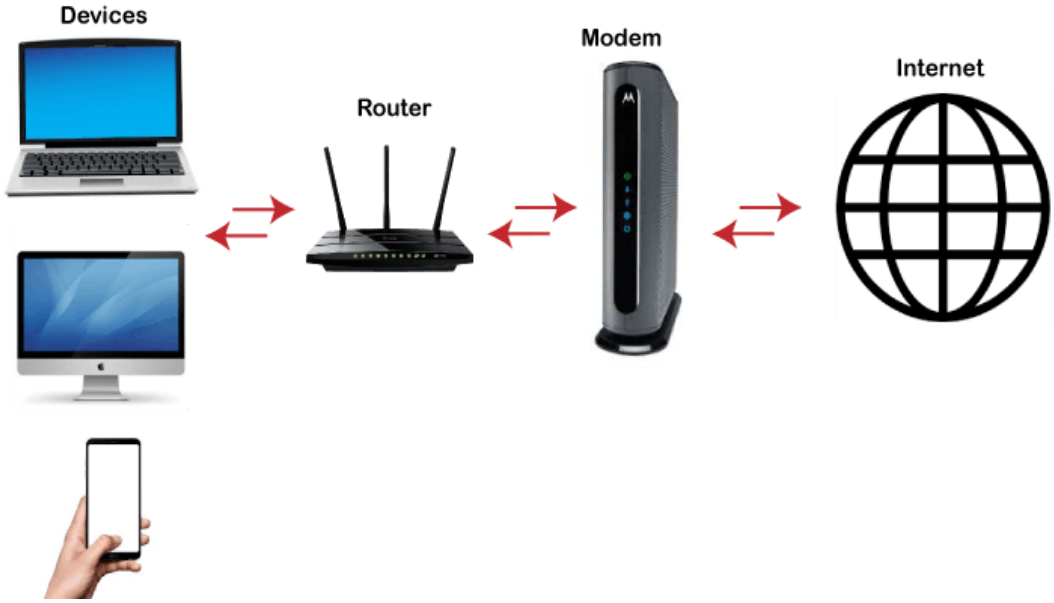
Name: Atish Kumar
Roll No: 120CS0173
Date: 12 Jan,2023

1. **Study about functionality of intermediate devices used inInternet and compare it.**

Network Devices: Network devices are physical devices that allow hardware on a computer network to communicate and interact with one another. example Repeater, Hub, Bridge, Switch, Routers, Gatewayetc.

Modem: Any electronic devices that convert digital data signals into modulated analog signals suitable for transmission over analog telecommunications circuits. By converting the data into a signal, it becomes incredibly easier to send the information over a wifi connection, phone line, etc. In the olden days, you could connect to the internet by using the telephone line.



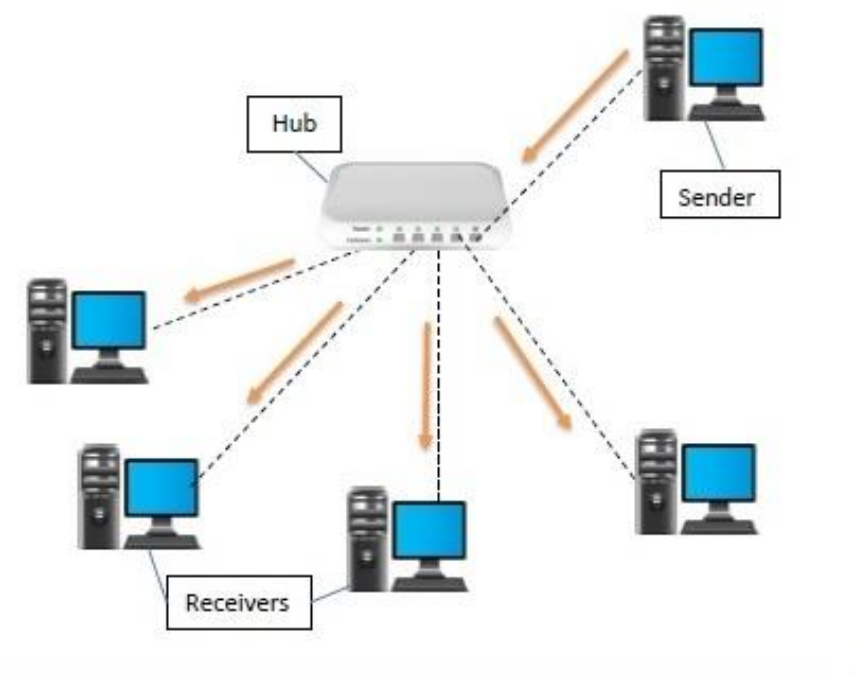
Hub: Hub is a node that broadcasts data to every computer or Ethernet-based deviceconnected to it. A hub is less sophisticated than a switch, the latter of which can isolate data transmissions to specific devices. Network hubs are best suited for small, simple local area network (LAN) environments.

Types of hub:

Active Hub:- These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center.

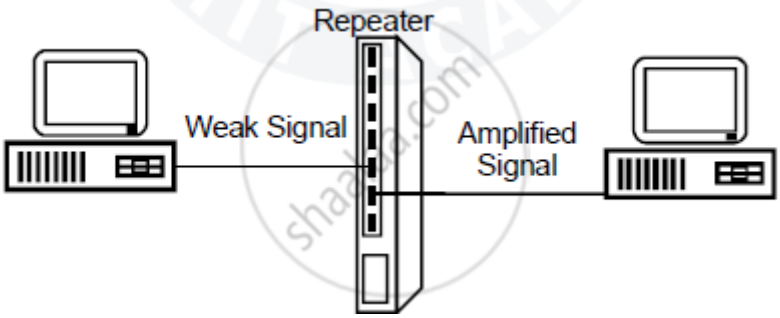
Passive Hub:- These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.

Intelligent Hub:- It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices.



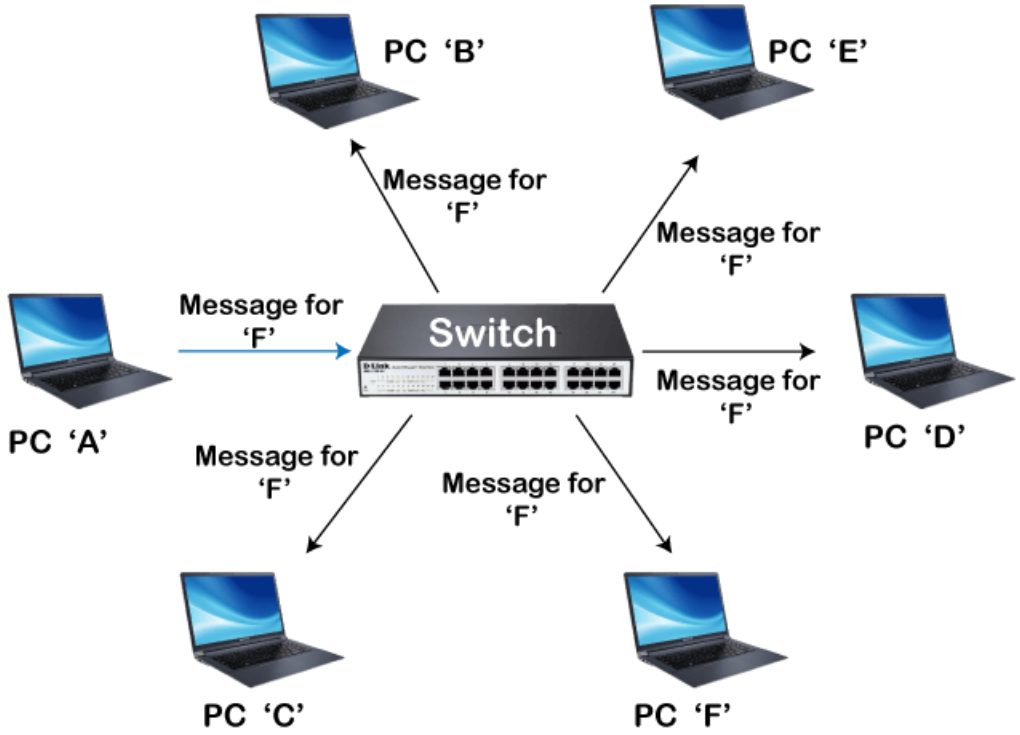
Repeater: A dynamic network device used to reproduce the signals when theytransmit over a greater distance so that the signal's strength remains equal.

- It can be used to create an Ethernet network.
- A repeater that occurs as the first layer of the OSI layer is the physical layer



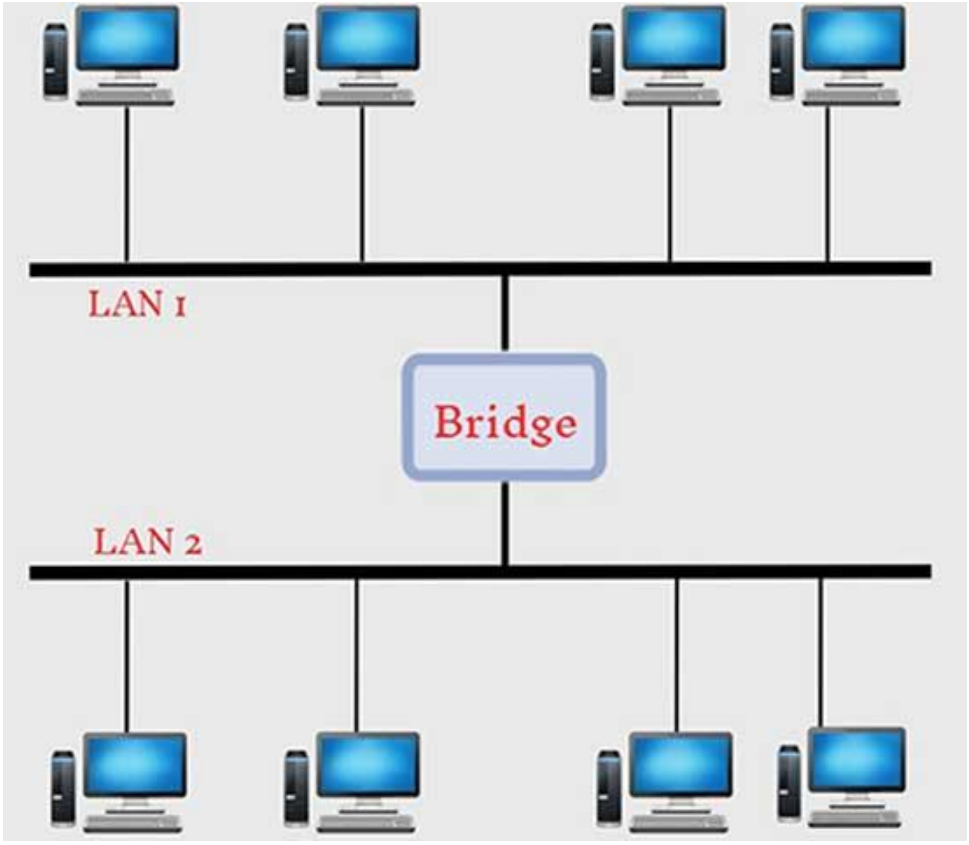
Switch: Network switch connects devices in a network to each other, enabling them totalk by exchanging data packets.

Switches can be hardware devices that manage physical networks or software-based virtual devices. Switches form the vast majority of network devices in modern data networks.

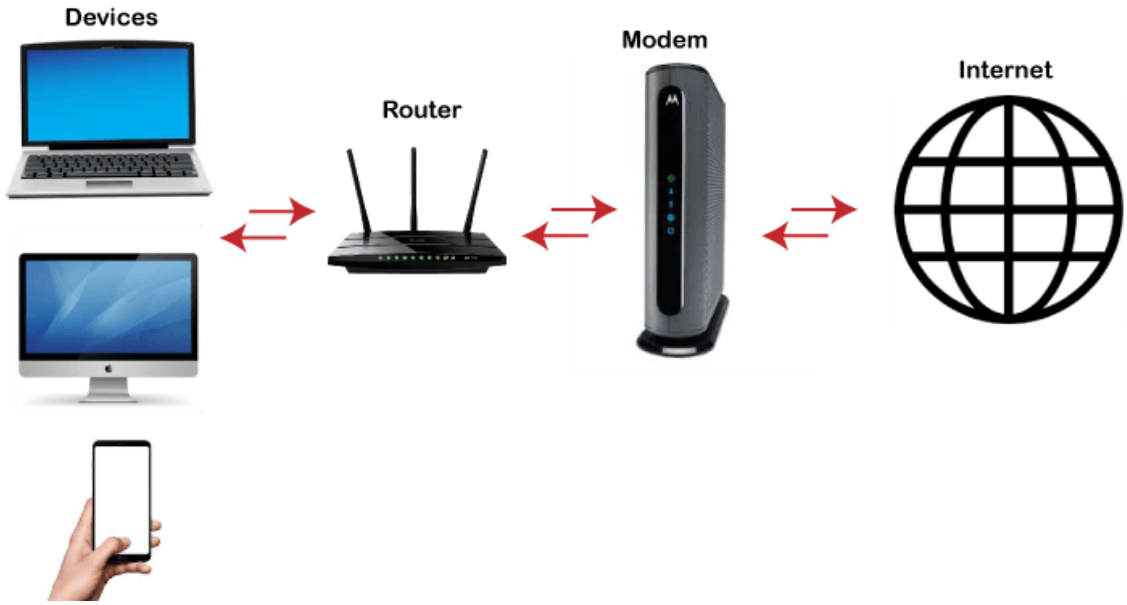


Bridge: A bridge in a computer network is a device used to connect multiple LANstogether with a larger Local Area Network (LAN).

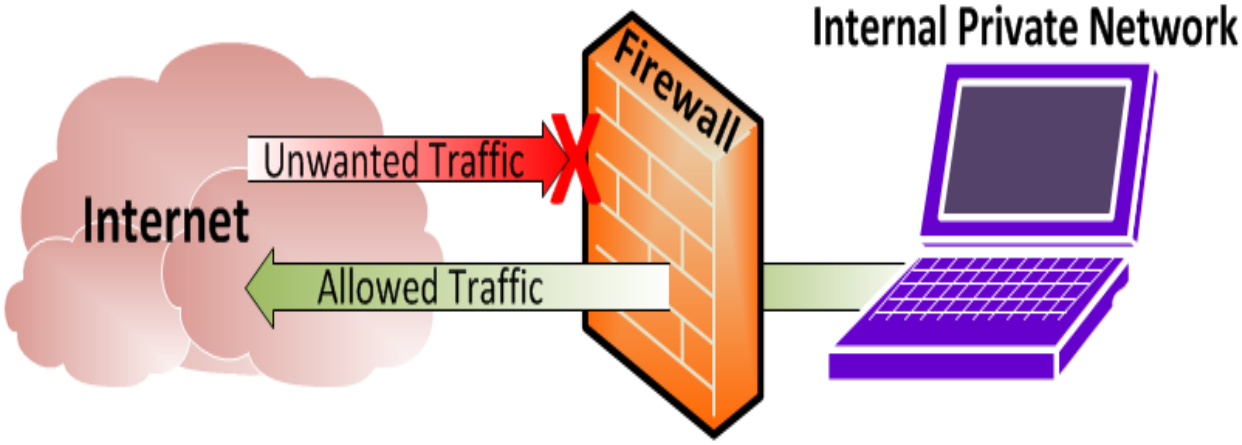
The mechanism of network aggregation is known as bridging. The bridge is a physical or hardware device but operates at the OSI model's data link layer and is also known as a layer of two switches.



Router: A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use thesame Internet connection.

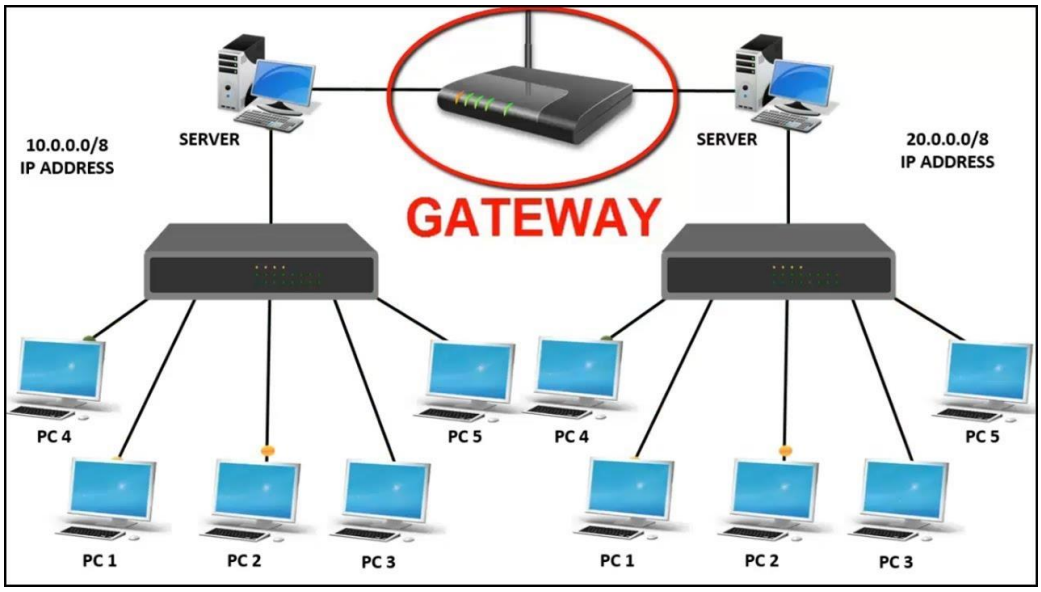


Firewall: Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.



Gateway: A gateway is a network node used in telecommunications that connectstwo networks with different transmission protocols together.

Gateways serve as an entry and exit point for a network as all data must pass through or communicate with the gateway prior to being routed.
A gateway is also called a protocol converter.



2. Study about UNIX commands used in TCP/IP. Commands are:
ftp, host, ifconfig, netstat, ip, ping, route, scp, sftp etc.

*The Unix operating system is case sensitive; type all commands in lower-case letters unless noted otherwise.

1. hostname

hostname with no options displays the machine's hostname

hostname –d displays the domain name the machine belongs to
hostname –f displays the fully qualified host and domain name
hostname –i displays the IP address for the current machine

2. ping

It sends packets of information to the user-defined source. If the packets are received, thedestination device sends packets back. Ping can be used for two purposes

* To ensure that a network connection can be established.

* Timing information as to the speed of the connection.

Use ctrl+C to stop the test.

3. ifconfig

View network configuration, it displays the current network adapter configuration.

It is handyto determine if you are getting transmit (TX) or receive (RX) errors.

4. netstat

Most useful and very versatile for finding a connection to and from the host. You can find outall the multicast groups (network) subscribed by this host by issuing "netstat -g"

netstat -nap | grep port will display process id of application which isusing that port
netstat -a or netstat –all will display all connections including TCP andUDP
netstat --tcp or **netstat –t** will display only TCP connection netstat --udp or
netstat –u will display only UDP connection **netstat -g** will display all multicast network subscribed by this host.

5. nslookup

If you know the IP address it will display the hostname. To find all the IP addresses for agiven domain name, the command nslookup is used. You must have a connection to the internet for this utility to be useful,

example: $ nslookup blogger.com

You can also use the nslookup to convert hostname to IP Address and from IP Address from the hostname.

6. traceroute

A handy utility to view the number of hops and response time to get to a remote system or website is a traceroute. Again you need an internet connection to make use of this tool.

7. finger

View user information, displays a user's login name, real name, terminal name, and write status. this is pretty old Unix command and rarely used nowadays.

8. telnet

Connects destination host via the telnet protocol, if telnet connection establishes on any port means connectivity between two hosts is working fine.

$ telnet hostname port

will telnet hostname with the port specified. Normally it is used to seewhether the host is alive and the network connection is fine or not.

9. ip

ipconfig command displays the basic IP addressing information for each network interface on the Windows system. This information includes both the IP address and subnet mask.

10.route

The route command allows you to make manual entries into the network routing tables. The route command distinguishes between routes to hosts and routes to networks by interpreting the network address of the Destination variable, which can be specified either by symbolic name or numeric address.

11. scp

(the scp command) to securely copy files and directories between remote hosts without starting an FTP session or logging into the remote systems explicitly.
The scp command uses SSH to transfer data, so it requires a password or passphrase for authentication

12.sftp

sftp is an interactive file transfer program, similar to ftp(1), which performs all operations over an encrypted ssh(1) transport. It may also use many features of ssh, such as public key authentication and compression. sftp connects and logs into the specified host, then enters an interactive command mode.

13.Displaying a Directory

ls–Lists the names of files in a particular Unix directory. If you type the ls command with no parameters or qualifiers, the command displays the files listed in your current working directory. When you give the ls command, you can add one or more modifiers to get additional information.

Example: **ls**
Result: Lists the names of files in your default directory, in alphabetical order.

Example: **ls -l**
Result: Gives a "long listing" of the files in your directory. In addition to the file name, the long listing shows protection information, file owner, number of characters in file, and the date and time of the last change to the file.

Example: **ls -a**
Result: Causes all your files to be listed, including those files that begin with a period (i.e., hidden files).

For more information, type **man ls** at the Unix system prompt.

14.Displaying and Concatenating (Combining) Files

more–Enables examination of a continuous text one screenful at a time on a terminal. It normally pauses after each screenful, printing -- More -- at the bottom of the screen. Press RETURN to display one more line. Press the SPACE BAR to display another screenful. Press the letter Q to stop displaying the file.

Example: **more newfile**
Result: Displays the contents of "newfile" one screen ("page") at a time.

For more information about this command, type **man more** at the Unix system prompt.

cat-- Displays the contents of a file on your terminal.

Example: **cat newfile**
Result: Displays the contents of the file "newfile" on your terminal.

Example: **cat newfile oldfile**
Result: Displays the contents of two files–"newfile" and "oldfile"–on your terminal as one continuous display.

Example: **cat fileone filetwo filethree > newfile**
Result: Links together three files–fileone, filetwo, and filethree–into a new file called "newfile." The original files remain intact.

15.Copying Files

cp–Makes copies of your files. You can use it to make copies of files in your default directory, to copy files from one directory to another directory, or to copy files from other devices.

Example: **cp fileone filetwo**
Result: Copies the contents of fileone to a file named filetwo. Two separate files now exist.

Example: **cp /usr/neighbor/testfile .**
Result: Copies the file testfile from the directory /user/neighbor to your Unix account. The period(.) at the end of the command line indicates that the file is to be copied to your current working directory and the name will remain the same.

To copy a file from another user's directory on Unix, you must know the person's username.

Example: **cp ~username/file1 yourfile**
Result: Copies the file "file1" from user to your Unix account. The name of the file in your directory becomes yourfile. (Protections must be set for file to be readable by you in the other user's directory in order to be able to copy the file.)

16.Deleting Files

rm–Deletes specific files. You can enter more than one file specification on a command line by separating the file specifications with spaces.

Example: **rm newfile**
Result: Deletes the file named "newfile."

Example: **rm newfile oldfile**
Result: Deletes two files–"newfile" and "oldfile."

Example: **rm new***
Result: Deletes all files that begin with the prefix new.

For more information, type **man rm** at the Unix system prompt.

17.Renaming Files

mv–This command changes the identification (name) of one or more files.

Example: **mv oldfile newfile**
Result: Changes the name of the file "oldfile" to "newfile." Only one file will exist.

Example: **mv oldfile bin/newfile**
Result: Changes the name of the file "oldfile" to "newfile" and places it in the directory /bin. Only one file will exist.

18.Printing from Unix

The **lpr** command prints files on Unix. Use the -Pqueuename option to select a printer.

Example: lpr -Ppittprint sample.file

19. ftp

ftp is the user interface to the Internet standard File Transfer Protocol. The program allows a user to transfer files to and from a remote network site.

TAG	DESCRIPTION
-A'	Use active mode for data transfers. This is useful fortransmissions to serverswhich do not support passive connections(for whatever reason.).
-p'	Use passive mode for data transfers. Allows use of ftp in environments where a firewall prevents connections from the outside world back to the client machine. Requires that the ftp server support the PASV command. This is the default now for all clients (ftp and pftp) due to security concerns using the PORT transfer mode. The flag is kept for compatibility only and hasno effect anymore.
-i'	Turns off interactive prompting during multiple file transfers.
n'	Restrains ftp from attempting "auto-login" upon initial connection. If auto- login is enabled, ftp will check the . netrc (see netrc(5)) file in the user's homedirectory for an entry describing an account on the remote machine. If no entry exists, ftp will prompt for the remote machine login name (default is the user identity on the local machine), and, if necessary, prompt for a password and an account with which to login.
-e'	Disables command editing and history support, if it was compiled into the ftp executable. Otherwise, does nothing

-g'	Disables file name globbing

-m'	The default requires that ftp explicitly binds to the same interface for the data channel as the control channel in passive mode. Useful on multi-homed clients. This option disables this behavior. Files cannot be extracted from a thin ftpchive.
-v'	Verbose option forces ftp to show all responses from the remote server, aswell as report on data transfer statistics
-d'	Enables debugging.