**Networking**

A computer network or data network is a telecommunications network that allows computers to exchange data. The physical connection between networked computing devices is established using either cable media or wireless media. The best-known computer network is the Internet.

Network devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as servers and personal computers, as well as networking hardware. Two devices are said to be networked when a process in one device is able to exchange information with a process in another device.

Computer networks support applications such as access to the World Wide Web, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications. The remainder of this article discusses local area network technologies and classifies them according to the following characteristics: the physical media used to transmit signals, the communications protocols used to organize network traffic, along with the network's size, its topology and its organizational intent.

A computer network has the following properties:

* Facilitates interpersonal communications

People can communicate efficiently and easily via email, instant messaging, chat rooms, telephone, video telephone calls, and video conferencing.

* Allows sharing of files, data, and other types of information

Authorized users may access information stored on other computers on the network. Providing access to information on shared storage devices is an important feature of many networks.

* Allows sharing of network and computing resources

Users may access and use resources provided by devices on the network, such as printing a document on a shared network printer. [Distributed computing](http://en.wikipedia.org/wiki/Distributed_computing) uses computing resources across a network to accomplish tasks.

* May be insecure

A computer network may be used by [computer Hackers](http://en.wikipedia.org/wiki/Hacker_(computer_security)) to deploy [computer viruses](http://en.wikipedia.org/wiki/Computer_virus) or [computer worms](http://en.wikipedia.org/wiki/Computer_worm) on devices connected to the network, or to prevent these devices from accessing the network ([denial of service](http://en.wikipedia.org/wiki/Denial-of-service_attack)).

* May interfere with other technologies

[Power line communication](http://en.wikipedia.org/wiki/Power_line_communication) strongly disturbs certain forms of radio communication, e.g., amateur radio. It may also interfere with [last mile](http://en.wikipedia.org/wiki/Last_mile) access technologies such as [ADSL](http://en.wikipedia.org/wiki/ADSL) and [VDSL](http://en.wikipedia.org/wiki/VDSL).

* May be difficult to set up

A complex computer network may be difficult to set up. It may be costly to set up an effective computer network in a large organization.

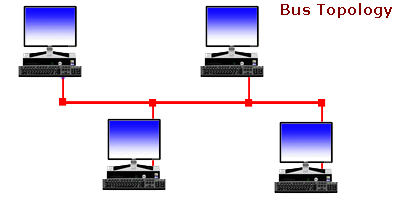
[Network topology](http://en.wikipedia.org/wiki/Network_topology) is the layout or organizational hierarchy of interconnected nodes of a computer network.

**Common layout**

Common layout are:

**Bus Network**

A [bus network](http://en.wikipedia.org/wiki/Bus_network): Bus networks are the simplest as well as the easiest way to connect multiple clients, but may have problems when two clients want to transmit at the same time on the same bus. Thus systems which use bus network architectures normally have some scheme of collision handling or collision avoidance for communication on the bus, quite often using [Carrier Sense Multiple Access](http://en.wikipedia.org/wiki/Carrier_Sense_Multiple_Access) or the presence of a [bus master](http://en.wikipedia.org/wiki/Bus_master) which controls access to the shared bus resource.

[](http://www.google.co.uk/url?sa=i&rct=j&q=Bus+Network&source=images&cd=&cad=rja&docid=KK0T5_oRQk6CFM&tbnid=4p8HEqyYOx1zCM:&ved=0CAUQjRw&url=http://www.klbict.co.uk/gcse/theory/5_3/5_3_4_topologies.htm&ei=EAL9Ue6_C6mw0QX97oAo&psig=AFQjCNE4cSE_jh2ZZ076pFXU4bge92rgPw&ust=1375621823858304)

**Advantages**

* Ease of installation.
* Simple and cheap.
* If one computer fails it does not affect the other computers.
* Minimizes the amount cable used connecting the network.

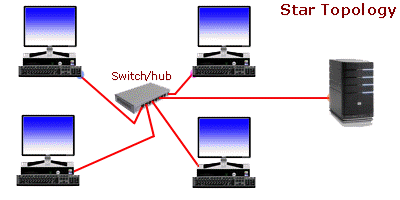
**Disadvantages**

* If the main cable fails, all the other sources will die
* Reconfiguration, fault isolation and installation of new devices tend to be difficult since the network is designed to be most efficient during installation.
* The longer the distance covered by a signal along the shared communication line the greater the heat is produced due to energy being transformed to heat making the signal weaker the farther it travels.
* A fault along the shared communication line stops all transmissions in the network.
* Connection Limitation can also occur
* Data can be transmitted only in one direction and is removed from the line once it reaches the end of the line else it will lead to repetition.

**Star Network**

Star networks are one of the most common computer network topologies. In its simplest form, a star network consists of one central switch, hub or computer, which acts as a conduit to transmit messages. This consists of a central node, to which all other nodes are connected; this central node provides a common connection point for all nodes through a hub. In star topology, every node (computer workstation or any other peripheral) is connected to central node called hub or switch. The switch is the server and the peripherals are the clients. Thus, the hub and leaf nodes, and the transmission lines between them, form a graph with the topology of a star. If the central node is passive, the originating node must be able to tolerate the reception of an echo of its own transmission, delayed by the two-way transmission time (i.e. to and from the central node) plus any delay generated in the central node. An active star network has an active central node that usually has the means to prevent echo-related problems.

The star topology reduces the chance of network failure by connecting all of the systems to a central node. When applied to a bus-based network, this central hub rebroadcasts all transmissions received from any peripheral node to all peripheral nodes on the network, sometimes including the originating node. All peripheral nodes may thus communicate with all others by transmitting to, and receiving from, the central node only. The failure of a transmission line linking any peripheral node to the central node will result in the isolation of that peripheral node from all others, but the rest of the systems will be unaffected.

[](http://www.google.co.uk/url?sa=i&rct=j&q=Star+Network&source=images&cd=&cad=rja&docid=KK0T5_oRQk6CFM&tbnid=Ltsc8YNZbofe9M:&ved=0CAUQjRw&url=http://www.klbict.co.uk/gcse/theory/5_3/5_3_4_topologies.htm&ei=_QH9UY7RNcyb1AWBqYDoDQ&psig=AFQjCNFaszaYIxd5hn4DzLr9-GlS-4GXww&ust=1375622000638776)

**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.
* Easy to detect faults and to remove parts.
* No disruptions to the network when connecting or removing devices.
* Installation and configuration is easy since every one device only requires a link and one input/output port to connect it to any other device(s).

**Disadvantages**

* High dependence of the system on the functioning of the central hub. Failure of the central hub renders the network inoperable

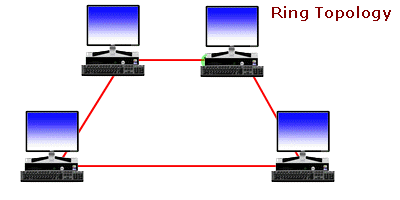
**Ring Network**

A ring network is a [network topology](http://en.wikipedia.org/wiki/Network_topology) in which each node connects to exactly two other nodes, forming a single continuous pathway for signals through each node - a ring. Data travels from node to node, with each node along the way handling every packet.

Because a ring topology provides only one pathway between any two nodes, ring networks may be disrupted by the failure of a single link. A node failure or cable break might isolate every node attached to the ring.

[FDDI](http://en.wikipedia.org/wiki/FDDI) networks overcome this vulnerability by sending data on a clockwise and a counterclockwise ring: in the event of a break data is wrapped back onto the complementary ring before it reaches the end of the cable, maintaining a path to every node along the resulting "C-Ring".

Many ring networks add a "counter-rotating ring" to form a [redundant topology](http://en.wikipedia.org/wiki/Redundant_topologies). Such "dual ring" networks include [Spatial Reuse Protocol](http://en.wikipedia.org/wiki/Spatial_Reuse_Protocol), [Fiber Distributed Data Interface](http://en.wikipedia.org/wiki/Fiber_distributed_data_interface) (FDDI), and [Resilient Packet Ring](http://en.wikipedia.org/wiki/Resilient_Packet_Ring).

[](http://www.google.co.uk/url?sa=i&rct=j&q=Ring+Network&source=images&cd=&cad=rja&docid=KK0T5_oRQk6CFM&tbnid=xO83fCuBap6zjM:&ved=0CAUQjRw&url=http://www.klbict.co.uk/gcse/theory/5_3/5_3_4_topologies.htm&ei=WgT9UYnSNeuW0QWA5IC4Dw&psig=AFQjCNHkQd8_YD7sHS_BhBlI4CdBZziZ1A&ust=1375622613267898)

**Advantages**

* Very orderly network where every device has access to the token and the opportunity to transmit
* Performs better than a bus topology under heavy network load
* Does not require a central node to manage the connectivity between the computers
* Due to the point to point line configuration of devices with a device on either side (each device is connected to its immediate neighbour), it is quite easy to install and reconfigure since adding or removing a device requires moving just two connections.
* Point to point line configuration makes it easy to identify and isolate faults.

**Disadvantages**

* One malfunctioning workstation can create problems for the entire network. This can be solved by using a dual ring or a switch that closes off the break.
* Moving, adding and changing the devices can affect the network
* Communication delay is directly proportional to number of nodes in the network
* Bandwidth is shared on all links between devices
* More difficult to configure than a Star: node adjunction ⇨ Ring shutdown and reconfiguration