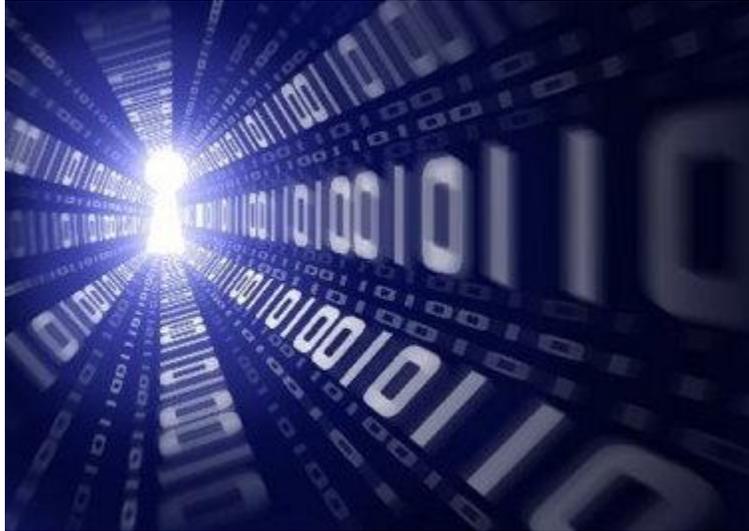


Computer Skills



[Online Safety](#) | [Security Practices](#) | [History](#) | [Components](#) | [Programming](#) | [Software Piracy](#) | [Music Piracy](#)

Online Safety

[Online Safety Details, Prevention, Definition and Good practices](#)

Children

Every year over 3 million children are victims of violence and almost 1.8 million are abducted. Nearly 600,000 children live in foster care. Every day 1 out of 7 kids and teens are approached *online* by predators.

Identity Theft

Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.

Cyber-bullying

Cyber-Bullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others.

Phishing

In computing, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from PayPal, eBay, YouTube or online banks are commonly used to lure the unsuspecting. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a web site. Phishing is an example of social engineering techniques used to fool users. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measure

Virus' and Spies

A computer virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user. The term "virus" is also commonly used, albeit erroneously, to refer to many different types of malware and adware programs. The original virus may modify the copies, or the copies may modify themselves, as occurs in a metamorphic virus. A virus can only spread from one computer to another when its host is taken to the uninfected computer, for instance by a user sending it over a network or the Internet, or by carrying it on a removable medium such as a floppy disk, CD, or USB drive. Meanwhile viruses can spread to other computers by infecting files on a network file system or a file system that is accessed by another computer. Viruses are sometimes confused with computer worms and Trojan horses. A worm can spread itself to other computers without needing to be transferred as part of a host, and a Trojan horse is a file that appears harmless. Worms and Trojans may cause harm to either a computer system's hosted data, functional performance, or networking throughput, when executed. In general, a worm does not actually harm either the system's hardware or software, while at least in theory, a Trojan's payload may be capable of almost any type of harm if executed. Some can't be seen when the program is not running, but as soon as the infected code is run, the Trojan horse kicks in. That is why it is so hard for people to find viruses and other malware themselves and why they have to use spyware programs and registry processors.

Computer surveillance or spying is the act of surveilling people, generally their computer activity, without their knowledge, using the computer itself.

Computers make excellent surveillance tools because they can be programmed (even surreptitiously) to record data without their owners' knowledge or consent. Most computers have connections to networks, which can be exploited (through security cracking) to gain access to any confidential data that may be stored on the computer. Additionally, if someone is able to install certain types of software on a system, they can turn it into an unsuspected surveillance device.

Data Safeguards

Data in this era plays a crucial role in our lives. Data is a source of information that is stored on hard disk drive. Data on hard disk drives is not secure. Virus attack, Human Error, Software malfunction and Software corruption often result in Data Loss.

One of the greatest challenges we have faced during the past decade is maintaining the data integrity and protecting the computer information assets of an organization that is safeguard the data. An organization has many assets building, people, machinery and business information. The business information could be about stocks, accounts, finance, research, engineering, marketing and sales. Automation of business processes has resulted in all the information being stored in computer storage systems instead of the paper.

[- Top -](#)

Eight Cyber Computer Security Practices

[Detailed here](#)

- Protect your personal information. It's valuable.
- Know who you're dealing with online.
- Use anti-virus software, a firewall, and anti-spyware software to help keep your computer safe and secure.

- Be sure to set up your operating system and Web browser software properly, and update them regularly.
- Use strong passwords or strong authentication technology to help protect your personal information.
- Back up important files.
- Learn what to do if something goes wrong.
- Protect children online.

[- Top -](#)

History of Computers

The history of computing is longer than the history of computing hardware and modern computing technology and includes the history of methods intended for pen and paper or for chalk and slate, with or without the aid of tables. The [timeline](#) of computing presents a summary list of major developments in computing by date.

The development of the modern day computer was the result of advances in technologies and man's need to quantify. The abacus was one of the first counting machines. Papyrus helped early man to record language and numbers. Some of the earlier counting machines lacked the technology to make the design work. For instance, some had parts made of wood prior to metal manipulation and manufacturing. Imagine the wear on wooden gears.

[Illustrated History of Computers](#) (John Kopplin © 2002)

[History of Computers #1](#) (PPS 1,951 KB)

[History of Computers #2](#) (PPS 1,878 KB)

[History of Computers #3](#) (PPS 1,178 KB)

[Historic Timeline of Computers](#) (350 millions years ago through 2008)

[- Top -](#)

Parts and Components of a Computer System

[Basic System Components](#) with Descriptions

Input and Output Devices

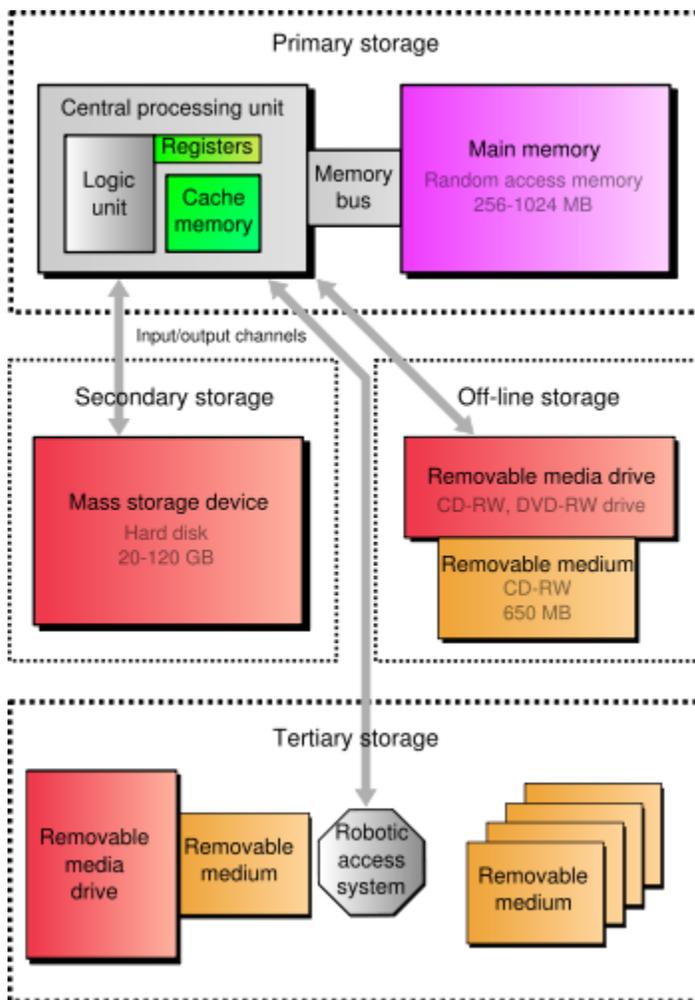
In computing, input/output, or I/O, refers to the communication between an information processing system (such as a computer), and the outside world – possibly a human, or another information processing system. Inputs are the signals or data received by the system, and outputs are the signals or data sent from it. The term can also be used as part of an action; to "perform I/O" is to perform an input or output operation. I/O devices are used by a person (or other system) to communicate with a computer. For instance, keyboards and mice are considered input devices of a computer, while

monitors and printers are considered output devices of a computer. Devices for communication between computers, such as modems and network cards, typically serve for both input and output.

Note that the designation of a device as either input or output depends on the perspective. Mice and keyboards take as input physical movement that the human user outputs and convert it into signals that a computer can understand. The output from these devices is input for the computer. Similarly, printers and monitors take as input signals that a computer outputs. They then convert these signals into representations that human users can see or read. (For a human user the process of reading or seeing these representations is receiving input.)

Today a Thumb Drive or Flash memory device could be considered both input and output, the same as a CD, DVD, Floppy disk or any removable storage medium.

Storage Media



Computer **data storage**, often called **storage** or (incorrectly) **memory**, refers to computer components, devices, and recording media that retain digital data used for computing for some interval of time. Computer data storage provides one of the core functions of the modern computer, that of information retention. It is one of the fundamental components of all modern computers, and coupled with a central processing unit (CPU, a processor), implements the basic computer model used since the 1940s.

In contemporary usage, memory usually refers to a form of semiconductor storage known as random access memory (RAM) and sometimes other forms of fast but temporary storage. Similarly, storage today more commonly refers to mass storage - optical discs, forms of magnetic storage like hard

disks, and other types slower than RAM, but of a more permanent nature. Historically, memory and storage were respectively called primary storage and secondary storage.

The contemporary distinctions are helpful, because they are also fundamental to the architecture of computers in general. As well, they reflect an important and significant technical difference between memory and mass storage devices, which has been blurred by the historical usage of the term storage. Nevertheless, this article uses the traditional nomenclature.

Various forms of storage, based on various natural phenomena, have been invented. So far, no practical universal storage medium exists, and all forms of storage have some drawbacks. Therefore a computer system usually contains several kinds of storage, each with an individual purpose.

A digital computer represents each datum using the binary numeral system. Text, numbers, pictures, audio, and nearly any other form of information can be converted into a string of bits, or binary digits, each of which has a value of 1 or 0. The most common unit of storage is the byte, equal to 8 bits. A piece of information can be handled by any computer whose storage space is large enough to accommodate the binary representation of the piece of information, or simply data. For example, using eight million bits, or about one megabyte, a typical computer could store a small novel.

Traditionally the most important part of every computer is the central processing unit (CPU, or simply a processor), because it actually operates on data, performs any calculations, and controls all the other components.

Without significant amount of memory, a computer would merely be able to perform fixed operations and immediately output the result. It would have to be reconfigured to change its behavior. This is acceptable for devices such as desk calculators or simple digital signal processors. Von Neumann machines differ in that they have a memory in which they store their operating instructions and data. Such computers are more versatile in that they do not need to have their hardware reconfigured for each new program, but can simply be reprogrammed with new in-memory instructions; they also tend to be simpler to design, in that a relatively simple processor may keep state between successive computations to build up complex procedural results. Most modern computers are von Neumann machines.

In practice, almost all computers use a variety of memory types, organized in a storage hierarchy around the CPU, as a tradeoff between performance and cost. Generally, the lower a storage is in the hierarchy, the lesser its bandwidth and the greater its access latency is from the CPU. This traditional division of storage to primary, secondary, tertiary and off-line storage is also guided by cost per bit.

[- Top -](#)

There are 4 types of storage:

Primary storage

Primary storage, presently known as memory, is the only one directly accessible to the CPU. The CPU continuously reads instructions stored there and executes them. Any data actively operated on is also stored there in uniform manner.

Secondary storage

Secondary storage, or *storage* in popular usage, differs from primary storage in that it is not directly accessible by the CPU. The computer usually uses its input/output channels to access secondary storage and transfers desired data using intermediate area in primary storage. Secondary storage does not lose the data when the device is powered down—it is non-volatile. Per unit, it is typically also an

order of magnitude less expensive than primary storage. Consequently, modern computer systems typically have an order of magnitude more secondary storage than primary storage and data is kept for a longer time there.

In modern computers, hard disks are usually used as secondary storage. The time taken to access a given byte of information stored on a hard disk is typically a few thousandths of a second, or milliseconds. By contrast, the time taken to access a given byte of information stored in random access memory is measured in billionths of a second, or nanoseconds. This illustrates the very significant access-time difference which distinguishes solid-state memory from rotating magnetic storage devices: hard disks are typically about a million times slower than memory. Rotating optical storage devices, such as CD and DVD drives, have even longer access times.

Tertiary storage

Tertiary storage or tertiary memory, provides a third level of storage. Typically it involves a robotic mechanism which will mount (insert) and dismount removable mass storage media into a storage device according to the system's demands; this data is often copied to secondary storage before use. It is primarily used for archival of rarely accessed information since it is much slower than secondary storage (e.g. 5-60 seconds vs. 1-10 milliseconds). This is primarily useful for extraordinarily large data stores, accessed without human operators. Typical examples include tape libraries and optical jukeboxes.

When a computer needs to read information from the tertiary storage, it will first consult a catalog database to determine which tape or disc contains the information. Next, the computer will instruct a robotic arm to fetch the medium and place it in a drive. When the computer has finished reading the information, the robotic arm will return the medium to its place in the library.

Off-line storage

Off-line storage, also known as disconnected storage, is a computer data storage on a medium or a device that is not under the control of a processing unit.[3] The medium is recorded, usually in a secondary or tertiary storage device, and then physically removed or disconnected. It must be inserted or connected by a human operator before a computer can access it again. Unlike tertiary storage, it cannot be accessed without human interaction.

Off-line storage is used to transfer information, since the detached medium can be easily physically transported. Additionally in case a disaster, for example a fire, destroys the original data, a medium in a remote location will be probably unaffected, enabling disaster recovery. Off-line storage increases a general information security, since it is physically inaccessible from a computer, and data confidentiality or integrity cannot be affected by computer-based attack techniques. Also, if the information stored for archival purposes is accessed seldom or never, off-line storage is less expensive than tertiary storage.

In modern personal computers, most secondary and tertiary storage media are also used for off-line storage. Optical discs and flash memory devices are most popular, and to much lesser extent removable hard disk drives. In enterprise uses, magnetic tape is predominant. Older examples are floppy disks, Zip disks, or punched cards.

Memory

When you think about it, it's amazing how many different types of electronic memory you encounter in daily life. Many of them have become an integral part of our vocabulary, here is a basic list of the common types of things we call memory today:

- RAM

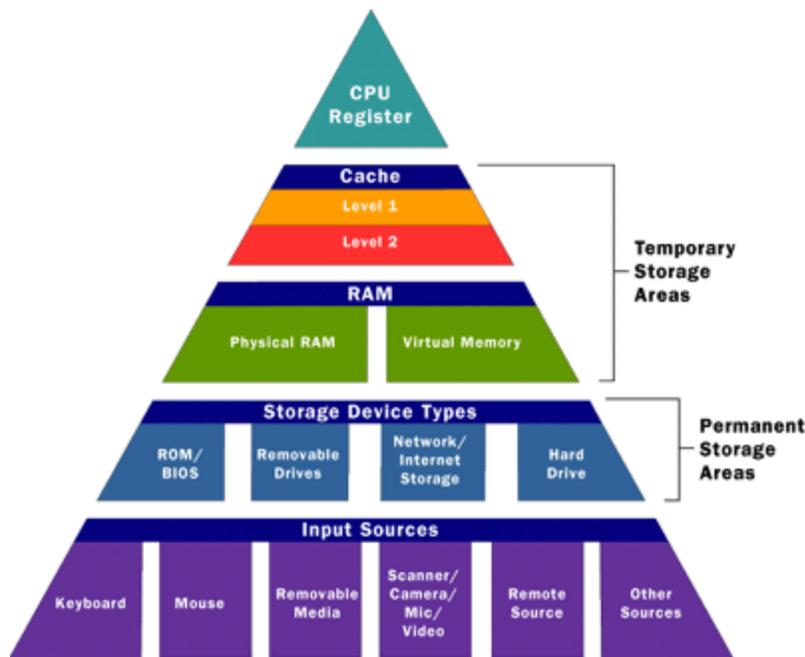
- ROM
- Cache
- Dynamic RAM
- Static RAM
- Flash memory
- Memory Sticks
- Virtual memory
- Video memory
- BIOS

[-Top-](#)

You already know that the computer in front of you has memory. What you may not know is that most of the electronic items you use every day have some form of memory also. Here are just a few examples of the many items that use memory

- Cell phones
- PDA
- Xbox
- Wii
- PS2
- Gameboys
- Ipods
- Zune
- TV
- VCR
- DVD/DVR
- Microwaves
- Many, many more

Although memory is technically any form of electronic storage, it is used most often to identify fast, temporary forms of storage. If your computer's CPU had to constantly access the hard drive to retrieve every piece of data it needs, it would operate very slowly. When the information is kept in memory, the CPU can access it much more quickly. Most forms of memory are intended to store data temporarily.



As you can see in the diagram above, the CPU accesses memory according to a distinct hierarchy. Whether it comes from permanent storage (the hard drive) or input (the keyboard), most data goes in random access memory (RAM) first. The CPU then stores pieces of data it will need to access, often in a cache, and maintains certain special instructions in the register.

All of the components in your computer, such as the CPU, the hard drive and the operating system, work together as a team, and memory is one of the most essential parts of this team. From the moment you turn your computer on until the time you shut it down, your CPU is constantly using memory. Let's take a look at a typical scenario:

1. You turn the computer on.
2. The computer loads data from read-only memory (ROM) and performs a power-on self-test (POST) to make sure all the major components are functioning properly. As part of this test, the memory controller checks all of the memory addresses with a quick read/write operation to ensure that there are no errors in the memory chips. Read/write means that data is written to a bit and then read from that bit.
3. The computer loads the basic input/output system (BIOS) from ROM. The BIOS provides the most basic information about storage devices, boot sequence, security, Plug and Play (auto device recognition) capability and a few other items.
4. The computer loads the operating system (OS) from the hard drive into the system's RAM. Generally, the critical parts of the operating system are maintained in RAM as long as the computer is on. This allows the CPU to have immediate access to the operating system, which enhances the performance and functionality of the overall system.
5. When you open an application, it is loaded into RAM. To conserve RAM usage, many applications load only the essential parts of the program initially and then load other pieces as needed.
6. After an application is loaded, any files that are opened for use in that application are loaded into RAM.
7. When you save a file and close the application, the file is written to the specified storage device, and then it and the application are purged from RAM. In the list above, every time something is loaded or opened, it is placed into RAM. This simply means that it has been put in the computer's temporary storage area so that the CPU can access that information more easily. The CPU requests the data it needs from RAM, processes it and writes new data back

to RAM in a continuous cycle. In most computers, this shuffling of data between the CPU and RAM happens millions of times every second. When an application is closed, it and any accompanying files are usually purged (deleted) from RAM to make room for new data. If the changed files are not saved to a permanent storage device before being purged, they are lost. One common question about desktop computers that comes up all the time is,

"Why does a computer need so many memory systems?"

In the list above, every time something is loaded or opened, it is placed into RAM. This simply means that it has been put in the computer's temporary storage area so that the CPU can access that information more easily. The CPU requests the data it needs from RAM, processes it and writes new data back to RAM in a continuous cycle. In most computers, this shuffling of data between the CPU and RAM happens millions of times every second. When an application is closed, it and any accompanying files are usually purged (deleted) from RAM to make room for new data. If the changed files are not saved to a permanent storage device before being purged, they are lost.

[- Top -](#)

Processors

There are many types of "processors", commonly referred to as the "Brains" of the computer.

The fundamental operation of most CPUs, regardless of the physical form they take, is to execute a sequence of stored instructions called a program. The program is represented by a series of numbers that are kept in some kind of computer memory. There are four steps that nearly all von Neumann CPUs use in their operation: **fetch, decode, execute, and writeback.**

A **Central Processing Unit** (CPU), or sometimes just called **processor**, is a description of a class of logic machines that can execute computer programs. This broad definition can easily be applied to many early computers that existed long before the term "CPU" ever came into widespread usage. The term itself and its initialism have been in use in the computer industry at least since the early 1960s (Weik 1961). The form, design and implementation of CPUs have changed dramatically since the earliest examples, but their fundamental operation has remained much the same.

Early CPUs were custom-designed as a part of a larger, sometimes one-of-a-kind, computer. However, this costly method of designing custom CPUs for a particular application has largely given way to the development of mass-produced processors that are suited for one or many purposes. This standardization trend generally began in the era of discrete transistor mainframes and minicomputers and has rapidly accelerated with the popularization of the integrated circuit (IC). The IC has allowed increasingly complex CPUs to be designed and manufactured to tolerances on the order of nanometers. Both the miniaturization and standardization of CPUs have increased the presence of these digital devices in modern life far beyond the limited application of dedicated computing machines. Modern microprocessors appear in everything from automobiles to cell phones to children's toys.

A **microprocessor** incorporates most or all of the functions of a central processing unit (CPU) on a single integrated circuit (IC). The first microprocessors emerged in the early 1970s and were used for electronic calculators, using BCD arithmetic on 4-bit words. Other embedded uses of 4 and 8-bit microprocessors, such as terminals, printers, various kinds of automation etc, followed rather quickly. Affordable 8-bit microprocessors with 16-bit addressing also led to the first general purpose microcomputers in the mid-1970s.

Processors were for a long period constructed out of small and medium-scale ICs containing the equivalent of a few to a few hundred transistors. The integration of the whole CPU onto a single VLSI chip therefore greatly reduced the cost of processing capacity. From their humble beginnings, continued increases in microprocessor capacity have rendered other forms of computers almost completely obsolete (see history of computing hardware), with one or more microprocessor as processing element in everything from the smallest embedded systems and handheld devices to the largest mainframes and supercomputers.

Since the early 1970s, the increase in processing capacity of evolving microprocessors has been known to generally follow Moore's Law. It suggests that the complexity of an integrated circuit, with respect to minimum component cost, doubles every 18 months. In the late 1990s, heat generation (TDP), due to current leakage and other factors, emerged as a leading developmental constraint.

[-Top -](#)

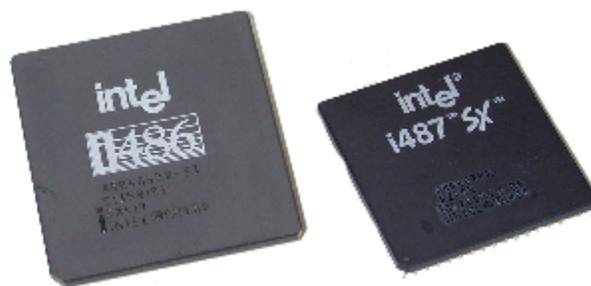
Co-Processors

A co-processor is NOT a dual processor. A dual processor is an exact duplicate of the first to double computer power and generally more than doubling the cost of the computer.

A coprocessor is a computer processor used to supplement the functions of the primary processor (the CPU). Operations performed by the coprocessor may be floating point arithmetic, graphics, signal processing, string processing, or encryption. By offloading processor-intensive tasks from the main processor, coprocessors can accelerate system performance. Coprocessors allow a line of computers to be customized, so that customers who do not need the extra performance need not pay for it.

Coprocessors were first seen on mainframe computers, where they added additional "optional" functionality such as floating point math support. A more common use was to control input/output channels, although in this role they were more often referred to as channel controllers.

Back in the day, or back during the beginning of the modern computing age almost every personal computer came with a co-processor slot. If you bought a computer with an Intel 8088 processor you could add in an 8087 co-processor which was a mathematical floating point processor.



Click for larger images

The last one I remember seeing that was common was around 1989 when Intel put out the 80486 chip and its processor was the 80487. Again a floating point chip to speed up math functions. See above for illustration.

[-Top -](#)

Modems



What exactly is a modem? Well it happens to be an Acronym for "**modulator-demodulator**". It is a device that modulates an analog carrier signal to encode digital information, and also demodulates such a carrier signal to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data. Modems can be used over any means of transmitting analog signals, from driven diodes to radio.

The most familiar example is a voice and modem that turns the digital 1s and 0s of a personal computer into sounds that can be transmitted over the telephone lines of Plain Old Telephone Systems (POTS), and once received on the other side, converts those 1s and 0s back into a form used by a USB, Ethernet, serial, or network connection. Modems are generally classified by the amount of data they can send in a given time, normally measured in bits per second, or "bps". They can also be classified by Baud, the number of times the modem changes its signal state per second.

Baud is NOT the modem's speed. The baud rate varies, depending on the modulation technique used. Original Bell 103 modems used a modulation technique that saw a change in state 300 times per second. They transmitted 1 bit for every baud, and so a 300 bit/s modem was also a 300-baud modem. However, casual computerists confused the two. A 300 bit/s modem is the only modem whose bit rate matches the baud rate. A 2400 bit/s modem changes state 600 times per second, but due to the fact that it transmits 4 bits for each baud, 2400 bits are transmitted by 600 baud, or changes in states.

Faster modems are used by Internet users every day, notably cable modems and ADSL modems. In telecommunications, "radio modems" transmit repeating frames of data at very high data rates over microwave radio links. Some microwave modems transmit more than a hundred million bits per second. Optical modems transmit data over optical fibers. Most intercontinental data links now use optical modems transmitting over undersea optical fibers. Optical modems routinely have data rates in excess of a billion (1×10^9) bits per second. One kilobit per second (kbit/s or kb/s or kbps) as used in this article means 1000 bits per second and not 1024 bits per second. For example, a 56k modem can transfer data at up to 56,000 bits per second over the phone line.

Mobile Modems - Modems which use mobile phone lines (GPRS, UMTS, HSPA, EVDO, WiMax, etc.), are known as Cellular Modems. Cellular modems can be embedded inside a laptop or appliance, or they can be external to it. External cellular modems are data cards and cellular routers. The data card is a PC card or Express Card which slides into a PCMCIA/PC card/Express Card slot on a computer. The most famous brand of Radio modem data cards is the Air Card made by Sierra Wireless. (Many people just refer to all makes and models as "AirCards", when in fact this is a trademarked brand name.) Nowadays, there are USB cellular modems as well that use a USB port on the laptop instead of a PC card or Express card slot. A cellular router may or may not have an external data card ("Air card") that slides into it. Most cellular routers do allow such data cards or USB modems, except for the WAAV, Inc. CM3 mobile broadband cellular router. Cellular Routers may not be modems per se,

but they contain modems or allow modems to be slid into them. The difference between a cellular router and a cellular modem is that a cellular router normally allows multiple people to connect to it (since it can "route"), while the modem is made for one connection.

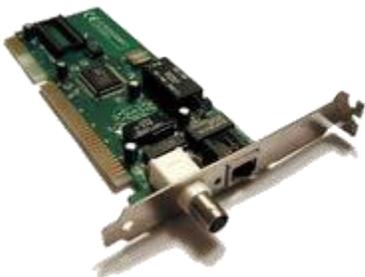
Voice modem Voice modems are regular modems that are capable of recording or playing audio over the telephone line. They are used for telephony applications. See Voice modem command set for more details on voice modems. This type of modem can be used as FXO card for Private branch exchange systems (compare V.92).

[- Top -](#)

Broadband Modems

- **ADSL modems**, a more recent development, are not limited to the telephone's "voice band" audio frequencies. Some ADSL modems use coded orthogonal frequency division modulation (DMT).
- **Cable modems** use a range of frequencies originally intended to carry RF television channels. Multiple cable modems attached to a single cable can use the same frequency band, using a low-level media access protocol to allow them to work together within the same channel. Typically, 'up' and 'down' signals are kept separate using frequency division multiple access.
- New types of broadband modems are beginning to appear, such as doubleway satellite and power line modems.
- Broadband modems should still be classed as modems, since they use complex waveforms to carry digital data. They are more advanced devices than traditional dial-up modems as they are capable of modulating/demodulating hundreds of channels simultaneously.
- Many broadband modems include the functions of a router (with Ethernet and WiFi ports) and other features such as DHCP, NAT and firewall features.
- When broadband technology was introduced, networking and routers were unfamiliar to consumers. However, many people knew what a modem was as most internet access was through dialup. Due to this familiarity, companies started selling broadband modems using the familiar term "modem" rather than vaguer ones like "adapter" or "transceiver".
- Many broadband modems must be configured in bridge mode before they can use a router.

Network Cards



A network card is an expansion card which installs into a computer and enables that computer to physically connect to a local area network.

The most common form of network card in current use is the Ethernet card. Other types of network cards include wireless network cards and Token Ring network cards.

Ethernet network cards most often use RJ-45 jacks. Wireless network cards usually have no external connections other than a possible antenna jack.

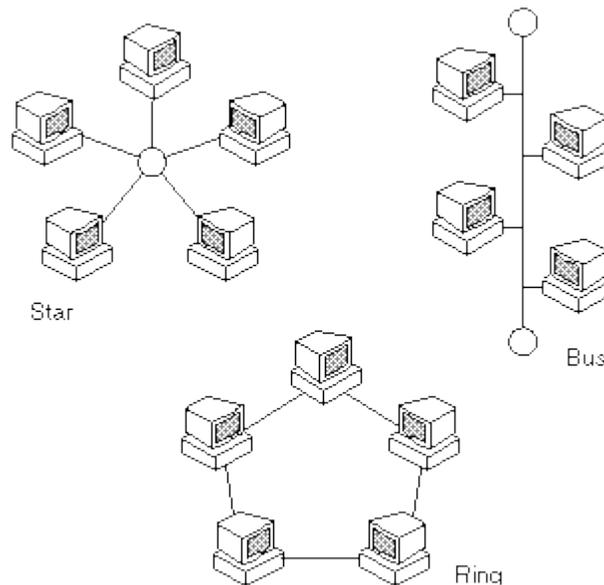
Other terms for network card include network adapter, network interface card and NIC.

A Network card, Network Adapter, LAN Adapter or NIC (network interface card) is a piece of computer hardware designed to allow computers to communicate over a computer network. It is both an OSI layer 1 (physical layer) and layer 2 (data link layer) device, as it provides physical access to a networking medium and provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using cables or wirelessly.

[- Top -](#)

Networks

In the world of computers, networking is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software.



Computer networks allow you to share files with friends, family, coworkers and customers. Before the Internet and home networks became popular, files were often shared using floppy disks. Nowadays, some people still use CD-ROM / DVD-ROM disks and USB keys for transferring their photos and videos, but networks give you more flexible options.

Network file sharing is the process of copying files from one computer to another using a live network connection. This article describes the different methods and networking technologies available to help you share files.

Microsoft Windows (and other personal computer operating systems) contain built-in features for file sharing. For example, Windows file folders can be shared across a local area network (LAN) or the Internet using the Explorer interface and network drive mappings. You can also set up security access restrictions that control who can obtain the shared files.

Networks can be categorized in several different ways. One approach defines the type of network according to the geographic area it spans. Local area networks (LAN's), for example, typically reach across a single home, whereas wide area networks (WAN's), reach across cities, states, or even across the world. The Internet is the world's largest public WAN.

Many of the same network protocols, like TCP/IP, work in both wired and wireless networks. Networks with Ethernet cables predominated in businesses, schools, and homes for several decades. Recently, however, wireless networking alternatives have emerged as the premier technology for building new computer networks.

From [Webopedia](#) and [WikiPedia](#)

[- Top -](#)

World Wide Web/Internet

A system of Internet servers that support specially formatted documents. The documents are formatted in a markup language called HTML (HyperText Markup Language) that supports links to other documents, as well as graphics, audio, and video files. This means you can jump from one document to another simply by clicking on hot spots. Not all Internet servers are part of the World Wide Web.

There are several applications called Web browsers that make it easy to access the World Wide Web; Two of the most popular being Mozilla Firefox and for reason's unknown, Microsoft's Internet Explorer.

World Wide Web is not synonymous with the Internet.

Many people use the terms Internet and World Wide Web (aka. the Web) interchangeably, but in fact the two terms are not synonymous. The Internet and the Web are two separate but related things.

The Internet is a massive network of networks, a networking infrastructure. It connects millions of computers together globally, forming a network in which any computer can communicate with any other computer as long as they are both connected to the Internet. Information that travels over the Internet does so via a variety of languages known as protocols.

The World Wide Web, or simply Web, is a way of accessing information over the medium of the Internet. It is an information-sharing model that is built on top of the Internet. The Web uses the HTTP protocol, only one of the languages spoken over the Internet, to transmit data. Web services, which use HTTP to allow applications to communicate in order to exchange business logic, use the the Web to share information. The Web also utilizes browsers, such as Internet Explorer or Firefox, to access Web documents called Web pages that are linked to each other via hyperlinks. Web documents also contain graphics, sounds, text and video.

The Web is just one of the ways that information can be disseminated over the Internet. The Internet, not the Web, is also used for e-mail, which relies on SMTP, Usenet news groups, instant messaging and FTP. So the Web is just a portion of the Internet, albeit a large portion, but the two terms are not synonymous and should not be confused.

The World Wide Web (commonly shortened to the Web) is a system of interlinked hypertext documents accessed via the Internet. With a Web browser, a user views Web pages that may contain text, images, videos, and other multimedia and navigates between them using hyperlinks. The World Wide Web was created in 1989 by Sir Tim Berners-Lee, working at the European Organization for Nuclear Research (CERN) in Geneva, Switzerland and released in 1992. Since then, Berners-Lee has played an active role in guiding the development of Web standards (such as the markup languages in which Web pages are composed), and in recent years has advocated his vision of a Semantic Web.

Electronic Mail

E-Mail — Short for electronic mail, the transmission of messages over communications networks. The messages can be notes entered from the keyboard or electronic files stored on disk. Most mainframes, minicomputers, and computer networks have an e-mail system. Some electronic-mail systems are confined to a single computer system or network, but others have gateways to other computer systems, enabling users to send electronic mail anywhere in the world. Companies that are fully computerized make extensive use of e-mail because it is fast, flexible, reliable and most important - Free.

Most e-mail systems include a basic text editor for composing messages, but many allow you to edit your messages using any editor you want. You then send the message to the recipient by specifying the recipient's address. You can also send the same message to several users at once. This is called broadcasting.

Sent messages are stored in electronic mailboxes until the recipient fetches them. To see if you have any mail, you may have to check your electronic mailbox periodically, although many systems alert you when mail is received. After reading your mail, you can store it in a text file, forward it to other users, or delete it. Copies of memos can be printed out on a printer if you want a paper copy.

All online services and Internet Service Providers (ISP's) offer e-mail, and most also support gateways so that you can exchange mail with users of other systems. Usually, it takes only a few seconds or minutes for mail to arrive at its destination. This is a particularly effective way to communicate with a group because you can broadcast a message or document to everyone in the group at once.

[- Top -](#)

WiFi

The name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. The WiFi Alliance, the organization that owns the Wifi (registered trademark) term specifically defines Wifi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards."

Initially, Wifi was used in place of only the 2.4GHz 802.11b standard, however the Wifi Alliance has expanded the generic use of the Wifi term to include any type of network or WLAN product based on any of the 802.11 standards, including 802.11b, 802.11a, dual-band, and so on, in an attempt to stop confusion about wireless LAN interoperability.

Wifi works with no physical wired connection between sender and receiver by using radio frequency (RF) technology, a frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space. The cornerstone of any wireless network is an access point (AP). The primary job of an access point is to broadcast a wireless signal that computers can detect and "tune" into. In order to connect to an access point and join a wireless network, computers and devices must be equipped with wireless network adapters.

Wifi is supported by many applications and devices including video game consoles, home networks, PDA's, mobile phones, major operating systems, and other types of consumer electronics. Any products that are tested and approved as "Wifi Certified" (a registered trademark) by the Wifi Alliance

are certified as interoperable with each other, even if they are from different manufacturers. For example, a user with a Wifi Certified product can use any brand of access point with any other brand of client hardware that also is also "Wifi Certified". Products that pass this certification are required to carry an identifying seal on their packaging that states "Wifi Certified" and indicates the radio frequency band used (2.5GHz for 802.11b, 802.11g, or 802.11n, and 5GHz for 802.11a).

A common misconception is that the term Wifi is short for "wireless fidelity," however this is not the case. Wifi is simply a trademarked term meaning IEEE 802.11x.

From [Webopedia](#)

[-Top-](#)

Computer Programs

What is it?

An organized list of instructions that, when executed, causes the computer to behave in a predetermined manner. Without programs, computers are useless.

A program is like a recipe. It contains a list of ingredients (called variables) and a list of directions (called statements) that tell the computer what to do with the variables. The variables can represent numeric data, text, or graphical images.

There are many programming languages -- C, C++, Java, Assembly, Pascal, BASIC, FORTRAN, COBOL, and LISP are just a few. These are all high-level languages. One can also write programs in low-level languages called assembly languages, although this is more difficult. Low-level languages are closer to the language used by a computer, while high-level languages are closer to human languages.

Eventually, every program must be translated into a machine language that the computer can understand. This translation is performed by compilers, interpreters, and assemblers.

When you buy software, you normally buy an executable version of a program. This means that the program is already in machine language -- it has already been compiled and assembled and is ready to execute.

How is it done?

Computer software engineers apply the principles of computer science and mathematical analysis to the design, development, testing, and evaluation of the software and systems that make computers work. The tasks performed by these workers evolve quickly, reflecting new areas of specialization or changes in technology, as well as the preferences and practices of employers. (A separate section on computer hardware engineers appears in the engineers section of the Handbook.)

Software engineers can be involved in the design and development of many types of software, including computer games, word processing and business applications, operating systems and network distribution, and compilers, which convert programs to machine language for execution on a computer.

Computer software engineers begin by analyzing users' needs, and then design, test, and develop software to meet those needs. During this process they create the detailed sets of instructions, called algorithms, that tell the computer what to do. They also may be responsible for converting these instructions into a computer language, a process called programming or coding, but this usually is the responsibility of computer programmers. Computer software engineers must be experts in operating systems and middleware to ensure that the underlying systems will work properly.

Computer applications software engineers analyze users' needs and design, construct, and maintain general computer applications software or specialized utility programs. These workers use different programming languages, depending on the purpose of the program. The programming languages most often used are C, C++, and Java, with Fortran and COBOL used less commonly. Some software engineers develop both packaged systems and systems software or create customized applications.

Computer systems software engineers coordinate the construction, maintenance, and expansion of an organization's computer systems. Working with the organization, they coordinate each department's computer needs—ordering, inventory, billing, and payroll record keeping, for example—and make suggestions about its technical direction. They also might set up the organization's intranet's—networks that link computers within the organization and ease communication among various departments.

Systems software engineers also work for companies that configure, implement, and install the computer systems of other organizations. These workers may be members of the marketing or sales staff, serving as the primary technical resource for sales workers. They also may help with sales and provide customers with technical support. Since the selling of complex computer systems often requires substantial customization to meet the needs of the purchaser, software engineers help to identify and explain needed changes. In addition, systems software engineers are responsible for ensuring security across the systems they are configuring.

Computer software engineers often work as part of a team that designs new hardware, software, and systems. A core team may comprise engineering, marketing, manufacturing, and design people, who work together to release a product.

[- Top -](#)

Software Piracy

"Hey man that's a really excellent program, I wish I had that"
"No problem, I'll burn you a copy and you can take it home"
Cool?

No. Illegal.



What is Software Piracy?

Software piracy is the unauthorized use of software. It includes the illegal duplication of copyrighted software or the installation of copyrighted software on more computers than authorized under terms of the software license agreement. (Encarta® World English Dictionary [North American Edition] © & (P) 2001 Microsoft Corporation. All rights reserved. Developed for Microsoft by Bloomsbury Publishing Plc.)

When an individual or institution purchases software, they only purchase the right to use the software. The copyright belongs to the developers of corporation who produces the software.

Isn't it okay to use a software program on any number of machines? - No, you can only use the software for the number of licenses purchased. For example, it is illegal to copy a software program from your office machine to use at home even if it is for work purposes unless you purchase an additional license for the additional machine. It is also illegal to loan or to create copies of software and give it to friends.

What are my responsibilities as a consumer? - Purchase only legal copies of software. Legal copies can include discs, manuals, and registration numbers. In addition, install only on machines you have purchased licenses for, if you buy one copy you may only install one copy on one machine.

What are the maximum civil penalties for copyright infringement? - If convicted, conspiracy to infringe a copyright carries a maximum penalty of five years in prison and a \$250,000 fine, or, as an alternative, the Court may impose a fine totaling twice the gross gain to any defendant or twice the gross loss to any victim, whichever is greater. Restitution is mandatory. The Court, however, would determine the appropriate sentence to be imposed under the United States Sentencing Guidelines. Taken from "<http://www.usdoj.gov/criminal/cybercrime/pirates.htm>"

What exactly does the law say about copying software? - The law says that anyone who purchases a copy of software has the right to load that copy onto a single computer and to make another copy "for archival purposes only". It is illegal to use that software on more than one computer.

Documents from <http://www.siaa.net>

[Software Use & the Law](#)

[The Copyright Act & Fair Use](#)

[The US Code](#)

[- Top -](#)

Music Piracy

"Cool song, can I make a copy for my iPod™"

"Sure, I download it myself last night"

Cool?

No. Illegal. Punishable by up to 5 years in prison and a fine of up to \$250,000.

First off, who is the definitive authority on this? You can find contradicting policy, law, etc all over the World Wide Web.

For this section, I've used "[Recording Industry Association of America](#)" as my prime resource on music piracy. I would suggest that ALL parents and Kids check this site out before they get involved with something that could significantly change your life for the worse.

The Facts

Music piracy is any form of unauthorized duplication and/or distribution of music including downloading, file sharing, and CD-burning.

Most of us would never even consider stealing something—say, a picture or a piece of clothing — from a friend's house. Our sense of right and wrong keeps most of us from doing something so selfish and antisocial. Yet when it comes to stealing digital recordings of copyrighted music, people somehow seem to think the same rules don't apply—even though criminal penalties can be as high as five years in prison or \$250,000 in fines. Contrary to popular opinion, illegally downloading or copying copyrighted music is the same as stealing; there is no difference.

Stealing music is the same as stealing anything else. It is illegal and the consequences are real - for you and for the music.

- Stealing music is against the law.
- Stealing music betrays the songwriters and recording artists who create it.
- Stealing music stifles the careers of new artists and up-and-coming bands.
- Stealing music threatens the livelihood of the thousands of working people—from recording engineers to music retailers and their staffs.

Enjoy the music! But please respect copyrights. Stop burning multiple copies. Stop offering to upload music files to millions of users on the Internet. Stop downloading from unauthorized sites.

Music piracy doesn't just affect the music industry, it affects you as well. When you use software that facilitates illegal downloads, you open your computer to unwanted pornography, security breaches, and viruses. Illegal downloading and file-sharing is also subject to federal prosecution. Here are a few facts:

- The RIAA (Recording Industry Association of America) can sue for as much as \$150,000 per song illegally downloaded.
- Almost 4000 individuals have been sued by the RIAA for illegally downloading as of March, 2008.
- More than 900 individuals have settled, paying fines averaging \$3000.
- The Department of Justice recently announced the creation of the Intellectual Property Task Force, which examines all aspects of how the DOJ handles intellectual property issues.

The explosion in illegal copying is affecting the entire music community. It has a very real and harmful impact on virtually everyone - from countless musicians, songwriters, performers, producers, recording engineers and others who use music as their platform as their voice.

What is Copyright©?

The principle that the work one has created belongs to the creator and should be controlled by them is as timeless as it is global. Around the world, this principle is encoded in law. "Copyright" is a term of intellectual property law that prohibits the unauthorized duplication, adaptation or distribution of a creative work. In the recording industry, there are usually two copyrighted works involved:

1. The copyright in the musical composition, i.e. the actual lyrics and notes on paper. This is usually owned by the songwriter or music publisher.
2. The copyright in the sound recording, i.e. the recording of the performer singing or playing a given song. This is usually owned by the record company.

On the federal level, titles 17 and 18 of the U.S. Code protect copyright owners from the unauthorized reproduction, adaptation or distribution of sound recordings, as well as certain digital performances to the public. The penalties differ slightly, depending upon whether the infringing activity is for commercial advantage or private financial gain. Under U.S. copyright law, "financial gain" includes bartering or trading anything of value, including sound recordings. Where the infringing activity is for commercial advantage or private financial gain, sound recording infringements can be punishable by up to five years in prison and \$250,000 in fines. Repeat offenders can be imprisoned for up to 10 years. Violators can also be held civilly liable for actual damages, lost profits, or statutory damages up to \$150,000 per infringement, as well as attorney's fees and costs. The online infringement of copyrighted music can be punished by up to 3 years in prison and \$250,000 in fines. Repeat offenders can be imprisoned up to 6 years. Individuals also may be held civilly liable, regardless of whether the activity is for profit, for actual damages or lost profits, or for statutory damages up to \$150,000 per infringed copyright. For more information, please go to: <http://www.riaa.com>.