What is a computer network?

- Series of computers connected together.
- Consists of hardware and software to allow computers and other devices to communicate.
- Networks can be wired or wireless.
- There are different types of computer networks.

Hardware used in a network?

- **Gateway**-this device is placed at a network node and interfaces with another network that uses different protocols.
- **Router**-a specialized network device that determines the next network point to which it can forward a data packet towards the ultimate destination of the packet. Unlike a gateway, it cannot interface different protocols.
- **Hub**-a device that connects multiple Ethernet segments, making them act as a single segment.
- **Switch**-a device that allocates traffic from one network segment to certain lines (intended destination(s) which connect the segment to another network segment. Unlike a hub, a switch splits the network traffic and sends it to different destinations rather than to all systems on the network.
- **Bridge**- a device that connects multiple network segments along the data link layer.
- **Modem**- device that modulates an analog "carrier" signal (such as sound) to encode digital information, and that also demodulates such a carrier signal to decode the transmitted information, such as a computer communicating with another computer over a telephone network.

Software used in a network

- Operating system
- Applications
- Firewall
- Virus software

Equipment and methods used to transfer data over wireless and wired networks.

Wireless
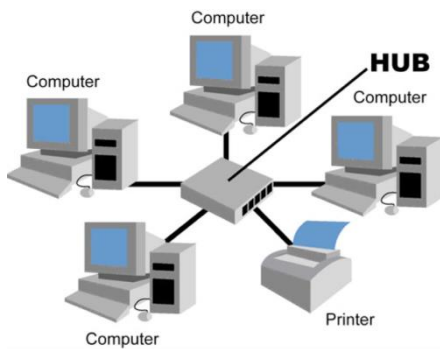
- Email
- Cloud
- Modem
- Radio Waves

Wired

- Ethernet cable (CAT5, CAT6)
- Router

Architectures

- Peer to peer
- Client server

Topology

Star

Advantages

- **Better performance:** Star topology prevents the passing of data packets through an excessive number of nodes. At most, 3 devices and 2 links are involved in any communication between any two devices. Although this topology places a huge overhead on the central hub, with adequate capacity, the hub can handle very high utilization by one device without affecting others.
- **Isolation of devices:** Each device is inherently isolated by the link that connects it to the hub. This makes the isolation of individual devices straightforward and amounts to disconnecting each device from the others. This isolation also prevents any non-centralized failure from affecting the network.
- **Benefits from centralization:** As the central hub is the bottleneck, increasing its capacity, or connecting additional devices to it, increases the size of the network very easily. Centralization also allows the inspection of traffic through the network. This facilitates analysis of the traffic and detection of suspicious behavior.

Scope

- WAN
- LAN
- PAN

Different Protocols

Ethernet- Ethernet/IP (Ethernet Industrial Protocol) is a network communication standard capable of handling large amounts of data at speeds of 10 Mbps or 100 Mbps, and at up to 1500 bytes per packet. The specification uses an open protocol at the application layer. It is especially popular for control applications.

What is a frame-An Ethernet frame is preceded by a preamble and start frame delimiter (SFD), which are both part of the layer 1 Ethernet packet. Each Ethernet frame starts with an Ethernet header, which contains destination and source MAC addresses as its first two fields. The middle section of the frame is payload data including any headers for other protocols (for example Internet Protocol) carried in the frame. The frame ends with a frame check sequence (FCS), which is a 32-bit cyclic redundancy check used to detect any in-transit corruption of data.

What is a packet- A data packet on an Ethernet link is called an *Ethernet packet*, which transports an **Ethernet frame** as payload.

Internet Protocol (IP) - a set of rules governing the format of data sent over the Internet or other network.

What is DCHP- the **Dynamic Host Configuration Protocol** (**DHCP**) is a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.

Transmission control protocol (TCP) - The **Transmission Control Protocol** (**TCP**) is a core protocols of the Internet Protocol Suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as *TCP/IP*. TCP provides reliable, ordered, and error-checked delivery of a stream of octets between applications running on hosts communicating over an IP network. TCP is the protocol that major Internet applications such as the World Wide Web, email, remote administration and file transfer rely on. Applications that do not require reliable data stream service, may use the User Datagram Protocol (UDP), which provides a connectionless datagram service that emphasizes reduced latency over reliability. This is the protocol that creates the data back to its original form.

<u>Best protocol for a multi-user environment and why -</u> In this paper, a relay selection issue is studied to improve data rate performance in a multi-user environment. Previous opportunistic relay selection protocols only consider channel condition in relay selection. However, the target performance is affected by other system attributes, such as delay and load in relay node (RN). The proposed relay selection scheme, which is based on analytic hierarchy process (AHP), adopts signal-to-noise ratio (SNR), switching, and the number of connections to RN as a selection criteria. Also, a special form of eigenvector is proposed and proved analytically. From the proposed eigenvector, the computational complexity is obviously reduced. Target system performance is examined under different weighting parameter values to the above attributes. This work shows that average data rate can be maximized corresponding to the number of RN. Simulation results reveal the benefits of the proposed scheme over the conventional opportunistic relay selection scheme and the threshold-based relay switching selection scheme. The performance of our scheme is verified in terms of average data rate and distribution of the data rate.

<u>How do you keep networks secure?</u>

Methods of backing up data?

You can back up data on the cloud or e-mail it to yourself.

What is malware?

Short for malicious software, if any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

Phishing: The phishing scam masquerades as a legitimate website or link to a site, but what it's really trying to do is "fish" for information. By fooling you into thinking that you're visiting your bank or a shopping or government website, the scam gets you to divulge personal or financial information, which the Bad Guys then exploit.

Trojan horse: The Trojan program is malware that masquerades as a legitimate program. The program may have a legitimate function, but it carries ulterior motives. Trojans can delete data, compromise security, relay spam and otherwise infect your computer.

How can a firewall be used to control incoming and out going data.

A **firewall** is a network security system that controls the incoming and outgoing network traffic based on an applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is assumed not to be secure and trusted. Firewalls exist both as a software solution and as a hardware appliance.

Many hardware-based firewalls also offer other functionality to the internal network they protect, such as acting as a DHCP server for that network.

How can network access permissions be controlled?

On some types of proprietary computer hardware (in particular routers and switches), an Access Control List refers to rules that are applied to port numbers or IP Addresses that are available on a host or other layer 3, each with a list of hosts and/or networks permitted to use the service. Different users and passwords can also be used to control permissions and grouping

How can a wireless network connection be secured?

Put a password on the connection.

<u>What is bandwidth?</u>

A range of frequencies within a given band, in particular that used for transmitting a signal.

Types of cable

- **Coaxial-** of a cable or line transmitting by means of two concentric conductors separated by an insulator. Speed: 12GHz
- **Untwisted pair (UTP)-** Short for **unshielded twisted pair**, a popular type of cable that consists of two **unshielded** wires twisted around each other. Due to its low cost, UTP cabling is used extensively for local-area networks (LANs) and telephone connections. Speed: 100Mbps
- **Fibre optic- Optical** fibres are widely used in **fibre**-**optic** communications, where they permit transmission over longer distances and at higher bandwidths (data rates) than wire **cables**. Fibres are used instead of metal wires because signals travel along them with less loss and are also immune to electromagnetic interference. Speed: 100 petabits per second