

## Networking Facts

A *network* is a group of computers that can share information through their interconnections. A network is made up of the following components:

- Computers (often called *nodes* or *hosts*)
- Transmission media--a path for electrical signals between devices
- Network interfaces--devices that send and receive electrical signals
- Protocols--rules or standards that describe how hosts communicate and exchange data

Despite the costs of implementation and maintenance, networks actually save organizations money by allowing them to:

- Consolidate (centralize) data storage
- Share peripheral devices like printers
- Increase internal and external communications
- Increase productivity and collaboration

There are several ways to classify networks. The following table lists several ways to describe a network.

Network Type	Description
<b>Host Role</b>	
Peer-to-peer	<p>In a peer-to-peer network, each host can provide network resources to other hosts or access resources located on other hosts, and each host is in charge of controlling access to those resources. Advantages of peer to peer networks include:</p> <ul style="list-style-type: none"><li>• Easy implementation</li><li>• Inexpensive</li></ul> <p>Disadvantages of peer to peer networks include:</p> <ul style="list-style-type: none"><li>• Difficult to expand (not scalable)</li><li>• Difficult to support</li><li>• Lack centralized control</li><li>• No centralized storage</li></ul>
Client/server	<p>In a client/server network, hosts have specific roles. For example, some hosts are assigned server roles which allows them to provide network resources to other hosts. Other hosts are assigned client roles which allows them to consume network resources. Advantages of client/server networks include:</p> <ul style="list-style-type: none"><li>• Easily expanded (scalable)</li><li>• Easy support</li><li>• Centralized services</li><li>• Easy to backup</li></ul> <p>Disadvantages of client/server networks include:</p> <ul style="list-style-type: none"><li>• Server operating systems are expensive</li></ul>





	<ul style="list-style-type: none"> <li>Requires extensive advanced planning</li> </ul>
<b>Geography and Size</b>	
Local Area Network (LAN)	A local area network (LAN) is a network in a small geographic area, like in an office.
Wide Area Network (WAN)	A wide area network (WAN) is a group of LANs that are geographically isolated but connected to form a large internetwork.
<b>Management</b>	
Network	The term <i>network</i> often describes a network under a single organization with control over the entire network. This could be a local area network at a single location, or a wide area network used by a single business or organization. If, for example, two companies connected their internal networks to share data, you could call it one network. In reality, however, it is two networks, because each network is managed by a different company.
Subnet	<p>A <i>subnet</i> is a portion of a network with a common network address.</p> <ul style="list-style-type: none"> <li>All devices on the subnet share the same network address, but have unique host addresses.</li> <li>Each subnet in a larger network has a unique subnet address.</li> <li>Devices connected through hubs or switches are on the same subnet; routers are used to connect multiple subnets.</li> </ul>
Internetwork	A network that includes geographically disperse (WAN) connections that connect multiple LANs is often called an <i>internetwork</i> . Additionally, connecting two networks under different management is a form of internetworking, as data must travel between two networks.
<b>Participation</b>	
Internet	<p>The Internet is a large, world-wide, public network. The network is public because virtually anyone can connect to the network, and users or organizations make services freely available on the Internet.</p> <ul style="list-style-type: none"> <li>Users and organizations connect to the Internet through an Internet service provider (ISP).</li> <li>The Internet uses a set of communication protocols for providing services called TCP/IP.</li> <li>Individuals and organizations can make services (such as a Web site) available to other users on the Internet.</li> </ul>
Intranet	An <i>intranet</i> is a private network that uses Internet technologies. Services on an intranet are only available to hosts that are connected to the private network. For example, your company might have a Web site that only users who are connected to the private network can access.
Extranet	An <i>extranet</i> is a private network that uses Internet technologies, but whose resources are made available to external (but trusted) users. For example, you might create a Web site on a private network that only users from a partner company can access.

## Topology Facts

*Topology* is the term used to describe how devices are connected and how messages flow from device to device. There are two types of network topologies:

- The physical topology describes the physical way the network is wired.
- The logical topology describes the way in which messages are sent.

The following table describes several common physical topologies.

Topology	Description
 <p data-bbox="224 779 276 806">Bus</p>	<p data-bbox="321 512 1390 573">A physical bus topology consists of a trunk cable with nodes either inserted directly into the trunk, or nodes tapping into the trunk using offshoot cables called drop cables.</p> <ul data-bbox="370 615 1373 737" style="list-style-type: none"> <li>• Signals travel from one node to all other nodes on the bus.</li> <li>• A device called a <i>terminator</i> is placed at both ends of the trunk cable.</li> <li>• Terminators absorb signals and prevent them from reflecting repeatedly back and forth on the cable.</li> </ul> <p data-bbox="321 774 529 802">The physical bus:</p> <ul data-bbox="370 844 915 905" style="list-style-type: none"> <li>• Requires less cable than the star</li> <li>• Can be difficult to isolate cabling problems</li> </ul> <p data-bbox="321 947 1383 1003">A broken cable anywhere on the bus breaks the termination and prevents communications between any device on the network.</p>
 <p data-bbox="224 1178 276 1205">Ring</p>	<p data-bbox="321 1022 1414 1108">A ring topology connects neighboring nodes until they form a ring. Signals travel in one direction around the ring. In ring topologies, each device on the network acts as a repeater to send the signal to the next device. With a ring:</p> <ul data-bbox="370 1150 1425 1272" style="list-style-type: none"> <li>• Installation requires careful planning to create a continuous ring.</li> <li>• Isolating problems can require going to several physical locations along the ring.</li> <li>• A malfunctioning node or cable break can prevent signals from reaching nodes further along on the ring.</li> </ul>
 <p data-bbox="224 1486 276 1514">Star</p>	<p data-bbox="321 1327 1341 1383">A star topology uses a hub or switch to concentrate all network connections to a single physical location. Today it is the most popular type of topology for a LAN. With the star:</p> <ul data-bbox="370 1425 1313 1577" style="list-style-type: none"> <li>• All network connections are located in a single place, which makes it easy to troubleshoot and reconfigure.</li> <li>• Nodes can be added to or removed from the network easily.</li> <li>• Cabling problems usually affect only one node.</li> <li>• Requires more cable than any other topology. Every node has its own cable.</li> </ul>
 <p data-bbox="224 1766 276 1793">Mesh</p>	<p data-bbox="321 1631 1403 1751">A mesh topology exists when there are multiple paths between any two nodes on a network. Mesh topologies are created using point-to-point connections. This increases the network's fault tolerance because alternate paths can be used when one path fails. Two variations of mesh topologies exist:</p> <ul data-bbox="370 1793 1321 1854" style="list-style-type: none"> <li>• Partial Mesh--Some redundant paths exist.</li> <li>• Full Mesh--Every node has a point-to-point connection with every other node.</li> </ul>

Full mesh topologies are usually impractical because the number of connections increases dramatically with every new node added to the network. However, a full mesh topology becomes more practical through the implementation of an ad-hoc wireless network. With this topology, every wireless network card can communicate directly with any other wireless network card on the network. A separate and dedicated network interface and cable for each host on the network is not required.

You should be able to identify the physical topology by looking at the way in which devices are connected. However, it is not as easy to identify the logical topology. As the following table describes, there is often more than one way for messages to travel for a given physical topology.

Logical Topology	Physical Topology	Description
Bus	<a href="#">Bus</a> <a href="#">Star</a>	Messages are sent to all devices connected to the bus.
Ring	<a href="#">Ring</a> <a href="#">Star</a>	Messages are sent from device-to-device in a predetermined order until they reach the destination device.
Star	<a href="#">Star</a>	Messages are sent directly to (and only to) the destination device.

## Network Architecture Facts

A network *architecture* is a set of standards for how computers are physically connected and how signals are passed between hosts. Some typical network architectures are described in the table below.

Network Architecture	Description
Ethernet	Ethernet is a wired networking standard and is the most common networking architecture used in LANs (both in business and home networks).
Dial-up modem	Dial-up networking is a common way to connect a computer (often your home computer) to a remote network, such as the Internet or a business network. A modem on each computer uses the phone lines to send and receive data.
Digital Subscriber Line (DSL)	DSL is a fast-growing alternative to dial-up networking to connect to the Internet. DSL uses regular phone lines to send digital broadband signals.
Integrated Services Digital Network (ISDN)	ISDN is another alternative to traditional dial-up that can be used to connect to the Internet or to directly communicate with another computer connected to the ISDN network. ISDN is more common in Europe than in the U.S. ISDN sends digital signals and can use regular telephone wiring, but must be connected to a special ISDN network.
Wireless	Wireless networking uses radio waves or infrared light (with the air as the transmission medium) to send data between hosts. Wireless networks are common in homes, businesses, airports, and hotels. Most wireless networks connect into

larger wired networks (such as LANs) which are in turn connected to the Internet.

## Common TCP/IP Protocols

A protocol is a set of standards for communication between network hosts. Protocols often provide services, such as e-mail or file transfer. Most protocols are not intended to be used alone, but instead rely on and interact with other dependent or complimentary protocols. A group of protocols that is intended to be used together is called a protocol *suite*.

The Internet protocol suite (normally referred to as TCP/IP) is the most widely used protocol suite today. The following table lists several protocols in the TCP/IP protocol suite.

Category	Protocol	Description
Web browsing	HyperText Transfer Protocol (HTTP)	HTTP is used by Web browsers and Web servers to exchange files (such as Web pages) through the World Wide Web and intranets. HTTP can be described as an information requesting and responding protocol. It is typically used to request and send Web documents, but is also used as the protocol for communication between agents using different TCP/IP protocols.
	HTTP over SSL (HTTPS)	HTTPS is a secure form of HTTP that uses SSL to encrypt data before it is transmitted.
Security protocols	Secure Sockets Layer (SSL)	SSL secures messages being transmitted on the Internet. It uses RSA for authentication and encryption. Web browsers use SSL (Secure Sockets Layer) to ensure safe Web transactions. URLs that begin with <i>https://</i> trigger your Web browser to use SSL.
	Transport Layer Security (TLS)	<p>TLS ensures that messages being transmitted on the Internet are private and tamper proof. TLS is implemented through two protocols:</p> <ul style="list-style-type: none"> <li>• TLS Record--Can provide connection security with encryption (with DES for example).</li> <li>• TLS Handshake--Provides mutual authentication and choice of encryption method.</li> </ul> <p>TLS and SSL are similar but not interoperable.</p>
File transfer	File Transfer Protocol (FTP)	FTP provides a generic method of transferring files. It can include file security through usernames and passwords, and it allows file transfer between dissimilar computer systems. FTP can transfer both binary and text files, including HTML, to another host. FTP URLs are preceded by <i>ftp://</i> followed by the DNS name of the FTP server. To log in to an FTP server, use: <i>ftp://username@servername</i> .
	Trivial File Transfer Protocol (TFTP)	TFTP is similar to FTP. It lets you transfer files between a host and an FTP server. However, it provides no user authentication and no error detection. TFTP is often used when transferring files such as video, audio, or images. Because it does not perform error detection, TFTP is faster than FTP, but might be subject to file errors.
	Secure File Transfer Protocol (SFTP)	SFTP is a file transfer protocol that uses Secure Shell (SSH) to secure data transfers. SSH ensures that SFTP transmissions use encrypted commands and data which prevent data from being transmitted over

		the network in clear text.
	Secure Copy (SCP)	SCP is associated with Unix/Linux networks and used to transfer files between systems. Like SFTP, SCP relies on SSH to ensure that data and passwords are not transmitted over the network in clear text.
E-mail	Simple Mail Transfer Protocol (SMTP)	SMTP is used to route electronic mail through the internetwork. SMTP is used: <ul style="list-style-type: none"> <li>• Between mail servers for sending and relaying mail.</li> <li>• By all e-mail clients to send mail.</li> <li>• By some e-mail client programs, such as Microsoft Outlook, for receiving mail from an Exchange server.</li> </ul>
	Internet Message Access Protocol (IMAP)	IMAP is an e-mail retrieval protocol designed to enable users to access their e-mail from various locations without the need to transfer messages or files back and forth between computers. Messages remain on the remote mail server and are not automatically downloaded to a client system. <b>Note:</b> An e-mail client that uses IMAP for receiving mail uses SMTP for sending mail.
	Post Office Protocol 3 (POP3)	POP3 is part of the TCP/IP protocol suite and used to retrieve e-mail from a remote server to a local client over a TCP/IP connection. With POP3, e-mail messages are downloaded to the client. <b>Note:</b> An e-mail client that uses POP3 for receiving mail uses SMTP for sending mail.
Network services	Dynamic Host Configuration Protocol (DHCP)	DHCP is a method for automatically assigning addresses and other configuration parameters to network hosts. Using a DHCP server, hosts receive configuration information at startup, reducing the amount of manual configuration required on each host.
	Domain Name System (DNS)	DNS is a system that is distributed throughout the internetwork to provide address/name resolution. For example, the name <b>www.mydomain.com</b> would be identified with a specific IP address.
	Network Time Protocol (NTP)	NTP is used to communicate time synchronization information between systems on a network.
	Network News Transport Protocol (NNTP)	NNTP is the most widely-used protocol that manages notes posted on Usenet Newsgroups.
	Lightweight Directory Access Protocol (LDAP)	LDAP is used to allow searching and updating of a directory service. The LDAP directory service follows a client/server model. One or more LDAP servers contain the directory data, the LDAP client connects to an LDAP Server to make a directory service request.
Network management	Simple Network Management Protocol (SNMP)	SNMP is a protocol designed for managing complex networks. SNMP lets network hosts exchange configuration and status information. This information can be gathered by management software and used to monitor and manage the network.
	Remote Terminal Emulation (Telnet)	Telnet allows an attached computer to act as a dumb terminal, with data processing taking place on the TCP/IP host computer. It is still widely used to provide connectivity between dissimilar systems. Telnet can also be used to test a service by the use of HTTP commands.
	Secure Shell (SSH)	SSH allows for secure interactive control of remote systems. SSH uses RSA public key cryptography for both connection and authentication. SSH uses the IDEA algorithm for encryption by default, but is able to use Blowfish and DES. SSH is a secure and acceptable alternative to

		Telnet.
Transport protocols	Transmission Control Protocol (TCP)	TCP provides services that ensure accurate and timely delivery of network communications between two hosts. TCP provides the following services to ensure message delivery: <ul style="list-style-type: none"> <li>• Sequencing of data packets</li> <li>• Flow control</li> <li>• Error checking</li> </ul>
	User Datagram Protocol (UDP)	UDP is a host-to-host protocol like TCP. However, it does not include mechanisms for ensuring timely and accurate delivery. Because it has less overhead, it offers fast communications, but at the expense of possible errors or data loss.
Control protocols	Internet Control Message Protocol (ICMP)	ICMP works closely with IP in providing error and control information, by allowing hosts to exchange packet status information, which helps move the packets through the internetwork. Two common management utilities, <b>ping</b> and <b>tracert</b> , use ICMP messages to check network connectivity. ICMP also works with IP to send notices when destinations are unreachable, when devices' buffers overflow, the route and hops packets take through the network, and whether devices can communicate across the network.
	Internet Group Membership Protocol (IGMP)	IGMP is a protocol for defining host groups. All group members can receive broadcast messages intended for the group (called multicasts). Multicast groups can be composed of devices within the same network or across networks (connected with a router).

The TCP/IP protocol suite was developed to work independently of the physical network architecture. You can use a wide variety of architectures with the TCP/IP protocol suite.

## Internet Connectivity Parameters

The following table summarizes the configuration settings required to connect to a TCP/IP network.

Parameter	Purpose
IP address	The IP address identifies both the logical host and the logical network addresses. <ul style="list-style-type: none"> <li>• Each host on the entire network must have a unique IP address.</li> <li>• Two devices on the same subnet must have IP addresses with the same network portion of the address.</li> <li>• Two devices on the same subnet must have unique host portions of the IP address.</li> <li>• Do not use the first or the last host address on a subnet address range.</li> </ul>
Subnet mask	The subnet mask identifies which portion of the IP address is the network address, and which portion is the host address. Two devices on the same subnet must be configured with the same subnet mask.
Default gateway	The default gateway identifies the router to which communications for remote networks are sent. The default gateway address is the IP address of the router interface on the same subnet as the local host. Without a default gateway set, most clients will be unable to communicate with hosts outside of the local subnet.

DNS server	The DNS server address identifies the DNS server that is used to resolve host names to IP addresses.
Host name	The host name identifies the logical name of the local system.

## Internet Connectivity Parameters

The following table summarizes the configuration settings required to connect to a TCP/IP network.

Parameter	Purpose
IP address	<p>The IP address identifies both the logical host and the logical network addresses.</p> <ul style="list-style-type: none"> <li>• Each host on the entire network must have a unique IP address.</li> <li>• Two devices on the same subnet must have IP addresses with the same network portion of the address.</li> <li>• Two devices on the same subnet must have unique host portions of the IP address.</li> <li>• Do not use the first or the last host address on a subnet address range.</li> </ul>
Subnet mask	The subnet mask identifies which portion of the IP address is the network address, and which portion is the host address. Two devices on the same subnet must be configured with the same subnet mask.
Default gateway	The default gateway identifies the router to which communications for remote networks are sent. The default gateway address is the IP address of the router interface on the same subnet as the local host. Without a default gateway set, most clients will be unable to communicate with hosts outside of the local subnet.
DNS server	The DNS server address identifies the DNS server that is used to resolve host names to IP addresses.
Host name	The host name identifies the logical name of the local system.

## OSI Layer Facts

The following table compares the functions performed at each OSI model layer.

Layer	Description and Keywords
Application (Layer 7)	<p>The Application layer integrates network functionality into the host operating system, and enables network services. The Application layer does not include specific applications that provide services, but rather provides the capability for services to operate on the network.</p> <p>Most Application layer protocols operate at multiple layers down to the Session and even Transport layers. However, they are classified as Application layer protocols because they start at the Application layer (the Application layer is the highest layer where they operate). Services typically associated with the Application layer include:</p> <ul style="list-style-type: none"> <li>• HTTP</li> <li>• Telnet</li> </ul>



		<ul style="list-style-type: none"> <li>• FTP</li> <li>• TFTP</li> <li>• SNMP</li> </ul>
Presentation (Layer 6)		<p>The Presentation layer formats or "presents" data into a compatible form for receipt by the Application layer or the destination system. Specifically, the Presentation layer ensures:</p> <ul style="list-style-type: none"> <li>• Formatting and translation of data between systems.</li> <li>• Negotiation of data transfer syntax between systems, through converting character sets to the correct format.</li> <li>• Encapsulation of data into message envelopes by encryption and compression.</li> <li>• Restoration of data by decryption and decompression.</li> </ul>
Session (Layer 5)		<p>The Session layer's primary function is managing the sessions in which data is transferred. Functions at this layer include:</p> <ul style="list-style-type: none"> <li>• Management of multiple sessions (each client connection is called a <i>session</i>). A server can concurrently maintain thousands of sessions.</li> <li>• Assignment of the session ID number to each session to keep data streams separate.</li> <li>• Set up, maintain, and tear down communication sessions.</li> </ul>
Transport (Layer 4)		<p>The Transport layer provides a transition between the upper and lower layers of the OSI model, making the upper and lower layers transparent from each other. Transport layer functions include:</p> <ul style="list-style-type: none"> <li>• End-to-end flow control.</li> <li>• Port and socket numbers.</li> <li>• Segmentation, sequencing, and combination.</li> <li>• Connection services, either reliable (connection-oriented) or unreliable (connectionless) delivery of data.</li> </ul> <p>Data at the Transport layer is referred to as a <i>segment</i>.</p>
Network (Layer 3)		<p>The Network layer describes how data is routed across networks and on to the destination. Network layer functions include:</p> <ul style="list-style-type: none"> <li>• Identifying hosts and networks using logical addresses.</li> <li>• Maintaining a list of known networks and neighboring routers.</li> <li>• Determining the next network point to which data should be sent. Routers use a routing protocol to take into account various factors such as the number of hops in the path, link speed, and link reliability to select the optimal path for data.</li> </ul> <p>Data at the Network layer is referred to as a <i>packet</i>.</p>
Data Link (Layer 2)	Logical Link Control (LLC)	<p>The Data Link layer defines the rules and procedures for hosts as they access the Physical layer. These rules and procedures specify or define:</p>

	Media Access Control (MAC)	<ul style="list-style-type: none"> <li>• How hosts on the network are identified (physical or MAC address).</li> <li>• How and when devices can transmit on the network medium (media access control and logical topology).</li> <li>• How to verify that the data received from the Physical layer is error free (parity and CRC).</li> <li>• How devices control the rate of data transmissions between hosts (flow control).</li> </ul> <p>Data at the Data Link layer is referred to as a <i>frame</i>.</p>
Physical (Layer 1)		<p>The Physical layer of the OSI model sets standards for sending and receiving electrical signals between devices. Protocols at the Physical layer identify:</p> <ul style="list-style-type: none"> <li>• How digital data (bits) are converted to electric pulses, radio waves, or pulses of lights.</li> <li>• Specifications for cables and connectors.</li> <li>• The physical topology.</li> </ul> <p>Data at the Physical layer is referred to as <i>bits</i>.</p>