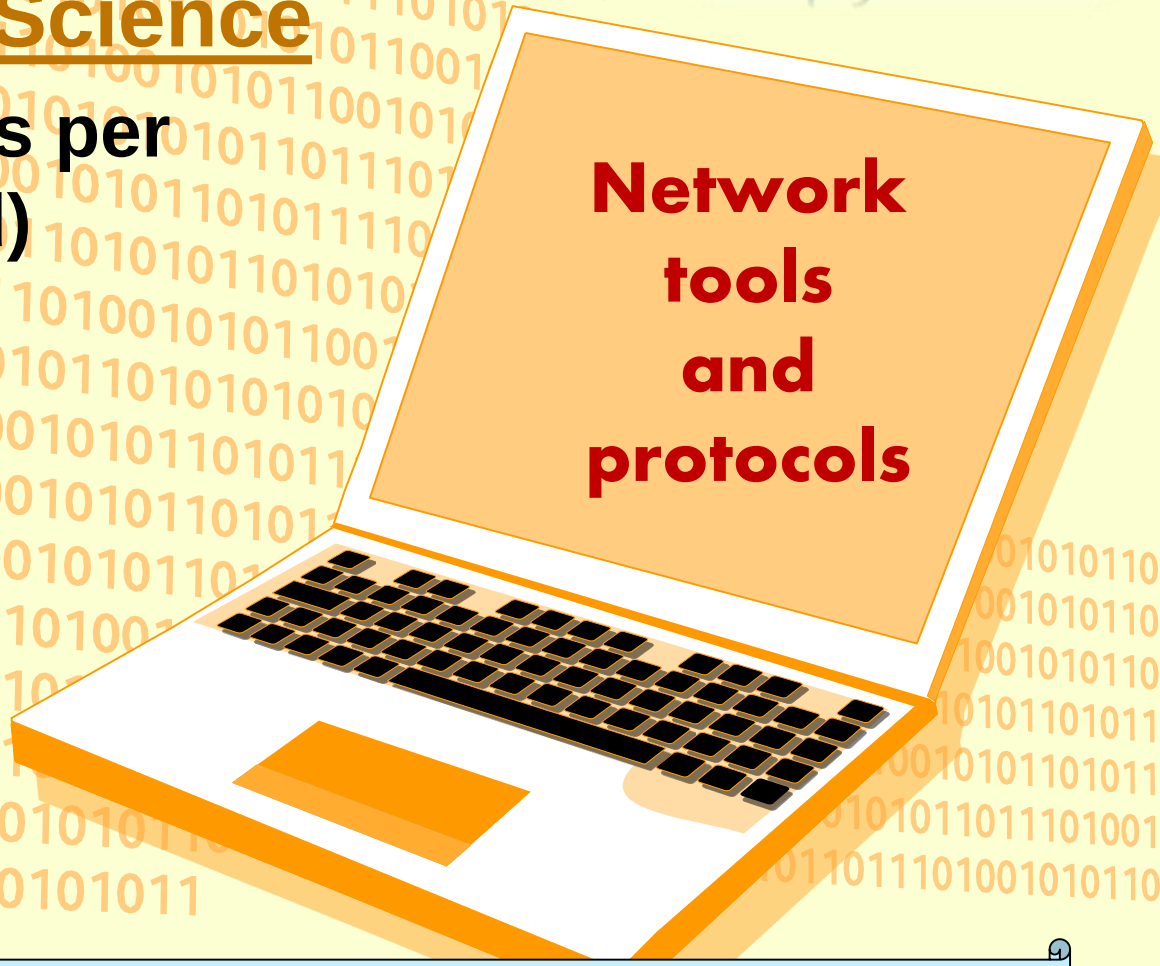
Chapter 11 :

Computer Science

Class XII (As per CBSE Board)



New Syllabus 2019-20

Visit : python.mykvs.in for regular updates

Basic Network tools

Traceroute -

Traceroute is a network diagnostic tool initially developed by Van Jacobson to determine whether routing problems exist on the network. Traceroute can be used to determine which path IP packets are taking to get from our computer to the remote computer. It should not be used in the network where there are no routers in between. It is not really useful unless there are at least two routers in the network. The Internet has thousands of routers so traceroute is perfect for the Internet. Traceroute was designed to reveal when network failures such as routing loops and black holes occur and displays roughly where those failures exist.In windows environment we have to use the **tracert** (tracerout) command.

Open command prompt in windows and Type

> **tracert python.mykvs.in**

It will display a list with no of hopes in between the computer we are using and the server of python.mykvs.in

On linux same command can be given like **traceroute python.mykvs.in**

In place of domain name we can write the ip address also of the remove system e.g. **tracert 182.156.84.26**

Traceroute command graphical version can be downloaded from https://visualtraceroute.net/

Basic Network tools

Traceroute –

Following are the characters may be displayed during tracing of remote computer while traceroute command is under process.

IP Traceroute Text Characters	
Character	**Description**
*	The probe timed out
A	Administratively prohibited
Q	Source quench
I	User interrupted test
U	Port unreachable
H	Host unreachable
N	Network unreachable
P	Protocol Unreachable
T	Timeout
?	Unknown packet type

Basic Network tools

ping –

The ping command is the basic troubleshooting tool for TCP/IP. We can use it to determine whether basic TCP/IP connectivity has been established between two computers or not.

It is a simple, widely used, cross-platform networking utility for testing if a host is reachable on an Internet Protocol (IP) network.

It works by sending a series of Internet Control Message Protocol (ICMP) echo_request messages to the target host and waiting for response.Most of the network administrator use this utility/protocol to check that two computers are properly connected with each other or not on network.

In windows open command prompt and type

- **ping python.mykvs.in**

It will display the no of bytes returned by the remote computer.

In place of domain name we can specify ip address also like

> **ping 182.156.84.26**

>ping –c

It will display the no of options and attributes which can be used along with ping command.

Basic Network tools

ipconfig –

Ipconfig is a useful networking troubleshooting command in windows. It is often used to display the basic networking information (addresses etc.) on a given computer but it can do much more than that. It can release and renew IP addresses for any adapter, it can refresh DHCP leases for dynamic adapters, it can also flush the DNS cache, and more.Open command prompt and type.

>ipconfig

It will display networking information of the computer we are using.

ipconfig - Briefly show you the configured network adapter's information, such as IP address, subnet mask and gateway.
ipconfig /all - Show detailed information of network adapter that includes IP address, subnet mask, gateway, DNS, DHCP, MAC address, etc.
ipconfig /release - Release the IP address of network adapter, mainly used for network adapter that relies on DHCP server to obtain IP address.
ipconfig /renew - Renew the IP address of network adapter, mainly used for network adapter that relies on DHCP server to obtain IP address.
ipconfig /displaydns - Display the contents of the DNS Resolver Cache.
ipconfig /flushdns - Clear the DNS Resolver cache.
ipconfig /? - Display detailed command usage info/manual.

Basic Network tools

nslookup –

Nslookup is a command line utility supplied as part of most of operating systems that can reveal information related to domain names and the Internet Protocol (IP) addresses associated with them.
Type the following command in command prompt

>**nslookup python.mykvs.in**

This command send the request to local DNS server ,the domain name supplied along with this command.DNS Server resolve it and respond the server name and ip address of the server.Here it will return.

Server: **python.mykvs.in**
Address: **182.156.84.26**

In simple terms, it is a tool which provide information by interrogating DNS servers either locally or remotely assuming the required DNS server responsible (or knowledgeable) about the requested domain is contactable from where you are operating - over the Internet.

Basic Network tools

whois –

Whois is a service/protocol that provides basic information about a registered domain like domain owner, contact information, domain availability status and the company with which the domain is registered (known as Registrar). Whois also provides registration and expiration dates of a domain along with the nameservers the domain is using.Open the command prompt and type

>whois python.mykvs.in

It will display the domain information of domain name python.mykvs.in

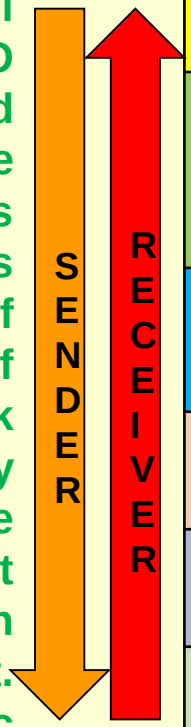
Speedtest –

- **Speedtest.net** is a web service which provides free analysis of Internet access performance metrics like connection data rate and latency. It was founded by Ookla in 2006, and is based in Seattle, Washington.
- **FAST.com** speed test gives you an estimate of your current Internet speed. You will generally be able to get this speed from leading Internet services, which use globally distributed servers.
- **ping-test.net** - is fast and accurate tool for quality measurements of the Internet connection. It checks delays in millisecond between your computer and selecter remote server. The ping value strongly depends on the distance to the server - the bigger distance the ping value is higher. Your connection is stable if the chart is like straight horizontal line.

Network Protocols

OSI –

Open System Interconnection (OSI) is a network model developed by ISO (International Standard Organization) in 1978 where peer-to-peer communications are divided into seven layers for the purpose of standardization of development of network hardware or software by different software/hardware companies, which can interact with each other in heterogeneous environment. Each layer performs a specific task or tasks and builds upon the preceding layer until the communications are complete.



7. APPLICATION LAYER	Human interaction through application which access network services(HTTP,FTP,Telnet etc.)
6. PRESENTATION LAYER	Data encryption to present those data to be displayed over application(IMAP,SSL,JPEG etc.)
5. SESSION LAYER	To maintain session to deliver data over network(API,Socket etc.)
4. TRANSPORT LAYER	Transmit data using TCP (TCP,UDP)
3. NETWORK LAYER	Decide network path to move over data(IP,ICMP,IPsec)
2. DATALINK LAYER	Defines format of data for network (Ethernet,SWITCH,BRIDGE,PPP)
1. PHYSICAL LAYER	Transmit raw bit stream over physical medium(FIBER,COAX,HUB etc.)

Software layer

Heart of OSI

Hardware layer

Network Protocols

Application Layer –

The application layer is at the topmost position of the protocol hierarchy. It is the layer where actual communication is initiated. It uses the services of the lower layer as proposed in OSI reference mode to transfer data to a remote host. Following are some of the protocols used under Application Layer.

- **HTTP**
- **working of email**
- **secure communication: encryption and certificates (HTTPS),**
- **network applications: remote desktop, remote login, HTTP, FTP, SCP, SSH, POP/IMAP, SMTP, VoIP, NFC**

Network Protocols

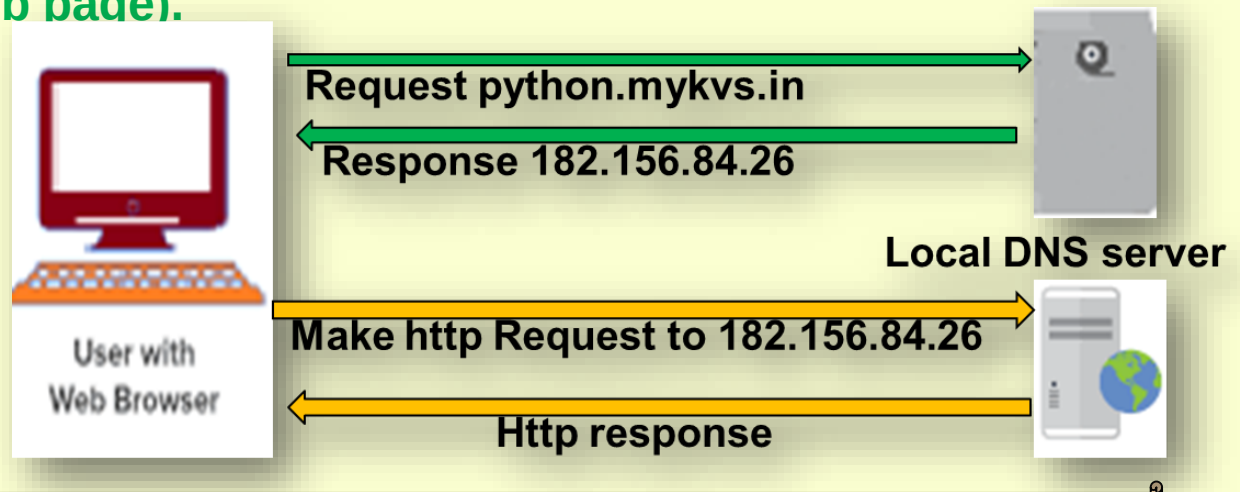
Application Layer –

HTTP - HTTP stands for hypertext transfer protocol and is used to transfer data across the Web. It allow users of the World Wide Web to exchange information found on web pages. When accessing any web page entering http:// in front of the address tells the browser to communicate over HTTP.

How It Works-

It is a connectionless text based protocol. Clients (web browsers) send requests through ***request object*** of http to web servers for web pages / images etc.Web server respond accordingly through ***response object*** of http After this cycle(request – response), the connection between client and server across the Internet is disconnected. A new connection must be made for each request(means for each web page).

This diagram shows the working of http protocol. Working with dns server and working with web Server both.

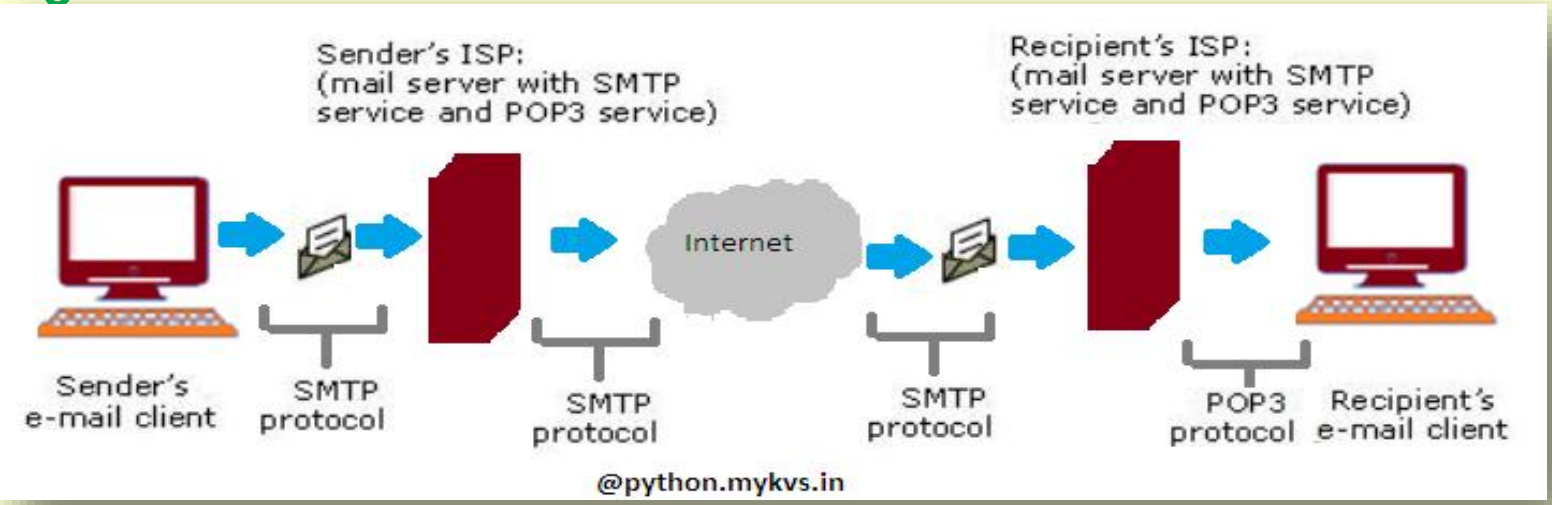


Network Protocols

Application Layer –

Working of email

Email –Electronic mail is a facility that allows users to transmit messages across the internet in fast and secure manner.



Email created using email client program->on press of send button ,it is delivered to sender's mail server through SMTP(Simple mail transfer protocol)->which further transmit the same through internet to recipient's mail server->whenever recipient's email client program's inbox is opened,that email is delivered to inbox through POP3 (post office protocols 3rd version)->which user will read in email client program.

Network Protocols

Application Layer –

Secure communication –

Secure communication is when sender and receiver are communicating and do not want a third party to listen it. For that they need to communicate in a way not susceptible to eavesdropping or interception(message stolen from the media).Generally encryption techniques are used to secure the message.
Encryption - to change electronic information or signals into a secret code (= system of letters/numbers/symbols) that people cannot understand .
Decryption It is the process of decoding the data which has been encrypted.
Encryption is done at sender's site where as decryption is done at receiver site.

Network Protocols

Application Layer –

Secure communication – HTTPS

HTTPS(Hyper text transfer protocol secure) scramble the messages using that "code" so that no one in between can read the message. It keeps our information safe from hackers.

Https uses the "code" on a **Secure Sockets Layer (SSL)**, sometimes called Transport Layer Security (TLS) to send the information back and forth.

Essentially, we need three things to encrypt data:

- The data to be sent/encrypted
- A unique encryption key
- An encryption algorithm (a math function that garbles the data)

asymmetric encryption is used in https. Asymmetric means we are using two different keys, one to encrypt and one to decrypt. This encryption is now done at TLS rather than SSL.

Network Protocols

Application Layer –

Network applications:

Remote desktop – A computer program/utility that enable us to connect our computer across the Internet virtually with any other computer, Pocket PC, or smartphone.

To start Remote Desktop on the computer we want to work from in windows

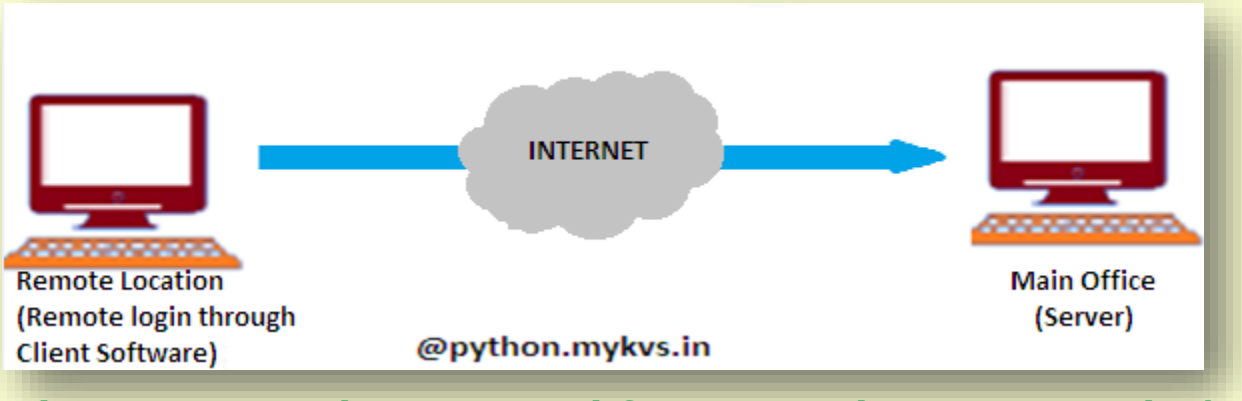
- **Open Remote Desktop Connection by clicking the Start button Start button icon. In the search box, type Remote Desktop Connection, and then, in the list of results, click Remote Desktop Connection.**
- **In the Computer box, type the name of the computer that we want to connect to, and then click Connect. (we can also type the IP address instead of the computer name.)**

Network Protocols

Application Layer –

Network applications:

Remote login – A remote login facility permits a user who is using one computer to login to remote computer or interact with a program on another computer. Command given at remote location is processed by server and result displayed over remote location.



Telnet – Telnet is most popular protocol for accessing remote site/server. Using telnet client software on our computer, we can make a connection to a telnet server (that is, the remote host). Once our telnet client establishes a connection to the remote host, our client becomes a virtual terminal, allowing us to communicate with the remote host from our computer. In most cases, we need to log into the remote host, which requires that we have an account on that system. Occasionally, we can log in as guest or public without having an account.Generally it is used in unix based client server system to interact.

Network Protocols

Application Layer –

Network applications:

How to Enable telnet in Windows –

1. Open Start menu and select Control Panel.
2. Click on Programs.
3. Click on "Turn Windows features on or off."
4. Put a checkmark next to Telnet Client then click OK.
5. Wait for Windows to update your system then close the Control Panel.

Working on telnet

Working on telnet is very easy we have to type following in run dialog box of windows to connect to remote server telnet hostname port or telnet ipaddress port

e.g.

we can even use Telnet to talk to an artificially intelligent psychotherapist named *Eliza*.(one of the game,there are no of games on internet)

Type telnet telehack.com in run dialog box .it will open command prompt with list of telehack commands to communicate.some of command like you may type

>.eliza

Auto response will be given

>hi, my name is python

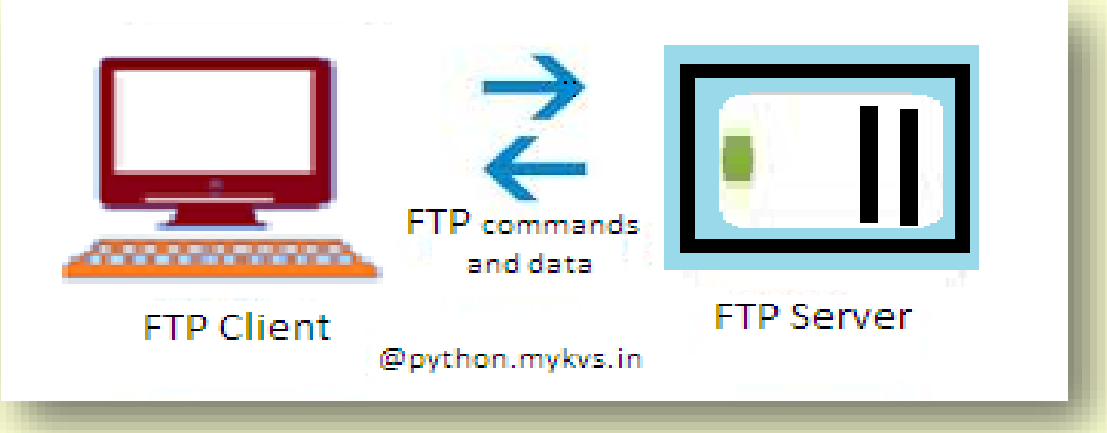
Auto response will be given

Network Protocols

Application Layer –

Network applications:

FTP – FTP, or File Transfer Protocol, is one of the standard internet protocols used to transfer data files between a client(FTP client) and a server(FTP server) over a computer network. It was developed in the early 1970s by Abhay Bhushan (alumni IIT Kanpur),while he was a student at MIT. FTP was initially created to allow for the secure transfer of files between servers and host computers over the ARPANET Network Control Program (a precursor to the modern internet).Nowadays it is being used for uploading files on webserver after non anonymous ftp(means username and password available with you).downloading is possible as anonymous ftp(no password is required).FTP is available in two mode –text mode ftp(where user have to give commands in text form) and GUI ftp(graphical interaction is possible)



Some of the more popular, and reliable, FTP Clients currently operating in the industry are FileZilla,WinSCP,Cyberduck,gFTP

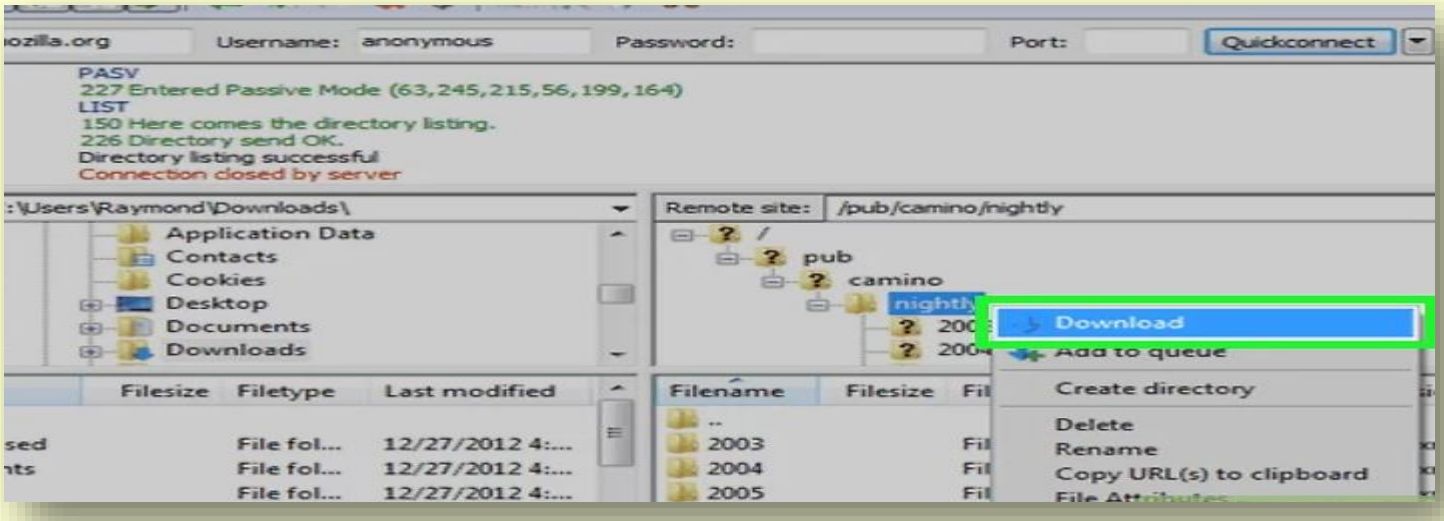
Network Protocols

Application Layer –

Network applications:

How to work on FTP – Here we are using Filezilla.

1. Download filezilla
2. Install filezilla
3. Open site manager from file menu and click on new site button
4. Type credential available of any domain
5. Press ok, It will connect our computer with remote computer ,screen will be something like this



6. Left side pan will display the folder/files of our computer and right side pan will display the file structure of remote computer.through simple drag and drop we can download upload(receive file from remote computer to local computer) or upload(sending file to remote computer from local computer) the files.

Network Protocols

Application Layer –

Network applications:

SSH – It is referred to as Secure Shell is a method for secure remote login from one computer to another with strong authentication, and it protects the communications security and integrity with strong encryption. It is a secure alternative to the non-protected login protocols (such as telnet, rlogin) and insecure file transfer methods (such as FTP).

The protocol is used in corporate networks for:

- **providing secure access for users and automated processes**
- **interactive and automated file transfers**
- **issuing remote commands**
- **managing network infrastructure and other mission-critical system components.**

Network Protocols

Application Layer –

Network applications:

SCP – It is the abbreviation of 'secure copy protocol‘. SCP is better designed for a one-time transfer between two computers on the same network, though it can be used remotely over the Internet as well.

The SCP command can be used to send a file to a server or retrieve a file from a server. Because it uses the SSH protocol for authentication SCP is more secure than FTP which transmits passwords in plain text. We can use PSCP utility in windows that is available at PuTTy.org. download and install it ,open the command prompt and set the path.

To receive

pscp free@example.com:/etc/hosts c:\temp\example-hosts.txt

To send

pscp c:\documents\myfile.txt free@example.com:/tmp/foo

Network Protocols

Application Layer –

Network applications:

POP3 – Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. POP3 allows us to download email messages on our local computer and read them even when we are offline. Note, that when we use POP3 to connect to our email account, messages are downloaded locally and removed from the email server. This means that if we access our account from multiple locations, that may not be the best option for us. On the other hand, if we use POP3, our messages are stored on our local computer, which reduces the space of email account uses on your web server.

IMAP - Internet Message Access Protocol is a standard email protocol that stores email messages on a mail server, but allows the end user to view and manipulate the messages as though they were stored locally on the end user's computing device(s). This allows users to organize messages into folders, have multiple client applications know which messages have been read, flag messages for urgency or follow-up and save draft messages on the server.

Network Protocols

Application Layer –

Network applications: Difference between POP3 and IMAP

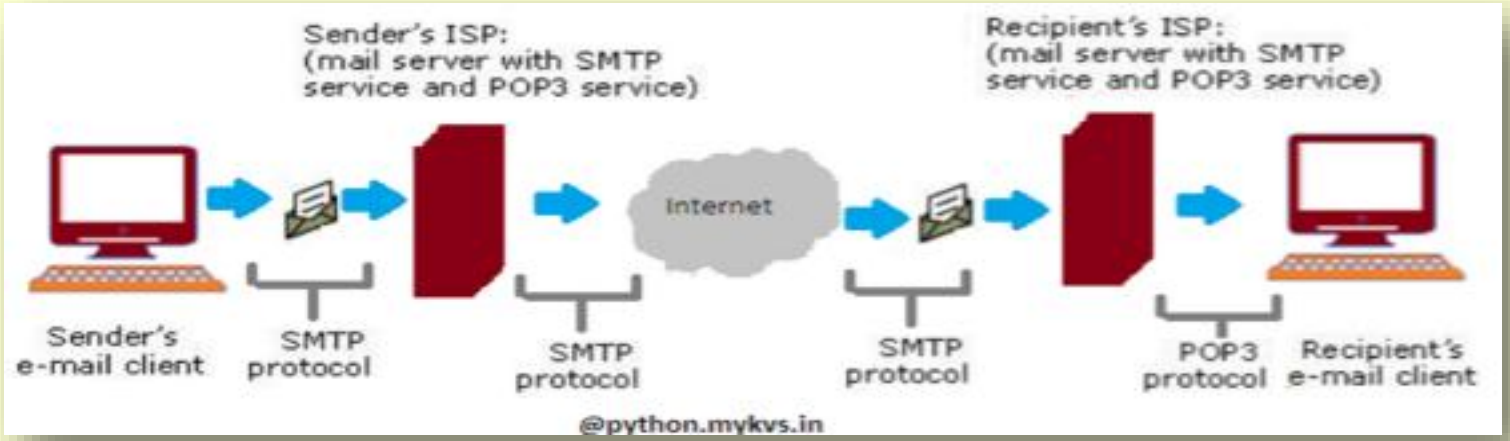
BASIS FOR COMPARISON	POP3	IMAP
Basic	To read the mail it has to be downloaded first.	Email content can be checked partially before download.
Organize	Mails can't be organized in mailbox of mail server by user.	User can organize the mails on the server.
Folder	User cannot create, delete or rename mailboxes on a mail server.	User can create, delete or rename mailboxes on the mail server.
Content	User cannot search the content of mail for prior downloading.	User can search the content of mail for specific string of character before downloading.
Partial Download	User has to download the mail for accessing it.	User can partially download the mail if bandwidth is limited.
Functions	POP3 is simple and has limited functions.	IMAP is more powerful and has more features over POP3.

Network Protocols

Application Layer –

Network applications:

SMTP – Most of the internet systems use SMTP as a method to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail to email server. it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server.An alternative to SMTP that is widely used in Europe is X.400. Many mail servers now support Extended Simple Mail Transfer Protocol (ESMTP), which allows multimedia files to be delivered as e-mail.



The SMTP model is of two type :

- **End-to- end method**
- **Store-and- forward method**

The end to end model is used to communicate between different organizations whereas the store and forward method is used within an organization.

Network Protocols

Application Layer –

Network applications:

VOIP – Voice over Internet Protocol (VoIP), is a technology that allows us to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line.

VoIP services convert our voice into a digital signal that travels over the Internet. If we are calling a regular phone number, the signal is converted to a regular telephone signal before it reaches the destination. VoIP can allow us to make a call directly from a computer, a special VoIP phone. In addition, wireless "hot spots" in locations such as airports, parks, and cafes allow us to connect to the Internet and may enable us to use VoIP service wirelessly.

Advantages:

- **Less Cost**
- **Accessibility**
- **Flexibility**
- **Voice Quality**
- **Extra/Less Expensive Features**

Disadvantages:

- **Reliable Internet Connection Required**
- **Power Outages/Emergencies**
- **Latency**

Network Protocols

Application Layer –

Network applications:

Services provided by VOIP – Phone to phone,pc to phone ,phone to pc,voice to email,ip phone,toll free number,call center applications,vpn,unified messaging etc.

Protocols used for VOIP are

- **Session Initiation Protocol (SIP)- connection management protocol developed by the IETF**
- **H.323 - one of the first VoIP call signaling and control protocols that found widespread implementation.**
- **Real-time Transport Protocol (RTP)- transport protocol for real-time audio and video data**
- **Real-time Transport Control Protocol (RTCP)- sister protocol for RTP providing stream statistics and status information**
- **Secure Real-time Transport Protocol (SRTP) - encrypted version of RTP**
- **Session Description Protocol (SDP) - file format used principally by SIP to describe VoIP connections**

Network Protocols

Application Layer –

Network applications:

NFC – Near field communication is a standards-based technology to provide short range wireless connection technology to carry secure two-way interactions between electronic devices.For Communication,it is not required to set-up by users as in the case of many other wireless communications.

It provides contactless communication up to distances of 4 or 5 centimeters. so communications are inherently more secure because devices normally only come into contact and hence communication when the user intends to do so.

The connection is more reliable as no physical connectors are used in NFC and does not suffer problems of contact wear, corrosion and dirt experienced by systems using physical connectors.

NFC applications

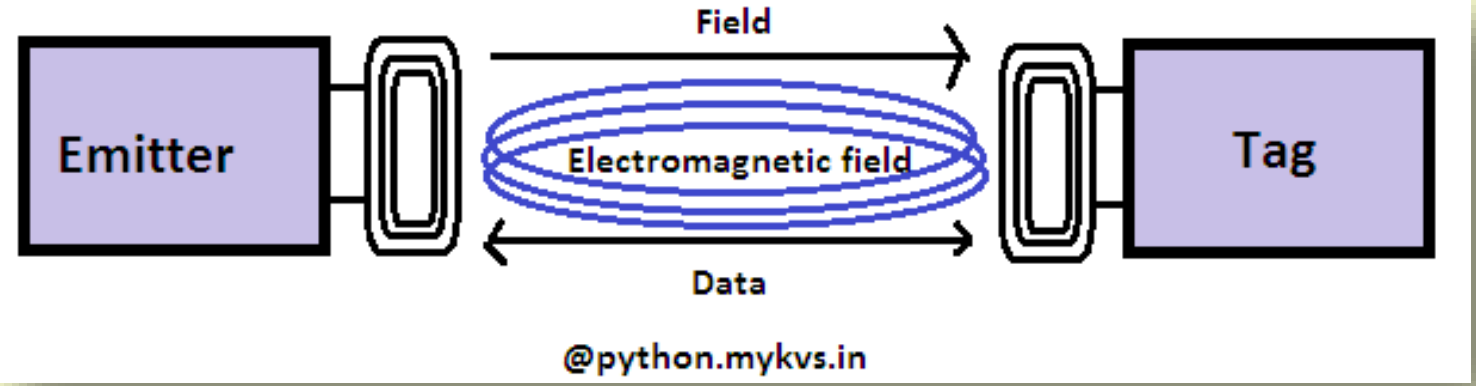
- **Payment cards**
- **Ticketing**
- **Mobile phones, PDAs, etc**
- **Check-out cash registers or "point-of-sale" equipment**
- **Vending machines**
- **Parking meters etc.**

Network Protocols

Application Layer –

Network applications:

How NFC works –



The antennas of the Emitter and Tag are coupled via an Electromagnetic Field known as Air-Core Transformer. An alternating current passes through the primary coil (Emitter) and this current induces a field thru the air, inducing current in the secondary coil (Tag). The Tag may use the current from the field to power itself. In general, inductive coupling thru air is very inefficient, and therefore, the read/write range is quite limited. tag contain an antenna(Inlay) & small amount of memory. A tag is a passive device, and the power the device needs to operate comes from the electromagnetic field, generated by the emitter. RFID Inlays are attached to the EEPROM Memory for the antenna. These inlays are customized for the antenna design and application.