CHAPTER 2: COMPUTER NETWORKING

Unit of learning code: IT/CU/ICT/CR/1/5

Related Unit of Competency in Occupational Standard: Perform Computer Networking

2.1 Introduction to the unit of learning

This unit specifies the competencies required to perform computer Networking. It involves Identification of network types, Connection of networking devices, configuration of network devices, network testing, configuration of LAN network type and monitoring network connectivity.

2.2 Summary of Learning Outcomes

1. Identify network type and components
2. Connect network devices
3. Configure network devices
4. Configure LAN Network type
5. Perform Network testing

2.2.1 Learning Outcome 1: Identify Network Type and Components

2.2.1.2 Introduction to the Learning Outcome

This learning outcome covers identification of different types of computer networks, identification of Network components, identification of network topologies, identification of transmission media and benefits of computer networking.

2.2.1.3 Performance Standard

2.2.1.3.1 Types of computer networks are identified.

2.2.1.3.2 Network components are identified

2.2.1.3.3 Network topologies are identified.

2.2.1.3.4 Transmission media is identified.

2.2.1.3.5 Benefits of computer Networking are identified.

2.2.1.4 Information Sheet

a) Definition of Computer Network

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications. 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.

b) Key terms in Computer Networks

Table 24: Common terms in Networking

Terms	Definition
1. ISO	The OSI model is a product of the Open Systems Interconnection project at the International Organization for Standardization. ISO is a voluntary organization.
2. OSI Model	Open System Interconnection is a model consisting of seven logical layers.
3. TCP/IP Model	Transmission Control Protocol and Internet Protocol Model is based on four layer model which is based on Protocols.
4. UTP	Unshielded Twisted Pair cable is a Wired/Guided media which consists of two conductors usually copper, each with its own colour plastic insulator
5. STP	Shielded Twisted Pair cable is a Wired/Guided media has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Shielding also eliminates crosstalk
6. PPP	Point-to-Point connection is a protocol which is used as a communication link between two devices.
7. LAN	Local Area Network is designed for small areas such as an office, group of building or a factory.
8. WAN	Wide Area Network is used for the network that covers large distance such as cover states of a country
9. MAN	Metropolitan Area Network uses the similar technology as LAN.

It is designed to extend over the entire city.

10. Crosstalk

Undesired effect of one circuit on another circuit. It can occur when one line picks up some signals travelling down another line. Example: telephone conversation when one can hear background conversations. It can be eliminated by shielding each pair of twisted pair cable.

11. PSTN

Public Switched Telephone Network consists of telephone lines, cellular networks, satellites for communication, fiber optic cables etc. It is the combination of world's (national, local and regional) circuit switched telephone network.

12. File Transfer, Access and Management (FTAM)

Standard mechanism to access files and manages it. Users can access files in a remote computer and manage it.

13. Analog Transmission

The signal is continuously variable in amplitude and frequency. Power requirement is high when compared with Digital Transmission.

14. Digital Transmission

It is a sequence of voltage pulses. It is basically a series of discrete pulses. Security is better than Analog Transmission.

15. Asymmetric digital subscriber line(ADSL)

A data communications technology that enables faster data transmission over copper telephone lines than a conventional voice band modem can provide.

16. Access Point

Alternatively referred to as a base station and wireless router, an access point is a wireless receiver which enables a user to connect wirelessly to a network or the Internet. This term can refer to both Wi-Fi and Bluetooth devices.

17. Acknowledgement (ACK)

Short for acknowledgement, ACK is an answer given by another computer or network device indicating to another computer that it acknowledged the SYN/ACK or other request sent to it. **Note:** If the signal is not properly received an NAK is sent.

18. Active Topology

The term active topology describes a network topology in which the signal is amplified at each step as it passes from one computer to the next.

19. Aloha — Protocol for satellite and terrestrial radio transmissions. In pure Aloha, a user can communicate at any time, but risks collisions with other users' messages. Slotted Aloha reduces the chance of collisions by dividing the channel into time slots and requiring that the user send only at the beginning of a time slot.

20. Address Resolution Protocol(ARP) — ARP is a used with the IP for mapping a 32-bit Internet Protocol address to a MAC address that is recognized in the local network specified in RFC 826.

c) Network Topologies

A network topology is the arrangement of computer devices in computer network to establish communication among them. It defines a layout of a network that means it determines how different nodes are connected and communicated together within a network.

Network topology can be according to logical aspect or on physical aspect. Physical topology describes placement of different components of the network while logical topology describes the data flow within a network instead of physical design.

Physical and Logical Topology

There are two approaches to network topology: physical and logical. Physical network topology, as the name suggests, refers to the physical connections and interconnections between nodes and the network—the wires, cables, and so forth. Logical network topology is a little more abstract and strategic, referring to the conceptual understanding of how and why the network is arranged the way it is, and how data moves through it.

Network topology can be categorize in 2 main categories on the basis of connection: Point to point and multi point.

Point to point topology

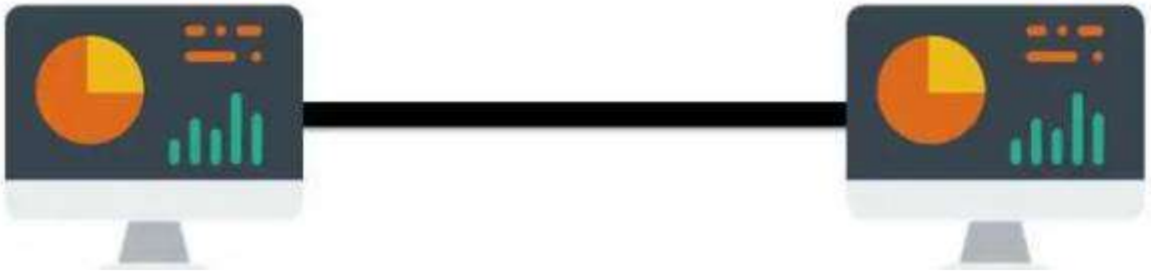


Figure 29: Point to point Topology

Point to Point topology is the simplest topology that connects two nodes directly together with a common link. The entire bandwidth of the common link is reserved for transmission between those two nodes. The point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as satellite links, or microwaves are also possible.

Multipoint: This is a case where more than two specific devices share a single link.

i. Types of Topology

There are five types of topology in computer networks. Hybrid topology is also common

- Star
- Bus
- Ring
- Tree
- Mesh
- Hybrid

1. Star Topology

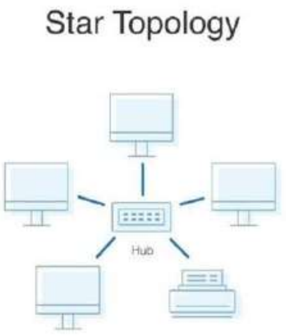


Figure 29 Star topology

A star topology, the most common network topology, is laid out so every node in the network is directly connected to one central hub via coaxial, twisted-pair, or fiber-optic cable. Acting as a server, this central node manages data transmission—as information sent from any node on the network has to pass through the central one to reach its destination—and functions as a repeater, which helps prevent data loss.

Advantages of Star Topology

Star topologies are common since they allow you to conveniently manage your entire network from a single location. Because each of the nodes is independently connected to the central hub, should one go down, the rest of the network will continue functioning unaffected, making the star topology a stable and secure network layout.

Additionally, devices can be added, removed, and modified without taking the entire network offline.

On the physical side of things, the structure of the star topology uses relatively little cabling to fully connect the network, which allows for both straightforward setup and management over time as the network expands or contracts. The simplicity of the network design makes life easier for administrators, too, because it’s easy to identify where errors or performance issues are occurring.

Disadvantages of Star Topology

On the flipside, if the central hub goes down, the rest of the network can't function. But if the central hub is properly managed and kept in good health, administrators shouldn't have too many issues.

The overall bandwidth and performance of the network are also limited by the central node's configurations and technical specifications, making star topologies expensive to set up and operate.

2. Bus Topology

A bus topology orients all the devices on a network along a single cable running in a single direction from one end of the network to the other—which is why it's sometimes called a "line topology" or "backbone topology." Data flow on the network also follows the route of the cable, moving in one direction.

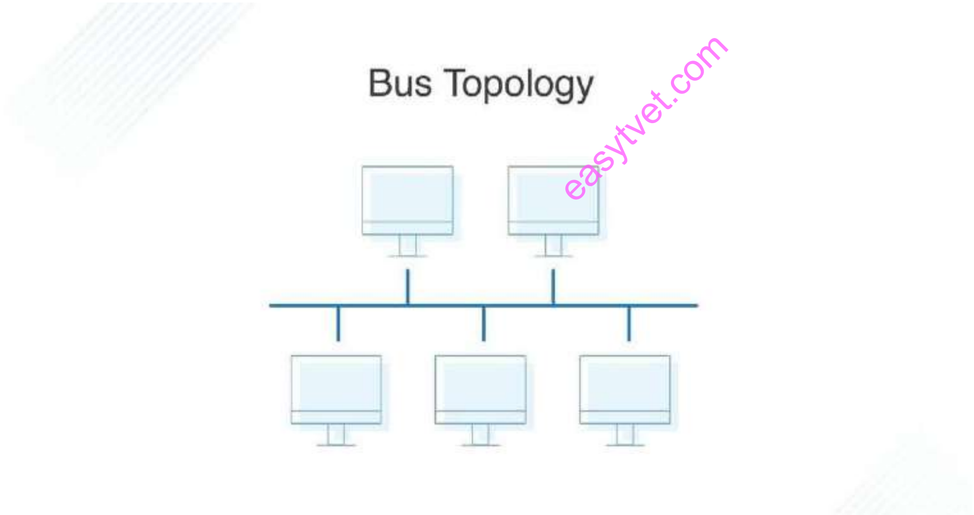


Figure 30 Bus toplolgy

Advantages of Bus Topology

Bus topologies are a good, cost-effective choice for smaller networks because the layout is simple, allowing all devices to be connected via a single coaxial or RJ45 cable. If needed, more nodes can be easily added to the network by joining additional cables.

Disadvantages of Bus Topology

However, because bus topologies use a single cable to transmit data, they're somewhat vulnerable. If the cable experiences a failure, the whole network goes down, which can be time-consuming and expensive to restore, which can be less of an issue with smaller networks.

Bus topologies are best suited for small networks because there's only so much bandwidth, and every additional node will slow transmission speeds.

Furthermore, data is "half-duplex," which means it can't be sent in two opposite directions at the same time, so this layout is not the ideal choice for networks with huge amounts of traffic.

3. Ring Topology - Single vs. Dual

Ring topology is where nodes are arranged in a circle (or ring). The data can travel through the ring network in either one direction or both directions, with each device having exactly two neighbors.

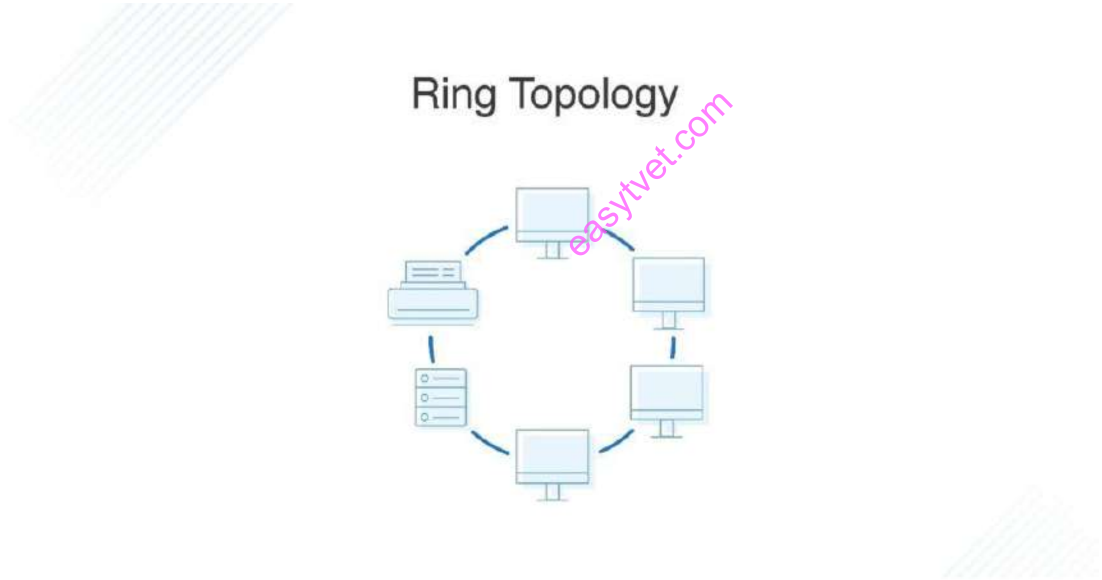


Figure 31: Ring topology

Pros of Ring Topology

Since each device is only connected to the ones on either side, when data is transmitted, the packets also travel along the circle, moving through each of the intermediate nodes until they arrive at their destination. If a large network is arranged in a ring topology, repeaters can be used to ensure packets arrive correctly and without data loss.

Only one station on the network is permitted to send data at a time, which greatly reduces the risk of packet collisions, making ring topologies efficient at transmitting data without errors.

By and large, ring topologies are cost-effective and inexpensive to install, and the intricate point-to-point connectivity of the nodes makes it relatively easy to identify issues or misconfigurations on the network.

Cons of Ring Topology

Even though it's popular, a ring topology is still vulnerable to failure without proper network management. Since the flow of data transmission moves unidirectionally between nodes along each ring, if one node goes down, it can take the entire network with it. That's why it's imperative for each of the nodes to be monitored and kept in good health. Nevertheless, even if you're vigilant and attentive to node performance, your network can still be taken down by a transmission line failure.

The question of scalability should also be taken into consideration. In a ring topology, all the devices on the network share bandwidth, so the addition of more devices can contribute to overall communication delays. Network administrators need to be mindful of the devices added to the topology to avoid overburdening the network's resources and capacity.

Additionally, the entire network must be taken offline to reconfigure, add, or remove nodes. And while that's not the end of the world, scheduling downtime for the network can be inconvenient and costly.

Dual-Ring Topology

A network with ring topology is half-duplex, meaning data can only move in one direction at a time. Ring topologies can be made full-duplex by adding a second connection between network nodes, creating a dual ring topology.

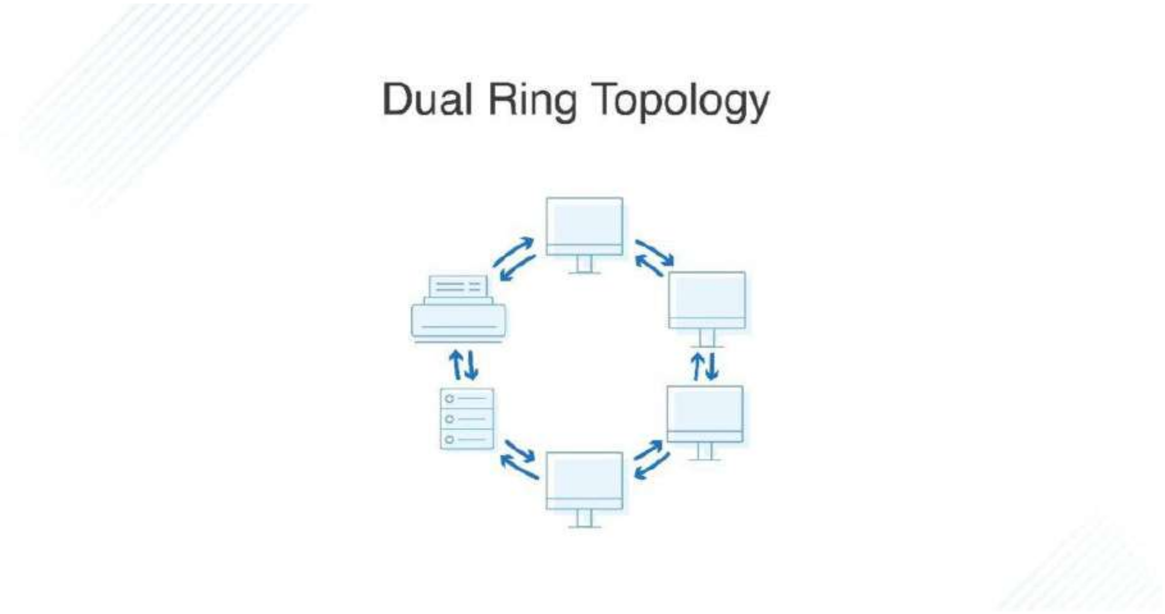


Figure 32: Dual ring topology

Advantages of Dual-Ring Topology

The primary advantage of dual ring topology is its efficiency: because each node has two connections on either side, information can be sent both clockwise and counterclockwise along the network. The secondary ring included in a dual-ring topology setup can act as a redundant layer and backup, which helps solve for many of the disadvantages of traditional ring topology. Dual ring topologies offer a little extra security, too: if one ring fails within a node, the other ring is still able to send data.

4. Tree Topology

The tree topology structure gets its name from how the central node functions as a sort of trunk for the network, with nodes extending outward in a branch-like fashion. However, where each node in a star topology is directly connected to the central hub, a tree topology has a parent-child hierarchy to how the nodes are connected. Those connected to the central hub are connected linearly to other nodes, so two connected nodes only share one mutual connection. Because the tree topology structure is both extremely flexible and scalable, it’s often used for wide area networks to support many spread-out devices.

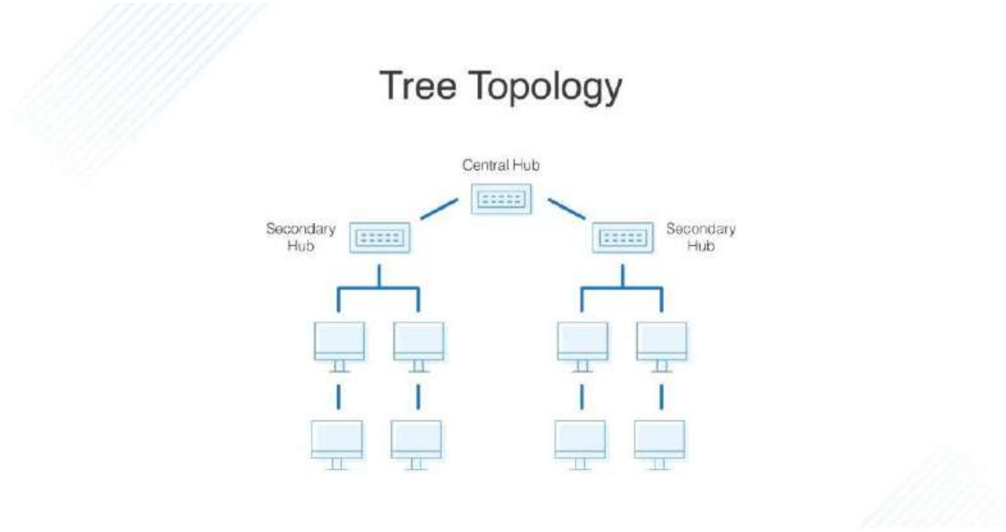


Figure 33: Tree topology

Pros of Tree Topology

Combining elements of the star and bus topologies allows for the easy addition of nodes and network expansion. Troubleshooting errors on the network is also a straightforward process, as each of the branches can be individually assessed for performance issues.

Cons of Tree Topology

As with the star topology, the entire network depends on the health of the root node in a tree topology structure. Should the central hub fail, the various node branches will become disconnected, though connectivity within—but not between—branch systems will remain.

Because of the hierarchical complexity and linear structure of the network layout, adding more nodes to a tree topology can quickly make proper management an unwieldy, not to mention costly, experience. Tree topologies are expensive because of the sheer amount of cabling required to connect each device to the next within the hierarchical layout.

5. Mesh Topology

A mesh topology is an intricate and elaborate structure of point-to-point connections where the nodes are interconnected. Mesh networks can be full or partial mesh. Partial mesh topologies are mostly interconnected, with a few nodes with only two or three connections, while full-mesh topologies are—surprise!—fully interconnected.

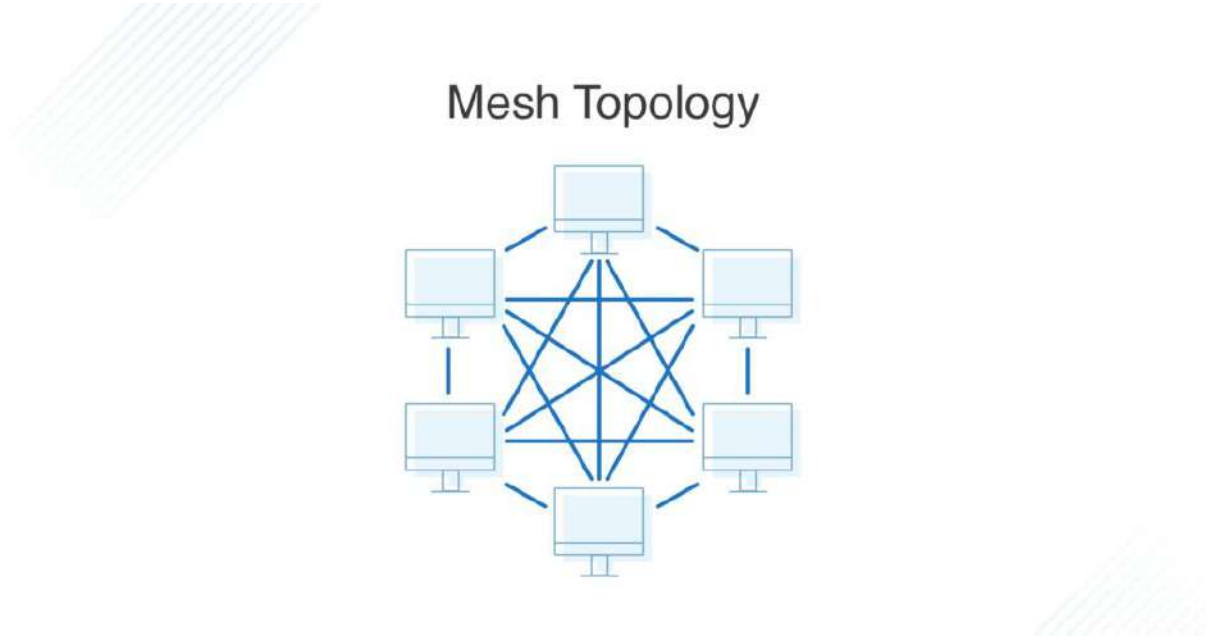


Figure 34: Mesh topology

The web-like structure of mesh topologies offers two different methods of data transmission: routing and flooding. When data is routed, the nodes use logic to determine the shortest distance from the source to destination, and when data is flooded, the information is sent to all nodes within the network without the need for routing logic.

Advantages of Mesh Topology

Mesh topologies are reliable and stable, and the complex degree of interconnectivity between nodes makes the network resistant to failure. For instance, no single device going down can bring the network offline.

Disadvantages of Mesh Topology

Mesh topologies are incredibly labor-intensive. Each interconnection between nodes requires a cable and configuration once deployed, so it can also be time-consuming to set up. As with other topology structures, the cost of cabling adds up fast, and to say mesh networks require a lot of cabling is an understatement.

6. Hybrid Topology

Hybrid topologies combine two or more different topology structures—the tree topology is a good example, integrating the bus and star layouts. Hybrid structures are most commonly found in larger companies where individual departments have personalized network topologies adapted to suit their needs and network usage.

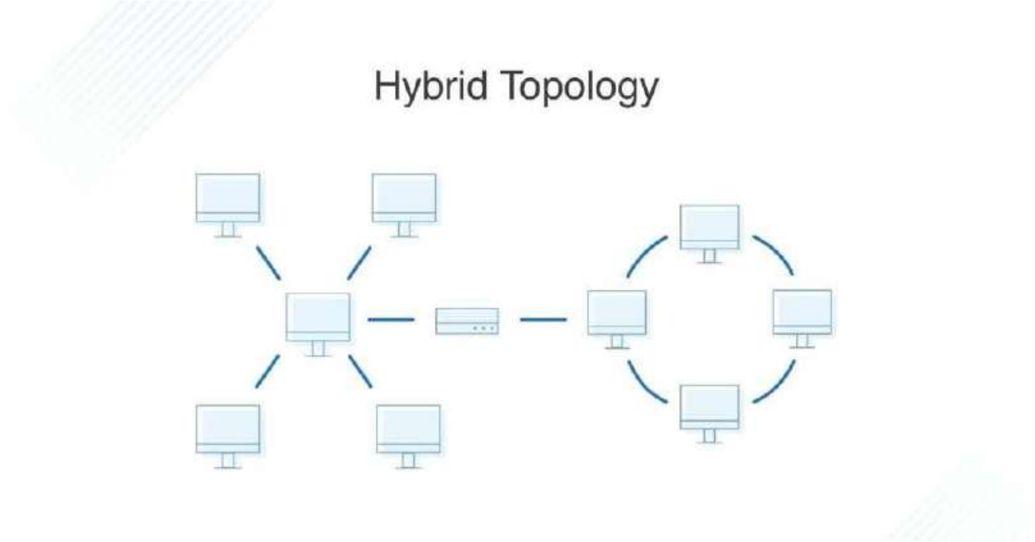


Figure 35: Hybrid topology

Advantages of Hybrid Topology

The main advantage of hybrid structures is the degree of flexibility they provide, as there are few limitations on the network structure itself that a hybrid setup can't accommodate.

Disadvantages of Hybrid Topology

However, each type of network topology comes with its own disadvantages, and as a network grows in complexity, so too does the experience and know-how required on the part of the admins to keep everything functioning optimally. There's also the monetary cost to consider when creating a hybrid network topology.

d) Computer Network Types

There are various types of computer networks available. We can categorize them according to their size as well as their purpose.

The size of a network should be expressed by the geographic area and number of computers, which are a part of their networks. It includes devices housed in a single room to millions of devices spread across the world. Some of the most popular network types are:

1. Personal Area Network (PAN)

A personal area network, or PAN, is a computer network that enables communication between computer devices near a person. It is a computer network organized around an individual for personal use only. PANs can be wired, such as USB or FireWire, or they can be wireless, such as infrared, ZigBee, Bluetooth and ultra-wideband. The range of a PAN typically is a few meters. Examples of wireless PAN, or WPAN, devices include cell phone headsets, wireless keyboards, wireless mice, printers, bar code scanners and game consoles.

Wireless PANs feature battery-operated devices that draw very little current. Sleep modes commonly are used to further extend battery life.

2. Local Area Network (LAN)

A Local Area Network (LAN) is a group of computers and other devices that are connected together over a network and are all in the same location, within a single building like an office or home.

On a typical home or small office LAN, you might find a modem that provides an internet connection (and a basic firewall against intrusion *from* the internet), a router that lets other devices share that connection and connect to one another, and a Wi-Fi access point that lets devices access the network wirelessly. Sometimes, those functions are combined into a single device.

3. Wireless Local Area Network (WLAN)

Functioning like a LAN, a WLAN provides wireless network communication over short distances using radio signals instead of traditional network cabling. Typically, a wireless local area network (WLAN) extends an existing wired local area network to devices not connected to the LAN.

4. Metropolitan Area Network (MAN)

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

5. **Wide Area Network (WAN)**

A wide-area network (or WAN) is a computer network that connects smaller networks. Since WANs are not tied to a specific location, they allow localized networks to communicate with one another across great distances. They also facilitate communication and the sharing of information between devices from anywhere in the world.

WANs allow organizations to create unified networks so that employees, customers, and other stakeholders can work together online, regardless of location. Though WANs cover a large area, connections can be either wired or wireless. Wired WANs usually consist of broadband internet services and multiprotocol label switching (MPLS), which is a form of data-forwarding technology used to control traffic flow and speed up connection, while wireless WANs normally include 4G/5G and Long-Term Evolution (LTE) networks.

e) **Computer Network Components**

Computer networks components comprise both physical parts as well as the software required for installing computer networks. Some important physical 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:

1. NIC

NIC stands for Network Interface Card is an adapter card that plugs into the system bus of a computer and allows the computer to send and receive signals on a network. A network interface card (NIC) is also known as a network adapter card or simply a network card.

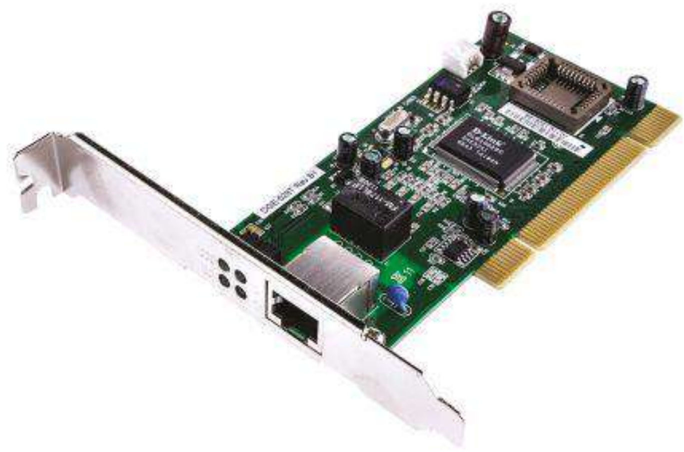


Figure 36: Network interface card

Wired NIC: The Wired NIC is present inside the motherboard. Cables and connectors are used with wired NIC to transfer data.

Wireless NIC: The wireless NIC contains the antenna to obtain the connection over the wireless network. For example, laptop computer contains the wireless NIC.

2. Hub

A Hub is a hardware device that divides the network connection among multiple devices. When a computer network requests for some information from another in the network, it first sends the request to the Hub through a cable. The hub will broadcast this request to the entire network. All the devices will check whether or not the request belongs to them. If not, the request will be dropped.

The process used by the Hub consumes more bandwidth and limits the amount of communication. Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches and Routers.

Figure 37: Computer Network hub

3. Switch

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.

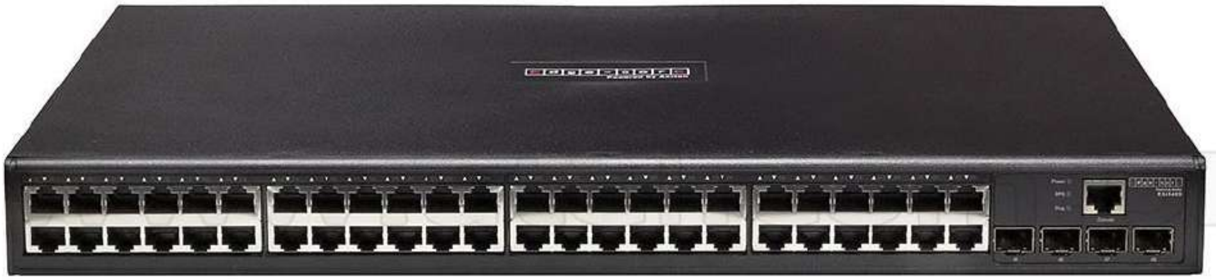


Figure 38: A Network Switch

4. Router

- A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network.
- A router works in a **Layer 3 (Network layer)** of the OSI Reference model.
- A router forwards the packet based on the information available in the routing table.
- It determines the best path from the available paths for the transmission of the packet.

Advantages of Router:

- **Security:** The information which is transmitted to the network will traverse the entire cable, but the only specified device which has been addressed can read the data.
- **Reliability:** If the server has stopped functioning, the network goes down, but no other networks are affected that are served by the router.
- **Performance:** Router enhances the overall performance of the network. Suppose there are 24 workstations in a network generates a same amount of traffic. This increases the traffic load on the network. Router splits the single network into two networks of 12 workstations each, reduces the traffic load by half.

Figure 39: A wireless Router

5. **Modem**

- A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line.
- A modem is not integrated with the motherboard rather than it is installed on the PCI slot found on the motherboard.
- 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

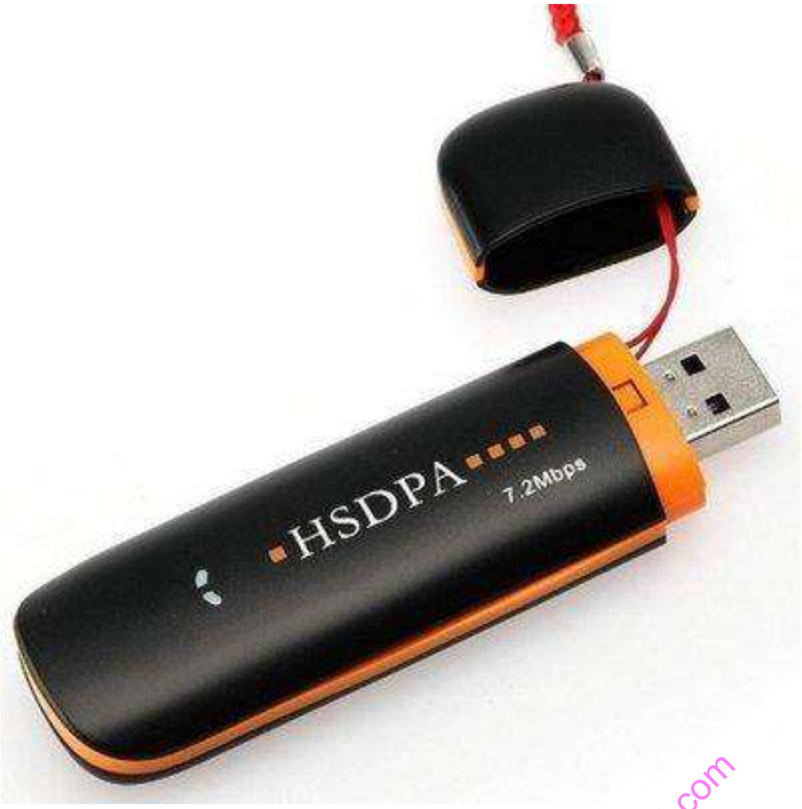


Figure 40: modem

6. Cables and Connectors (media)

Cable is a transmission media used for transmitting a signal.

There are three types of cables used in transmission:

- Twisted pair cable
- Coaxial cable
- Fibre-optic cable

7. Ports

A port is a physical docking point using which an external device can be connected to the computer. It can also be programmatic docking point through which information flows from a program to the computer or over the Internet.

A network port which is provided by the Transport Layer protocols of Internet Protocol suite, such as Transmission Control Protocol (TCP) and User Diagram Protocol (UDP) is a number which serving endpoint communication between two computers.

8. Computers

Computers connected to a network can share files and documents with each other. Personal computers connected to a business network can choose which files and folders are available to share on the network.

2.2.1.5 Learning Activities

- The trainee should visit the nearest computer lab, Cyber Café or office setup and identify 4 network devices. On a computer using Ms Word, draw a table with two columns, namely device and use. Record the use of at least 6 devices on this table.
- In the visit above, in two paragraphs, the trainee need to determine and illustrate the network type and topologies in place.
- Save the document and submit to the trainer, via a storage device or email.

Special instructions related to learning activities

- Lessons can be delivered in person or virtually.
- Trainees taking this unit are highly recommended to own a working computer

2.2.1.6 Self-Assessment

1. What is a computer network?
2. With an aid of a diagram, differentiate between a star and ring topology.
3. With respect to the OSI reference model, from which layer does a router operate?
4. What is POLAN?
5. In a Network Interface Card, what is meant by a MAC address?

2.2.1.7 Tools, Equipment, Supplies and Materials

Tools

1. Network tool kit
2. Signal testers

Equipment

- Computer
- Cables
- Switches
- Routers/modem
- Bridges
- Repeaters
- Fibre modules
- Antistatic gloves
- Ports
- RJ45
- NIC
- Gateways
- Microwave dishes

Materials and supplies

Consumables for maintaining Network including:

- RJ45
- Fibre Modules
- Cables

Replacement parts including:

- Points
- Switches
- Routers
- NIC
- Modem
- Cables

Cleaning materials;

Hand cleaner.

2.2.1.8 References

Stieglitz, N. (2003). Digital dynamics and types of industry convergence: the evolution of the handheld computers market. The industrial dynamics of the new digital economy, 2, 179-208

Székely, A., Talanow, R., & Bágyi, P. (2013). Smartphones, tablets and mobile applications for radiology. European journal of radiology, 82(5), 829-836.

Chlamtac, I., & Fumagalli, A. (1994). Quadro-star: A high performance optical WDM star network. IEEE Transactions on Communications, 42(8), 2582-2591

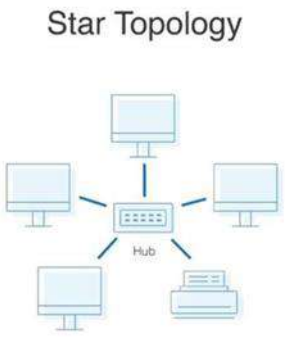
2.2.1.8 Model answers to self-assessment

What is a computer network?

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.

With an aid of a diagram, demonstrate a star topology.

A star topology, the most common network topology, is laid out so every node in the network is directly connected to one central hub via coaxial, twisted-pair, or fiber-optic cable. Acting as a server, this central node manages data transmission—as information sent from any node on the network has to pass through the central one to reach its destination—and functions as a repeater, which helps prevent data loss



With respect to the OSI reference model, from which layer does a router operate?

A router works in a ***Layer 3 (Network layer)*** *of the OSI Reference model.*

What is POLAN?

POLAN uses optical splitters to split an optical signal from one strand of single mode optical fiber into multiple signals to serve users and devices.

In a Network Interface Card, what is meant by a MAC address?

The MAC address or physical address is encoded on the network card chip which is assigned by the IEEE to identify a network card uniquely. The MAC address is stored in the PROM (Programmable read-only memory).

2.2.1 **Learning Outcome 2: Connect Network Devices**

2.2.2.1 Introduction to the Learning Outcome

This learning outcome covers identification of network connection media, characteristics of connection medium and connecting devices to the network.

2.2.2.2 Performance Standard

2.2.2.2.1 Tools, materials and devices for network are identified.

2.2.2.2.2 Network devices connection is done according National and international communication standards.

2.2.2.2.3 Strength and connectivity tests of cables and equipment are done.

2.2.2.3 Information Sheet

a) Network connection media

In network communications, a connection or transmission medium is a physical connection or an interface between the transmitter and the receiver. There are two major categories of transmission media, namely:

- Wired or guided and
- Wireless or unguided.

Wired Medium

There are three general classes of wired media types: coaxial cable, twisted pair and fiber optic cable.

Figure 41: Network cables

1. Coaxial Cable

Coaxial cable uses a single conductor in the middle of a cable. The central conductor is surrounded by an insulator called the dielectric. A conductive shield is put around the dielectric. This shield acts as the second conductor for the circuit as well serves to protect the inner conductor from interference. Coaxial cable for local area network (LAN) connections is obsolete. Coaxial cable is being used in some cases for delivering the last mile of service. For e.g., coaxial cables are being used by Cable TV networks to deliver high-speed service customer premises.

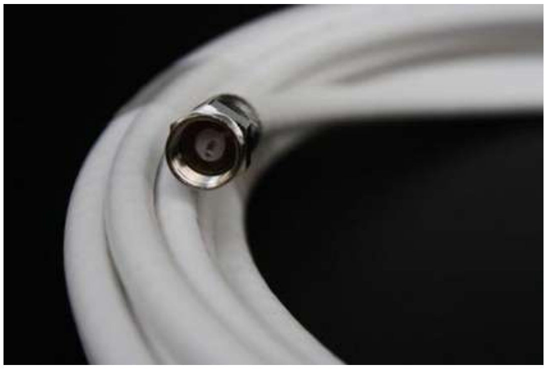


Figure 42: Coaxial cable with a central conductor

2. Unshielded Twisted Pair

Unshielded twisted pair cabling, or UTP cabling, is the most common type of network cabling. It consists of four twisted pairs of wire, each with a different number of twists per foot, all encased on one sheath. UTP cabling is graded according to category. Category 3 and 4 were replaced by Category 5 cabling by the year 2000. Category 5 is recommended for running Ethernet at speeds of 100 Mbps. Category 5e, was introduced to run gigabit Ethernet or 1000BaseT networks. Category 6 and Category 6a have since been introduced to give better performance at higher speeds. UTP cabling has an intrinsic impedance of 100 ohms.

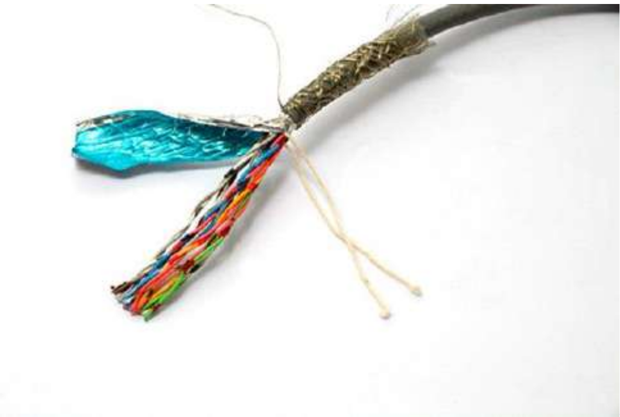


Figure 43: Unshielded twisted pair cable

3. Twisted Pair Cable

There are two types of shielded twisted pair wiring. In the 1980s and 1990s shielded twisted pair was promoted as the best wire type for Token Ring networks. This had an intrinsic impedance of 150 ohms. A new wiring trend is to use 100 ohm shielded twisted pair. The shielding reduces noise and increases the performance of the cable. These are sometimes called foiled twisted pair, or FTP (not to be confused with file transfer protocol) or sometimes called screened twisted pair, or ScTP. These types of cables are compatible with normal UTP.

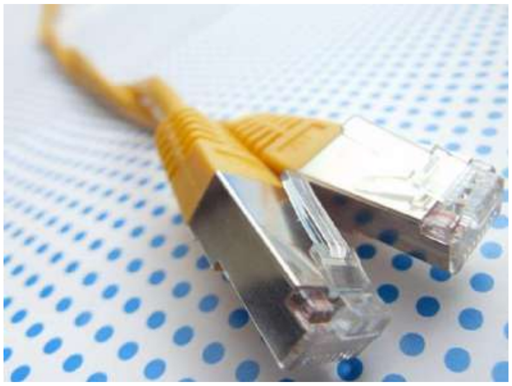


Figure 44: FTP or ScTP has a metal back to ground the shield.

4. Multi-mode fiber Optic

Fiber optic cable is sometimes called wave guide or light guide because it guides the light waves along the length of the cable. Multi-mode fiber is used for short cable runs, usually 1.6 mi (approximately 2 km) or less.

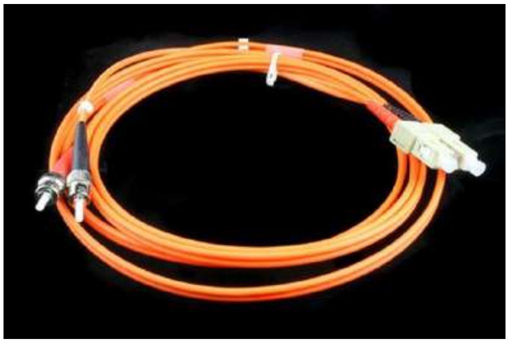


Figure 45: Multi-mode fiber optic

5. Single Mode Fiber Optic Cable

Single mode fiber optic cable can operate over much longer distances. Because the fiber only allows one mode of light to propagate, light pulses put on the fiber keep their shape much longer. This allows the light pulses to travel much further without interfering with other pulses. Single mode fiber is recommended for cable runs in excess of 1.6 mi.

Figure 46: Single mode fiber is used outdoors and for long distances.

Wireless Transmission Media

Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.

When an antenna is attached to electrical circuit of a computer or wireless device, it converts the digital data into wireless signals and spread all over within its frequency range. The receptor on the other end receives these signals and converts them back to digital data.

1. Radio Transmission

Radio frequency is easier to generate and because of its large wavelength it can penetrate through walls and structures alike. Radio waves can have wavelength from 1 mm – 100,000 km and have frequency ranging from 3 Hz (Extremely Low Frequency) to 300 GHz (Extremely High Frequency). Radio frequencies are sub-divided into six bands.

Radio waves at lower frequencies can travel through walls whereas higher RF can travel in straight line and bounce back.The power of low frequency waves decreases sharply as they cover long distance. High frequency radio waves have more power.

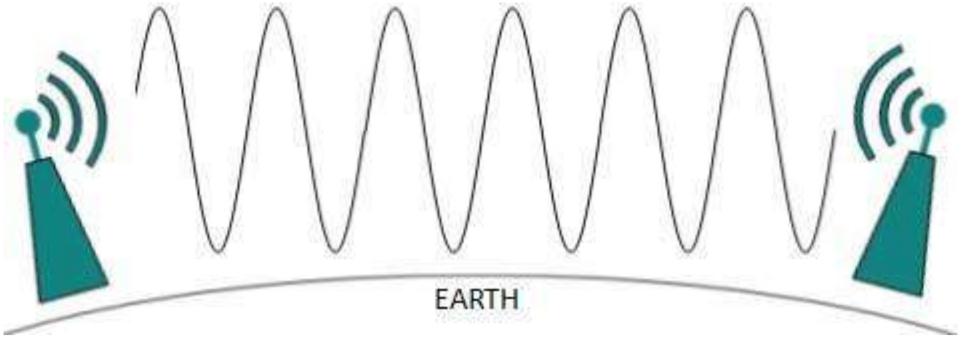
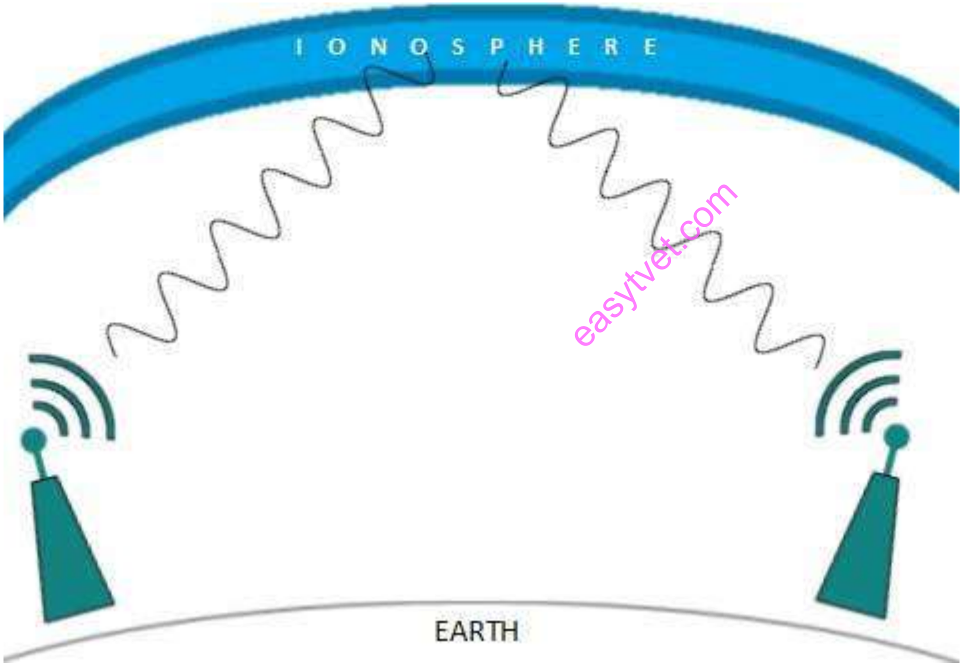


Figure 47: Radio Transmission earth

Radio waves of high frequencies are prone to be absorbed by rain and other obstacles. They use Ionosphere of earth atmosphere. High frequency radio waves such as HF and VHF bands are spread upwards. When they reach Ionosphere, they are refracted back to the earth.



2. Microwave Transmission

Electromagnetic waves above 100 MHz tend to travel in a straight line and signals over them can be sent by beaming those waves towards one particular station. Because Microwaves travels in straight lines, both sender and receiver must be aligned to be strictly in line-of-sight.

Microwaves can have wavelength ranging from 1 mm – 1 meter and frequency ranging from 300 MHz to 300 GHz.

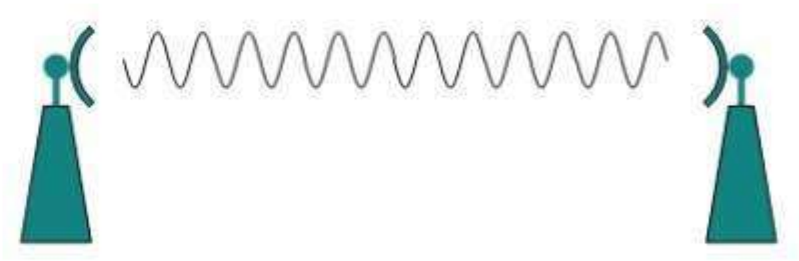


Figure 48: Microwave transmission

Microwave antennas concentrate the waves making a beam of it. As shown in picture above, multiple antennas can be aligned to reach farther. Microwaves have higher frequencies and do not penetrate wall like obstacles.

Microwave transmission depends highly upon the weather conditions and the frequency it is using.

3. Infrared Transmission

Infrared wave lies in between visible light spectrum and microwaves. It has wavelength of 700-nm to 1-mm and frequency ranges from 300-GHz to 430-THz.

Infrared wave is used for very short range communication purposes such as television and it's remote. Infrared travels in a straight line hence it is directional by nature. Because of high frequency range, Infrared cannot cross wall-like obstacles.

4. Light Transmission

Highest most electromagnetic spectrum which can be used for data transmission is light or optical signaling. This is achieved by means of LASER.

Because of frequency light uses, it tends to travel strictly in straight line.Hence the sender and receiver must be in the line-of-sight. Because laser transmission is unidirectional, at both ends of communication the laser and the photo-detector needs to be installed. Laser beam is generally 1mm wide hence it is a work of precision to align two far receptors each pointing to lasers source.

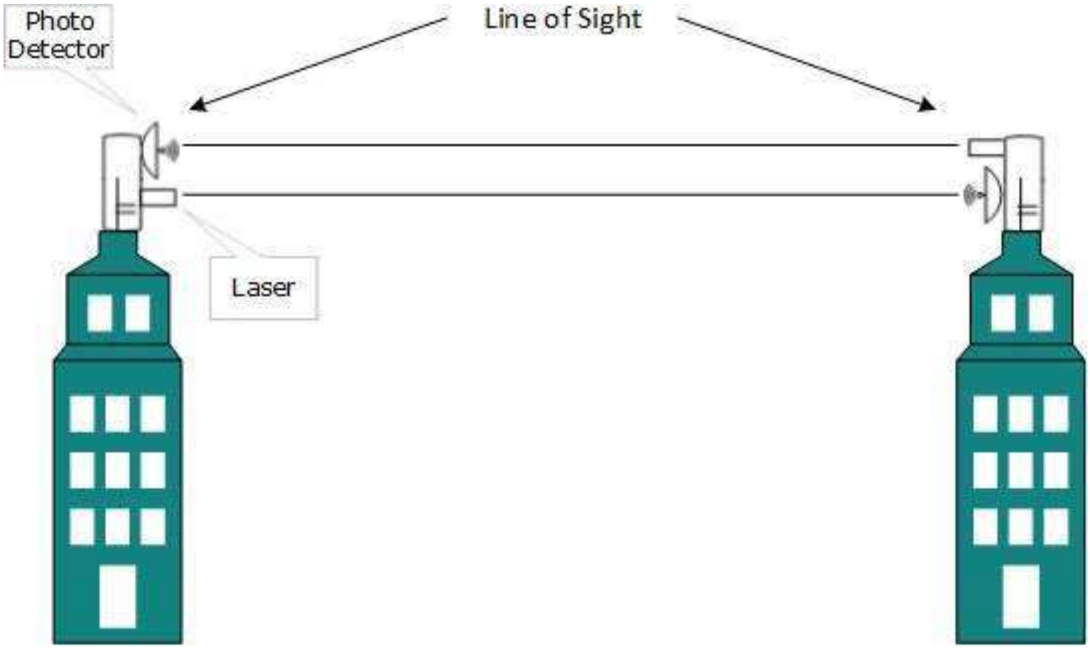


Figure 49: Light transmission

Laser works as Tx (transmitter) and photo-detectors works as Rx (receiver).

Lasers cannot penetrate obstacles such as walls, rain and thick fog. Additionally, laser beam is distorted by wind, atmosphere temperature, or variation in temperature in the path.

Laser is safe for data transmission as it is very difficult to tap 1mm wide laser without interrupting the communication channel.

c) How to connect computers to a network

Connecting your computers to your home network grants access to the Internet, networked printers and attached devices and other computers on the network. Most networks in the home or workplace are Ethernet wired networks or Wi-Fi wireless networks. How you connect to a network and what equipment you need depends primarily on the network connection you're setting up.

i.Required Equipment

If you're setting up a wired network, you need an Ethernet modem, a router -- unless your modem has a built-in router -- and Ethernet cables. If you're setting up a wireless network, you still need an Ethernet modem and a wireless-enabled router, as well as an Ethernet cable to connect the two. You also need one wireless adapter per computer, unless your computer has a built-in wireless card.

If you're building a hybrid network involving both wired and wireless connections, a wireless router is the best choice, as they usually also have Ethernet ports. Some modems feature built-in wireless routers, making them a good all-in-one device choice if you have limited space.

ii.Connecting to a wired network

1. Connect the Internet coaxial or DSL cable to your modem's **Internet** or **Cable** port.
2. Connect the modem to the router's **Internet**, **Modem** or **WAN** port with an Ethernet cable. Skip this step if your modem has a built-in router.
3. Connect an Ethernet cable between each computer's Ethernet port and one of the open ports on the router or modem.
4. Click the **Network** icon in the System Tray and check for the wired connection.
5. Start a Web browser and connect to a website. If the site loads, your connection is complete. Otherwise, consult your modem and router's user manuals to see if further setup is required.

Pros

- Wired connections offer faster and more stable connections than wireless.
- Wired-only networks are generally more secure than wireless, as unauthorized users have to directly connect to the router in order to gain access to the network.
- Ethernet cables are less expensive than wireless adapters.

Cons

- Wired-only networks have limited range compared to wireless. While this situation can be mitigated with longer Ethernet cables, you have to run wires throughout your home to access the Internet from any room.
- The number of computers that can connect to the router is limited to the number of available Ethernet ports.

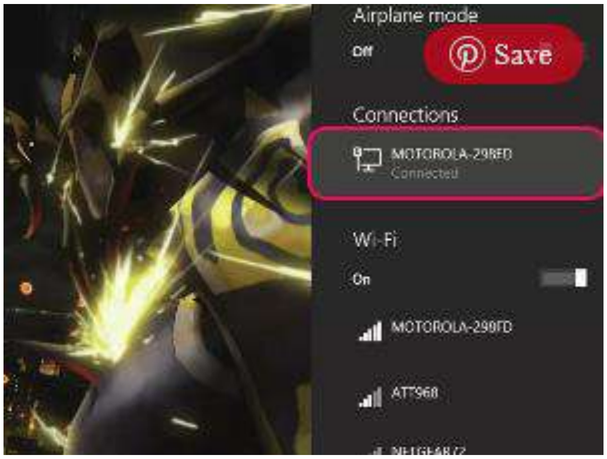


Figure 50: Connecting to a wired network

Connecting to a wireless network

1. Connect the Internet coaxial or DSL cable to your modem's **Internet** or **Cable** port.
2. Connect the modem to the router's **Internet**, **Modem** or **WAN** port with an Ethernet cable. Skip this step if your modem has a built-in router.
3. Click the **Network** icon in the System Tray and find your wireless network in the list.
4. Select your network and click **Connect**. If you want your computer to automatically connect to this network when you start it up, fill the **Connect Automatically** check box.
5. Enter your wireless network's security key when prompted.
6. Start a Web browser and connect to a website. If the site loads, your connection is complete. Otherwise, make sure the security key you entered is correct, then check signal strength and whether further set-up is required according to your user's manual.

- Pro: You can take your computer to most rooms of your house without having to route Ethernet cables through your home.
- Pro: The only Ethernet cable required is the one running from your modem to your router, assuming your modem doesn't have a built-in router.
- Con: Wireless connections aren't as fast as wired connections, as they have to transmit bandwidth over the wireless signal.
- Con: The design of your home and nearby electronics can interfere with a wireless signal, weakening or even completely blocking your connection.

- Con: Without a security key, your wireless connection can be detected and used by anyone -- including cyber-criminals engaged in illicit behavior, which may be traced back to you.

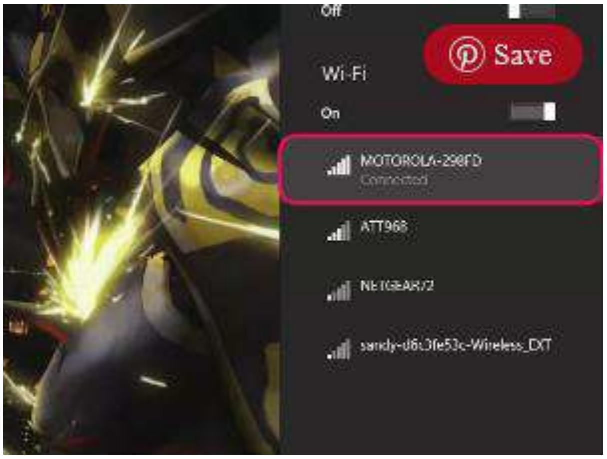
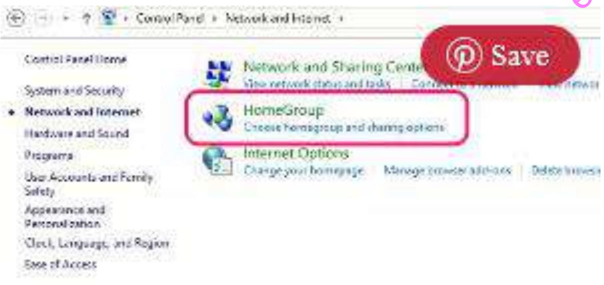


Figure 51: Wireless connection

iii.Creating Home groups

A Home group is a network used by Windows to connect your computers together and share files. After you create a Home group, your other computers and devices like printers can be added to it.


Control Panel › Network and Internet ›
Save
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts and Family Safety
Appearance and Personalization
Clock, Language, and Region
Ease of Access
Network and Sharing Center
View network status and tasks
HomeGroup
Choose homegroup and sharing options
Internet Options
Change your homepage
Manage browser add-ons

i. Creating a Homegroup

1. Press **Windows-X** on your keyboard and select **Control Panel** from the power user menu.
2. Select **Network and Internet**, followed by **Homegroup**.
3. Click **Create**, followed by **Next**.
4. Select the libraries, devices and files you want to share with other computers on the network, then click **Next**.

5. Write down the Homegroup password when it's presented and click **Finish**.

ii. Adding Computers to the Homegroup

1. Sign onto the computer you're adding.
2. Press **Windows-X** and select **Control Panel**.
3. Select **Network and Internet**, followed by **Homegroup**.
4. Click **Join now**, followed by **Next**.
5. Select the libraries, devices and files you want to share from this computer, then click **Next**.
6. Enter the homegroup password and click **Next**, then **Finish**.

iii. Adding Printers

1. Sign onto the computer to which your printer is installed/connected.
2. Follow the steps to join a homegroup listed above.
3. Set the **Printers & Devices** permission to **Shared**.

d) Network Devices

1. Hub

A Hub is a hardware device that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable. Hub will broadcast this request to the entire network. All the devices will check whether the request belongs to them or not. If not, the request will be dropped.

The process used by the Hub consumes more bandwidth and limits the amount of communication. Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches, Routers.

2 Switch

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.

3 Router

A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network.

A router works in a Layer 3 (Network layer) of the OSI Reference model.

A router forwards the packet based on the information available in the routing table.

It determines the best path from the available paths for the transmission of the packet.

4 Cables and Connectors (media)

Cable is a transmission media used for transmitting a signal.

There are three types of cables used in transmission:

- Twisted pair cable
- Coaxial cable
- Fibre-optic cable

5 Ports

A port is a physical docking point using which an external device can be connected to the computer. It can also be programmatic docking point through which information flows from a program to the computer or over the Internet.

A network port which is provided by the Transport Layer protocols of Internet Protocol suite, such as Transmission Control Protocol (TCP) and User Diagram Protocol (UDP) is a number which serving endpoint communication between two computers.

6 Computers

Computers connected to a network can share files and documents with each other. Personal computers connected to a business network can choose which files and folders are available to share on the network.

2.2.2.4 Learning Activities

- The trainee is required to build a hybrid network involving both wired and wireless connections. Use the most suitable hub and any other devices available, creating a star topology.
- In the above setup, the trainee will be required to create a home group.
- The trainee will then add three computers and a printer to the workgroup.

Special instructions

The trainee should be provided with a wireless router as they have Ethernet ports or modems featuring built-in wireless routers.

2.2.2.5 Self-Assessment

1. Using suitable descriptions, identify the three general classes of wired media types
2. Why do you think a single mode fiber optic cable can operate over much longer distances compared to the other contemporary cables?
3. When building a hybrid network involving both wired and wireless connections, explain the choice of the router you would use, and give reasons.
4. Demonstrate the procedure for creating a Homegroup
5. Demonstrate the process of adding Computers to the Homegroup

2.2.2.6 Tools, Equipment, Supplies and Materials

Tools

1. Network tool kit
2. Signal testers

Equipment

- Computer
- Cables
- Switches
- Routers/modem
- Bridges
- Repeaters

- Fibre modules
- Antistatic gloves
- Ports
- RJ45
- NIC
- Gateways
- Microwave dishes

Materials and supplies

Consumables for maintaining Network including:

- RJ45
- Fibre Modules
- Cables

Replacement parts including:

- Points
- Switches
- Routers
- NIC
- Modem
- Cables

Cleaning materials;

Hand cleaner.

2.2.2.7 References

1. *Ma, W., Trusina, A., El-Samad, H., Lim, W. A., & Tang, C. (2009). Defining network topologies that can achieve biochemical adaptation. Cell, 138(4), 760-773.*
2. *Haeder, A. (2004). Conducting the Network Administrator Job Interview: IT Manager Guide with Cisco CCNA Interview Questions (Vol. 4). Rampant TechPress.*
3. *Pelle, I., Lévai, T., Németh, F., & Gulyás, A. (2015, June). One tool to rule them all: A modular troubleshooting framework for sdn (and other) networks. In Proceedings of the 1st ACM SIGCOMM Symposium on Software Defined Networking Research (pp. 1-7).*

4. *https://www.tutorialspoint.com/computer_fundamentals/computer_output_devices.htm*
5. *https://www.tutorialspoint.com/computer_fundamentals/computer_software.htm*

2.2.2.8 Model answers to Self-Assessment

1. ***Using suitable descriptions, identify the three general classes of wired media types***

   Three general classes of wired media types: coaxial cable, twisted pair and fiber optic cable.

2. ***Demonstrate why single mode fiber optic cable can operate over much longer distances.***

   Because the fiber only allows one mode of light to propagate, light pulses put on the fiber keep their shape much longer. This allows the light pulses to travel much further without interfering with other pulses. Single mode fiber is recommended for cable runs in excess of 1.6 mi.

2a If you're building a hybrid network involving both wired and wireless connections, which router is the best choice?

A wireless router is the best choice as they usually also have Ethernet ports. Some modems feature built-in wireless routers, making them a good all-in-one device choice if you have limited space.

2b Demonstrate the procedure for creating a Home group

- *Press Windows-X on your keyboard and select Control Panel from the power user menu.*
- *Select Network and Internet, followed by Home group.*
- *Click Create, followed by Next.*
- *Select the libraries, devices and files you want to share with other computers on the network, then click next.*
- *Write down the Home group password when it's presented and click Finish.*

2c Demonstrate the process of adding Computers to the Home group

- *Sign onto the computer you're adding.*
- *Press Windows-X and select Control Panel.*
- *Select Network and Internet, followed by Home group.*
- *Click Join now, followed by Next.*
- *Select the libraries, devices and files you want to share from this computer, then click next.*
- *Enter the home group password and click Next, then Finis*

2.2.3 Learning Outcome 3: Configure Network Devices

2.2.3.1 Introduction to the learning outcome

This learning outcome covers procedures on installation and configuration of Network software, configuration of the TCP/IP and Ethernet network architectures, connection and configuration of network devices, and performing connectivity tests for cables and equipment.

2.2.3.2 Performance Standard

2.2.3.2.1 Network software is installed and configured according to user manuals.

2.2.3.2.2 IP addressing scheme configuration is done

2.2.3.2.3 Types of subnet masks are identified.

2.2.3.3 Information Sheet

a) What is Network Configuration?

Network configuration allows a system administrator to set up a network to meet communication objectives. The process involves the following tasks:

- Router configuration: Specifies the correct IP addresses and route settings, etc.
- Host configuration: Sets up a network connection on a host computer/laptop by logging the default network settings, such as IP addressing, proxy, network name and ID/password, to enable network connection and communication.
- Software configuration: Any network-based software, like an intrusion detection system (IDS), is allowed access and provided with the appropriate credentials to monitor network traffic.

Moreover, network configuration includes Internet/network sharing, software/application installation and firewall installation/configuration.

b) Network architecture

Network architecture refers to the way network devices and services are structured to serve the connectivity needs of client devices.

- Network devices typically include switches and routers.
- Types of services include DHCP and DNS.

- Client devices comprise end-user devices, servers, and smart things.

c) Ethernet and TCP/IP suites

Ethernet is a layer 2 data link protocol that is widely used with the TCP/IP protocol, which resides at layers 3 and 4. To understand network communications, it is essential to learn about the protocol layers (see OSI model below).

The IP layer 3 breaks apart the data being transmitted into variable length packets, known as "Ethernet frames," up to 1,500 bytes long. Each frame has a header containing source and destination addresses and a trailer with error correction data.

d) TCP/IP Ensures Complete Delivery

Ethernet transmits the frames from one node to the next and only guarantees that if the frame arrives, it arrived intact. If a frame goes missing, it is none the wiser. However, the TCP part of TCP/IP ensures that the entire set of data has been delivered intact. For details about the protocols, see data link protocol, CSMA/CD, TCP/IP and Internet protocol

e) Network protocols

Network protocols are a set of rules, conventions, and data structures that dictate how devices exchange data across networks. In other words, network protocols can be equated to languages that two devices must understand for seamless communication of information, regardless of their infrastructure and design disparities.

b. The OSI model: How network protocols work

To understand the nuances of network protocols, it's imperative to know about the Open Systems Interconnection (OSI) model first. Considered the primary architectural model for internet working communications, the majority of network protocols used today are structurally based on the OSI model.

The OSI model splits the communication process between two network devices into 7 layers. A task or group of tasks is assigned to each of these 7 layers. All the layers are self-contained, and the tasks assigned to them can be executed independently.

To put this into context, here is a representation of the communication process between two network devices following the OSI model:

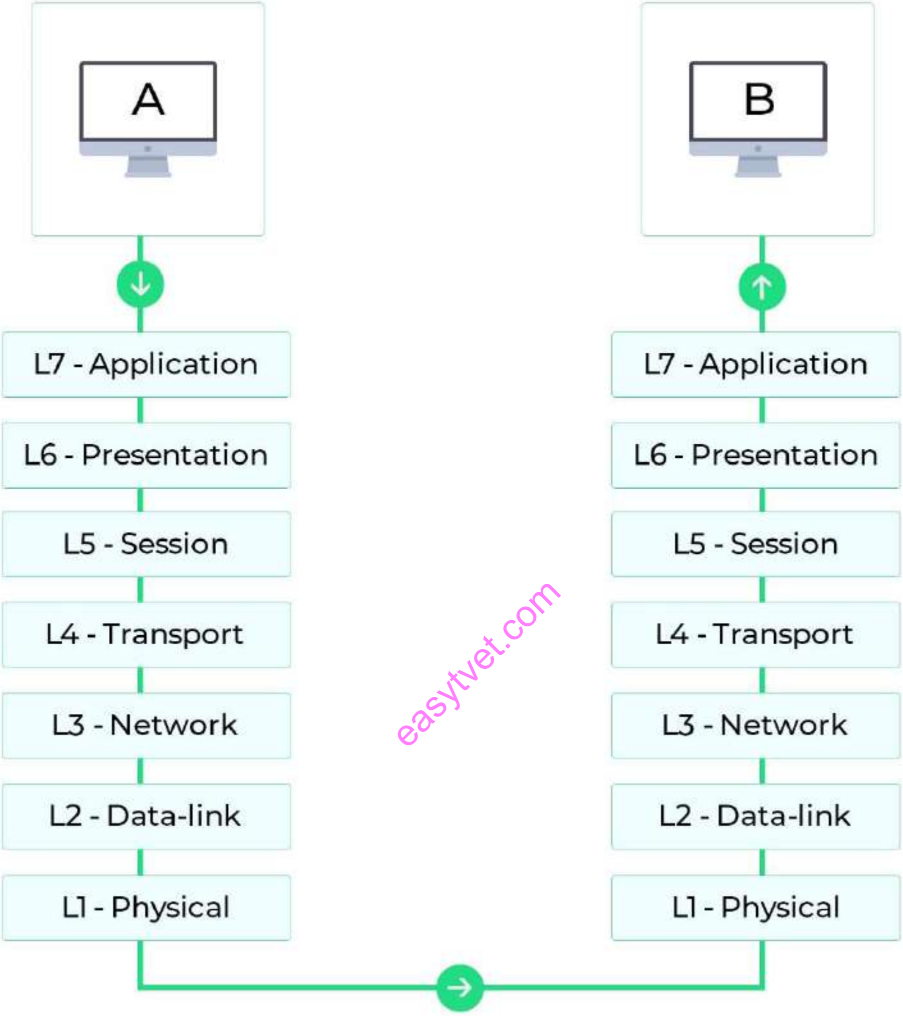


Figure 52: OSI Model

The seven layers in the OSI model can be divided into two groups: upper layers, including layers 7, 6, and 5, and lower layers, including layers 4, 3, 2, and 1. The upper layers deal with application issues, and the lower layers deal with data transport issues.

Network protocols divide the communication process into discrete tasks across every layer of the OSI model. One or more network protocols operate at each layer in the communication exchange.

Following are the detailed descriptions of the functioning of network protocols in each layer of the OSI model:

Table 25:OSI network protocol functions

Layer 7: Application layer network protocols	• Provides standard services such as virtual terminal, file, and job transfer and operations.
Layer 6: Presentation layer network protocols	• Masks the differences in data formats between dissimilar systems. • Encodes and decodes data, encrypts and decrypts data, and compresses and decompresses data.
Layer 5: Session layer network protocols	• Manages user sessions and dialogues. • Establishes and terminates sessions between users.
Layer 4: Transport layer network protocols	• Manages end-to-end message delivery in networks. • Renders reliable and sequential packet delivery through error recovery and flow control mechanisms.
Layer 3: Network layer protocols	• Routes packets according to unique network device addresses. • Renders flow and congestion control to prevent network resource depletion.
Layer 2: Data link layer network protocols	• Frames packets. • Detects and corrects packet transmit errors.
Layer 1: Physical layer network protocols	• Interfaces between network medium and devices. • Defines optical, electrical, and mechanical characteristics.

c. TCP/IP model

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Functions of TCP/IP layers:

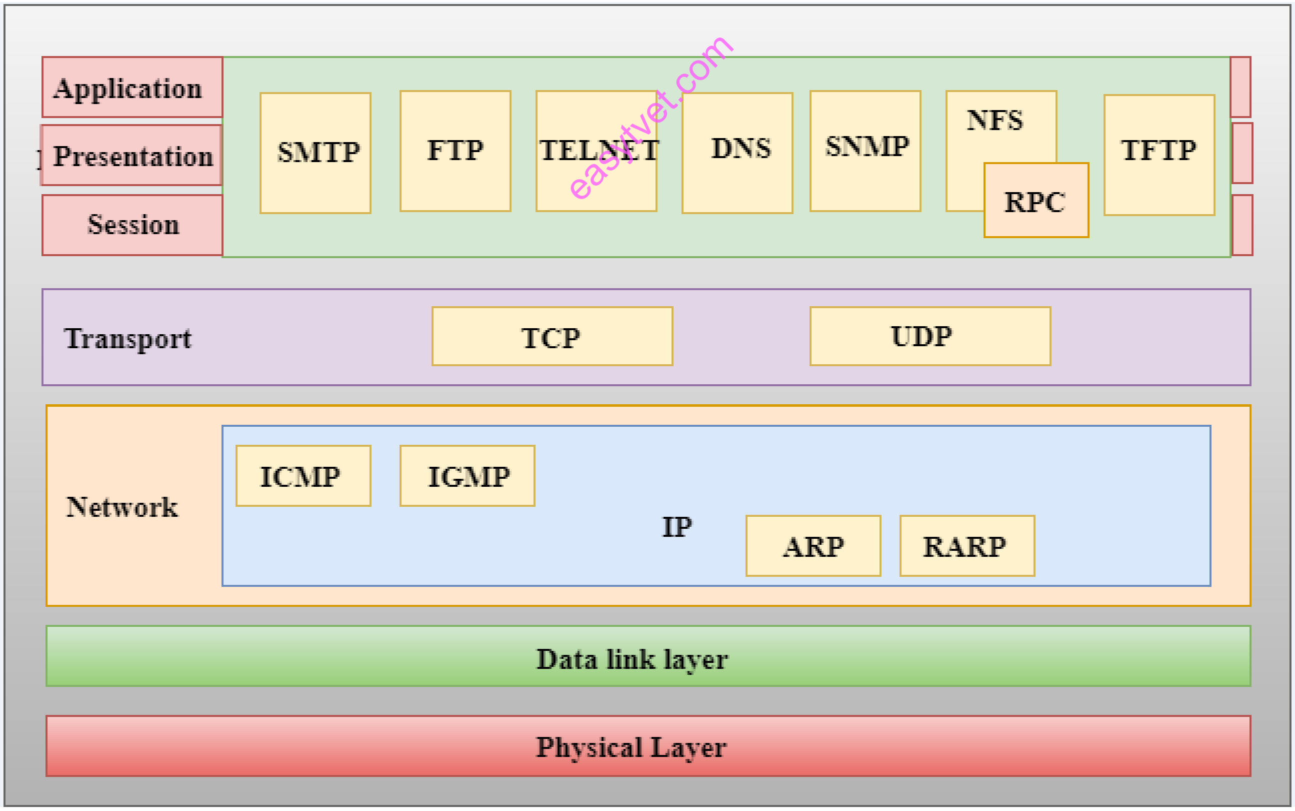


Figure 53: TCP/IP Layers

i. Network Access Layer

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

ii. Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols used in this layer:

IP Protocol: IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.

- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP Protocol

- ARP stands for **Address Resolution Protocol**.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- **The two terms are mainly associated with the ARP Protocol:**
    - **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
    - **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

ICMP Protocol

- **ICMP** stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on

fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.

- An ICMP protocol mainly uses two terms:
    - **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
    - **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.
- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

iii. Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

- **User Datagram Protocol (UDP)**
    - It provides connectionless service and end-to-end delivery of transmission.
    - It is an unreliable protocol as it discovers the errors but not specify the error.
    - User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
    - **UDP consists of the following fields:**
      Source port address: The source port address is the address of the application program that has created the message.
      Destination port address: The destination port address is the address of the application program that receives the message.
      Total length: It defines the total number of bytes of the user datagram in bytes.
      Checksum: The checksum is a 16-bit field used in error detection.

- UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.

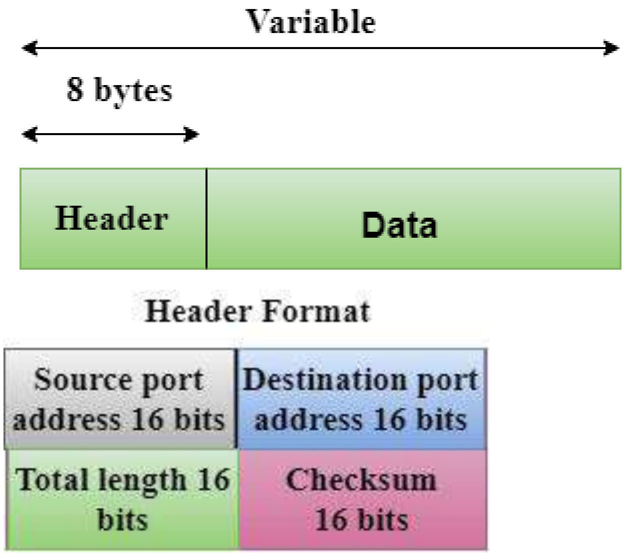


Figure 54: User Datagram protocol

- **Transmission Control Protocol (TCP)**
  - It provides a full transport layer services to applications.
  - It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
  - TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
  - At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
  - At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

iv. Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.

- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

Following are the main protocols used in the application layer:

- **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the World Wide Web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.
- **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
- **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
- **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

f) Network Operating System

An operating system (OS) is basically a collection of software that manages computer hardware resources and provides common services for computer programs. Operating system is a crucial component of the system software in a computer system.

Network Operating System is one of the important type of operating system.

Network Operating System runs on a server and gives the server the capability to manage data, users, groups, security, applications, and other networking functions. The basic purpose of the network operating system is to allow shared file and printer access among multiple computers in a network, typically a local area network (LAN), a private network or to other networks.

Types of network operating systems

There are two basic types of network operating systems, the peer-to-peer NOS and the client/server NOS:

1. Peer-to-peer network operating systems allow users to share network resources saved in a common, accessible network location. In this architecture, all devices are treated equally in terms of functionality. Peer-to-peer usually works best for small to medium LANs and is cheaper to set up.
2. Client/server network operating systems provide users with access to resources through a server. In this architecture, all functions and applications are unified under one file server that can be used to execute individual client actions regardless of physical location. Client/server tends to be most expensive to implement and requires a large amount of technical maintenance. An advantage to the client/server model is that the network is controlled centrally, makes changes or additions to technology easier to incorporate.

Common features of network operating systems

Features of network operating systems are typically associated with user administration, system maintenance and resource management functionality. This includes:

- Basic support for operating systems like protocol and processor support, hardware detection and multiprocessing.
- Printer and application sharing.
- Common file system and database sharing.
- Network security capabilities such as user authentication and access control Directory
- Backup and web services.
- Internetworking.

Examples of network operating systems

True network operating systems are categorized as software that enhances the functionality of operating systems by providing added network features. A few examples of these network operating systems and their service providers are:

- Artisoft's LANtastic- This is a simple, user-friendly NOS that supports most PC operating systems.
- Banyan's VINES- This uses a client-server architecture to request specific functions and services.
- Novell's NetWare- This was the first network operating system to be released and is designed based on XNS protocol architecture.
- Microsoft's LAN Manager- This operates as a server application and was developed to run under the Microsoft OS. Now, most of the functionality of LAN Manager is included in the Windows OS itself.

In addition, some multi-purpose operating systems, such as Windows NT and Digital's OpenVMS come with capabilities that enable them to be described as a network operating system. Further, the most popular operating systems like Windows, UNIX, Linux and Mac include built-in networking functions that may not require additional network services.

2.2.3.4 Learning Activities

- The trainee should visit the nearest server room and identify the network operating system running on the various servers.
- In the visit above, the trainee should determine the various resources running on the server, if any. The trainee will also determine if there are more resources that can be included, giving reasons for each.

  Special instructions

  The trainee can be exposed to both Windows and LINUX environments.

2.2.3.5 Self-Assessment

1. What are Network protocols?
2. Illustrate how network protocols work using the OSI model.
3. What is ARP and which two terms are associated with this protocol?
4. What is a Network Operating System?
5. Illustrate some examples of network operating systems

2.2.3.6 Tools, Equipment, Supplies and Materials

Tools

1. Network tool kit
2. Signal testers

Equipment

- Computer
- Cables
- Switches
- Routers/modem
- Bridges
- Repeaters
- Fibre modules
- Antistatic gloves
- Ports
- RJ45

- NIC
- Gateways
- Microwave dishes

Materials and supplies

Consumables for maintaining Network including:

- RJ45
- Fibre Modules
- Cables

Replacement parts including:

- Points
- Switches
- Routers
- NIC
- Modem
- Cables

Cleaning materials;

Hand cleaner.

2.2.3.7 References

1. Pelle, I., Lévai, T., Németh, F., & Gulyás, A. (2015, June). One tool to rule them all: A modular troubleshooting framework for sdn (and other) networks. In Proceedings of the 1st ACM SIGCOMM Symposium on Software Defined Networking Research (pp. 1-7).
2. Chen, C. W. (2005). U.S. Patent Application No. 10/776,527.
3. Kessler, G., & Shepard, S. (1994). RFC1739: A Primer On Internet and TCP/IP Tools.

2.2.3.8 Model Answers to Self -Assessment

What are Network protocols?

Network protocols are a set of rules, conventions, and data structures that dictate how devices exchange data across networks.

Illustrate how network protocols work using the OSI model.

The OSI model splits the communication process between two network devices into 7 layers. A task or group of tasks is assigned to each of these 7 layers. All the layers are self-contained, and the tasks assigned to them can be executed independently.

What is ARP and which two terms are associated with this protocol?

ARP stands for Address Resolution Protocol. ARP is a network layer protocol which is used to find the physical address from the IP address.

The two terms are mainly associated with the ARP Protocol:

- ***ARP request:*** *When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.*
- ***ARP reply:*** *Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header*

What is a Network Operating System?

A network Operating system is one of the important type of operating system. Network Operating System runs on a server and gives the server the capability to manage data, users, groups, security, applications, and other networking functions. The basic purpose of the network operating system is to allow shared file and printer access among multiple computers in a network, typically a local area network (LAN), a private network or to other networks.

Illustrate some examples of network operating systems

True network operating systems are categorized as software that enhances the functionality of operating systems by providing added network features. A few examples of these network operating systems and their service providers are:

- *Artisoft's LANtastic- This is a simple, user-friendly NOS that supports most PC operating systems.*
- *Banyan's VINES- This uses a client-server architecture to request specific functions and services.*
- *Novell's NetWare- This was the first network operating system to be released and is designed based on XNS protocol architecture.*

- *Microsoft's LAN Manager- This operates as a server application and was developed to run under the Microsoft OS. Now, most of the functionality of LAN Manager is included in the Windows OS itself*

2.2.4 Learning Outcome 4: Configure LAN Network Types

2.2.4.1 Introduction to the learning outcome

This learning outcome covers the procedures to assemble prerequisite components and medium, connecting to establish the network, configuring individual network components, and configuring network protocols.

2.2.4.2.1 Performance Standard

2.2.4.2.2 Devices for LAN network configuration are identified.

2.2.4.2.3 Connection of the devices in LAN is done.

2.2.4.2.4 Configuration of the LAN network is done.

2.2.4.3 Information Sheet

How to setup and configure a Local Area Network

A LAN (Local Area Network), allows connected computers and devices to talk to each other and access the internet. They are smaller networks, usually within an office base. LAN is used to connect computing resources, typically inside one building. The computing resources can be computers, printers, servers, IP phones, or routers. Connections between the workstations are physical, with cables, and all the office resources are shared and distributed between the network workstations. The most common type of LAN is that of Ethernet. This is a family of frame-based computer networking technologies for LANs.

What You Need While Setting up LAN Network

While setting up a Local Area Network, you will need a cable router**,** Crossover Ethernet cables**,** Ethernet cables**,** Ethernet switch**,** and Network interfaces.

Determining Your Network Needs

When setting up a LAN, you'll need to know how many computers will be connecting to the network via Ethernet. This will determine the number of ports you'll need.

1. If you have four or less computers that you need to hardwire, you'll just need a router. If you have more than four, you'll likely need to get a switch to extend the number of ports available on your router.
2. If you want to allow devices to connect wirelessly, you'll need a router that can broadcast a wireless network. Most routers you'll find at the store or online have wireless capabilities. Network switches do not allow wireless devices to connect, and can only be used for hardwired LANs or to extend the number of ports available to the router.
3. If you want all of the connected devices to have access to the internet, you'll need a router to handle the connections. If you don't need the devices to have a network connection, you can just use a network switch.
4. Measure the distances for all hardwired devices**.** This isn't much of an issue in most homes, but network cables cannot run longer than 100m (328 ft). If you have to run cable farther than this, you'll need switches in between.

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.

1. 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.
2. 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.

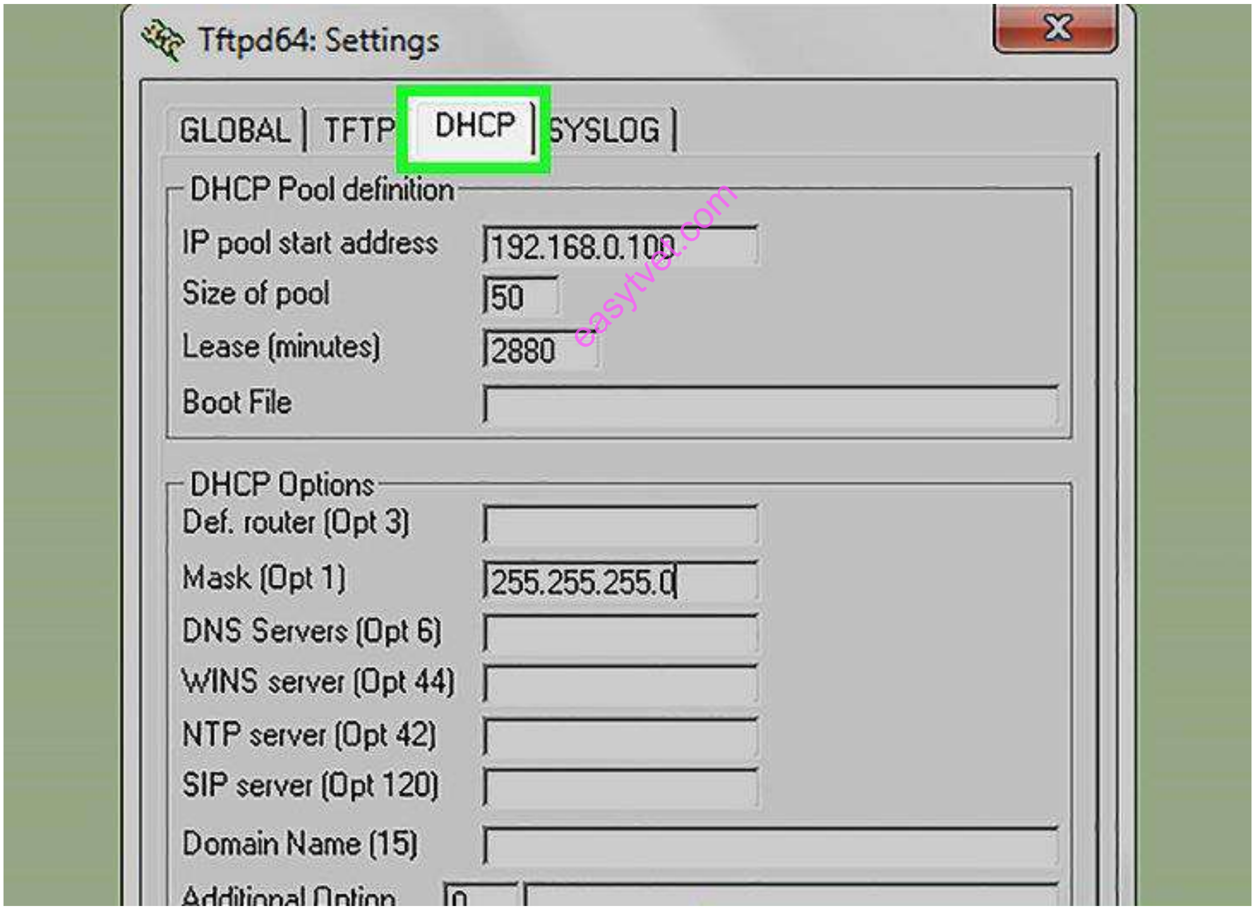
You don't need to do much to set up a router for a basic LAN. Just plug it into a power source, preferably close to your modem if you plan on sharing the internet connection through it.

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 color 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.



DHCP Pool definition
IP pool start address 192.168.0.100
Size of pool 50
Lease (minutes) 2880
Boot File

DHCP Options
Def. router (Opt 3)
Mask (Opt 1) 255.255.255.0
DNS Servers (Opt 6)
WINS server (Opt 44)
NTP server (Opt 42)
SIP server (Opt 120)
Domain Name (15)
Additional Option 0

Figure 55: Connect switch

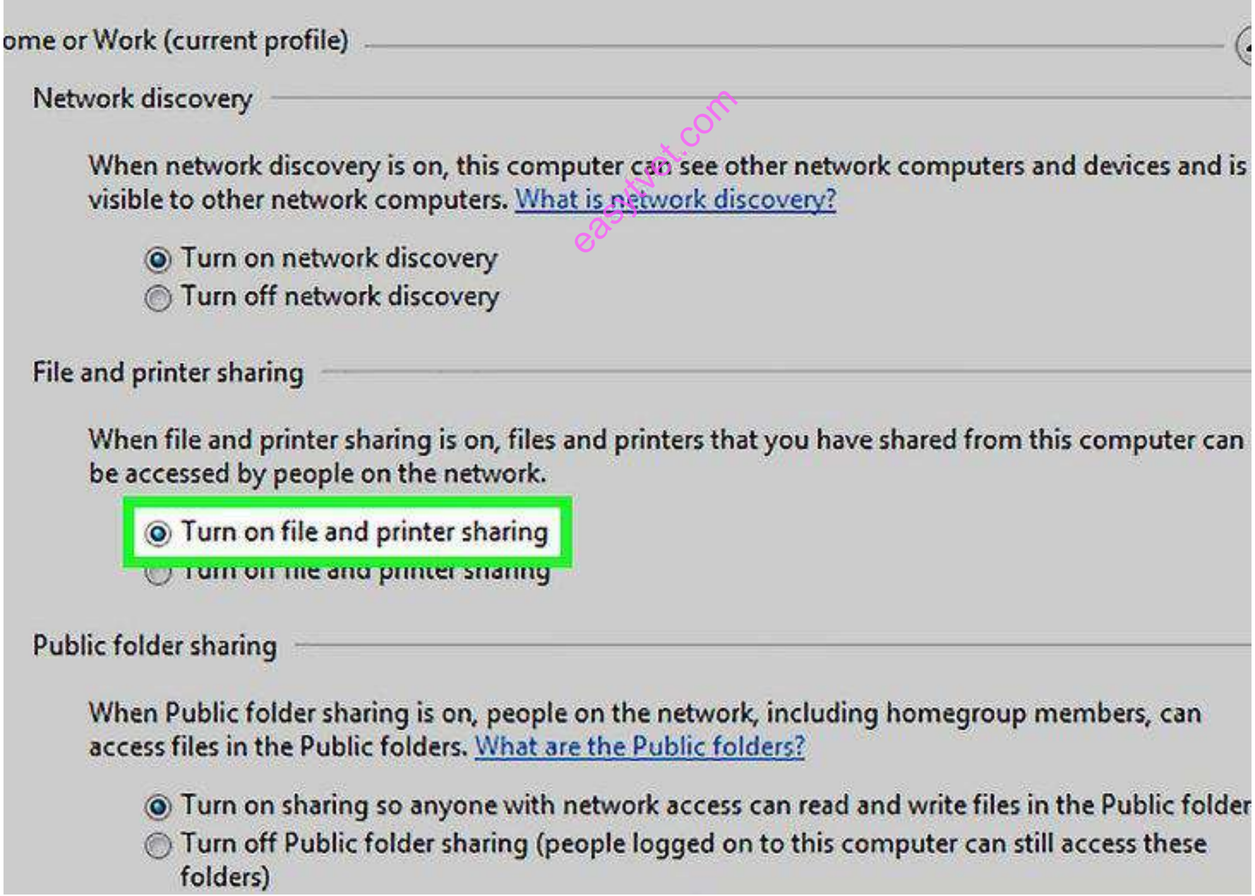
Setup one PC as a DHCP server if you're just using a switch.

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 by installing a third-party utility.
- 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.



ome or Work (current profile)

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. What is network discovery?

● Turn on network discovery
○ Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

● Turn on file and printer sharing
○ Turn off file and printer sharing

Public folder sharing

When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders. What are the Public folders?

● Turn on sharing so anyone with network access can read and write files in the Public folder
○ Turn off Public folder sharing (people logged on to this computer can still access these folders)

Figure 56: Verify network connection

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. You can designate files, folders, drives, printers, and other devices as shared so that anyone on the network, or just specific users, can access them.

Creating a Wireless Network

Set up your router.

When you're setting up a wireless router, you'll need to keep a few things in mind:

- For easy troubleshooting, the router should usually be placed close to your modem.
- It should be located centrally to allow for maximum wireless coverage.
- You'll need to connect a computer to the router via Ethernet during the setup process.

Plug a computer into one of the router's LAN ports.

You'll be using your computer's web browser to configure the router's wireless network

Open a web browser on your computer.

You can use any web browser.

Type in the router's IP address.

You can typically find this printed on the bottom of the router, or in your router's documentation. If you can't find it, there are a couple things you can try:

- Windows - Right-click the Network button in the System Tray → click Open Network and Sharing Center → click the Ethernet link → click Details → find the Default Gateway entry for your router's IP address.
- Mac - Click the Apple menu and select System Preferences → click Network → click your Ethernet connection → find the Router entry for your router's IP address.

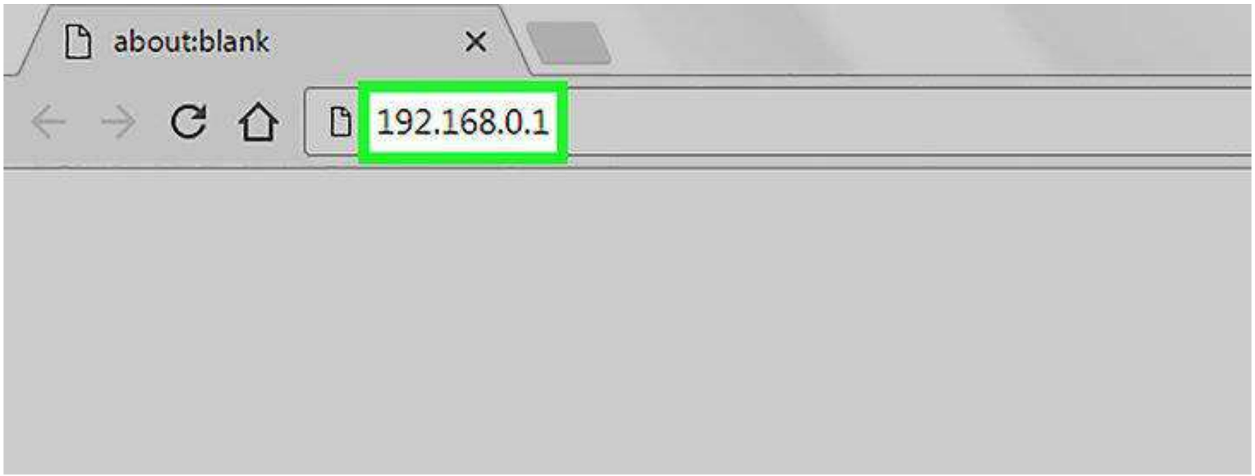
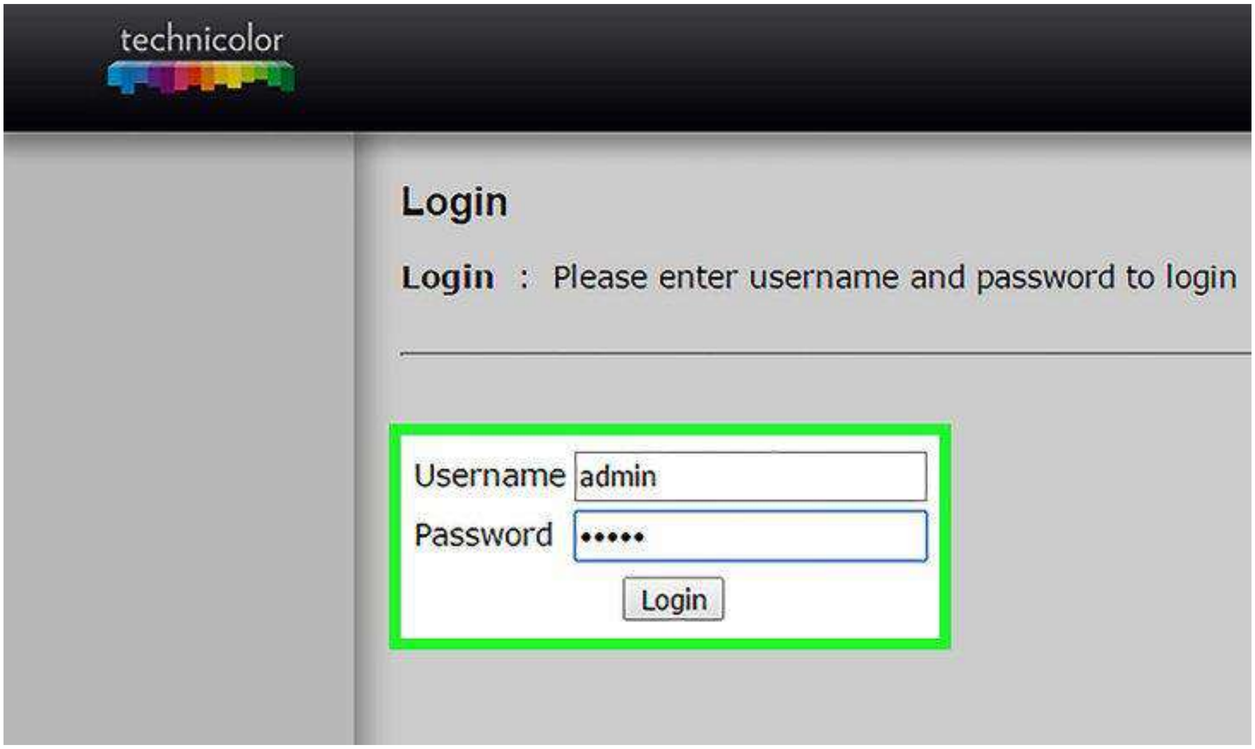


Figure 57: Router IP address

Log in with the administrator account.

You'll be prompted for the login information for your router. The default login information varies depending on your router model, but the username is often "admin" and the password is often "admin," "password," or blank.

- You can look up your router model at https://portforward.com/router-password/ to find the default login information.



Login

Login : Please enter username and password to login

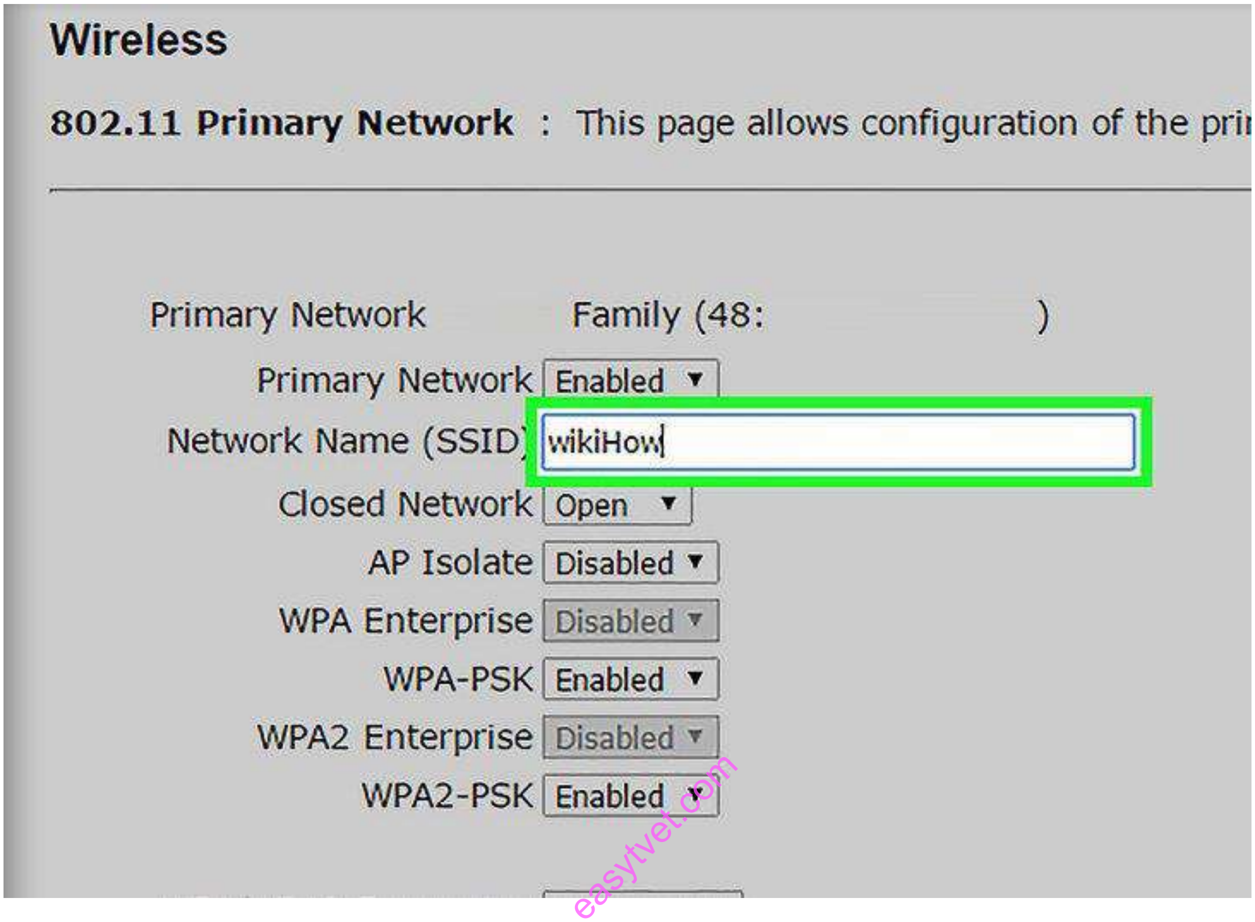
Username admin

Password •••••

Figure 58: Login to router

Open the Wireless section of the router settings.

The exact location and wording of this section varies from router to router.



Wireless

802.11 Primary Network : This page allows configuration of the pri

Primary Network Family (48:)

Primary Network Enabled ▼

Network Name (SSID) wikiHow

Closed Network Open ▼

AP Isolate Disabled ▼

WPA Enterprise Disabled ▼

WPA-PSK Enabled ▼

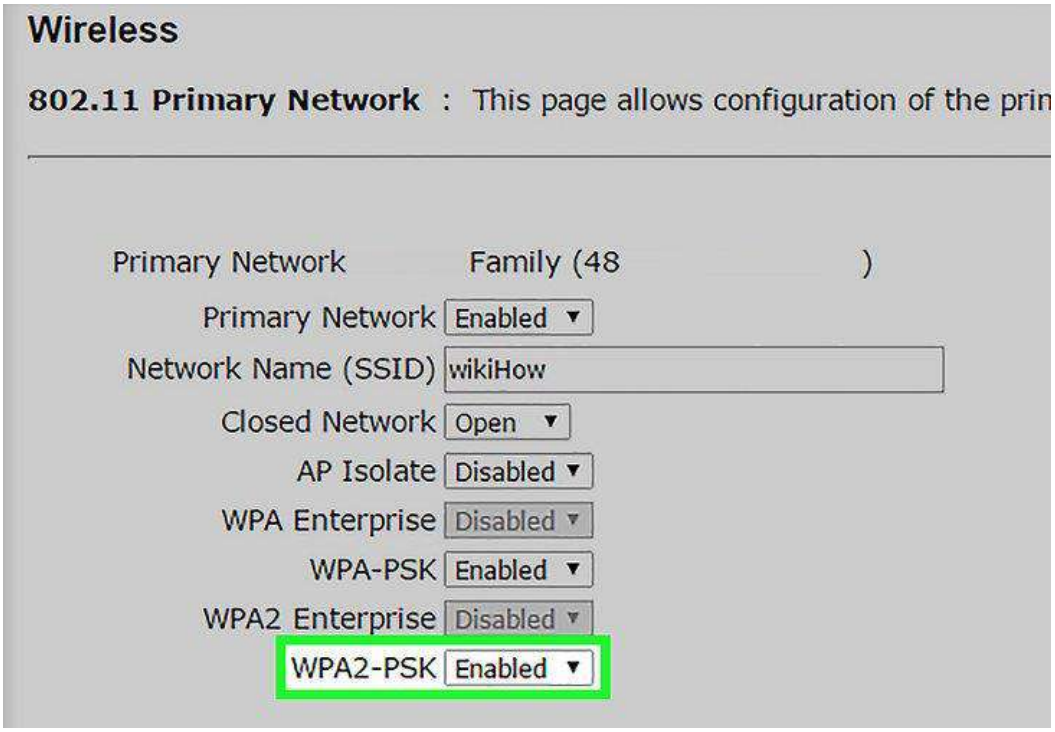
WPA2 Enterprise Disabled ▼

WPA2-PSK Enabled ▼

Figure 59: wireless router setup

Change the name of your network in the SSID field.

This may also be called "Network name." This is the name that appears in the list of available wireless networks



Wireless

802.11 Primary Network : This page allows configuration of the prin

Primary Network Family (48)

Primary Network: Enabled ▼

Network Name (SSID): wikiHow

Closed Network: Open ▼

AP Isolate: Disabled ▼

WPA Enterprise: Disabled ▼

WPA-PSK: Enabled ▼

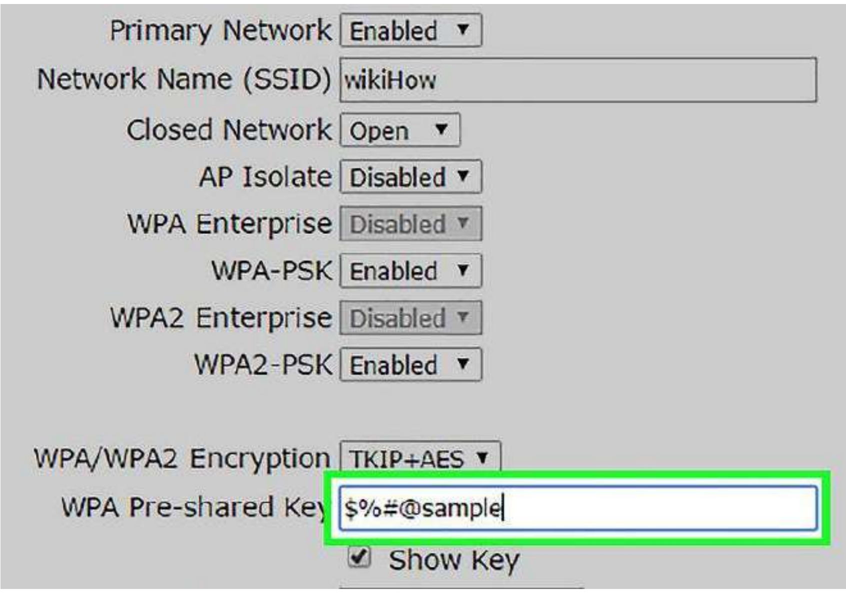
WPA2 Enterprise: Disabled ▼

WPA2-PSK: Enabled ▼

Figure 60: wireless router security settings

Select WPA2-Personal as the Authentication or Security option.

This is the most secure option currently available on most routers. Avoid WPA and WEP except when explicitly required by older, incompatible devices.



Primary Network: Enabled ▼

Network Name (SSID): wikiHow

Closed Network: Open ▼

AP Isolate: Disabled ▼

WPA Enterprise: Disabled ▼

WPA-PSK: Enabled ▼

WPA2 Enterprise: Disabled ▼

WPA2-PSK: Enabled ▼

WPA/WPA2 Encryption: TKIP+AES ▼

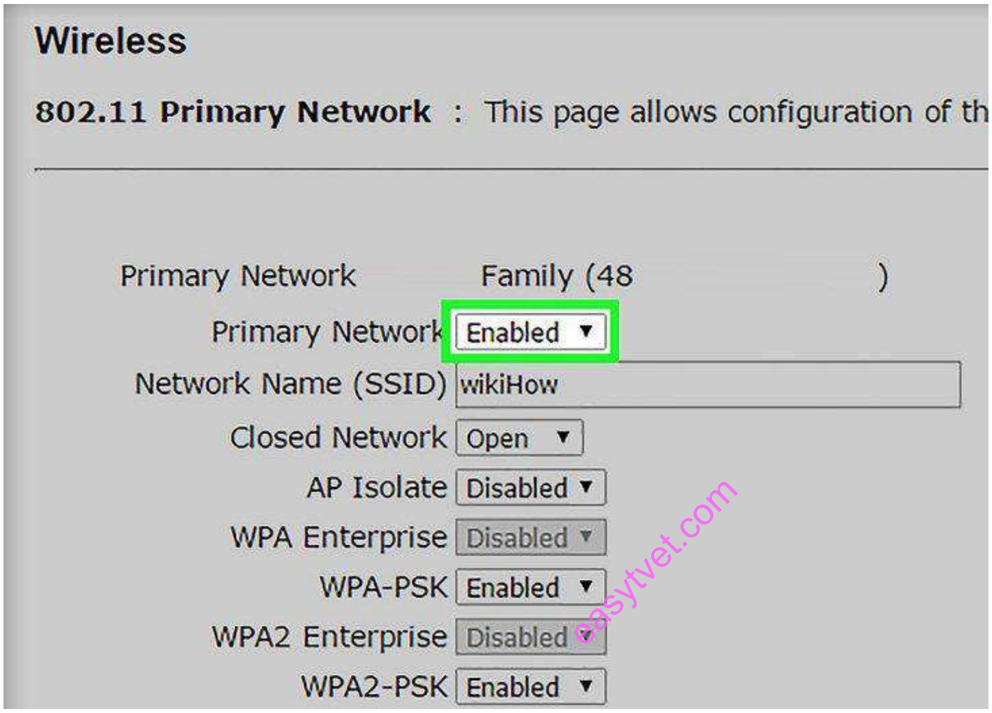
WPA Pre-shared Key: $%#@sample

☑ Show Key

Figure 61: Wireless router key setup

Create a strong password.

This password will be required in order to connect to the network. The field may be labeled "Pre-Shared Key."



Wireless

802.11 Primary Network : This page allows configuration of th

Primary Network Family (48)

Primary Network Enabled ▾

Network Name (SSID) wikiHow

Closed Network Open ▾

AP Isolate Disabled ▾

WPA Enterprise Disabled ▾

WPA-PSK Enabled ▾

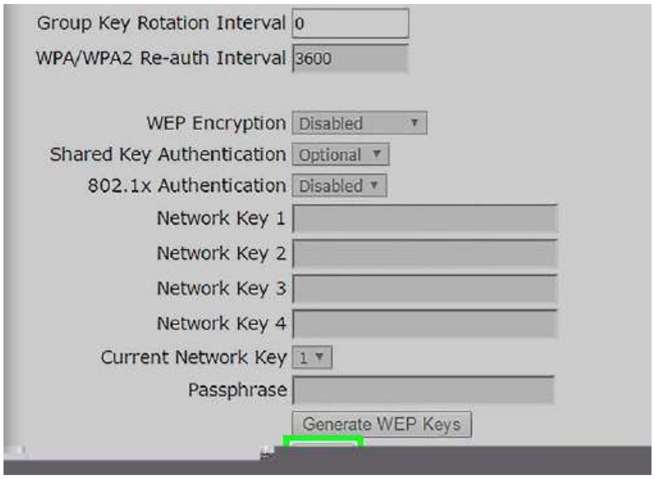
WPA2 Enterprise Disabled ▾

WPA2-PSK Enabled ▾

Figure 62: Router configuration

Ensure the wireless network is enabled.

Depending on the router, you may have to check a box or click a button at the top of the Wireless menu to enable the wireless network.



Group Key Rotation Interval	0
WPA/WPA2 Re-auth Interval	3600
WEP Encryption	Disabled
Shared Key Authentication	Optional
802.1x Authentication	Disabled
Network Key 1	
Network Key 2	
Network Key 3	
Network Key 4	
Current Network Key	1
Passphrase	

Figure 63: Router authentication

Click the Save or Apply button.

This will save the changes to your router.

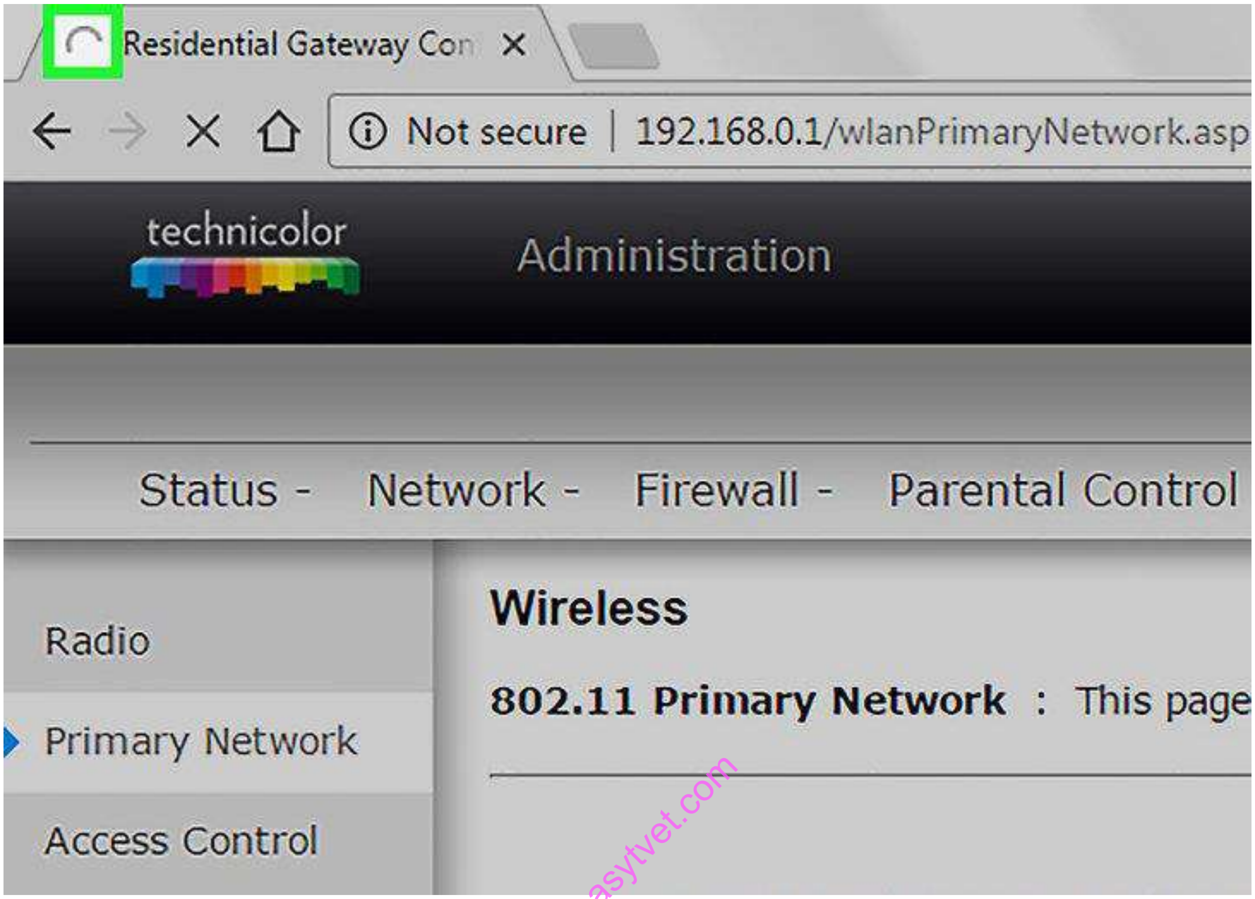


Figure 64: wireless router settings

Wait while your router restarts.

It may take a minute for the router and network to come back online

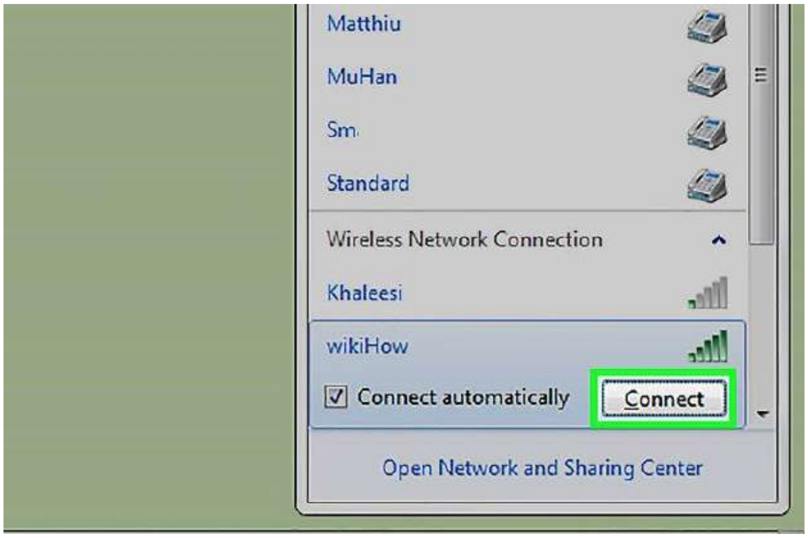


Figure 65: connect to wireless router

Connect to the wireless network on your wireless devices.

Once the network is back up, it will appear on the available network list on any wireless devices in range. When connecting to the network, users will be prompted to enter the password you created.

- Computers connected to the router via Ethernet will not require a password.

2.2.4.4 Learning Activities

The trainee is required to set up one computer as a DHCP (Dynamic Host Configuration Protocol) server and configure all of the connected computers to obtain IP addresses.

Setup a wireless network using a router.

Special instructions

Use a switch as your network hub, 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.

2.2.4.5 Self-Assessment

1. What do you Need While Setting up LAN Network?
2. To create a LAN, why do you need a router or switch?
3. How do you Setup one PC as a DHCP server if you're just using a switch.

4. When you're setting up a wireless router, what are the three things you'll need to keep in mind?
5. Why is it necessary to select WPA2-Personal as the Authentication or Security option?

2.2.4.6 Tools, Equipment, Supplies and Materials

Tools

1. Network tool kit
2. Signal testers

Equipment

- Computer
- Cables
- Switches
- Routers/modem
- Bridges
- Repeaters
- Fibre modules
- Antistatic gloves
- Ports
- RJ45
- NIC
- Gateways
- Microwave dishes

Materials and supplies

Consumables for maintaining Network including:

- RJ45
- Fibre Modules
- Cables

Replacement parts including:

- Points
- Switches
- Routers

- NIC
- Modem
- Cables

Cleaning materials;

Hand cleaner.

2.2.4.7 References

1. Brooks, R. R. (2014). *Introduction to computer and network security: navigating shades of gray*. Boca Raton ; London: CRC Press, Taylor & Francis Group.

2. Haeder, A. (2004). *Conducting the Network Administrator Job Interview: IT Manager Guide with Cisco CCNA Interview Questions* (Vol. 4). Rampant TechPress.

3. Pelle, I., Lévai, T., Németh, F., & Gulyás, A. (2015, June). *One tool to rule them all: A modular troubleshooting framework for sdn (and other) networks. In Proceedings of the 1st ACM SIGCOMM Symposium on Software Defined Networking Research.*

4.https://www.tutorialspoint.com/microwave_engineering/microwave_engineering_components.htm

5. https://en.wikipedia.org/wiki/Wireless_network#Underlying_technology

6. https://www.tutorialspoint.com/Wireless-Networks

2.2.4.8 Model answers to self-assessment

What do you Need While Setting up LAN Network?

*While setting up a Local Area Network, you will need a cable router***,** *Crossover Ethernet cables***,** *Ethernet cables***,** *Ethernet switch***,** *and Network interfaces.*

To create a LAN, why do you need a router or switch?

- *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 route*r

How do you 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 by installing a third-party utility.*
- *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.*

When you're setting up a wireless router, what are the three things you'll need to keep in mind?

- *For easy troubleshooting, the router should usually be placed close to your modem.*
- *It should be located centrally to allow for maximum wireless coverage.*
- *You'll need to connect a computer to the router via Ethernet during the setup process.*

Why is it necessary to select WPA2-Personal as the Authentication or Security option?

This is the most secure option currently available on most routers. Avoid WPA and WEP except when explicitly required by older, incompatible devices

2.2.5 Learning Outcome 5: Perform Network Testing

2.2.5.1 Introduction to the learning outcome

This learning outcome covers outline of a network test plan, demonstration of network testing tools, testing network components, entire network testing, and generating a network test report.

2.2.5.2 Performance Standard

2.2.5.2.1 Testing tools are assembled

2.2.5.2.2 Network components are tested

2.2.5.2.3 Testing of connectivity medium between components is done

2.2.5.2.4 Network testing is done

2.2.5.2.5 Testing report is generated

2.2.5.3 Information Sheet

a) Creating a Network Test Plan

To prepare a plan to test the network. The plan defines the scope, approach, criteria, schedule, responsibilities, resources, and procedures.

i. Define Objectives

Define the objectives of the test by identifying the areas of the network to be tested including:

- Volume Testing. Ensures that the network operates smoothly when subjected to production volumes of data over long periods of time.

- Stress Testing. Ensures that the network operates smoothly when subjected to the maximum load expected in production, all at one time. A good rule of thumb is to subject the network to 25 percent more data and processing than is expected during peak loads.
- Recovery Testing. Ensures that backup and recovery procedures are working properly.
- Security Testing. Verifies that the network meets the security requirements.
- Performance Testing. Verifies that performance criteria are met (e.g., response times).

ii. Define Acceptance Criteria

For each test objective, define the criteria for successful completion. For example:

- All expected results are achieved on the initial run.
- All severe, and high priority faults are corrected and the associated test(s) rerun successfully.
- A documented plan is put in place specifying how and when outstanding low and medium priority faults will be resolved.

iii. Define Schedule

Identify the high-level activities and tasks together with expected start and completion dates.

iv. Define Responsibilities

Identify the individuals who will be involved in the test and their roles and responsibilities.

v. Define Resources

Identify the staff, hardware, and software requirements. Confirm that the Network Deployment Plan has accounted for these requirements and resolve any differences.

vi. Define Procedures

Define the procedures to be followed in preparing the test cases, preparing test scripts, preparing the test environment, conducting tests, and verifying test results.

vii. Tips and Hints

Document any assumptions made while preparing the plan.

Plan to use automated test tools wherever possible to significantly reduce the testing effort and duration. Automated test tools can be used to generate and apply an adequate number of transactions to facilitate stress and performance testing.

b) Network Performance Testing Tools

Whenever you suspect something wrong with the performance of a network, your best course of action is to run some tests to confirm that there is indeed an issue and also to help you locate it and, eventually, fix it. There are many network performance testing tools available. So many that picking the one that is the best fit for your specific need can turn out to be a hefty challenge.

c) What is network performance?

Network performance refers to measures of service quality of a network as seen by the customer". There are three essential elements to that definition. The first is the *measures* part. It established clearly that network performance is something one has to measure. The next important bit is the *service quality* of a network. Service quality is a generic concept but, as you'll see, a few specific metrics are associated with it. The last important part is the customer. We're not interested in network performance as a theoretical thing. What we need to measure is the true user experience.

Several different factors affect perceived network performance and are generally considered important. The first two are bandwidth and throughput but there is often some confusion between these two terms. Bandwidth refers to the carrying capacity of a network. As an analogy, think of it as the number of lanes in a highway. Throughput, on the other hand, refers to the actual usage of the available bandwidth. To keep our previous analogy, a four-lane highway has a bandwidth of 4 000 vehicles per hour but its current throughput could be only 400 vehicles per hours or 10% of its capacity.

Latency, delay, and jitter are more factor affecting the perceived performance of networks. Latency refers to the time data takes to travel from source to destination. It is mainly a function of the signal's travel time and processing time at any nodes it traverses. It is a physical limitation that cannot be reduced. Delay, on the other hand, can sometimes be improved. It has to do with the time it takes for networking equipment to process, queue, and forward data. Faster, more powerful equipment will generally add less delay to the transmission. As for jitter, it refers to the variation in packet delay at the receiving end of the conversation. Real-time or near-real-time traffic is particularly affected by it as it can cause data packets to arrive out of sequence. In the case of voice over IP, for example, this could result in unintelligible speech.

Many other factors can also affect network performance. The error rate is one of them. It refers to the number of corrupted bits expressed as a percentage or fraction of the total sent.

d) Testing the Network

How does one go about measuring performance from a true user's perspective? Well, there is, of course, the possibility of having real users running tests but this can tend to be rather impractical. The next best thing is using a network performance testing system that uses probes deployed at strategic location throughout your network and that can run actual simulation tests between each other to measure true performance using specific types of traffic. This, however, can also tend to be impractical as it requires some preliminary setup. It won't be of much assistance to help troubleshoot a sudden issue.

In these cases, what you need is a quick and dirty solution. A simple application that you can quickly deploy or install at either end of the segment you need to test and that will let you manually configure and run simulation tests.

e) Testing vs monitoring

Another important distinction to be made is the one between performance monitoring and performance testing. These are two similar concepts but there are a few differences. The basic idea is the same: simulating real user traffic and measuring the actual performance of the network. Where it differs is in how and when it is done. Monitoring systems run constantly and perform recurring tests between preconfigured locations and using predefined simulation models. A dashboard will typically be available to display the latest test results and reports can often be generated for various purposes.

Testing is different in that it is typically an ad-hoc process that is run manually whenever a problem is reported or suspected. Tests are also typically run between two specific points on the network where one suspects a problem is. The test will often help identify and pinpoint the problem.

f) Network testing tools

i. Clamp Meter

A clamp meter is an electrical test tool that combines a basic digital multimeter with a current sensor.

Clamps measure current. Probes measure voltage. Having a hinged jaw integrated into an electrical meter allows technicians to clamp the jaws around a wire, cable or other conductor at any point in an electrical system, then measure current in that circuit without disconnecting/deenergizing it.

Beneath their plastic moldings, hard jaws consist of ferrite iron and are engineered to detect, concentrate and measure the magnetic field being generated by current as it flows through a conductor.

ii. Voltmeter

A voltmeter is an instrument used for measuring electric 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.

iii. Cable Tester/ Signal Tester

A cable tester is a device used to test the strength and connectivity of a particular type of cable or other wired assemblies. There are many different types of cable testers. Each of them can test a specific type of cable or wire (some may be able to test different types of cables or wires). A cable tester can test whether a cable or wire is set up properly, connected correctly, and the signal strength between the source and destination.

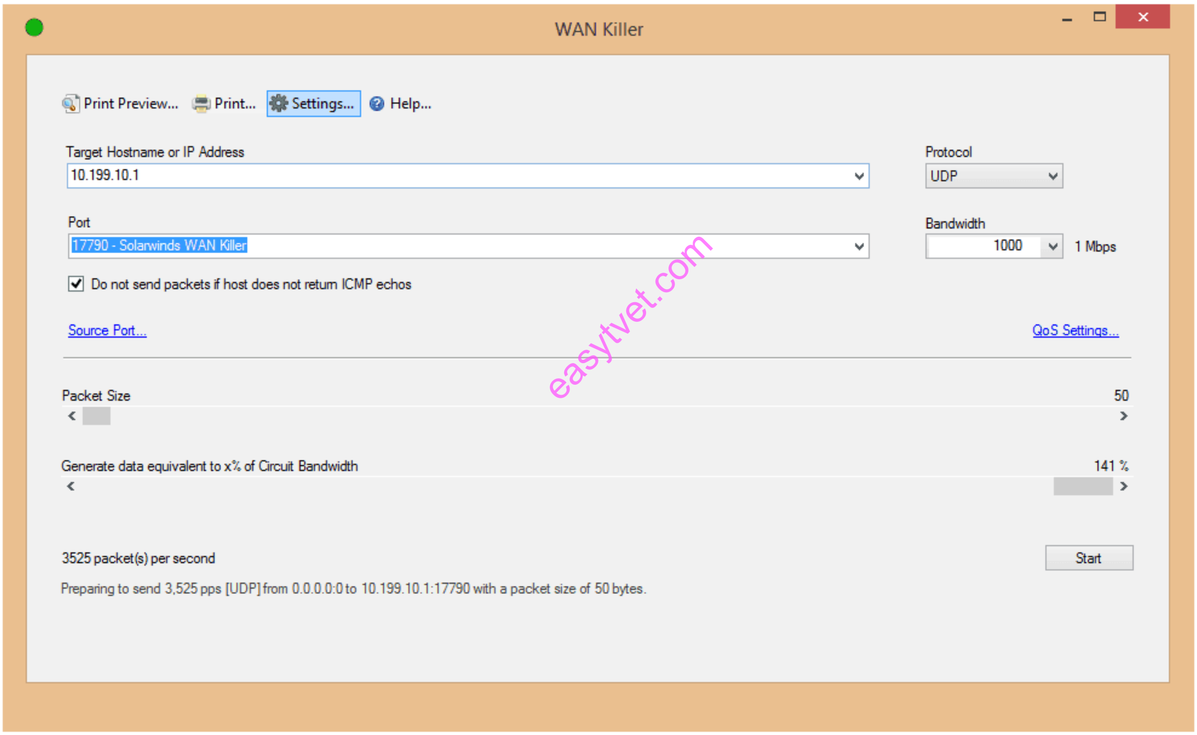
g) Some network performance network utilities

1. SolarWinds WAN Killer (Part Of The Engineer's Toolset)

SolarWinds is a common name in the field of network administration. The company is famous for making some of the best network administration tools on the market. Its flagship product, the *Network Performance Monitor* is generally recognized as one of the best network bandwidth monitoring tools available. And as if it wasn't enough, *SolarWinds* has also gifted us with several free tools, each addressing a specific need of network administrators. Such tools include the famous SolarWinds TFTP Server and the Advanced Subnet Calculator.

Although it’s not a network performance testing tool per se, the **WAN Killer Network Traffic Generator** can be very useful in combination with other tools. Its sole purpose is generating network traffic. It allows administrators to use other performance testing tools for testing performance under high traffic situations, something that not many tools do by themselves.

The tool, which is part of the SolarWinds Engineer’s Toolset, will let you easily set the IP address and hostname you want to send the random traffic to. It will also let you specify parameters such as port numbers, packet size, and percentage of bandwidth to use. It can even let you modify the Differentiated Services Code Point (DSCP) and Explicit Congest Notification (ECN) settings.



Target Hostname or IP Address: 10.199.10.1

Protocol: UDP

Port: 17790 - Solarwinds WAN Killer

Bandwidth: 1000 1 Mbps

☑ Do not send packets if host does not return ICMP echos

Packet Size: 50

Generate data equivalent to x% of Circuit Bandwidth: 141 %

3525 packet(s) per second

Preparing to send 3,525 pps [UDP] from 0.0.0.0:0 to 10.199.10.1:17790 with a packet size of 50 bytes.

Figure 66 An official download link has been provided below

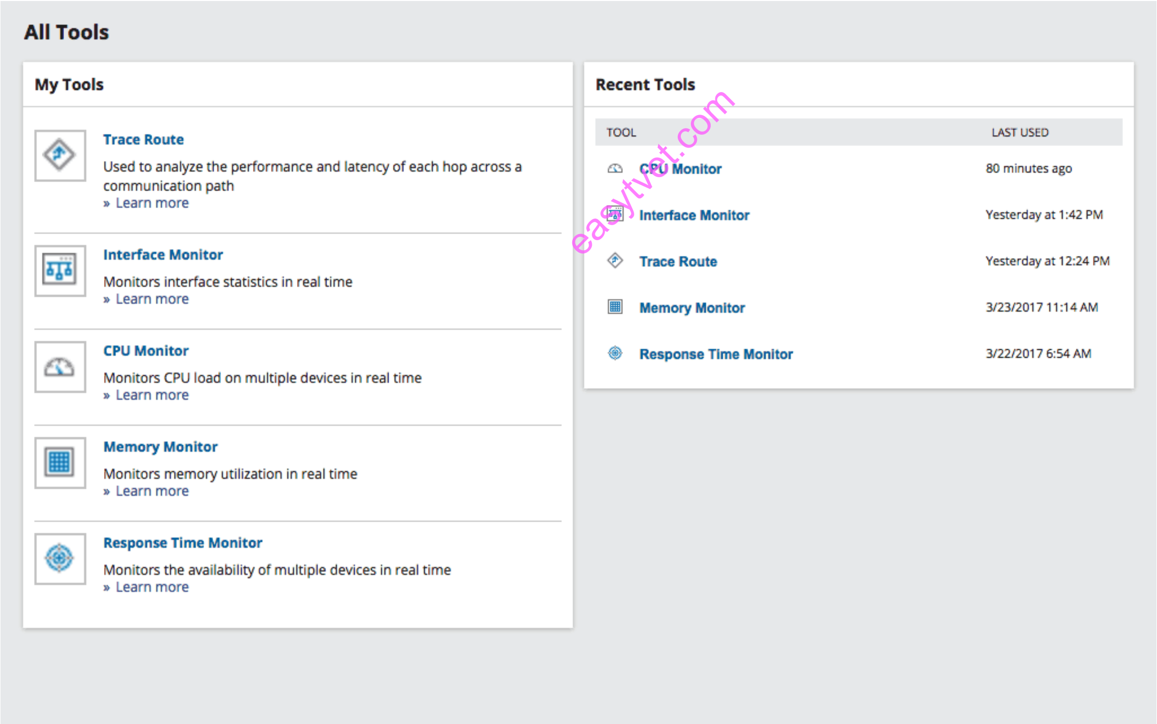
- **Official download link: https://www.solarwinds.com/engineers-toolset/registration**

This tool’s primary use is for tasks such as testing traffic prioritization and load balancing. You can also use it to make sure that your network is correctly set up and that huge amounts of unimportant traffic—as generated by this tool—won’t have adverse effect critical traffic. The level of fine-tuning the tool allows will let you simulate almost any type of situation.

The **SolarWinds WAN Killer Network Traffic Generator** is part of the **Engineer's Toolset**, a bundle of over 60 different tools. The toolset includes a mix of the most important free tools from SolarWinds combined with many exclusive tools that you won't find elsewhere. And most of the included tools are integrated into a common dashboard from where they can be easily accessed.

Other Components Of The SolarWinds Engineer's Toolset

The **SolarWinds Engineer's Toolset** includes several dedicated troubleshooting tools. Tools like Ping Sweep, DNS Analyzer and TraceRoute can be used to perform network diagnostics and help resolve complex network issues quickly. For the security-oriented administrators, some of the toolset's tools can be used to simulate attacks and help identify vulnerabilities.



All Tools

My Tools

Trace Route
Used to analyze the performance and latency of each hop across a communication path
» Learn more

Interface Monitor
Monitors interface statistics in real time
» Learn more

CPU Monitor
Monitors CPU load on multiple devices in real time
» Learn more

Memory Monitor
Monitors memory utilization in real time
» Learn more

Response Time Monitor
Monitors the availability of multiple devices in real time
» Learn more

Recent Tools

TOOL	LAST USED
CPU Monitor	80 minutes ago
Interface Monitor	Yesterday at 1:42 PM
Trace Route	Yesterday at 12:24 PM
Memory Monitor	3/23/2017 11:14 AM
Response Time Monitor	3/22/2017 6:54 AM

Figure 67: Solarwinds toolset

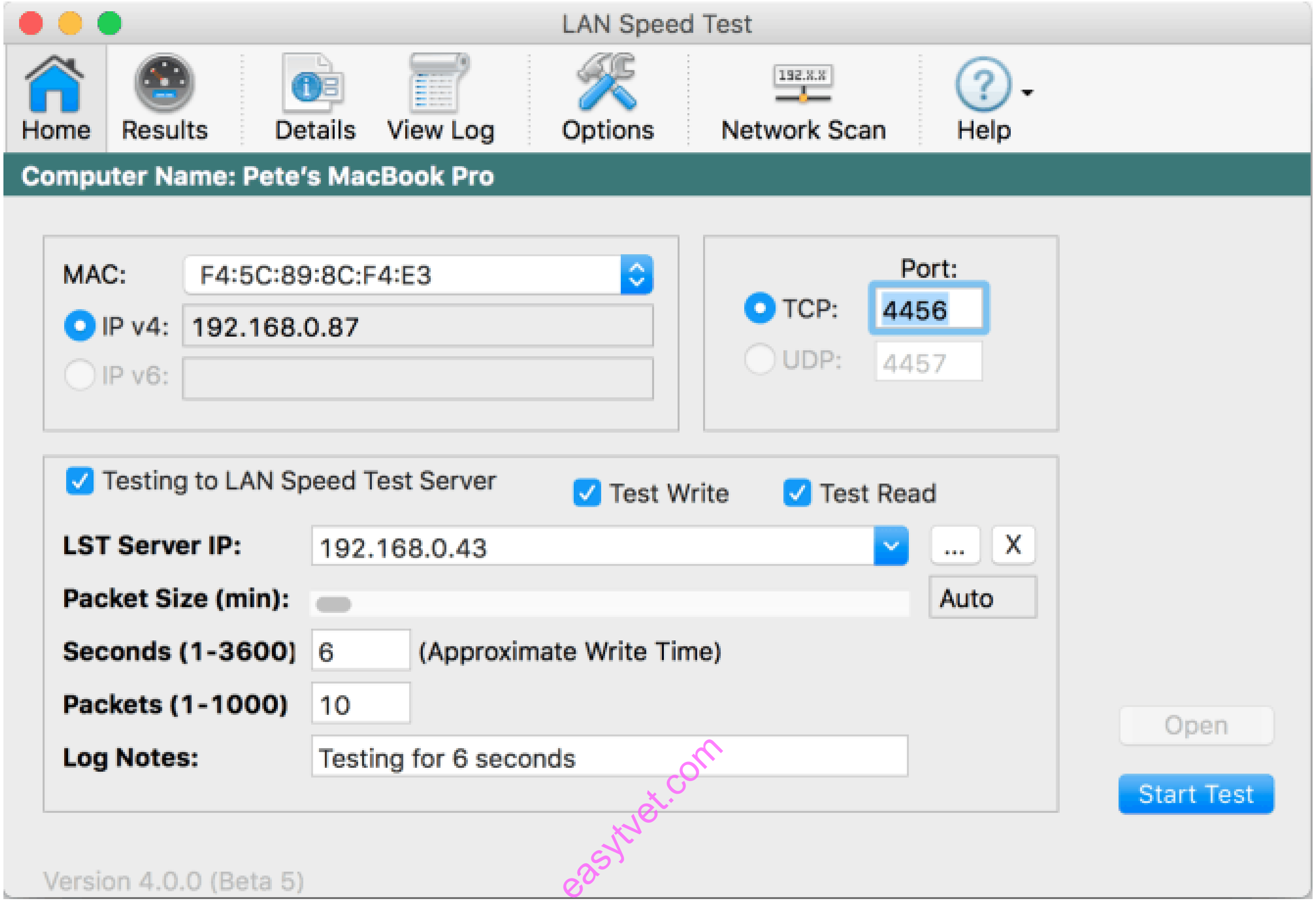
The toolset also features some excellent monitoring and alerting capabilities. Some of its tools will monitor your devices and raise alerts for availability or health issues. And finally, you can use some of the included tools for configuration management and log consolidation.

Here's a list of some of the other tools you'll find in the **SolarWinds Engineer's Toolset**:

- Port Scanner
- Switch Port Mapper
- SNMP sweep
- IP Network Browser
- MAC Address Discovery
- Ping Sweep
- Response Time Monitor
- CPU Monitor
- Memory Monitor
- Interface Monitor
- TraceRoute
- Router Password Decryption
- SNMP Brute Force Attack
- SNMP Dictionary Attack
- Config Compare, Downloader, Uploader, and Editor
- SNMP trap editor and SNMP trap receiver
- Subnet Calculator
- DHCP Scope Monitor
- DNS Structure Analyzer
- DNS Audit
- IP Address Management

2. LAN Speed Test

LAN Speed Test from *TotuSoft* is a simple but powerful tool for measuring file transfer, hard drive, USB Drive, and network speeds. All you need to do is pick a destination on the server where you want to test the WAN connection. The tool will then build a file in memory and transfer it both ways while measuring the time it takes. It then does all the calculations for you and gives you an evaluation of the transfer's performance.



Computer Name: Pete's MacBook Pro

MAC: F4:5C:89:8C:F4:E3

● IP v4: 192.168.0.87

○ IP v6:

Port:

● TCP: 4456

○ UDP: 4457

☑ Testing to LAN Speed Test Server ☑ Test Write ☑ Test Read

LST Server IP: 192.168.0.43

Packet Size (min):

Seconds (1-3600) 6 (Approximate Write Time)

Packets (1-1000) 10

Log Notes: Testing for 6 seconds

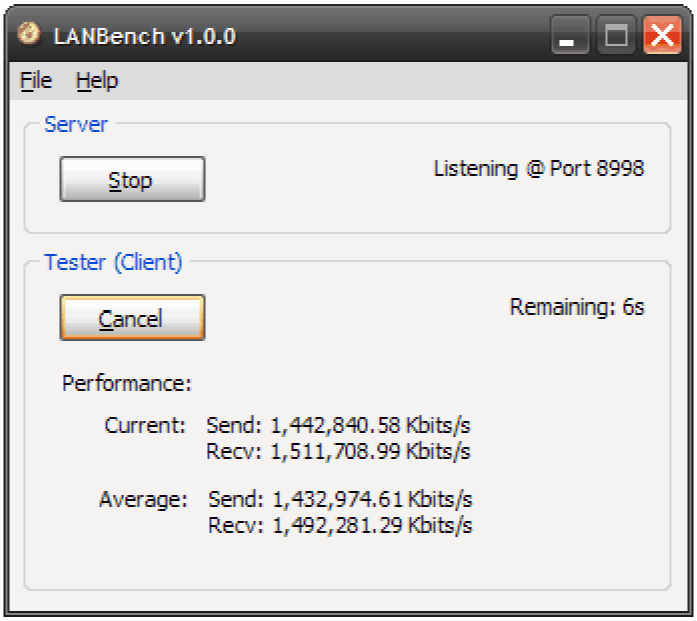
Version 4.0.0 (Beta 5)

Figure 68: LAN Speed Test

You can also choose a computer running the **LAN Speed Test Server** instead of a shared folder as a destination. This effectively takes disk access component out of the equation, giving you a true measure of the network's performance. The tool is initially set up in its *Lite*, feature-limited version. To access the advanced features of the standard version, you must purchase a license which is available for only ten dollars, with quantity discounts available. The tool is portable and will run on any Windows version since Windows 2000.

3. LAN Bench

Despite the fact that its developer's site no longer exists, **LAN Bench** from *Zack Saw* is still readily available for download from several software download websites. It is a free and portable TCP network benchmarking utility. The tool is based on Winsock 2.2, a rather old framework but one with minimal CPU usage. That way, you can be reasonably sure that poor CPU performance won’t come and pollute your network performance test results. All the tool does is test the network performance between two computers but what it does, it does well.



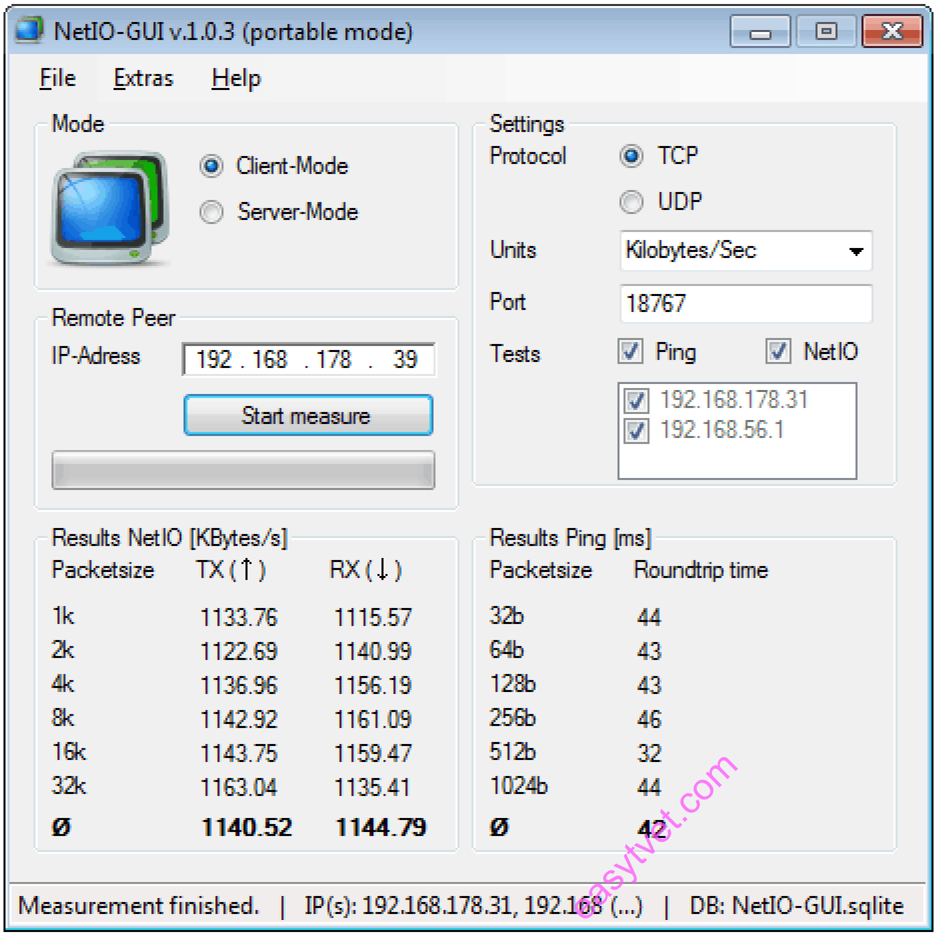
```
Listening @ Port 8998

Remaining: 6s

Performance:
    Current:  Send: 1,442,840.58 Kbits/s
              Recv: 1,511,708.99 Kbits/s

    Average:  Send: 1,432,974.61 Kbits/s
              Recv: 1,492,281.29 Kbits/s
```

Figure 69: LAN Bench

You’ll need to run **LAN Bench** on two computers, at either end of the network segment you want to test. One instance runs as the server and the other one is the client. The server-side requires no configuration. All you need to do is click the *Listen* button. The tool’s testing configuration is all done on the client side, before starting the test. You will need to specify the server’s IP address and you can adjust several testing parameters such as the total duration of the test, the packet size used for testing, as well as the connection and transfer mode.

4. NetIO & NetIO-GUI

NetIO-GUI is actually a free front end for the multi-platform command line utility NetIO. Together, they form a very potent performance testing tool. It can be used to measures ICMP response times as well as network transfer speeds for different packet sizes and protocols. All the results are stored in an SQLite database and can easily be compared. This Windows tool is available either as an installable software or as a portable tool.



Mode

○ Client-Mode (selected)

○ Server-Mode

Remote Peer

IP-Adress 192 . 168 . 178 . 39

Settings

Protocol ● TCP ○ UDP

Units Kilobytes/Sec

Port 18767

Tests ☑ Ping ☑ NetIO

☑ 192.168.178.31

☑ 192.168.56.1

Results NetIO [KBytes/s]

Packetsize	TX (↑)	RX (↓)
1k	1133.76	1115.57
2k	1122.69	1140.99
4k	1136.96	1156.19
8k	1142.92	1161.09
16k	1143.75	1159.47
32k	1163.04	1135.41
Ø	**1140.52**	**1144.79**

Results Ping [ms]

Packetsize	Roundtrip time
32b	44
64b	43
128b	43
256b	46
512b	32
1024b	44
Ø	**42**

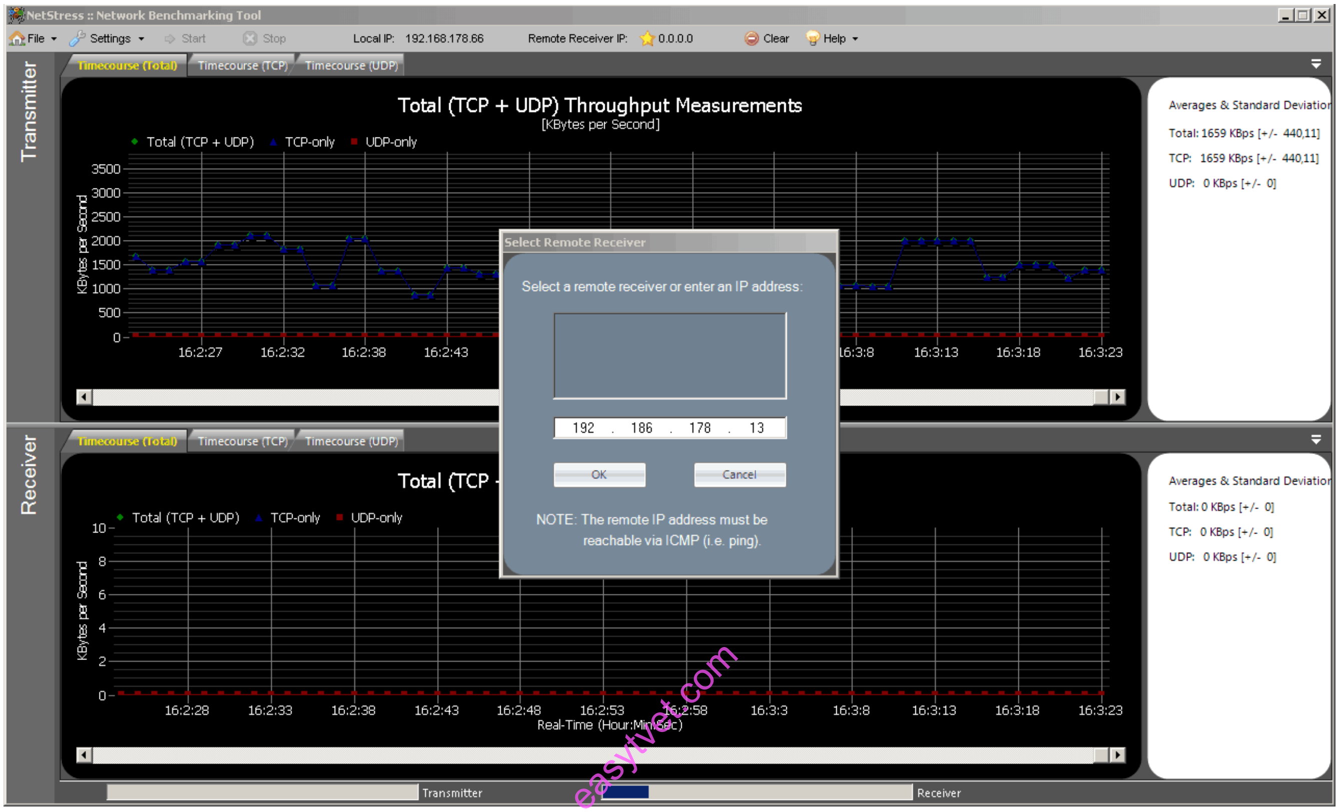
Measurement finished. | IP(s): 192.168.178.31, 192.168 (...) | DB: NetIO-GUI.sqlite

Figure 70: NetIO-GUI

In order to run tests, you need two instances of the tool, one at either end. One side will run in client mode while the other will run in server mode. Using it is rather simple, once you have it running at both ends, you click the start button on the server (typically running at the far end) and, on the client, you simply enter the server's IP address and pick the protocol (TCP or UDP) that you want to use to run the test. You start the test and let NetIO test the connectivity using various packet sizes before it returns the test results.

5. NetStress

Initially created as an internal tool by *Nuts About Nets*, NetStress has since started being offered to the public. It is yet another free and simple network benchmarking tool. Like most other similar products, you'll have to run the tool on two computers at either end of the network that you need to test. It is somewhat easier to use than other tools because it can automatically find the receiver IP address.



Total: 1659 KBps [+/- 440,11]
TCP: 1659 KBps [+/- 440,11]
UDP: 0 KBps [+/- 0]

Total: 0 KBps [+/- 0]
TCP: 0 KBps [+/- 0]
UDP: 0 KBps [+/- 0]

Select Remote Receiver

Select a remote receiver or enter an IP address:

192 . 186 . 178 . 13

OK Cancel

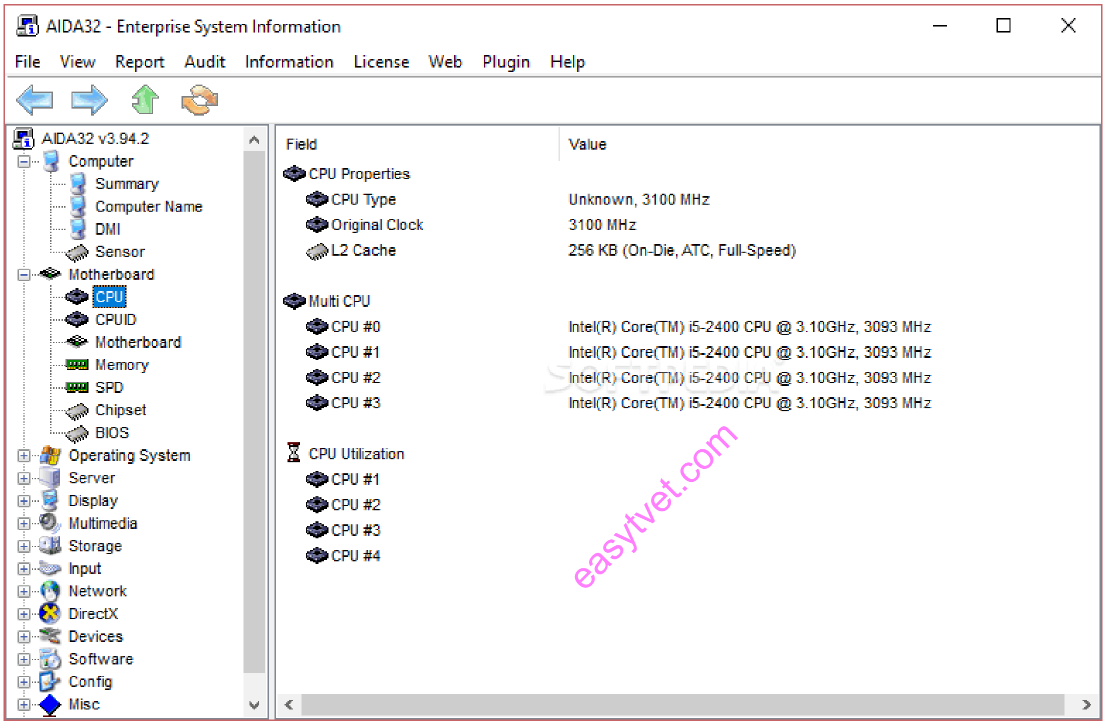
NOTE: The remote IP address must be reachable via ICMP (i.e. ping).

Figure 71: NetStress

Running a test with NetStress is very simple, although some might not find it self-explanatory. What you need to do is click on the 0.0.0.0 next to *Remote Received IP*. You then select the IP address that is listed in the window and click OK. Doing that will enable the *Start* button. Once enabled, you simply click it and the tool starts testing and measuring the TCP and UDP throughput. An interesting option found in this tool the ability to modify the MTU size used for testing. Despite some quirks such as the inability to resize its full-screen window, NetStress is a pretty good tool.

6. Aida32

Aida32 is officially a discontinued product that has been replaced by *Aida64* but this older version still very popular and easy to find. *Aida* is a hardware information and benchmarking tool that can perform many different tests. The reason this specific—and older—version has made it to our list is because it includes an excellent Network Benchmark tool which is no longer available in recent versions. Using the plugin is easy and it can be started from the tool's *Plugin* Menu



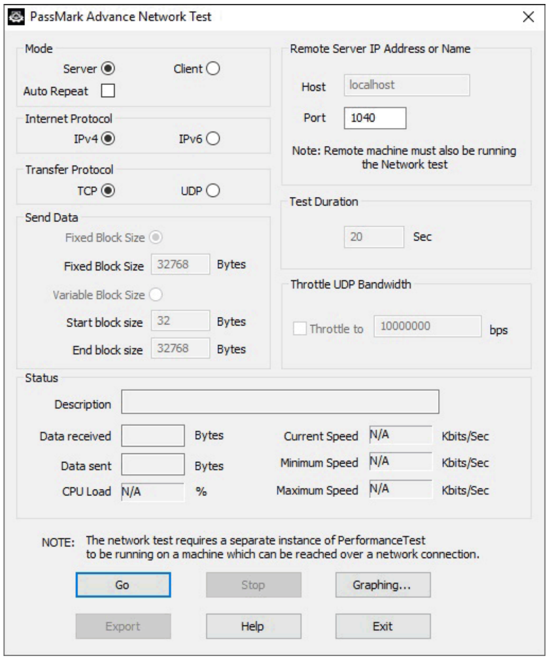
Field	Value
CPU Properties	
CPU Type	Unknown, 3100 MHz
Original Clock	3100 MHz
L2 Cache	256 KB (On-Die, ATC, Full-Speed)
Multi CPU	
CPU #0	Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz, 3093 MHz
CPU #1	Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz, 3093 MHz
CPU #2	Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz, 3093 MHz
CPU #3	Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz, 3093 MHz
CPU Utilization	
CPU #1	
CPU #2	
CPU #3	
CPU #4	

Figure 72: AIDA 32

Aida32 tool is not very diffèrent in its opérations from most others on this list and you'll need to run it at both ends of the path you want to test. On one of the computers, you need to select *Master* from the drop-down list that you'll find at the bottom of the tool's window. You then go to the *Bandwidth* tab and click the Start button. On the other computer, you select *Slave* instead of *Master* and enter the IP address of the master. Just like you did on the master, you go to the *Bandwidth* tab and click *Start*. Once the test completes, the Save button can be used to conveniently save the bandwidth chart in bitmap format.

7. PerformanceTest

Pass Mark’s **Performance Test** is a complete PC performance benchmarking software. It made it to our list because it features a pretty decent advanced network testing tool that one can use to run network performance tests. The too can run tests on both IPv4 and IPv6 networks. Furthermore, it will let users set the data block size used for testing. It will also allow you to enable UDP bandwidth throttling if you so desire. The network module is well-hidden within the **PerformanceTest** application. You can access it by clicking advanced and then Network from the tool’s menu bar.



PassMark Advance Network Test

Mode: Server ● Client ○

Auto Repeat □

Internet Protocol: IPv4 ● IPv6 ○

Transfer Protocol: TCP ● UDP ○

Send Data

Fixed Block Size ●

Fixed Block Size 32768 Bytes

Variable Block Size ○

Start block size 32 Bytes

End block size 32768 Bytes

Remote Server IP Address or Name

Host localhost

Port 1040

Note: Remote machine must also be running the Network test

Test Duration: 20 Sec

Throttle UDP Bandwidth

□ Throttle to 10000000 bps

Status

Description

Data received Bytes

Data sent Bytes

CPU Load N/A %

Current Speed N/A Kbits/Sec

Minimum Speed N/A Kbits/Sec

Maximum Speed N/A Kbits/Sec

NOTE: The network test requires a separate instance of PerformanceTest to be running on a machine which can be reached over a network connection.

Figure 73:PassMArk Advance

2.2.5.4 Learning Activities

- The trainee is required to download **SolarWinds WAN Killer** from the official download link and install the free 14 day trial on their personal computer.
- Using the accompanying and appropriate toolsets, specify parameters such as port numbers, packet size, and percentage of bandwidth to use.

Special instructions

Use only the toolsets available on free trial.

2.2.5.5 Self-Assessment

1. What is network performance?
2. Create a distinction between network testing and network monitoring.

2.2.5.6 Tools, Equipment, Supplies and Materials

Tools

1. Network tool kit
2. Signal testers

Equipment

- Computer
- Cables
- Switches
- Routers/modem
- Bridges
- Repeaters
- Fibre modules
- Antistatic gloves
- Ports
- RJ45
- NIC
- Gateways
- Microwave dishes

Materials and supplies

Consumables for maintaining Network including:

- RJ45
- Fibre Modules
- Cables

Replacement parts including:

- Points
- Switches
- Routers
- NIC

- Modem
- Cables

Cleaning materials;

- Hand cleaner.

2.2.5.7 References

Brooks, R. R. (2014). *Introduction to computer and network security: navigating shades of gray.* Boca Raton ; London: CRC Press, Taylor & Francis Group.

Pelle, I., Lévai, T., Németh, F., & Gulyás, A. (2015, June). One tool to rule them all: A modular troubleshooting framework for sdn (and other) networks. In Proceedings of the 1st ACM SIGCOMM Symposium on Software Defined Networking Research (pp. 1-7).

Chen, C. W. (2005). U.S. Patent Application No. 10/776,527

https://docs.oracle.com/cd/E19504-01/802-5753/planning3-78185/index.html

https://www.practicalnetworking.net/stand-alone/classful-cidr-flsm-vlsm/#vlsm

https://www.vskills.in/certification/tutorial/basic-network-support/a-b-and-c-classes-of-networks/

2.2.5.8 Model answers to self-assessment

What is network performance?

Network performance refers to measures of service quality of a network as seen by the customer". There are three essential elements to that definition. The first is the measures part. It established clearly that network performance is something one has to measure. The next important bit is the service quality of a network. Service quality is a generic concept but, as you'll see, a few specific metrics are associated with it. The last important part is the customer. We're not interested in network performance as a theoretical thing. What we need to measure is the true user experience.

Create a distinction between network testing and network monitoring.

These are two similar concepts but there are a few differences. The basic idea is the same: simulating real user traffic and measuring the actual performance of the network. Where it differs is in how and when it is done. Monitoring systems run constantly and perform recurring tests between preconfigured locations and using predefined simulation models. A dashboard will *typically be available to display the latest test results and reports can often be generated for various purposes.*

Testing is different in that it is typically an ad-hoc process that is run manually whenever a problem is reported or suspected. Tests are also typically run between two specific points on the network where one suspects a problem is. The test will often help identify and pinpoint the problem.