**What are the Different Types of Ethernet Cables?**

[eBay](http://www.ebay.com/usr/ebaybuyingguides?rt=nc)

206K Views 26 Likes

[Like **if this guide is helpful**](javascript:;)

Share

March 3, 2016



Anyone who has plugged their [computer](http://www.ebay.com/rpp/computers-networking) into a broadband Internet connection such as cable or DSL has used an [Ethernet cable](http://www.ebay.com/sch/Ethernet-Cables-RJ-45-8P8C/64035/bn_1648244/i.html). Ethernet cables are the standard cables commonly used to connect a modem to a router, and, likewise, to connect a router to a computer's network interface card (NIC). These thick, flexible cables are all practically indistinguishable to the untrained eye, but not all Ethernet cables are the same.

**The Major Categories of Ethernet Cables**

Ethernet cables have been evolving since the beginning of the Ethernet standard in 1985. Many different categories of Ethernet cable have been developed, and each category has different specifications as far as shielding from electromagnetic interference, data transmission speed, and the possible bandwidth frequency range required to achieve that speed. It is understandable that some confusion can arise when looking at all the available options for Ethernet cabling. Luckily, the category of cable is usually clearly printed on the cable's sheath, so there can be no doubt as to the type of cable being used. There are also certain types of cables recognized as common industry standards. This guide will describe a few of the most common categories of Ethernet cable that are used in modern networks.

**Category 3**

[Category 3 Ethernet cable](http://www.ebay.com/sch/Ethernet-Cables-RJ-45-8P8C/64035/bn_1648244/i.html), also known as Cat 3 or station wire, is one of the oldest forms of Ethernet cable still in use today. It is an unshielded twisted pair (UTP) cable that is capable of carrying 10 megabits per second (Mbps) of data or voice transmissions. Its maximum possible bandwidth is 16 MHz. Cat 3 cable reached the peak of its popularity in the early 1990s, as it was then the industry standard for computer networks. With the debut of the faster Category 5 cable, however, Cat 3 fell out of favor. It still can be seen in use in two-line telephone systems and older 10BASE-T Ethernet installations.

**Category 5**

[Category 5 (Cat 5) Ethernet cable](http://www.ebay.com/sch/Ethernet-Cables-RJ-45-8P8C/64035/bn_1648244/i.html) is the successor to the earlier Category 3. Like Cat 3, it is a UTP cable, but it is able to carry data at a higher transfer rate. Cat 5 cables introduced the 10/100Mbps speed to the Ethernet, which means that the cables can support either 10 Mbps or 100 Mbps speeds. A 100 Mbps speed is also known as Fast Ethernet, and Cat 5 cables were the first Fast Ethernet-capable cables to be introduced. They also can be used for telephone signals and video, in addition to Ethernet data. This category has been superseded by the newer Category 5e cables.

**Category 5e**

The [Category 5e](http://www.ebay.com/sch/Ethernet-Cables-RJ-45-8P8C/64035/bn_1648244/i.html) standard is an enhanced version of Cat 5 cable, which is optimized to reduce crosstalk, or the unwanted transmission of signals between data channels. This category works for 10/100 Mbps and 1000 Mbps (Gigabit) Ethernet, and it has become the most widely used category of Ethernet cable available on the market. While Cat 5 is common in existing installations, Cat 5e has completely replaced it in new installations. While both Cat 5 and Cat 5e cables contain four twisted pairs of wires, Cat 5 only utilizes two of these pairs for Fast Ethernet, while Cat 5e uses all four, enabling Gigabit Ethernet speeds. Bandwidth is also increased with Cat 5e cables, which can support a maximum bandwidth of 100 MHz. Cat 5e cables are backward compatible with Cat 5 cables, and can be used in any modern network installation.

**Category 6**

One of the major differences between Category 5e and the newer [Category 6](http://www.ebay.com/sch/Ethernet-Cables-RJ-45-8P8C/64035/bn_1648244/i.html) is in transmission performance. While Cat 5e cables can handle Gigabit Ethernet speeds, Cat 6 cables are certified to handle Gigabit Ethernet with a bandwidth of up to 250 MHz. Cat 6 cables have several improvements, including better insulation and thinner wires, that provide a higher signal-to-noise ratio, and are better suited for environments in which there may be higher electromagnetic interference. Some Cat 6 cables are available in shielded twisted pair (STP) forms or UTP forms. However, for most applications, Cat 5e cable is adequate for gigabit Ethernet, and it is much less expensive than Cat 6 cable. Cat 6 cable is also backwards compatible with Cat 5 and 5e cables.

**Category 6a**

[Category 6 a cable](http://www.ebay.com/sch/Ethernet-Cables-RJ-45-8P8C/64035/bn_1648244/i.html), or augmented Category 6 cable, improves upon the basic Cat 6 cable by allowing 10,000 Mbps data transmission rates and effectively doubling the maximum bandwidth to 500 MHz. Category 6a cables are usually available in STP form, and, as a result, must have specialized connectors that ground the cable.

**Category 7**

[Category 7 cable](http://www.ebay.com/sch/Ethernet-Cables-RJ-45-8P8C/64035/bn_1648244/i.html), also known as Class F, is a fully shielded cable that supports speeds of up to 10 Gbps (10,000 Mbps) and bandwidths of up to 600 Mhz. Cat 7 cables consist of a screened, shielded twisted pair (SSTP) of wires, and the layers of insulation and shielding contained within them are even more extensive than that of Cat 6 cables. Because of this shielding, they are thicker, more bulky, and more difficult to bend. Additionally, each of the shielding layers must be grounded, or else performance may be reduced to the point that there will be no improvement over Cat 6, and performance may be worse than Cat 5. For this reason, it's very important to understand the type of connectors at the ends of a Cat 7 cable.

The following table summarizes the most common types of Ethernet cables, including their maximum data transmission speeds and maximum bandwidths.

|  | **Cable Type** | **Maximum Data Transmission Speed** | **Maximum Bandwidth** |
| --- | --- | --- | --- |
| [**Category 3**](http://www.ebay.com/sch/i.html?_nkw=Cat+3&_sacat=64035&_odkw=Cat+3&_osacat=64035) | UTP | 10 Mbps | 16 MHz |
| [**Category 5**](http://www.ebay.com/sch/Ethernet-Cables-RJ-45-8P8C/64035/bn_1648244/i.html) | UTP | 10/100 Mbps | 100 MHz |
| [**Category 5 e**](http://www.ebay.com/sch/Ethernet-Cables-RJ-45-8P8C/64035/bn_1648244/i.html) | UTP | 1000 Mbps | 100 MHz |
| [**Category 6**](http://www.ebay.com/sch/Ethernet-Cables-RJ-45-8P8C/64035/bn_1648244/i.html) | UTP or STP | 1000 Mbps | 250 MHz |
| [**Category 6 a**](http://www.ebay.com/sch/Computer-Cables-and-Connectors/31491/bn_1642147/i.html?_nkw=cat+6a) | STP | 10,000 Mbps | 500 MHz |
| [**Category 7**](http://www.ebay.com/sch/Ethernet-Cables-RJ-45-8P8C/64035/bn_1648244/i.html) | SSTP | 10,000 Mbps | 600 MHz |

With each successive category, there has been an increase in data transmission speed and bandwidth. To fully future-proof a network installation, the highest categories are recommended, but only if all of the other equipment on the network is capable of similar speeds. Otherwise, expensive cables will be only as fast as the slowest piece of hardware on the network.

**Ethernet Cable Connectors**

The ends of Ethernet cables that connect into a NIC, router, or other network device are known by several names. Modular connector, jack, or plug are the most commonly used terms. Shorter lengths of Ethernet cable are usually sold with the connectors already installed, but for custom installations requiring longer lengths, cable is often sold in bulk quantities, and connectors must be installed on the ends.

The most common type of connector for Ethernet installations is referred to as an "RJ-45" connector. It is officially known as an 8P8C connector, but this term is rarely used in the field, and the term "RJ-45," which was the telephone industry's term for this connector's wiring pattern, has become the customary colloquial name for the connector itself. Categories 3 through 6 all use the RJ-45 connector, but Cat 7 utilizes a specialized version of the RJ-45 called the GigaGate45 (GG45), which grounds the cable and allows for higher data transmission rates. There are two standard pin assignment configurations for RJ-45 connectors: T568A and T568B. The T568A standard is typically used in home applications, while T568B is used in business applications.

In every case, the specifications of the cable, such as its category, whether or not it is shielded, and whether or not it needs to be grounded, must match the specifications of the connector. For those who are confused or uncertain about crimping and installing connectors to cables manually, it is best to buy cables that already have connectors professionally installed.

**Other Qualities of Ethernet Cables to Consider**

There are a few important considerations that apply to all Ethernet cables. Data transmission rate and bandwidth both decrease with the increase of cable length, so the shorter the length, the better. For 10/100/1000BASE-T networks (those that have maximum speeds of 10, 100, or 1000 Mbps, including all the aforementioned cable types except for Categories 6a and 7), 100 meters is the maximum allowable cable length before the signal will degrade. For category 6a cables running at 10 Gbps speeds, 55 meters is the maximum allowable length, and even this length is only allowed in very good alien crosstalk conditions, or areas of low interference, such as when the cable is located far away from other cables that could cause interference.

There are some other terms regarding cable terminations that can complicate the shopping experience. Some cables are referred to as [patch cables](http://www.ebay.com/sch/Ethernet-Cables-RJ-45-8P8C/64035/bn_1648244/i.html), while others are called [crossover cables](http://www.ebay.com/sch/Ethernet-Cables-RJ-45-8P8C/64035/bn_1648244/i.html). Even though crossover and patch cables may look the same, they function differently. A patch cable is one that terminates with the same type of connector standard at both ends. The connectors terminating a patch cable can use the T568A or T568B standards, but both ends must be the same. A crossover cable, on the other hand, has one end that terminates in a T568A connector and another that terminates in a T568B connector. Patch cables are used to connect devices that are different from one another, such as a switch and a computer. Crossover cables are used to connect similar devices, as when a switch is connected to another switch, for example.

Another important distinction in Ethernet cables is whether they contain [solid](http://www.ebay.com/sch/Networking-Cables-and-Adapters/20311/bn_1637588/i.html) or [stranded](http://www.ebay.com/sch/Ethernet-Cables-RJ-45-8P8C/64035/bn_1648244/i.html) conductors. Solid conductor cables have one solid wire per conductor, while stranded conductor cables have several strands of wire (typically seven) wrapped around each other to form a single conductor. Each type has its own advantages and disadvantages. Solid conductor cables are best for fixed wires within the walls or structure of a building. The single conductors are sturdy enough to be punched down into wall jacks and patch panels, but not as easy to install into a typical RJ-45 connector. Stranded conductors, on the other hand, can fray when punched down into wall jacks, so they are better suited to be crimped into an RJ-45 connector. They are also more flexible and forgiving when bent at sharp angles, so they are better suited for patch cables and applications where the cable may be rolled up or otherwise moved around.

**Conclusion**

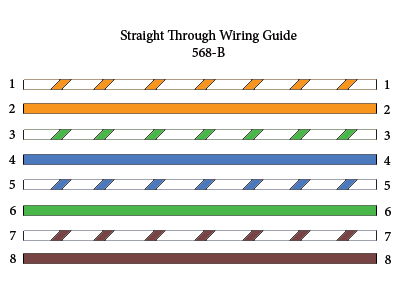
When you're setting up an Internet connection in your home or office, you'll need to obtain the proper Ethernet cable to attach your computer to the modem. While connecting the cable is typically a simple task, finding the right one may be a bit more complex. While Ethernet cables may all look similar to one another, their specifications vary widely. It's important to research what type of cable will work with your equipment, and you'll also want to consider things like the price and quality of the cable, as well as the types and number of devices you'll be connecting to your network. You could go for a cheap, industry standard solution such as Cat 5e cable or future-proof your network by opting for a Cat 7 cable. If you're looking to connect one switch to another or bypass a router, maybe crossover cables are the solution, or maybe you need a lot of patch cables to connect more devices to your network. In any case, you'll also want to ensure you're purchasing the right length of Ethernet cable, and properly addressing any interference concerns. No matter what your [networking](http://www.ebay.com/rpp/computers-networking) needs are, eBay is sure to have the category, length, and condition of Ethernet cable to get you connected.

**Straight-through, Crossover, and Rollover Wiring**

When talking about cable pinouts we often get questions as to the difference in Straight-through, Crossover, and Rollover wiring of cables and the intended use for each type of cable. These terms are referring to the way the cables are wired (which pin on one end is connected to which pin on the other end). Below we will try shed some light on this commonly confused subject.

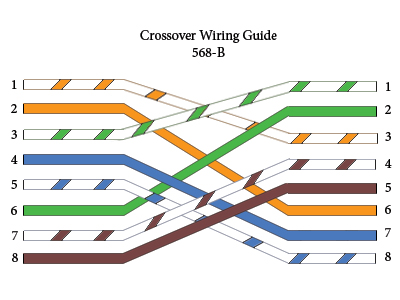
Straight-Through Wired Cables

Straight-Through refers to cables that have the pin assignments on each end of the cable. In other words Pin 1 connector A goes to Pin 1 on connector B, Pin 2 to Pin 2 ect. Straight-Through wired cables are most commonly used to connect a host to client. When we talk about cat5e patch cables, the Straight-Through wired cat5e patch cable is used to connect computers, printers and other network client devices to the router switch or hub (the host device in this instance).



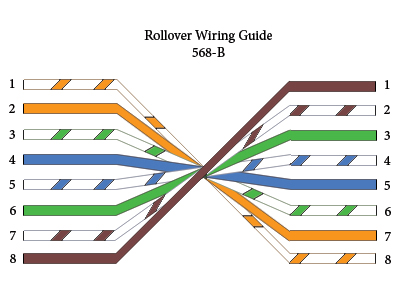
Crossover Wired Cables

Crossover wired cables (commonly called crossover cables) are very much like Straight-Through cables with the exception that TX and RX lines are crossed (they are at oposite positions on either end of the cable. Using the 568-B standard as an example below you will see that Pin 1 on connector A goes to Pin 3 on connector B. Pin 2 on connector A goes to Pin 6 on connector B ect. Crossover cables are most commonly used to connect two hosts directly. Examples would be connecting a computer directly to another computer, connecting a switch directly to another switch, or connecting a router to a router.*Note: While in the past when connecting two host devices directly a crossover cable was required. Now days most devices have auto sensing technology that detects the cable and device and crosses pairs when needed.*



Rollover Wired Cables

Rollover wired cables most commonly called rollover cables, have opposite Pin assignments on each end of the cable or in other words it is "rolled over". Pin 1 of connector A would be connected to Pin 8 of connector B. Pin 2 of connector A would be connected to Pin 7 of connector B and so on. Rollover cables, sometimes referred to as Yost cables are most commonly used to connect to a devices console port to make programming changes to the device. Unlike crossover and straight-wired cables, rollover cables are not intended to carry data but instead create an interface with the device.



Fiber Optic Tutorial

**What are Fiber Optic Cables?**  
Fiber optic cables consist of a glass core and cladding, buffer coating, Kevlar strength members and a protective outer jacket. Fiber optic cables use light pulses as opposed to electrical signals to send information.

**How are Fiber Optic Cables used?**  
Fiber optic cables can be plugged into communications equipment and patch panels to provide a physical connection to a network or device.

**Where are Fiber Optic Cables used?**  
Fiber optic cables are used by commercial business, governments, the military and many other industries for myriad applications involving the transmission of voice, video and data.

|  |
| --- |
| **Fiber Optic Terms** |

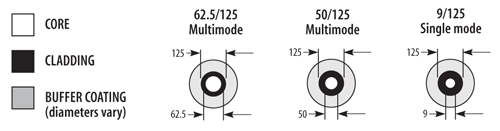
|  |
| --- |
| **Absorption:** One cause of attenuation where light signal is absorbed into the glass during transmission. |
| **Attenuation:** Optical loss of power. Attenuation is measured in dB loss per length of cable. Attenuation is usually caused by absorption and scattering. |
| **Attenuator:** A device used to reduce the power of an optical signal. |
| **Back Reflection:** A measure of the light reflected off the polished end of a fiber connector. Measured in negative dB relative to incident power. |
| **Bandwidth:** The range of signal frequencies that a fiber optic cable will transmit. |
| **Buffer:** The protective coating over the fiber. |
| **Insertion Loss:** The attenuation caused by the insertion of a device (such as a splice or connection point) to a cable. |
| **Loss Budget:** The maximum amount of power that is allowed to be lost per optical link. |
| **Multimode:** A type of fiber optic cable where the core diameter is much larger than the wavelength of light transmitted. Two common multimode fiber types are 50/125 and 62.5/125. |
| **Return Loss:** The ratio of the power launched into a cable and the power of the light returned down the fiber. This measurement is expressed in positive decibel units (dB). A higher number is better. Return Loss = 10 log (incident power / returned power). |
| **Scattering:** A second cause of attenuation. Scattering occurs when light collides with individual atoms in the glass. |
| **Single mode:** A type of fiber with a small core that allows only one mode of light to propagate. |
| **Wavelength:** A means of measuring light color. Expressed in nanometers (nm). |

|  |
| --- |
| **A Quick Lesson In Optical Transmission** |

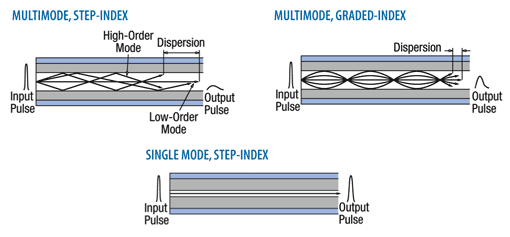
|  |
| --- |
| Where copper cabling uses electricity to transmit signals from one end to another, fiber optics use light pulses to accomplish the same purpose. The fiber cable is made of a transparent glass core surrounded by a mirror like covering called cladding. Light passes through the cable, bouncing off the cladding until it reaches the other end of the fiber channel - this is called total internal reflection.  In today’s high speed networks, Graded Index Multimode fiber or Step Index Single mode fiber is used to improve light transmission over long distances. Multimode fiber has a larger core and is typically used in short runs within buildings. Single mode fiber has a smaller core and is used in long distance runs typically outside between buildings. |

|  |
| --- |
| **Fiber Core Sizes** |

|  |
| --- |
| Fiber specifications list the core and cladding diameters as a ratio. Multimode fiber is commonly 62.5/125 or 50/125 micron, single mode fiber is commonly 9/125 micron. |



|  |
| --- |
| **Fiber Glass Types** |



|  |  |
| --- | --- |
| **How Do Fiber Optics Work?** | [[See the Video](http://www.l-com.com/content/Article.aspx?Type=L&ID=400) www.L-com.com/Videos/A15](http://www.l-com.com/content/Article.aspx?Type=L&ID=400) |

|  |  |
| --- | --- |
| **Commonly Used Fiber Connectors** | [[See the Video](http://www.l-com.com/content/Article.aspx?Type=L&ID=395) www.L-com.com/Videos/A21](http://www.l-com.com/content/Article.aspx?Type=L&ID=395) |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Connector Type** | **Coupling Type** | **Fiber Type** | **Polish** | **No. of Fibers** | **Typical Applications** | **Comment** |
| ST | ST | Twist on | Single mode /Multimode | PC, UPC | 1 | LANs | Keyed |
| FC | FC | Screw on | Single mode /Multimode | PC, UPC, APC | 1 | Datacom, Telecommuni- cations | Keyed |
| SC | SC | Snap on | Single mode /Multimode | PC, UPC, APC | 1 | CATV, Test Equipment | Keyed |
| LC | LC | Snap on RJ45 style | Single mode /Multimode | PC, UPC, APC | 1 | Gigabit Ethernet, Video Multimedia | Small Form Factor (SFF) |
| MU | MU | Push/Pull | Single mode /Multimode | PC, UPC, APC | 1 | Medical, Military | Small Form Factor (SFF) |
| MT-RJ | MT-RJ | Snap on RJ45 style | Single mode /Multimode | N/A | 2 | Gigabit Ethernet, Asynchronous Transmission Mode (ATM) | One of Mating Connectors must have Alignment Pins |
| MTP | MPO  (MTP) | Push/Pull | Single mode /Multimode | N/A | 4, 8,  12, 16, 24 | Active Device Transceiver, Interconnec- tions for O/E Modules | One of Mating Connectors must have Alignment Pins |

**The Fiber Optic Association - Tech Topics**

**Fiber Optic Cable And Connector Color Codes**

Users have been installing hybrid (MM+SM) cables in the backbone for years. With the premises fiber optic cabling now including two varieties of 50/125 fiber, 62.5/125 and singlemode fibers, managing the cable plant is more difficult. We have already seen instances of users and installers being confused and getting bad test results, as well as having problems with networks operating when connected over the wrong fiber type.

There is a color code standard in process, TIA-598C that addresses this issue, which we could adopt and reference. Here is what it recommends:

Colored outer jackets or print may be used on Premises Distribution Cable, Premises Interconnect Cable or Interconnect Cord, or Premises Breakout Cable to identify the classification and fiber sizes of the fiber.

When colored jackets are used to identify the type of fiber in cable containing only one fiber type, the colors shall be as indicated in Table 3. Other colors may be used providing that the print on the outer jacket identifies fiber classifications in accordance with subclause 4.3.3. Such colors should be as agreed upon between manufacturer and user.

Unless otherwise specified, the outer jacket of premises cable containing more than one fiber type shall use a printed legend to identify the quantities and types of fibers within the cable. Table 3 shows the preferred nomenclature for the various fiber types, for example "12 Fiber 8 x 50/125, 4 x 62.5/125."

When the print on the outer jacket of premises cable is used to identify the types and classifications of the fiber, the nomenclature of Table 3 is preferred for the various fiber types. Distinctive print characters for other fiber types may be considered for addition to Table 3 at some future date.

|  |  |  |  |
| --- | --- | --- | --- |
| Fiber Type | Color Code | | |
| . | Non-military Applications(3) | Military Applications | Suggested Print Nomenclature |
| Multimode (50/125) (TIA-492AAAB) (OM2) | Orange | Orange | 50/125 |
| Multimode (50/125) (850 nm Laser-optimized)  (TIA-492AAAC) (OM3, OM4) | Aqua | Undefined | 850 LO 50 /125 |
| Multimode (62.5/125)  (TIA-492AAAA) (OM1) | Orange | Slate | 62.5/125 |
| Multimode (100/140) | Orange | Green | 100/140 |
| Single-mode (TIA-492C000 / TIA-492E000) (OS1, OS2) | Yellow | Yellow | SM/NZDS, SM |
| Polarization Maintaining Single-mode | Blue | Undefined | Undefined (2) |

NOTES:  
1) Natural jackets with colored tracers may be used instead of solid-color jackets.   
2) Because of the limited number of applications for these fibers, print nomenclature are to be agreed upon between manufacturer and enduser   
3) Other colors may be used providing that the print on the outer   
jacket identifies fiber classifications per subclause 4.3.3.   
4) For some Premises Cable functional types (e.g., plenum cables), colored jacketing material may not be available. Distinctive jacket colors for other fiber types may be considered for addition to Table 3 at some future date.

**Fiber Color Codes**  
Inside the cable or inside each tube in a loose tube cable, individual fibers will be color coded for identification. Fibers follow the convention created for telephone wires except fibers are identified individually, not in pairs. For splicing, like color fibers are spliced to ensure continuity of color codes throughout a cable run.

|  |  |
| --- | --- |
| **Fiber Number** | **Color** |
| 1 | Blue |
| 2 | Orange |
| 3 | Green |
| 4 | Brown |
| 5 | Slate |
| 6 | White |
| 7 | Red |
| 8 | Black |
| 9 | Yellow |
| 10 | Violet |
| 11 | Rose |
| 12 | Aqua |

There is a publicly available document that defines the twelve TIA/EIA colors for fiber conductors: <http://munsell.com/color-blog/color-codingchart-wire-color-coding/>

**Connector Color Codes:**

Since the earliest days of fiber optics, orange, black or gray was multimode and yellow singlemode. However, the advent of metallic connectors like the FC and ST made connector color coding difficult, so colored strain relief boots were often used.

|  |  |  |
| --- | --- | --- |
| **Fiber type** | **Connector Body** | **Strain Relief/ Mating Adapter** |
| 62.5/125 | Beige | Beige |
| 50/125 | Black | Black |
| 50/125 laser optimized | Aqua | Aqua |
| Singlemode | Blue | Blue |
| Singlemode APC | Green | Green |

**Introduction**  
This section briefly discusses the modes of channel operation, namely, simplex, half-duplex and full-duplex operation. Each is suited a particular type of application, and has its own advantages and disadvantages.

Modes of Channel Operation

[http://uva.ulb.ac.be/cit_courseware/datacomm/images/up.gif](http://uva.ulb.ac.be/cit_courseware/datacomm/dc_014.htm#up)**Simplex**  
Data in a simplex channel is always one way. Simplex channels are not often used because it is not possible to send back error or control signals to the transmit end.

|  |  |
| --- | --- |
| Simplex channel | It's like a one way street. An example of simplex is Television, or Radio. The simplex channel also corresponds directly to Shannon's [model of communication](http://uva.ulb.ac.be/cit_courseware/datacomm/dc_001.htm#shannonmodel) discussed earlier. |

[http://uva.ulb.ac.be/cit_courseware/datacomm/images/up.gif](http://uva.ulb.ac.be/cit_courseware/datacomm/dc_014.htm#up)**Half Duplex**  
A half-duplex channel can send and receive, but not at the same time. It's like a one-lane bridge where two way traffic must give way in order to cross. Only one end transmits at a time, the other end receives. In addition, it is possible to perform error detection and request the sender to retransmit information that arrived corrupted. In some aspects, you can think of [Internet](http://uva.ulb.ac.be/cit_courseware/datacomm/dc_005.htm#internet) surfing as being half-duplex, as a user issues a request for a web document, then that document is downloaded and displayed before the user issues another request.

|  |  |
| --- | --- |
| Half-duplex channel | Another example of half-duplex is talk-back radio, and CB Radio (Citizens Band). You might have seen movies where truckies (drivers of very big trucks) communicate to each other, and when they want the other person to speak they say "over". This is because only one person can talk at a time. |

[http://uva.ulb.ac.be/cit_courseware/datacomm/images/up.gif](http://uva.ulb.ac.be/cit_courseware/datacomm/dc_014.htm#up)**Full Duplex**  
Data can travel in both directions simultaneously. There is no need to switch from transmit to receive mode like in half duplex. Its like a two lane bridge on a two-lane highway. Have you ever watched these television talk shows where the host has a number of people on the show, and they all try to talk at once. Well, that's full duplex!

|  |  |
| --- | --- |
| Full-duplex channel | Of course, in the world of data communications, full duplex allows both way communication simultaneously. An example can be a consumer which uses a cable connection to not only receive TV channels, but also the same cable to support their phone and Internet surfing. All these activities can occur simultaneously. |

[http://uva.ulb.ac.be/cit_courseware/datacomm/images/up.gif](http://uva.ulb.ac.be/cit_courseware/datacomm/dc_014.htm#up)**Summary**  
The three modes of channel operation are simplex, half-duplex and full-duplex.

Simple is a one way communication and there is no means of informing the sender to retransmit data in case of errors. There is however a good example of the retransmission of data, and that is TeleText, which sends text based data on top of a Television signal. A special decoder displays the Teletext data as a series of pages. These pages are sequenced and repeated, so if a page arrives corrupted, the user just needs to wait a little while till it is resent.

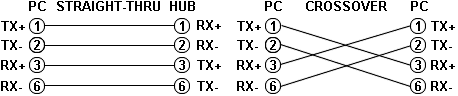
Half-duplex and full-duplex are the other two methods. As telephone companies become more aware of the added services that customers require, such as Internet access and Television, it is probable that a single connection to your home will provide you with a range of services, which you can use. This would require a full-duplex connection.

**Ethernet Cables - RJ45/Colors & Crossover**

|  |
| --- |
| http://www.bb-elec.com/Images/EthernetRJ45A-%281%29.aspx   http://www.bb-elec.com/Images/EthernetRJ45B.aspx  This diagram shows how Ethernet cable color coding works. Alter cables at your own risk.   Ethernet cable color-coding exists as part of the industry standard - T568A/T458B. Standards exist so technicians can know how the cable should work and can reliably alter the cable when necessary. |

**COLOR-CODE STANDARDS  
Last updated: 8/9/2004**

Again, please bear with me...  Let's start with simple pin-out diagrams of the two types of UTP Ethernet cables and watch how committees can make a can of worms out of them.  Here are the diagrams:

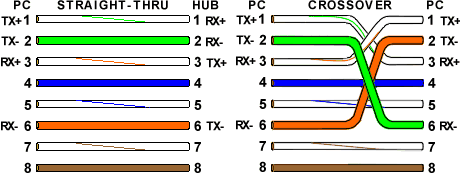


Note that the TX (transmitter) pins are connected to corresponding RX (receiver) pins, plus to plus and minus to minus.  And that  you must use a crossover cable to connect units with identical interfaces.  If you use a straight-through cable, one of the two units must, in effect, perform the cross-over function.

Two wire color-code standards apply: EIA/TIA 568A and EIA/TIA 568B.The codes are commonly depicted with RJ-45 jacks as follows (the view is from the front of the jacks):

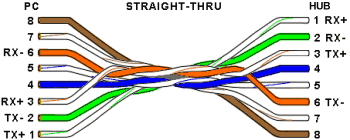
|  |  |
| --- | --- |
| http://www.duxcw.com/digest/Howto/network/cable/568ajck.gif | http://www.duxcw.com/digest/Howto/network/cable/568bjck.gif |

If we apply the 568A color code and show all eight wires, our pin-out looks like this:

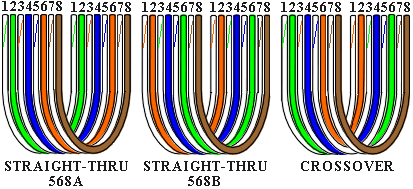


Note that pins 4, 5, 7, and 8 and the blue and brown pairs are not used in either standard.  Quite contrary to what you may read elsewhere, these pins and wires are not used or required to implement 100BASE-TX duplexing--they are just plain wasted.

However, the actual cables are not physically that simple.  In the diagrams, the orange pair of wires are not adjacent.  The blue pair is upside-down.  The right ends match RJ-45 jacks and the left ends do not.  If, for example, we invert the left side of the 568A "straight"-thru cable to match a 568A jack--put one 180° twist in the entire cable from end-to-end--and twist together and rearrange the appropriate pairs, we get the following can-of-worms:

This further emphasizes, I hope,  the importance of the word "twist" in making network cables which will work.  You cannot use an flat-untwisted telephone cable for a network cable.  Furthermore, you must use a pair of twisted wires to connect a set of transmitter pins to their corresponding receiver pins.  You cannot use a wire from one pair and another wire from a different pair.

Keeping the above principles in mind, we can simplify the diagram for a 568A straight-thru cable by untwisting  the wires, except the 180° twist in the entire cable, and bending the ends upward.  Likewise, if we exchange the green and orange pairs in the 568A diagram we will get a simplified diagram for a 568B straight-thru cable.  If we cross the green and orange pairs in the 568A diagram we will arrive at a simplified diagram for a crossover cable.  All three are shown below.



**FIBER OPTIC COLOR CODING**

Color code, used in fiber optics, resembles that of copper. the major difference is 12-color sequence as oppose to 10-color for copper. The sequence of colors is the same, with addition of two colors - Rose (11-th) and Aqua (12-th).

Fiber color codes are specified by TIA/EIA 598-A. in loose tube cables, this color code will be used for tubes as well as fibers within the tubes and subgroups

[](http://3.bp.blogspot.com/_ksZWE-7dhXo/Ssm9Ht3l1CI/AAAAAAAAAFw/539O1j5lR1U/s1600-h/asdfafasdf.bmp)

For cables that consist of more than 12 strands, the color code repeats itself. Each group of 12 strands is identified with some other means such as:

    - Multiple buffer tubes each with 12 or less strands either numbered or colored following the same color code, e.g., 1st tube is blue, 2nd is orange, etc.

    -   24 strand groups with the color code repeating with some variation, e.g., the 1st group of 12 strands are solid colors and the 2nd group are solid colors with a stripe or some other identifying mark.

**FIBER OPTIC CABLE JACKET COLOR**

For **outdoor aerial and burial type cables**, the jacket color is usually black polyethelene for both multimode and singlemode cables to prevent UV radiation damage.

For **indoor cables**, the outer most fiber cable jacket may be any color but the de facto industry standard is:

        **Orange** for **multimode fibers**

        **Yellow** for **singlemode fibers**

This is also generally true for fiber optic patch cords.

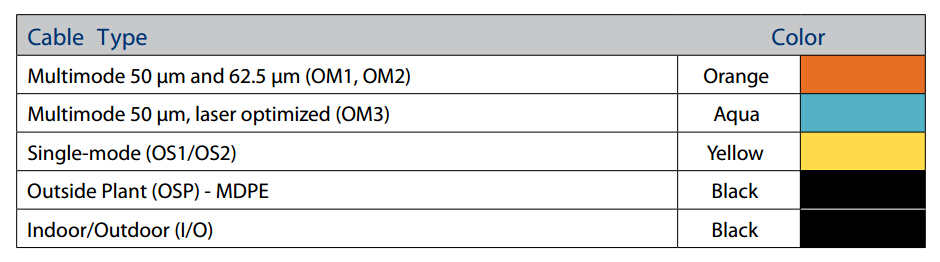
**Fiber Optic Cabling Components Color Coding Standard**

Posted on [November 5, 2015](http://www.fiber-optic-transceiver-module.com/fiber-optic-cabling-components-color-coding-standard.html) by [Admin](http://www.fiber-optic-transceiver-module.com/author/admin)

Various colors of fiber optic cabling components including fiber optic cables, connectors and adapters add color and life to data center. Image if there is no color coding of these fiber optic cabling components, the data centers which are full of a dense mass of server racks and cabinets will get into a mess. But if we make the fiber optic cabling components coding as we wished, it will cause many issues for the systems. Thus, the industry provides some standard to solve the issues.

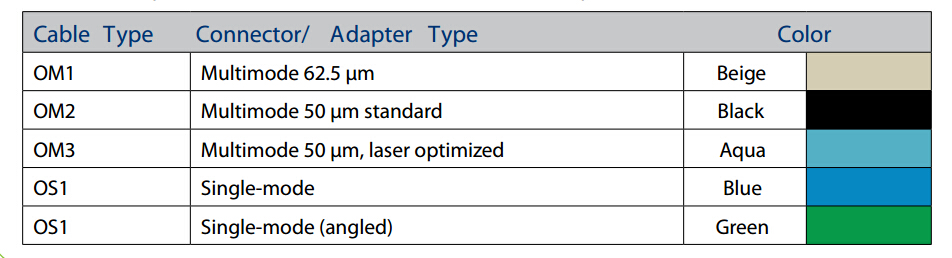
**Identify Types of Fiber by Color**

The jacket color of fiber optic cable is typically defined by the fiber type, and will almost always follow the color definitions below. Both multimode and single-mode cables designed for outdoor use will typically have a black jacket to protect the cable from damage due to solar exposure and UV light.



**Connectors and Adapters Identification**

TIA-568-C.3 standard specifies the color codings for fiber connectors and adapters. Unless the color coding is used for some other purpose, the connector strain relief and adapter housing should be identifiable by the following colors:



As introduced above, the color codings of fiber optic cabling components are not just for looking pretty but for better management. In practical applications, we will need different color jackets of cable, connectors or adapters for individual management. But most of the times, we should obey the standards for our fiber optic cabling. And we can manage our cabling with different color ties and markers.

This entry was posted in [Cables Management](http://www.fiber-optic-transceiver-module.com/category/cable-management), [Connectors & Adapters](http://www.fiber-optic-transceiver-module.com/category/connectors-and-adapters), [Fiber Optic Cabling](http://www.fiber-optic-transceiver-module.com/category/fiber-optic-network/fiber-optic-cabling) and tagged [color coding](http://www.fiber-optic-transceiver-module.com/tag/color-coding), [fiber adapters](http://www.fiber-optic-transceiver-module.com/tag/fiber-adapters), [fiber optic cabling](http://www.fiber-optic-transceiver-module.com/tag/fiber-optic-cabling), [Fiber optic connectors](http://www.fiber-optic-transceiver-module.com/tag/fiber-optic-connectors). Bookmark the [permalink](http://www.fiber-optic-transceiver-module.com/fiber-optic-cabling-components-color-coding-standard.html).

**What is Network Cabling?**

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

The following sections discuss the types of cables used in networks and other related topics.

* Unshielded Twisted Pair (UTP) Cable
* Shielded Twisted Pair (STP) Cable
* Coaxial Cable
* Fiber Optic Cable
* Cable Installation Guides
* Wireless LANs
* Unshielded Twisted Pair (UTP) Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks (See fig. 1).

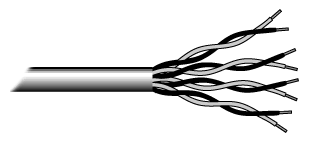


Fig.1. Unshielded twisted pair

The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated six categories of wire (additional categories are emerging).

**Categories of Unshielded Twisted Pair**

|  |  |  |
| --- | --- | --- |
| **Category** | **Speed** | **Use** |
| 1 | 1 Mbps | Voice Only (Telephone Wire) |
| 2 | 4 Mbps | LocalTalk & Telephone (Rarely used) |
| 3 | 16 Mbps | 10BaseT Ethernet |
| 4 | 20 Mbps | Token Ring (Rarely used) |
| 5 | 100 Mbps (2 pair) | 100BaseT Ethernet |
| 1000 Mbps (4 pair) | Gigabit Ethernet |
| 5e | 1,000 Mbps | Gigabit Ethernet |
| 6 | 10,000 Mbps | Gigabit Ethernet |

**Unshielded Twisted Pair Connector**

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (See fig. 2). A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

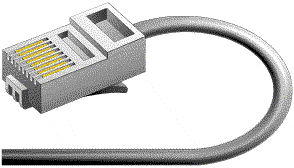


Fig. 2. RJ-45 connector

**Shielded Twisted Pair (STP) Cable**

Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.). If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may be the solution. Shielded cables can also help to extend the maximum distance of the cables.

Shielded twisted pair cable is available in three different configurations:

1. Each pair of wires is individually shielded with foil.
2. There is a foil or braid shield inside the jacket covering all wires (as a group).
3. There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).

**Coaxial Cable**

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield (See fig. 3). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

http://fcit.usf.edu/network/chap4/pics/coaxial.gif

Fig. 3. Coaxial cable

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters. Thin coaxial cable has been popular in school networks, especially linear bus networks.

Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

**Coaxial Cable Connectors**

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector (See fig. 4). Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather screw, onto the cable.

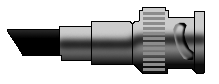


Fig. 4. BNC connector

**Fiber Optic Cable**

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials (See fig. 5). It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

The center core of fiber cables is made from glass or plastic fibers (see fig 5). A plastic coating then cushions the fiber center, and kevlar fibers help to strengthen the cables and prevent breakage. The outer insulating jacket made of teflon or PVC.

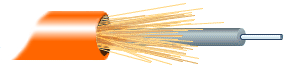


Fig. 5. Fiber optic cable

There are two common types of fiber cables -- single mode and multimode. Multimode cable has a larger diameter; however, both cables provide high bandwidth at high speeds. Single mode can provide more distance, but it is more expensive.

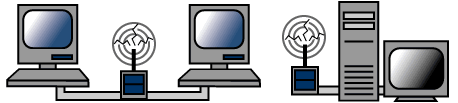
|  |  |
| --- | --- |
| **Specification** | **Cable Type** |
| **10BaseT** | Unshielded Twisted Pair |
| **10Base2** | Thin Coaxial |
| **10Base5** | Thick Coaxial |
| **100BaseT** | Unshielded Twisted Pair |
| **100BaseFX** | Fiber Optic |
| **100BaseBX** | Single mode Fiber |
| **100BaseSX** | Multimode Fiber |
| **1000BaseT** | Unshielded Twisted Pair |
| **1000BaseFX** | Fiber Optic |
| **1000BaseBX** | Single mode Fiber |
| **1000BaseSX** | Multimode Fiber |

**Installing Cable - Some Guidelines**

When running cable, it is best to follow a few simple rules:

* Always use more cable than you need. Leave plenty of slack.
* Test every part of a network as you install it. Even if it is brand new, it may have problems that will be difficult to isolate later.
* Stay at least 3 feet away from fluorescent light boxes and other sources of electrical interference.
* If it is necessary to run cable across the floor, cover the cable with cable protectors.
* Label both ends of each cable.
* Use cable ties (not tape) to keep cables in the same location together.

**Wireless LANs**



More and more networks are operating without cables, in the wireless mode. Wireless LANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations, servers, or hubs. Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.

Wireless networks are great for allowing laptop computers, portable devices, or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables.

The two most common types of infrared communications used in schools are line-of-sight and scattered broadcast. Line-of-sight communication means that there must be an unblocked direct line between the workstation and the transceiver. If a person walks within the line-of-sight while there is a transmission, the information would need to be sent again. This kind of obstruction can slow down the wireless network. Scattered infrared communication is a broadcast of infrared transmissions sent out in multiple directions that bounces off walls and ceilings until it eventually hits the receiver. Networking communications with laser are virtually the same as line-of-sight infrared networks.

**Wireless standards and speeds**

The Wi-Fi Alliance is a global, non-profit organization that helps to ensure standards and interoperability for wireless networks, and wireless networks are often referred to as WiFi (Wireless Fidelity). The original Wi-Fi standard (IEEE 802.11) was adopted in 1997. Since then many variations have emerged (and will continue to emerge). Wi-Fi networks use the Ethernet protocol.

|  |  |  |
| --- | --- | --- |
| **Standard** | **Max Speed** | **Typical Range** |
| **802.11a** | 54 Mbps | 150 feet |
| **802.11b** | 11 Mbps | 300 feet |
| **802.11g** | 54 Mbps | 300 feet |
| **802.11n** | 100 Mbps | 300+ feet |

**Wireless Security**

Wireless networks are much more susceptible to unauthorized use than cabled networks. Wireless network devices use radio waves to communicate with each other. The greatest vulnerability to the network is that rogue machines can "eves-drop" on the radio wave communications. Unencrypted information transmitted can be monitored by a third-party, which, with the right tools (free to download), could quickly gain access to your entire network, steal valuable passwords to local servers and online services, alter or destroy data, and/or access personal and confidential information stored in your network servers. To minimize the possibility of this, all modern access points and devices have configuration options to encrypt transmissions. These encryption methodologies are still evolving, as are the tools used by malicious hackers, so always use the strongest encryption available in your access point and connecting devices.

A NOTE ON ENCRYPTION: As of this writing WEP (Wired Equivalent Privacy) encryption can be easily hacked with readily-available free tools which circulate the internet. WPA and WPA2 (WiFi Protected Access versions 1 and 2) are much better at protecting information, but using weak passwords or passphrases when enabling these encryptions may allow them to be easily hacked. If your network is running WEP, you must be very careful about your use of sensitive passwords or other data.

Three basic techniques are used to protect networks from unauthorized wireless use. Use any and all of these techniques when setting up your wireless access points:

Encryption.

Enable the strongest encryption supported by the devices you will be connecting to the network. Use strong passwords (strong passwords are generally defined as passwords containing symbols, numbers, and mixed case letters, at least 14 characters long).

Isolation.

Use a wireless router that places all wireless connections on a subnet independent of the primary private network. This protects your private network data from pass-through internet traffic.

Hidden SSID.

Every access point has a Service Set IDentifier (SSID) that by default is broadcast to client devices so that the access point can be found. By disabling this feature, standard client connection software won't be able to "see" the access point. However, the eves-dropping programs discussed previously can easily find these access points, so this alone does little more than keep the access point name out of sight for casual wireless users.

**Advantages of wireless networks:**

* Mobility - With a laptop computer or mobile device, access can be available throughout a school, at the mall, on an airplane, etc. More and more businesses are also offering free WiFi access ("Hot spots").
* Fast setup - If your computer has a wireless adapter, locating a wireless network can be as simple as clicking "Connect to a Network" -- in some cases, you will connect automatically to networks within range.
* Cost - Setting up a wireless network can be much more cost effective than buying and installing cables.
* Expandability - Adding new computers to a wireless network is as easy as turning the computer on (as long as you do not exceed the maximum number of devices).

**Disadvantages of wireless networks:**

* Security - Be careful. Be vigilant. Protect your sensitive data with backups, isolated private networks, strong encryption and passwords, and monitor network access traffic to and from your wireless network.
* Interference - Because wireless networks use radio signals and similar techniques for transmission, they are susceptible to interference from lights and electronic devices.
* Inconsistent connections - How many times have you hears "Wait a minute, I just lost my connection?" Because of the interference caused by electrical devices and/or items blocking the path of transmission, wireless connections are not nearly as stable as those through a dedicated cable.
* Speed - The transmission speed of wireless networks is improving; however, faster options (such as gigabit Ethernet) are available via cables. If you are only using wireless for internet access, the actual internet connection for your home or school is generally slower than the wireless network devices, so that connection is the bottleneck. If you are also moving large amounts of data around a private network, a cabled connection will enable that work to proceed much faster.

**What is a Topology?**

The physical topology of a network refers to the configuration of cables, computers, and other peripherals. Physical topology should not be confused with logical topology which is the method used to pass information between workstations. Logical topology was discussed in the Protocol chapter.

**Main Types of Physical Topologies**

The following sections discuss the physical topologies used in networks and other related topics.

* [Linear Bus](http://fcit.usf.edu/network/chap5/chap5.htm#LinearBusnetwork)
* [Star](http://fcit.usf.edu/network/chap5/chap5.htm#StarNetwork)
* [Tree (Expanded Star)](http://fcit.usf.edu/network/chap5/chap5.htm#TreeNetwork)
* [Considerations When Choosing a Topology](http://fcit.usf.edu/network/chap5/chap5.htm#Considerations)
* [Summary Chart](http://fcit.usf.edu/network/chap5/chap5.htm#Summary)

**Linear Bus**

A linear bus topology consists of a main run of cable with a terminator at each end (See fig. 1). All nodes (file server, workstations, and peripherals) are connected to the linear cable.

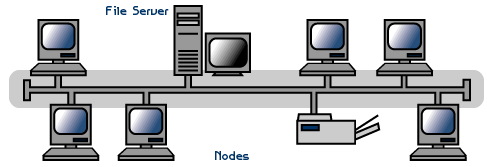


Fig. 1. Linear Bus topology

**Advantages of a Linear Bus Topology**

* Easy to connect a computer or peripheral to a linear bus.
* Requires less cable length than a star topology.

**Disadvantages of a Linear Bus Topology**

* Entire network shuts down if there is a break in the main cable.
* Terminators are required at both ends of the backbone cable.
* Difficult to identify the problem if the entire network shuts down.
* Not meant to be used as a stand-alone solution in a large building.

**Star**

A star topology is designed with each node (file server, workstations, and peripherals) connected directly to a central network hub, switch, or concentrator (See fig. 2).

Data on a star network passes through the hub, switch, or concentrator before continuing to its destination. The hub, switch, or concentrator manages and controls all functions of the network. It also acts as a repeater for the data flow. This configuration is common with twisted pair cable; however, it can also be used with coaxial cable or fiber optic cable.

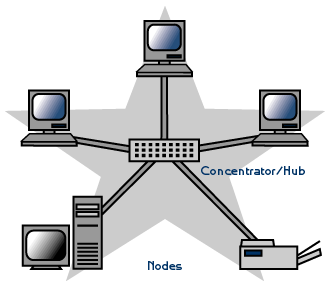


Fig. 2. Star topology

**Advantages of a Star Topology**

* Easy to install and wire.
* No disruptions to the network when connecting or removing devices.
* Easy to detect faults and to remove parts.

**Disadvantages of a Star Topology**

* Requires more cable length than a linear topology.
* If the hub, switch, or concentrator fails, nodes attached are disabled.
* More expensive than linear bus topologies because of the cost of the hubs, etc.

**Tree or Expanded Star**

A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable (See fig. 3). Tree topologies allow for the expansion of an existing network, and enable schools to configure a network to meet their needs.

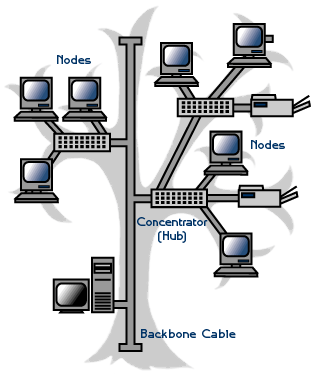


Fig. 3. Tree topology

**Advantages of a Tree Topology**

* Point-to-point wiring for individual segments.
* Supported by several hardware and software venders.

**Disadvantages of a Tree Topology**

* Overall length of each segment is limited by the type of cabling used.
* If the backbone line breaks, the entire segment goes down.
* More difficult to configure and wire than other topologies.

**5-4-3 Rule**

A consideration in setting up a tree topology using Ethernet protocol is the 5-4-3 rule. One aspect of the Ethernet protocol requires that a signal sent out on the network cable reach every part of the network within a specified length of time. Each concentrator or repeater that a signal goes through adds a small amount of time. This leads to the rule that between any two nodes on the network there can only be a maximum of 5 segments, connected through 4 repeaters/concentrators. In addition, only 3 of the segments may be populated (trunk) segments if they are made of coaxial cable. A populated segment is one that has one or more nodes attached to it . In Figure 4, the 5-4-3 rule is adhered to. The furthest two nodes on the network have 4 segments and 3 repeaters/concentrators between them.

NOTE: This rule does not apply to other network protocols or Ethernet networks where all fiber optic cabling or a combination of a fiber backbone with UTP cabling is used. If there is a combination of fiber optic backbone and UTP cabling, the rule would translate to a 7-6-5 rule.The speed of networking switches is vastly improved over older technologies, and while every effort should be made to limit network segment traversal, efficient switching can allow much larger numbers of segments to be traversed with little or no impact to the network.

**Considerations When Choosing a Topology**

* **Money**. A linear bus network may be the least expensive way to install a network; you do not have to purchase concentrators.
* **Length of cable needed**. The linear bus network uses shorter lengths of cable.
* **Future growth**. With a star topology, expanding a network is easily done by adding another concentrator.
* C**able type**. The most common cable in schools is unshielded twisted pair, which is most often used with star topologies.

**Summary Chart**

|  |  |  |
| --- | --- | --- |
| **Physical Topology** | **Common Cable** | **Common Protocol** |
| **Linear Bus** | Twisted Pair Coaxial Fiber | Ethernet |
| **Star** | Twisted Pair Fiber | Ethernet |
| **Tree** | Twisted Pair Coaxial Fiber | Ethernet |

**10Base2** - Ethernet specification for thin coaxial cable, transmits signals at 10 Mbps (megabits per second) with a distance limit of 185 meters per segment.

**10Base5** - Ethernet specification for thick coaxial cable, transmits signals at 10 Mbps (megabits per second) with a distance limit of 500 meters per segment.

**10BaseF** - Ethernet specification for fiber optic cable, transmits signals at 10 Mbps (megabits per second) with a distance limit of 2000 meters per segment.

**10BaseT** - Ethernet specification for unshielded twisted pair cable (category 3, 4, or 5), transmits signals at 10 Mbps (megabits per second) with a distance limit of 100 meters per segment.

**100BaseT** - Ethernet specification for unshielded twisted pair cabling that is used to transmit data at 100 Mbps (megabits per second) with a distance limit of 100 meters per segment.

**1000BaseTX** -Ethernet specification for unshielded twisted pair cabling that is used to transmit data at 1 Gbps (gigabits per second) with a distance limitation of 220 meters per segment.

**Asynchronous Transfer Mode (ATM)** - A network protocol that transmits data at a speed of 155 Mbps and higher. It is most often used to interconnect two or more local area networks.

**AppleTalk** - Apple Computer's network protocol originally designed to run over LocalTalk networks, but can also run on Ethernet and Token Ring.

**AUI Connector** (Attachment Unit Interface) - A 15 pin connector found on Ethernet cards that can be used for attaching coaxial, fiber optic, or twisted pair cable.

**Backbone** - A cable to which multiple nodes or workstations are attached.

**Bit** - Binary digit in the binary numbering system. Its value can be 0 or 1. In an 8-bit character scheme, it takes 8 bits to make a byte (character) of data.

**BNC Connector** (Bayone-Neill-Concelman) - Standard connector used to connect 10Base2 coaxial cable.

**Bridge** - Devices that connect and pass packets between two network segments that use the same communications protocol.

**Byte** - an 8-bit long binary value, which originally mapped to text character values (between 0 and 255 decimal). For example, a decimal value of 65, represented in a binary byte is "01000001" and represents the capital letter "A". A byte also is the atomic value of data storage, so a megabyte is the amount of memory required to store a million bytes.

**Cable** - Transmission medium of copper wire or optical fiber wrapped in a protective cover.

**Client/Server** - A networking system in which one or more file servers (Server) provide services; such as network management, application and centralized data storage for workstations (Clients).

**CSMA/CA** - Carrier Sense Multiple Access Collision Avoidance is a network access method in which each device signals its intent to transmit before it actually does so. This prevents other devices from sending information, thus preventing collisions from occurring between signals from two or more devices. This is the access method used by LocalTalk.

**CSMA/CD** - Carrier Sense Multiple Access Collision Detection is a network access method in which devices that are ready to transmit data first check the channel for a carrier. If no carrier is sensed, a device can transmit. If two devices transmit at once, a collision occurs and each computer backs off and waits a random amount of time before attempting to retransmit. This is the access method used by Ethernet.

**Coaxial Cable** - Cable consisting of a single copper conductor in the center surrounded by a plastic layer for insulation and a braided metal outer shield.

**Concentrator** - A device that provides a central connection point for cables from workstations, servers, and peripherals. Most concentrators contain the ability to amplify the electrical signal they receive.

**DIN** - A plug and socket connector consisting of a circular pattern of pins in a metal sleeve. This type of connector is commonly seen on keyboards.

**Dumb Terminal** - Refers to devices that are designed to communicate exclusively with a host (main frame) computer. It receives all screen layouts from the host computer and sends all keyboard entry to the host. It cannot function without the host computer.

**E-mail** - An electronic mail message sent from a host computer to a remote computer.

**End User** - Refers to the human executing applications on the workstation.

**Ethernet** - A network protocol invented by Xerox Corporation and developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks use CSMA/CD and run over a variety of cable types at 10 Mbps (megabits per second).

**Expansion Slot** - Area in a computer that accepts additional input/output boards to increase the capability of the computer.

**Fast Ethernet** - An Ethernet standard that supports 100 Mbps using category 5 twisted pair or fiber optic cable.

**Fiber Distributed Data Interface (FDDI)** - A network protocol that is used primarily to interconnect two or more local area networks, often over large distances.

**Fiber Optic Cable** - A cable, consisting of a center glass core surrounded by layers of plastic, that transmits data using light rather than electricity. It has the ability to carry more information over much longer distances.

**File Server** - A computer connected to the network that contains primary files/applications and shares them as requested with the other computers on the network. If the file server is dedicated for that purpose only, it is connected to a client/server network. An example of a legacy client/server network is Novell Netware. All the computers connected to a peer-to-peer network are capable of being the file server. Most modern operating systems can operate as servers or as clients, greying the distinction in the server architecture.

**Firewall** - A security device which inspects traffic entering and leaving a network, and allows or disallows the traffic, depending on rules describing acceptable use of the network, by filtering out unwanted packets. The firewall is usually positioned as the gateway device to another network, such as the internet. Many routers now contain firewalls. A personal firewall is usually software that runs on a workstation or server to filter unwanted traffic at the individual machine.

**Gigabit Ethernet** - An Ethernet protocol that raises the transmission rates to 1 Gbps (gigabits per second). Most school, corporate, and household networks provide gigabit ethernet to the workstations via cabled connections.

**Gigabyte** (GB) - One billion bytes of information. One thousand megabytes.

**Hub** - A hardware device that contains multiple independent but connected modules of network and internetwork equipment. Hubs can be active (where they repeat signals sent through them) or passive (where they do not repeat but merely split signals sent through them).

**Infrared** - Electromagnetic waves whose frequency range is above that of microwaves, but below that of the visible spectrum.

**Intranet** - Network internal to an organization that uses Internet protocols.

**Internet** - A global network of networks used to exchange information using the TCP/IP protocol. It allows for electronic mail and the accessing ad retrieval of information from remote sources.

**LAN** (Local Area Network) - A network connecting computers in a relatively small area such as a building.

**Linear Bus** - A network topology in which each node attaches directly to a common cable.

**LocalTalk** - Apple Corporation proprietary protocol that uses CSMA/CA media access scheme and supports transmissions at speeds of 230 Kbps (Kilobits per second).

**MAN** (Metropolitan Area Network) - A network connecting computers over a large geographical area, such as a city or school district.

**MAU** (Multistation Access Unit) - A Token Ring wiring hub.

**Modem** (Modulator/Demodulator) - Devices that convert digital and analog signals. Modems allow computer data (digital) to be transmitted over voice-grade telephone lines (analog).

**Multiplexer** - A device that allows multiple logical signals to be transmitted simultaneously across a single physical channel.

**Network Modem** - A modem connected to a Local Area Network (LAN) that is accessible from any workstation on the network.

**Network Interface Card** (NIC) - A board that provides network communication capabilities to and from a computer.

**Network Operating System** (NOS) - Operating system designed to pass information and communicate between more than one computer. Examples include Linux/Unix and Windows Server.

**Node** - End point of a network connection. Nodes include any device attached to a network such as file servers, printers, or workstations.

**Node Devices** - Any computer or peripheral that is connected to the network.

**PCMCIA** - (later versions were **PCMCIA2** and **PC Card**) An expansion slot found in many laptop computers. Largely replaced by USB in the 2000-2010 period.

**Peer-to-Peer Network** - A network in which resources and files are shared without a centralized management source.

**Physical Topology** - The physical layout of the network; how the cables are arranged; and how the computers are connected.

**Point-to-Point** - A direct link between two objects in a network.

**Ports** - A connection point for a cable.

**Protocol** -A formal description of a set of rules and conventions that govern how devices on a network exchange information.

**RAID** (Redundant Array of Inexpensive Disks) - A configuration of multiple disks designed to preserve data after a disk casualty.

**RAM** (Random Access Memory) - The working memory of a computer where data and programs are temporarily stored. RAM only holds information when the computer is on.

**Repeater** - A device used in a network to strengthen a signal as it is passed along the network cable.

**RJ-45** - Standard connectors used for unshielded twisted-pair cable.

**Router** -A device that routes information between interconnected networks. It can select the best path to route a message, as well as translate information from one network to another. Many routers now contain firewalls. Home routers can contain firewall, router, switching (for cabled connections), and a wireless access point.

**SCSI (Small Computer Serial Interface)** - An interface controller that allows several peripherals to be connected to the same port on a computer.

**Segment** - Refers to a section of cable on a network. In Ethernet networks, two types of segments are defined. A populated or trunk segment is a network cable that has one or more nodes attached to it. A link segment is a cable that connects a computer to an interconnecting device, such as a repeater or concentrator, or connects a interconnecting device to another interconnecting device.

**Sneaker-Net** - Refers to a manual method of sharing files in which a file is copied from a computer to a floppy disk, transported to a second computer by a person physically walking (apparently wearing sneakers) to the second computer, and manually transferring the file from floppy disk to the second computer.

**Speed of Data Transfer** - The rate at which information travels through a network, usually measured in megabits per second.

**Star Topology** - LAN topology in which each node on a network is connected directly to a central network hub or concentrator.

**Star-Wired Ring** - Network topology that connects network devices (such as computers and printers) in a complete circle.

**Switch** - A "intelligent" type of hub, in that it sends packets only to the intended ports, rather than all computers on the network.

**Tape Back-Up** - A common server or network peripheral which allows copying data and programs from a computer system to magnetic tape. On tape, data is stored sequentially. When retrieving data, the tape is searched from the beginning of tape until the data is found.

**Terminator** - A device that provides electrical resistance at the end of a transmission line. Its function is to absorb signals on the line, thereby keeping them from bouncing back and being received again by the network.

**Thicknet** - A thick coaxial cable that is used with a 10Base5 Ethernet LAN.

**Thinnet** - A thin coaxial cable that is used with a 10Base2 Ethernet LAN.

**Token** - A special packet that contains data and acts as a messenger or carrier between each computer and device on a ring topology. Each computer must wait for the messenger to stop at its node before it can send data over the network.

**Token Ring** - A network protocol developed by IBM in which computers access the network through token-passing. Usually uses a star-wired ring topology.

**Topology** - There are two types of topology: physical and logical. The physical topology of a network refers to the configuration of cables, computers, and other peripherals. Logical topology is the method used to pass the information between workstations. Issues involving logical topologies are discussed on the Protocol chapter

**Transceiver** (Transmitter/Receiver) - A Device that receives and sends signals over a medium. In networks, it is generally used to allow for the connection between two different types of cable connectors, such as AUI and RJ-45.

**Tree Topology** - LAN topology similar to linear bus topology, except that tree networks can contain branches with multiple nodes.

**Twisted Pair** - Network cabling that consists of four pairs of wires that are manufactured with the wires twisted to certain specifications. Available in shielded and unshielded versions.

**USB/ USB2 Port** - A hardware interface for peripherals from keyboards to hard drives, widely used on all computers.

**WAN** (Wide Area Network) - A network connecting computers within very large areas, such as states, countries, and the world.

**Workgroup** - A collection of workstations and servers on a LAN that are designated to communicate and exchange data with one another.

**Workstation** - A computer connected to a network at which users interact with software stored on the network.

## Compiler vs Interpreter : Difference

**Difference between Compiler and Interpreter**

|  |  |  |
| --- | --- | --- |
| **No** | **Compiler** | **Interpreter** |
| **1** | Compiler Takes **Entire** program as input | Interpreter Takes **Single** instruction as input . |
| **2** | Intermediate Object Code is **Generated** | **No** Intermediate Object Code is **Generated** |
| **3** | Conditional Control Statements are Executes **faster** | Conditional Control Statements are Executes **slower** |
| **4** | **Memory Requirement** : **More** (Since Object Code is Generated) | **Memory Requirement** is **Less** |
| **5** | Program need not be **compiled** every time | Every time higher level program is converted into lower level program |
| **6** | **Errors** are displayed after **entire program** is checked | **Errors** are displayed for **every instruction** interpreted (if any) |
| **7** | **Example** : C Compiler | **Example** : BASIC |

**Explanation : Compiler Vs Interpreter**

Just understand the concept of the compiler and interpreter –

1. We give complete program as input to the compiler. Our program is in the human readable format.
2. Human readable format undergoes many [passes and phases of compiler](http://www.c4learn.com/c-programming/what-is-compiler/) and finally it is converted into the machine readable format.
3. However interpreter takes single line of code as input at a time and execute that line. It will terminate the execution of the code as soon as it finds the error.
4. Memory requirement is less in [Case of interpreter](http://www.c4learn.com/c-programming/what-is-interpreter/) because no object code is created in case of interpreter.

Following video will say much more about compiler –

**Interpreter Vs Compiler : Difference Between Interpreter and Compiler**

We generally write a computer program using a high-level language. A high-level language is one which is understandable by us humans. It contains words and phrases from the English (or other) language. But a computer does not understand high-level language. It only understands program written in 0's and 1's in binary, called the machine code. A program written in high-level language is called a source code. We need to convert the source code into machine code and this is accomplished my compilers and interpreters. Hence, a compiler or an interpreter is a program that converts program written in high-level language into machine code understood by the computer.

The difference between an interpreter and a compiler is given below:

|  |  |
| --- | --- |
| **Interpreter** | **Compiler** |
| Translates program one statement at a time. | Scans the entire program and translates it as a whole into machine code. |
| It takes less amount of time to analyze the source code but the overall execution time is slower. | It takes large amount of time to analyze the source code but the overall execution time is comparatively faster. |
| No intermediate object code is generated, hence are memory efficient. | Generates intermediate object code which further requires linking, hence requires more memory. |
| Continues translating the program until the first error is met, in which case it stops. Hence debugging is easy. | It generates the error message only after scanning the whole program. Hence debugging is comparatively hard. |
| Programming language like Python, Ruby use interpreters. | Programming language like C, C++ use compilers. |



**Assembler:** A computer will not understand any program written in a language, other than its machine language. The programs written in other languages must be translated into the machine language. Such translation is performed with the help of software. A program which translates an assembly language program into a machine language program is called an assembler. If an assembler which runs on a computer and produces the machine codes for the same computer then it is called self assembler or resident assembler. If an assembler that runs on a computer and produces the machine codes for other computer then it is called Cross Assembler.

Assemblers are further divided into two types: One Pass Assembler and Two Pass Assembler. One pass assembler is the assembler which assigns the memory addresses to the variables and translates the source code into machine code in the first pass simultaneously. A Two Pass Assembler is the assembler which reads the source code twice. In the first pass, it reads all the variables and assigns them memory addresses. In the second pass, it reads the source code and translates the code into object code.

**Compiler:** It is a program which translates a high level language program into a machine language program. A compiler is more intelligent than an assembler. It checks all kinds of limits, ranges, errors etc. But its program run time is more and occupies a larger part of the memory. It has slow speed. Because a compiler goes through the entire program and then translates the entire program into machine codes. If a compiler runs on a computer and produces the machine codes for the same computer then it is known as a self compiler or resident compiler. On the other hand, if a compiler runs on a computer and produces the machine codes for other computer then it is known as a cross compiler.

**Interpreter:** An interpreter is a program which translates statements of a program into machine code. It translates only one statement of the program at a time. It reads only one statement of program, translates it and executes it. Then it reads the next statement of the program again translates it and executes it. In this way it proceeds further till all the statements are translated and executed. On the other hand, a compiler goes through the entire program and then translates the entire program into machine codes. A compiler is 5 to 25 times faster than an interpreter.

By the compiler, the machine codes are saved permanently for future reference. On the other hand, the machine codes produced by interpreter are not saved. An interpreter is a small program as compared to compiler. It occupies less memory space, so it can be used in a smaller system which has limited memory space.

An assembler translates mnemonics to machine code. It helps with branching, as it processes labels that are inserted in the source code, so that you can branch to the label, without having to calculate the address yourself. The idea is it's supposed to make programming the hardware a bit easier than just dealing with a lot of numbers that don't mean much to humans (but are the means by which the computer executes a program).

C, C++, Java, and C# are examples of compiled languages. The first two typically compile down to machine code. The latter two compile down to bytecode, which are executed on a software virtual machine. They also contain JIT'ers that compile some of the bytecode down to machine code during execution, so it will run directly on the hardware, to help it run faster.

Ruby is an example of an interpreted language.

GAS, or AS (GNU Assembler) is an example of an assembler. There are a lot of assemblers out there. In my experience, each CPU had its own assembler, though my understanding is GAS is a cross-platform assembler. It standardizes on one assembly language, but it translates that to the equivalent machine code for a target processor. So, in that sense it acts a bit like a compiler, since it doesn't just do a one-to-one translation between mnemonics and machine opcodes.

|  |  |
| --- | --- |
| **Networking Terms**   1. ADSP - AppleTalk data stream protocol manages the flow of data between two established socket connections. 2. AEP - AppleTalk echo protocol uses echoes to tell if a computer, or node, is available. 3. AFP - AppleTalk Filing protocol - Makes network files appear local by managing file sharing at the presentation layer. 4. AGP - Accelerated Graphics Port. This bus is developed for fast video cards. It is currently up to 4X mode speed. 5. API - Application Programming Interface. 6. APPC - Advanced Peer-to-Peer Communications provides peer to peer services at the transport and session layer. 7. APPN - Advanced Peer-to-Peer Networking supports the computer connections at the network and transport layers. 8. Architecture - The method that is used to transmit packets on a network. Sometimes the term architecture includes topology. An example is ethernet. 9. ARCnet - Attached Resource Computer Network is an architecture using star and bus topology. 10. ARP - Address resolution Protocol is used to resolve the hardware address of a card to package the ethernet data. It works at the data link layer. RFC 826. 11. ARUP - AppleTalk update routing is a newer version of RTMP. 12. ASP - AppleTalk session protocol controls the starting and ending of sessions between computers called nodes. It works at the session level. 13. ATM - Asynchronous Transfer Mode may be used over a variety of media with both baseband and broadband systems. It uses fixed length data packets of 53 bytes called cell switching. 14. ATP - AppleTalk Transaction Protocol provides a Transport Layer connection between computers. 15. attenuation - signal loss due to impedance. 16. AU - Access Unit provides access to resources like fax, telex, and teletex. 17. AUI - Attachment uint interface used to attach a station to a thicknet cable. 18. Backbone - Main cable used to connect computers on a network. 19. Bandwidth - Indicates the amount of data that can be sent in a time period. Measured in Mbps which is one million bits per second. 20. Baseband - Data bits are defined by discrete signal changes. 21. BDC - Backup Domain Controller is a backup for a PDC 22. BGP - Border Gateway Protocol, a dynamic routing protocol. RFC 1267. 23. BNC - British Naval Connector. 24. BOOTP - Boot Protocol. RFC 951, 1542. 25. Bridge - Read the outermost section of data on the data packet, to tell where the message is going. It reduces the traffic on other network segments, since it does not send all packets but only sends packets intended for that segment they are attached to. 26. Broadband - Uses analog signals to divide the cable into several channels with each channel at its own frequency. Each channel can only transmit one direction. 27. Broadcast - A transmission to all interface cards on the network. 28. Brouter - Will function similar to a bridge for network transport protocols that are not routable, and will function as a router for routable protocols. 29. BSC - Binary Synchronous Communication sends bits in frames which are timed sequences of data. A possible SNA communications architecture, 30. CCITT - International Telegraph and Telephone Consultative Committee. 31. CDDI - A copper version of FDDI which uses category 5 cable. Obviously the distance is more limited than FDDI. 32. CHAP - Challenge Handshake Authentication Protocol is a three way handshake protocol which is considered more secure than PAP. 33. CIDR - Classless Inter Domain Routing. 34. Client - This computer requests resources for its use from a computer that provides the resource (a server). 35. CDPD - Cellular Digital Packet Data will allow network connections for mobile users using satellites. 36. CSMA/CD - Carrier-sense multiple-access with collision detection for controlling access to the network media. 37. CSU - Channel service unit used to connect to digital leased lines on the line side. 38. DAS - Dual attachment stations are used by FDDI networks for servers and concentrators are attached to both rings. 39. DAT - Digital Audio Tape |  |

* DBMS - Database Management Systems are used to share data on a network.
* DCE - Data communications equipment.
* DDP - Datagram Delivery Protocol is a routable protocol that provides for data packet transportation. It operates at the network layer at the same level of the IP protocol.
* DDS - Digital data service is a leased dedicated digital line.
* DECnet - From Digital Equipment Corporation is a suite of protocols which may be used on large networks that integrate mainframe and minicomputer systems
* DHCP - Dynamic Host Configuration Protocol is used to assign IP addresses dynamically to network cards works at the application layer. RFC 1541.
* Direct sequence modulation - The data is broken into parts and transmitted simultaneously on multiple frequencies.
* DLC - Data Link Control operates at the data link layer and is designed for communications between Hewlett-Packard network printers and IBM mainframe computers on a DECnet network.
* DNA - Digital Network Architecture is a term from DECNet
* DNS - Domain Name System is used on the internet to correlate between IP address and readable names. RFC 1034, 1035, 1535-1537, 1591.
* DRDA - Distributed Relational Database Architecture is from IBM.
* DSU - Digital service unit used to connect to digital leased lines on the LAN side.
* DTD - Document Type Definition.
* DTE - Data terminal equipment.
* DUN - Dial up networking.
* DVM - Digital volt meter.
* EGP - Exterior Gateway Protocol. Used between routers of different systems.
* EIA - Electronic Industries Association .
* EISA - Extended ISA used when the 80286 through 80486 series microprocessors were being produced. It is backward compatible with ISA.
* EMI - Electromagnetic Interference.
* Ethernet - A network architecture that uses carrier-sense multiple-access with collision detection (CSMA/CD) for controlling access to the network media and baseband broadcasts. It uses star topology.
* FDDI - Fiber Distributed Data Interface is a network architecture normally used to send longer distances. Topology is ring with two counter rotating rings for reliability with no hubs. Cable type is fiber-optic.
* Frame Relay - Error checking is handled by devices at both sides of the connection. Frame relay uses frames of varying length and it operates at the data link layer of the OSI model. A permanent virtual circuit (PVC) is established between two points on the network. Frame relay speed is between 56Kbps and 1.544Mbps.
* Frequency hopping - The transmitter and receiver change predetermined frequencies at the same time (in a synchronized manner).
* FTP - File Transport Protocol is a TCP/IP protocol running at the application layer.
* Gateway - A gateway can translate information between different network data formats or network architectures. It can translate TCP/IP to AppleTalk so computers supporting TCP/IP can communicate with Apple brand computers. Not the same as a default gateway used by a client to send packets to.
* HTML - Hypertext Markup Language is the format many files for web viewing are in. It is a language with "mark-up" text included for formatting.
* HTTP - Hypertext Transfer Protocol is the protocol used to communicate between web servers and web browser software clients.
* Hub - A type of repeater used on several network architectures which usually connects several stations.
* IAB - Internet Architecture Board
* IANA - Internet Assigned Numbers Authority.
* ICMP - Internet Control Message Protocol is used to perform network error reporting and status. It works at the transport layer. RFC 792.
* IETF - Internet Engineering Task Force. Sets Internet technical standards.
* IGMP - Internet Group Management Protocol, used for managing multicast groups. RFC 1112.
* IMAP4 - Internet Mail Access Protocol version 4 is the replacement for POP3
* Impedance - The amount of resistance to the transmission device.
* Infared - Infared is just below the visible range of light between 100Ghz and 1000Thz.
* Interference - Electromagnetic Interference (EMI). Crosstalk - When wires pick up electromagnetic signals from nearby wires also carrying signals.
* InterNIC - Internet Network Information Center, the authority for allocating internet addresses.
* Intranet - Refers to using internet technologies such as a web server on an internal network.
* IP - Internet Protocol os used for software addressing of computers and works at the data link layer. RFC 791.
* IPIP tunneling - Tunneling IP packets in IP packets. Used for VPN tunneling.
* IPSec - Internet protocol security, developed by IETF, implemented at layer 3. it is a collection of security measures that address data privacy, integrity, authentication, and key management, in addition to tunneling. Used for VPN.
* IPX - Internetwork Packet Exchange supports the transport and network layers of the OSI network model. Provides for network addressing and routing. It provides fast, unreliable, communication with network nodes using a connection less datagram service.
* IRQ- Interrupt Request
* IRTF - Internet Research Task force.
* ISA - Industry Standard Architecture internal computer bus. Used when the original 8088 8bit microprocessor based personal computers were produced. (16 bit).
* ISAKMP/Oakley - Internet Security Association and Key Management Protocol Authentication.
* ISDN - Integrated Services Digital Network is a method of sending voice and data information on a digital phone line. Two 64Kbps B-channels with one 16Kbps D channel is provided with basic ISDN service
* ISP - Internet Service Provider
* ISOC - Internet Society, promotes internet policies.
* ITU - International Telecommunication Union.
* FTP - File Transfer Protocol.
* L2F - Layer2 Forwarding, works at the link layer of the OSI model. It has no encryption. Being replaced by L2TP. It is used for VPN.
* L2TP - Layer 2 tunneling protocol (RFC 2661). Used for VPN tunneling.
* LAN - Local Area Network
* LDA - Local delivery agent on the receiving machine receives the mail from its MTA. This program is usually procmail.
* LU - Logical Units are ports that users use to access network resources is an SNA term.
* MAC - Media Access Control address. Basically a network card unique hardware address.
* Mail notifier - This program notifies the recipient that they have mail. Normally this requires two programs, biff and comsat. Biff allows the administrator or user to turn on comsat service.
* MAN- Metropolitan area network refers to a network which connects several LANS over various media that is large enough to cover an area the size of a city.
* MAPI - Microsoft's Messaging API which is incorporated throughout Microsoft's office products supports mail at the application level.
* MAU - Multistation access unit used by Token Ring Networks.
* MBONE - Being on the MBONE means you are on a network that supports multicasting.
* MCI - Microchannel architecture by IBM and used mainly on IBM brand computers for the internal bus. Established in 1988. (16 or 32 bits).
* Media - The hardware method used to connect computers over a network. The three main types are copper cable, fiber optic cable, and wireless.
* Media converter - Used to adapt from one cable type to another.
* MHS - Message Handling Service by Novell is used for mail on Netware networks.
* MIB - Management Information BASE specifies variables the network elements maintain. Works with the TCP/IP protocol SNMP.
* MIME - Multipurpose Internet Mail Extension is the protocol that defines the way files are attached to SMTP messages.
* MOTIS - Message-oriented text interchange system.
* MS - Message Store is a storage area for messages that can't be delivered immediately when the recipient is off-line.
* MTA - Message transfer agent is used to pass mail from the sending machine to the receiving machine. There is a MTA program running on both the sending and receiving machine. Sendmail is a MTA.
* MTU - Maximum Transmission Unit is the maximum size of each data packet for the ethernet protocol.
* MUA - Mail users agent. This is the program a user will use to type e-mail. It usually incorporates an editor for support. The user types the mail and it is passed to the sending MTA. This may also be called the user agent (UA).
* Multicasting - Transmitting to a group of interface cards on the network.
* NADN - Nearest Active Downstream Neighbor is a Token ring Architecture term.
* NAU - Network Addressable Units is an SNA term.
* NAUN - Nearest Active Upstream Neighbor is a Token ring Architecture term.
* NAT - Network Address Translation.
* NBF - NetBIOS Frame Protocol.
* NBNS - NetBIOS Name Server. A server that maps NetBIOS names to IP addresses. This service is provided by the nmbd daemon on Linux.
* NBP - Name-binding protocol of the AppleTalk suite of protocols translates addresses into names.
* NBT - NetBIOS over TCP/IP defined by RFC 1002.
* NCP - NetWare Core Protocol provides for client/server interactions such as file and print sharing. It works at the application, presentation, and session levels.
* NCP - Network Control Program performs routing, session management tasks. It runs in the communications controller. It is an SNA networking term.
* NDIS - Network Driver Interface Specification from Microsoft, is used on Microsoft networks. It allows multiple protocols to be used on a network card and supports the data link layer of the network model.
* NetBEUI - NetBIOS Extended User Interface works at the transport layer and provides data transportation. It is not a routable transport protocol which is why NBT exists on large networks to use routable TCP protocol on large networks.
* NetBIOS - Network Basic Input Output System by Microsoft.
* Network Operating System - Typically used to run computers that act as servers, but may be used on various types of computers today.
* NFS - Network File System. A protocol that allows UNIX and Linux systems remotely mount each other's file systems. RFC 1094
* NIC - Network interface card. Also called LAN adapters.
* NNTP - Network News Transport Protocol is used to link newsgroups for discussions on the web
* OC - Optical Carrier level, see SONET.
* ODBC - Open Database Connectivity (ODBC) from Microsoft lets application developers integrate database connections in applications. It is an application programming interface (API). ODBC drivers convert an application's query int SQL and send it to the database engine program.
* ODI - Open Data-link Interface operates at the data link layer allowing IPX to work with any network interface card.
* OSI - Open Systems Interconnect is a suite of protocols developed by the International Standards Organization (ISO) which corresponds with the layers of the OSI model.
* OSPF - Open Shortest Path First, a dynamic routing protocol. RFC 1247.
* PAP - Password Authentification Protocol is a two way handshake protocol designed for use with PPP.
* PAP - Printer access protocol of the AppleTalk suite of protocols manages information between workstations and printers.
* PCI - Peripheral Component Interconnect internal computer bus. The popular expansion bus of choice. It is significantly faster than EISA. This is a 32bit bus with plug and play capability from Intel.
* PDC - Primary Domain Controller is an NT server providing central control of user access permissions and accounts on a network.
* PDL - Page description language is a printing language.
* PDN - Public data network.
* Peer - A computer that can act as both a client and a server.
* Plenum - Space above a false ceiling in an office area where heat ducts and cables may be run. Plenum cabling is special fire resistant cabling required for use in these areas due to fire hazards.
* POP - Point of presence is each point at the end of the transport media (internet) when talking about VPN.
* POP3 - Post Office Protocol version 3 is used by clients to access an internet mail server to get mail. It is not a transport layer protocol.
* Protocol - A set of standards sets of standards that define all operations within a network. There are various protocols that operate at various levels of the OSI network model such as transport protocols include TCP, SPX.
* PPP - Point to Point Protocol, used for serial connections to a network ot the internet. (RFC 1332, 1548)
* PPTP - Point to point tunneling protocol (RFC 2637) Used for VPN tunneling.
* PU - Physical Units are a network device used to communicate with hosts. It is an SNA term.
* PVC - Permanent virtual circuit is set up once in communication switches to establish a permanent circuit.
* RADIUS - Remote Authentication Dial-In User Service is used for dial in clients to connect to other computers or a network. It provides authentication and accounting when using PPTP or L2TP tunneling.
* RAID - Redundant Array of Inexpensive disks is a fault tolerant method of storing data, meaning that a failure can occur and the system will still function.
* RARP -Reverse Address Resolution Protocol used for disk less computers to determine their IP address using the network. It works at the data link layer. RFC 903.
* RAS - Remote Access Service (RAS) with Windows NT allows users connecting to the network using a modem to use network resources. The NT RAS server can handle 256 connections.
* Redirector - it runs on a windows operating system and directs requests for network resources to the appropriate server and makes network resources seem to be local resources.
* Repeater - Used on a network to regenerate signals to be sent over long distances or tie computers together on a network.
* Resolver - Used as part of DNS, it is the client side asking for DNS information.
* RIP - Routing Information Protocol, a dynamic routing protocol. A distance-vector algorithm is used to calculate the best route for a packet. RFC 1058, 1388 (RIP2).
* Rlogin - Remote login between UNIX hosts. This is outdated and is replaced by Telnet.
* Router - Routes data packets between two networks. It reads the information in each packet to tell where it is going.
* RPC - Remote Procedure Call. A protocol invented by Sun Microsystem to allow remote computers to invoke functions on other hosts. RFC 1057.
* RR - Resource Records are a part of the DNS database.
* RTMP - Routing table maintenance protocol is used to update routers with information about network status and address tables. The whole address table is sent across the network.
* S/Key - A one time password system, secure against replays. RFC 2289.
* SAP - Service Advertising Protocol packets are used by file and print servers to periodically advertise the address of the server and the services available. It works at the application, presentation, and session levels.
* SAS - Single Attachment stations attached to one ring and used by FDDI networks to attach workstations to concentrators.
* SDH - Synchronous Digital Hierarchy
* SDLS - Synchronous Data Link Control is a possible SNA communications architecture.
* Sector Sparing - A method of fault tolerance that automatically identifies and marks bad sectors as not available. It is also called hot-fixing.
* Server - For the most part it provides resources on the network for other computers to use.
* SGML - Standardized General Markup Language is the base language for document publishing and is used to define XML, HTML and more.
* Shielding - Used to minimize interference.
* SLED - Single Large Inexpensive disk - The concept that a large disk costs less per amount of storage than several smaller ones. Somehow this concept is used as a means of fault tolerance.
* SLIP - Serial Line interface Protocol used to connect serially to a network or internet. RFC 1055, 1144 (Compressed). Replaced by PPP.
* SMAU - Smart Multistation Access Unit.
* SMB - Server Message Block protocol works at the presentation level to provide peer to peer communication.
* SMDS - Switched Multi-megabit Data Service uses fixed length cell switching and runs at speeds of 1.533 to 45Mbps.
* SMS - SMS - Systems Management Server from Microsoft can collect information of software on each computer and can install and configure new software on the client computers. It will also monitor network traffic.
* SMTP - Simple Mail Transfer Protocol is a TCP protocol for mail transport running at the application layer. RFC 821, 822.
* SNA - System Network Architecture by IBM is a suite of protocols mainly used with IBM mainframe and AS/400 computers.
* SNMP - Simple Network Management Protocol. RFC 1155, 1157, 1213, 1441.
* SONET - Synchronous Optical Network is a physical layer standard that defines voice, data, and video delivery methods over fiber optic media. It defines data rates in terms of optical carrier (OC) levels.
* Spread spectrum - It uses several frequencies at the same time.
* SPX - Sequenced Packet Exchange operates at the transport layer providing connection oriented communication on top of IPX.
* SQL - Structured Query Language is a database access language. It is used by most client/server database applications.
* SSCP - Systems Services Control Point manages all resources in the host's domain. An SNA term.
* STP - Shielded Twisted Pair cable. 100 meter maximum length. 16-155 Mbps speed. Lower electrical interference than UTP
* STS
* SVC - Switched virtual circuit is temporarily set up by switching mechanisims to establish a connection between devices for a session.
* TACACS - Offers authentication, accounting, and authorization.
* T Carrier - Multiplexors are used to allow several channels on one line. The T1 line is basic T Carrier service.
* TCP - Transport Control protocol is a connection oriented reliable protocol working at the transport layer. RFC 793.
* TDI - Transport Driver Interface is a standard for passing messages between the drivers at the data link layer and the protocols working at the network layer such as IP or NetBEUI. It was produced by Microsoft.
* TDR - Time-domain reflectometer sends a sonar like electrical pulse down a cable and can determine the location of a break in the cable.
* TFTP - Trivial File Transfer Protocol. RFC 1350.
* Telnet - Remote session at the application layer. RFC 854.
* Thicknet - Half inch rigid cable. Maximum cable length is 500 meters. Transmission speed is 10Mbps. Expensive and is not commonly used. (RG-11 or RG-8).
* Thinnet - Thinnet uses a British Naval Connector (BNC) on each end. Thinnet is part of the RG-58 family of cable\*. Maximum cable length is 185 meters. Transmission speed is 10Mbps.
* TIA - Telecommunications Industries Association .
* TLD - Top Level domain
* Token Ring - A network architecture developed by IBM which sends tokens around a ring of computers to allow media access. Standardized to IEEE 802.5
* Topology - The shape of the physical connection of a network with regard to repeaters and networked computers. The three main types are ring, bus, and star.
* UA - Users agent. This is the program a user will use to type e-mail. It usually incorporates an editor for support. The user types the mail and it is passed to the sending MTA. This may also be called the mail user agent (MUA).
* UDP - User Datagram Protocol is a connection less unreliable protocol working at the transport layer. RFC 768.
* UNC - Universal Naming Convention is used to allow the use of shared resources without mapping a drive to them.
* Unicast - A transmission to a single interface card.
* URL - Universal Resource Location is a term used to describe the name of a web based resource such as a web page or location of a file for down loading.
* UTP - Unshielded Twisted Pair cable. Normally UTP contains 8 wires or 4 pair. 100 meter maximum length. 4-100 Mbps speed.
* VIM - Vendor-Independent Messaging protocol from Lotus supports mail at the application level and is supported by many vendors exclusive of Microsoft.
* VPN - Virtual Private Networking. The function of VPN is to allow two computers or networks to talk to each other over a transport media that is not secure, but the network is made secure by VPN security protocols.
* W3C - World Wide Web Consortium, sets standards for the web working with the IETF.
* WAN - Wide Area Network is larger than a MAN and may be an enterprise network or a global network.
* WINS - Windows Internet Name Service is the Microsoft implementation of NetBIOS name service.
* wireless bridge - Microwave or Infared is used between two line of site points where it is difficult to run wire.
* X.25 - This is a set of protocols developed by the CCITT/ITU which specifies how to connect computer devices over a internetwork.
* X.400 - International Telecommunication Union standard defines transfer protocols for sending mail between mail servers.
* X.500 - This is a recommendation outlining how an organization can share objects and names on a large network. It is hierarchical similar to DNS, defining domains consisting of organizations, divisions, departments, and workgroups.
* XML - Extensible Markup Language is a subset of SGML and is used widely on the web.
* ZIP - Zone information protocol used with RTMP to map zones. Routers use zone information tables (ZITs) to define network addresses and zone names.

**List of FTP commands for the Microsoft command-line FTP client**

**Command-line options**

As you're starting the program from a DOS prompt:  
ftp [-v] [-d] [-i] [-n] [-g] [-s:filename] [-a] [-w:windowsize] [computer]

* **-v** - Suppresses [verbose](http://www.nsftools.com/tips/MSFTP.htm#verbose) display of remote server responses.
* **-n** - Suppresses auto-login upon initial connection.
* **-i** - Turns off interactive [prompting](http://www.nsftools.com/tips/MSFTP.htm#prompt) during multiple file transfers.
* **-d** - Enables [debugging](http://www.nsftools.com/tips/MSFTP.htm#debug), displaying all ftp commands passed between the client and server.
* **-g** - Disables filename [globbing](http://www.nsftools.com/tips/MSFTP.htm#glob), which permits the use of wildcard chracters in local file and path names.
* **-s:filename** - Specifies a text file containing ftp commands; the commands will automatically run after ftp starts. No spaces are allowed in this parameter. Use this switch instead of redirection (>).
* **-a** - Use any local interface when binding data connection.
* **-w:windowsize** - Overrides the default transfer buffer size of 4096.
* **computer** - Specifies the computer name or IP address of the remote computer to connect to. The computer, if specified, must be the last parameter on the line.

**Client commands**

* [!](http://www.nsftools.com/tips/MSFTP.htm#%21) - Runs the specified command on the local computer
* [?](http://www.nsftools.com/tips/MSFTP.htm#?) - Displays descriptions for ftp commands
* [append](http://www.nsftools.com/tips/MSFTP.htm#append) - Appends a local file to a file on the remote computer
* [ascii](http://www.nsftools.com/tips/MSFTP.htm#ascii) - Sets the file transfer type to ASCII, the default
* [bell](http://www.nsftools.com/tips/MSFTP.htm#bell) - Toggles a bell to ring after each file transfer command is completed (default = OFF)
* [binary](http://www.nsftools.com/tips/MSFTP.htm#binary) - Sets the file transfer type to binary
* [bye](http://www.nsftools.com/tips/MSFTP.htm#bye) - Ends the FTP session and exits ftp
* [cd](http://www.nsftools.com/tips/MSFTP.htm#cd) - Changes the working directory on the remote computer
* [close](http://www.nsftools.com/tips/MSFTP.htm#close) - Ends the FTP session and returns to the command interpreter
* [debug](http://www.nsftools.com/tips/MSFTP.htm#debug) - Toggles debugging (default = OFF)
* [delete](http://www.nsftools.com/tips/MSFTP.htm#delete) - Deletes a single file on a remote computer
* [dir](http://www.nsftools.com/tips/MSFTP.htm#dir) - Displays a list of a remote directory's files and subdirectories
* [disconnect](http://www.nsftools.com/tips/MSFTP.htm#disconnect) - Disconnects from the remote computer, retaining the ftp prompt
* [get](http://www.nsftools.com/tips/MSFTP.htm#get) - Copies a single remote file to the local computer
* [glob](http://www.nsftools.com/tips/MSFTP.htm#glob) - Toggles filename globbing (wildcard characters) (default = ON)
* [hash](http://www.nsftools.com/tips/MSFTP.htm#hash) - Toggles hash-sign (#) printing for each data block transferred (default = OFF)
* [help](http://www.nsftools.com/tips/MSFTP.htm#help) - Displays descriptions for ftp commands
* [lcd](http://www.nsftools.com/tips/MSFTP.htm#lcd) - Changes the working directory on the local computer
* [literal](http://www.nsftools.com/tips/MSFTP.htm#literal) - Sends arguments, verbatim, to the remote FTP server
* [ls](http://www.nsftools.com/tips/MSFTP.htm#ls) - Displays an abbreviated list of a remote directory's files and subdirectories
* [mdelete](http://www.nsftools.com/tips/MSFTP.htm#mdelete) - Deletes one or more files on a remote computer
* [mdir](http://www.nsftools.com/tips/MSFTP.htm#mdir) - Displays a list of a remote directory's files and subdirectories
* [mget](http://www.nsftools.com/tips/MSFTP.htm#mget) - Copies one or more remote files to the local computer
* [mkdir](http://www.nsftools.com/tips/MSFTP.htm#mkdir) - Creates a remote directory
* [mls](http://www.nsftools.com/tips/MSFTP.htm#mls) - Displays an abbreviated list of a remote directory's files and subdirectories
* [mput](http://www.nsftools.com/tips/MSFTP.htm#mput) - Copies one or more local files to the remote computer
* [open](http://www.nsftools.com/tips/MSFTP.htm#open) - Connects to the specified FTP server
* [prompt](http://www.nsftools.com/tips/MSFTP.htm#prompt) - Toggles prompting (default = ON)
* [put](http://www.nsftools.com/tips/MSFTP.htm#put) - Copies a single local file to the remote computer
* [pwd](http://www.nsftools.com/tips/MSFTP.htm#pwd) - Displays the current directory on the remote computer (literally, "print working directory")
* [quit](http://www.nsftools.com/tips/MSFTP.htm#quit) - Ends the FTP session with the remote computer and exits ftp (same as "bye")
* [quote](http://www.nsftools.com/tips/MSFTP.htm#quote) - Sends arguments, verbatim, to the remote FTP server (same as "literal")
* [recv](http://www.nsftools.com/tips/MSFTP.htm#recv) - Copies a remote file to the local computer
* [remotehelp](http://www.nsftools.com/tips/MSFTP.htm#remotehelp) - Displays help for remote commands
* [rename](http://www.nsftools.com/tips/MSFTP.htm#rename) - Renames remote files
* [rmdir](http://www.nsftools.com/tips/MSFTP.htm#rmdir) - Deletes a remote directory
* [send](http://www.nsftools.com/tips/MSFTP.htm#send) - Copies a local file to the remote computer (same as "put")
* [status](http://www.nsftools.com/tips/MSFTP.htm#status) - Displays the current status of FTP connections
* [trace](http://www.nsftools.com/tips/MSFTP.htm#trace) - Toggles packet tracing (default = OFF)
* [type](http://www.nsftools.com/tips/MSFTP.htm#type) - Sets or displays the file transfer type (default = ASCII)
* [user](http://www.nsftools.com/tips/MSFTP.htm#user) - Specifes a user to the remote computer
* [verbose](http://www.nsftools.com/tips/MSFTP.htm#verbose) - Toggles verbose mode (default = ON)

**!**

Runs the specified command on the local computer.

*Syntax:* ! *[command]*

Parameter(s):  
*command* - Specifies the command to run on the local computer. If command is omitted, the local command prompt is displayed; type "exit" to return to ftp.

**?**

Displays descriptions for ftp commands. ? is identical to [help](http://www.nsftools.com/tips/MSFTP.htm#help).

*Syntax:* ? *[command]*

Parameter(s):  
*command* - Specifies the name of the command about which you want a description. If command is not specified, ftp displays a list of all commands.

**append**

Appends a local file to a file on the remote computer using the current file type setting.

*Syntax:* append *local-file [remote-file]*

Parameter(s):  
*local-file* - Specifies the local file to add.   
*remote-file* - Specifies the file on the remote computer to which local-file will be added. If remote-file is omitted, the local filename is used for the remote filename.

**ascii**

Sets the file transfer type to ASCII, the default.

*Syntax:* ascii

Note  
FTP supports two file transfer types, ASCII and binary image. ASCII should be used when transferring text files. See also [binary](http://www.nsftools.com/tips/MSFTP.htm#binary).

In ASCII mode, character conversions to and from the network standard character set are performed. For example, end-of-line characters are converted as necessary, based on the target operating system.

**bell**

Toggles a bell to ring after each file transfer command is completed. By default, the bell is off.

*Syntax:* bell

**binary**

Sets the file transfer type to binary.

*Syntax:* binary

Note  
FTP supports two file transfer types, ASCII and binary image. Binary should be used when transferring executable files. In binary mode, the file is moved byte-by-byte. See also [ascii](http://www.nsftools.com/tips/MSFTP.htm#ascii).

**bye**

Ends the FTP session with the remote computer and exits ftp.

*Syntax:* bye

**cd**

Changes the working directory on the remote computer.

*Syntax:* cd *remote-directory*

Parameter(s):  
*remote-directory* - Specifies the directory on the remote computer to change to.

**close**

Ends the FTP session with the remote server and returns to the command interpreter.

*Syntax:* close

**debug**

Toggles debugging. When debugging is on, each command sent to the remote computer is printed, preceded by the string --->. By default, debugging is off.

*Syntax:* debug

**delete**

Deletes a single file on a remote computer. See also [mdelete](http://www.nsftools.com/tips/MSFTP.htm#mdelete), which can delete multiple files.

*Syntax:* delete *remote-file*

Parameter(s):  
*remote-file* - Specifies the file to delete.

**dir**

Displays a list of a remote directory's files and subdirectories. See also [mdir](http://www.nsftools.com/tips/MSFTP.htm#mdir), which can list multiple directories.

*Syntax:* dir *[remote-directory] [local-file]*

Parameter(s):  
*remote-directory* - Specifies the directory for which you want to see a listing. If no directory is specified, the current working directory on the remote computer is used.   
*local-file* - Specifies a local file to store the listing. If not specified, output is displayed on the screen.

**disconnect**

Disconnects from the remote computer, retaining the ftp prompt.

*Syntax:* disconnect

**get**

Copies a remote file to the local computer using the current file transfer [type](http://www.nsftools.com/tips/MSFTP.htm#type). See also [mget](http://www.nsftools.com/tips/MSFTP.htm#mget), which can copy multiple files.

*Syntax:* get *remote-file [local-file]*

Parameter(s):  
*remote-file*  
Specifies the remote file to copy.

*local-file*  
Specifies the name to use on the local computer. If not specified, the file is given the remote-file name.

**glob**

Toggles filename globbing. Globbing permits use of wildcard characters in local file or path names. By default, globbing is on.

*Syntax:* glob

**hash**

Toggles hash-sign (#) printing for each data block transferred. The size of a data block is 2048 bytes. By default, hash mark printing is off.

*Syntax:* hash

**help**

Displays descriptions for ftp commands.

*Syntax:* help *[command]*

Parameter(s):  
*command* - Specifies the name of the command about which you want a description. If command is not specified, ftp displays a list of all commands.

**lcd**

Changes the working directory on the local computer. By default, the working directory is the directory in which ftp was started.

*Syntax:* lcd *[directory]*

Parameter(s):  
*directory* - Specifies the directory on the local computer to change to. If directory is not specified, the current working directory on the local computer is displayed.

**literal**

Sends arguments, verbatim, to the remote FTP server. A single FTP reply code is expected in return.

*Syntax:* literal *argument [ ...]*

Parameter(s):  
*argument* - Specifies the argument to send to the FTP server.

**ls**

Displays an abbreviated list of a remote directory's files and subdirectories.

*Syntax:* ls *[remote-directory] [local-file]*

Parameter(s):  
*remote-directory* - Specifies the directory for which you want to see a listing. If no directory is specified, the current working directory on the remote computer is used.   
*local-file* - Specifies a local file to store the listing. If not specified, output is displayed on the screen.

**mdelete**

Deletes one or more files on a remote computer.

*Syntax:* mdelete *remote-files [ ...]*

Parameter(s):  
*remote-files* - Specifies the remote files to delete.

**mdir**

Displays a list of a remote directory's files and subdirectories. Mdir allows you to specify multiple files.

*Syntax:* mdir *remote-files [ ...] local-file*

Parameter(s):  
*remote-files* - Specifies the directory for which you want to see a listing. Remote-files must be specified; type "-" to use the current working directory on the remote computer.   
*local-file* - Specifies a local file to store the listing. Type "-" to display the listing on the screen.

**mget**

Copies one or more remote files to the local computer using the current file transfer [type](http://www.nsftools.com/tips/MSFTP.htm#type).

*Syntax:* mget *remote-files [ ...]*

Parameter(s):  
*remote-files* - Specifies the remote file(s) to copy to the local computer.

**mkdir**

Creates a remote directory.

*Syntax:* mkdir *directory*

Parameter(s):  
*directory* - Specifies the name of the new remote directory.

**mls**

Displays an abbreviated list of a remote directory's files and subdirectories.

*Syntax:* mls *remote-files [ ...] local-file*

Parameter(s):  
*remote-files* - Specifies the files for which you want to see a listing. Remote-files must be specified; type "-" to use the current working directory on the remote computer.   
*local-file* - Specifies a local file to store the listing. Type "-" to display the listing on the screen.

**mput**

Copies one or more local files to the remote computer using the current file transfer [type](http://www.nsftools.com/tips/MSFTP.htm#type).

*Syntax:* mput *local-files [ ...]*

Parameter(s):  
*local-files* - Specifies the local files to copy to the remote computer.

**open**

Connects to the specified FTP server.

*Syntax:* open *computer [port]*

Parameter(s):  
*computer* - Specifies the remote computer to connect to. Computer can be specified by IP address or computer name (a DNS or HOSTS file must be available). If auto-login is on (default), FTP also attempts to automatically log the user in to the FTP server (see Ftp command-line options to disable auto-login).   
*port* - Specifies a port number to use to contact an FTP server.

**prompt**

Toggles prompting. Ftp prompts during multiple file transfers to allow you to selectively retrieve or store files; [mget](http://www.nsftools.com/tips/MSFTP.htm#mget) and [mput](http://www.nsftools.com/tips/MSFTP.htm#mput) transfer all files if prompting is turned off. By default, prompting is on.

*Syntax:* prompt

**put**

Copies a local file to the remote computer using the current file transfer [type](http://www.nsftools.com/tips/MSFTP.htm#type). See also [mput](http://www.nsftools.com/tips/MSFTP.htm#mput), which can copy multiple files.

*Syntax:* put *local-file [remote-file]*

Parameter(s):  
*local-file* - Specifies the local file to copy.   
*remote-file* - Specifies the name to use on the remote computer. If not specified, the file is given the local-file name.

**pwd**

Displays the current directory on the remote computer.

*Syntax:* pwd

**quit**

Ends the FTP session with the remote computer and exits ftp.

*Syntax:* quit

**quote**

Sends arguments, verbatim, to the remote FTP server. A single FTP reply code is expected in return. Quote is identical to [literal](http://www.nsftools.com/tips/MSFTP.htm#literal).

*Syntax:* quote *argument [ ...]*

Parameter(s):  
*argument* - Specifies the argument to send to the FTP server.

**recv**

Copies a remote file to the local computer using the current file transfer [type](http://www.nsftools.com/tips/MSFTP.htm#type). Recv is identical to [get](http://www.nsftools.com/tips/MSFTP.htm#get).

*Syntax:* recv *remote-file [local-file]*

Parameter(s):  
*remote-file* - Specifies the remote file to copy.   
*local-file* - Specifies the name to use on the local computer. If not specified, the file is given the remote-file name.

**remotehelp**

Displays help for remote commands.

*Syntax:* remotehelp *[command]*

Parameter(s):  
*command* - Specifies the name of the command about which you want help. If command is not specified, ftp displays a list of all remote commands.

**rename**

Renames remote files.

*Syntax:* rename *filename newfilename*

Parameter(s):  
*filename* - Specifies the file you want to rename.   
*newfilename* - Specifies the new filename.

**rmdir**

Deletes a remote directory.

*Syntax:* rmdir *directory*

Parameter(s):  
*directory* - Specifies the name of the remote directory to delete.

**send**

Copies a local file to the remote computer using the current file transfer [type](http://www.nsftools.com/tips/MSFTP.htm#type). Send is identical to [put](http://www.nsftools.com/tips/MSFTP.htm#put).

*Syntax:* send *local-file [remote-file]*

Parameter(s):  
*local-file* - Specifies the local file to copy.   
*remote-file* - Specifies the name to use on the remote computer. If not specified, the file is given the local-file name.

**status**

Displays the current status of FTP connections and toggles.

*Syntax:* status

**trace**

Toggles packet tracing; trace displays the route of each packet when running an ftp command.

*Syntax:* trace

**type**

Sets or displays the file transfer type.

*Syntax:* type *[type-name]*

Parameter(s):  
*type-name* - Specifies the file transfer type; the default is ASCII. If type-name is not specified, the current type is displayed.

Note  
FTP supports two file transfer types, ASCII and binary image.

[ASCII](http://www.nsftools.com/tips/MSFTP.htm#ascii) should be used when transferring text files. In ASCII mode, character conversions to and from the network standard character set are performed. For example, end-of-line characters are converted as necessary, based on the destination's operating system.

[Binary](http://www.nsftools.com/tips/MSFTP.htm#binary) should be used when transferring executable files. In binary mode, the file is moved byte-by-byte.

**user**

Specifes a user to the remote computer.

*Syntax:* user *user-name [password] [account]*

Parameter(s):  
*user-name* - Specifies a user name with which to log in to the remote computer.   
*password* - Specifies the password for user-name. If not specified, but required, ftp prompts for the password.   
*account* - Specifies an account with which to log on to the remote computer. If account is not specified, but required, ftp prompts for the account.

**verbose**

Toggles verbose mode. If on, all ftp responses are displayed; when a file transfer completes, statistics regarding the efficiency of the transfer are also displayed. By default, verbose is on.

*Syntax:* verbose

**How do I use FTP from a command line?**

Note: FTP is not an encrypted transmission, which means any data sent over it, including your username and password, could be read by anyone who may intercept your transmission. If you're wanting a more secure transmission, we suggest using [SFTP](http://www.computerhope.com/jargon/s/sftp.htm).

[**Connect using FTP**](http://www.computerhope.com/issues/ch001246.htm#connect)[**Send and receive a file in FTP**](http://www.computerhope.com/issues/ch001246.htm#send)[**FTP commands**](http://www.computerhope.com/issues/ch001246.htm#command)

**Connect using FTP**

To connect to another computer using FTP at the MS-DOS prompt, command line, or Linux shell type **FTP** and press Enter. Once in FTP, use the **open** command to connect to the FTP server, as shown in the example below.

open ftp.example.com

In the above example, you'd substitute *example.com* for the [domain name](http://www.computerhope.com/jargon/d/domain.htm) or [IP address](http://www.computerhope.com/jargon/i/ip.htm) of where you are connecting. An example would be **open 192.168.1.12**.

Note: By default, the **open** command uses the TCP port 21 to make the FTP connection. If a different TCP port is needed for connecting to the domain name or IP address you are using, enter the port number after the domain name or IP address in the open command.

Once connected, a username and password prompt will appear. Once these credentials have been entered, the server allows you to browse, send, or receive files, depending on your rights. Some servers may also allow anonymous logins using *guest* or an e-mail address.

**Send and receive a file in FTP**

To get files from the server onto your own computer, use the get command as shown in the example below. In this example, you would get the file *myfile.htm*.

get myfile.htm

Tip: If you want to get more than one file, use mget and [wildcards](http://www.computerhope.com/jargon/w/wildcard.htm). For example, if you wanted to get all files that end with .htm, you could type **mget \*.htm**. Finally, if you do not want to be prompted as each file is being sent, make sure to type **prompt** to disable prompting.

To send a file from your computer to the computer you are connected to, assuming you have the rights, use the **send** command as shown in the example below. In this example, we are sending the myfile.htm to the [current directory](http://www.computerhope.com/jargon/c/currentd.htm).

send myfile.htm

It is important to realize that the files being sent must be in your local working directory, which is the directory you were in when you typed the FTP command. If you want to change to the directory that contains your files, use the **lcd** command. For example, in Windows, you'd type **lcd c:\windows** to set the local directory to the Windows directory.

**FTP Commands**

Depending upon the version of FTP and the operating system being used, each of the below commands may or may not work. Typing -help or a ? will list the commands available to you. Below is a general description of FTP commands available in the Windows command line FTP command.

* [Linux and Unix FTP command help and information.](http://www.computerhope.com/unix/ftp.htm)

|  |  |
| --- | --- |
| **Command** | **Information** |
| **!** | This command toggles back and forth between the operating system and ftp. Once back in the operating system, typing exit takes you back to the FTP command line. |
| **?** | Access the Help screen. |
| **append** | Append text to a local file. |
| **ascii** | Switch to [ASCII](http://www.computerhope.com/jargon/a/ascii.htm) transfer mode |
| **bell** | Turns bell mode on or off. |
| **binary** | Switches to binary transfer mode. |
| **bye** | Exits from FTP. |
| **cd** | Changes directory. |
| **close** | Exits from FTP. |
| **delete** | Deletes a file. |
| **debug** | Sets debugging on or off. |
| **dir** | Lists files if connected.  dir -C = Will list the files in wide format. dir -1 = Lists the files in bare format in alphabetic order dir -r = Lists directory in reverse alphabetic order. dir -R = Lists all files in current directory and sub directories. dir -S = Lists files in bare format in alphabetic order. |
| **disconnect** | Exits from FTP. |
| **get** | Grabs file from the computer to which you are connected. |
| **glob** | Sets globbing on or off. When turned off the file name in the put and get commands is taken literally and wildcards are not used. |
| **hash** | Sets hash mark printing on or off. When turned on for each 1024 bytes of data received a hash-mark (#) is displayed. |
| **help** | Access the Help screen and displays information about command if command typed after help. |
| **lcd** | Displays local directory if typed alone or if path typed after lcd will change local directory. |
| **literal** | Sends a literal command to the connected computer with an expected one line response. |
| **ls** | Lists files of the remotely connected computer. |
| **mdelete** | Multiple delete. |
| **mdir** | Lists contents of multiple remote directories. |
| **mget** | Get multiple files. |
| **mkdir** | Make directory. |
| **mls** | Lists contents of multiple remote directories. |
| **mput** | Sent multiple files |
| **open** | Opens address. |
| **prompt** | Enables or disables the prompt. |
| **put** | Send one file |
| **pwd** | Print working directory |
| **quit** | Exits from FTP. |
| **quote** | Same as the literal command. |
| **recv** | Receive file. |
| **remotehelp** | Get help from remote server. |
| **rename** | Renames a file. |
| **rmdir** | Removes a directory on the remote computer. |
| **send** | Send single file. |
| **status** | Shows status of currently enabled and disabled options |
| **trace** | Toggles packet tracing. |
| **Type** | Set file transfer type. |
| **user** | Send new user information. |
| **verbose** | Sets verbose on or off. |

**FTP**

|  |  |
| --- | --- |
| Note: | The parts of this text that are displayed in magenta are valid for Windows 2000 (and later) only |

* [Command Line Syntax](http://www.robvanderwoude.com/ftp.php#CommandLine)
* [FTP's Interactive Commands](http://www.robvanderwoude.com/ftp.php#InteractiveCommands)
* [Creating Unattended FTP Scripts](http://www.robvanderwoude.com/ftp.php#UnattendedFTP)
* [Summary](http://www.robvanderwoude.com/ftp.php#Summary)
* [Alternatives](http://www.robvanderwoude.com/ftp.php#Alternatives)
  + [WGET](http://www.robvanderwoude.com/ftp.php#WGET)
  + [WinSCP](http://www.robvanderwoude.com/ftp.php#WinSCP)
  + [Fileaze](http://www.robvanderwoude.com/ftp.php#Fileaze)
  + [VBScript](http://www.robvanderwoude.com/ftp.php#VBScript)

Looking through the FreeFind log files of my site, I noticed that (unattended) FTP scripts are a frequently returning subject.

On this page I will show some examples of unattended FTP download (or upload, the difference in script commands is small) scripts.

**Command Line Syntax**

|  |  |  |
| --- | --- | --- |
|  | FTP [-v] [-d] [-i] [-n] [-g] [-s:filename] [-a] [-w:windowsize] [host] | |
|  | where: | |
|  | -v | Suppresses display of remote server responses. |
|  | -n | Suppresses auto-login upon initial connection. |
|  | -i | Turns off interactive prompting during multiple file transfers. |
|  | -d | Enables debugging. |
|  | -g | Disables filename globbing (see GLOB command). |
|  | -s:filename | Specifies a text file containing FTP commands; the commands will automatically run after FTP starts. |
|  | -a | Use any local interface when binding data connection. |
|  | -A | Login as anonymous. |
|  | -w:buffersize | Overrides the default transfer buffer size of 4096. |
|  | host | Specifies the host name or IP address of the remote host to connect to. |

|  |  |  |
| --- | --- | --- |
| Notes: | (1) | mget and mput commands take y/n/q for yes/no/quit. |
|  | (2) | Use Control-C to abort commands. |

The **-s** switch is the most valuable switch for batch files that take care of unattended downloads and uploads:  
FTP -s:ftpscript.txt  
On some operating systems [redirection](http://www.robvanderwoude.com/redirection.php) may do the same:  
FTP < ftpscript.txt  
However, unlike the **-s** switch its proper functioning cannot be guaranteed.

**FTP's Interactive Commands**

The following table shows the FTP commands available in Windows NT 4. The difference with other operating systems is marginal.  
The actual commands available can be found by starting an FTP session and then typing a question mark at the FTP> prompt.  
To get a short description af a particular command, type a question mark followed by that command: (user input shown in bold italics):

|  |
| --- |
| C:\>***ftp*** ftp> ***? get*** get             receive file ftp> ***? mget*** mget            get multiple files ftp> ***bye***  C:\> |

| **FTP commands** | |
| --- | --- |
| **Command** | **Description** |
| ! | escape to the shell |
| ? | print local help information |
| append | append to a file |
| ascii | set ascii transfer type |
| bell | beep when command completed |
| binary | set binary transfer type |
| bye | terminate ftp session and exit |
| cd | change remote working directory |
| close | terminate ftp session |
| debug | toggle debugging mode |
| delete | delete remote file |
| dir | list contents of remote directory |
| disconnect | terminate ftp session |
| get | receive file |
| glob | toggle metacharacter expansion of local file names |
| hash | toggle printing `#' for each buffer transferred |
| help | print local help information |
| lcd | change local working directory |
| literal | send arbitrary ftp command |
| ls | nlist contents of remote directory |
| mdelete | delete multiple files |
| mdir | list contents of multiple remote directories |
| mget | get multiple files |
| mkdir | make directory on the remote machine |
| mls | nlist contents of multiple remote directories |
| mput | send multiple files |
| open | connect to remote tftp |
| prompt | force interactive prompting on multiple commands |
| put | send one file |
| pwd | print working directory on remote machine |
| quit | terminate ftp session and exit |
| quote | send arbitrary ftp command |
| recv | receive file |
| remotehelp | get help from remote server |
| rename | rename file |
| rmdir | remove directory on the remote machine |
| send | send one file |
| status | show current status |
| trace | toggle packet tracing |
| type | set file transfer type |
| user | send new user information |
| verbose | toggle verbose mode |

**Creating Unattended FTP Scripts**

Suppose an interactive FTP session looks like this (user input shown in bold italics):

|  |
| --- |
| C:\>***ftp ftp.myhost.net*** Connected to ftp.myhost.net. 220 \*\*\* FTP SERVER IS READY \*\*\* User (ftp.myhost.net:(none)): ***MyUserId*** 331 Password required for MyUserId. Password: ***\*\*\*\**** 230- Welcome to the FTP site 230- Available space: 8 MB 230 User MyUserId logged in. ftp> ***cd files/pictures*** 250 CWD command successful. "files/pictures" is current directory. ftp> ***binary*** 200 Type set to B. ftp> ***prompt n*** Interactive mode Off. ftp> ***mget \*.\**** 200 Type set to B. 200 Port command successful. 150 Opening data connection for firstfile.jpg. 226 File sent ok 649 bytes received in 0.00 seconds (649000.00 Kbytes/sec) 200 Port command successful. 150 Opening data connection for secondfile.gif. 226 File sent ok 467 bytes received in 0.00 seconds (467000.00 Kbytes/sec) ftp> ***bye*** 221 Goodbye.  C:\> |

An FTP script for unattended file transfer would then look like this:

USER MyUserId

MyPassword

cd files/pictures

binary

prompt n

mget \*.\*

Note that I left out the BYE (or QUIT) command, it isn't necessary to specify this command in unattended FTP scripts (though it doesn't do any harm either).

As you can see, using a script like this is a potential security risk: the password is stored in the script in a readable form.

As [Tom Lavedas](http://replay.waybackmachine.org/20081016011937/http:/members.cox.net/tglbatch/) once pointed out in the [alt.msdos.batch](http://groups.google.com/group/alt.msdos.batch/topics) newsgroup, it is safer to create the script "on the fly" and delete it afterwards:

@ECHO OFF

:: Check if the password was given

IF "%1"=="" GOTO Syntax

:: Create the temporary script file

> script.ftp ECHO USER MyUserId

>>script.ftp ECHO %1

>>script.ftp ECHO cd files/pictures

>>script.ftp ECHO binary

>>script.ftp ECHO prompt n

>>script.ftp ECHO mget \*.\*

:: Use the temporary script for unattended FTP

:: Note: depending on your OS version you may have to add a '-n' switch

FTP -v -s:script.ftp ftp.myhost.net

:: For the paranoid: overwrite the temporary file before deleting it

TYPE NUL >script.ftp

DEL script.ftp

GOTO End

:Syntax

ECHO Usage: %0 password

:End

Sometimes it may be necessary to make the script completely unattended, without the user having to know the password, or even the user ID, but with the possibility to check for errors during transfer.  
There are several ways to do this.  
One is to [redirect](http://www.robvanderwoude.com/redirection.php) FTP's output to a log file and either display it to the user or use [FIND](http://www.robvanderwoude.com/find.php) to search the log file for any error messages.  
Another way to do this, on the fly, is by displaying FTP's output on screen, in the mean time using [FIND](http://www.robvanderwoude.com/find.php) /V to hide the output you do not want the user to see (like the password and maybe even the USER command):

FTP -s:script.ftp ftp.myhost.net | FIND /V "USER" | FIND /V "%1"

It is important ***not*** to use FTP's **-v** switch in either case.

**Summary**

To create a semi interactive FTP script, you may need to split it into several smaller parts, like an unattended FTP script to read a list of remote files, the output of which is redirected to a temporary file, which in turn is used by a batch file to create a new unattended FTP script on the fly to download and/or delete some of these files.

Create these files by writing down *every* command and *all* screen output in an interactive FTP session, analyze this "log" thoroughly, and *test, test, and test again!*

And don't forget to log the results by redirecting the script's output to a log file. You may need it later for debugging purposes...

**Alternatives**

Instead of Windows' own native FTP command, you can choose from a multitude of "third party" alternatives.  
I'll discuss three of those alternatives here: a command-line tool, a GUI-tool and VBScript with a third party ActiveX component.

|  |  |
| --- | --- |
| Note: | The alternatives discussed here, [GNU WGET](http://www.gnu.org/software/wget/), [Fileaze](http://www.robvanderwoude.com/fileazeftp.php), and VBScript (with [WinHTTP](http://msdn.microsoft.com/en-us/library/aa382925%28VS.85%29.aspx)), handle HTTP downloads just as easily. |

**WGET**

WGET is a port of the UNIX wget command.

WGET is perfect for anonymous FTP or HTTP *downloads* (sorry, no uploads), but it can be used for downloads requiring authentication too.

[GNU WGET](http://www.gnu.org/software/wget/) comes with help both in the (text mode) console and in Windows Help format.

The basic syntax for an FTP download doesn't get any simpler than this:

WGET ftp://ftp.mydomain.com/path/file.ext

for anonymous downloads, or:

WGET ftp://user:password@ftp.mydomain.com/path/file.ext

when authentication is required.

|  |  |
| --- | --- |
| Note: | This is *not* secure, as you would need to store your user ID and password in unencrypted format in the batch file. Besides that, the user ID and password will be logged together with the rest of the URL on all servers associated with the file transfer. Read the GNU WGET help file for more information on securing user IDs and passwords. |

**WinSCP**

[WinSCP](http://winscp.net/eng/docs/introduction) is a free open-source SFTP and FTP client with a command line/[scripting interface](http://winscp.net/eng/docs/script_commands) as well as a GUI.

WinSCP can be used for uploads and downloads.

**Fileaze**

Prefer a GUI to create interactive as well as unattended jobs?

To be honest, I hardly ever use the text mode native FTP command myself.

For these web pages, my photographs, or any other FTP job, I have always used Coffeecup FreeFTP (no longer available, unfortunately).

Recently, I automated my own web page uploads using [Fileaze](http://www.robvanderwoude.com/fileazeftp.php).

Fileaze is a great GUI program to automate file related tasks like rename, copy, upload and download, send by e-mail, etcetera, in batch (no, not in batch *files* but in batch *mode*, i.e. in groups of files, and unattended).

Have a look at the [tutorial](http://www.robvanderwoude.com/fileazeftp.php) I wrote, based on my own "efforts" to generate an [automated FTP upload job](http://www.robvanderwoude.com/fileazeftp.php).

And did I mention the uploads are *fast*?

You can download the [free Fileaze trial version](http://hotdownloads.com/trialware/download/Download_FileazeSetup1.0Trial.exe?item=15038-1&affiliate=72212) or [buy it here](http://www.regnow.com/softsell/nph-softsell.cgi?item=15038-1&affiliate=72212).  
You can also download the free Fileaze LITE version from the [Fileaze website](http://www.robvanderwoude.com/fileazeftp.php). The LITE version may be used indefinitely, without limitations, but it has limited functionality (i.e. no FTP and no e-mail).

Make sure you read the tutorials included in the help file.  
The program may not be that hard to learn without help, but speaking from experience: reading them *will* save you a lot of time.

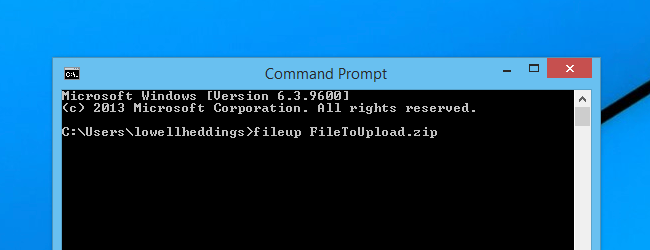
And once you created one or more jobs, make sure you make a backup.  
Fileaze stores the data (jobs, encrypted account settings, etcetera) in the registry key "HKEY\_CURRENT\_USER\Software\Resolware".  
The registry as a whole is included in Windows's SystemState backups, but it doesn't support selectively restoring registry keys.  
So (of course) I made myself a batch file which I scheduled, to make unattended backups. [View this batch file's source](http://www.robvanderwoude.com/files/fileazebackup_nt.txt), or [download the ZIPped batch file](http://www.robvanderwoude.com/files/feazbkup.zip) (for Windows NT 4 and later).

**VBScript**

In my [VBScript Scripting Techniques](http://www.robvanderwoude.com/vbstech.php) section, sample scripts are available for [FTP](http://www.robvanderwoude.com/vbstech_internet_ftp.php) and [HTTP](http://www.robvanderwoude.com/vbstech_internet_download.php) file transfers.  
The FTP scripts require one of these free ActiveX components:

* [Chilkat FTP ActiveX](http://www.robvanderwoude.com/vbsaddons.php#ChilkatFTP)
* [Sapien FTP Automation Component](http://www.robvanderwoude.com/vbsaddons.php#SapienFTP)

## [How to Automate FTP Uploads from the Windows Command Line](http://www.howtogeek.com/howto/windows/how-to-automate-ftp-uploads-from-the-windows-command-line/)



Windows has included batch files since before it existed… batch files are really old! Old or not, I still find myself frequently creating batch files to help me automate common tasks. One common task is uploading files to a remote FTP server. Here’s the way that I got around it.

First, you will have to create a file called fileup.bat in your windows directory, or at least inside some directory included in your path. You can use the “path” command to see what the current path is.

Inside the batch file, you will want to paste the following:

@echo off  
echo user MyUserName> ftpcmd.dat  
echo MyPassword>> ftpcmd.dat  
echo bin>> ftpcmd.dat  
echo put %1>> ftpcmd.dat  
echo quit>> ftpcmd.dat  
ftp -n -s:ftpcmd.dat SERVERNAME.COM  
del ftpcmd.dat

You will want to replace the MyUserName, MyPassword and SERVERNAME.COM with the correct values for your ftp server. What this batch file is doing is scripting the ftp utility using the -s option for the command line utility.

The batch file uses the “echo” command to send text to the ftp server as if you had typed it. In the middle of the file you can add extra commands, potentionally a change directory command:

echo cd /pathname/>>ftpcmd.dat

In order to call this batch file, you will call the batchfile using the fileup.bat name that we gave it, and pass in the name of a file as the parameter. You don’t have to type the .bat part of the filename to make it work, either.

Example:

> fileup FileToUpload.zip

Connected to [ftp.myserver.com](ftp://ftp.myserver.com).  
220 Microsoft FTP Service  
ftp> user myusername  
331 Password required for myusername.

230 User myusername logged in.  
ftp> bin  
200 Type set to I.  
ftp> put FileToUpload.zip  
200 PORT command successful.  
150 Opening BINARY mode data connection for FileToUpload.zip  
226 Transfer complete.  
ftp: 106 bytes sent in 0.01Seconds 7.07Kbytes/sec.  
ftp> quit

And that’s all there is to it. Now your file should be sitting on the remote server.

## 3. Beginner's guide to using ftp

**A quick guide to using ftp.**

The standard ftp program is the original ftp client. It comes standard with most Linux distributions. It first appeared in 4.2BSD, which was developed by the University of California, Berkeley.

## 3.1 Running the ftp program

It's easy to use ftp. Let's say you want to connect to the anonymous ftp site metalab.unc.edu, to download the latest Linux kernel source.

At the command line, type:

$ ftp metalab.unc.edu

The ftp program will attempt to connect to metalab.unc.edu. Another way to do this is to run ftp from the command line with no parameters, and use the open command, with the site name as an argument:

$ ftp

ftp> open metalab.unc.edu

## 3.2 Logging into an FTP server

When you connect to an FTP site, it will ask you for a login (pressing enter will log in as your local user name, in this case, foo: We log in as anonymous or ftp, to get to the public archive.

220 helios.oit.unc.edu FTP server (Version wu-2.6.0(2) Wed Nov 17 14:44:12

EST 1999) ready.

Name (metalab.unc.edu:foo):

Now, we enter a complete e-mail address as the password (this is what most public FTP sites request).

331 Guest login ok, send your complete e-mail address as password.

Password:

After a successful login, the following information is given to us:

Remote system type is UNIX.

Using binary mode to transfer files.

ftp>

## 3.3 File transfer types

After you log in to an ftp site, ftp will print out the file transfer type. In our case, it is binary. Binary mode transfers the files, bit by bit, as they are on the FTP server. Ascii mode, however, will download the text directly. You can type ascii or binary to switch between the types.

You want to download the kernel source, so you leave the file transfer type at binary. The binary type is also what you would use for any non-text files -- such as graphic images, zip/gzip archives, executable programs, etc. If in doubt, use binary mode.

## 3.4 Navigating and listing directories

You do an ls to see a list of the files. The ls command on ftp servers is executed on the remote server, so the command line options that you can use with it vary from server to server. The most common options are generally available, check the manpage for ls for details.

ftp> ls

200 PORT command successful.

150 Opening ASCII mode data connection for /bin/ls.

total 33590

-r--r--r-- 1 root other 34348506 Dec 03 03:53 IAFA-LISTINGS

lrwxrwxrwx 1 root other 7 Jul 15 1997 README -> WELCOME

-rw-r--r-- 1 root other 890 Nov 15 13:11 WELCOME

dr-xr-xr-x 2 root other 512 Jul 15 1997 bin

dr-xr-xr-x 2 root other 512 Jul 15 1997 dev

dr-xr-xr-x 2 root other 512 Jul 18 1997 etc

drwxrwxrwx 11 ftp 20 4608 Nov 28 16:00 incoming

lrwxrwxrwx 1 root other 13 Jun 04 1998 ls-lR -> IAFA-LISTINGS

dr-xr-xr-x 17 root root 512 Jun 08 11:43 pub

dr-xr-xr-x 3 root other 512 Jul 15 1997 unc

dr-xr-xr-x 5 root other 512 Jul 15 1997 usr

226 Transfer complete.

If the ls command lists so many files that they scroll off the top of the screen, you can use Shift-PageUp to scroll up. This works in Linux console mode as well as in xterm or rxvt.

On public FTP archives, the downloadable resources are usually held in the /pub directory. In this example, you already know that the kernel sources are in the directory /pub/Linux/kernel, so you type the following to get into that directory:

ftp> cd pub/Linux/kernel

250-README for kernel

250-

250-What you'll find here: kernel sources and patches

250-

250-

250 CWD command successful.

The messages you see, which begin with "250", are information messages sent by the server. In this case, the ftp server is configured to automatically send you the README file when you cd into the directory.

## 3.5 Downloading and uploading files

Now, after doing another ls, you see that you want to cd into the v2.2 directory. You do yet another ls, and find the file you want to download. It is linux-2.2.13.tar.gz. So you type this:

ftp> get linux-2.2.13.tar.gz

local: linux-2.2.13.tar.gz remote: linux-2.2.13.tar.gz

200 PORT command successful.

150 Opening BINARY mode data connection for linux-2.2.13.tar.gz (15079540

bytes).

The ftp program has started saving the remote file linux-2.2.13.tar.gz as the local file linux-2.2.13.tar.gz.

If you wanted to save it as the local file foo.tar.gz, you could have specified it like this:

ftp> get linux-2.2.13.tar.gz foo.tar.gz

local: foo.tar.gz remote: linux-2.2.13.tar.gz

200 PORT command successful.

150 Opening BINARY mode data connection for linux-2.2.13.tar.gz (15079540

bytes).

If you want to download more than one file at a time, you'll have to use the mget (multiple get) command. You can use mget together with a space-delimited list of filenames you want to download, or you can use wildcards with the mget command. For example:

ftp> mget linux\*

Would get all files starting with the string "linux". Normally, mget will prompt you for each file before it downloads it. You can toggle this by using the prompt command.

Now let's say you've written a piece of software, and you want to upload it to MetaLab to be included in their Linux software archive. First, you'd change to the /incoming directory (most public FTP servers have a directory, usually called incoming or uploads, where files can be uploaded), then you'd use the put command:

ftp> cd /incoming

ftp> put foo.tar.gz

local: foo.tar.gz remote: foo.tar.gz

200 PORT command successful.

150 Opening BINARY mode data connection for foo.tar.gz.

226 Transfer complete.

10257 bytes sent in 0.00316 secs (3.2e+03 Kbytes/sec)

The put command works the same way as the get command, so you can use mput to upload multiple files at the same time. You can also upload a local file with a different filename on the server by specifying the remote filename and/or pathname as an argument.

What if the file foo.tar.gz is not in your current local directory when you try to upload it? You can switch local directories by using the lcd (local change directory) command:

ftp> lcd /home/foo/

Local directory now /home/foo

## 3.6 Running shell commands

The ftp client supports using the bang (!) to run local commands. For example, to get a listing of files in your current local directory, do this:

ftp> !ls

The way this works is that ftp calls the shell (specified in the $SHELL environment variable), and it is the shell which runs ls. Thus, you can run any command-line which works with your shell simply by prepending "!" to it (the default shell in most Linux distributions is bash, the Bourne Again SHell). Please note that !cd does not work as you would expect, this is why the lcd command exists.

## 3.7 Hash marks and tick

Wouldn't it be nice if you could watch the progress while you're downloading a file with ftp? You can use the hash command to print out hash marks as you download a file:

ftp> hash

Hash mark printing on (1024 bytes/hash mark).

As you can tell, ftp will print a hash mark for every 1024 bytes of data you download.

There is also a tick option.

ftp> tick

Tick counter printing on (10240 bytes/tick increment).

This will print something to this effect as you download a file:

Bytes transferred: 11680

## 3.8 Other ftp commands

There are many other ftp commands. If you have the permissions to do so (which you should, if you are connected to your own private shell account), you can make a directory on the remote server using the mkdir command. You can remove a file on the remote server using the delete command, or rmdir to remove a directory. You can also change file permissions using the chmod command.

For more elaborate information on using ftp, please see the online help in the ftp program (accessible by typing help with no arguments for a list of commands, or help <commandname> for specific help on a command). You can also read the Unix man page for ftp by typing man ftp at your command prompt.

**Example syntax for Secure Copy (scp)**

**What is Secure Copy?**

**scp** allows files to be copied to, from, or between different hosts. It uses **ssh** for data transfer and provides the same authentication and same level of security as **ssh**.

**Examples**

**Copy the file "foobar.txt" from a remote host to the local host**

|  |
| --- |
| $ scp your\_username@remotehost.edu:foobar.txt /some/local/directory |

**Copy the file "foobar.txt" from the local host to a remote host**

|  |
| --- |
| $ scp foobar.txt your\_username@remotehost.edu:/some/remote/directory |

**Copy the directory "foo" from the local host to a remote host's directory "bar"**

|  |
| --- |
| $ scp -r foo your\_username@remotehost.edu:/some/remote/directory/bar |

**Copy the file "foobar.txt" from remote host "rh1.edu" to remote host "rh2.edu"**

|  |
| --- |
| $ scp your\_username@rh1.edu:/some/remote/directory/foobar.txt \ your\_username@rh2.edu:/some/remote/directory/ |

**Copying the files "foo.txt" and "bar.txt" from the local host to your home directory on the remote host**

|  |
| --- |
| $ scp foo.txt bar.txt your\_username@remotehost.edu:~ |

**Copy the file "foobar.txt" from the local host to a remote host using port 2264**

|  |
| --- |
| $ scp -P 2264 foobar.txt your\_username@remotehost.edu:/some/remote/directory |

**Copy multiple files from the remote host to your current directory on the local host**

|  |
| --- |
| $ scp your\_username@remotehost.edu:/some/remote/directory/\{a,b,c\} . |

|  |
| --- |
| $ scp your\_username@remotehost.edu:~/\{foo.txt,bar.txt\} . |

**scp Performance**

By default **scp** uses the Triple-DES cipher to encrypt the data being sent. Using the Blowfish cipher has been shown to increase speed. This can be done by using option *-c blowfish* in the command line.

|  |
| --- |
| $ scp -c blowfish some\_file your\_username@remotehost.edu:~ |

It is often suggested that the *-C* option for compression should also be used to increase speed. The effect of compression, however, will only significantly increase speed if your connection is very slow. Otherwise it may just be adding extra burden to the CPU. An example of using blowfish and compression:

|  |
| --- |
| $ scp -c blowfish -C local\_file your\_username@remotehost.edu:~ |

**Contributions**

Thanks **Stewart Macleod** for port example.

**How To Use awk In Bash Scripting**

by Vivek Gite on August 15, 2009 *last updated* August 14, 2009

in [BASH Shell](http://www.cyberciti.biz/faq/category/bash-shell/), [CentOS](http://www.cyberciti.biz/faq/category/centos/), [Debian / Ubuntu](http://www.cyberciti.biz/faq/category/debian-ubuntu/), [FAQ](http://www.cyberciti.biz/faq/category/faq/), [FreeBSD](http://www.cyberciti.biz/faq/category/freebsd/), [Linux](http://www.cyberciti.biz/faq/category/linux/), [RedHat and Friends](http://www.cyberciti.biz/faq/category/redhat-and-friends/), [Suse](http://www.cyberciti.biz/faq/category/suse/), [Ubuntu Linux](http://www.cyberciti.biz/faq/category/ubuntu-linux/), [UNIX](http://www.cyberciti.biz/faq/category/unix/)

[](http://www.cyberciti.biz/faq/category/bash-shell/)

How do I use awk pattern scanning and processing language under bash scripts? Can you provide a few examples?  
  
Awk is an excellent tool for building UNIX/Linux shell scripts. AWK is a programming language that is designed for processing text-based data, either in files or data streams, or using shell pipes. In other words you can combine awk with shell scripts or directly use at a shell prompt.

**Print a Text File**

awk '{ print }' /etc/passwd  
OR  
awk '{ print $0 }' /etc/passwd

**Print Specific Field**

Use : as the input field separator and print first field only i.e. usernames (will print the the first field. all other fields are ignored):  
awk -F':' '{ print $1 }' /etc/passwd  
Send output to sort command using a shell pipe:  
awk -F':' '{ print $1 }' /etc/passwd | sort

**Pattern Matching**

You can only print line of the file if pattern matched. For e.g. display all lines from Apache log file if HTTP error code is 500 (9th field logs status error code for each http request):  
awk '$9 == 500 { print $0}' /var/log/httpd/access.log  
The part outside the curly braces is called the “pattern”, and the part inside is the “action”. The comparison operators include the ones from C:

== != < > <= >= ?:

If no pattern is given, then the action applies to all lines. If no action is given, then the entire line is printed. If “print” is used all by itself, the entire line is printed. Thus, the following are equivalent:  
awk '$9 == 500 ' /var/log/httpd/access.log  
awk '$9 == 500 {print} ' /var/log/httpd/access.log  
awk '$9 == 500 {print $0} ' /var/log/httpd/access.log

**Print Lines Containing tom, jerry AND vivek**

Print pattern possibly on separate lines:  
awk '/tom|jerry|vivek/' /etc/passwd

**Print 1st Line From File**

awk "NR==1{print;exit}" /etc/resolv.conf  
awk "NR==$line{print;exit}" /etc/resolv.conf

**Simply Arithmetic**

You get the sum of all the numbers in a column:  
awk '{total += $1} END {print total}' earnings.txt  
Shell cannot calculate with floating point numbers, but awk can:  
awk 'BEGIN {printf "%.3f\n", 2005.50 / 3}'

**Call AWK From Shell Script**

A shell script to list all IP addresses that accessing your website. This script use awk for processing log file and verification is done using shell script commands.

|  |
| --- |
| *#!/bin/bash*  d=$1  OUT=**/**tmp**/**spam.ip.$$  HTTPDLOG="/www/$d/var/log/httpd/access.log"  **[** $# -eq 0 **]** **&&** **{** **echo** "Usage: $0 domain-name"; **exit** 999; **}**  **if** **[** -f $HTTPDLOG **]**;  **then**  **awk** '{print}' $HTTPDLOG **>**$OUT  **awk** '{ print $1}' $OUT **|** **sort** -n **|** **uniq** -c **|** **sort** -n  **else**  **echo** "$HTTPDLOG not found. Make sure domain exists and setup correctly."  **fi**  **/**bin**/rm** -f $OUT |

**AWK and Shell Functions**

Here is another example. chrootCpSupportFiles() find out the shared libraries required by each program (such as perl / php-cgi) or shared library specified on the command line and copy them to destination. This code calls awk to print selected fields from the ldd output:

|  |
| --- |
| chrootCpSupportFiles**()** **{**  *# Set CHROOT directory name*  **local** BASE="$1" *# JAIL ROOT*  **local** pFILE="$2" *# copy bin file libs*    **[** **!** -d $BASE **]** **&&** **mkdir** -p $BASE **||** :    FILES="$(ldd $pFILE | awk '{ print $3 }' |egrep -v ^'\(')"  **for** i **in** $FILES  **do**  dcc="$(dirname $i)"  **[** **!** -d $BASE$dcc **]** **&&** **mkdir** -p $BASE$dcc **||** :  **/**bin**/cp** $i $BASE$dcc  **done**    sldl="$(ldd $pFILE | grep 'ld-linux' | awk '{ print $1}')"  sldlsubdir="$(dirname $sldl)"  **if** **[** **!** -f $BASE$sldl **]**;  **then**  **/**bin**/cp** $sldl $BASE$sldlsubdir  **else**  :  **fi**  **}** |

This function can be called as follows:  
chrootCpSupportFiles /lighttpd-jail /usr/local/bin/php-cgi

**AWK and Shell Pipes**

List your top 10 favorite commands:  
history | awk '{print $2}' | sort | uniq -c | sort -rn | head  
Sample Output:

172 ls

144 cd

69 vi

62 grep

41 dsu

36 yum

29 tail

28 netstat

21 mysql

20 cat

whois cyberciti.com | awk ‘/Domain Expiration Date:/ { print $6″-“$5”-“$9 }’

**Awk Program File**

You can put all awk commands in a file and call the same from a shell script using the following syntax:  
awk -f mypgoram.awk input.txt

**Awk in Shell Scripts – Passing Shell Variables TO Awk**

You can pass shell variables to awk using the -v option:

|  |
| --- |
| n1=5  n2=10  **echo** **|** **awk** -v x=$n1 -v y=$n2 -f program.awk |

Assign the value n1 to the variable x, before execution of the program begins. Such variable values are available to the BEGIN block of an AWK program:

|  |
| --- |
| BEGIN**{**ans=x+y**}**  **{**print ans**}**  END**{}** |

**HowTo: Read a File Line By Line Using awk**

by Vivek Gite on February 21, 2007 *last updated* October 1, 2011

in [BASH Shell](http://www.cyberciti.biz/faq/category/bash-shell/), [Debian / Ubuntu](http://www.cyberciti.biz/faq/category/debian-ubuntu/), [FreeBSD](http://www.cyberciti.biz/faq/category/freebsd/), [HP-UX Unix](http://www.cyberciti.biz/faq/category/hp-ux-unix/), [Linux](http://www.cyberciti.biz/faq/category/linux/), [Openbsd](http://www.cyberciti.biz/faq/category/openbsd/), [RedHat and Friends](http://www.cyberciti.biz/faq/category/redhat-and-friends/), [Solaris-Unix](http://www.cyberciti.biz/faq/category/solaris-unix/), [Suse](http://www.cyberciti.biz/faq/category/suse/), [UNIX](http://www.cyberciti.biz/faq/category/unix/)

[](http://www.cyberciti.biz/faq/category/bash-shell/)

How do I read a file line by line using awk utility under Unix / Linux operating systems?  
  
awk is pattern scanning and text processing language. It is useful for manipulation of data files, text retrieval and processing, and for prototyping and experimenting with algorithms. The name AWK is derived from the surnames of its authors — Alfred Aho, Peter Weinberger, and Brian Kernighan.

By default it process one line at a time. For example following command will simply process one line at a time:  
$ cat /etc/passwd | awk '{ print $0}'  
Or better try  
$ awk '{ print $0}' /etc/passwd

The **print** command is used to output text. $0 is field name for entire line. By default white space (blank line) act as field separator. You can set new field separator with -F option. For example, to use : as a field separator, enter:  
$ awk -F':' '{ print $1 }' /etc/passwd

Above command will print all username using the first field ($1) for current line. You can print username ($1), shell ($7) and login home dir ($6) report as follows:  
$ awk -F':' '{ print "User " $1 " login using " $7 " shell with as " $6 " home dir"}' /etc/passwd  
Output:

User root login using /bin/bash shell with as /root home dir

User daemon login using /bin/sh shell with as /usr/sbin home dir

User bin login using /bin/sh shell with as /bin home dir

User sys login using /bin/sh shell with as /dev home dir

....

....

User gdm login using /bin/false shell with as /var/lib/gdm home dir

User vivek login using /bin/bash shell with as /home/vivek home dir

User sshd login using /usr/sbin/nologin shell with as /var/run/sshd home dir

**Linux / Unix: Awk Print Variable**

by Vivek Gite on January 15, 2011 *last updated* February 15, 2013

in [UNIX](http://www.cyberciti.biz/faq/category/unix/)

[](http://www.cyberciti.biz/faq/category/unix/)

How do I print variables using Awk interpreted programming language under Linux or Unix like operating systems?  
  
  
Awk pattern scanning and processing language. It is small, fast, and simple. It has a clean syntax and most useful for text processing. awk has built-in variables that are automatically set. For example, $0 variable holds the entire current input line. In this example, print hello world using awk:

|  |
| --- |
| **echo** 'Hello world' **|** **awk** '{ print $0 }' |

Sample outputs:

Hello world

In this following example, pass two values to awk to print addition:

|  |
| --- |
| **echo** 3 4 **|** **awk** '{ print $1 + $2 }' |

Sample outputs:

7

To print third word from input, enter:

|  |
| --- |
| **echo** This is a **test** **|awk** '{print $3}' |

Sample outputs:

a

**Printing a text file**

Create a file called foo.txt:  
$ cat foo.txt  
Sample outputs:

Holding on to anger is like grasping a hot coal with the intent of throwing it at someone else; you are the one who gets burned.

In a controversy the instant we feel anger we have already ceased striving for the truth, and have begun striving for ourselves.

To print the entire file line by line, enter:

|  |
| --- |
| **awk** '{ print }' foo.txt |

OR

|  |
| --- |
| **awk** '{ print $0 }' foo.txt |

**awk define and print variable**

Create a variable called x and y:

|  |
| --- |
| **awk** 'BEGIN{x=3; y=4;}END{ print "x=" x " and y=" y}'**</**dev**/**null |

To print total of x and y, enter:

|  |
| --- |
| **echo|awk** 'BEGIN{x=3; y=4; total=0}{ total= x+y}END{ print x " + " y " = " total }' |

Sample outputs:

7

**Say hello to printf**

To format and print use a printf statement. The printf works like c printf.

|  |
| --- |
| **echo** Total 5000.5686 **|** **awk** '{ printf "%s $%.2f\n", $1, $2 }' |

Sample outputs:

Total $5000.57

See awk man page for more details:  
$ man awk

**Linux / Unix: Sed / Grep / Awk Print Lines If It Got 3 Words Only**

by Vivek Gite on November 9, 2012 *last updated* November 9, 2012

in [BASH Shell](http://www.cyberciti.biz/faq/category/bash-shell/)

[](http://www.cyberciti.biz/faq/category/bash-shell/)

I have a sample data file:

This is a test.  
Unix is Best.  
No Linux is the Best.  
Space in simple understanding is an area or volume.  
Outer space .  
  
I need the output:  
  
Unix is Best.  
Outer space .  
  
  
How do I print all lines that have three (3) words only?

The awk command is well suitable for this kind of pattern processing text file. Awk set the variable called NF. It is set to the total number of fields in the input record. So if NF equal to three print the line. The syntax is as follows:

|  |
| --- |
| **awk** '{ if ( NF == 3 ) print } ' **/**path**/**to**/**input |

It is also possible to emulate awk command output using a [shell script while loop](http://www.cyberciti.biz/faq/bash-while-loop/) and [IFS (internal field separator) in loops](http://www.cyberciti.biz/faq/unix-linux-bash-while-read-function-define-ifs-delimiter/):

|  |
| --- |
| *#!/bin/bash*  *# AWK NF if condition (awk '{ if ( NF == 3 ) print } ' $\_input) emulation using bash*  *# Author: nixCraft <www.cyberciti.biz>*  *# -----------------------------------------------------------------------------------*  \_input="/path/to/data.txt"  \_word=3  **while** IFS= **read** -r line  **do**  **set** -- $line  **[** $# -eq $\_word **]** **&&** **echo** "$line"  **done** **<** "$\_input" |

Sample outputs:

Unix is Best.

Outer space .

**Linux / Unix: Sed / Grep / Awk Print Lines If It Got 3 Words Only**

by Vivek Gite on November 9, 2012 *last updated* November 9, 2012

in [BASH Shell](http://www.cyberciti.biz/faq/category/bash-shell/)

[](http://www.cyberciti.biz/faq/category/bash-shell/)

I have a sample data file:

This is a test.  
Unix is Best.  
No Linux is the Best.  
Space in simple understanding is an area or volume.  
Outer space .  
  
I need the output:  
  
Unix is Best.  
Outer space .  
  
  
How do I print all lines that have three (3) words only?

The awk command is well suitable for this kind of pattern processing text file. Awk set the variable called NF. It is set to the total number of fields in the input record. So if NF equal to three print the line. The syntax is as follows:

|  |
| --- |
| **awk** '{ if ( NF == 3 ) print } ' **/**path**/**to**/**input |

It is also possible to emulate awk command output using a [shell script while loop](http://www.cyberciti.biz/faq/bash-while-loop/) and [IFS (internal field separator) in loops](http://www.cyberciti.biz/faq/unix-linux-bash-while-read-function-define-ifs-delimiter/):

|  |
| --- |
| *#!/bin/bash*  *# AWK NF if condition (awk '{ if ( NF == 3 ) print } ' $\_input) emulation using bash*  *# Author: nixCraft <www.cyberciti.biz>*  *# -----------------------------------------------------------------------------------*  \_input="/path/to/data.txt"  \_word=3  **while** IFS= **read** -r line  **do**  **set** -- $line  **[** $# -eq $\_word **]** **&&** **echo** "$line"  **done** **<** "$\_input" |

Sample outputs:

Unix is Best.

Outer space .

http://www.cyberciti.biz/faq/bash-scripting-using-awk/