ODIA ANITA 16/SCI01/029 CSC 402

FILE TRANSFER PROTOCOLS,

A protocol is a system of rules that networked computers use to communicate with one another. FTP is a client-server protocol that may be used to transfer files between computers on the internet. The client asks for the files and the server provides them. It is a client/server protocol used for transferring files to or exchanging files with a host computer. It may be authenticated with user names and passwords. Anonymous FTP allows users to access files, programs and other data from the Internet without the need for a user ID or password. Web sites are sometimes designed to allow users to use 'anonymous' or 'guest' as a user ID and an email address for a password. Publicly available flies are often found in a directory called pub and can be easily FTP to a user’s computer. FTP is also the Internet standard for moving or transferring files from one computer to another using TCP or IP networks. You can work with FTP using a simple command-line interface, such as the DOS console in Windows and Terminal in Linux and macOS. If you don’t want to use those, though, there are graphical user interface solutions, such as [Filezilla](https://filezilla-project.org/download.php?type=client" \t "_blank) or [WS FTP Pro](https://www.ipswitch.com/ftp-client). Browsers also allow you to download files via FTP.

SIMPLE MAIL TRANSFER PROTOCOL (SMTP),

SMTP is part of the application layer of the TCP/IP protocol. Using a process called "store and forward," SMTP moves your email on and across networks. It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox.

SMTP spells out and directs how your email moves from your computer's MTA to an MTA on another computer, and even several computers.

SMTP provides those codes, and email server software is designed to understand what they mean. As each message travels towards its destination, it sometimes passes through a number of computers as well as their individual MTAs. As it does, it's briefly stored before it moves on to the next computer in the path. Think of it as a letter going through different hands as it winds its way to the right mailbox. The SMTP could also stand for STOP, Each ISP relies on its SMTP to determine (and govern) the email that can be sent out by one connection. For some people who work at home or manage large mailing lists, that could be a problem. After they hit their limit, the ISP will simply stop sending emails. If they think you're a spammer, they might even shut down your account.

INTERNET PROTOCOL,

Internet Protocol (IP) is the principal set (or communications protocol) of digital message formats and rules for exchanging messages between computers across a single network or a series of interconnected networks, using the Internet Protocol Suite (often referred to as TCP/IP). Messages are exchanged as datagrams, also known as data packets or just packets.   
The main purpose and task of IP is the delivery of datagrams from the source host (source computer) to the destination host (receiving computer) based on their addresses. To achieve this, IP includes methods and structures for putting tags (address information, which is part of metadata) within datagrams.

The process of putting these tags on datagrams is called encapsulation.

USER DATAGRAM PROTOCOL (UDP),

The User Datagram Protocol, or UDP for short, is a protocol that allows **datagrams to be sent without connection** in IP-based networks. To achieve the desired services on the target hosts, it uses ports that are listed as one of the core components in the UDP header. Like many other network protocols, UDP belongs to the **internet protocol family**, where it is classified as a mediator between the network layer and the application layer at the **transport level**.

UDP provides an unreliable packet delivery system built on top of the IP protocol. As with IP, each packet is an individual, and is handled separately. Because of this, the amount of data that can be sent in a UDP packet is limited to the amount that can be contained in a single IP packet.

UDP packets can arrive out of order or not at all. No packet has any knowledge of the preceding or following packet. The recipient does not acknowledge packets, so the sender does not know that the transmission was successful. UDP has no provisions for flow control--packets can be received faster than they can be used. We call this type of communication connectionless because the packets have no relationship to each other and because there is no state maintained.

INTERNET PROTOCOL AND THE USER DATAGRAM PROTOCOL,

When you load a web page, your computer sends IP packets to the web server’s address, asking it to send the web page to you. The web server responds by sending a stream of IP packets, which your web browser stitches together to form the web page and display it to you. When you click a link, sign in, post a comment, or do anything else, your web browser sends IP packets to the server and the server sends IP packets back. IP is not just one way communication — the remote system sends packets back to acknowledge it is received your packets. On the other hand when using UDP, packets are just sent to the recipient. The sender will not wait to make sure the recipient received the packet, it will just continue sending the next packets. If you are the recipient and you miss some UDP packets, too bad, you cannot ask for those packets again. There is no guarantee you are getting all the packets and there is no way to ask for a packet again if you miss it, but losing this entire overhead means the computers can communicate more quickly.