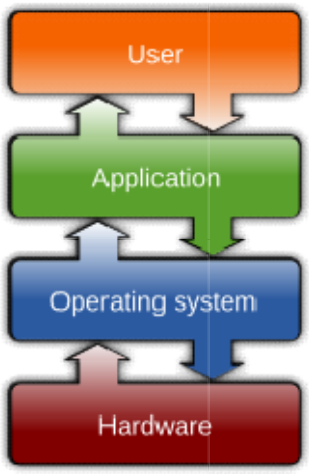
# SUBJECT-Computer network

[Bca –IIIrd Yr]




A **computer network** is a set of computers sharing resources located on or provided by network nodes. Computers use common communication protocols over digital interconnections to communicate with each other. These interconnections are made up of telecommunication network technologies based on physically wired, optical, and wireless radio-frequency methods that may be arranged in a variety of network topologies.

The nodes of a computer network can include personal computers, servers, networking hardware, or other specialized or general-purpose hosts. They are identified by network addresses and may have hostnames. Hostnames serve as memorable labels for the nodes and are rarely changed after initial assignment. Network addresses serve for locating and identifying the nodes by communication protocols such as the Internet Protocol.

Computer networks may be classified by many criteria, including the transmission medium used to carry signals, bandwidth, communications protocols to organize network traffic, the network size, the topology, traffic control mechanisms, and organizational intent.[*citation needed*]

Computer networks support many applications and services, such as access to the World Wide Web, digital video and audio, shared use of application and storage servers, printers and fax machines, and use of email and instant messaging applications.

# History

Computer networking may be considered a branch of computer science, computer engineering, and telecommunications, since it relies on the theoretical and practical application of the related disciplines. Computer networking was influenced by a wide array of technological developments and historical milestones.

- In the late 1950s, a network of computers was built for the U.S. military Semi-Automatic Ground Environment (SAGE) radar system[1][2][3] using the Bell 101 modem. It was the first commercial modem for computers, released by AT&T Corporation in 1958. The modem allowed digital data to be transmitted over regular unconditioned telephone lines at a speed of 110 bits per second (bit/s).
- In 1959, Christopher Strachey filed a patent application for time-sharing in the United Kingdom and John McCarthy initiated the first project to implement time-sharing of user programs at MIT.[4][5][6][7] Strachey passed the concept on to J. C. R. Licklider at the inaugural UNESCO Information Processing Conference in Paris that year.[8] McCarthy was instrumental in the creation of three of the earliest time-sharing systems (the Compatible Time-Sharing System in 1961, the BBN Time-Sharing System in 1962, and the Dartmouth Time Sharing System in 1963).
- In 1959, Anatoly Kitov proposed to the Central Committee of the Communist Party of the Soviet Union a detailed plan for the re-organization of the control of the Soviet armed forces and of the Soviet economy on the basis of a network of computing centers.[9] Kitov's proposal was rejected, as later was the 1962 OGAS economy management network project.[10]
- In 1960, the commercial airline reservation system semi-automatic business research environment (SABRE) went online with two connected mainframes.
- In 1963, J. C. R. Licklider sent a memorandum to office colleagues discussing the concept of the "Intergalactic Computer Network", a computer network intended to allow general communications among computer users.
- In 1965, Western Electric introduced the first widely used telephone switch that implemented computer control in the switching fabric.
- Throughout the 1960s,[11][12] Paul Baran and Donald Davies independently invented the concept of packet switching for data communication between computers over a network.[13][14][15][16] Baran's work addressed adaptive routing of message blocks across a distributed network, but did not include routers with software switches, nor the idea that users, rather than the network itself, would provide the reliability.[17][18][19][20] Davies' hierarchical network design included high-speed routers, communication protocols and the essence of the end-to-end principle.[21][22][23][24] The NPL network, a local area network at the National Physical Laboratory (United Kingdom), pioneered the implementation of the concept in 1968-69 using 768 kbit/s links.[25][23][26] Both Baran's and Davies' inventions were seminal contributions that influenced the development of computer networks.[27][28][29][30]
- In 1969, the first four nodes of the ARPANET were connected using 50 kbit/s circuits between the University of California at Los Angeles, the Stanford Research Institute, the University of California at Santa Barbara, and the University of Utah.[31] Designed principally by Bob Kahn, the network's routing, flow control, software design and network control were developed by the IMP team working for Bolt Beranek & Newman.[32][33][34] In the early 1970s, Leonard Kleinrock carried out mathematical work to model the performance of packet-switched networks, which underpinned the development of the ARPANET.[35][36] His theoretical work on hierarchical routing in the late 1970s with student Farouk Kamoun remains critical to the operation of the Internet today.[37][38]
- In 1972, commercial services were first deployed on experimental public data networks in Europe.[39][40]
- In 1973, the French CYCLADES network, directed by Louis Pouzin was the first to make the hosts responsible for the reliable delivery of data, rather than this being a centralized service of the network itself.[41]

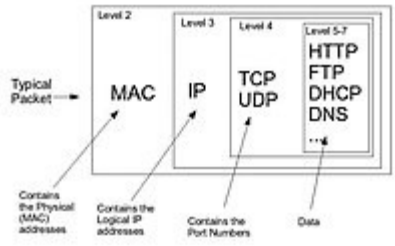
- In 1973, Peter Kirstein put internetworking into practice at University College London (UCL), connecting the ARPANET to British academic networks, the first international heterogeneous computer network.[42][43]
- In 1973, Robert Metcalfe wrote a formal memo at Xerox PARC describing Ethernet, a networking system that was based on the Aloha network, developed in the 1960s by Norman Abramson and colleagues at the University of Hawaii. Metcalfe, with John Shoch, Yogen Dalal, Ed Taft, and Butler Lampson also developed the PARC Universal Packet for internetworking.[44]
- In 1974, Vint Cerf and Bob Kahn published their seminal 1974 paper on internetworking, *A Protocol for Packet Network Intercommunication.*[45] Later that year, Cerf, Yogen Dalal, and Carl Sunshine wrote the first Transmission Control Protocol (TCP) specification, RFC 675, coining the term *Internet* as a shorthand for internetworking.[46]
- In July 1976, Robert Metcalfe and David Boggs published their paper "Ethernet: Distributed Packet Switching for Local Computer Networks"[47] and collaborated on several patents received in 1977 and 1978.
- Public data networks in Europe, North America and Japan began using X.25 in the late 1970s and interconnected with X.75.[14] This underlying infrastructure was used for expanding TCP/IP networks in the 1980s.[48]
- In 1976, John Murphy of Datapoint Corporation created ARCNET, a token-passing network first used to share storage devices.
- In 1977, the first long-distance fiber network was deployed by GTE in Long Beach, California.
- In 1979, Robert Metcalfe pursued making Ethernet an open standard.[49]
- In 1980, Ethernet was upgraded from the original 2.94 Mbit/s protocol to the 10 Mbit/s protocol, which was developed by Ron Crane, Bob Garner, Roy Ogus,[50] and Yogen Dalal.[51]
- In 1995, the transmission speed capacity for Ethernet increased from 10 Mbit/s to 100 Mbit/s. By 1998, Ethernet supported transmission speeds of 1 Gbit/s. Subsequently, higher speeds of up to 400 Gbit/s were added (as of 2018). The scaling of Ethernet has been a contributing factor to its continued use.[49]

# Use

Computer networks enhance how users communicate with each other by using various electronic methods like email, instant messaging, online chat, voice and video calls, and video conferencing. Networks also enable the sharing of computing resources. For example, a user can print a document on a shared printer or use shared storage devices. Additionally, networks allow for the sharing of files and information, giving authorized users access to data stored on other computers. Distributed computing leverages resources from multiple computers across a network to perform tasks collaboratively.

# Network packet

[




Network Packet

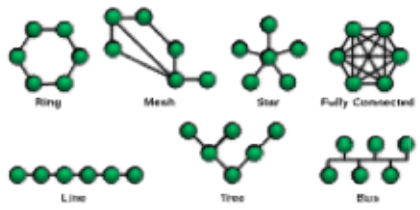
Most modern computer networks use protocols based on packet-mode transmission. A network packet is a formatted unit of data carried by a packet-switched network.

Packets consist of two types of data: control information and user data (payload). The control information provides data the network needs to deliver the user data, for example, source and destination network addresses, error detection codes, and sequencing information. Typically, control information is found in packet headers and trailers, with payload data in between.

With packets, the bandwidth of the transmission medium can be better shared among users than if the network were circuit switched. When one user is not sending packets, the link can be filled with packets from other users, and so the cost can be shared, with relatively little interference, provided the link is not overused. Often the route a packet needs to take through a network is not immediately available. In that case, the packet is queued and waits until a link is free.

The physical link technologies of packet networks typically limit the size of packets to a certain maximum transmission unit (MTU). A longer message may be fragmented before it is transferred and once the packets arrive, they are reassembled to construct the original message.

# Network topology




Common network topologies

The physical or geographic locations of network nodes and links generally have relatively little effect on a network, but the topology of interconnections of a network can significantly affect its throughput and reliability. With many technologies, such as bus or star networks, a single failure can cause the network to fail entirely. In general, the more interconnections there are, the more robust the network is; but the more expensive it is to install. Therefore, most network diagrams are arranged by their network topology which is the map of logical interconnections of network hosts.

Common topologies are:

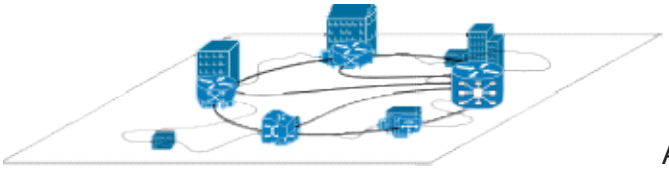
- Bus network: all nodes are connected to a common medium along this medium. This was the layout used in the original Ethernet, called 10BASE5 and 10BASE2. This is still a

common topology on the data link layer, although modern physical layer variants use point-to-point links instead, forming a star or a tree.

- Star network: all nodes are connected to a special central node. This is the typical layout found in a small switched Ethernet LAN, where each client connects to a central network switch, and logically in a wireless LAN, where each wireless client associates with the central wireless access point.
- Ring network: each node is connected to its left and right neighbor node, such that all nodes are connected and that each node can reach each other node by traversing nodes left- or rightwards. Token ring networks, and the Fiber Distributed Data Interface (FDDI), made use of such a topology.
- Mesh network: each node is connected to an arbitrary number of neighbors in such a way that there is at least one traversal from any node to any other.
- Fully connected network: each node is connected to every other node in the network.
- Tree network: nodes are arranged hierarchically. This is the natural topology for a larger Ethernet network with multiple switches and without redundant meshing.

The physical layout of the nodes in a network may not necessarily reflect the network topology. As an example, with FDDI, the network topology is a ring, but the physical topology is often a star, because all neighboring connections can be routed via a central physical location. Physical layout is not completely irrelevant, however, as common ducting and equipment locations can represent single points of failure due to issues like fires, power failures and flooding.

## Overlay network



A sample overlay network

An overlay network is a virtual network that is built on top of another network. Nodes in the overlay network are connected by virtual or logical links. Each link corresponds to a path, perhaps through many physical links, in the underlying network. The topology of the overlay network may (and often does) differ from that of the underlying one. For example, many peer-to-peer networks are overlay networks. They are organized as nodes of a virtual system of links that run on top of the Internet.[52]

Overlay networks have been used since the early days of networking, back when computers were connected via telephone lines using modems, even before data networks were developed.

The most striking example of an overlay network is the Internet itself. The Internet itself was initially built as an overlay on the telephone network.[52] Even today, each Internet node can communicate with virtually any other through an underlying mesh of sub-networks of wildly different topologies and technologies. Address resolution and routing are the means that allow mapping of a fully connected IP overlay network to its underlying network.

Another example of an overlay network is a distributed hash table, which maps keys to nodes in the network. In this case, the underlying network is an IP network, and the overlay network is a table (actually a map) indexed by keys.

Overlay networks have also been proposed as a way to improve Internet routing, such as through quality of service guarantees achieve higher-quality streaming media. Previous

proposals such as IntServ, DiffServ, and IP multicast have not seen wide acceptance largely because they require modification of all routers in the network.[citation needed] On the other hand, an overlay network can be incrementally deployed on end-hosts running the overlay protocol software, without cooperation from Internet service providers. The overlay network has no control over how packets are routed in the underlying network between two overlay nodes, but it can control, for example, the sequence of overlay nodes that a message traverses before it reaches its destination[citation needed].

For example, Akamai Technologies manages an overlay network that provides reliable, efficient content delivery (a kind of multicast). Academic research includes end system multicast,[53] resilient routing and quality of service studies, among others.

# Network links

The transmission media (often referred to in the literature as the *physical medium*) used to link devices to form a computer network include electrical cable, optical fiber, and free space. In the OSI model, the software to handle the media is defined at layers 1 and 2 — the physical layer and the data link layer.

A widely adopted *family* that uses copper and fiber media in local area network (LAN) technology are collectively known as Ethernet. The media and protocol standards that enable communication between networked devices over Ethernet are defined by IEEE 802.3. Wireless LAN standards use radio waves, others use infrared signals as a transmission medium. Power line communication uses a building's power cabling to transmit data.

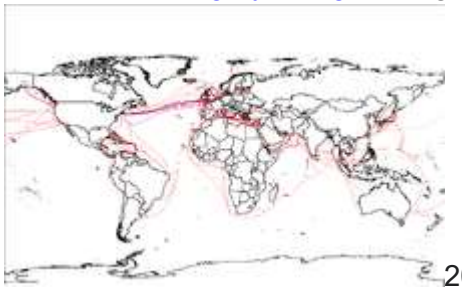
## Wired


Fiber-optic cables are used to transmit light from one computer/network node to another.

The following classes of wired technologies are used in computer networking.

- *Coaxial cable* is widely used for cable television systems, office buildings, and other work-sites for local area networks. Transmission speed ranges from 200 million bits per second to more than 500 million bits per second.[citation needed]
- ITU-T G.hn technology uses existing home wiring (coaxial cable, phone lines and power lines) to create a high-speed local area network.
- *Twisted pair* cabling is used for wired Ethernet and other standards. It typically consists of 4 pairs of copper cabling that can be utilized for both voice and data transmission. The use of

two wires twisted together helps to reduce crosstalk and electromagnetic induction. The transmission speed ranges from 2 Mbit/s to 10 Gbit/s. Twisted pair cabling comes in two forms: unshielded twisted pair (UTP) and shielded twisted-pair (STP). Each form comes in several category ratings, designed for use in various scenarios.


2007 map showing submarine optical fiber telecommunication cables around the world

- An *optical fiber* is a glass fiber. It carries pulses of light that represent data via lasers and optical amplifiers. Some advantages of optical fibers over metal wires are very low transmission loss and immunity to electrical interference. Using dense wave division multiplexing, optical fibers can simultaneously carry multiple streams of data on different wavelengths of light, which greatly increases the rate that data can be sent to up to trillions of bits per second. Optic fibers can be used for long runs of cable carrying very high data rates, and are used for undersea communications cables to interconnect continents. There are two basic types of fiber optics, single-mode optical fiber (SMF) and multi-mode optical fiber (MMF). Single-mode fiber has the advantage of being able to sustain a coherent signal for dozens or even a hundred kilometers. Multimode fiber is cheaper to terminate but is limited to a few hundred or even only a few dozens of meters, depending on the data rate and cable grade.[54]

## Wireless


Computers are very often connected to networks using wireless links.

Network connections can be established wirelessly using radio or other electromagnetic means of communication.

- *Terrestrial microwave* – Terrestrial microwave communication uses Earth-based transmitters and receivers resembling satellite dishes. Terrestrial microwaves are in the low gigahertz range, which limits all communications to line-of-sight. Relay stations are spaced approximately 40 miles (64 km) apart.
- *Communications satellites* – Satellites also communicate via microwave. The satellites are stationed in space, typically in geosynchronous orbit 35,400 km (22,000 mi) above the equator. These Earth-orbiting systems are capable of receiving and relaying voice, data, and TV signals.

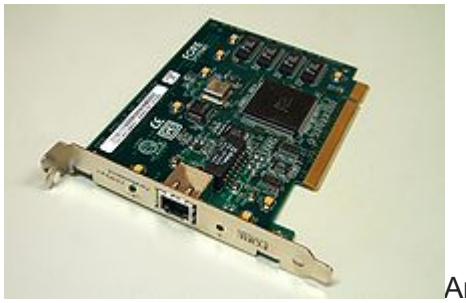
- *Cellular networks* use several radio communications technologies. The systems divide the region covered into multiple geographic areas. Each area is served by a low-power transceiver.
- *Radio and spread spectrum technologies* – Wireless LANs use a high-frequency radio technology similar to digital cellular. Wireless LANs use spread spectrum technology to enable communication between multiple devices in a limited area. IEEE 802.11 defines a common flavor of open-standards wireless radio-wave technology known as Wi-Fi.
- *Free-space optical communication* uses visible or invisible light for communications. In most cases, line-of-sight propagation is used, which limits the physical positioning of communicating devices.
- Extending the Internet to interplanetary dimensions via radio waves and optical means, the Interplanetary Internet.[55]
- IP over Avian Carriers was a humorous April fool's Request for Comments, issued as RFC 1149. It was implemented in real life in 2001.[56]

The last two cases have a large round-trip delay time, which gives slow two-way communication but does not prevent sending large amounts of information (they can have high throughput).

# Network nodes

Apart from any physical transmission media, networks are built from additional basic system building blocks, such as network interface controllers, repeaters, hubs, bridges, switches, routers, modems, and firewalls. Any particular piece of equipment will frequently contain multiple building blocks and so may perform multiple functions.

## Network interfaces



An ATM network interface in the form of an accessory card. A lot of network interfaces are built-in.

A network interface controller (NIC) is computer hardware that connects the computer to the network media and has the ability to process low-level network information. For example, the NIC may have a connector for plugging in a cable, or an aerial for wireless transmission and reception, and the associated circuitry.

In Ethernet networks, each NIC has a unique Media Access Control (MAC) address—usually stored in the controller's permanent memory. To avoid address conflicts between network devices, the Institute of Electrical and Electronics Engineers (IEEE) maintains and administers MAC address uniqueness. The size of an Ethernet MAC address is six octets. The three most significant octets are reserved to identify NIC manufacturers. These manufacturers, using only their assigned prefixes, uniquely assign the three least-significant octets of every Ethernet interface they produce.

## Repeaters and hubs

A repeater is an electronic device that receives a network signal, cleans it of unnecessary noise and regenerates it. The signal is retransmitted at a higher power level, or to the other side of obstruction so that the signal can cover longer distances without degradation. In most twisted-pair Ethernet configurations, repeaters are required for cable that runs longer than 100 meters. With fiber optics, repeaters can be tens or even hundreds of kilometers apart.

Repeaters work on the physical layer of the OSI model but still require a small amount of time to regenerate the signal. This can cause a propagation delay that affects network performance and may affect proper function. As a result, many network architectures limit the number of repeaters used in a network, e.g., the Ethernet 5-4-3 rule.

An Ethernet repeater with multiple ports is known as an Ethernet hub. In addition to reconditioning and distributing network signals, a repeater hub assists with collision detection and fault isolation for the network. Hubs and repeaters in LANs have been largely obsoleted by modern network switches.

## Bridges and switches

Network bridges and network switches are distinct from a hub in that they only forward frames to the ports involved in the communication whereas a hub forwards to all ports.[57] Bridges only have two ports but a switch can be thought of as a multi-port bridge. Switches normally have numerous ports, facilitating a star topology for devices, and for cascading additional switches.

Bridges and switches operate at the data link layer (layer 2) of the OSI model and bridge traffic between two or more network segments to form a single local network. Both are devices that forward frames of data between ports based on the destination MAC address in each frame.[58] They learn the association of physical ports to MAC addresses by examining the source addresses of received frames and only forward the frame when necessary. If an unknown destination MAC is targeted, the device broadcasts the request to all ports except the source, and discovers the location from the reply.

Bridges and switches divide the network's collision domain but maintain a single broadcast domain. Network segmentation through bridging and switching helps break down a large, congested network into an aggregation of smaller, more efficient networks.

## Routers

A typical home or small office router showing the ADSL telephone line and Ethernet network cable connections

A router is an internetworking device that forwards packets between networks by processing the addressing or routing information included in the packet. The routing information is often processed in conjunction with the routing table. A router uses its routing table to determine

where to forward packets and does not require broadcasting packets which is inefficient for very big networks.

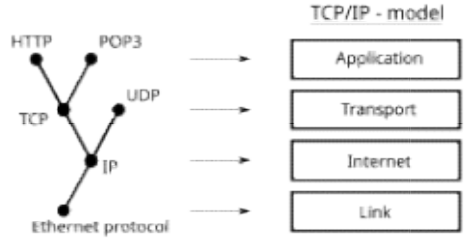
### Modems

Modems (modulator-demodulator) are used to connect network nodes via wire not originally designed for digital network traffic, or for wireless. To do this one or more carrier signals are modulated by the digital signal to produce an analog signal that can be tailored to give the required properties for transmission. Early modems modulated audio signals sent over a standard voice telephone line. Modems are still commonly used for telephone lines, using a digital subscriber line technology and cable television systems using DOCSIS technology.

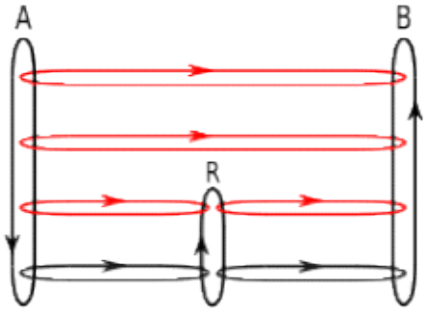
### Firewalls

A firewall is a network device or software for controlling network security and access rules. Firewalls are inserted in connections between secure internal networks and potentially insecure external networks such as the Internet. Firewalls are typically configured to reject access requests from unrecognized sources while allowing actions from recognized ones. The vital role firewalls play in network security grows in parallel with the constant increase in cyber attacks.

## Communication protocols




The TCP/IP model and its relation to common protocols used at different layers of the model




Message flows between two devices (A-B) at the four layers of the TCP/IP model in the presence of a router (R). Red flows are effective communication paths, black paths are across the actual network links.

A communication protocol is a set of rules for exchanging information over a network. Communication protocols have various characteristics. They may be connection-oriented or connectionless, they may use circuit mode or packet switching, and they may use hierarchical addressing or flat addressing.

In a protocol stack, often constructed per the OSI model, communications functions are divided up into protocol layers, where each layer leverages the services of the layer below it until the lowest layer controls the hardware that sends information across the media. The use of protocol layering is ubiquitous across the field of computer networking. An important example of a protocol stack is HTTP (the World Wide Web protocol) running over TCP over IP (the Internet protocols) over IEEE 802.11 (the Wi-Fi protocol). This stack is used between the wireless router and the home user's personal computer when the user is surfing the web.

There are many communication protocols, a few of which are described below.

### Internet protocol suite

The Internet protocol suite, also called TCP/IP, is the foundation of all modern networking. It offers connection-less and connection-oriented services over an inherently unreliable network traversed by datagram transmission using Internet protocol (IP). At its core, the protocol suite defines the addressing, identification, and routing specifications for Internet Protocol Version 4 (IPv4) and for IPv6, the next generation of the protocol with a much enlarged addressing capability. The Internet protocol suite is the defining set of protocols for the Internet.[59]

### IEEE 802

IEEE 802 is a family of IEEE standards dealing with local area networks and metropolitan area networks. The complete IEEE 802 protocol suite provides a diverse set of networking capabilities. The protocols have a flat addressing scheme. They operate mostly at layers 1 and 2 of the OSI model.

For example, MAC bridging (IEEE 802.1D) deals with the routing of Ethernet packets using a Spanning Tree Protocol. IEEE 802.1Q describes VLANs, and IEEE 802.1X defines a port-based Network Access Control protocol, which forms the basis for the authentication mechanisms used in VLANs[60] (but it is also found in WLANs[61]) – it is what the home user sees when the user has to enter a "wireless access key".

#### Ethernet

Ethernet is a family of technologies used in wired LANs. It is described by a set of standards together called IEEE 802.3 published by the Institute of Electrical and Electronics Engineers.

#### Wireless LAN

Wireless LAN based on the IEEE 802.11 standards, also widely known as WLAN or WiFi, is probably the most well-known member of the IEEE 802 protocol family for home users today. IEEE 802.11 shares many properties with wired Ethernet.

### SONET/SDH

Synchronous optical networking (SONET) and Synchronous Digital Hierarchy (SDH) are standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber using lasers. They were originally designed to transport circuit mode communications from a variety of different sources, primarily to support circuit-switched digital telephony. However, due to its protocol neutrality and transport-oriented features, SONET/SDH also was the obvious choice for transporting Asynchronous Transfer Mode (ATM) frames.

### Asynchronous Transfer Mode

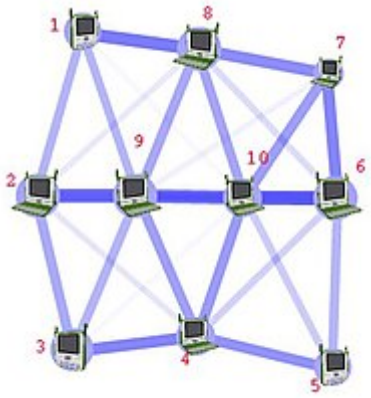
Asynchronous Transfer Mode (ATM) is a switching technique for telecommunication networks. It uses asynchronous time-division multiplexing and encodes data into small, fixed-sized cells. This differs from other protocols such as the Internet protocol suite or Ethernet that use variable-sized packets or frames. ATM has similarities with both circuit and packet switched networking. This makes it a good choice for a network that must handle both traditional high-throughput data traffic, and real-time, low-latency content such as voice and video. ATM uses a connection-oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins.

ATM still plays a role in the last mile, which is the connection between an Internet service provider and the home user.

### Cellular standards

There are a number of different digital cellular standards, including: Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), cdmaOne, CDMA2000, Evolution-Data Optimized (EV-DO), Enhanced Data Rates for GSM Evolution (EDGE), Universal Mobile Telecommunications System (UMTS), Digital Enhanced Cordless Telecommunications (DECT), Digital AMPS (IS-136/TDMA), and Integrated Digital Enhanced Network (iDEN).[63]

## Routing




Routing calculates good paths through a network for information to take. For example, from node 1 to node 6 the best routes are likely to be 1-8-7-6, 1-8-10-6 or 1-9-10-6, as these are the shortest routes.

Routing is the process of selecting network paths to carry network traffic. Routing is performed for many kinds of networks, including circuit switching networks and packet switched networks.

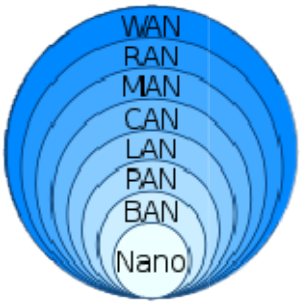
In packet-switched networks, routing protocols direct packet forwarding through intermediate nodes. Intermediate nodes are typically network hardware devices such as routers, bridges, gateways, firewalls, or switches. General-purpose computers can also forward packets and perform routing, though because they lack specialized hardware, may offer limited performance. The routing process directs forwarding on the basis of routing tables, which maintain a record of the routes to various network destinations. Most routing algorithms use only one network path at a time. Multipath routing techniques enable the use of multiple alternative paths.

Routing can be contrasted with bridging in its assumption that network addresses are structured and that similar addresses imply proximity within the network. Structured addresses allow a

single routing table entry to represent the route to a group of devices. In large networks, the structured addressing used by routers outperforms unstructured addressing used by bridging. Structured IP addresses are used on the Internet. Unstructured MAC addresses are used for bridging on Ethernet and similar local area networks.

# Geographic scale

**Computer network types by scale**




- 
- 

Networks may be characterized by many properties or features, such as physical capacity, organizational purpose, user authorization, access rights, and others. Another distinct classification method is that of the physical extent or geographic scale.

## Nanoscale network

A nanoscale network has key components implemented at the nanoscale, including message carriers, and leverages physical principles that differ from macroscale communication mechanisms. Nanoscale communication extends communication to very small sensors and actuators such as those found in biological systems and also tends to operate in environments that would be too harsh for other communication techniques.[64]

## Personal area network

A personal area network (PAN) is a computer network used for communication among computers and different information technological devices close to one person. Some examples of devices that are used in a PAN are personal computers, printers, fax machines, telephones, PDAs, scanners, and video game consoles. A PAN may include wired and wireless devices. The reach of a PAN typically extends to 10 meters.[65] A wired PAN is usually constructed with USB and FireWire connections while technologies such as Bluetooth and infrared communication typically form a wireless PAN.

## Local area network

A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as a home, school, office building, or closely positioned group of

buildings. Wired LANs are most commonly based on Ethernet technology. Other networking technologies such as ITU-T G.hn also provide a way to create a wired LAN using existing wiring, such as coaxial cables, telephone lines, and power lines.[66]

A LAN can be connected to a wide area network (WAN) using a router. The defining characteristics of a LAN, in contrast to a WAN, include higher data transfer rates, limited geographic range, and lack of reliance on leased lines to provide connectivity.[citation needed] Current Ethernet or other IEEE 802.3 LAN technologies operate at data transfer rates up to and in excess of 100 Gbit/s,[67] standardized by IEEE in 2010.

## Home area network

A home area network (HAN) is a residential LAN used for communication between digital devices typically deployed in the home, usually a small number of personal computers and accessories, such as printers and mobile computing devices. An important function is the sharing of Internet access, often a broadband service through a cable Internet access or digital subscriber line (DSL) provider.

## Storage area network

A storage area network (SAN) is a dedicated network that provides access to consolidated, block-level data storage. SANs are primarily used to make storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the storage appears as locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network by other devices. The cost and complexity of SANs dropped in the early 2000s to levels allowing wider adoption across both enterprise and small to medium-sized business environments.[citation needed]

## Campus area network

A campus area network (CAN) is made up of an interconnection of LANs within a limited geographical area. The networking equipment (switches, routers) and transmission media (optical fiber, Cat5 cabling, etc.) are almost entirely owned by the campus tenant or owner (an enterprise, university, government, etc.).

For example, a university campus network is likely to link a variety of campus buildings to connect academic colleges or departments, the library, and student residence halls.

## Backbone network

A backbone network is part of a computer network infrastructure that provides a path for the exchange of information between different LANs or subnetworks. A backbone can tie together diverse networks within the same building, across different buildings, or over a wide area. When designing a network backbone, network performance and network congestion are critical factors to take into account. Normally, the backbone network's capacity is greater than that of the individual networks connected to it.

For example, a large company might implement a backbone network to connect departments that are located around the world. The equipment that ties together the departmental networks constitutes the network backbone. Another example of a backbone network is the Internet backbone, which is a massive, global system of fiber-optic cable and optical networking that

carry the bulk of data between wide area networks (WANs), metro, regional, national and transoceanic networks.

### Metropolitan area network

A metropolitan area network (MAN) is a large computer network that interconnects users with computer resources in a geographic region of the size of a metropolitan area.

### Wide area network

A wide area network (WAN) is a computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances. A WAN uses a communications channel that combines many types of media such as telephone lines, cables, and airwaves. A WAN often makes use of transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI model: the physical layer, the data link layer, and the network layer.

### Enterprise private network

An enterprise private network is a network that a single organization builds to interconnect its office locations (e.g., production sites, head offices, remote offices, shops) so they can share computer resources.

### Virtual private network

A virtual private network (VPN) is an overlay network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. The data link layer protocols of the virtual network are said to be tunneled through the larger network. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

VPN may have best-effort performance or may have a defined service level agreement (SLA) between the VPN customer and the VPN service provider.

### Global area network

A global area network (GAN) is a network used for supporting mobile users across an arbitrary number of wireless LANs, satellite coverage areas, etc. The key challenge in mobile communications is handing off communications from one local coverage area to the next. In IEEE Project 802, this involves a succession of terrestrial wireless LANs.[68]

## Organizational scope

Networks are typically managed by the organizations that own them. Private enterprise networks may use a combination of intranets and extranets. They may also provide network access to the Internet, which has no single owner and permits virtually unlimited global connectivity.

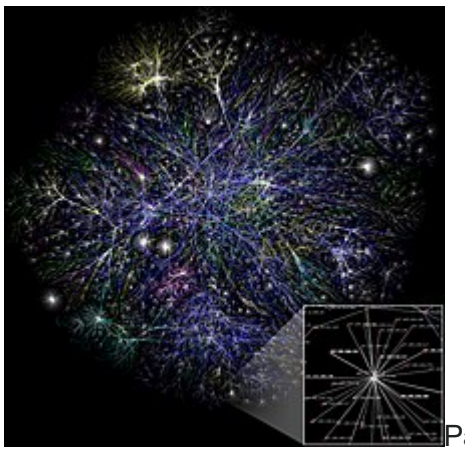
### Intranet

An intranet is a set of networks that are under the control of a single administrative entity. An intranet typically uses the Internet Protocol and IP-based tools such as web browsers and file transfer applications. The administrative entity limits the use of the intranet to its authorized users. Most commonly, an intranet is the internal LAN of an organization. A large intranet typically has at least one web server to provide users with organizational information.

## Extranet

An extranet is a network that is under the administrative control of a single organization but supports a limited connection to a specific external network. For example, an organization may provide access to some aspects of its intranet to share data with its business partners or customers. These other entities are not necessarily trusted from a security standpoint. The network connection to an extranet is often, but not always, implemented via WAN technology.

## Internet


Partial map of the Internet based on 2005 data.[69] Each line is drawn between two nodes, representing two IP addresses. The length of the lines indicates the delay between those two nodes.

An internetwork is the connection of multiple different types of computer networks to form a single computer network using higher-layer network protocols and connecting them together using routers.

The Internet is the largest example of internetwork. It is a global system of interconnected governmental, academic, corporate, public, and private computer networks. It is based on the networking technologies of the Internet protocol suite. It is the successor of the Advanced Research Projects Agency Network (ARPANET) developed by DARPA of the United States Department of Defense. The Internet utilizes copper communications and an optical networking backbone to enable the World Wide Web (WWW), the Internet of things, video transfer, and a broad range of information services.

Participants on the Internet use a diverse array of methods of several hundred documented, and often standardized, protocols compatible with the Internet protocol suite and the IP addressing system administered by the Internet Assigned Numbers Authority and address registries. Service providers and large enterprises exchange information about the reachability of their address spaces through the Border Gateway Protocol (BGP), forming a redundant worldwide mesh of transmission paths.

## Darknet

A darknet is an overlay network, typically running on the Internet, that is only accessible through specialized software. It is an anonymizing network where connections are made only between trusted peers — sometimes called *friends* (F2F)[70] — using non-standard protocols and ports.

Darknets are distinct from other distributed peer-to-peer networks as sharing is anonymous (that is, IP addresses are not publicly shared), and therefore users can communicate with little fear of governmental or corporate interference.[71]

# Network service

Network services are applications hosted by servers on a computer network, to provide some functionality for members or users of the network, or to help the network itself to operate.

The World Wide Web, E-mail,[72] printing and network file sharing are examples of well-known network services. Network services such as Domain Name System (DNS) give names for IP and MAC addresses (people remember names like *nm.lan* better than numbers like *210.121.67.18*),[73] and Dynamic Host Configuration Protocol (DHCP) to ensure that the equipment on the network has a valid IP address.[74]

Services are usually based on a service protocol that defines the format and sequencing of messages between clients and servers of that network service.

# Network performance

## Bandwidth

Bandwidth in bit/s may refer to consumed bandwidth, corresponding to achieved throughput or goodput, i.e., the average rate of successful data transfer through a communication path. The throughput is affected by processes such as bandwidth shaping, bandwidth management, bandwidth throttling, bandwidth cap and bandwidth allocation (using, for example, bandwidth allocation protocol and dynamic bandwidth allocation).

## Network delay

*Network delay* is a design and performance characteristic of a telecommunications network. It specifies the latency for a bit of data to travel across the network from one communication endpoint to another. Delay may differ slightly, depending on the location of the specific pair of communicating endpoints. Engineers usually report both the maximum and average delay, and they divide the delay into several components, the sum of which is the total delay:

- Processing delay – time it takes a router to process the packet header
- Queuing delay – time the packet spends in routing queues
- Transmission delay – time it takes to push the packet's bits onto the link
- Propagation delay – time for a signal to propagate through the media

A certain minimum level of delay is experienced by signals due to the time it takes to transmit a packet serially through a link. This delay is extended by more variable levels of delay due to network congestion. IP network delays can range from less than a microsecond to several hundred milliseconds.

## Performance metrics

The parameters that affect performance typically can include throughput, jitter, bit error rate and latency.

In circuit-switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads.[75] Other types of performance measures can include the level of noise and echo.

In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique, and modem enhancements.[76][*verification needed*][*full citation needed*]

There are many ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured. For example, state transition diagrams are often used to model queuing performance in a circuit-switched network. The network planner uses these diagrams to analyze how the network performs in each state, ensuring that the network is optimally designed.[77]

## Network congestion

Network congestion occurs when a link or node is subjected to a greater data load than it is rated for, resulting in a deterioration of its quality of service. When networks are congested and queues become too full, packets have to be discarded, and participants must rely on retransmission to maintain reliable communications. Typical effects of congestion include queueing delay, packet loss or the blocking of new connections. A consequence of these latter two is that incremental increases in offered load lead either to only a small increase in the network throughput or to a potential reduction in network throughput.

Network protocols that use aggressive retransmissions to compensate for packet loss tend to keep systems in a state of network congestion even after the initial load is reduced to a level that would not normally induce network congestion. Thus, networks using these protocols can exhibit two stable states under the same level of load. The stable state with low throughput is known as *congestive collapse*.

Modern networks use congestion control, congestion avoidance and traffic control techniques where endpoints typically slow down or sometimes even stop transmission entirely when the network is congested to try to avoid congestive collapse. Specific techniques include: exponential backoff in protocols such as 802.11's CSMA/CA and the original Ethernet, window reduction in TCP, and fair queueing in devices such as routers.

Another method to avoid the negative effects of network congestion is implementing quality of service priority schemes allowing selected traffic to bypass congestion. Priority schemes do not solve network congestion by themselves, but they help to alleviate the effects of congestion for critical services. A third method to avoid network congestion is the explicit allocation of network resources to specific flows. One example of this is the use of Contention-Free Transmission Opportunities (CFTXOPs) in the ITU-T G.hn home networking standard.

For the Internet, RFC 2914 addresses the subject of congestion control in detail.

## Network resilience

Network resilience is "the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation."[78]

# Security

]

Computer networks are also used by security hackers to deploy computer viruses or computer worms on devices connected to the network, or to prevent these devices from accessing the network via a denial-of-service attack.

## Network security

Network Security consists of provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and its network-accessible resources.[79] Network security is used on a variety of computer networks, both public and private, to secure daily transactions and communications among businesses, government agencies, and individuals.

## Network surveillance

Network surveillance is the monitoring of data being transferred over computer networks such as the Internet. The monitoring is often done surreptitiously and may be done by or at the behest of governments, by corporations, criminal organizations, or individuals. It may or may not be legal and may or may not require authorization from a court or other independent agency.

Computer and network surveillance programs are widespread today, and almost all Internet traffic is or could potentially be monitored for clues to illegal activity.

Surveillance is very useful to governments and law enforcement to maintain social control, recognize and monitor threats, and prevent or investigate criminal activity. With the advent of programs such as the Total Information Awareness program, technologies such as high-speed surveillance computers and biometrics software, and laws such as the Communications Assistance For Law Enforcement Act, governments now possess an unprecedented ability to monitor the activities of citizens.[80]

However, many civil rights and privacy groups—such as Reporters Without Borders, the Electronic Frontier Foundation, and the American Civil Liberties Union—have expressed concern that increasing surveillance of citizens may lead to a mass surveillance society, with limited political and personal freedoms. Fears such as this have led to lawsuits such as *Hepting v. AT&T*.[80][81] The hacktivist group Anonymous has hacked into government websites in protest of what it considers "draconian surveillance".[82][83]

## End to end encryption

End-to-end encryption (E2EE) is a digital communications paradigm of uninterrupted protection of data traveling between two communicating parties. It involves the originating party encrypting data so only the intended recipient can decrypt it, with no dependency on third parties. End-to-end encryption prevents intermediaries, such as Internet service providers or application service providers, from reading or tampering with communications. End-to-end encryption generally protects both confidentiality and integrity.

Examples of end-to-end encryption include HTTPS for web traffic, PGP for email, OTR for instant messaging, ZRTP for telephony, and TETRA for radio.

Typical server-based communications systems do not include end-to-end encryption. These systems can only guarantee the protection of communications between clients and servers, not between the communicating parties themselves. Examples of non-E2EE systems are Google Talk, Yahoo Messenger, Facebook, and Dropbox.

The end-to-end encryption paradigm does not directly address risks at the endpoints of the communication themselves, such as the technical exploitation of clients, poor quality random number generators, or key escrow. E2EE also does not address traffic analysis, which relates to things such as the identities of the endpoints and the times and quantities of messages that are sent.

### SSL/TLS

The introduction and rapid growth of e-commerce on the World Wide Web in the mid-1990s made it obvious that some form of authentication and encryption was needed. Netscape took the first shot at a new standard. At the time, the dominant web browser was Netscape Navigator. Netscape created a standard called secure socket layer (SSL). SSL requires a server with a certificate. When a client requests access to an SSL-secured server, the server sends a copy of the certificate to the client. The SSL client checks this certificate (all web browsers come with an exhaustive list of root certificates preloaded), and if the certificate checks out, the server is authenticated and the client negotiates a symmetric-key cipher for use in the session. The session is now in a very secure encrypted tunnel between the SSL server and the SSL client.[54]

## Views of networks

Users and network administrators typically have different views of their networks. Users can share printers and some servers from a workgroup, which usually means they are in the same geographic location and are on the same LAN, whereas a network administrator is responsible for keeping that network up and running. A community of interest has less of a connection of being in a local area and should be thought of as a set of arbitrarily located users who share a set of servers, and possibly also communicate via peer-to-peer technologies.

Network administrators can see networks from both physical and logical perspectives. The physical perspective involves geographic locations, physical cabling, and the network elements (e.g., routers, bridges and application-layer gateways) that interconnect via the transmission media. Logical networks, called, in the TCP/IP architecture, subnets, map onto one or more transmission media. For example, a common practice in a campus of buildings is to make a set of LAN cables in each building appear to be a common subnet, using VLANs.

Users and administrators are aware, to varying extents, of a network's trust and scope characteristics. Again using TCP/IP architectural terminology, an intranet is a community of interest under private administration usually by an enterprise, and is only accessible by authorized users (e.g. employees).[84] Intranets do not have to be connected to the Internet, but generally have a limited connection. An extranet is an extension of an intranet that allows secure communications to users outside of the intranet (e.g. business partners, customers).[84]

Unofficially, the Internet is the set of users, enterprises, and content providers that are interconnected by Internet Service Providers (ISP). From an engineering viewpoint, the Internet is the set of subnets, and aggregates of subnets, that share the registered IP address space and exchange information about the reachability of those IP addresses using the Border Gateway Protocol. Typically, the human-readable names of servers are translated to IP

addresses, transparently to users, via the directory function of the Domain Name System (DNS).

Over the Internet, there can be business-to-business, business-to-consumer and consumer-to-consumer communications. When money or sensitive information is exchanged, the communications are apt to be protected by some form of communications security mechanism. Intranets and extranets can be securely superimposed onto the Internet, without any access by general Internet users and administrators, using secure VPN technology.