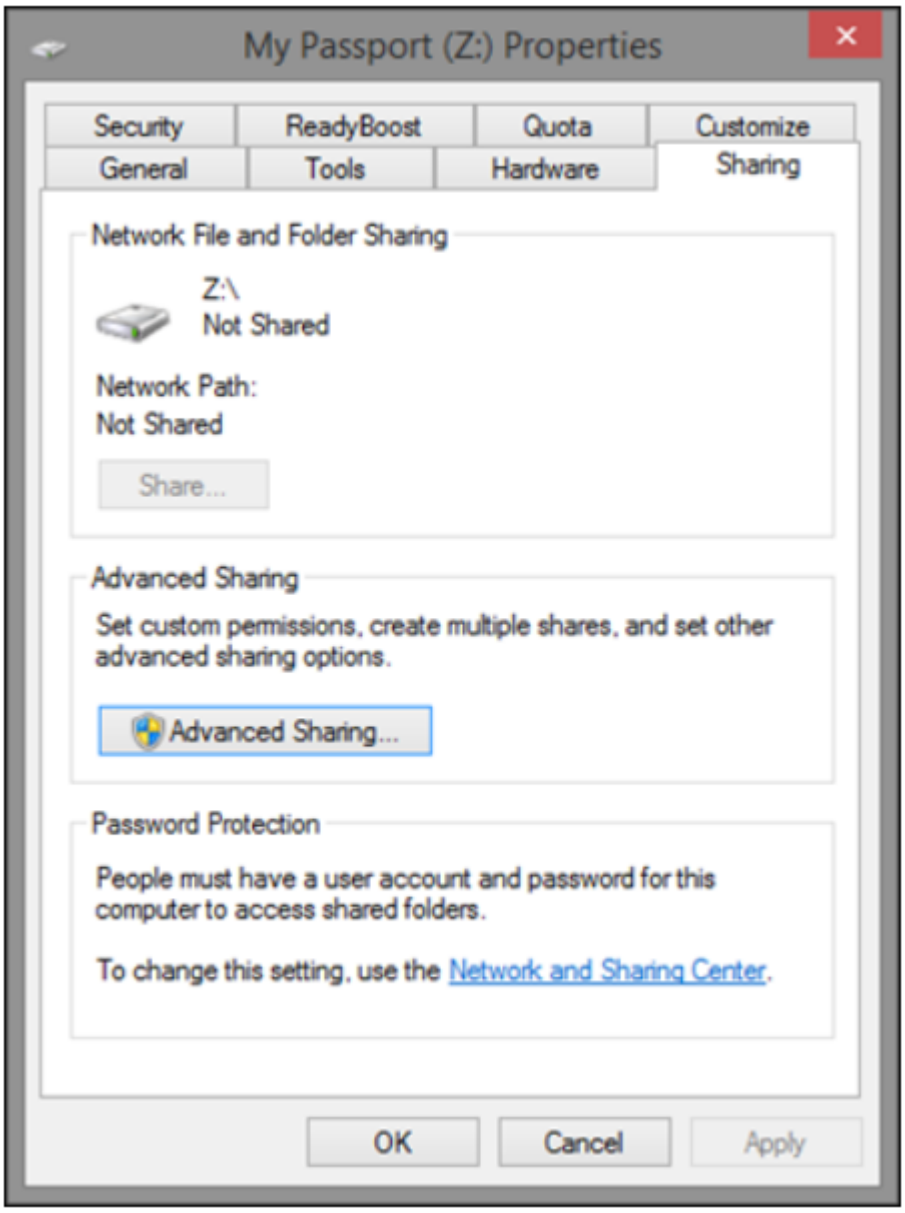
Sharing entire partitions or external hard drives with others on the network is done only through "Advanced Sharing". If you need a refresher about this concept, please read Lesson 7. In this section we won't spend time explaining all the available sharing options and we will only take you through the procedure that's involved when sharing a drive.

If you are using Windows 8.x, open File Explorer and go to This PC. If you are using Windows 7, open Windows Explorer and go to Computer.

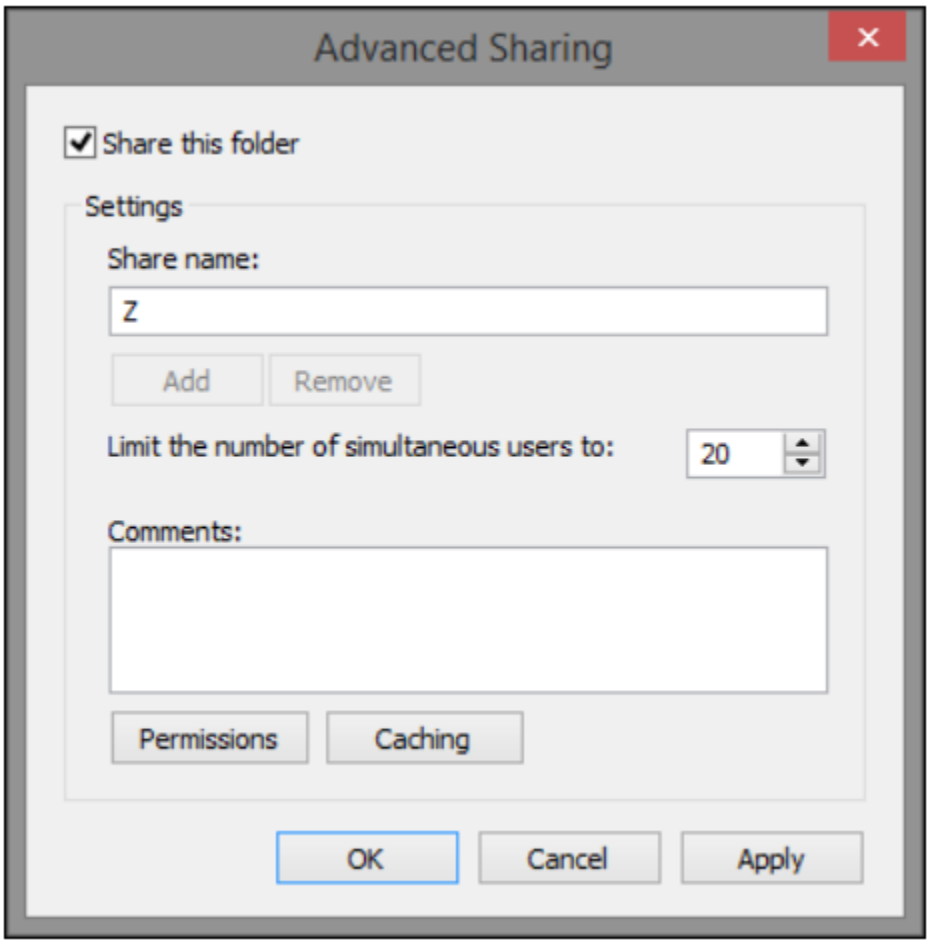
Find the partition or the external hard drive you want to share with others on the network and right-click or press and hold on it. In the right-click menu go to "Share with > Advanced sharing".



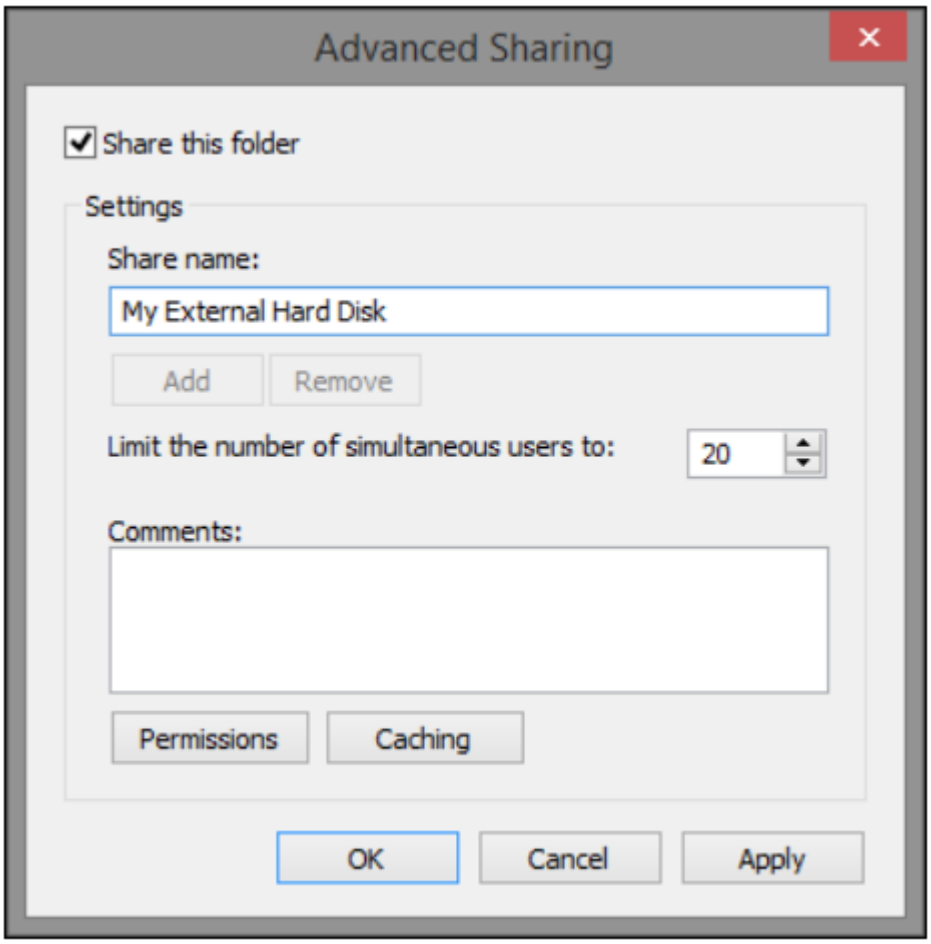
The “Properties” window is shown for the selected drive. In the “Network File and Folder” sharing section of the “Share” tab you can view if it is already shared or not. Press the “Advanced Sharing” button.



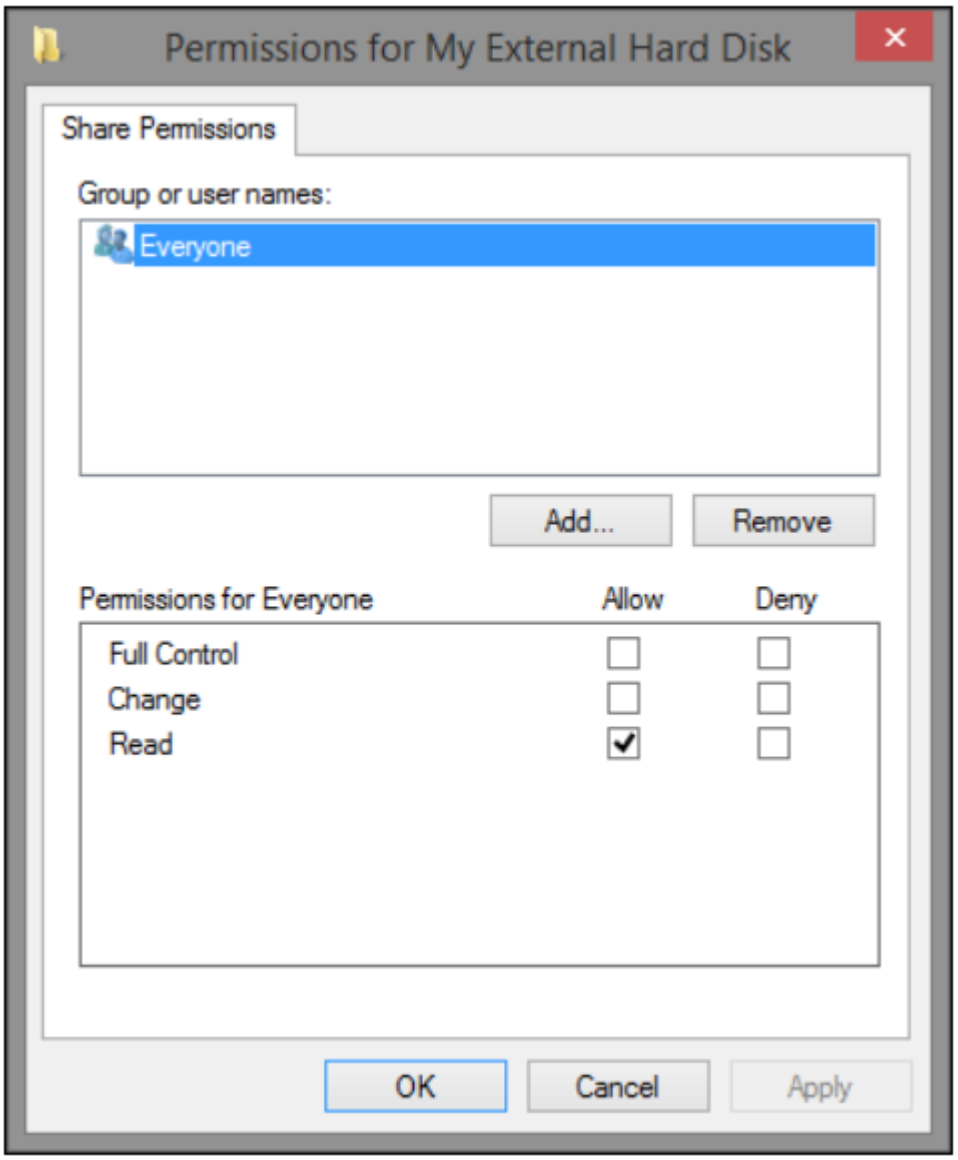
In the “Advanced Sharing” window, check the box that says “Share this folder”. By default, drives are shared using their letter.



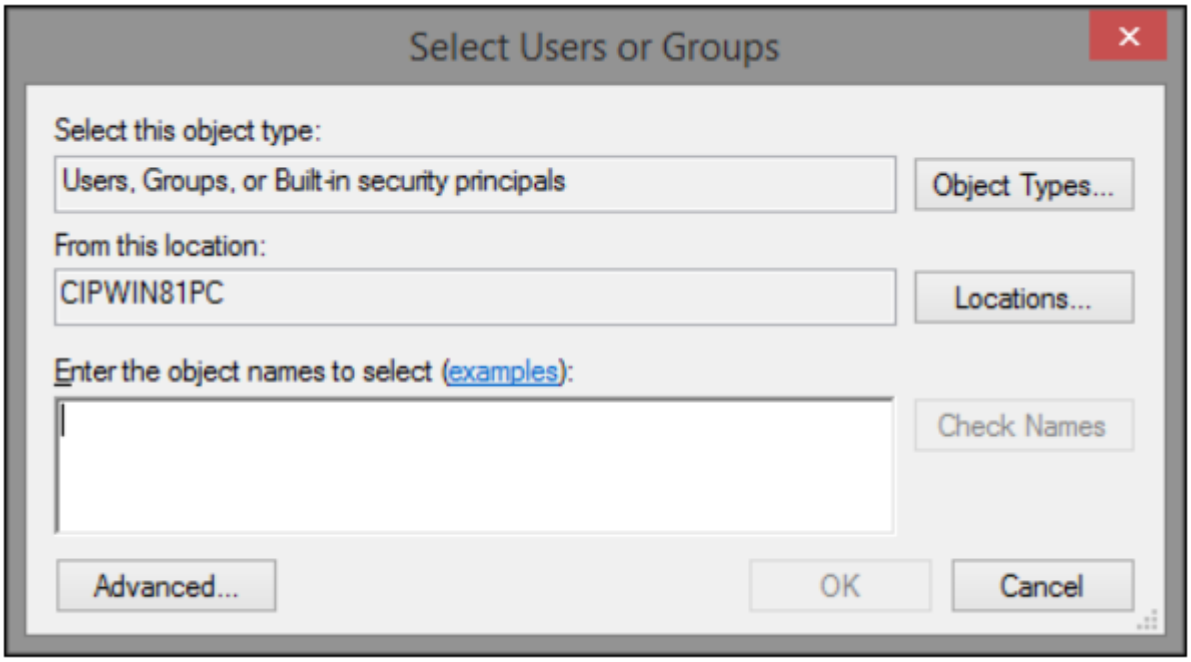
You can type a more descriptive share name. You can also limit the number of simultaneous users connecting to it over the network. To edit who received permissions for accessing this share drive, press the “Permissions” button.



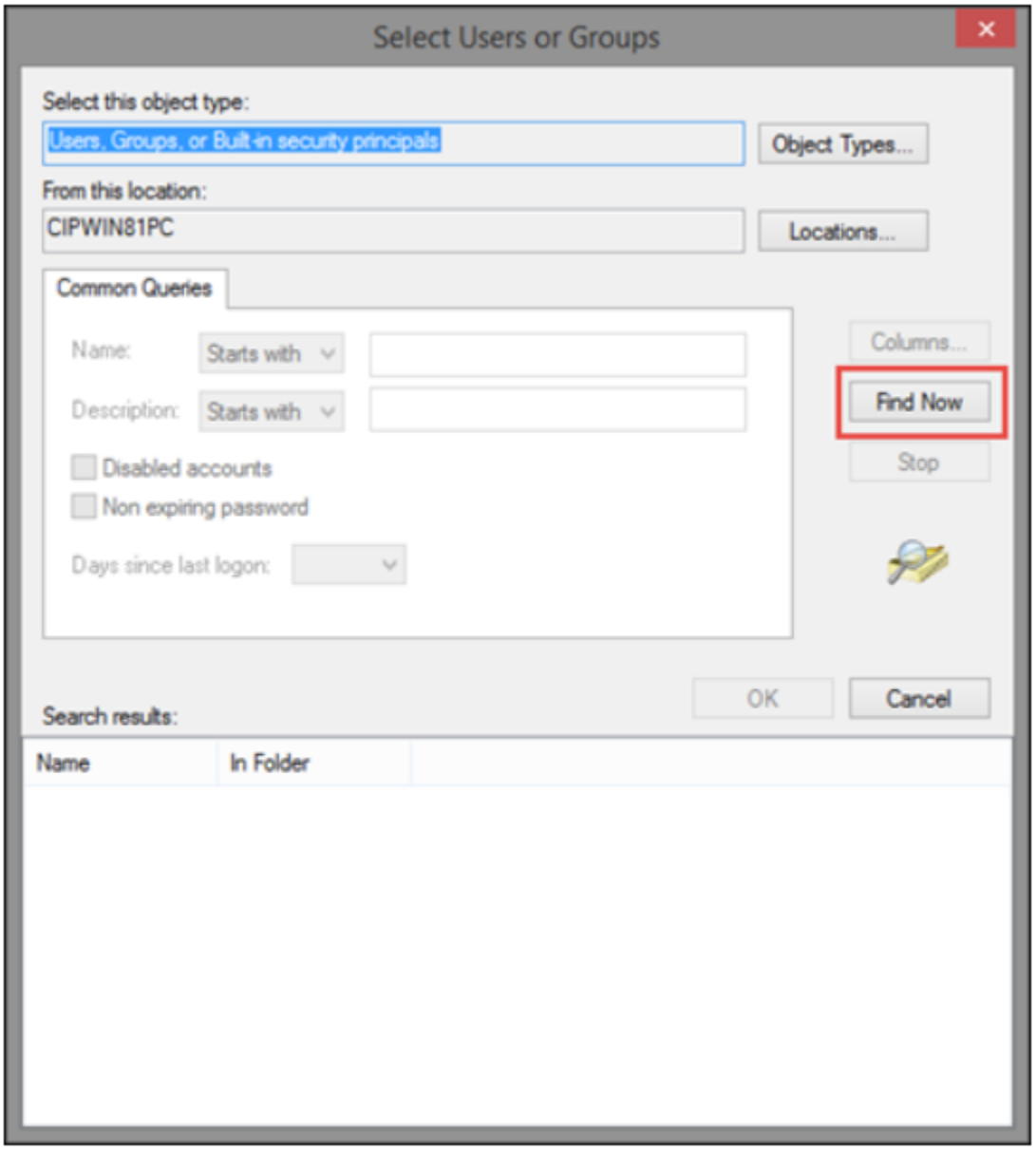
In the “Permissions” window you will see that the drive is shared with the “Everyone” user group. If you don’t want to share your printer with everyone on your network, then “Remove” this user group and press “Add” to give access to someone else.



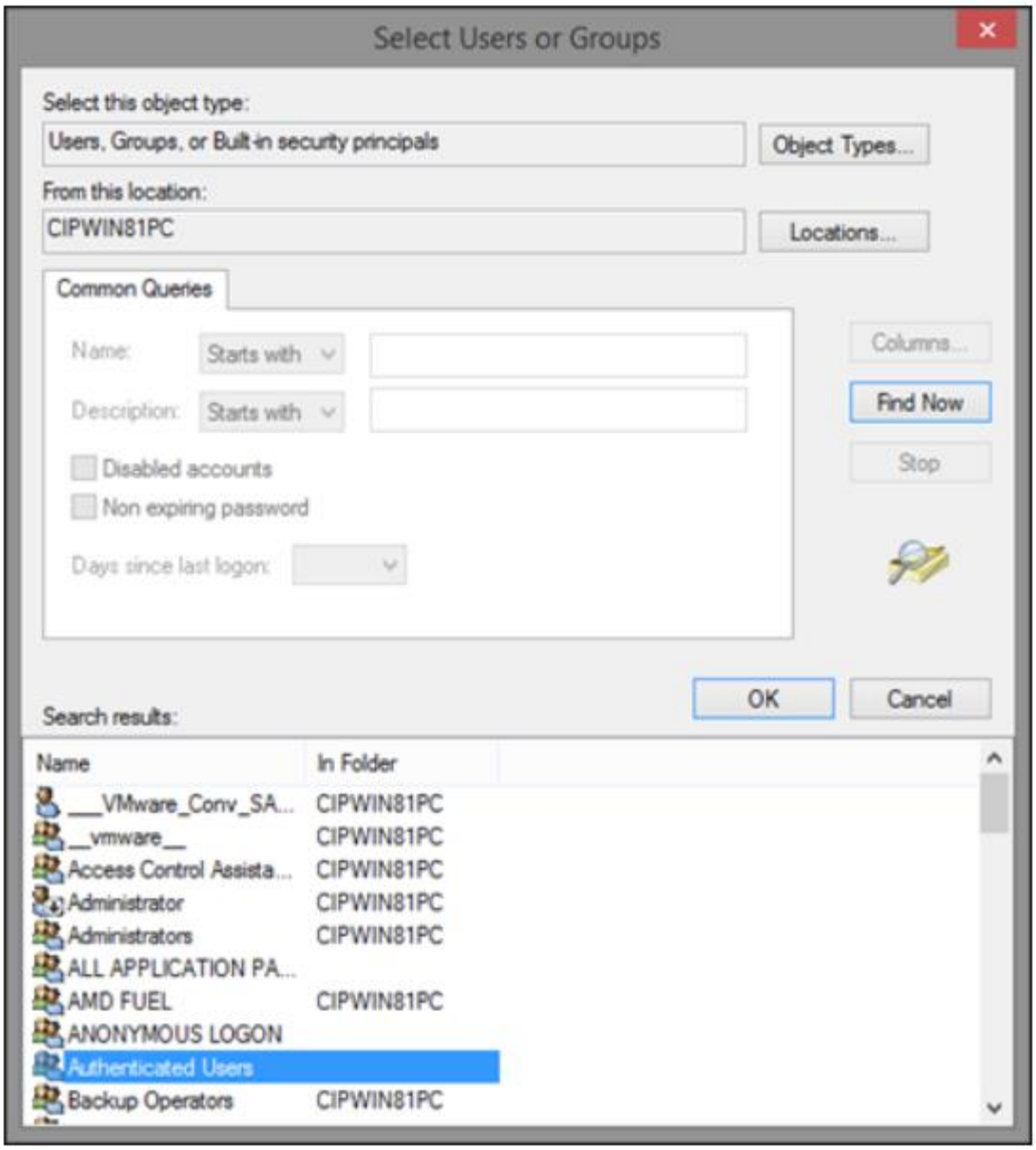
The “Select Users or Groups” window is now shown. Press the “Advanced” button.



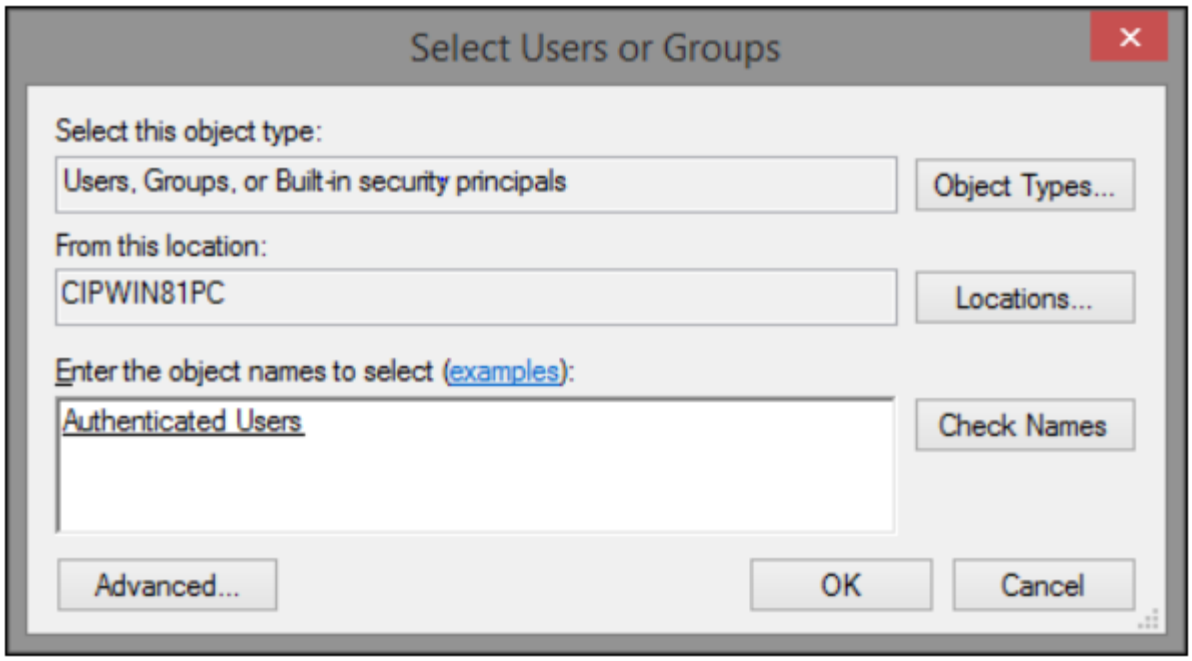
Then, click or tap “Find Now”.



Windows displays a list with all the user accounts and user groups existing on your computer. Select the user account or the user group you want to share the printer with. If you want to share it with the Homegroup, you need to select the “HomeUsers” group, then click or tap “OK”.

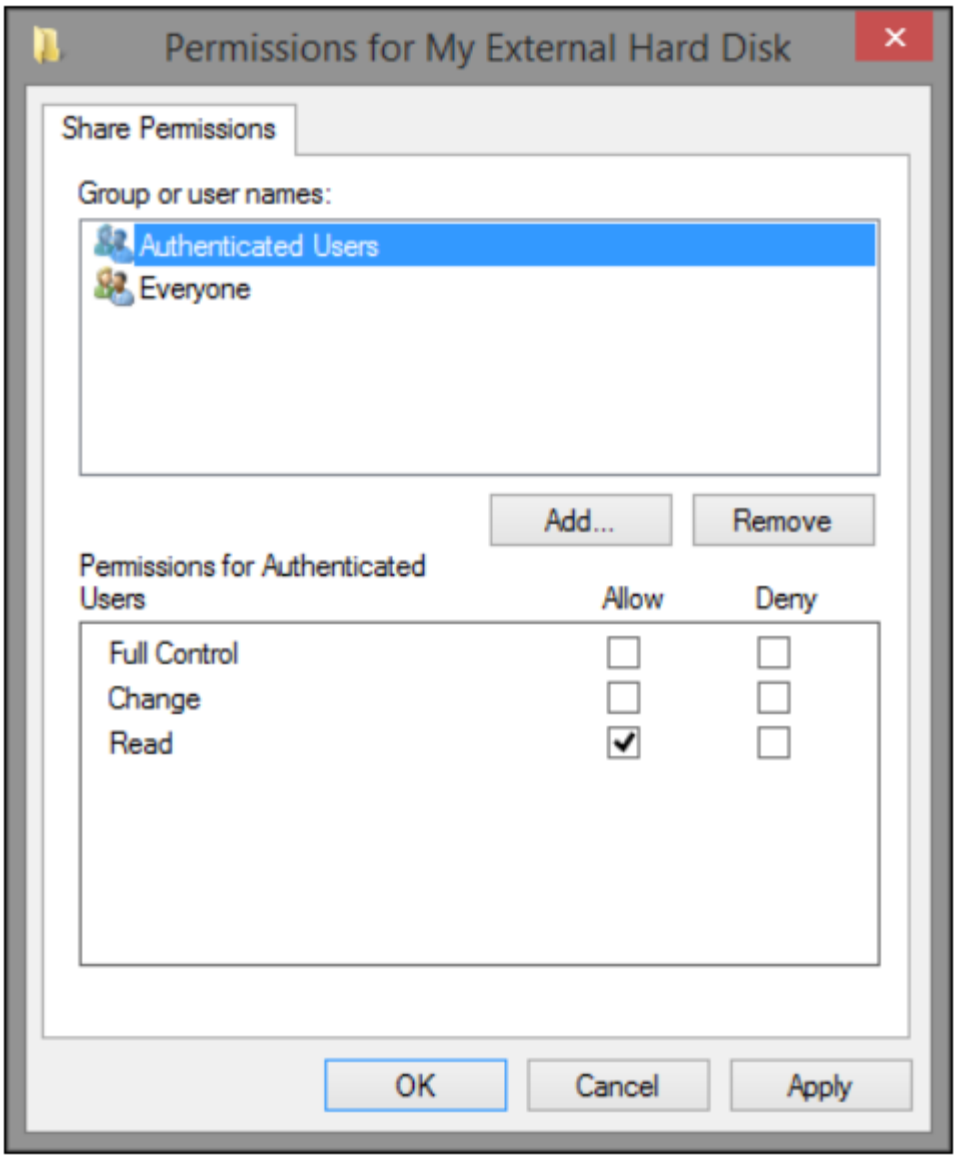


Click or tap “OK” in the Select Users or Groups window.



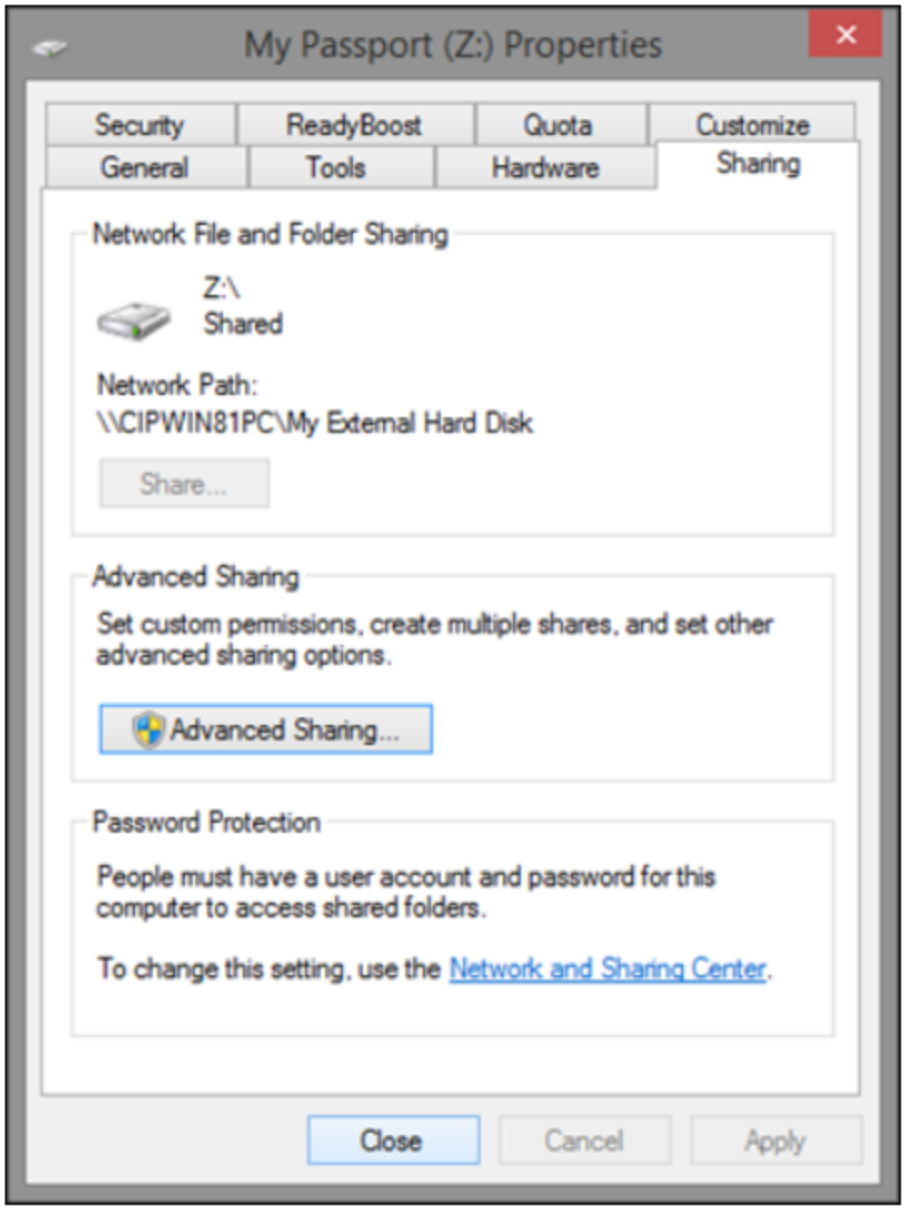
You are back to the “Permissions” window. Here you can modify the permissions assigned to all the user accounts or user groups you have added. If you would like to learn more about all the available permission levels and what they do, please read Lesson 7.

When you are done setting things up, press “OK”.

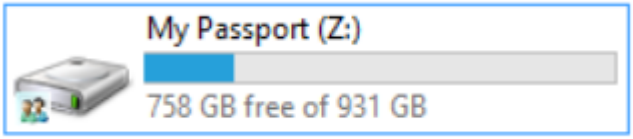


The selected drive is now shared with the network and you can see its network path in the "Network File and Folder Sharing" section.

Press "Close" and you are done.



Each time you view the shared drive in File Explorer or Windows Explorer, it will see a small icon on its bottom-left corner, signaling that the drive is shared with others.

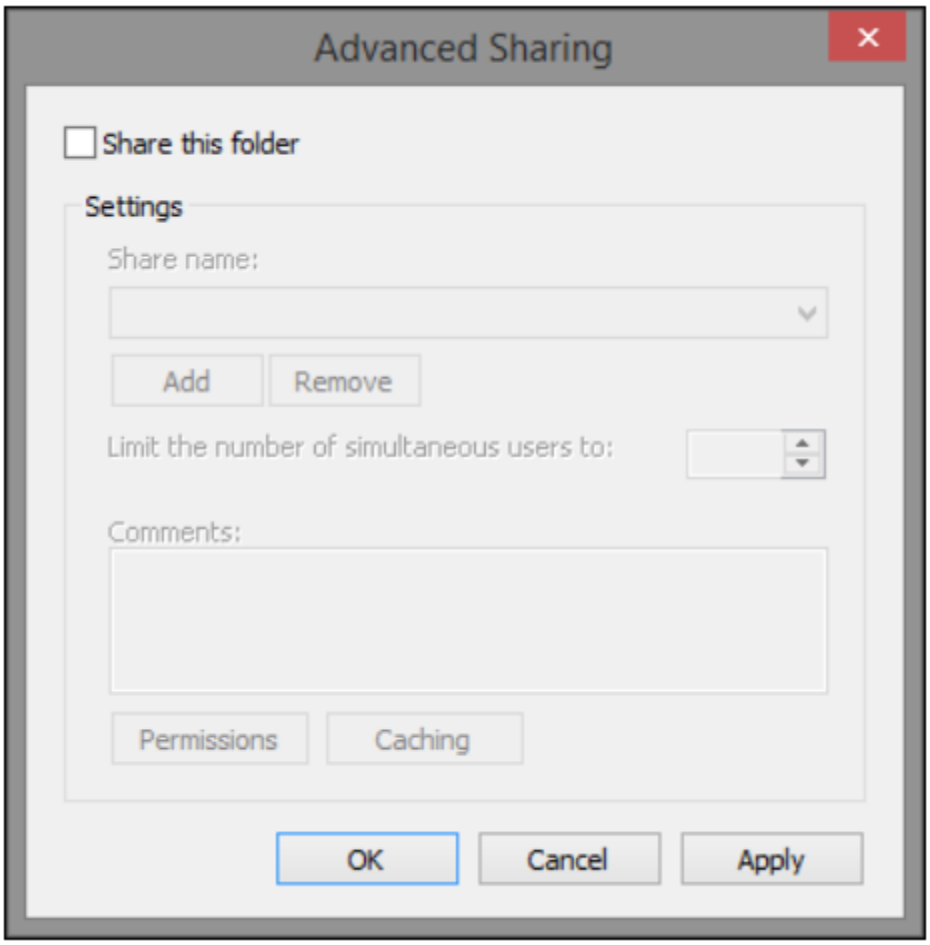


If you will stop sharing this drive, the icon will be no longer displayed.

How to Stop Sharing a Partition or an External Hard Drive

To stop sharing a drive from your computer, you need to follow the same steps as for sharing it.

When you get to the Advanced Sharing window, clear the box that says “Share this folder”.



Learning Unit 2 – Conduct site survey

LO 2.1 – Analyze facilities and existing networks

- Content/Topic 1 Analysis of site planning process

Site planning in landscape architecture and architecture refers to the organizational stage of the landscape design **process**.

Site planning process in network creation include: Initial environment evaluation and Selection of router deployment that match on the location of where signals are worked properly.

✓ **Initial environment evaluation: Initial environment** examinations describe the environmental condition of the project, including potential impact, formulation of mitigation measurement and preparation of institutional requirements and environmental monitoring.

✓ **Selection of router deployment:** you can select router that match on the location where signals are work properly.

Environment evaluation is a Process of estimating and **evaluating** significant short-term and long-term effects of a program or project on the quality of its location's **environment**.

A. **Physical site survey methodology**

- **Passive physical site survey methodology:** Passive surveys are surveys that are performed with a listen-only mode. Passive site surveys listen to existing access points and, outside your managed infrastructure, for signal strength, wireless interference, and AP coverage.
- **Active survey methodology**: This survey is performed after a wireless network has been just deployed, or to check the health of an existing network. An Active Survey measures signal coverage, throughput tests SSID and VLAN per AP allocation and behaviour of data packets. There are two main methods used in active surveys:

  - **Basic Service Set Identifier (BSSID)** Method USE 48-Bits that identifies an AP in an infrastructure network or STP in an Ad Hoc network.

  - **Service Set Identifier (SSID)** Method is simply the technical term for a wi-fi network name. When you set up a wireless home network, you give it name to distinguish it from other network in your neighbourhood.

  You should expect the following information from a site survey:

- Provide accurate information on the working condition of each current access point.
- Provide accurate information for access point locations.
- Provide detailed wireless coverage maps.
- Provide detailed data rates.
- Identify sources and locations of interference.
- Discover, and locate, rogue access points.
- Reveal coverage voids in existing deployment.
- Identify and classify neighbouring networks and channel usage.
- Predictive and on-site surveys are consolidated into a complete report.

✓ **Analysis of existing system**

The purpose of designing a new system is to replace an existing system in your infrastructure. If so, you can benefit from analyzing your existing system because this analysis will give you a better idea of what problems you are facing. This analysis is also useful if you are trying to upgrade a Sun Fire server. A proper analysis will ensure that you are upgrading the right parts of the system to address the issues

- Current network usage: Network usage takes into account the following:
  - Number of users
  - Types of applications
  - Environment changes as a function of seasons
  - Mobility or roaming needs
  - Devices Supported
  - Site Architecture
  - Range of RF Coverage

Future network usage: Over time, network bandwidth can grow rapidly with new applications. Future network usage predicts the network expansion in respect of meeting user requirement in the near future.

LO 2.2 – Identify components, devices, tools, connectors and media

- **Content/Topic 1 Identification of Hardware components and hardware Devices**

1. Internetworking devices

✓ **Router**

Cisco Integrated Services Router (ISR)

Cisco provides various series and models of routers geared towards different types of customer and requirements. Some of them just do routing whereas others provide some other functions such as Wireless connectivity, Security features and Voice-over-IP services. Cisco's ISR series routers are example of routers that provide various services.

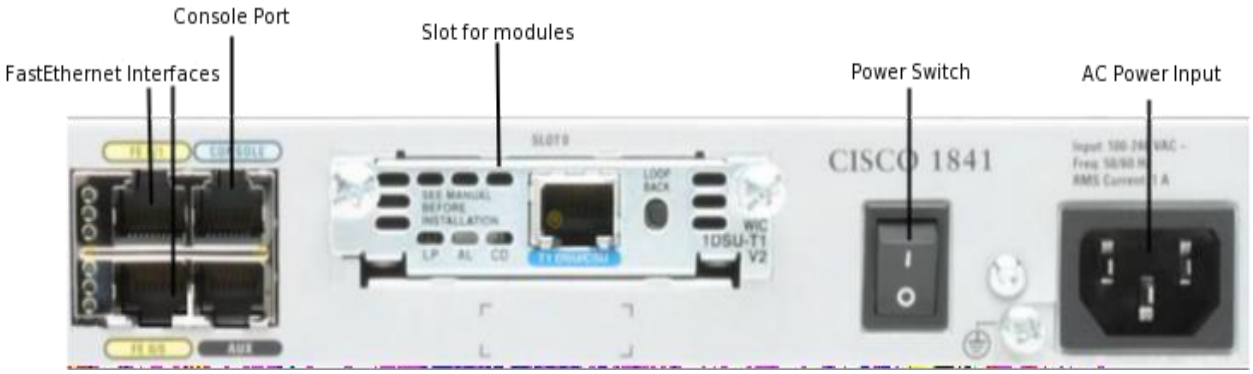


Figure: Rear view of a Cisco1800 Series ISR

- ✓ **Multilayer switch**

A multilayer switch is a network device that has the ability to operate at higher layers of the OSI reference model, unlike the Data Link Layer (DLL) traditionally used by switches. A multilayer switch can perform the functions of a switch as well as that of a router at incredibly fast speeds

What is Layer 3 switching in networking?

Simply put, a layer 3 switch combines the functionality of a switch and a router. It acts as a switch to connect devices that are on the same subnet or virtual LAN at lightning speeds and has IP routing intelligence built into it to double up as a router.

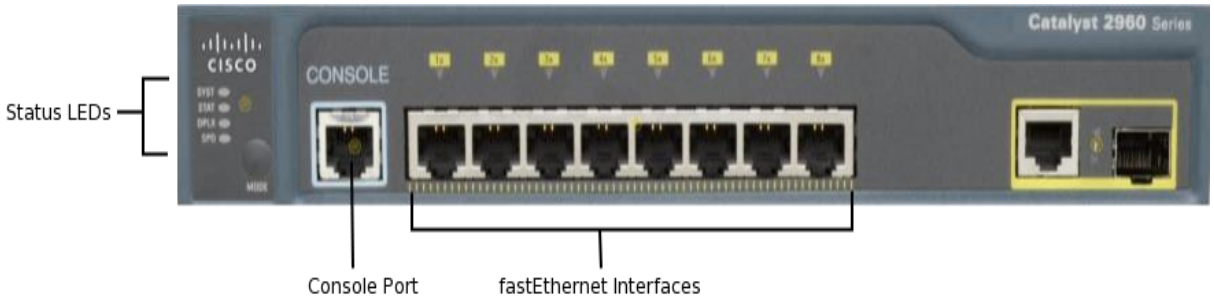


Figure4: Front plane of a Cisco Catalyst 2960 Switch

- ✓ **Wireless router**

A wireless router is a device that performs the functions of a router and also includes the functions of a wireless access point. It is used to provide access to the Internet or a private computer network.

Figure: Wireless Router

2. **Network Access Devices**

- **Switches is** a computer networking device that connects devices on a computer network by using packet **switching** to receive, process, and forward data to the destination device.
- **Wireless router** is a hardware device or configured node on a local area **network** (LAN) that allows **wireless** capable devices and wired **networks** to connect through a **wireless** standard, including Wi-Fi.
- **Access point** in a wireless local area **network** (WLAN), an **access point** is a station that transmits and receives data (sometimes referred to as a transceiver).
- Modem is Short for modulator-demodulator. A **modem** is a device or program that enables a computer to transmit data over, for example, telephone or cable lines.

3. **Security device**

- Firewall is a system designed to prevent unauthorized access to or from a private **network**.

4. **End device**

- **Person computer** include (laptops, desktops, printers, scanners etc…)
- **Security cameras**: is a video camera that records people's activities in order to detect and prevent crime.
- **Network printer** is
- **Mobiles handheld devices** (smart phone, tablets, PDA) **PDA** Short for personal digital assistant, a handheld **device** that combines computing, telephone/fax, Internet and networking features.

- **Smartphone**: A **Smartphone** is a cell phone that allows you to do more than make phone calls and send text messages. Smartphone can browse the Internet and run software programs like a computer. Smartphone use a touch screen to allow users to interact with them.
- **Tablet** is a mobile device, typically with a mobile operating system and touch screen display processing circuitry, and a rechargeable battery in a single thin, flat package. A tablet is a wireless, portable personal computer with a touch screen interface.

✓ **Hardware components**

- NIC: Short for network interface card, the **NIC** is also referred to as an Ethernet card and network adapter. It is an expansion card that enables a computer to connect to a network; such as a home network, or the Internet using an Ethernet cable with an RJ-45 connector.
- Wireless Adapter cards: A wireless adapter is a hardware device that is generally attached to a computer or other workstation device to allow it to connect to a wireless system.

- **Content /Topic 2 Identification of Troubleshooting tools**

- Ipconfig /all
- Ping
- Trace router:
- NSLookup
- Debug
- Netstart
- Putty/ terra term
- Subnet and ip calculation
- Speedtest.net/pingtest.netpat hpin/mtr
- Route

F **1. Ipconfig** displays **all** current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. **Used** without parameters, **ipconfig** displays the IP address, subnet mask, and default gateway for **all** adapters.

```
Syntax

   IPCONFIG /all          Display full configuration information.

   IPCONFIG /release [adapter]
                          Release the IP address for the specified adapter.

   IPCONFIG /renew [adapter]
                          Renew the IP address for the specified adapter.

   IPCONFIG /flushdns     Purge the DNS Resolver cache.

   IPCONFIG /registerdns Refresh all DHCP leases and re-register DNS names.

   IPCONFIG /displaydns   Display the contents of the DNS Resolver Cache.

   IPCONFIG /showclassid adapter
                          Display all the DHCP class IDs allowed for adapter.

   IPCONFIG /setclassid   adapter [classid]
                          Modify the dhcp class id.
```

2. Ping

The most commonly used network tool is the ping utility. This utility is used to provide a basic connectivity test between the requesting host and a destination host. This is done by using the Internet Control Message Protocol (ICMP) which has the ability to send an echo packet to a destination host and a mechanism to listen for a response from this host. Simply stated, if the requesting host receives a response from the destination host, this host is reachable. This utility is commonly used to provide a basic picture of where a specific networking problem may exist. For example, if an Internet connection is down at an office, the ping utility can be used to figure out whether the problem exists within the office or within the network of the Internet provider. Figure 1 below shows an example of the ping utility being used to obtain the reachability status of the locally connected router.

3. Tracert/traceroute

Typically, once the ping utility has been used to determine basic connectivity, the tracert/traceroute utility can used to determine more specific information about the path to the destination host including the route the packet takes and the response time of these intermediate hosts. Figure 2 below shows an example of the tracert utility being used to find the path from a host inside an office to www.google.com. The tracert utility and traceroute utilities perform the same function but operate on different operating systems, Tracert for Windows machines and traceroute for Linux/*nix based machines.

4. Ipconfig/ifconfig

One of the most important things that must be completed when troubleshooting a networking issue is to find out the specific IP configuration of the variously affected hosts. Sometimes this information is already known when addressing is configured statically, but when a dynamic addressing method is used, the IP address of each host can potentially change often. The utilities that can be used to find out this IP configuration information include the ipconfig utility on Windows machines and the ifconfig utility on Linux/*nix based machines. Figure 3 below shows an example of the ifconfig utility showing the IP configuration information of a queries host.

5. Nslookup

Some of the most common networking issues revolve around issues with Dynamic Name System (DNS) address resolution issues. DNS is used by everyone using the Internet to resolve commonly known domain names (i.e. google.com) to commonly unknown IP addresses (i.e. 74.125.115.147). When this system does not work, most of the functionality that people are used to goes away, as there is no way to resolve this information. The nslookup utility can be used to lookup the specific IP address(es) associated with a domain name. If this utility is unable to resolve this information, there is a DNS issue. Along with simple lookup, the nslookup utility is able to query specific DNS servers to determine an issue with the default DNS servers configured on a host. Figure 4 below shows an example of how the nslookup utility can be used to query the associated IP address information.

6. Netstat

Often, one of the things that are required to be figured out is the current state of the active network connections on a host. This is very important information to find for a variety of reasons. For example, when verifying the status of a listening port on a host or to check and see what remote hosts are connected to a local host on a specific port. It is also possible to use the netstat utility to determine which services on a host that is associated with specific active ports. Figure 5 below shows an example of the netstat utility being used to display the currently active ports on a Linux machine.

7. PuTTY/Tera Term

When connecting to a variety of different types of equipment, a telnet, SSH or serial client is required; when this is required both the puTTY and Tera Term programs are able to provide these

functionalities. The selection of one over the other is strictly a personal preference. Figures 6 and 7 below show both puTTY and Tera Term being used to connect to a host via SSH.

8. Subnet and IP Calculator

One of the most important tools in the belt of a junior network engineer is an IP network calculator. These can be used to unsure a correct IP address selection and with this a correct IP address configuration. While this type of tool is used by senior level network engineers, much of the information obtained from the tool becomes simpler to calculate the longer and more experience you have in the field. Two of the more commonly used free IP calculators include Wildpackets (Bitcricket) Network Calculator and Solarwinds Advanced Subnet Calculator which can be found at the links below.

9. Speedtest.net/pingtest.net

A very easy test that can be used to both determine the Internet bandwidth available to a specific host and to determine the quality of an Internet connection is the use of the tools available at the speedtest.net and pingtest.net websites. The speedtest.net site provides the ability to determine the amount of bandwidth that is available to a specific host at a specific point in time; this is often a good tool to use when measuring how long it is going to take to upload or download information from a local to remote host. This measurement can also be used to determine whether the connection is offering the amount of bandwidth that was purchased from the Internet provider; keep in mind however that some amount of bandwidth difference is expected between the quoted bandwidth purchased and the measured bandwidth. The pingtest.net website is used to determine the quality of the connection by measuring the ping response times and jitter amounts over a short period of time. This information can be used to determine a likelihood of how well the measured connection will deal with certain types of high demand traffic like Voice over IP (VoIP) or gaming. Figure 9 and 10 below show example output from both of these sites.

10. Pathping/mtr

In an effort to take advantage of the benefits of both the ping and tracert/traceroute commands, the pathping and mtr utilities were developed. Both of these tools take the functionality and information that can be obtained from these types of tools and provide a more detailed single

picture of the path characteristics from a specific host to a specific destination. Figure 11 and 12 below show examples of these two tools and what information they provide

11. Route

The last of the tools covered in this article is the route utility. This utility is used to display the current status of the routing table on a host. While the use of the route utility is limited in common situations where the host only has a single IP address with a single gateway, it is vital in other situations where multiple IP address and multiple gateways are available. Figure 13 below shows an example of the route utility being used on a Windows machine.

12. **Debug command** display information about the cisco devices operating generated or received traffic, and any error message. The debug operation take a lot of CPU resources and should not be used often in production environment. It meant to be used as a troubleshooting tools for only a short time.

- **Software Tools**

✓ **Packet Tracer:** Packet Tracer is a network simulator software. It simulates networking devices that are used to build CCNA practice labs. An average CCNA lab costs more than $300. A packet tracer cuts this cost by simulating all essential CCNA lab devices. A simulation-based learning environment helps students and instructors.

✓ **Edraw Max :**

Edraw Max is an extremely powerful all-in-one diagramming tool that can serve all of your purposes. Whether you need to draw flowcharts, fishbone diagrams, it is also an all-in-one diagram software for more than 200 diagram types such as business presentations, building plans, mind maps, science illustration, ...

- **Content /Topic 3: Description of Internetwork Operating System(IOS)**

Cisco Internetwork Operating System (IOS) is an operating system used on Cisco devices, such as routers and switches. It is a multitasking operating system that implements and controls logic and functions of a Cisco device. Cisco IOS uses a monolithic architecture, which means that it runs as a single image and all processes share the same memory space.

To configure a Cisco device running IOS, the command-line interface (CLI) is used. The CLI comes with a predefined number of commands and can be used to configure routing, switching,

internetworking, and any other feature supported by a Cisco device that is being configured. The CLI is usually accessed from a remote computer running Telnet or SSH.

IOS has three modes of operation, each with its own set of commands. The modes are:

- **User exec mode –** when you access an IOS device (using Telnet, SSH, or console access method), you are initially placed in this mode. This mode is mostly used to view statistics and run commands like ping or telnet. It is represented with the > character after the hostname (for example Router_HQ>).
- **Privileged exec mode –** this mode is accessed by typing the enable command in the user exec mode. This mode is called privileged because it allows you to execute more powerful commands, such as reload. It is represented with the # character after the hostname (for example Router_HQ#).
- **Global configuration mode –** this mode is accessed by typing the configure terminal command from the privileged exec mode. It is used to make global changes to the device and change its configuration. It is represented with the config keyword after the hostname (for example Router_HQ(config)).
- **IOS versions**

Current iOS versions						
Version	Build	Architecture	Release date	Device end-of-life		
				iPad	iPhone	iPod Touch
3.1.3	7E18	32-bit ARM	February 2, 2010	N/A	1st gen	1
4.2.1	8C148		November 22, 2010		3G	2
5.1.1	9B206		May 7, 2012	1st gen	N/A	3
6.1.6	10B500		February 21, 2014	N/A	3GS	4
7.1.2	11D257	32/64-bit ARM[7][8]	June 30, 2014		4	N/A
9.3.5	13G36		August 25, 2016	2, 3, Mini	N/A	5
9.3.6	13G37		July 22, 2019		4S	N/A
10.3.3	14G60		July 19, 2017	4	5C	
10.3.4	14G61		July 22, 2019		5	
12.4.8	16G201	64-bit ARM[9]	July 15, 2020	Air, Mini 2, Mini 3	5S, 6	6
13.6	17G68			N/A		
14.0 beta 4	18A5342e		August 4, 2020			
Legend: Discontinued Current Beta						

Figure: IOS versions

✓ **Updating and upgrading IOS**

What update means?

Video shows what update means. An advisement providing more up-to-date information than currently known. A change in information, a modification of existing or known data. An additional piece of information. An addition to existing information.

Update your device wirelessly

If a message says that an update is available, tap Install Now. You can also follow these steps:

1. Plug your device into power and connect to the Internet with Wi-Fi.

2. Go to Settings > General, then tap Software Update.

3. Tap Download and Install. If a message asks to temporarily remove apps because the software needs more space for the update, tap Continue or Cancel. Later, iOS or iPadOS will reinstall apps that it removed. If you tap Cancel.
4. To update now, tap Install. Or you can tap Later and choose Install Tonight or Remind Me Later. If you tap Install Tonight, just plug your device into power before you go to sleep. Your device will update automatically overnight.
5. If asked, enter your passcode. If you don't know your passcode,

Customize Automatic Updates

With iOS 12 or later, or iPadOS, you can have your device update automatically overnight while it's charging. To turn on automatic updates, go to Settings > General > Software Update > Customize Automatic Updates, then turn on Install iOS Updates. Your device will automatically update to the latest version of iOS or iPadOS. Some updates might need to be installed manually.

With iOS 13.6, or iPadOS, you can choose not to download software updates automatically. Go to Settings > General > Software Update > Customize Automatic Updates, then turn off Download iOS updates.

What upgrade means?

Upgrading is the process of replacing a product with a newer version of the same product. In computing and consumer electronics an **upgrade** is generally a replacement of hardware, software or firmware with a newer or better version, in order to bring the system up to date or to improve its characteristics.

- ✓ **Types of IOS/NOS**

Types of Network Operating Systems

1. Peer-to-peer network operating systems allow users to share resources and files located on their computers and to access shared resources found on other computers. In a peer-to-peer network, all computers are considered equal; they all have the same privileges to use the resources available on the network. Peer-to-peer networks are designed primarily for small to medium local area networks. Windows for Workgroups is an example of the program that can function as peer-to-peer network operating systems.

2. Client/server network operating systems allow the network to centralise functions and applications in one or more dedicated file servers. The file servers become the heart of the system, providing access to resources and providing security. The workstations (clients) have access to the resources available on the file servers. The network operating system allows multiple users to share

the same resources irrespective of physical location simultaneously. Novell Netware and Windows 2000 Server are examples of client/ server network operating systems.

Each computer in the workgroup run an autonomous operating system; yet cooperate to allow a variety of facilities including sharing of files, sharing of hardware resources and execution of remote machines etc.

- **Content /Topic 4: identification of Connectors**

1. **RJ45, RJ11 (registered jack RJ45, RJ11)**

What is the difference between RJ45 and RJ11?

The main difference between these two is their actual use. RJ11 is the cable connector that using in telephone sets while RJ45 is used in networking, where you connect computers or other network elements to each other.

Aside from the application, there are differences in their appearance. The first of which is in the number of cables that are accommodated in each connector. RJ45 has 8 wires inside whereas Rj11 has 4 wires. As a consequence of having to accommodate more wires, RJ45 connectors are also a little bit bigger than RJ11s.

Figure5: RJ45, RJ11 (registered jack RJ45, RJ11)

BNC

The BNC (Bayonet Neill–Concelman) connector is a miniature quick connect / disconnect radio frequency connector used for coaxial cable. It features two bayonet lugs on the female connector; mating is fully achieved with a quarter turn of the coupling nut. BNC connectors are most commonly made in 50 ohm and 75 ohm versions, matched for use with cables of the same characteristic

impedance. The 75 ohm connector is dimensionally slightly different from the 50 ohm variant, but the two nevertheless can be made to mate.

Figure: Bayonet Neill–Concelman (BNC)

2. **USB**

Universal Serial Bus (USB) is an industry standard that establishes specifications for cables and connectors and protocols for connection, communication and power supply (interfacing) between computers, peripherals and other computers.

Figure: Universal Serial Bus (USB) Connector

3. **Firewire**

FireWire is a method of transferring information between digital devices, especially audio and video equipment. Also known as IEEE 1394, FireWire is fast -- the latest version achieves speeds up to 800 Mbps.

Figure: Firewire connector

4. VGA

A Video Graphics Array (VGA) connector is a three-row 15-pin DE-15 connector. The 15-pin VGA connector was provided on many video cards, computer monitors, laptop computers, projectors, and high definition television sets.

Figure: Video Graphics Array (VGA) connector

5. Serial

In computing, a serial port is a serial communication interface through which information transfers in or out sequentially one bit at a time. This is in contrast to a parallel port, which communicates multiple bits simultaneously in parallel.

Figure: Serial connector

6. BNC-T

A tee connector is an electrical connector that connects three cables together. It is usually in the shape of a capital T. It is usually used for coax cables and the three connector points can be either female or male gender, and could be different or the same standard, such as F type, BNC or N type. Tee connectors can be used to split radio frequency power from a cable into two. They can be used to attach a piece of electronic test equipment. Tee connectors were much used on co-axial 10M Ethernet networks.

Figure: BNC-T connector

7. **F type**

The F connector (also F-type connector) is a coaxial RF connector commonly used for "over the air" terrestrial television, cable television and universally for satellite television and cable modems, usually with RG-6/U cable or, in older installations, with RG-59/U cable.

Figure: F-type connector

8. **MT-RG**

A series of standard types of coaxial cable were specified for military uses, in the form "RG-#" or "RG-#/U". They date from World War II and were listed in MIL-HDBK-216 published in 1962. These designations are now obsolete. The RG designation stands for Radio Guide; the U designation stands for Universal.

Figure: MT-RG connector

9. **RS-232**

RS232 connector is a port used for data exchange between equipments. It was designed for data exchange between DTE (Data Terminal Equipment) or PC and DCE (Data Communication Equipment) or MODEM. ... Although RS232 is later replaced by faster USB (Universal Serial Bus) it is still popular in some areas.

Figure: RS232 connector

- **Content/ Topic 5: Identification of LAN Connection Media**

WAN cables(serial cable)

Which cable is used in WAN network?

However, to connect to and communicate with devices over a WAN you have to use a serial cable rather than a patch cable. Serial cables transmit data differently to LAN cables and other cables like parallel cables. With serial cables, the data is sent along the cable one bit at a time.

WAN Serial Connections

Perhaps you are reading these notes at college, or perhaps at home. Either way, unless you have saved this web page to your hard drive, you will be reading them over an Internet connection. Somehow, the contents of this page traveled from the web server it is stored on across the Internet, to your ISP's server and then onto your PC.

You should be familiar with the patch cables used on local area networks - used to connect devices together so they can communicate. However, to connect to and communicate with devices over a

WAN you have to use a serial cable rather than a patch cable. Serial cables transmit data differently to LAN cables and other cables like parallel cables. With serial cables, the data is sent along the cable one bit at a time.

Now, I don't suppose you ran a serial cable all the way from your computer to your ISP's computer - did you? No, thought not!

If you have a dial-up connection, you will have a serial cable that runs from your pc to your modem. Another cable runs from your modem to your telephone socket that connects over the telephone line to your ISP's network.

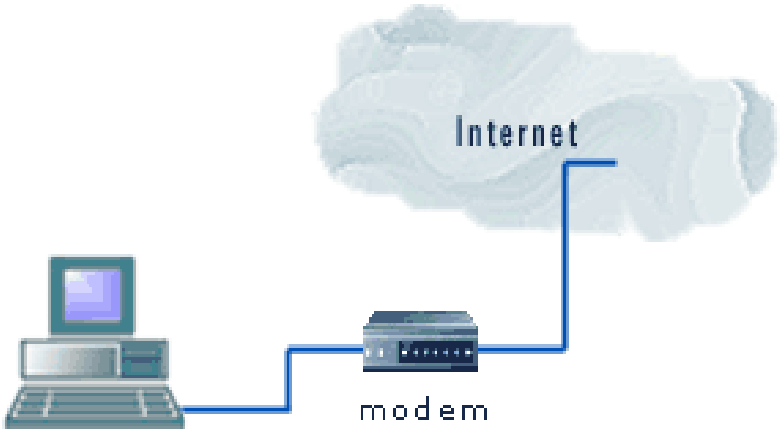


Figure: Serial cable used to connect modem to PC

On a LAN, the principle is the same, but the device used to connect to the ISP's network is likely to be a device with a higher throughput, such as an ISDN or ADSL line or dedicated high bandwidth lines like T1 or E1. Most WAN links are simply methods of serially connecting two routers through the public telephone network. Some links happen to be faster than others.

✓ **LAN cables (Straight and Cross over cable)**

When you connect two devices of different types together, you use a straight through cable. When you connect two devices of the same type together, you use a crossover cable.

All cables are straight through if you insert a network device between two devices of the same kind.

- **straight through cable**

Straight-through cable is used to connect computers and other end-user devices (e.g., printers) to networking devices such as hubs and switches. It can also be used to directly connect like devices (e.g., two hubs or two switches) if the cable is plugged into an uplink port on one (but not both) of the devices.

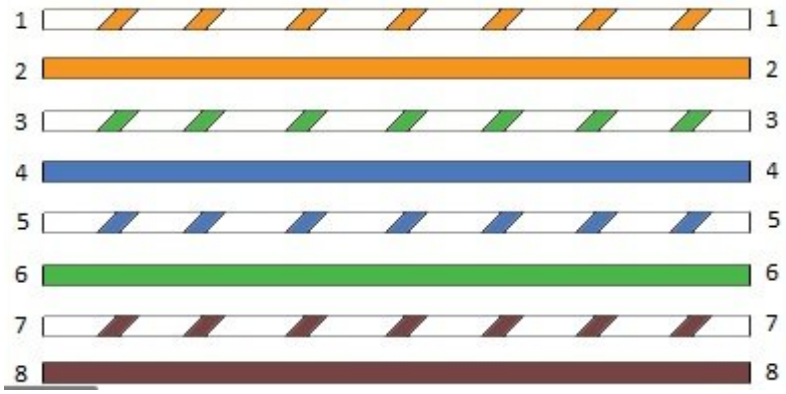


Figure: Straight-through cable

- **crossover cable**

  An Ethernet crossover cable is a crossover cable for Ethernet used to connect computing devices together directly. It is most often used to connect two devices of the same type, e.g. two computers (via their network interface controllers) or two switches to each other.

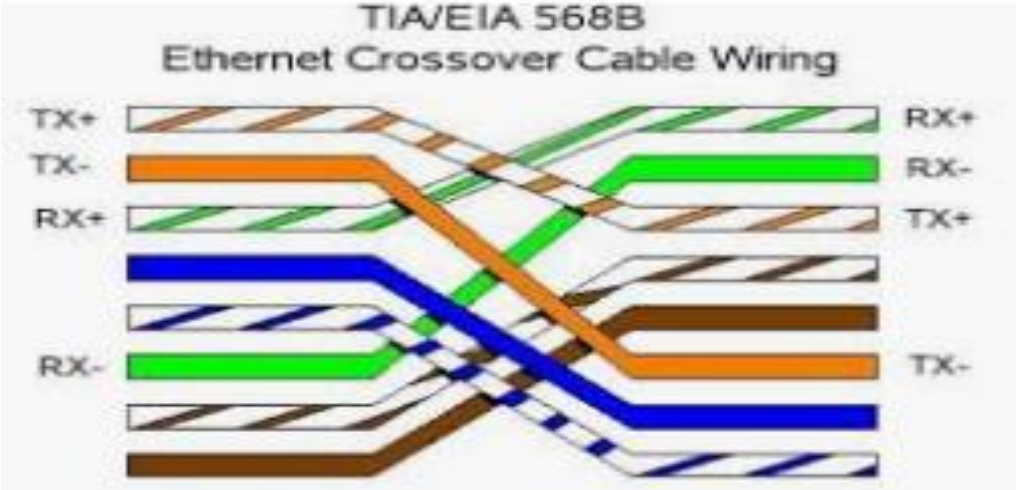


Figure6: crossover cable

- ✓ **Console cable :**

Figure: Console cable

- A rollover cable is a network cable that connects a computer terminal to a network router's console port**. It is also referred to as a Cisco console cable** and is normally flat and light blue so as to distinguish it from other network cable types.
- A serial cable is a cable used to transfer information between two devices using a serial communication protocol. The form of connectors depends on the particular serial port used. A cable wired for connecting two DTEs directly is known as a null modem cable.

✓ **Aux cable:**

What is AUX cable? An aux cable is a portable cable that usually comes with a 3.5 mm jack on both its ends. ... You can use an auxiliary cable to connect your smartphone to an amplifier, like home theatre, car stereo, external Speakers, and more.

Figure: Aux cable

✓ **USB to Serial Converter**

Figure: USB to Serial Converter

This USB to Serial converter allows you to connect an RS-232 serial device such as a modem to a USB port on your desktop or laptop. USB. Supports USB 1.1 and compatible with USB 2.0 and USB 3.0 ports. RS-232 Serial Connector.

LO 2.3 – Identify Security requirements

- Content /Topic 1 Identification of security requirements

- **Authentication:** is a security process required when a computer on a **network** tries to connect to the server in order to use its resources. If the user's identity has been stored by the server, entering a valid username and password completes the connection.
- **Auditing:** -is the process of recording and checking events to detect whether any unexpected activity take place
- **Confidentiality:** refers to protecting information from being accessed by unauthorized parties. In other words, only the people who are authorized to do so can gain access to sensitive data. ... Such a failure of confidentiality, commonly known as a breach, typically cannot be remedied. Prevent the disclosure of sensitive information from unauthorized people, resources, and processes

LO 2.4 – Design and interpret Building blueprint

- **Content/Topic 1 Draw a schematic of the system using Packet tracer**

Definition of packet tracer Packet Tracer is a medium fidelity, network-capable, simulation-based learning environment for networking novices to design, configure, and troubleshoot computer networks at a CCNA-level of complexity. Packet Tracer is an integrated simulation, visualization, collaboration, and assessment environment.

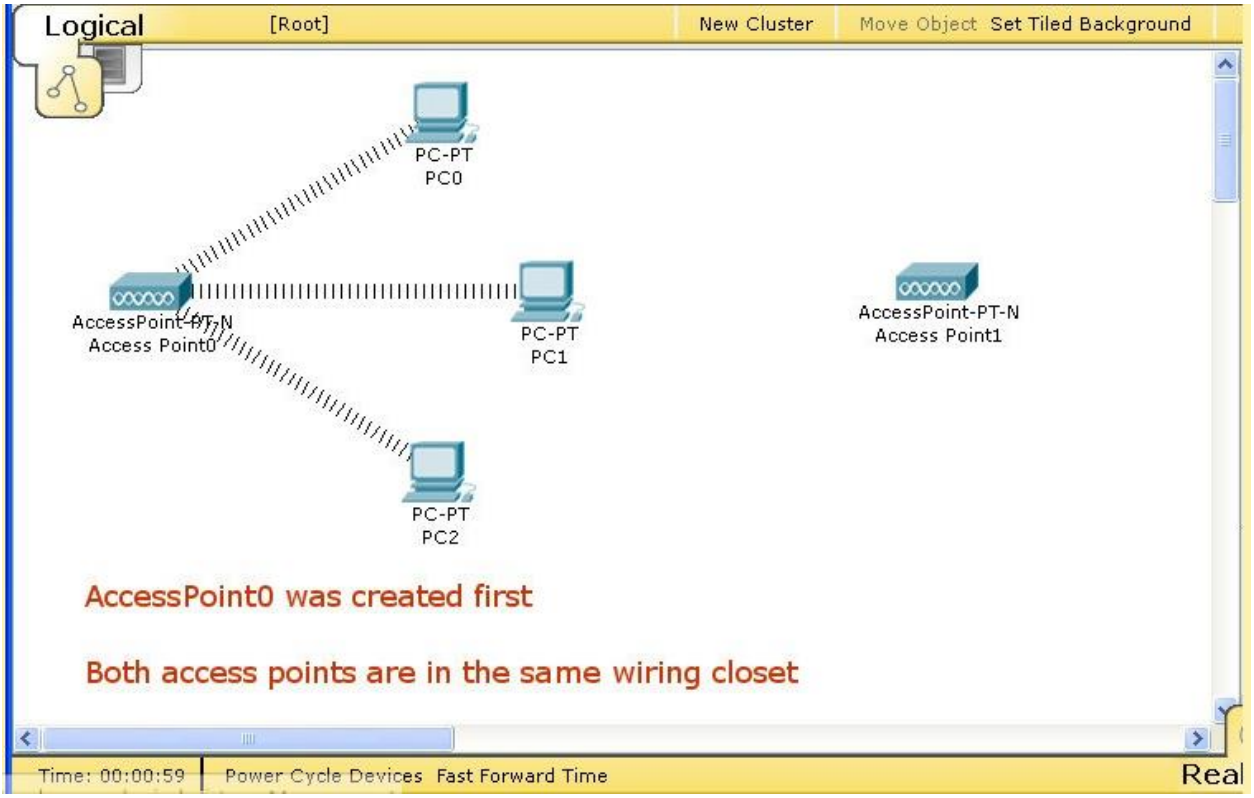
Components of pack tracer

Connections / Links

Cable Type	*Description*
Console	Console connections can be made between PCs and routers or switches. Certain conditions must be met for the console session from the PC to work: the speed on both sides of the connection must be the same, the data bits must be 7 for both or 8 for both, the parity must be the same, the stop bits must be 1 or 2 (but they do not have to be the same), and the flow control can be anything for either side.
Copper Straight-through	This cable type is the standard Ethernet media for connecting between devices that operate at different OSI layers (such as hub to router, switch to PC, and router to hub). It can be connected to the following port types: 10 Mbps Copper (Ethernet), 100 Mbps Copper (Fast Ethernet), and 1000 Mbps Copper (Gigabit Ethernet).
Copper Cross-over	This cable type is the Ethernet media for connecting between devices that operate at the same OSI layer (such as hub to hub, PC to PC, PC to printer). It can be connected to the following port types: 10 Mbps Copper (Ethernet), 100 Mbps Copper (Fast Ethernet), and 1000 Mbps Copper (Gigabit Ethernet).
Fiber	Fiber media is used to make connections between fiber ports (100 Mbps or 1000 Mbps).
Phone	Phone line connections can only be made between devices with modem ports. The standard application for modem connections is an end device (such as a PC) dialing into a network cloud.
Coaxial	Coaxial media is used to make connections between coaxial ports such as a cable modem connected to a Packet Tracer Cloud.
Serial DCE and DTE	Serial connections, often used for WAN links, must be connected between serial ports. Note that you must enable clocking on the DCE side to bring up the line protocol. The DTE clocking is optional. You can tell which end of the connection is the DCE side by the small "clock" icon next to the port. If you choose the **Serial DCE** connection type and then connect two devices, the first device will be the DCE side and the second device will be automatically set to the DTE side. The reverse is true if you choose the **Serial DTE** connection type.
Octal	The 8-port asynchronous cable provides the high-density connector on one end and eight RJ-45 plugs on the other.

Wireless Links

You can establish wireless links between access points and end devices (PCs, servers, and printers). To establish a link, simply remove the existing module on an end device, insert a wireless module, and turn on the device. The device will automatically try to associate itself with an access point. Typically, this means it will associate (physically) with the nearest access point. See the Wireless Devices page under the Physical Workspace section for more information regarding distances. However, if two or more access points are in the same closet, the distance from any access point to any end device is essentially the same. In this case, an end device will associate with the access point that was created first. Recall that the logical topology does not reflect physical distances, and everything that is created in the Logical Workspace is initially placed in the same wiring closet in the Physical Workspace. The process for establishing wireless links between Linksys routers and end devices with Linksys network modules is similar, but described elsewhere

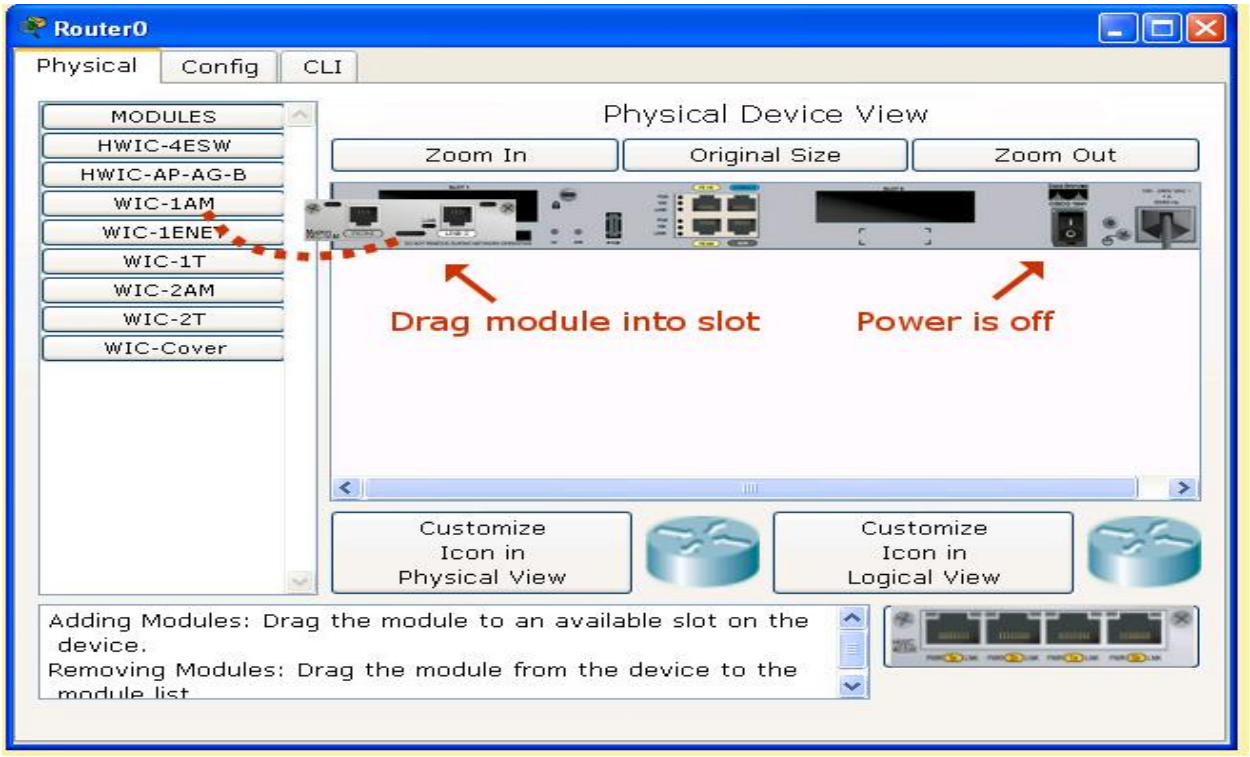


Device and Module

Packet Tracer supports a wide array of modules for networking devices. To change a module in any device, you must first turn off the power for that device.

Physical Configuration and Module List

When you click on a device in the workspace, you are first presented with the Physical Device View of the selected device. You will see an interactive photo on the main panel and a list of compatible modules on the left. You can interact with the device by pressing its power button, adding a module by dragging it from the list into a compatible bay, or removing a module by dragging it from the bay back to the list. You can also zoom in and out of the photo with the zoom controls. The pages in this section show all of the Packet Tracer devices and their supported modules. On these pages, you can click on the thumbnail image of each device or module to view a larger image.



Operating Modes

Packet Tracer operating modes reflect the network time scheme.

In **Realtime Mode**, your network runs in a model of real time, within the limits of the protocol models used. The network responds to your actions immediately as they would in a real device. For example, as soon as you make an Ethernet connection, the link lights for that connection will appear, showing the connection state (see the "Connections/Links" page for details). Whenever you type a command in the CLI (such as **ping** or **show**), the result or response is generated in real time and you see it as such. All network activity, particularly the flow of PDUs across the network, happens in the Packet Tracer model of real time.

In **Simulation Mode**, you can "freeze" time -- you have direct control over time related to the flow of PDUs. You can see the network run step by step, or event by event, however quickly or slowly you like. You can set up scenarios, such as sending a ping packet from one device to another. However, nothing "runs" until you capture it (the first time through, as with a protocol sniffer) or play it (re-playing the captured events as an animation). When you capture or play the simulation, you will see graphical representations of packets traveling from one device to another. You can

pause the simulation, or step forward or backward in time, investigating many types of information on specific PDUs and devices at specific times. However, other aspects of the network will still run in real time. For example, if you turn off a port, its link light will respond immediately by turning red.

The Physical Workspace:

- ✓ **Navigation Panel**

  You can click on the **Navigation** button from the Physical Workspace Bar to bring up the navigation panel of the entire Physical Workspace. The navigation panel contains a physical locations tree that allows you to select a location and then jump to that particular location on the Physical Workspace. The Navigation panel also allows you to move devices from one place to another in physical mode. This is covered in the Moving Devices section.

- ✓ **Applying a Grid**

  You can click on the **Grid** button from the Physical Workspace Bar to apply a customizable grid to the Intercity, City, and Building levels. The Grid tool allows you to set the grid spacing for each level and the ability to choose the color of the grid lines. The grid size is in meters and grid size is affected by the by the Set Background image scaling factor.

- ✓ **Wiring Closet Limit**

  Each wiring closet can house as many as three racks, three tables, two tables and one rack, or two racks and one table. End devices are placed on tables; all other devices are mounted on racks. If the Logical Topology contains more devices than a single wiring closet can house, another wiring closet will automatically be created in the default building. That new wiring closet will become the default wiring closet. You will still be able to access the original wiring closet, although you may need to move wiring closet icons around the building so they do not visually overlap.

- ✓ **Deleting Objects**

  You can use the **Delete** tool from the Common Tools Bar to delete cities, buildings, and wiring closets. Devices, however, cannot be deleted in the Physical Workspace. If you delete a wiring closet from the Building environment, the devices in that closet will be extracted and placed directly onto the building "floor." If you delete that building from the City environment, the devices will be placed onto the city "streets."

- ✓ **Resizing Objects**

Just as in the Logical Workspace, you can use the **Resize Shape** tool from the Common Tools Bar to resize cities, buildings, wiring closets, devices, and shapes created drawn with the Drawing Palette.

- ***Keyboard Shortcuts***

Many actions in Packet Tracer are keyboard-accessible for your convenience. In addition to key combinations, the following keys deserve extra attention:

- **Alt:** Press this key to activate the **Menu Bar** options. Press **Alt** plus the underlined letter in the in the menu bar to open the menu. Then press the underlined letter in the command name that you want. In fact, whenever you see an underlined letter in any option or dialogue, you can press that key to select it.
- **Ctrl:** Use this key to quickly create multiple devices and connections. Press and hold the **Ctrl** key, choose a specific device or a connection type, and then release the key. You can now quickly place multiple instances of that device on the workspace or make multiple connections of that type between devices. Alternatively, you can press and hold the **Ctrl** key and drag a device on the workspace to duplicate the device. The **Ctrl** key can also be used to prevent windows from docking (press and hold the key as you drag a window).
- **Shift:** Use this key with the mouse to select multiple objects. Press and hold the **Shift** key, click and drag the cursor to draw a selection rectangle around the objects you want to select, and then release the key. Alternatively, you can hold **Shift**, click on all the devices you want to select, and then release the key. You can move the selected objects as one unit. You can also delete them with the **Del** key.
- **Esc:** This key is a shortcut to the Select tool in the Common Tools Bar. It also serves as a "cancel" key. It closes certain pop-up windows or cancels/stops the current action (e.g., continuously placing devices or continuously making connections).

- ***Configuring Devices***

- As with real networks, the networks you make in Packet Tracer must be properly configured before they "work." For simple devices, this may just mean entering some fields (such as an IP address and subnet mask) or selecting options in a graphical configuration panel (accessed by the **Config** tab). Routers and switches, on the other hand, are advanced devices that can be configured with much more sophistication. Some of their settings can be configured in the **Config** tab, but most advanced

configurations will need to be done through the Cisco IOS. This section explains the **Config** tab for all devices. You will also find the complete listing of supported IOS commands for routers and switches in this section.

✓ **Booting Sequence and IOS Image Loading in Routers and Switches**

- When a router or switch boots up, the booting sequence is displayed in the **CLI** tab of the Edit device dialog. The startup file is loaded if it is present, and the IOS image stored in **Flash memory** will be loaded into **RAM for execution**. While the model IOS image is loading, you cannot access the **Config** tab or enter any commands in the CLI tab. If there is no valid image stored in Flash memory or the image file instructed to load is not valid, the device will boot into ROM Monitor Mode. ROM Monitor Mode can also be entered using the break sequence (i.e., press **Ctrl + Break** or **Ctrl + C**) for the device in the first 60 seconds when it boots. Packet Tracer uses 10 seconds to give you faster access to the device. ROM Monitor Mode is a minimalist environment where you can manipulate files in the NVRAM and Flash memory, download IOS images via TFTP, and choose how the device is to be booted.
- When the booting sequence and the IOS image loading has been completed, the logout mode is loaded so that you can press ENTER to start.

✓ **Logging IOS Commands**

- If you enabled the IOS logging feature (found in **Options** > **Preferences**), you can keep track of all IOS commands you entered in a work session. Click the **View** button to bring up the **IOS Command Log** window.

Learning Unit 3 – Configure and troubleshoot a SOHO LAN

LO 3.1 – configure IOS

- **Content/Topic 1 Configuration of Internetworking Operating System(IOS)**

Cisco IOS (different from Apple's iOS) is a proprietary kernel which controls all functions of a Cisco router and most switches. Cisco IOS is based on the operating system created by William Yeager at Stanford University between 1980 and 1986. Cisco licensed Yeager's work and created the IOS out of it. The Cisco kernel allocates resources and manages things such as low-level hardware interfaces and security.

✓ **IOS bootcamp**

IOS bootcamps teach students the technologies and languages required to build IOS apps for iPhones which can be launched on the Apple App Store. These technologies include Objective-C, Swift, XCode, and more.

Booting Sequence and IOS Image Loading in Routers and Switches: when a router or switch boots up, the booting sequence is displayed in the **CLI** tab of the Edit device dialog. The start-up file is loaded if it is present, and the IOS image stored in **Flash memory** will be loaded into **RAM for execution**.

The ROM monitor is firmware runs when the router is powered up or reset. The firmware helps to initialize the processor hardware and boot the operating system software. It is a bootstrap program that initializes the hardware and boots the Cisco IOS XE software when you power on or reload a **router**.

Rom monitor use POST power on self Test to check availability of hardware and Bootstrap program to load operating system.

A **bootstrap** is the program that initializes the operating **system** (OS) during start-up.

The bootstrap program responsible for:

Initializing hardware

Finding where IOS program is located and then

Loading IOS image

✓ **IOS access device configuration**

The following are IOS access device configuration:

Consol: a **Console port** is **used to connect** a computer directly to a router or switch and manage the router or switch since there is no display device for a router or switch.

Configuring a Console Port Transport Map

This task describes how to configure a transport map for a console port interface on the Cisco ASR 1000 Series Router.

SUMMARY STEPS

- **enable**
- **configure terminal**
- **transport-map type console** *transport-map-name*
- **connection wait** [**allow interruptible** | **none**]
- exit
- **transport type console** *console-line-number* **input** *transport-map-name*

Examples

In the following example, a transport map to set console port access policies is created and attached to console

port 0:

Router(config)# **transport-map type console consolehandler**

Router(config-tmap)# **connection wait allow interruptible**

Router(config-tmap)# **exit**

Router(config)# **transport type console 0 input consolehandler**

Telnet or SSH: a Telnet is a **network** protocol that allows a user to communicate with a remote device. It is a virtual terminal protocol used mostly by **network** administrators to remotely access and manages devices.

Configuring Persistent Telnet

This task describes how to configure persistent Telnet on the Cisco ASR 1000 Series Routers.

Before you begin

For a persistent Telnet connection to access an IOS vty line on the Cisco ASR 1000 Series Router, local login

authentication must be configured for the vty line (the **login** command in line configuration mode). If local

login authentication is not configured, users will not be able to access IOS using a Telnet connection into the

Management Ethernet interface with an applied transport map.

SUMMARY STEPS

- **enable**
- **configure terminal**
- **transport-map type persistent telnet** *transport-map-name*
- **connection wait** [**allow** {**interruptible**}| **none** {**disconnect**}]
- **transport interface gigabitethernet 0**
- exit
- transport type persistent telnet input *transport-map-name*

Examples

In the following example, a transport map that will make all Telnet connections wait for an IOS vty line to

become available before connecting to the router, while also allowing the user to interrupt the process and

enter diagnostic mode, is configured and applied to the Management Ethernet interface (interface gigabitethernet 0).

The transport map is then applied to the interface when the **transport type persistent telnet input** command

is entered to enable persistent Telnet.

- Router(config)# transport-map type persistent telnet telnethandler
- Router(config-tmap)# connection wait allow interruptible
- Router(config-tmap)# transport interface gigabitethernet 0
- Router(config-tmap)# exit
- Router(config)# transport type persistent telnet input telnethandler

Configuring Persistent SSH

This task describes how to configure persistent SSH on the Cisco ASR 1000 Series Routers.

SUMMARY STEPS

- **enable**
- **configure terminal**
- **transport-map type persistent ssh** *transport-map-name*
- **connection wait** [**allow** {**interruptible**}| **none** {**disconnect**}]
- **rsa keypair-name** *rsa-keypair-name*
- authentication-retries number-of-retries
- time-out timeout-interval
- **transport interface gigabitethernet 0**
- exit
- transport type persistent ssh input *transport-map-name*

Examples

In the following example, a transport map that will make all SSH connections wait for the vty line to become

active before connecting to the router is configured and applied to the Management Ethernet interface (interface gigabitethernet 0). The RSA keypair is named sshkeys.

This example only uses the commands required to configure persistent SSH.

Router(config)# transport-map type persistent ssh sshhandler

Router(config-tmap)# connection wait allow

Router(config-tmap)# rsa keypair-name sshkeys

Router(config-tmap)# transport interface gigabitethernet 0

In the following example, a transport map is configured that will apply the following settings to any users attempting to access the Management Ethernet port via SSH:

- Users using SSH will wait for the vty line to become active, but will enter diagnostic mode if the attempt to access IOS through the vty line is interrupted.
- The RSA keypair name is sshkeys
- The connection allows one authentication retry.

- The banner " --Waiting for vty line-- " will appear if the connection is waiting for the vty line to become active.
- The transport map is then applied to the interface when the **transport type persistent ssh input** command is entered to enable persistent SSH:
- Router(config)# transport-map type persistent ssh sshhandler
- Router(config-tmap)# connection wait allow interruptible
- Router(config-tmap)# rsa keypair-name sshkeys
- Router(config-tmap)# authentication-retries 1

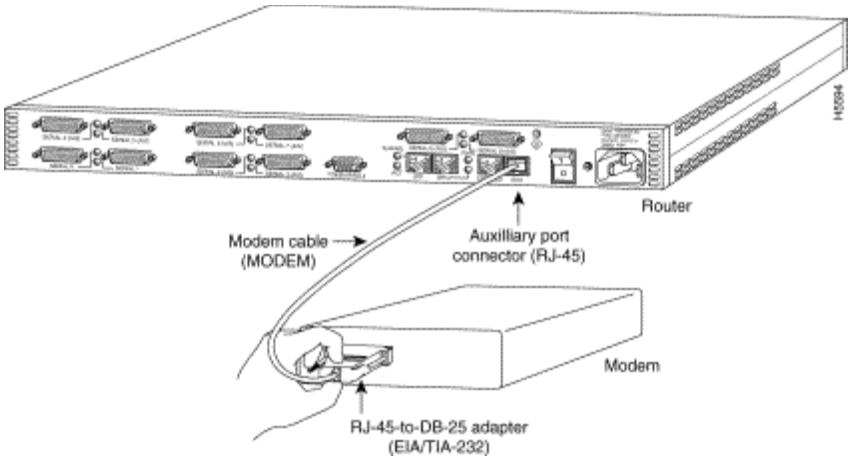
Aux port: an **Auxiliary Port** (**AUX Port**) allows a direct, non-**network** connection to the router, from a remote location. The **Auxiliary Port** (**AUX Port**) uses a connector type to which modems can plug into, which allows an administrator from a remote location to access the router like a console **port**.

Configure a Modem on the AUX Port

To configure a modem on the AUX Port for EXEC dialin connectivity, complete these steps:
Connect the cable from the AUX port of the router to the modem, as shown in figure 2.
Remember these points:
The AUX port on Cisco routers is either RJ-45 or DB-25. If the AUX port is RJ-45, use a flat-satin rolled RJ-45--RJ-45 cable (part number CAB-500RJ=), which is usually provided with every Cisco router for console connections. You also need an RJ-45 to DB-25 adapter marked "MODEM" (part number CAB-25AS-MMOD) to connect the rolled cable to the DB-25 port on the modem.

♦If your router has a DB-25 AUX port, use a straight-through DB-25Female - DB25Male RS-232 cable to connect the modem to the router.

♦For more information on cabling, see Modem-Router Connection Guide and Cabling Guide for RJ-45 Console and AUX Ports.



✓ **Explanation of IOS Configuration modes** and sub modes

There are three basic IOS configuration mode

1. User EXEC mode
2. Privileged EXEC mode
3. Global configuration mode

1. User executive mode

This is the main or the first mode that one can access on a router. It is limited to few verification and troubleshooting commands. By default, authentication is not required but as best practice we will configure security so as to ensure protection of our routers.

On accessing the router, you will notice the prompt that ends with this symbol “>” after the router’s name. By default the name of the router is usually “Router“. This prompt is shown below.

Router>

In this mode, we can view basic information using the “show” command.

2. Privileged executive mode

This is the second mode in the IOS CLI. In this mode, we can view various troubleshooting and verification commands such as “show and debug“. By default, this mode is also not secured, as best practice we will also secure this mode using a password.

This mode is denoted by the HASH (#) symbol proceeded by the name of the router. To enter this mode, we issue the command “enable” from the user exec mode.

Router#

NOTE: To move from the user exec mode to the privileged mode the command – “enable” should be entered from the user exec mode.

The “disable” command is used to exit the privileged exec mode and return to the user exec mode.

3. **Global configuration mode**

   The main configuration on a router is executed in this mode. Parameters such as the router’s name, ip domain lookup, banners among others can be configured. In this mode, we can also gain access to other specific configuration parameters such as interface configuration.

   The global configuration mode is shown by the prompt: (config)# as shown below:

   Router (config)#

   NOTE: To enter this mode from the privileged exec mode we enter the command: *“Configure terminal”*

   To exit we to the privileged mode we enter the command: *“exit”*

4. **Other Specific configuration mode.**

   There are other specific configuration modes on the router. These are entered in the global configuration mode and are used to configure various functions and options on the router such as the interfaces and sub interface, routing options, console lines among others.

✓ **IOS command structure**:

- **Prompt** a symbol on a display screen indicating that the computer is waiting for input. Once the computer has displayed a **prompt**, it waits for you to enter some information.
- **Command** is a Console Command which can be issued to the Command Line Interpreter (or command prompt) to display the network settings currently assigned to any or all network adapters in the machine.
- **Spaces** allow you to **configure** the model's **network** topology to restrict applications to posse only the **network** connectivity they need.
- **Keyword or arguments** Lists the available syntax options (**arguments** and **keywords**) for the command.
- **Hot key and shortcuts** you can **use shortcut keys** at any position where a command can be entered. After you **use** a **shortcut key**, the system displays the corresponding command on the screen.

✓ **IOS "Examination" Commands**

In order to verify and troubleshoot network operation, we must examine the operation of the devices. The basic examination command is the show command.

There are many different variations of this command. As you develop more skill with the IOS, you will learn to use and interpret the output of the show commands. Use the show? command to get a list of available commands in a given context, or mode.

The figure indicates how the typical show command can provide information about the configuration, operation, and status of parts of a Cisco router.

In this course, we use some of the more basic show commands.

Some of the most commonly used commands are:

Show interfaces Displays statistics for all interfaces on the device. To view the statistics for a specific interface, enter the show interfaces command followed by the specific interface slot/port number. For example:

Router#show interfaces serial 0/1

Show version Displays information about the currently loaded software version, along with hardware and device information. Some of the information shown from this command are:

Software Version - IOS software version (stored in flash)

Bootstrap Version - Bootstrap version (stored in Boot ROM)

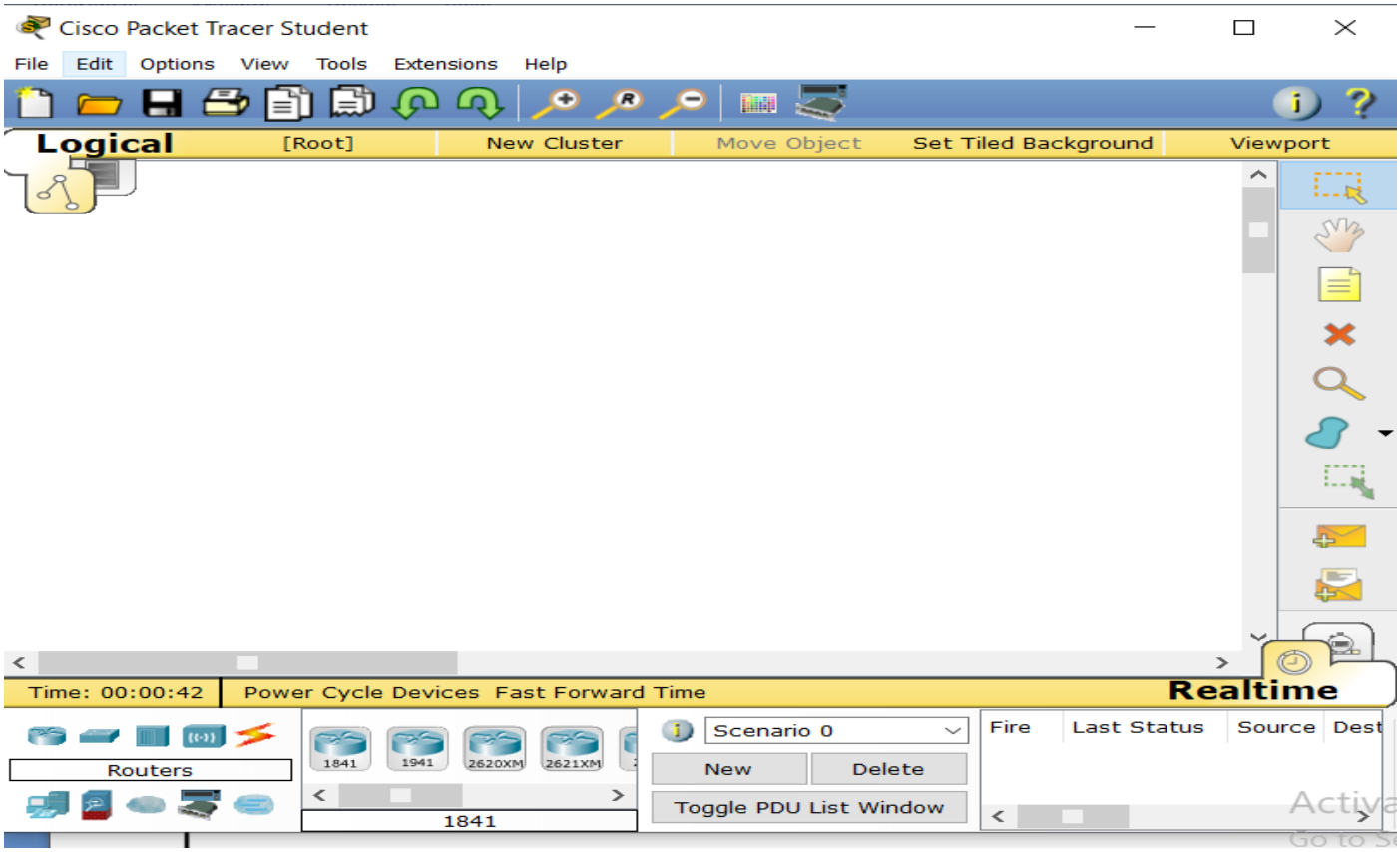
- **System up-time** - Time since last reboot
- **System restart info** - Method of restart (e.g., power cycle, crash)
- **Software image name** - IOS filename stored in flash
- **Router Type and Processor type** - Model number and processor type
- **Memory type and allocation (Shared/Main)** - Main Processor RAM and Shared Packet I/O buffering
- **Software Features** - Supported protocols / feature sets
- **Hardware Interfaces** - Interfaces available on router
- **Configuration Register** - Sets bootup specifications, console speed setting, and related parameters.

The IOS commands and their description

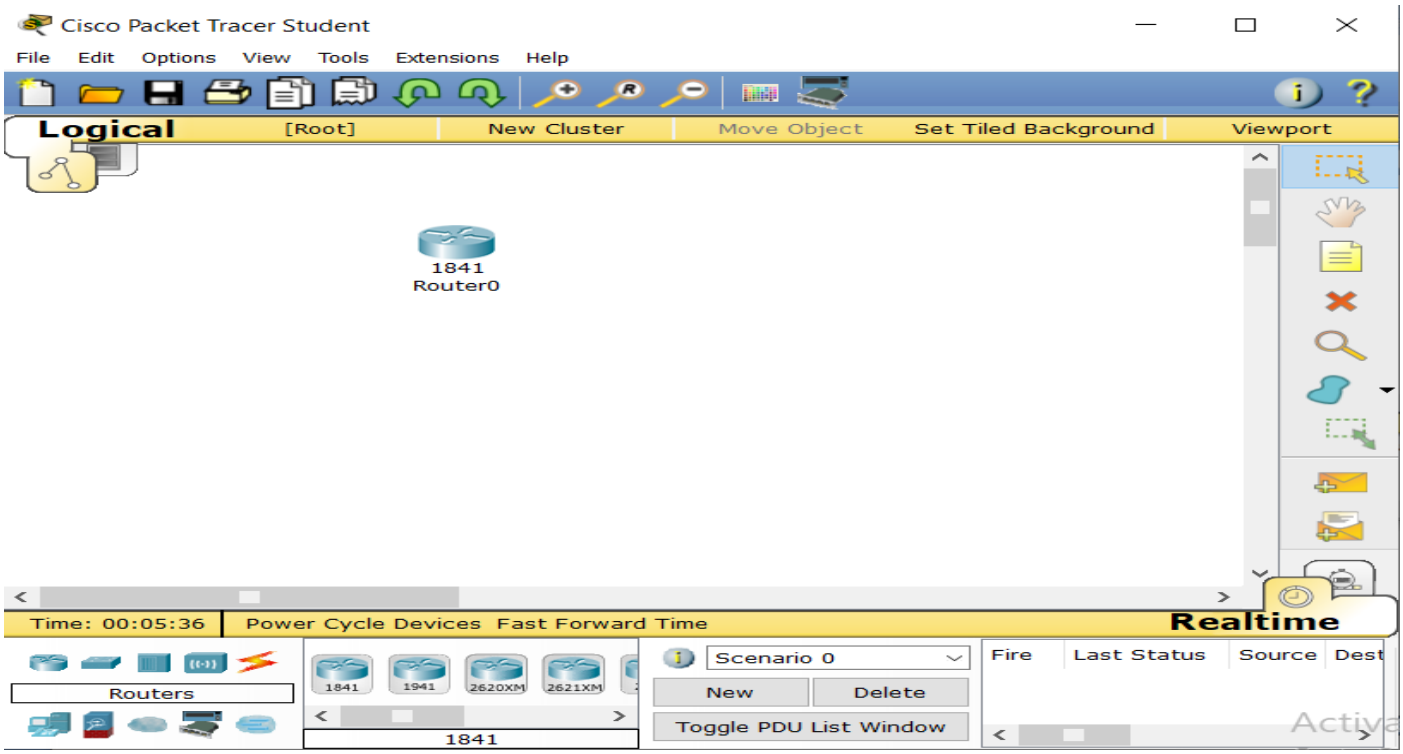
- **show arp** - Displays the ARP table of the device.
- **show mac-address-table** - (switch only) Displays the MAC table of a switch.
- **show startup-config** - Displays the saved configuration located in NVRAM.

- **show running-config** - Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.
- **show ip interfaces** - Displays IPv4 statistics for all interfaces on a router. To view the statistics for a specific interface, enter the **show ip interfaces** command followed by the specific interface slot/port number. Another important format of this command is **show ip interface brief**. This is useful to get a quick summary of the interfaces and their operational state.
- **Content/Topic 2 Practice of IOS configuration**

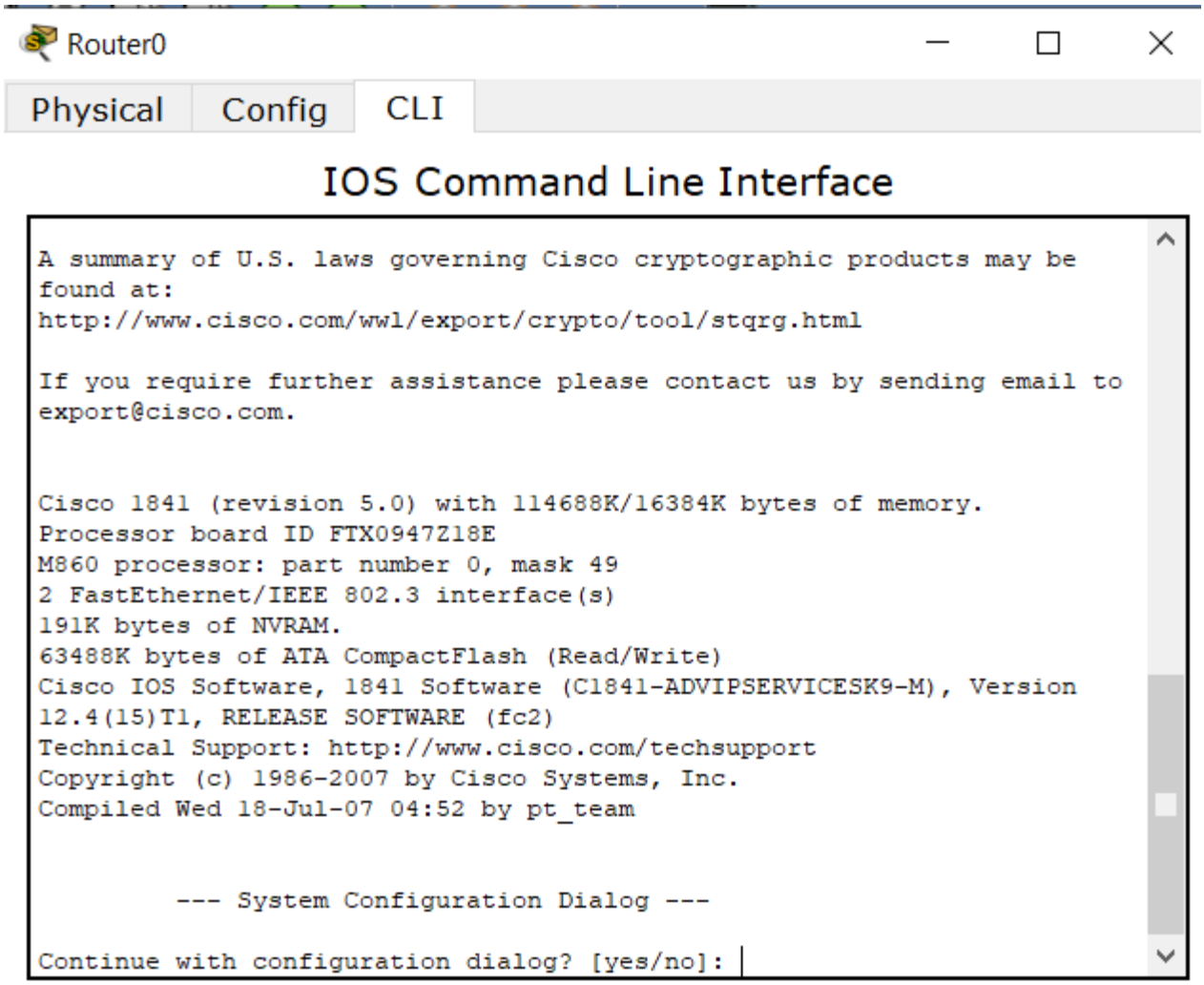
✓ Open cisco packet tracer application software on your computer



✓ **Drag router to work book**



✓ **Double click on router to boot IOS**



- ✓ **Type no then press enter key to enter IOS configuration mode**

  Continue with configuration dialog? [yes/no]: n

  Router>

- ✓ Type enable or en command to enter privilege Executive mode

  Router>en

  Router#

- ✓ Type show interfaces command to display interfaces information

```
Router#show interfaces
FastEthernet0/0 is administratively down, line protocol is down
(disabled)
  Hardware is Lance, address is 0001.c954.7201 (bia 0001.c954.7201)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

✓ Type configuration terminal or conf t command to enter in global configuration mode

Router#configure terminal

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

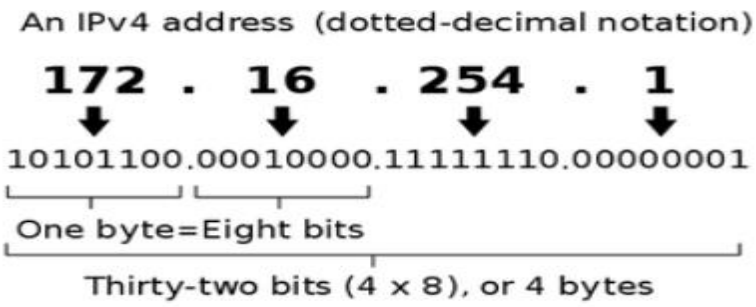
LO 3.2 – Configure SOHO LAN IP settings

- **Content/Topic 1: Application of IP addressing scheme**

✓ **IP address structure**

IPv4, also known as the fourth version of Internet Protocol, is the core protocol that routes most of the internet traffic. This is a connectionless protocol, which means that the state of the connection is not preserved and the data is transmitted to the receiver without ensuring that the recipient is available or not.

IPv4 uses 32-bit addressing which allows a total of 4,294,967,296 (2^{32}) addresses. Some addresses are reserved for public and private networks. An IP address consists of four octets which are separated by a period, which is also known as dotted-decimal notation. For example, the IP address 172.16.254.1 represents four octets, like you can see in the image below:



IPv4 Address Structure

A subnet mask is a number that defines a range of IP addresses available within a network. A single subnet mask limits the number of valid IPs for a specific network. Multiple subnet masks can organize a single network into smaller networks (called subnetworks or subnets). Systems within the same subnet can communicate directly with each other, while systems on different subnets must communicate through a router.

A subnet mask hides (or masks) the network part of a system's IP address and leaves only the host part as the machine identifier. It uses the same format as an IPv4 address — four sections of one to three numbers, separated by dots. Each section of the subnet mask can contain a number from 0 to 255, just like an IP address. For example, a typical subnet mask for a Class C IP address is:

255.255.255.0

In the example above, the first three sections are full (255 out of 255), meaning the IP addresses of devices within the subnet mask must be identical in the first three sections. The last section of each computer's IP address can be anything from 0 to 255. If the subnet mask is defined as 255.255.255.0, the IP addresses 10.0.1.99 and 10.0.1.100 are in the same subnet, but 10.0.2.100 is not.

A subnet mask of 255.255.255.0 allows for close to 256 unique hosts within the network (since not all 256 IP addresses can be used).

If your computer is connected to a network, you can view the network's subnet mask number in the Network control panel (Windows) or System Preference (macOS). Most home networks use the default subnet mask of 255.255.255.0. However, an office network may be configured with a different subnet mask such as 255.255.255.192, which limits the number of IP addresses to 64.

Large networks with several thousand machines may use a subnet mask of 255.255.0.0. This is the default subnet mask used by Class B networks and provides up to 65,536 IP addresses (256 x 256). The largest Class A networks use a subnet mask of 255.0.0.0, allowing for up to 16,777,216 IP addresses (256 x 256 x 256).

- ✓ **Configuring DNS**

  The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources. Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

- ➢ Dynamic use Dynamic Host Configuration protocol(DHCP) method which assign IP address dynamically to the hosts
- ➢ Static method where user assign IP address manually to the host

  The difference between Static and Dynamic IP address lies within the duration of assigned IP address. The static IP address is fixed IP address which is manually assigned to a device for a long period of time. On the other hand, the Dynamic IP address frequently changes whenever user boots his/her machine and it is automatically assigned.

BASIS FOR COMPARISON	STATIC IP ADDRESS	DYNAMIC IP ADDRESS
Provided by	ISP (For external IP address)	DHCP
Change acquirement	Once static IP is assigned, it doesn't change.	Dynamic IP changes each time when a user connects to a network.
Security	Risk is high.	More secure than static IP address.

How does DHCP work with the Wireless? The wireless is designed to act as a DHCP relay agent to the external DHCP server and acts like a DHCP server to the client. This is the sequence of events that occurs: Generally, WLAN is tied to an interface which is configured with a DHCP server.

When the wireless receives a DHCP request from the client on a WLAN, it relays the Request to the DHCP server with its management IP address.

The wireless shows its virtual IP address, which must be a non−routable address, usually configured as 192.168.0.1, as the DHCP server to the client.

- ✓ **How to configure LAN settings (DHCP and DNS) on D-Link gaming router (DGL-4100)?**

  This article teaches you how to set the D-Link gaming router to configure WAN settings, Include PPPOE and DHCP .D-Link gaming router such as DGL-4100,DGL-4300 and DGL-4500.

A. <u>DHCP</u> Case (Dynamic Host Control Protocol)

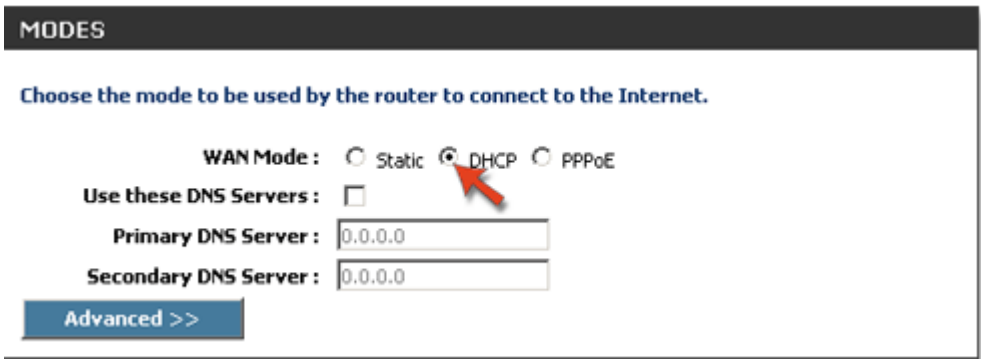
Step 1 Open a web browser and type the IP address of the gaming router in the address bar (default is 192.168.0.1). Press **Enter**.

Step 2 The default password is blank (nothing). Click **Log In**.

Step 3 Click **WAN** on the left side.

Step 4: In the *Modes* section configure the following:

- **WAN Mode** – Select **DHCP**
- **Use these DNS Servers** – Select this option to manually enter DNS servers. DNS servers translate domain names (i.e. dlink.com) to IP addresses (i.e. 64.7.210.130).
- **Primary DNS Server** – If you selected *Use these DNS Servers* enter the domain name or IP address of your primary DNS server.
- **Secondary DNS Server** – If you selected the *Use these DNS Server* enter the domain name or IP address of your secondary DNS server (optional).



Step 5: Click save settings at the top to save the new settings.

✓ **Assigning IP to the interface**

A Local Area Network (LAN) might be as big as several buildings or as small as a home. Everyone connected to the LAN is in the same physical location.

In a LAN, the router assigns each device its own unique internal IP address. They follow a pattern as follows:

10.0.0.0 /8 (10.x.x.x)

172.16.0.0 /12 (172.16.x.x - 172.31.x.x)

192.168.0.0 /16 (192.168.x.x)

How to Assign Static IP Addresses

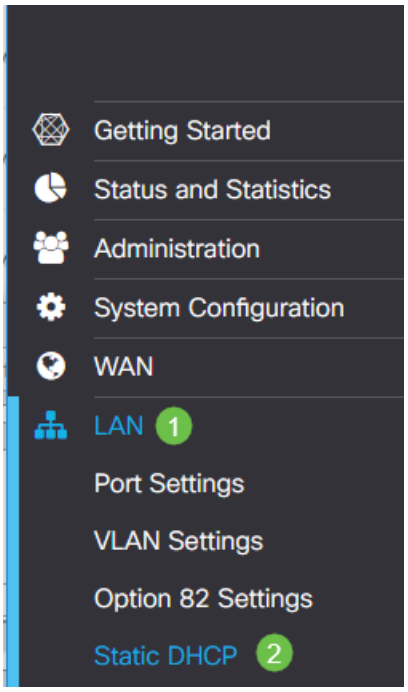
There are a few options for assigning a static IP address to a device. The first option is to configure all static IP addresses on the main router. This is an easy way to have all of the static IP addresses in one location. However, if you reset the router to factory settings, all IP addresses will be deleted.

The second option is to configure it directly on each device. If a static IP address is configured directly on a device, and it gets reset, it will likely revert to DHCP and pick up a different IP address.

Configuring Static DHCP on a Router

To configure static DHCP on the router, you will need to know the MAC address for each device. This is the unique identifier for each device that consists of letters and numbers. The MAC address does not change. It can be found on the body of the Cisco device. It is labeled *MAC* and is typically shown with a white background.

Step 1. Log into the router. Navigate to **LAN > Static DHCP**.



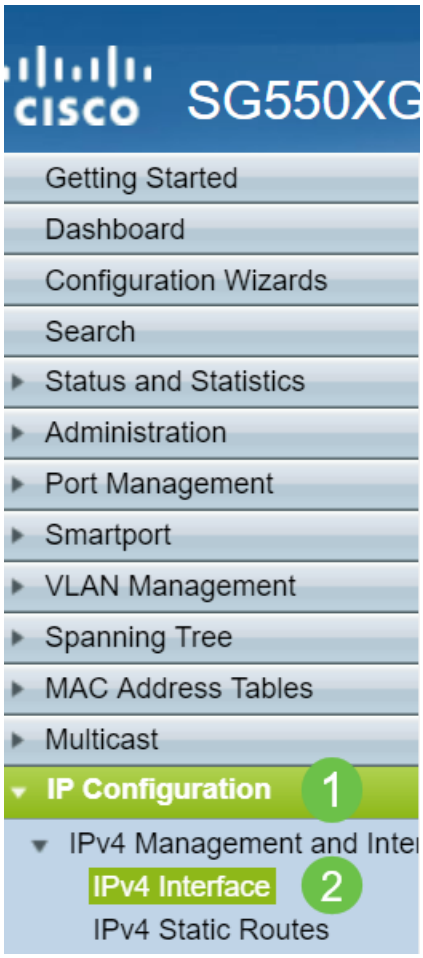
Step 2. Complete the following steps to assign a static IP.

- Click the **plus icon**.
- Create a **Name** that will help you associate the device that is listed, such as **SG550 Switch**.
- Enter the **MAC address** of the device.
- Enter the **Static IPv4 Address**. Make sure you use an address that is not in the DHCP pool.
- Make sure the **Enabled** box is checked.
- Click **Apply**.

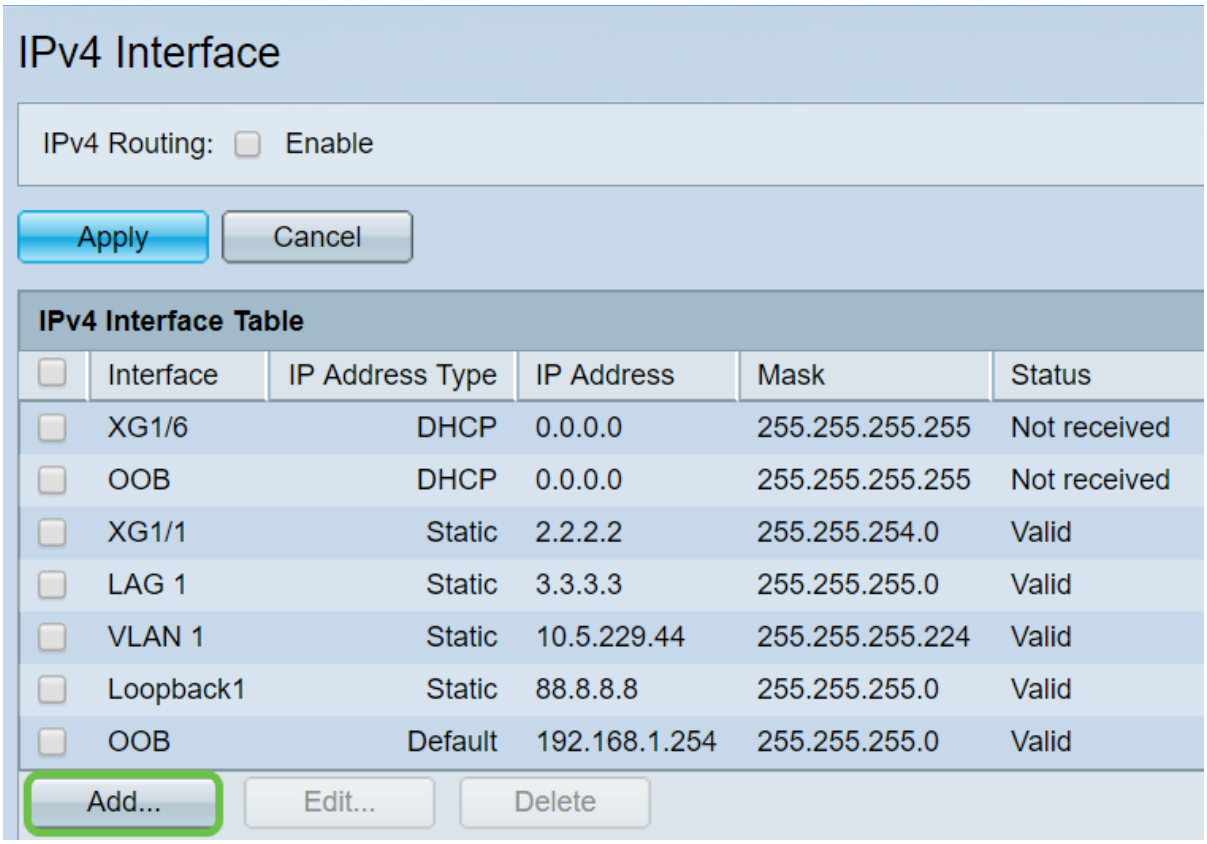
You will need to repeat this process for each device you would like to assign a static IP address.

Configuring Static IP Address on a Switch

Step 1. Log in to the switch. Navigate to **IP Configuration > IPv4 Interface**.

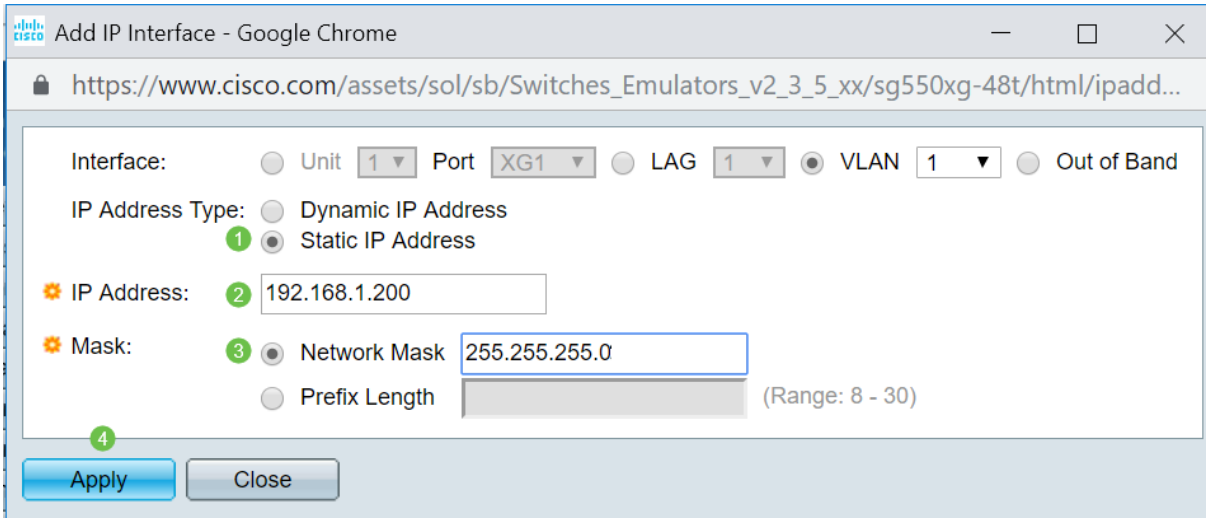


Step 2. Click **Add**.



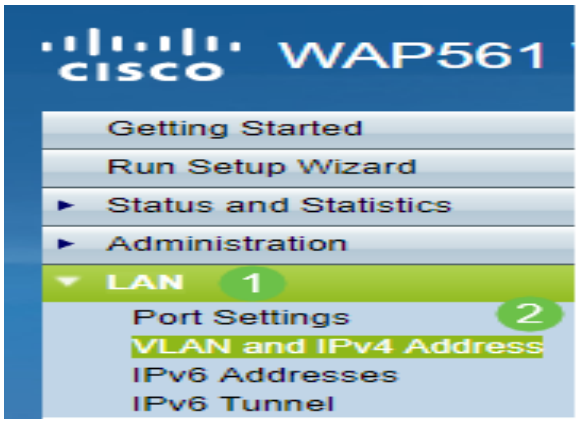
Step 3. Select the *Static IP Address* radio button. Enter the desired *Static IP address* and *Subnet Mask*.

Click **Apply**.



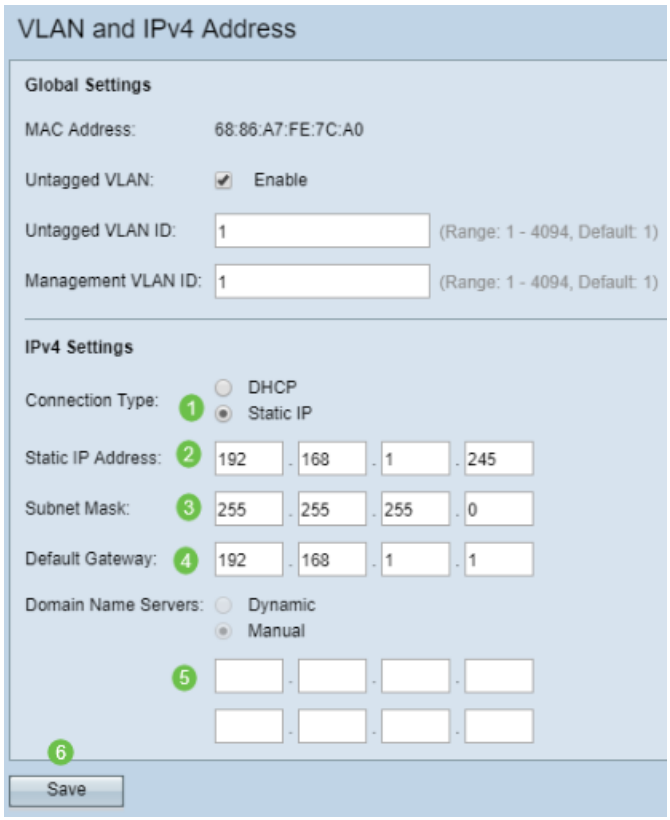
Configuring Static IP Address on a Wireless Access Point (WAP)

Step 1. Log into the WAP. Navigate to **LAN > VLAN and IPv4 Address**.



Step 2. Select the *Static IP* radio button. Enter the desired *Static IP address* and *Subnet Mask*. You also need to specify *Default Gateway* and *Domain Name Servers* (DNS) server address. Click **Save**.

Note: Usually both the default gateway and the DNS server are the LAN IP address of the router; however the DNS server for Google, 8.8.8.8, is sometimes utilized here.



✓ **Configuring switch virtual interface**

WHAT IS SVI?

A switch Virtual Interface (SVI) is a logical interface configured on layer 3 Switch where SVI has no physical interface and provides layer 3 processing of packets from all switch ports associated with the VLAN.

By default a switch virtual interface is created for default VLAN (VLAN1) to permit remote switch administration. A switch virtual interface cannot be activated unless associated with a physical port.

Multilayer switches support configuring a VLAN as logical routed interface (SVI). The switch virtual interface CISCO is referenced by the VLAN number as per below configuration

Sw(config)#vlan database

Sw(config)#vlan 2

Configure vlan interfaces with IP address

Sw(config)#interface vlan 2

Sw(config-if)#ip address 192.168.2.1 255.255.255.0

Sw(config-if)#no shutdown

So a switch virtual interface is routed interface in IOS representing the IP addressing space for particular VLAN connected to this interface.

✓ **Assigning IP to the end devices**

- Static Assignment

Procedure: On the host computer

On the host computer, follow these steps to share the Internet connection:

1. Log on to the host computer as Administrator or as Owner.
2. Click **Start**, and then click **Control Panel**.
3. Click **Network and Internet Connections**.
4. Click **Network Connections**.
5. Right-click the connection that you use to connect to the Internet. For example, if you connect to the Internet by using a modem, right-click the connection that you want under Dial-up / other network available.
6. Click **Properties**.
7. Click the **Advanced** tab.
8. Under **Internet Connection Sharing**, select the **Allow other network users to connect through this computer's Internet connection** check box.

9. If you are sharing a dial-up Internet connection, select the **Establish a dial-up connection whenever a computer on my network attempts to access the Internet** check box if you want to permit your computer to automatically connect to the Internet.

10. Click **OK**. You receive the following message:

When Internet Connection Sharing is enabled, your LAN adapter will be set to use IP address 192.168.0. 1. Your computer may lose connectivity with other computers on your network. If these other computers have static IP addresses, it is a good idea to set them to obtain their IP addresses automatically. Are you sure you want to enable Internet Connection Sharing?

11. Click **Yes**.

The connection to the Internet is shared to other computers on the local area network (LAN).

- Content/Topic 2 configuration of loopback address

✓ **Understanding the loopback interface**

The internet protocol (IP) specifies a loopback network with the IPV4 address 127.0.0.0/8. Most IP implementations support a loopback interface to represent the loopback facility. Any traffic that a computer program sends on the loopback network is addressed to the same computer. The most commonly used IP address on the loopback network 127.0.0.1 for IPV4 and :: 1for IPV6. The standard domain name for the address is local host.

A network device also includes an internal loopback address with address (100.16384). the internal loopback address is particular instance of the loopback address with the logical unit number 16384. The loopback interface is used to identify the device .while any interface address can be used to determine if the device is online; the loopback address is the preferred method. Whereas interface might be removed or addresses changed based on network topology changes the loopback address never changes.

When you ping an individual interface address, the result do not always indicate the health of the device.

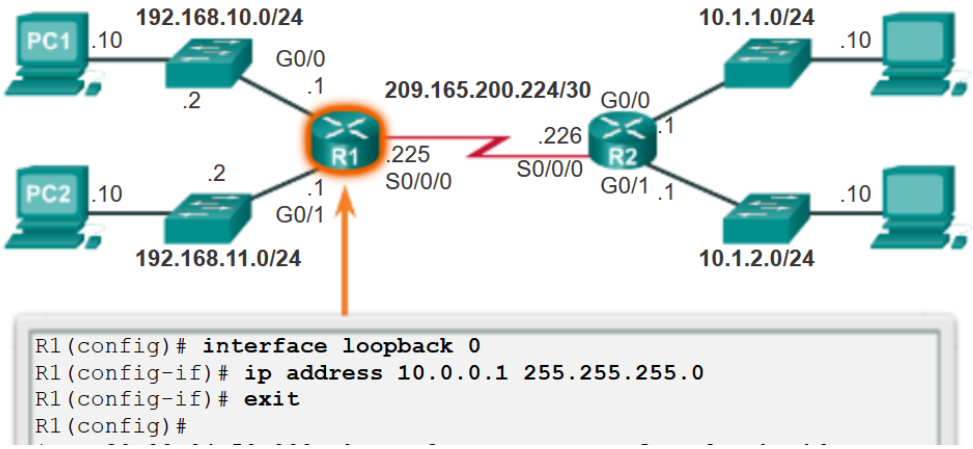
✓ **Configuring loopback address**

Enabling and assigning a loopback address is simple:

Router(config)# **interface loopback** *number*

Router(config-if)# **ip address** *ip-address subnet-mask*

Router(config-if)# **exit**



✓ **Testing interface assignment using show command**

Verify Connectivity of Directly Connected Networks

The first task to undertake once the basic settings and interfaces are configured is to verify and validate the configured settings. This is an important step and should be done before any other configurations are added to the router.

Verify Interface Settings (1.1.4.1)

There are several **show** commands that can be used to verify the operation and configuration of an interface. The following three commands are especially useful to quickly identify an interface status:

- **Show ip interface brief**: Displays a summary for all interfaces, including the IPv4 address of the interface and current operational status.
- **Show ip route**: Displays the contents of the IPv4 routing table stored in RAM. In Cisco IOS 15, active interfaces should appear in the routing table with two related entries identified by the code 'C' (Connected) or 'L' (Local). In previous IOS versions, only a single entry with the code 'C' will appear.
- **Show running-config interface** *interface-id*: Displays the commands configured on the specified interface.

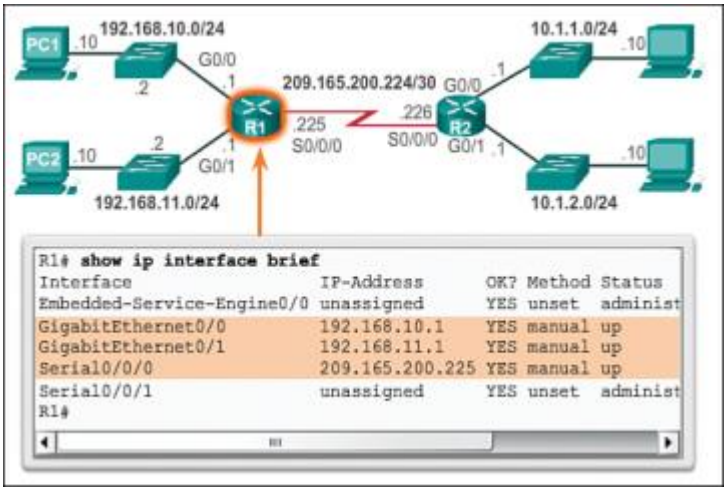


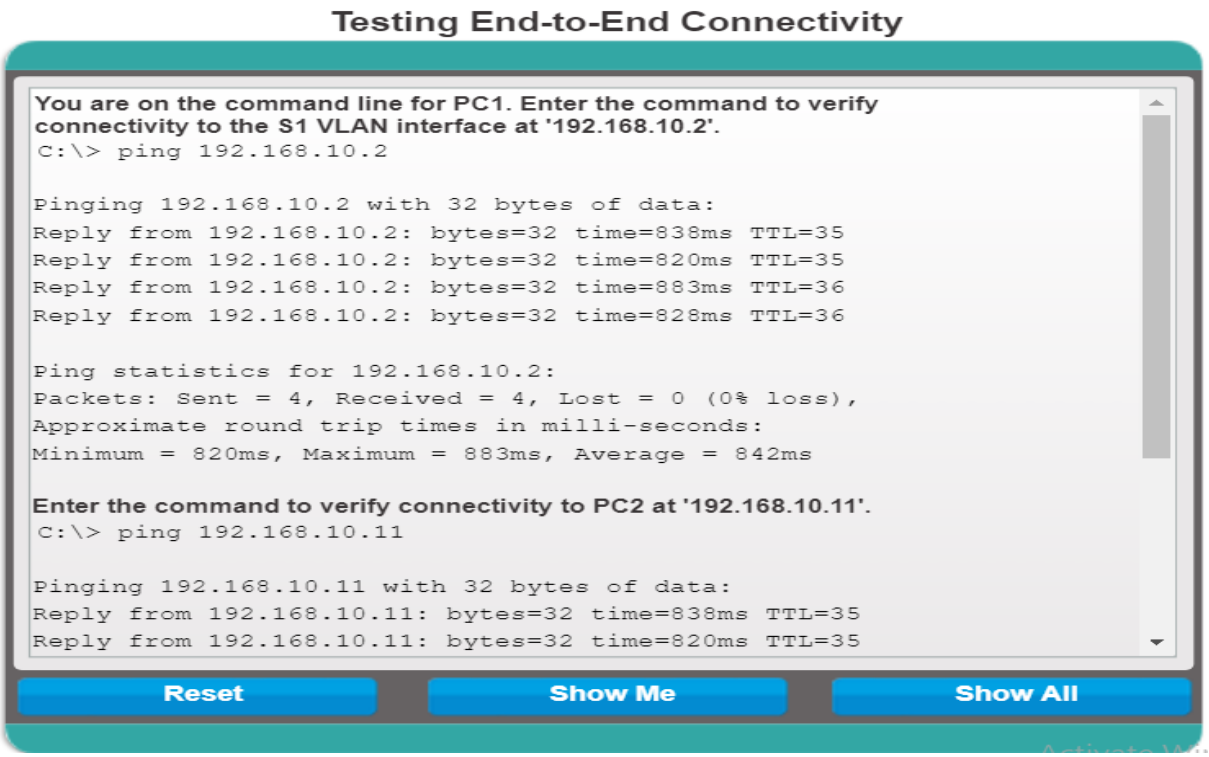
Figure display Interface Summaries

Testing end to end connectivity using ping command

Ping is a command-line utility, available on virtually any operating system with network connectivity that acts as a test to see if a networked device is reachable. The ping command sends a request over the network to a specific device.

Limitations of Ping

- Ping is not a good tool for diagnosing intermittent problems.
- Good results are reliable, but “bad results” could be caused by any number of things, and are not necessarily reliable!
- Ping uses ICMP, which has low priority, showing speeds that are slower than regular network traffic. Some computers reject ICMP, and therefore pinging, entirely.
- When an IP appears between the source and destination in a traceroute command it does not mean that that IP must be pingable.



➢

LO 3.3 – Troubleshoot local area network

- Content /Topic1 Identification of LAN Problems

A. Problem Identification

✓ **When the console does not respond**

This problem can arise due to the Serial Port Issues

Even a minor serial port problem can become a major issue. And without the skills and know-how to identify and resolve a serial port problem, a business could suffer due to ineffective serial connections.

Here's a closer look at five common serial port problems, along with ways to resolve such issues:

1. Incorrect Communication Parameters

The most common cause of serial port communication problems is incorrect communication parameter settings. To operate correctly it is essential that both devices are set up with the same communication parameters, which includes baud rate, parity, number of data bits, and number of stop bits.

2. Incorrect Serial Cable

Is a serial cable connected between a PC and a serial port? If a user leverages the wrong cable, he or she will be unable to establish a connection.

A serial port serves as a physical connector on the back of a computer that allows for the input and output of data, and there are two different types of serial port connectors: 9-pin and 25-pin. As such, the correct cable and/or adapter is necessary to ensure the proper connection at all times.

Another important cable characteristic that is often overlooked is whether the application requires a “null-modem” or “straight through” cable. Null modem cables typically have a female connector on each end and straight through cables have a female connector at one end and a male at the other. Be sure to use the correct cable for your particular application.

3. Bad Serial Cables

What happens if a serial cable is not working properly? This issue can limit data transmission and retrieval but can be easily fixed by replacing the serial cable.

In many cases, a loose cable may simple need to be reconnected to a serial port. But in other situations, an ineffective cable will need to be replaced immediately, especially if the serial port is functioning properly.

View the Stratus Engineering product line for industry leading solutions.

4. Software Conflicts

A software driver may result in a non-working serial port. If this driver is not installed properly or is not compatible with a serial port, it may cease to perform.

Re-installing the affected drivers can help a user overcome this problem. In addition, a user may be able to alter the serial port settings to ensure this issue is fully resolved.

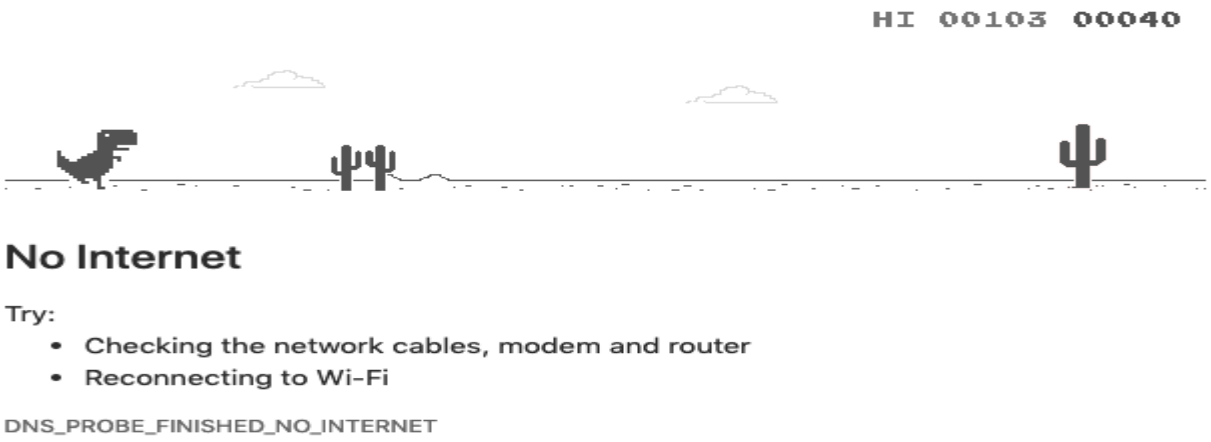
5. Faulty Wiring

When connecting a control system to a device, incorrect wiring can be problematic at times. Typically, the control systems transmit and ground pins must be connected to the connected device’s Receive and Ground pins, respectively. If a connected system needs to receive a response from a controlled device, however, a third wire also may be connected as well.

- ✓ **When the Traffic does not go through**

How to Troubleshoot a Network

Issues can arise at numerous points along the network. Before you start trying to troubleshoot any issue, you want to have a clear understanding of what the problem is, how it came up, who it's affecting, and how long it's been going on. By gathering the right information and clarifying the problem, you'll have a much better chance of resolving the issue quickly, without wasting time trying unnecessary fixes.



I always start troubleshooting using these simple network troubleshooting steps to help diagnose and refine the issue.

1. **Check the hardware**. When you're beginning the troubleshooting process, check all your hardware to make sure it's connected properly, turned on, and working. If a cord has come loose or somebody has switched off an important router, this could be the problem behind your networking issues. There's no point in going through the process of troubleshooting network issues if all you need to do is plug a cord in. Make sure all switches are in the correct positions and haven't been bumped accidentally.

   Next, turn the hardware off and back on again. This is the mainstay of IT troubleshooting, and while it might sound simplistic, often it really does solve the problem. Power cycling your modem, router, and PC can solve simple issues—just be sure to leave each device off for at least 60 seconds before you turn it back on.

2. **Use ipconfig**. Open the command prompt and type “ipconfig” (without the quotes) into the terminal. The Default Gateway (listed last) is your router’s IP. Your computer’s IP address is the number next to “IP Address.” If your computer’s IP address starts with 169, the computer is not receiving a valid IP address. If it starts with anything other than 169, your computer is being allocated a valid IP address from your router.

   Try typing in “ipconfig /release” followed by “ipconfig /renew” to get rid of your current IP address and request a new one. This will in some cases solve the problem. If you still can’t get a valid IP from your router, try plugging your computer straight into the modem using an ethernet cable. If it works, the problem lies with the router.
3. **Use ping and tracert**. If your router is working fine, and you have an IP address starting with something other than 169, the problems most likely located between your router and the internet. At this point, it’s time to use the ping tool. Try sending a ping to a well-known, large server, such as Google, to see if it can connect with your router. You can ping Google DNS servers by opening the command prompt and typing “ping 8.8.8.8”; you can also add “-t” to the end (ping 8.8.8.8 -t) to get it to keep pinging the servers while you troubleshoot. If the pings fail to send, the command prompt will return basic information about the issue.

   You can use the tracert command to do the same thing, by typing “tracert 8.8.8.8”; this will show you each step, or “hop,” between your router and the Google DNS servers. You can see where along the pathway the error is arising. If the error comes up early along the pathway, the issue is more likely somewhere in your local network.
4. **Perform a DNS check**. Use the command “nslookup” to determine whether there’s a problem with the server you’re trying to connect to. If you perform a DNS check on, for example, google.com and receive results such as “Timed Out,” “Server Failure,” “Refused,” “No Response from Server,” or “Network Is Unreachable,” it may indicate the problem originates in the DNS server for your destination. (You can also use nslookup to check your own DNS server.)
5. **Contact the ISP**. If all of the above turn up no problems, try contacting your internet service provider to see if they’re having issues. You can also look up outage maps and related information on a smartphone to see if others in your area are having the same problem.

6. **Check on virus and malware protection**. Next, make sure your virus and malware tools are running correctly, and they haven't flagged anything that could be affecting part of your network and stopping it from functioning.
7. **Review database logs.** Review all your database logs to make sure the databases are functioning as expected. If your network is working but your database is full or malfunctioning, it could be causing problems that flow on and affect your network performance.

✓ **Possible LAN problems causes**

- The remote or local interface is down
- Incorrect address of the remote or local interface
- A conflict of IP addresses
- Domain is down
- The interfaces are down

B. Troubleshooting steps

The common troubleshooting steps are following:

- Verification of cable connectivity
- Verification for the power supply
- Verification of LAN devices LEDs status
- Verification of network software

The common procedures flow to troubleshoot network

- Make Sure It's Actually Your Network Problem
- Power Cycle Everything and Check Other Devices

There's no need to get upset right away, as the fix to your problem might be as simple as rebooting your equipment. Restarting fixes a ton of issues, so make sure it's your first response to network problems, too.

Go ahead and reboot your PC, as well as your modem and router. To clear the modem and router caches, wait 60 seconds before you turn them back on again. When you plug everything back in, plug your modem in first and wait for it to power on before connecting your router.

Turning everything off and back on first ensures that it isn't a temporary network problem. It's better to reboot now than to waste 30 minutes continuing on when you don't need to.

Once you've restarted, if you have another computer (or a mobile device), try getting online with that machine. If you find that no devices can connect, it's likely an issue with your equipment or your ISP.

Should you find that only one computer can't get online, you can continue to narrow down the problem. On that device, make sure to run an antivirus scan to ensure you don't have malware interfering with your connection. You should also make sure that your firewall settings aren't blocking the connection.

Finally, try using a different browser to see if your usual one is somehow damaged.

2. Check Physical Connections

Does your network problem persist after rebooting? Before you start diving into settings and tests, the next step to check is that you're physically connected.

If you use an Ethernet cable to connect to your router, check to make sure that it's not unplugged or damaged. If your laptop has a physical wireless switch, make sure that it's not set to the off position.

Once you've verified a proper connection, check your equipment. Are the lights on your router and/or modem flashing green as normal? If no lights come on after the reboot, the device could be dead or malfunctioning. However, if you get red lights, or a power light but no connection light, your ISP is likely experiencing disruption.

3. Run the Windows Network Troubleshooter

Windows includes some built-in troubleshooters that can automatically find and fix issues. To run the troubleshooter for network problems, right-click the network icon in your System Tray and choose **Troubleshoot Problems**. Once the troubleshooter runs, it could fix issues, find issues but fail to fix them, or find nothing.

If the troubleshooter finds a problem that it fixes, try to connect again. If you get a specific error or problem name that Windows can't fix automatically, take note of it for later research.

4. Check for a Valid IP Address

At this point, you've verified that the problem is not temporary and that all your hardware works. Since Windows can't fix the problem on its own, we need to pinpoint the spot along the connection where the problem is occurring.

It's a good idea to make sure that you don't have any strange IP settings selected. To check this, open **Settings** and go to **Network & Internet > Status**. Below the **Change your network settings** header, choose **Change adapter options**. In the resulting window, double-click the name of your network.

Unless you've set up a static IP (if you don't know what this is, you probably don't use one), make sure you have both **Obtain an IP address automatically** and **obtain DNS server address automatically** checked. Repeat this process for **Internet Protocol Version 6** to ensure everything is automatic there, as well.

Reviewing Your IP Address Validity

Once you've done this, you can check to confirm the router is giving you a valid IP address. Open up a Command Prompt window by typing **cmd** into the Start Menu. Enter **ipconfig** and look for the text under **Ethernet adapter** (for wired connections) or **Wireless LAN Adapter** (for wireless connections).

If **IPv4 Address** starts with **169.x.x.x**, your computer is not receiving a valid IP address from your router. Typing the following two commands will release your computer's current IP address and request a new one, which may resolve this:

ipconfig /release

ipconfig /renew

Should you still have a **169.x.x.x** address after typing the above commands and **ipconfig** again, your machine still isn't receiving an IP from the router. Try plugging your PC directly into the modem with an Ethernet cable and see if you can get online. If so, your router is the problem.

5. Try a Ping and Trace Its Route

If your IP address starts with anything other than **169** when you run **ipconfig**, you have a valid IP address from your router. At this point, you've confirmed the problem is somewhere between your router and the internet.

Type this command to ping Google's DNS servers to see if you can get online (you can replace **8.8.8.8** with anything, such as **www.msn.com**):

ping 8.8.8.8

This will send four packets to Google. If they fail to send, you'll see some basic info about the failure. In case you want to continue pinging indefinitely so you can monitor it while troubleshooting, just add a **-t** to the end, like so:

ping 8.8.8.8 -t

You can press **Ctrl + C** to stop pinging at any time. For more information, type this command to trace the route between your computer and Google's DNS servers:

tracert 8.8.8.8

The above command gives you a step-by-step breakdown of the path the information takes to reach the destination you specify. Watch it, and if it fails, check to see where the problem occurs. If an error pops up early in the route, the issue is likely with your local network.

6. Contact Your ISP

Should all the above steps complete successfully, you've now verified that your equipment is working and confirmed you have a valid IP address from the router. Also, you're sure that the problem is occurring outside of the network for multiple devices. If this is the case, your next best option is to find out if your ISP is having issues.

7. Wait the Network Problems Out

Once you've let your ISP know of the issue and confirmed that it's not just one computer having a problem, all you can do is wait. Many times, you can't fix network issues on your own.

C. Troubleshooting tools:

- ✓ **Ping**

  This utility is used to provide a basic connectivity test between the requesting host and a destination host. This is done by using the Internet Control Message Protocol (ICMP) which has the ability to send an echo packet to a destination host and a mechanism to listen for a response from this host.

- ✓ **Tracert/ traceroute**

  Typically, once the ping utility has been used to determine basic connectivity, the tracert/ traceroute utility can used to determine more specific information about the path to the destination host including the route the packet takes and the response time of these intermediate hosts.

- ✓ **Ipconfig/ifconfig**

The utilities that can be used to find out this IP configuration information

- ✓ **Nslookup**

  The nslookup utility can be used to lookup the specific IP address(es) associated with a domain name. If this utility is unable to resolve this information, there is a DNS issue.

- ✓ **Netstat**

  It is also possible to use the netstat utility to determine which services on a host that is associated with specific active ports.

- ✓ **PuTTY/Tera Term**

  When connecting to a variety of different types of equipment, a telnet, SSH or serial client is required; when this is required both the puTTY and Tera Term programs are able to provide these functionalities.

- ✓ **Subnet and IP Calculator**

  One of the most important tools in the belt of a junior network engineer is an IP network calculator. These can be used to unsure a correct IP address selection and with this a correct IP address configuration.

- ✓ **Speedtest.net/pingtest.net**

  The speedtest.net site provides the ability to determine the amount of bandwidth that is available to a specific host at a specific point in time; this is often a good tool to use when measuring how long it is going to take to upload or download information from a local to remote host.

- ✓ **Pathping/mtr**

  These tools take the functionality and information that can be obtained from these types of tools and provide a more detailed single picture of the path characteristics from a specific host to a specific destination.

- ✓ **Route**

  The last of the tools covered in this article is the route utility. This utility is used to display the current status of the routing table on a host.

- ✓ **Diagnostic command**

Network Diagnostic commands are commands used to know status. These commands are typed in commands prompt of your computer after you have typed IPCONFIG just use "/ (command)". e.g. "IPconfig/all" for full display of configuration information.

- ✓ **Show command**

  Show command display the status of routers interfaces, among others things, this output provide information about interface status(up/ down) protocols status on the interfaces.

D. Basic utilities

- ✓ Putty/TeraTerm
- ✓ Subnet and Ip Calculator
- ✓ Utility application Software
- ✓ Speedtest.net/pingtest.netpathping/mtr

E. Hardware tools the figure below show as different hardware troubleshooting tools

Figure of Troubleshooting Tools kit

Learning Unit 4 – **Document the work done**

LO 4.1: Select timber according to availability

- Content/Topic 1 (Description of network status before)

A. Status of network infrastructure

What is a network infrastructure?

Network infrastructure refers to all of the resources of network that makes network or internet connectivity, management, business operations and communication possible. Network infrastructure comprises hardware and software, system and devices, and it enables computing and communication between users, services, applications and processes. Anything involved in the network, from servers to wireless routers, comes together to make up a system's network infrastructure. Network infrastructure allows for effective communication and service between users, applications and devices.

✓ **What is network status**

A network status is any situation when your business network infrastructure isn't operating as intended maybe you have lost power in your office, or you have experienced a data loss incident that keeps you from accessing crucial information.

B. Description of problems found

When your network goes down, problems found are:

✓ **Hacking attacks:** even if you don't expect to be hit by a hacking attack in the future, anything can happen. Most hackers do not intend to hit specific victims so even something like an unexpected malware infection cloud make problems for your network organization.

✓ **User errors:** all it takes is an employee moving an important file to the wrong location to cause downtime.

✓ **Natural disasters** are issues like power outages/surges, infrastructure fires, hurricanes, earthquakes, floods, and so much more all hold the power to bring your network down and lead to data loss.

C. **Review of user manual and previous report**

A great user manual educates people about a product, while also teaching them how to use product features effectively. As an author, your ultimate goal is comprehension—you want readers to easily be able to read, reference, and absorb information.

General guidelines for user manuals

- ✓ Provide a real (physical) user manual with the product.
- ✓ Make sure the instructions actually map on to the product in all respects.
- ✓ Include a one-page quick start guide.
- ✓ Present instructions as step-by-step procedures.
- ✓ Tell the user what functions there are, and what they are for — not just how to use them... but avoid marketing waffle (they already bought the product!)
- ✓ Ensure that the writers are part of the product design team.
- ✓ Write the user manual in synch with the product's development timeline — not under pressure of shipping deadlines.
- ✓ Make sure the writers have the product, understand the product, and actually use the product as they write.
- ✓ Consider the needs of disabled users (i.e., low vision, colour-blind) and provide alternative manuals in Braille, large print, audio etc.
- ✓ User-test the product and the user manual with real users (including disabled users).

Content/Topic 2: Description of problems, procedures suggestion and solution implementation

A. Solution implementation

1. Computer Virus

- **The problem:** I think I have a virus on my network!

Network viruses can completely disable a computer network, so this is the first issue we're going to tackle. There can be a number of causes of computer viruses. Viruses can come from a wide range of sources, such as e-mail attachments, malicious software, online advertisements, and yes, even social media.

What are some signs of computer viruses? While remediating an infection on a single computer can be daunting, removing a virus from an infected network is a real challenge since it can hide on any computer. So, here's how you can fix it.

- **The solution:**

  Step 1: Check the severity of the infection by running a complete network scan to find malicious files or programs. Make sure that your antivirus and anti-malware programs are up to date and able to scan hidden files, the root directory, and all running programs. Also, try to have your antivirus/anti-malware software scan your e-mail inbox for any malicious materials.

  Step 2: Back up all of your system files using the necessary tools. Running a complete system backup will ensure that your data isn't lost and that the network will remain stable. The Windows' "System Restore" option will allow you to set up a restoration that can often be useful in an emergency.

  Step 3: Confine all suspicious, irregular files. Isolating them will prevent their exchanging with other files or your network system. Then, disinfect or completely wipe all quarantined files. Manually delete any emails that were identified by your antivirus software.

2. **Unable to connect to the internet**

   Using a wireless or wired network is great for mobility, but can hinder your productivity when it decides to malfunction. There are a few different reasons why your wireless network is having connectivity issues, such as the wireless router or the network card itself. This issue will require a bit of network troubleshooting to find a solution, so let's get to work.

   Solution

   Step 1: If your router won't connect to the internet, try putting your computer or device right next to the router. If this causes your equipment to connect, then the system hardware may have been the issue. If this didn't fix the problem, proceed to Step 2

   Step 2 : Update the network card. Sometimes, your network card will receive a strong signal, but won't be able to transmit it quickly a nd effectively resulting in the need for network troubleshooting. Updating the driver might solve the problem entirely, but if it doesn't, you might need to contact your IT department or provider and consider replacing the hardware altogether.

3. **Duplicate of IP addresses**

   The problem: I got an error message that say that the IP address is already in use

   A small error window just popped up on your screen saying that your IP address is already in use. How is this even possible and what causes this IP address conflict? Well, there are a few reasons why this can happen:

- ✓ Your system administrator could have assigned two computers on a local area network(LAN)the same static IP address
- ✓ Your internet service provider accidentally assigned two people the same IP address.
- ✓ The network's Dynamic Host Configuration protocol (DHCP) server has allowed the same dynamic address to e assigned to multiple computers automatically.
- ✓ Your system administrator has assigned a static IP address to a computer within the local network's DHCP range, and the same address is automatically given y the local DHCP server.

These are just a few of the plethora of reasons why IP address conflicts take place. Here are some ways to fix this issue:

- **solution**

Window if you have a dynamic IP address:

Step 1: click the "start"button and click "Run"enter "cmd"into the text box and click "OK".the windows command prompt will open.

Step 2: Type "**IPconfig/renew**"into the command prompt and press "enter".this will refresh your dynamic IP address.

Step 3: check your network connection: your computer will receive an available IP address that is not already taken.

Windows if you have a static IP address:

Step 1: Right click "network neighbourhood"on your desktop on window 7 or Vista this will be labelled "network"click next the click properties.

Step 2: Right click on your network card and click "properties"in most cases, your network card will be labelled "local area network connection."

Step 3: select "TCP/IP"in the list and then, click the "properties"button under the list of options.

Enter in a new IP address in the opened window. Click "OK" to confirm the changes you have made.

MAC

Step 1: click on "system preferences"in your dock. Then click on "network".

Step 2: select "WIFI"on the left side of the window. Then click "Advanced", which is located on the butto right.

Step 3: on the next page select the “TCP/IP”tab and then click “Renew DHCP Lease”on the right side of the window.

4. **Slow performance**

Problem: My applications are responding very slowly

Why is my computer so slow?

Slow-running applications can put a damper on your productivity in the workplace. One of the most common network issues that business networks fight with is slow applications.

This happens especially when a computer first turns on or connects to a network. In most cases, this is caused by heavy bandwidth usage. In other instances, it can be caused by lack of hard drive space, running too many applications at once, having too many browser tabs open at one time, or even just a dusty room! The solution for this issue depends on the root of the problem.

Once you’ve gotten rid of some of your browser’s extensions, eliminated applications you aren’t using, or identified the application that’s eating up all of your processing power, you should be able to see a huge difference in your computer’s processing speed. (You can do this by using the Task Manager for Windows or the activity monitor for Mac to see which applications are slowing you down). If this solution did’t works for you, there is what you can do:

The solution:

Be sure to enforce proper network use by making sure that users aren’t viewing too much digital content via streaming or continuously downloading large files. Doing so will help you keep your bandwidth use under control. However, if you find that your employees are utilizing the network correctly, it might be time to upgrade your network to meet your business needs.

If you feel that the sluggishness of your applications is due to another issue, proceed to step 1.

Step 1: Try restarting your PC. Sometimes, a quick reset will fix any and all issues right away. Doing so will clear your system memory (RAM). If this works, remember to shut down your PC when it’s not in use. If this does not help, proceed to step 2

Step 2: Now, it’s time to check on your hard drive and make sure that it’s not approaching the end of its lifespan. So let’s run a hard driver check.

Right click on “Drive”. Then, click “Properties” and then click “Tools”. Click “Check Now”. Select “Scan for and attempt recovery of bad sectors”. Doing this will stop your computer from tapping into any malfunctioning area of the hard driver.

Mac

Click “Applications” from the “Finder”, then “Utilities”, and then “Disk Utility”. Highlight the hard drive that’ giving you trouble and then select”First Aid”.

If your hard drive is healthy, but you think it is becoming too full with data, proceed to step 3.

Step 3: Get rid of unnecessary files from programs that have gone unused. System backups and restore points can eat up a lot of space, so don’t hang onto more versions of this software than you need. You might also consider uploading your data on the cloud to save your hard drive.

Step 4: If you’ve completely deep-cleaned your computer and checked all of the possible issues above, but your computer is still running slowly, it might be time to upgrade your RAM so that your computer has more memory. Certain programs take more RAM to run properly than others and if you don’t have enough RAM ready, your computer will not be able to handle it. Look into RAM upgrade option

5. **IP Address Exhaustion**

The problem: I cannot get IP address.

So, your network seems to have gone down. Your operating system has sent you an alert stating that the address was not received from the DHCP server. You’ve just checked the network adapter status and noticed that there’s actually no IP address to be found. What now?

There are a few different reasons why this could happen. It could be that the DHCP server is out of addresses, the device might be set to use a static address rather than a DHCP address, or maybe the DHCP request from the device never made it to the server.

- **Solution**

Step 1: Check the network interface card (NIC). You can find this by opening the control panel, then the device manager. Then, select “Hardware and Sound” and then select “Device Manager”. Expand the Network Adapters item to view all network adapters, although you will most likely only have one. Verify that your system is configured to utilize DHCP.

Step 2: Check the switch to see which virtual LAN (VLAN) the port is set as a member. Verify that other devices on this particular VLAN are able to get an IP address. If they can't, the issue is that the network is not sending DHCP requests to the server.

If this issue is taking place with more than one device then the issue is likely the server itself.

6. VPN Errors

   The problem: I got an error message saying that my device was "unable to establish the VPN connection"or error 800.

   Your virtual private network (VPN) works to provide a safe connection between a local client and a remote server. When you can't connect to a VPN, you'll receive an error message that usually states something along the lines of "VPN error 800 – Unable to establish the VPN connection". This can happen if the client device disconnected from the local network, the network's firewall is blocking the VPN traffic, or if the name/address specified for the VPN server was incorrect.

- **Solution**

  Step 1: Check the connection between the client and server. Attempt to connect to the server from a different client device to verify whether the network issue is widespread or if it is affecting only one client.

  Step 2: Verify that the name entered on the client side matches the server name given by the VPN administrator. In some instances, users can specify an IP address rather than a name, while it's more typical for users to mistype the address than the name. VPN servers can also change their IP addresses in some instances, especially DHCP networks.

  Step 3: If the first two steps didn't clear up the issue, now it's time to make sure that the firewall isn't blocking your connection with the VPN. Do so by temporarily disabling it to retry the connection. If this solves the problem, you need to update the firewall settings specific to the port numbers that the VPN on the network is using to prevent this issue from happening again.

  If none of this troubleshooting solved the issue, it could be possible that the server is overloaded with clients or that it is offline. Check with your IT department to see what can done

7. **Connection errors and network connectivity**

   The problem: My network has limited connection or no connectivity all

Connection issues are some of the most annoying, frustrating network issues of all. These issues can be a result of all types of glitches and issues within the computer and/or the network itself. So, if your computer has handed you a lovely “limited or no connectivity”error message

- **Solution**

Step 1: Restart your computer. A quick reboot can often be a life-saver. If you’ve already tried this or restarting the computer did not fix anything, proceed to step 2

Step 2: Restart your router or modem. DO NOT reset the router or modem or restore its settings back to factory default. Simply turn the router or modem off and back on. If this doesn’t work or only works for a moment, keep going to step 3

Step 3: If you are connected to your network via Ethernet cable, unplug the cable and then reattach it. If needed, replace your cable with a new or different cable to see if this was the cause of the issue.

Step 4: If you’re connected via Wi-Fi when you see this error, it’s a possibility that the network adapter is attempting to conserve power. Stop this by finding the Network and Sharing Centre in the Control Panel. Right click “Wi-Fi Connection”, select “Properties”, click “Configure” and find the “Power Management” tab. Click and uncheck the option that allow your computer to turn off device to conserve power.

Step 5: If you’ve tried all of this and there’s still no connection, unplug your router and connect your computer directly to your modem. If this solves the issue, then your router is likely to be malfunctioning. If not, contact the router manufacturer for support.

If the error remains and the network is still down, reach out to your internet service provider for help.

- Content/Topic 3: Description of Network Devices, equipment and materials used

Here you describe all **materials** and equipment to be **used**, whether or not shown on.

What are the materials used for set up a SOHO LAN?

No	Materials /equipments	Description
1	router	Router is defined as a device that **connects two or more networks** and forwards data packets along **networks**.

2	switch	Switch is defined as a computer networking device that connects devices on a computer network by using packet **switching** to receive, process, and forward data to the destination device.
3	Person computers	**Person computer** is a microcomputer designed for use by one **person** at a time.
4	Rack mount	Rack mounting is commonly used with large companies to hold their network servers, routers, switches, or other network devices.
5	Network adapter	is a computer hardware component that allows a computer to connect a computer **network**
6	Network cable	Network cable 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.
7	Crimping tools	Crimping tool is designed to crimp or connect a connector to the end of cable.
8	Network connectors	A connector is a device that terminates a segment of cabling or provides a point of entry for networking device such as computers, HUB, Switches and routers.
9	Drilling machine	A drilling machine, called a drill press is used to cut holes into or through metal, wood, or other materials.
10	Modem	MODEM Short for modulator-demodulator. A **modem** is a device or program that enables a computer to transmit data over, for example,

		telephone or cable lines.
11	server	Server is a computer, a device or a program that is dedicated to managing network resources.
12	Access point	**Access point** is a station that transmits and receives data (sometimes referred to as a transceiver).
13	Shared device	Shared printers and peripherals are hardware resources provided to the users of the network by servers. Resources provided include data files, printers, software, or any other items used by clients on the network.
14	repeater	**Repeater** is device used to regenerate the signal over the same **network** before the signal becomes too weak or corrupted so as to extend the length to which the signal **can** be transmitted over the same **network**.

- ✓ **Write technical journal and recommendation**

1. Technical Journal

In the modern high performance computing systems, innovative as well as hi-tech research is required to address the challenges in the networking. The Journal of Networking Technology will act as a platform to publish and disseminate the cross cutting research in networking systems. The journal solicits original research in the following but not limited areas.

Computer network components

Network architecture and design

Digital networks

Broadband networks

Internet and Web Technology

Sensor networks

Adhoc networks

Mobile and wireless networks

Data networks

Next generation networks

Optical networks

Neural networks

Signal processing

Satellite communication

8. **Recommendation report**

Basic Network Recommendations

- ✓ **Correct User Rights**

Administrator rights should be granted with caution. Users who have administrator rights can potentially do things that could be seriously damaging. They can, and do, unintentionally make changes that decrease the level of network security. They can also be tricked into running malware, which would run with the user's administrator privileges.

If they are careless about protecting their authentication details, their user-name and password may be stolen. This may allow unauthorized third parties to log in and carry out damaging actions, intentionally or accidentally. For better security, make sure that users have a privilege level which is appropriate for the tasks they carry out and minimize the number of users that have administrator privileges.

- ✓ **Only Download from Trusted Websites**

You should determine who has a genuine business need to download files and applications from a website. Use web filtering to restrict this to people with a genuine requirement and ensure that the select few are educated in how to download files safely. Files can often be downloaded from multiple locations on the Internet, but not all locations are equally secure. Make sure that your

users can only download from trusted sites, such as primary source websites rather than file-sharing or generic websites.

- ✓ **Review Network Shares**

  Carry out an audit of network shares. Users should only have access to files and folders that they need as part of their day-to-day work. You should also be aware that a lot of malware can spread via networks. This is typically due to there being little or no security on network shares. Remove access to unnecessary shares and secure the others and their contents to limit network-aware malware from spreading.

- ✓ **Restrict Network Connections**

  When a computer connects to a network, it can adopt that network's security settings for that specific session. If the network is outside the administrator's control, the security settings may be weak and put the computer at risk. Restrict users from connecting computers to unapproved networks. In most instances users only need to connect to the main company network.

- ✓ **Change Your Default IP Range**

  Networks typically use standard IP ranges, like 10.1.x.x or 192.168.x.x. This standard approach means machines configured to look for this range could accidentally connect to a network outside your control. Change the default IP range so that computers are less likely to find a similar range. You should also consider adding firewall rules, which allows only approved users to connect.

- ✓ **Review Open Ports**

  You should periodically audit the open ports on your network and block all unused ones. If you leave them open for long periods of time without surveying them, you increase the chance of letting in intruders. If ports are left open, Trojans and Worms may use them to communicate with unauthorized third-parties.

- ✓ **Audit the Entry Points to Your Network**

  Networks undergo frequent change, so it is very important to review all the routes into your organization's infrastructure on a regular basis. For each means of entry, consider how to best secure the routes to stop unwanted files and applications entering undetected or sensitive information leaking out.

- ✓ **Network Segmentation**

  There are a number of advantages to segmenting your network.

  Improved security comes from the fact that broadcasts will be contained to local network and internal network structure will not be visible from outside. If an attacker gains unauthorized access to a network, segmentation or "zoning" can provide effective controls to limit further movement across the network.

  Improved performance can be achieved, because on a segmented network there are fewer hosts per subnetwork, thus minimizing local traffic. It can also help to containing network problems, limiting the effect of local failures on other parts of network.

  When business critical systems are affected, they can slow business processes significantly. To help protect them, consider having them on a different network from the one used for day-to-day activities.

- ✓ **Resist the Temptation to Live Test**

  Although most software developers are good people and rigorously test their software before releasing it, they are unlikely to have your infrastructure's exact configuration and setup. To ensure that a new software version or update does not cause problems, test it on a virtual system and check its effects before deploying to the real live network.

- ✓ **Block Unused USB Ports**

  Many devices, when connected to a USB port, can be automatically detected and mounted as a drive. USB ports may also allow attached devices to auto-run stored software. Users are often unaware that even the safest and most trusted devices can potentially introduce malware onto their computer. To prevent any accidents, it is much safer to disable all unused ports

Learning Outcome 4.2: Document on network status

Content/Topic 1: Description of network status before

- **Status of network infrastructure**

  Network infrastructure refers to all of the resources of a **network** that make **network** or internet connectivity, management, business operations and communication possible.

  The entire network infrastructure is interconnected, and can be used for internal communications, external communications or both. A typical network infrastructure includes:

- Networking Hardware:
- ✓ Routers
- ✓ Switches
- ✓ LAN cards
- ✓ Wireless routers
- ✓ Cables
- Networking Software:
- Network operations and management
- Operating systems
- Firewall
- Network security applications
- Network Services:
- T-1 Line
- DSL
- Satellite
- Wireless protocols
- IP addressing

  When you are making a report you have to describe or to make a good explanation on how the network was before you start to work.

- **Describe problems found**

  To describe the network problem found is to explain the Status of network infrastructure and describe problems of network to be handled.

  Simple network troubleshooting steps that help to diagnose and refine the problem

- **Check the hardware**. Check all your hardware to make sure it's connected properly, turned on, and working.
- **Use ipconfig**. Open the command prompt and type "ipconfig" (without the quotes) into the terminal. The Default Gateway (listed last) is your router's IP. Your computer's IP address is the number next to "IP Address." If your computer's IP address starts with 169, the computer is not receiving a valid IP address. If it starts with anything other than 169, your computer is being allocated a valid IP address from your router.

Try typing in “ipconfig /release” followed by “ipconfig /renew” to get rid of your current IP address and request a new one. This will in some cases solve the problem. If you still can’t get a valid IP from your router, try plugging your computer straight into the modem using an Ethernet cable. If it works, the problem lies with the router.

- **Use ping and tracert**. If your router is working fine, and you have an IP address starting with something other than 169, the problems most likely located between your router and the internet. At this point, it’s time to use the **ping** tool. Try sending a ping to a well-known, large server, such as Google, to see if it can connect with your router. You can ping Google DNS servers by opening the command prompt and typing “ping 8.8.8.8”; you can also add “-t” to the end (ping 8.8.8.8 -t) to get it to keep pinging the servers while you troubleshoot. If the pings fail to send, the command prompt will return basic information about the issue.

  You can use the **tracert** command to do the same thing, by typing “tracert 8.8.8.8”; this will show you each step, or “hop,” between your router and the Google DNS servers. You can see where along the pathway the error is arising. If the error comes up early along the pathway, the issue is more likely somewhere in your local network.
- **Perform a DNS check**. Use the command “nslookup” to determine whether there’s a problem with the server you’re trying to connect to. If you perform a DNS check on, for example, google.com and receive results such as “Timed Out,” “Server Failure,” “Refused,” “No Response from Server,” or “Network Is Unreachable,” it may indicate the problem originates in the DNS server for your destination. (You can also use nslookup to check your own DNS server.)
- **Contact the ISP**. If all of the above turn up no problems, try contacting your internet service provider to see if they’re having issues. You can also look up outage maps and related information on a smartphone to see if others in your area are having the same problem.
- **Check on virus and malware protection**. Next, make sure your virus and malware tools are running correctly, and they haven’t flagged anything that could be affecting part of your network and stopping it from functioning.
- **Review database logs**. Review all your database logs to make sure the databases are functioning as expected. If your network is working but your database is full or malfunctioning, it could be causing problems that flow on and affect your network performance.

Review of user manual and previous report

As the purpose of network documentation is to keep networks running as smoothly as possible while minimizing downtime when repairs are necessary.

Essential parts of network documentation include:

- Map of the entire network to include locations of hardware and the cabling that connects the hardware
- Server information such as data on the individual servers, schedules and locations of backups
- Software information such as current versions, dates, licensing and support
- Vendor and contractor information
- Service agreements
- Detailed record of problems and solutions: dated along with procedures and results

Notation that helps administrators remember key details are the basics of network documentation while visual representations assist in helping administrators understand how equipment and the notation relates to one another.

A user guide or user's guide, also commonly known as a manual, is a technical communication document intended to give assistance to people using a particular system. So maybe there are some other technicians came before you have to consult what they said, like the problems they faced and how they resolved those issues.

Having an expert review any existing *network implementation plan* document will definitely help identify any gaps or risks that may have not been highlighted. The *network implementation plan review* service provides this additional level of diligence needed to ensure project tasks are optimally planned and deliver on the promise with minimum risk.

- Content/Topic 2: Implementation of solutions on problems found

Problem finding: Before you start trying to troubleshoot any issue, you want to have a clear understanding of what the problem is, how it came up, who it's affecting, and how long it's been going on.

By gathering the right information and clarifying the problem, you'll have a much better chance of resolving the issue quickly, without wasting time trying unnecessary fixes.

On this level, you have to suggest the solutions to the problem found by explaining clearly the task to be accomplished regarding to the network devices, equipment, and materials to be used.

Most of the organizations are stuck with reactive mode due to the complexities of using the existing network management tools. At the same time, business users are more service-focused and less

particular about the underlying technology. Organizations demand reliable network maintenance support services that help to get their job done. In spite of using the latest gigabit network hardware, enterprises are plagued with intermittent bandwidth issues, performance issues, and complaints from users of slow network response.

Solution implementation: Organizations demand reliable network maintenance support services that help to get their job done.

Solution implementation involves:

- Being committed to a solution.
- Accepting responsibility for the decision.
- Identifying who will implement the solution.
- Resolving to carry out the chosen solution.
- Exploring the best possible means of implementing the solution.

Procedures of the task accomplished: Procedure is a sequence of steps that include preparation, conduct and completion of a task. Each step can be a sequence of activities and each activity a sequence of actions.

Procedures is needed when you have to perform the complex task or when the task is routine and you want it to be performed consistently. Procedures are driven by completion of the task; it includes:

- Meet with the teams responsible for the procedure
- Start with a short introduction
- Make a list of required resources
- Document the current procedure
- Add supporting media
- Include any relevant resources
- Check the procedure is accurate
- Test in a controlled environment
- Make improvements if necessary
- Deploy

- **Content/Topic 3: Report of Network Devices, equipment and materials used**

  When you are developing your report, remember to include the network devices, equipment and materials used for better understanding of someone who will read your report.

  The following are the examples of network devices, equipment and materials that can be used:

- LAN Cable
- Connectors
- Crimping tools
- Krone tools
- UTP Connector
- Punch down tool
- Cable tester
- Coaxial cable
- USB Wireless interface
- Wireless pc card
- WAP
- ADSL Modem
- Cable modem
- Router
- Switch

- **Body:** This is the main section of the report. There needs to be several sections, with each having a subtitle. Information is usually arranged in order of importance with the most important information coming first.
- **Conclusion**: This is where everything comes together. Keep this section free of jargon as most people will read the Summary and Conclusion.
- **Recommendations**: This is what needs to be done. In plain English, explain your recommendations, putting them in order of priority.
- **Appendices**: This includes information that the experts in the field will read. It has all the technical details that support your conclusions.

  Remember that the information needs to be organized logically with the most important information coming first.

LO4.2. Write technical journal and recommendation

- **Content/Topic 1: Description of network status before**

Status of network infrastructure

Network infrastructure refers to all of the resources of a **network** that make **network** or internet connectivity, management, business operations and communication possible. The entire network infrastructure is interconnected, and can be used for internal communications, external communications or both. A typical network infrastructure includes:

✓ Networking Hardware:

Routers

Switches

LAN cards

Wireless router

Cables

✓ Networking Software:

- Network operations and management
- Operating systems
- Firewall
- Network security applications

✓ Network Services:

- T-1 Line

- DSL
- Satellite
- Wireless protocols
- IP addressing

Network Performance Optimization

Network performance optimization is the process of assessing the network's status on an ongoing basis by monitoring and discovering network traffic and logs. Possible monitoring targets include the following: data rates, available bandwidth, WAN link status, backup time, device response rate, and component failures. The methods in which we will use to discover performance issues may include the following:

Packet shapingthis technique is used by specifying what traffic at what rate (rate limiting) in a span of time (bandwidth throttling) you are going to allow in or out of your network.

Traffic shaping is more common at the border routers of an environment working to delay traffic where appropriate as it enters the network.

Traffic policing **and** ***traffic contract*** are terms used to describe how packets are allowed in/out of the network and at what time.Enforcing compliance with the traffic contract is how traffic sources are aware of what traffic policy is in effect.Traffic shaping shapes the traffic into optimal network utilization for the allocated bandwidth on a particular link.

Load balancing*Load balancing* is a technique used on computer networks to distribute the incoming traffic upon other network devices if there are indications of increased network traffic or "load."Load balancing allows a group or cluster of data center servers to share the inbound traffic all the while seeming as if there actually is only one external connection.Once traffic enters the network via the one external entry point, it is distributed among other servers internally connected to share the high traffic volumes.

High availability*High availability* is a system design protocol, which once implemented assures a specific degree of uptime continuity in a specific period of time.The goal of high availability is to ensure users have the maximum uptime so they can access network resources anytime and anywhere.Reducing unplanned downtime increases a business's potential productivity.

Caching engines*Cache* is data that is copied from the original data and is saved for computers to access locally instead of having to retrieve the same data again from the source server.Accessing cached data is quicker since it is stored in a temporary location for a specific amount of time.Cache

engines are servers that are dedicated to caching data for clients.If an item in cache is not used often enough, it is discarded until the client requests it again.Common implementations of cache engines will target Web server content.

Fault tolerance Fault tolerance allows continued operations in the event of a system or system component failure.

When you are making a report you have to describe or to make a good explanation on how the network was before you start to work.

Describe problems found

To describe the network problem found is to explain the Status of network infrastructure and performance evaluation then describe problems of network to be handled.

Simple network troubleshooting steps that help to diagnose and refine the problem

- **Check the hardware**. Check all your hardware to make sure it's connected properly, turned on, and working.
- **Use ipconfig**. Open the command prompt and type "ipconfig" (without the quotes) into the terminal. The Default Gateway (listed last) is your router's IP. Your computer's IP address is the number next to "IP Address." If your computer's IP address starts with 169, the computer is not receiving a valid IP address. If it starts with anything other than 169, your computer is being allocated a valid IP address from your router.

  Try typing in "ipconfig /release" followed by "ipconfig /renew" to get rid of your current IP address and request a new one. This will in some cases solve the problem. If you still can't get a valid IP from your router, try plugging your computer straight into the modem using an Ethernet cable. If it works, the problem lies with the router.
- **Use ping and tracert**. If your router is working fine, and you have an IP address starting with something other than 169, the problem's most likely located between your router and the internet. At this point, it's time to use the **ping** tool. Try sending a ping to a well-known, large server, such as Google, to see if it can connect with your router. You can ping Google DNS servers by opening the command prompt and typing "ping 8.8.8.8"; you can also add "-t" to the end (ping 8.8.8.8 -t) to get it to keep pinging the servers while you troubleshoot. If the pings fail to send, the command prompt will return basic information about the issue.

  You can use the **tracert** command to do the same thing, by typing "tracert 8.8.8.8"; this will show you each step, or "hop," between your router and the Google DNS servers. You can see where along

the pathway the error is arising. If the error comes up early along the pathway, the issue is more likely somewhere in your local network.

- **Perform a DNS check**. Use the command "nslookup" to determine whether there's a problem with the server you're trying to connect to. If you perform a DNS check on, for example, google.com and receive results such as "Timed Out," "Server Failure," "Refused," "No Response from Server," or "Network Is Unreachable," it may indicate the problem originates in the DNS server for your destination. (You can also use nslookup to check your own DNS server.)
- **Contact the ISP**. If all of the above turn up no problems, try contacting your internet service provider to see if they're having issues. You can also look up outage maps and related information on a smartphone to see if others in your area are having the same problem.
- **Check on virus and malware protection**. Next, make sure your virus and malware tools are running correctly, and they haven't flagged anything that could be affecting part of your network and stopping it from functioning.

Review database logs. Review all your database logs to make sure the databases are functioning as expected. If your network is working but your database is full or malfunctioning, it could be causing problems that flow on and affect your network performance.

Review of user manual and previous report

As the purpose of network documentation is to keep networks running as smoothly as possible while minimizing downtime when repairs are necessary.

Essential parts of network documentation include:

- Map of the entire network to include locations of hardware and the cabling that connects the hardware
- Server information such as data on the individual servers, schedules and locations of backups
- Software information such as current versions, dates, licensing and support
- Vendor and contractor information
- Service agreements
- Detailed record of problems and solutions: dated along with procedures and results

Notation that helps administrators remember key details are the basics of network documentation while visual representations assist in helping administrators understand how equipment and the notation relates to one another.

A user guide or user's guide, also commonly known as a manual, is a technical communication document intended to give assistance to people using a particular system. So maybe there are some other technicians came before you have to consult what they said, like the problems they faced and how they resolved those issues.

Having an expert review any existing *network implementation plan* document will definitely help identify any gaps or risks that may have not been highlighted. The *network implementation plan review* service provides this additional level of diligence needed to ensure project tasks are optimally planned and deliver on the promise with minimum risk.

- **Content/Topic 2: Suggestion of solutions on problems found**

  Before you start trying to troubleshoot any issue, you want to have a clear understanding of what the problem is, how it came up, who it's affecting, and how long it's been going on.

  By gathering the right information and clarifying the problem, you'll have a much better chance of resolving the issue quickly, without wasting time trying unnecessary fixes.

  On this level, you have to suggest the solutions to the problem found by explaining clearly the task to be accomplished regarding to the network devices, equipment, and materials to be used.

  Description of solution implementation

  Most of the organizations are stuck with reactive mode due to the complexities of using the existing network management tools. At the same time, business users are more service-focused and less particular about the underlying technology. Organizations demand reliable network maintenance support services that help to get their job done. In spite of using the latest gigabit network hardware, enterprises are plagued with intermittent bandwidth issues, performance issues, and complaints from users of slow network response.

  Organizations demand reliable network maintenance support services that help to get their job done.

  Solution implementation involves but not limited to:

- To be committed to a solution
- Take responsibilities and accept the decision.
- Identification and selection of who will implement the solution.
- Carrying out the chosen solution.
- Exploring the best possible means of implementing the solution.

- **Content/Topic 3: Description of procedures of the task accomplished**

  Procedure is a sequence of steps that include preparation, conduct and completion of a task. Each step can be a sequence of activities and each activity a sequence of actions.

  Procedures is needed when you have to perform the complex task or when the task is routine and you want it to be performed consistently. Procedures are driven by completion of the task; It includes:

- Meet with the teams responsible for the procedure
- Start with a short introduction
- Make a list of required resources
- Document the current procedure
- Add supporting media
- Include any relevant resources
- Check the procedure is accurate
- Test in a controlled environment
- Make improvements if necessary
- Deploy

Network Devices, equipment and materials used

While developing the report, you have to include the network devices, equipment and materials used. The following are the examples of network devices, equipment and materials that can be used:

- LAN Cable
- Connectors
- Crimping tools
- Krone tools
- UTP Connector
- Punch down tool
- Cable tester
- Coaxial cable
- USB Wireless interface
- Wireless pc card
- WAP
- ADSL Modem
- Cable modem
- Router
- Switch

Description of the network status after work

After your work, you have to describe current network status by showing clearly the problems solved with more explanation, and give recommendation for further usage. The following is an example of the report form that summarizing the status of network and after work and the work of a network technician.

WORK REPORT OF A NETWORK TECHNICIAN

Company/Technician Address	
Company /Technician Name:	
Website /Email address:	
PO BOX :	
Office /Mobile Phone Contact :	
Company/Technician office Location:	
Customer Address	
Customer Name:	
Website /Email address	
PO BOX :	
Office /Mobile Phone Contact :	
Customer office Location:	
Status Before Work:	
User manual and previous report:	
Problems found :	
Solution and Implementation:	
Procedures of the task accomplished:	
Network Devices, equipment and materials used:	

Status After Work:	
Observations /Recommendations:	
Customer Verification	
Names:	
Signature /stamp Date:	
Company /Technician Verification	
Name:	
Signature/stamp Date:	

Content/Topic 4: Writing technical journal and recommendation report

When it comes to the writing of a technical journal and recommendation report, the format is very important because it is unique from other reports in that it carries technical information. A technical journal and recommendation report contains technical information which should be planned well. You need to understand all the structure to achieve your objective. It should contain the following:

The title page

The title page comes first when you write your technical journalreport. The title page contains the title of the journal report the date and the institution details. This first page is also referred to as the cover page. The title is a separate entity when it comes to word count, so you should not include it on your word count.

Introduction

In the introduction, you are supposed to highlight the main aims of the journal report to the reader. Let the reader understand the purpose of you writing. You can also comment on the flow of thejournal report so that the reader can know what to expect. You should avoid copying the introduction given in the lab hand out and instead come up with your own.

Experimental details

This is the part that you need to state every detail of the experiment starting from the equipment that you used to the procedure for the test. This section can be omitted if the report did not involve an experiment at all.

Results and discussions

This is where you are expected to explain the results that you obtained from your experiments. You should give a clear explanation so that the reader cannot ask themselves any question on your results.

The body

The body is the most important part of your journal report because it carries your content. You should introduce small subheadings in your journal report as per the point being put across. This will make your work look more presentable as the reader will be guided with this subheading what point you are talking about.

You can also place your points in number form or list so that it becomes easier for your reader to understand what you are talking about. You should also separate your points to avoid bringing confusion in your work; each point should be under its subtopic.

Conclusions

When it comes to the writing of your conclusion what you need to do is write a summary of the main points in the body of your report and wrap it up. In conclusion, you also need to use words that suggest you are concluding your work to prepare the reader psychologically, that you are about to finish. Remember also that the conclusion should be short and precise avoid a lot of stories in your concluding paragraph, spare all the stories for the body of your report.

Recommendations

The recommendation usually comes after the conclusion. In the recommendation, you are supposed to suggest solutions to the challenges that are there in the body. This is where your opinion is welcomed.

Reference(s):

APA format

- Computer networks, fourth edition, Andrew S.tanenbaurn, Prentice-Hall of India Pvt.Ltd., New Delhi, 2004
- Keiser, G.Local Area Networks. New York, NY:McGraw-Hill,2002.
- Network topology. (2010, February 8). In Wikipedia, The Free Encyclopedia. Retrieved February 9, 2010, from http://en.wikipedia.org/w/index.php?title=Network_topology&oldid=342762416
- https://www.computernetworkingnotes.com/networking-tutorials/differences-between-baseband-and-broadband-explained.html
- Configure Static Internet Protocol (IP) Address Settings on a Cisco IP Phone 6800, 7800, or 8800 Series Multiplatform Phone
- Setting a Static IPv4 Address on a Switch using the Graphical User Interface (GUI)
- Setting Static IPv4 Addesses on a Switch via Command Line Interface (CLI)
- Creating a Text File to Adjust IP Settings on a Switch