

## CHAPTER3: NETWORKING

### 3.1 Introduction

This unit specifies the competencies required to perform computer networking. It involves identification of network types and Components, Connection of networking devices, configuration of network devices, network testing, configuration of network types, perform network security, monitor network connectivity and maintain network.

### 3.2 Performance Standard

- Identified network components during the site survey such as network typology, network components - router, switches, hubs etc.
- Tested the strength and connectivity of cables and equipment
- Identified network types as per the network design
- Installed and configured network software according to user manuals
- Implement the network security policy
- Identified and implemented network security measures
- Identified and deployed monitoring tools

### 3.3 Learning Outcome

#### 3.3.1 List of the Learning Outcomes

These are the key learning outcomes, which make up workplace function:

- Identify network type and components
- Connection network devices
- Configuration of network devices
- Network testing
- Configuration of Network types
- Perform Network security
- Monitor Network connectivity and performance
- Maintain Network

#### 3.3.2 Learning Outcome 1: Identify network type and components

##### 3.3.2.1 Learning Activities

The following are the performance criteria:

- Site survey is conducted to determine the user needs and establish network topology
- Network components are identified according to the site survey
- Network design is developed according to the site survey

Trainees to demonstrate knowledge in relation to:

- Definition of Network
- Definition of network terms

- Network topologies: Star, Ring, Mesh, Hybrid, Point-to-Point
- Network types: WAN, LAN, PAN, MAN
- Components of a network: Switches/Hubs, Routers, Ports, Media, Computers
- Categories of computer network: Peer, Client Server

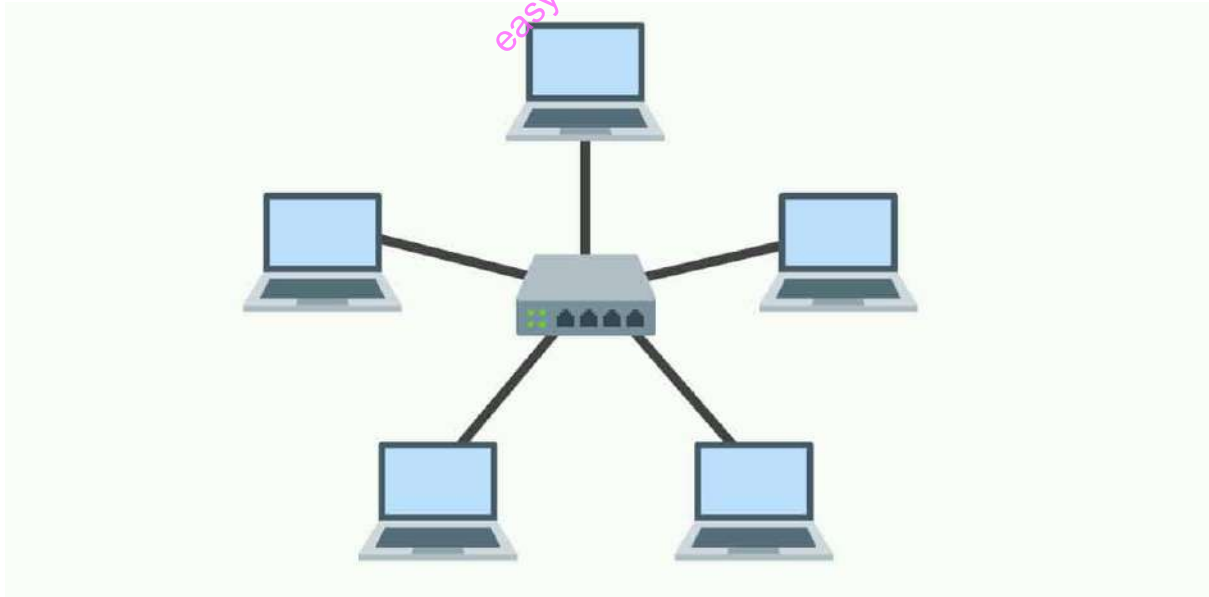
### 3.3.2.2 Information Sheet

A **computer network** is a set of computers connected together for the purpose of sharing resources. The most common resource shared today is connection to the Internet. Other shared resources can include a printer or a file server.

**Watch:** Introduction to different types of networks: <https://youtu.be/svkGASq8mNM>

**Network topology** is the arrangement of the elements (links, nodes, etc.) of a communication network. A wide variety of physical topologies have been used in LANs, including ring, bus, mesh and star. Conversely, mapping the data flow between the components (nodes) determines the logical topology of the network. Following are some of the topologies:

A **star topology** is a topology for a **Local Area Network (LAN)** in which all nodes are individually connected to a central connection point, like a hub or a switch. A star takes more cable than e.g. a bus, but the benefit is that if a cable fails, only one node will be brought down.

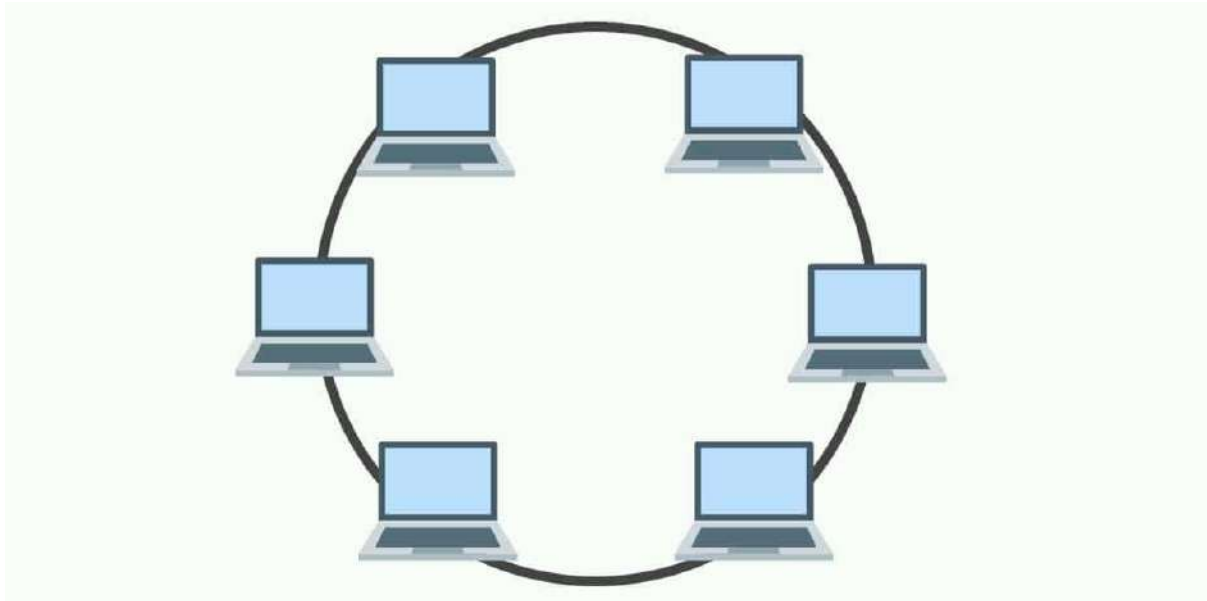


Source: <https://www.comparitech.com/net-admin/network-topologies-advantages-disadvantages/>

**Figure 30: Star topology**

**Watch:** Introduction to star topology: [https://youtu.be/6ogqMji\\_NA](https://youtu.be/6ogqMji_NA)

A **ring network** is a network topology in which each node connects to exactly two other nodes, forming a single continuous pathway for signals through each node - a ring. Data travels from node to node, with each node along the way handling every packet of information between the components.

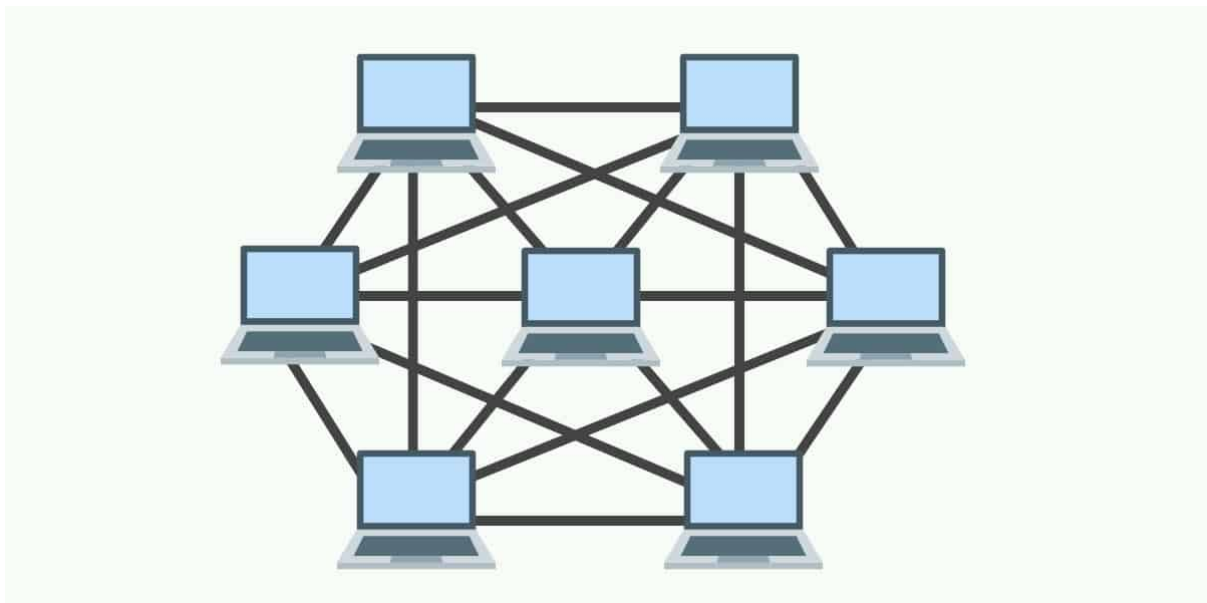


Source: <https://www.comparitech.com/net-admin/network-topologies-advantages-disadvantages/>

**Figure 31: Ring typology**

**Watch:** Introduction to ring network: <https://youtu.be/ZEhN8b50X64>

**Mesh topology** is a type of networking where all nodes cooperate to distribute data amongst each other.

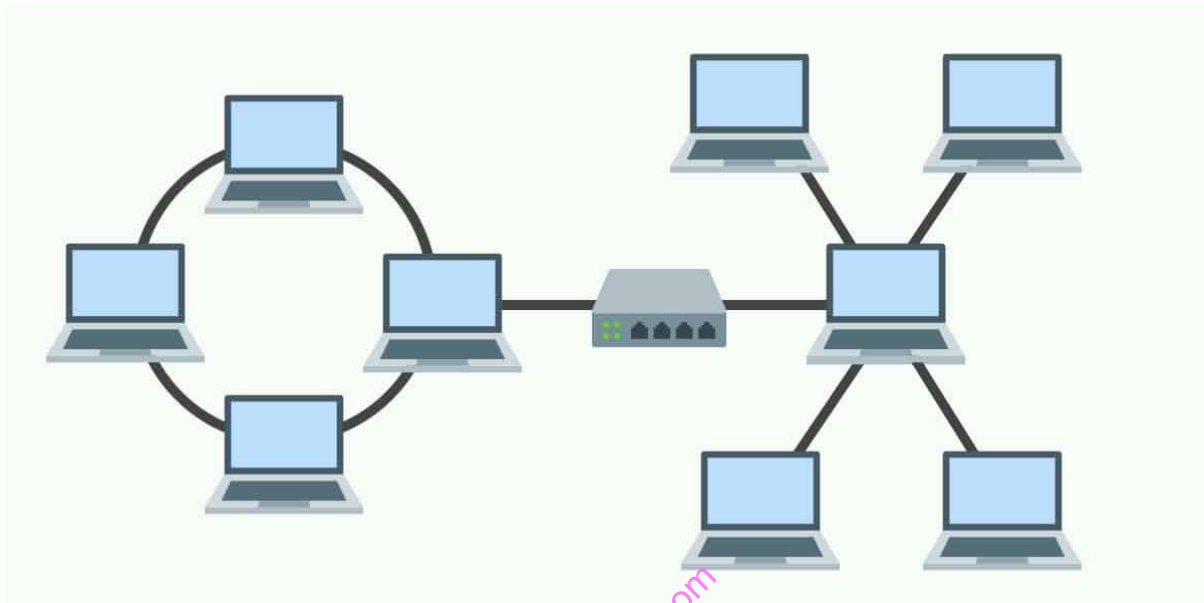


Source: <https://www.comparitech.com/net-admin/network-topologies-advantages-disadvantages/>

**Figure 32: Mesh typology**

**Watch:** Introduction to mesh topology: [https://youtu.be/tYLU755T6\\_I](https://youtu.be/tYLU755T6_I)

A **hybrid topology** is a type of network topology that uses two or more differing network topologies. These topologies include a mix of bus topology; mesh topology, ring topology, star topology, and tree topology.



Source: <https://www.comparitech.com/net-admin/network-topologies-advantages-disadvantages/>

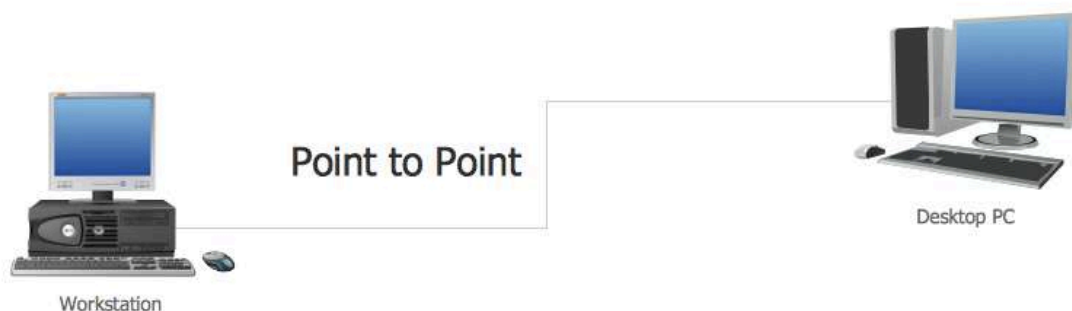
**Figure 33: Hybrid topology**

**Watch:** Introduction to hybrid topology and benefits:

<https://youtu.be/ZAPvScCty8c>

<https://youtu.be/5XtGfcqrZXE>

**Point-to-Point Topology** Point-to-point (PTP) topology connects two nodes directly together.

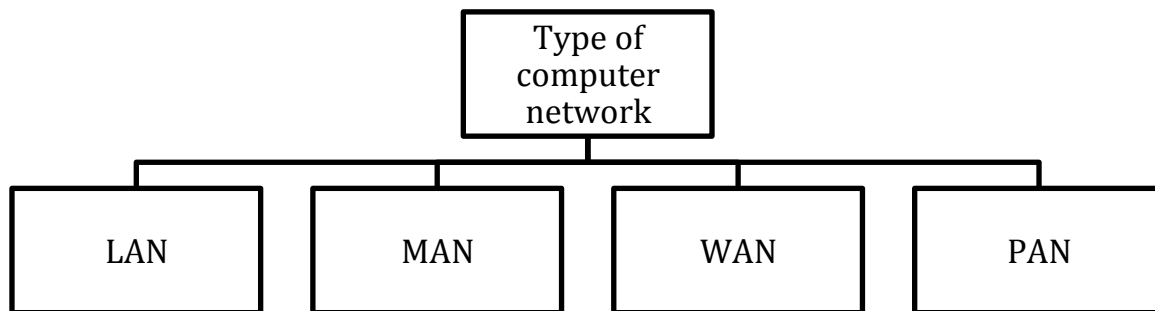


Source: <https://www.conceptdraw.com/How-To-Guide/point-to-point-network-topology>

**Figure 34: Point-to-point topology**

**Watch:** Introduction to point-to-point topology or PTP or P2P: [https://youtu.be/\\_ZnZlale0uI](https://youtu.be/_ZnZlale0uI)

A computer network can be categorized by their size. A **computer network** is mainly of **four types**:



**Figure 35: Classification of network types**

- LAN (Local Area Network)
- PAN (Personal Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network)

**Local Area Network (LAN)** is a group of computers connected to each other in a small area such as building, office. LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc. It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables. The data is transferred at an extremely faster rate in Local Area Network. Local Area Network provides higher security.



Source: <https://www.javatpoint.com>

**Figure 36: LAN**

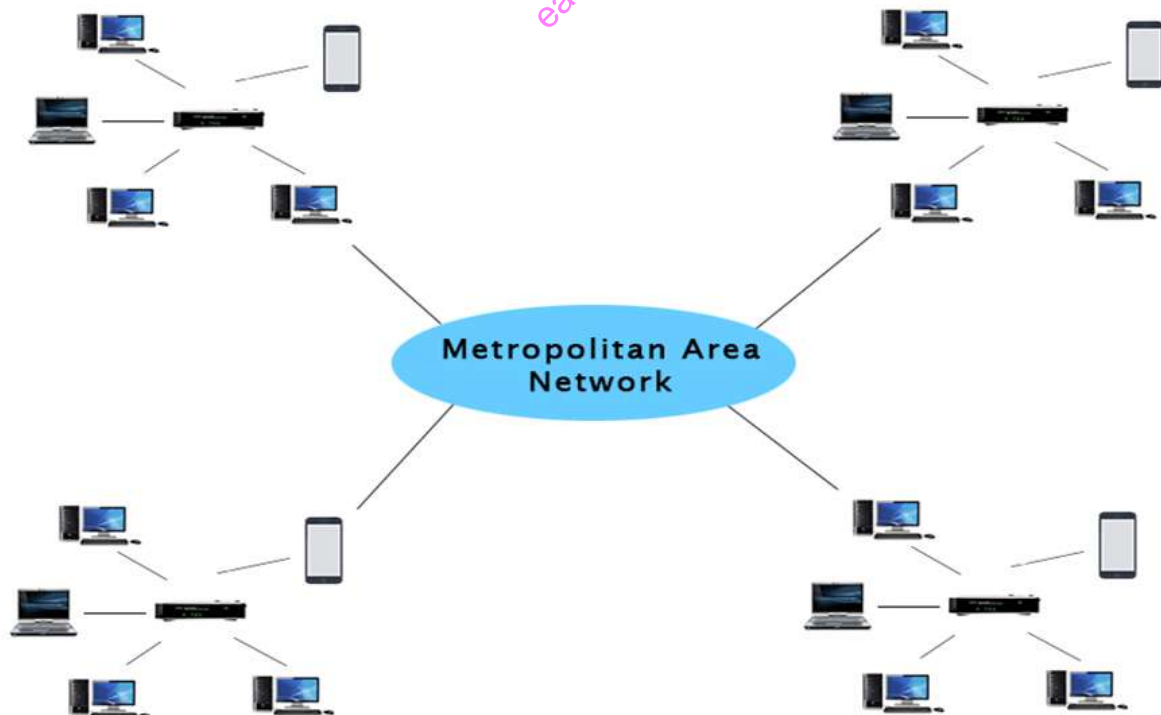
**Personal Area Network (PAN)** is a network arranged within an individual person, typically within a range of 10 meters. Personal Area Network is used for connecting the computer devices of personal use are known as Personal Area Network. **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network. Personal Area Network covers an area of **30 feet**. Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, and media player and play stations.



Source: <https://www.javatpoint.com>

**Figure 37: PAN**

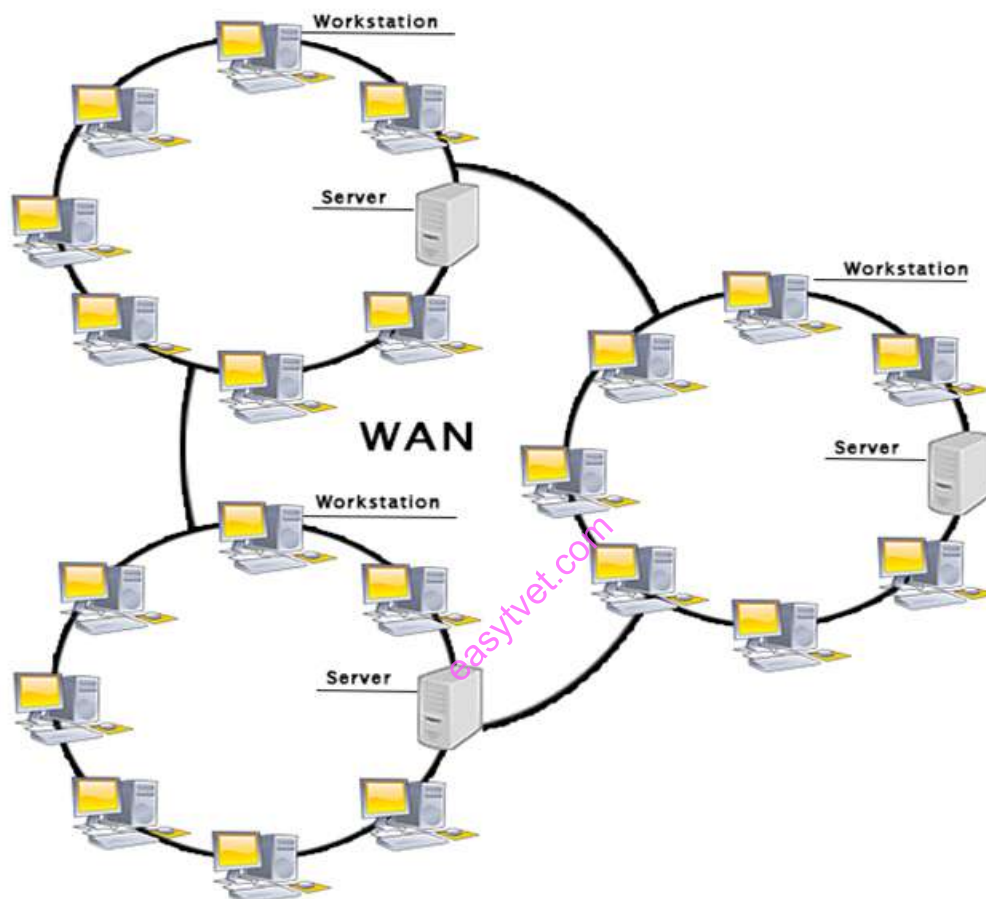
**Metropolitan Area Network (MAN)** is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network. Government agencies use MAN to connect to the citizens and private industries. In MAN, various LANs are connected to each other through a telephone exchange line the most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc. It has a higher range than Local Area Network (LAN).



Source: <https://www.javatpoint.com>

**Figure 38: MAN**

**Wide Area Network (WAN)** is a network that extends over a large geographical area such as states or countries. A Wide Area Network is quite bigger network than the LAN. A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links. The Internet is one of the biggest WAN in the world. A Wide Area Network is widely used in the field of Business, government, and education.



Source: <https://www.javatpoint.com>

**Figure 39: WAN**

**Read:** On different types of networks apart from WAN, PAN, LAN, MAN

<https://www.belden.com/blog/smart-building/11-types-of-networks-explained-vpn-lan-more>

**Computer network components** include the major parts that are needed to install a network both at the office and home level. Before delving into the installation process, you should be familiar with each part so that you could choose and buy the right component that fits with your network system.

**Network media** is the actual path over which an electrical signal travels as it moves from one component to another. A **computer network** is a digital telecommunications network which allows nodes to share resources. In computer networks, computing devices exchange data with each other using connections (data links) between nodes. These data links are

established over cable media such as wires or optic cables, or wireless media such as Wi-Fi.

**Switch** is a telecommunication device grouped as one of computer network components. Switch is like a Hub but built in with advanced features. It uses physical device addresses in each incoming messages so that it can deliver the message to the right destination or port.



Source: <https://www.lambda-tek.com>

**Figure 40: Switch**

**Hub** is a device that splits a network connection into multiple computers. It is like a distribution center. When a computer request information from a network or a specific computer, it sends the request to the hub through a cable. The hub will receive the request and transmit it to the entire network. Each computer in the network should then figure out whether the broadcast data is for them or not.



Source: <http://www.certiology.com>

**Figure 41: Hub**

When we talk about computer network components, the other device that used to connect a LAN with an Internet connection is called **Router**. When you have two distinct networks (LANs) or want to share a single Internet connection to multiple computers, we use a Router.





Source: <https://www.lifewire.com>

**Figure 42: Router**

A **network port** is a number that identifies one side of a connection between two computers. Computers use **port** numbers to determine to which process or application a message should be delivered. As **network** addresses are like street address, **port** numbers are like suite or room numbers.



Source: <https://basri.my>

**Figure 43: Port**

**Network media** is the actual path over which an electrical signal travels as it moves from one component to another. Types of **network media**,

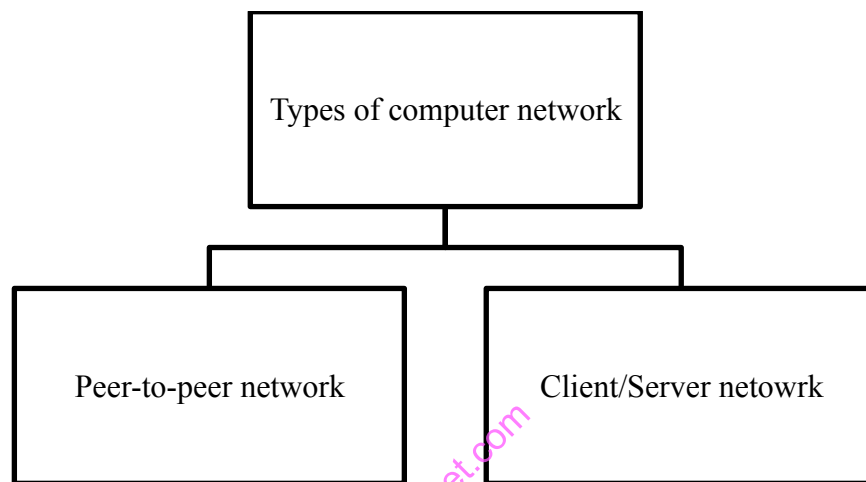
- Twisted-pair cable
- Coaxial cable
- Fiber-optic cable
- Wireless.

**Read:** Basics of network media: <https://www.vskills.in/certification/tutorial/basic-network->

<support/network-media/>

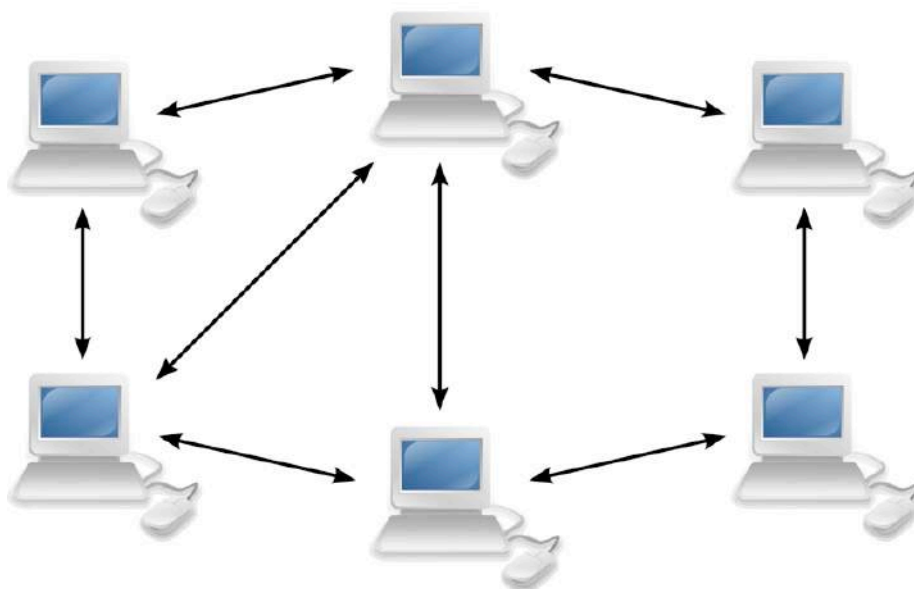
A **computer network** is a set of computers connected together for the purpose of sharing resources. The most common resource shared today is connection to the Internet. Other shared resources can include a printer or a file server. The Internet itself can be considered a computer network.

**Watch:** Introduction to computer network: <https://study.com/academy/lesson/what-is-a-computer-network-types-definition-quiz.html>



**Figure 44: Types of computer network**

**Peer-to-Peer network** is also called Workgroup. In Workgroup there is no dedicated server. All Computers are equal, Every Computers Works Both as a Client and a Server.



Source: <http://www.cyberagentsinc.com>

**Figure 45: Peer-to-peer network**

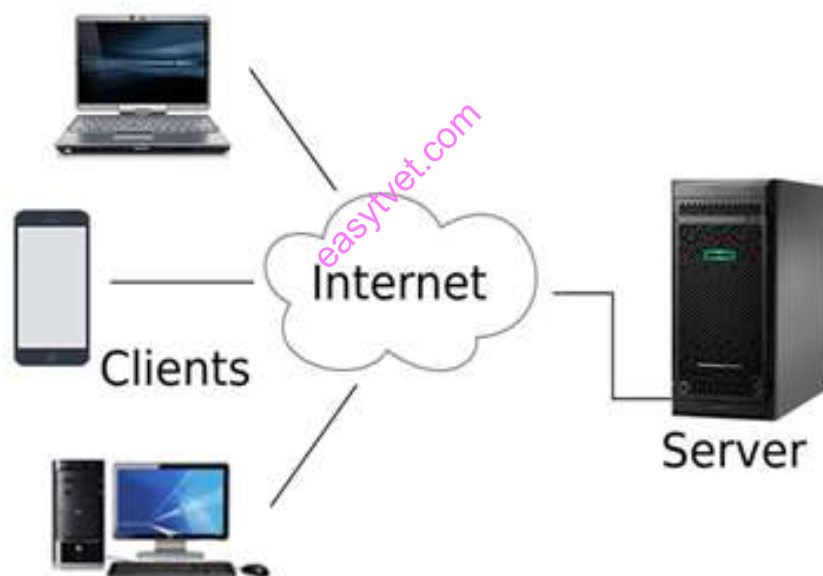
**Read:** Introduction to peer-to-peer network:

<https://www.onlinelms.org/mod/book/view.php?id=43&chapterid=452>

**Watch:** Introduction to peer-to-peer network: <https://youtu.be/wyVEqnDKIC0>

**Watch:** How to Test Network using different tool: <https://youtu.be/7zWswXer8i4>

**Client/Server network** is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server the central controller is known as a server while all other computers in the network are called clients a server performs all the major operations such as security and network management a server is responsible for managing all the resources such as files, directories, printer, etc. All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.



Source: <https://www.javatpoint.com>

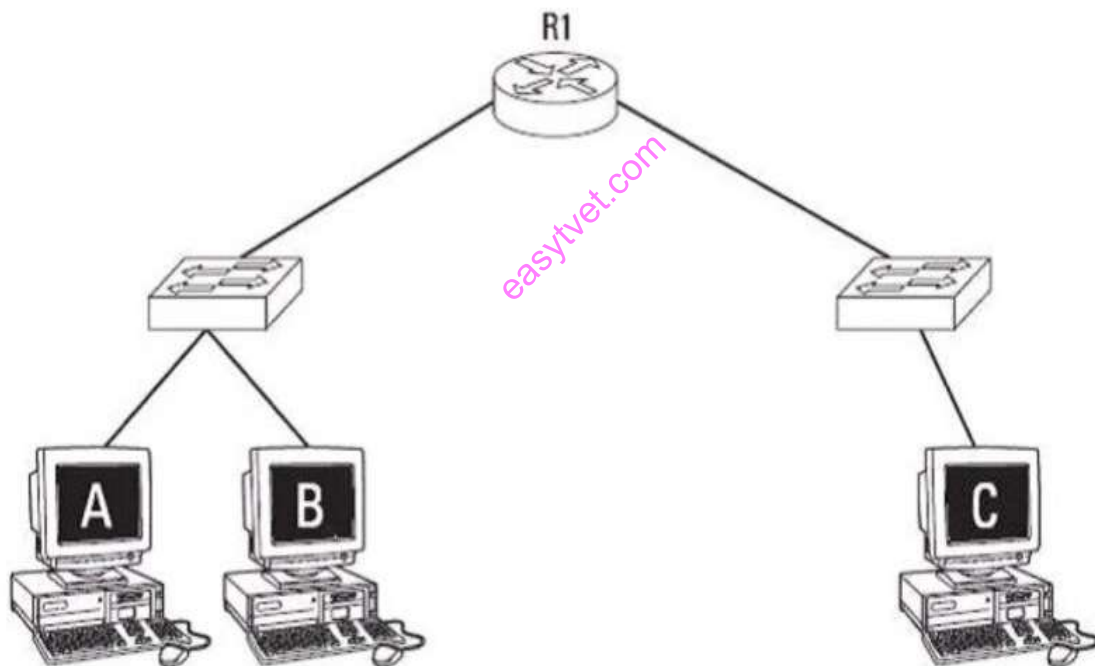
**Figure 46: Client or server network**

**Read:** Computer network architecture: <https://www.javatpoint.com/computer-network-architecture>

### 3.3.2.3 Self-Assessment

- i. What is client/server network?
- ii. Define HUB, SWITCH, ROUTER
- iii. What is a LAN?
- iv. What is the benefit of the Networking?
  - A. File Sharing

- B. Easier access to Resources
  - C. Easier Backups
  - D. All of the Above
- v. Each LAN type has its own strategy in sending of
    - A. Bits
    - B. Bytes
    - C. Data
    - D. Frames
  - vi. Describe star topology. What is the disadvantage of a star topology?
  - vii. What is Hybrid network?
  - viii. What type of network is used for communicating data across states, countries, or the whole world?
  - ix. What is peer-to-peer network?
  - x. Name the different types of network topologies and brief its advantages.
  - xi. Prepare ring topology in packet tracer.
  - xii. How many broadcast domains and collision domains are there in the diagram below?



Source: <https://www.networkbulls.com>

- A. 1 broadcast domain and 5 collision domains
- B. 2 broadcast domain and 5 collision domains
- C. 1 broadcast domain and 5 collision domains
- D. 2 broadcast domain and 5 collision domains

- xiii. You connect a laptop to an available port on a Cisco Catalyst switch. By default, how long does it take that port to start forwarding traffic?
  - A. 0 seconds
  - B. 15 seconds
  - C. 30 seconds
  - D. 50 seconds
- xiv. One of your clients is a Cyber Café owner. He has 10 laptops in a single room. He wants the laptops to be connected with each other and the printer. What will be your recommendation? What are the resources you will need?
- xv. What steps do you take when troubleshooting a networking issue?
- xvi. What are the first things you check when a user is experiencing problems accessing the network?
- xvii. A new switch is bought. What must the network technician do to install the new switch and make it work as a replacement for the failed device? Is this easy or hard to do? Why is it easy or hard?

#### 3.3.2.4 Tools, Equipment, Supplies and Materials

Patch Panels, Network Connectors, Network Testers, A punch down tool, Wiring Systems., Fiber Optic., Network Switches, URL Encode, RJ45, Switches, Computer, Gateway, bridges, antistatic gloves

#### 3.3.2.5 References

- <https://www.javatpoint.com/types-of-computer-network>
- [https://www.all-about-computer-parts.com/computer\\_network\\_components.html](https://www.all-about-computer-parts.com/computer_network_components.html)
- <http://www.pearsonitcertification.com/articles/article.aspx?p=30191>
- <https://www.javatpoint.com/computer-network-architecture>
- Network Topology: Star Network, Grid Network, Tree and Hypertree Networks, Spanning Tree Protocol, Metro Ethernet, Token Ring, Mesh Networking, authored by Books Llc, published by General Books LLC, 2010

### 3.3.3 Learning Outcome 2: Connection network devices

#### 3.3.3.1 Learning Activities

The following are the performance criteria:

- Tools, materials and devices for network are identified according to the network type
- Network connection is done according National and International Communication standards
- Strength and connectivity tests of cables and equipment is done as per the network type

Trainees to demonstrate knowledge in relation to:

- Definition of network devices
- Identification of Network connection Media: Wired, Wireless
- Characteristics of connection medium

- Network devices: Switches/Hubs, Ports, Computers
- Connect network devices

### 3.3.3.2 Information Sheet

**Network devices** are components used to connect computers or other electronic devices together so that they can share files or resources like printers. Devices used to setup a Local Area Network (LAN) are the most common type of network devices used by the public. A LAN requires a hub, switch, and router.

**Read:** Details on computer network devices:

<https://www.slideshare.net/RAJESHSHADHUKHA01/computer-networking-devices-16572482>

A **wired network** is a common type of wired configuration. Most wired networks use Ethernet cables to transfer data between connected PCs. In a small-wired network, a single router may be used to connect all the computers. Larger networks often involve multiple routers or switches that connect to each other.

**Read:** Wired network: <https://andersontech.com/three-critical-reasons-choose-wired-network-small-business/>

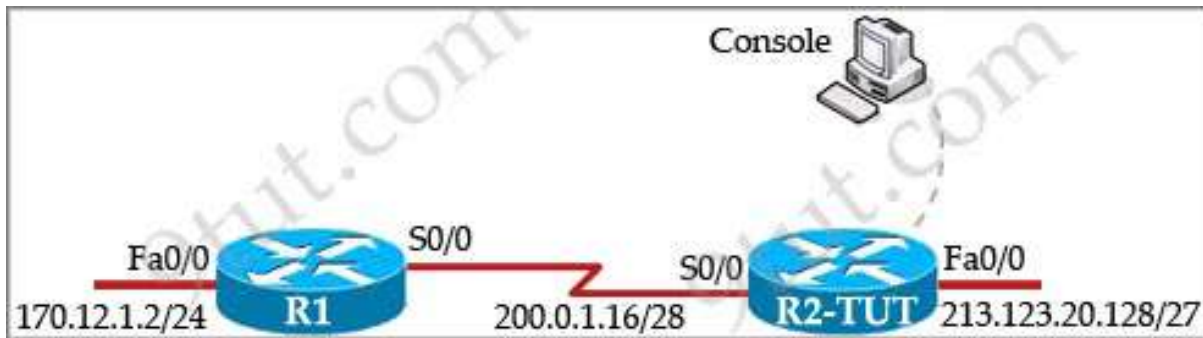
A **wireless network** is a computer network that uses wireless data connections between network nodes. A **medium** is a third-party or element through which a message is communicated.

**Watch:** Introduction of wireless and wired network: <https://youtu.be/u21INH072U>

### 3.3.3.3 Self-Assessment

- i. What are Routers?
- ii. What is the difference between Hub, Switch, and Router?
- iii. How a switch is different from a Hub?
- iv. Configure a new router within your lab.
- v. List the benefits of wired versus wireless network.
- vi. **Case situation:** You are a consultant to a small size hotel. You have been called to check the Internet WIFI network. According to your client, some of their guests are facing challenges with connecting their computer devices to the WIFI. How will you address the situation? What are the steps that you will consider?
- vii. Set up a wireless network for connecting 10 devices in your lab.
- viii. **Case situation:** You are a consultant at a coffee shop for their IT system. Your client is keen on providing their customer free Internet via WIFI. What will be your suggestions? What are the key challenges that you should make your client caution about?

- ix. **Case Study on Network Typology:** TUT Company recently installed a new router in their office. Complete the network installation by performing the initial router configurations and configuring RIPv2 routing using the router command line interface (CLI) on the R2-TUT. Following are the details for your reference.



Source: <https://www.9tut.com/59-ccna-configuration-sim-question/comment-page-5>

Name of the router is **R2-TUT**

Enable-secret password is **cisco1**

The password to access user EXEC mode using the console is **cisco2**

The password to allow telnet access to the router is **cisco3**

IPV4 addresses must be configured as follows:

**Ethernet network 213.123.20.128/27** – router has last assignable host address in subnet

**Serial network is 200.0.1.16/28** – router has last assignable host address in the subnet. Interfaces should be enabled.

Router protocol is **RIPv2**

- x. You need to connect two computers for file sharing. Is it possible to do this without using a hub or router?
- xi. What happens when you use cables longer than the prescribed length?
- xii. You are connecting a cubicle farm to your network. You install NICs in all the workstations and run cables to a workgroup hub. You then connect the MDI port on the workgroup hub to the main hub with a standard patch cable. Upon powering up the cubicle farm computers, none of them can see the servers on the network. What could you replace to solve this problem?
- xii. Briefly explain how wireless-networking systems can avoid collisions where possible?
- xiii. The meaning of straight-through cable is:
- A. Four wire pairs connect to the same pin on each end
  - B. The cable which directly connects computer-to-computer
  - C. Four wire pairs not twisted with each other
  - D. The cable which is not twisted
- xiv. What is the function of a router?
- A. Converting the data from one format to another
  - B. Forward the packet to the up links
  - C. Error detection in data
  - D. None of the above

- xv. What does router do in a network?
- A. Forwards a packet to all outgoing links
  - B. Forwards a packet to the next free outgoing link
  - C. Determines on which outgoing link a packet is to be forwarded
  - D. Forwards a packet to all outgoing links except the originated link
- xvi. Which of the following cables can be used to connect a PC and a Hub?
- A. Rollover cable
  - B. Straight cable
  - C. Cross cable
  - D. Any of the above

#### **3.3.3.4 Tools, Equipment, Supplies and Materials**

Installation and termination, Network and Ethernet cables, Punch down Tools, Wiring Systems, Fiber optic, Network Switches, Network Connectors

#### **3.3.3.5 References**

- <https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/>
- <https://andersontech.com/three-critical-reasons-choose-wired-network-small-business/>
- Cabling Part 1: LAN Networks and Cabling Systems, 5th Edition authored by Andrew Oliviero, published by Sybex, 2015
- Network Design Basics for Cabling Professionals authored by BICSI published by McGraw-Hill Professional; 1 edition

### **3.3.4 Learning Outcome 3: Configuration of network devices**

#### **3.3.4.1 Learning Activities**

The following are the performance criteria:

- Network software is installed and configured according to user manuals.
- IP addressing scheme, subnet masking and routing protocol configuration is done
- Network segmentation is determined as per the network design.
- Network privileges are allocated according to the network configuration.

Trainees to demonstrate knowledge in relation to:

- Definition of configuration
- Network Architecture: OSI, TCP/IP Protocol Suite, Ethernet, Network protocols. TCP/IP, UDP, HTTP, FTP, DCIP, DHCP
- Network Operating system
- Connect and configure network devices

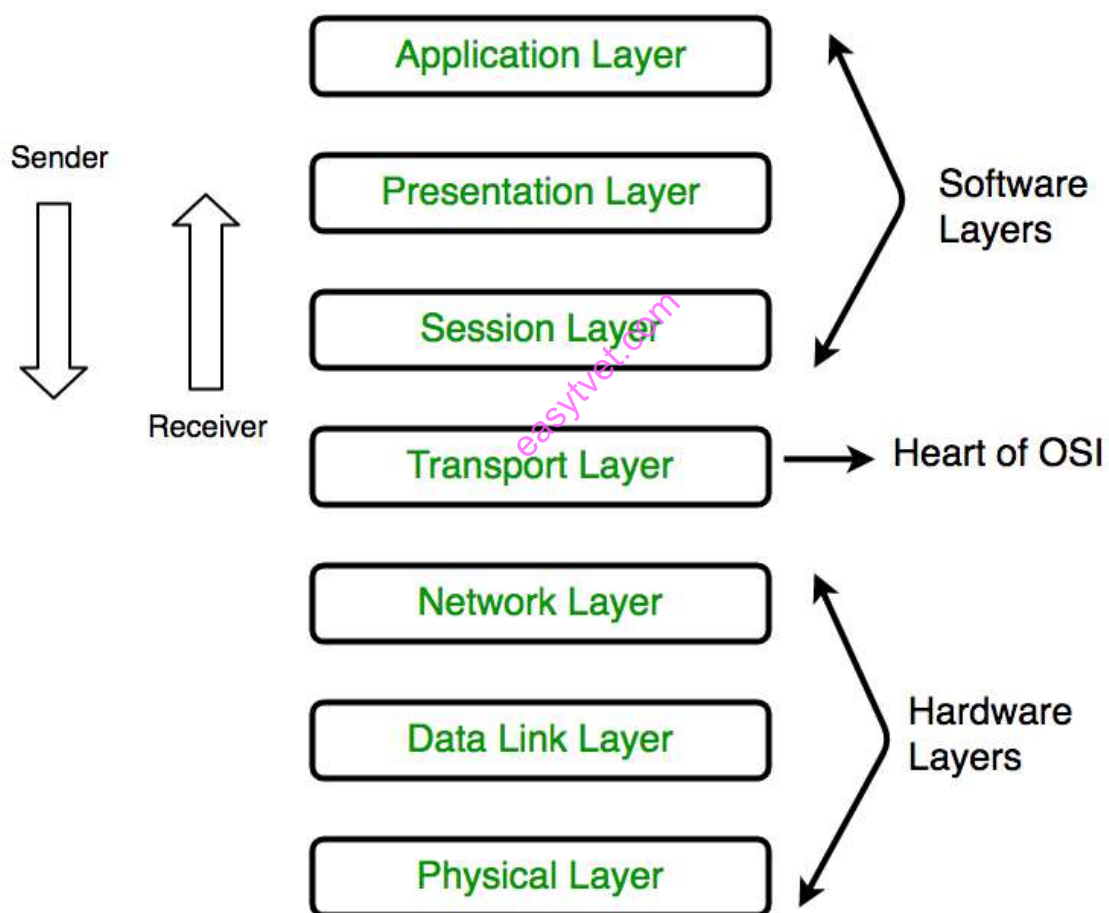


### 3.3.4.2 Information Sheet

**Network configuration** is the process of setting a network's controls, flow and operation to support the network communication of an organization and/or network owner. This broad term incorporates multiple configuration and setup processes on network hardware, software and other supporting devices and components.

**The Open Systems Interconnection model (OSI)** is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology.

**Read:** OSI model: <https://www.geeksforgeeks.org/layers-osi-model/>



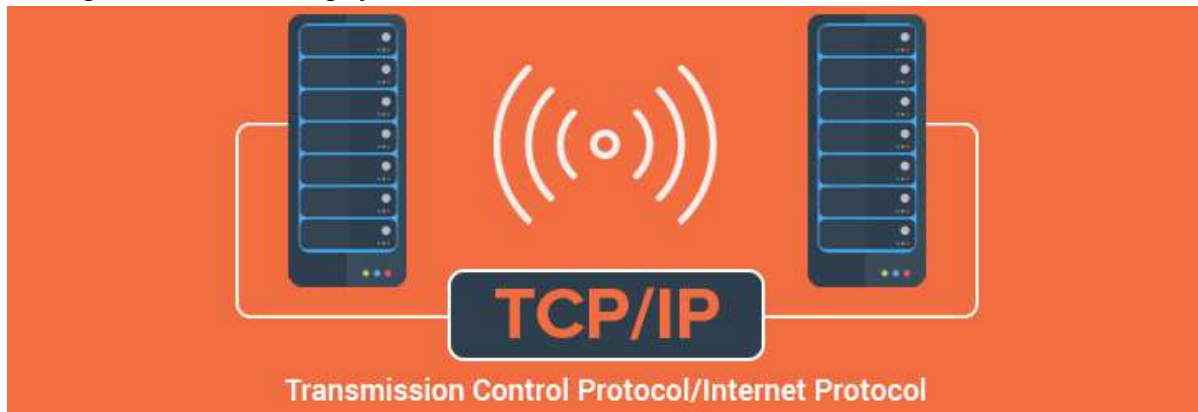
Source: <https://www.geeksforgeeks.org>

**Figure 47: Open Systems Interconnection (OSI) Model**

**The TCP/IP Protocol suite** is a set of protocols used on computer networks today (most notably on the Internet). It provides an end-to-end connectivity by specifying how data should be packetized, addressed, transmitted, routed and received on a TCP/IP network. This functionality is organized into four abstraction layers and each protocol in the suite resides in a particular layer.

**Read:** TCP/IP Protocol suite: <https://study-ccna.com/tcpip-suite-of-protocols/>

**TCP/IP** technically applies to network communications in which the TCP transport is used to deliver data across IP networks. Known as a connection-oriented protocol, TCP works by establishing a virtual connection between two devices via a series of request and reply messages sent across the physical network.



Source: <https://www.iplocation.net>

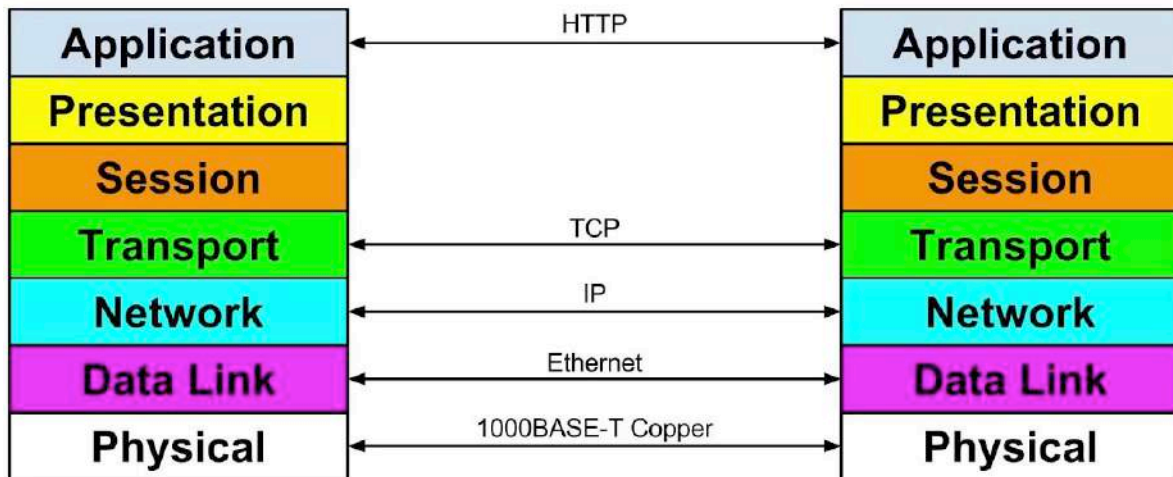
**Figure 48: TCP/IP**

**Read:** TCP/IP: <https://www.lifewire.com/transmission-control-protocol-and-internet-protocol-816255>

**Watch:** TCP/IP explained: [https://youtu.be/PpsEaqJV\\_A0](https://youtu.be/PpsEaqJV_A0)

**Ethernet** is the technology that is most commonly used in wired local area networks (LANs). A LAN is a network of computers and other electronic devices that covers a small area such as a room, office, or building. It is used in contrast to a Wide Area Network (WAN), which spans much larger geographical areas.

**Network protocols** are formal standards and policies made up of rules, procedures and formats that define communication between two or more devices over a network. Network protocols conduct the action, policies, and affairs of the end-to-end process of timely, secured and managed data or network communication.



Source: nikiemurphy.com

**Figure 49: Network protocols**

**Watch:** Network protocols: <https://youtu.be/QrNnRJqTMO8>

**User Datagram Protocol (UDP)** is an alternative communications protocol to **Transmission**

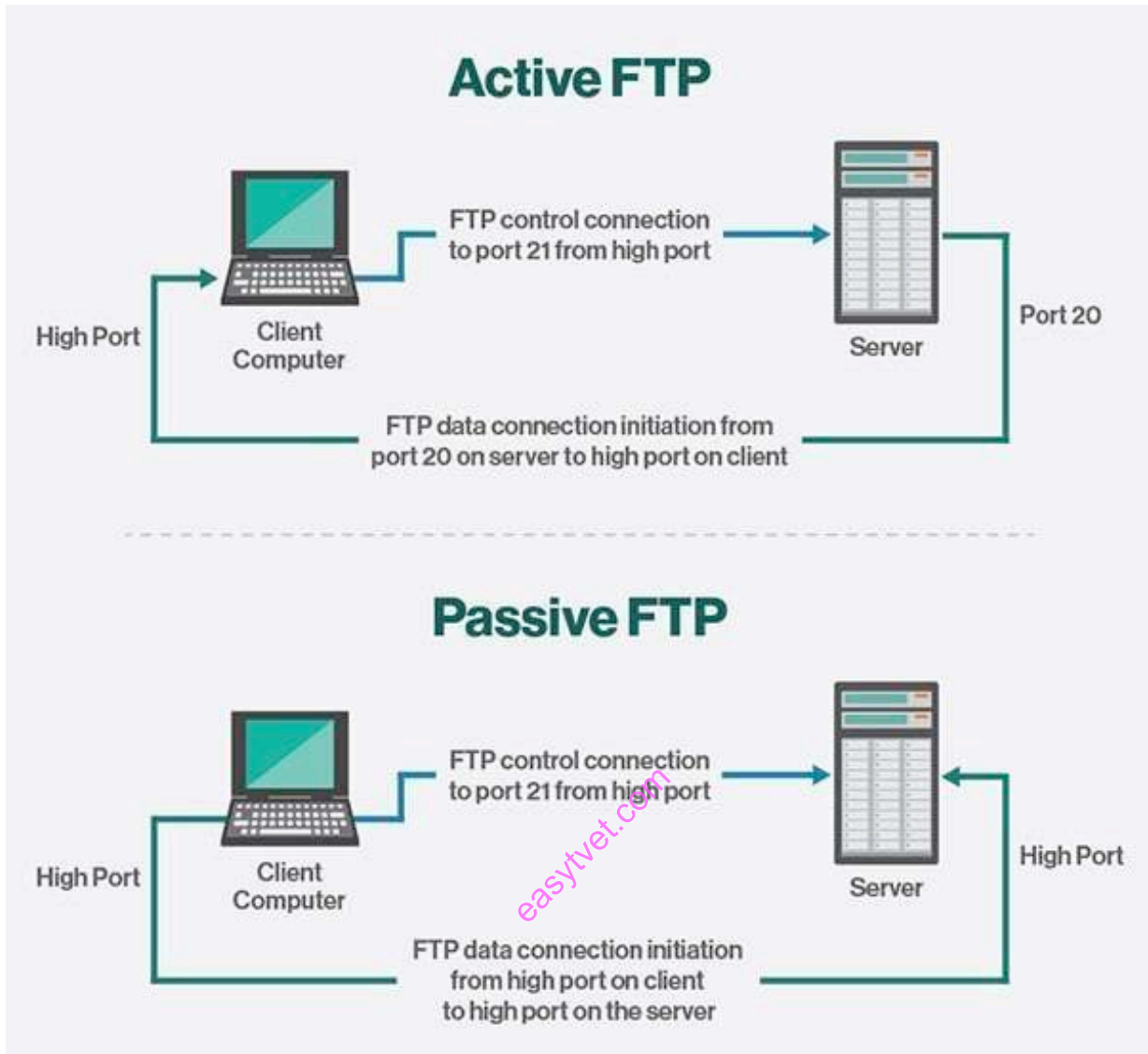
**Control Protocol (TCP)** used primarily for establishing low-latency and loss-tolerating connections between applications on the Internet.

**Watch:** UDP: <https://youtu.be/qIycyyxCnF0>

**File Transfer Protocol (FTP)** is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections.

FTP is a client-server protocol that relies on two communications channels between client and server: a command channel for controlling the conversation and a data channel for transmitting file content. Clients initiate conversations with servers by requesting to download a file. Using FTP, a client can upload, download, delete, rename, move and copy files on a server.

FTP sessions work in passive or active modes. In active mode, after a client initiates a session via a command channel request, the server initiates a data connection back to the client and begins transferring data. In passive mode, the server instead uses the command channel to send the client the information it needs to open a data channel. Because passive mode has the client initiating all connections, it works well across firewalls and Network Address Translation (NAT) gateways.



Source: <https://searchnetworking.techtarget.com>

**Figure 50: Active and passive FTP**

**HTTP** means Hypertext Transfer Protocol. **HTTP** is the underlying protocol used by the World Wide Web and this protocol defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

**Read:** Introduction to HTTP:

<https://www.webopedia.com/TERM/H/HTTP.html>

<https://study-cena.com/http-https/>

[https://www.w3schools.com/whatis/whatis\\_http.asp](https://www.w3schools.com/whatis/whatis_http.asp)

**The Dynamic Host Configuration Protocol** is a network management protocol used on UDP/IP 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.

This entire process is centralized so that TCP/IP configuration can also be completed from a central location. DHCP has “pool of IP addresses” from which it allocates the IP address to the network devices. DHCP cannot recognize if any device is configured manually and assigned with the same IP address from the DHCP pool. In this situation, it throws “IP address conflict” error.

DHCP environment requires DHCP servers to set-up the TCP/IP configuration. These servers then assign, release and renew the IP addresses as there might be a chance that network devices can leave the network and some of them can join back to the network.

**Read:** DHCP: <https://searchnetworking.techtarget.com/definition/DHCP>

**Read:** FTP: <https://searchnetworking.techtarget.com/definition/File-Transfer-Protocol-FTP>

A **Network Operating System (NOS)** is a computer Operating System (OS) that is designed primarily to support workstations, personal computers and, in some instances, older terminals that are connected on a local area network (LAN).

**Watch:** Network operating system: <https://youtu.be/41FKxGn99HA>

**Read:** Network operating system:  
<https://searchnetworking.techtarget.com/definition/network-operating-system>

**Watch:** Configuration of network: [https://youtu.be/2W\\_X49G-3qc](https://youtu.be/2W_X49G-3qc)

### 3.3.4.3 Self-Assessment

- i. Describe the layers of OSI model?
- ii. Explain TCP/IP Model
- iii. What is HTTP and what port does it use?
- iv. What are TCP and UDP?
- v. Explain DHCP briefly?
- vi. Expand DHCP and describe how it works?
- vii. Network Layer is in OSI's:
  - A. 7th layer
  - B. 4th Layer
  - C. 1st layer
  - D. 3rd Layer
- viii. What does UDP provide in OSI model?
  - A. It provide data segmentation
  - B. It secure the data
  - C. It is connection less protocol
  - D. It is a layer 3 protocol
- ix. You are IT support engineer, your IT manager wants you to Telnet R7 which is in LA, Which is the highest layer used to get access to LA's router from Telnet?

- A. Layer 7
  - B. Layer 1
  - C. Layer 4
  - D. Layer 5
- x. The physical layer translates logical communication requests from the \_\_\_\_\_ into hardware-specific operations.
- A. Data link layer
  - B. Network layer
  - C. Transport layer
  - D. Application layer
- xi. Which software troubleshooting tool could you use to determine which protocol is configured with the wrong address?
- xii. Which TCP/IP utility is most often used to test whether an IP host is up and functional?
- xiii. What protocol can be applied when you want to transfer files between different platforms, such between Unix systems and windows servers?

#### 3.3.4.4 Tools, Equipment, Supplies and Materials

TeemIP: Easy IP Address Management, Node-RED: Wiring Nodes to Solve Anything, Speedtest.net/pingtest.net, Subnet and IP Calculator, PuTTY/Tera Term, Netstat, Nslookup, Ipconfig/ifconfig, Tracert/traceroute, Ping

#### 3.3.4.5 References

- <https://www.webopedia.com/TERM/H/HTTP.html>
- <https://study-ccna.com/http-https/>
- [https://www.w3schools.com/whatis/whatis\\_http.asp](https://www.w3schools.com/whatis/whatis_http.asp)
- The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference, authored by Charles M. Kozierok, published by No Starch Press; 1<sup>st</sup> edition
- Elements of Network Protocol Design, authored by Mohamed G. Gouda published by Wiley-Interscience; 1<sup>st</sup> edition

### 3.3.5 Learning Outcome 4: Network testing

#### 3.3.5.1 Learning Activities

The following are the performance criteria:

- Network components are tested to determine the performance.
- Testing of connectivity medium between components is done as per the manual instructions.
- Network testing is done, and report generated.

Trainees to demonstrate knowledge in relation to:

- Outline network test plan
- Network testing tools: Clamp meter, Voltmeter, Cable tester, Signal tester
- Test network components
- Test the network
- Test report

#### 3.3.5.2 Information Sheet

A **test plan** is a detailed document that outlines the test strategy, Testing objectives, resources (manpower, software, hardware) required for testing, test schedule, Test Estimation and test deliverables. A **clamp meter** is an electrical test tool that combines a basic digital millimeter with a current sensor.



Source: <https://www.flukenetworks.com>

**Figure 51: Clamp meter**

A **voltmeter** is an instrument used for measuring electrical potential difference between two points in an electric circuit. Analog voltmeters move a pointer across a scale in proportion to the voltage of the circuit; digital voltmeters give a numerical display of voltage by use of an analog to digital converter.

A **cable tester** is an electronic device used to verify the electrical connections in a signal cable or other wired assembly.

**Watch:** How to network cable tester work: <https://youtu.be/sQ5V3cHIISk>

**The Signal Tester** will provide a summary of all networks found and their absolute and relative strengths. The information is shown directly on the LCD screen.



Source: <https://www.4grouter.co.uk>

**Figure 52: Signal tester**

**A network performance test** is any process that is used to quantitatively or qualitatively measures the performance of a computer network. It tests for and records certain behaviors and processes of networks that, when combined, define the network performance and/or quality of service.

**Testing the network include:**

- Identify the testing environment
- Identify performance metrics
- Plan and design performance tests
- Configure the test environment
- Implement test design
- Execute tests
- Analyze, report, retest

**Watch:** Testing Network: <https://youtu.be/i5cGw6vokW8>

**3.3.5.3 Self-Assessment**

- i. What is cable tester?
- ii. How to measure your network signal?
- iii. What is the role of clamp meter?
- iv. Differentiate clamp meter and voltmeter?
- v. Which device we use to test network signal?
  - A. Clamp meter



- B. Voltmeter
- C. Signal Tester
- D. None of them
- v. Voltmeter measures?
  - A. Electrical current
  - B. Network speed
  - C. Signal
  - D. None above all
- vi. How fast is 10baseT?
  - A. 100Mbps
  - B. 30Mbps
  - C. 10Mbps
  - D. 2Mbps
  - E. 1000Mbps
- vii. How fast can data travel over Cat3 UTP?
  - A. 200Mbps
  - B. 100Mbps
  - C. 10Mbps
  - D. 2Mbps
  - E. 1.5Mbps

#### **3.3.5.4 Tools, Equipment, Supplies and Materials**

Cable test, Voltmeter, Clamp meter, Signal tester

#### **3.3.5.5 References**

- <https://www.techopedia.com/definition/29991/network-performance-test>
- The Art of Testing Network Systems, authored by Robert W. Buchanan published by Wiley; 1 edition 1996
- Enterprise Network Testing: Testing Throughout the Network Lifecycle to Maximize Availability and Performance Networking Technology, authored by Tom Kunath, Andy Sholom, published by Cisco Press; 1 edition 2011

### 3.3.6 Learning Outcome 5: Configuration of Network types

#### 3.3.6.1 Learning Activities

The following are the performance criteria:

- Network types are identified as per the
- Network design Network types are configured as per the type of connection
- Network testing of network types is done

Trainees to demonstrate knowledge in relation to:

- Determine appropriate Network type
- Types of Network types
- Assemble prerequisite components and medium
- Network Components Configuration procedures
- Network protocols Configuration procedures

#### 3.3.6.2 Information Sheet

**Network configuration** is the process of setting a network's controls, flow and operation to support the network communication of an organization and/or network owner. This broad term incorporates multiple configuration and setup processes on network hardware, software and other supporting devices and components.

**Watch:** Network Component configuration: <https://youtu.be/gVrXLq5E-CQ>

**Network configurations procedures** take place along with the installation of the operating system software. At that time, certain IP configuration parameters must be stored in appropriate files so they can be read at boot time.

The procedure is a matter of creating or editing the network configuration files. How configuration information is made available to a machine's kernel depends on whether these files are stored locally (local files mode) or acquired from the network configuration server (network client mode).

Parameters supplied during network configuration are:

- IP address of each network interface on every machine
- Host names of each machine on the network. You can type the host name in a local file or a name service database.
- NIS, NIS+, or DNS domain name in which the machine resides, if applicable
- Default router addresses. You supply this only if you have a simple network topology with only one router attached to each network, or your routers don't run routing protocols such as the Router Discovery Server Protocol (RDISC) or the Router Information Protocol (RIP).
- Subnet mask (required only for networks with subnets)

### 3.3.6.3 Self-Assessment

- i. Define network configuration
- ii. Which parameter used during network configuration?
- iii. Conduct performance test in your lab.
- iv. **Case situation:** You are asked to visit a near-by high school and test their ICT lab. They are facing lot of challenges with their computer lab. What are the steps you will consider for diagnosis of their challenges?
- v. \_\_\_\_\_ is the process of setting a network control.
  - A. Network configuration
  - B. Network management
  - C. Network styling
  - D. Network wiring

### 3.3.6.4 Tools, Equipment, Supplies and Materials

Computer, cables, switch, hubs, router

### 3.3.6.5 References

- <https://youtu.be/gVrXLq5E-CQ>
- <https://www.techopedia.com/definition/25766/network-configuration>
- Computer Networking: Top-Down authored by Kurose, Ross, published by Pearson 2013

### 3.3.7 Learning Outcome 6: Perform network security

#### 3.3.7.1 Learning Activities

The following are the performance criteria:

- Identification and implementation of network security policy is done as per the Organization ICT policy.
- Network security measures are identified according to the threats defined.
- Network security measures are enforced in line with the Network security policy.

Trainees to demonstrate knowledge in relation to:

- Definition of network security
- Network threats: Internal and External
- Prevention measures: Firewalls, User accounts control, Security policies, Anti-viruses, Encryption
- Enforce network security measures
- Network Security Policy

#### 3.3.7.2 Information Sheet

**Network Security** is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure

platform for computers, users and programs to perform their permitted critical functions within a secure environment.

**Internal Threat** a threat originating inside a company, government agency, or institution, and typically an exploit by a disgruntled employee denied promotion or informed of employment termination.

**External threats** are malicious campaigns and threat actors that attempt to exploit security exposures in your attack surface that exist outside the firewall. All organizations with a digital presence are exposed to external threats by attackers who attempt to impersonate your brand and official communications channels on the internet, social media, and through mobile apps.

A **firewall** is software used to maintain the security of a private network. Firewalls block unauthorized access to or from private networks and are often employed to prevent unauthorized Web users or illicit software from gaining access to private networks connected to the Internet. A firewall may be implemented using hardware, software, or a combination of both.

**Watch:** How Firewall work: <https://youtu.be/KZc1KaE1OKU>

**User Account Control or UAC** for short is a security feature of Windows which helps prevent unauthorized changes to the operating system. Applications, users, viruses or other forms of malware can initiate these changes.

**Security policy** is a definition of what it means to be secure for a system, organization or other entity. For an organization, it addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls.

**Antivirus software**, or **anti-virus** software (abbreviated to AV software), also known as **anti-malware**, is a computer program used to prevent, detect, and remove malware.

**Encryption** is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.

A **network security policy**, or NSP, is a generic document that outlines rules for computer **network** access, determines how **policies** are enforced and lays out some of the basic architecture of the company **security/ network security** environment.

### 3.3.7.3 Self-Assessment

- i. Define antivirus?
- ii. What is the difference between antivirus and firewall?
- iii. What is firewall?

- iv. Differentiate internal threads and external threads?
- v. What is Network Security?
- vi. Which way to prevent unauthorized user to change the operating system?
  - A. Firewall
  - B. User account control
  - C. Encryption
- vii. **Case situation:** You have been hired by a pharmaceutical office. The manager of the sales team has asked you to ensure that none of the computers have access to any social media or entertainment sites on the Internet. What will be your approach to address the manager's request?
- viii. Review the different anti-viruses available and make a table on advantages and disadvantages.
- ix. **Case situation:** You are visiting a Cyber Café and you see that the anti-virus package is pirated. What will you consider doing?

#### **3.3.7.4 Tools, Equipment, Supplies and Materials**

Antivirus software, Computer

#### **3.3.7.5 References**

- <https://www.riskiq.com/products/external-threats/>
- Network Security authored by Jan L. Harrington, published by Elsevier Science & Technology

### **3.3.8 Learning Outcome 7: Monitor Network connectivity and performance**

#### **3.3.8.1 Learning Activities**

The following are the performance criteria:

- Monitoring tools are identified
- Deployment of monitoring tools is done as per the network connection type.
- Network status is determined as per the monitoring report.

Trainees to demonstrate knowledge in relation to:

- Monitoring tools and software: Ping, Tracert, NSLookup, Ipconfig, Speed test

#### **3.3.8.2 Information Sheet**

**Monitoring software** observes and tracks the operations and activities of users, applications and network services on a computer or enterprise systems. This type of software provides a way to supervise the overall processes that are performed on a computing system, and provides reporting services to the system or network administrator.

**Ping** is a computer network administration software utility used to test the reachability of a host on an Internet Protocol network. It is available for virtually all operating systems that have networking capability, including most embedded network administration software.

**Read:** Introduction to ping: <https://techterms.com/definition/ping>

**Watch:** How to ping: <https://youtu.be/A2nkwZh8hws>

Traceroute (or **tracert** on Microsoft Windows systems) displays information about each “hop” a packet takes from your computer to the remote host. It is often a good way to pinpoint possible ISP connection issues or network bottlenecks.

**Watch:** How traceroute work: [https://youtu.be/x\\_3dWSQkHB8](https://youtu.be/x_3dWSQkHB8)

The **nslookup** command will look up the IP addresses associated with a domain name.

**Watch:** How nslookup work: <https://youtu.be/mx8RP-XsEKw>

An **internet speed** test is a website or web application that measures a user's internet connection speed. It reports on: Upload speed and download speed.

### 3.3.8.3 Self-Assessment

- i. What is ping command and what are its uses?
- ii. Why is it necessary to test the speed of your Internet?
- iii. Explain briefly computer monitoring?
- iv. What are ipconfig and ifconfig?
- v. Differentiate between ping and tracert.
- vi. You need to troubleshoot your network IP connectivity. Which of the following commands would you use to find the IP address on your Ethernet 0 interface?
  - A. Ping
  - B. IPConfig
  - C. traceroute
  - D. Show interface Ethernet 0
- vii. We can use ping program to find, if a host is:
  - A. Alive
  - B. Dead
  - C. Responding
  - D. Both A and C
- viii. \_\_\_\_\_ command is used to manipulate TCP/IP routing table.
  - A. route
  - B. Ipconfig
  - C. Ifconfig
  - D. Traceroute
- ix. Ping can:

- A. Measure round-trip time
- B. Report packet loss
- C. Report latency
- D. All of the mentioned

### 3.3.8.4 Tools, Equipment, Supplies and Materials

Speed test, Computer, GUI, Software

### 3.3.8.5 References

- <https://techterms.com/definition/ping>
- <https://youtu.be/mx8RP-XsEKw>
- [https://youtu.be/x\\_3dWSQkHB8](https://youtu.be/x_3dWSQkHB8)
- Computer Networking: Top-Down authored by Kurose, Ross, published by Pearson 2013

## 3.3.9 Learning Outcome 8: Maintain Network

### 3.3.9.1 Learning Activities

The following are the performance criteria:

- Optimization between the network components and medium is done
- Network security is applied according to vulnerability of the network
- Maintenance schedule is performed
- User training is done according to the instruction manual

Trainees to demonstrate knowledge in relation to:

- Maintenance schedule plan
- Maintenance tools: Console, Wireshark, Nmap
- Corrective/preventive measures

### 3.3.9.2 Information Sheet

**Maintenance planning and scheduling includes** planning decisions related to what, how and time estimate for a job.

There are different types of maintenance tools for network. **Console** is the combination of display monitor and keyboard (or other device that allows input). Another term for console is terminal. The term console usually refers to a terminal attached to a minicomputer or mainframe and used to monitor the status of the system.

**Read:** Introduction to console: <https://www.webopedia.com/TERM/C/console.html>

**Wireshark** is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was later renamed to Wireshark.

**Read:** About Wireshark: <https://en.wikipedia.org/wiki/Wireshark>

**Watch:** How to analyze IP using wireshark: <https://youtu.be/S92h5Q4svds>

**Network Mapper (Nmap)** is a free and open-source network scanner created by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich). **Nmap** is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

**Read:** Introduction and use of Nmap in networks:

<https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html>

### 3.3.9.3 Self-Assessment

- i. What is Nmap?
- ii. Explain wireshark.
- iii. What is console?
- iv. In the virtual LAN of your lab, how many hosts are running? Please list their IP addresses. You should consider the router in all this and following questions, remember the router has different interfaces on different subnets.
  - A. If a computer is up, which services (TCP and UDP) are open on it?
  - B. Can you determine the Operating system and its possible version that is running on each alive computer?
  - C. All the answers should be included in a file named /tmp/nmap,
- v. Nmap was originally a command-line application for Unix, but a Windows version has been available since
  - A. 2005
  - B. 2008
  - C. 2019
  - D. 2000
- vi. Wireshark is free \_\_\_\_\_ Analyzer?
  - A. Console
  - B. Network
  - C. Packet
  - D. B and C

### 3.3.9.4 Tools, Equipment, Supplies and Materials

Computer, software, Graphic user interface (GUI)

### 3.3.9.5 References

- <https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html>
- Computer Networking: Top-Down authored by Kurose, Ross, published by Pearson 2013