Server Message Block Protocol (SMB Protocol)

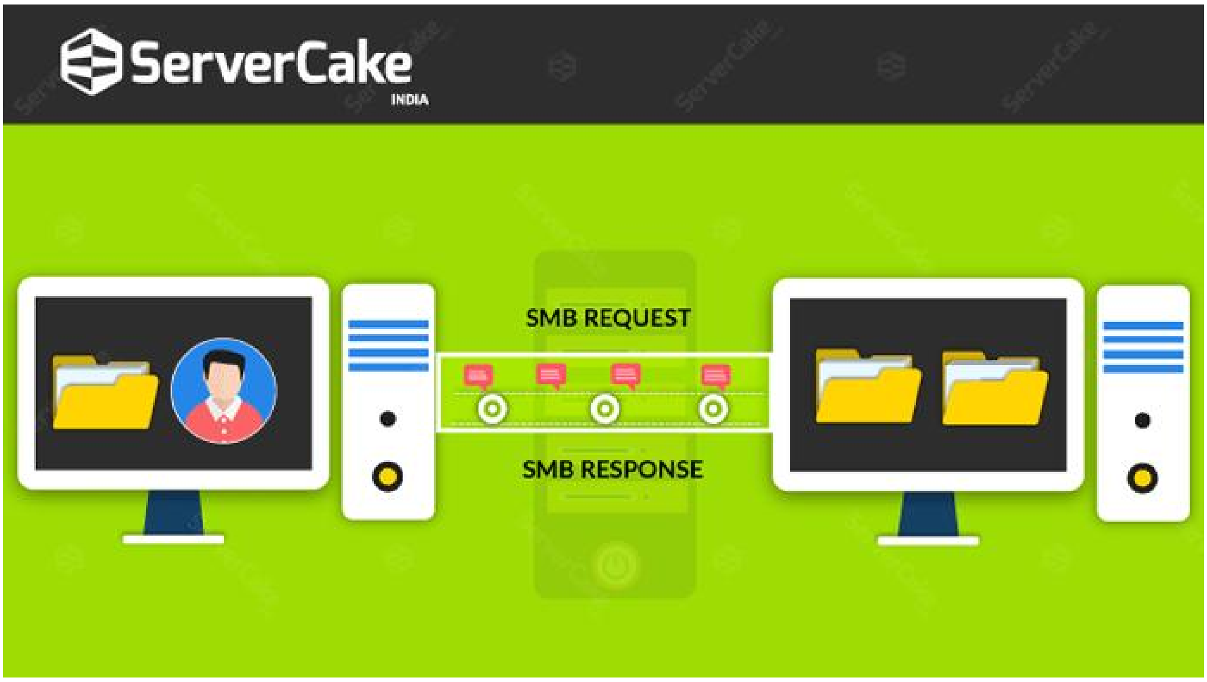
(also known as Common Interface File System (CIFS))

- **File sharing protocol in windows.**
- **Allows apps to read/write files.**
- **Urge requests for services from server manager for n/wconnected systems.**
- **Windows comes with default SMB v1.**
- **Also known as Client / Server Protocol.**
- **Information exchange b/w different process of s/m is handled by SMB protocol.**
- **Governs access to n/w resources like printer, router or interfaces open to n/w.**

Versions: SMB v1, SMB v2, SMB v3 - Current Version

PORT NUMBER: 139 & 445

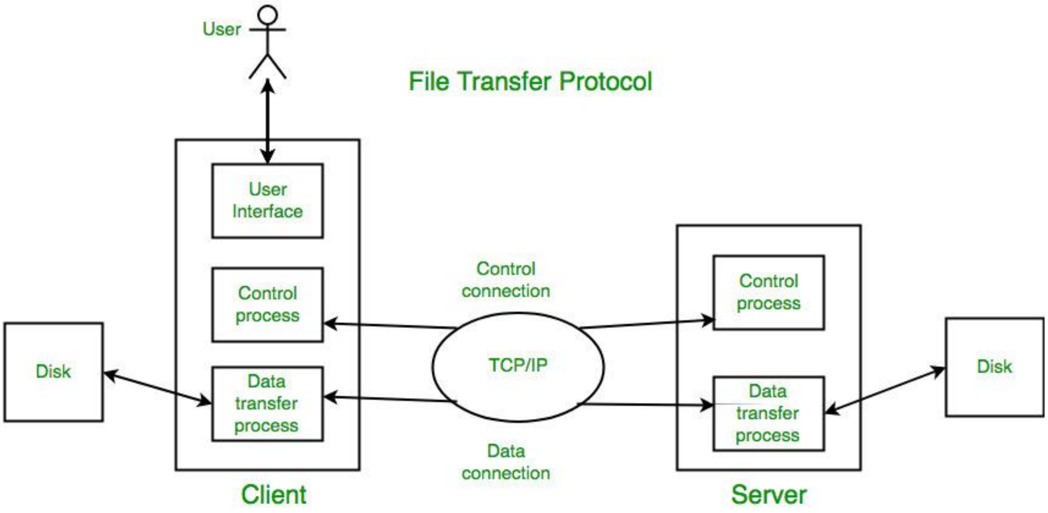
SUGGESTED TO DISABLE SMBv1 protocol to prevent from ransomeware attacks.



File Transfer Protocol (FTP)

- **Standard internet protocol provided by TCP/IP used for transmit files from ones host to another.**
- **Also used to download files from source to destination.**
- **Establishes two connections - one for data transfer and another for control the connection.**
- **Data size to transfer is max 2 GB.**
- **Doesn't allow simultaneous transfer to multiple receivers.**

PORT NUMBER: 20 & 21



Post Office Protocol (POP)

- Used to retreive email from mail server.
- POP is more secure that IMAP.

<u>**POINT OF PRESENCE**</u>

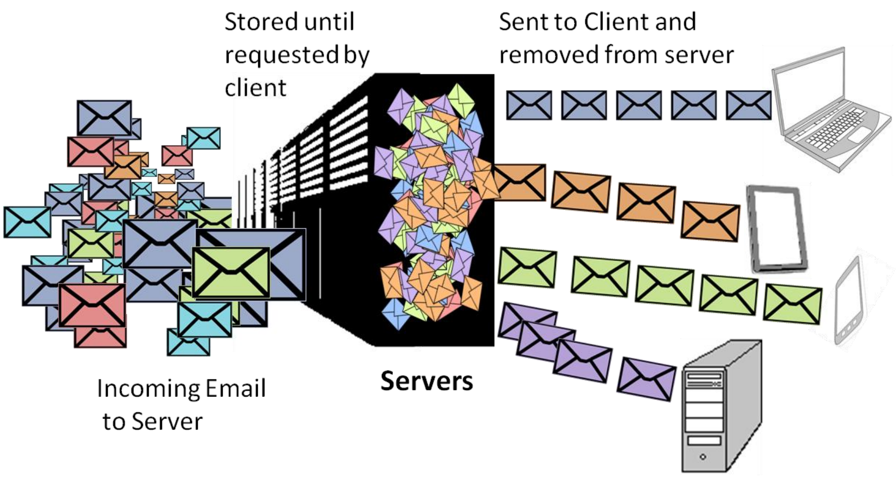
- Physical location that provides access b/w two or more n/w's or devices.

Port 110 is default POP3 non-encrypted port.
Port 995 is secure POP3 port.

PORT NUMBER: 110 & 995

Versions: POP, POP2, <u>POP3</u> - Current Version

Post Office Protocol


Stored until requested by client
Sent to Client and removed from server
Incoming Email to Server
Servers

---
------

Simple Mail Transfer Protocol (SMTP)

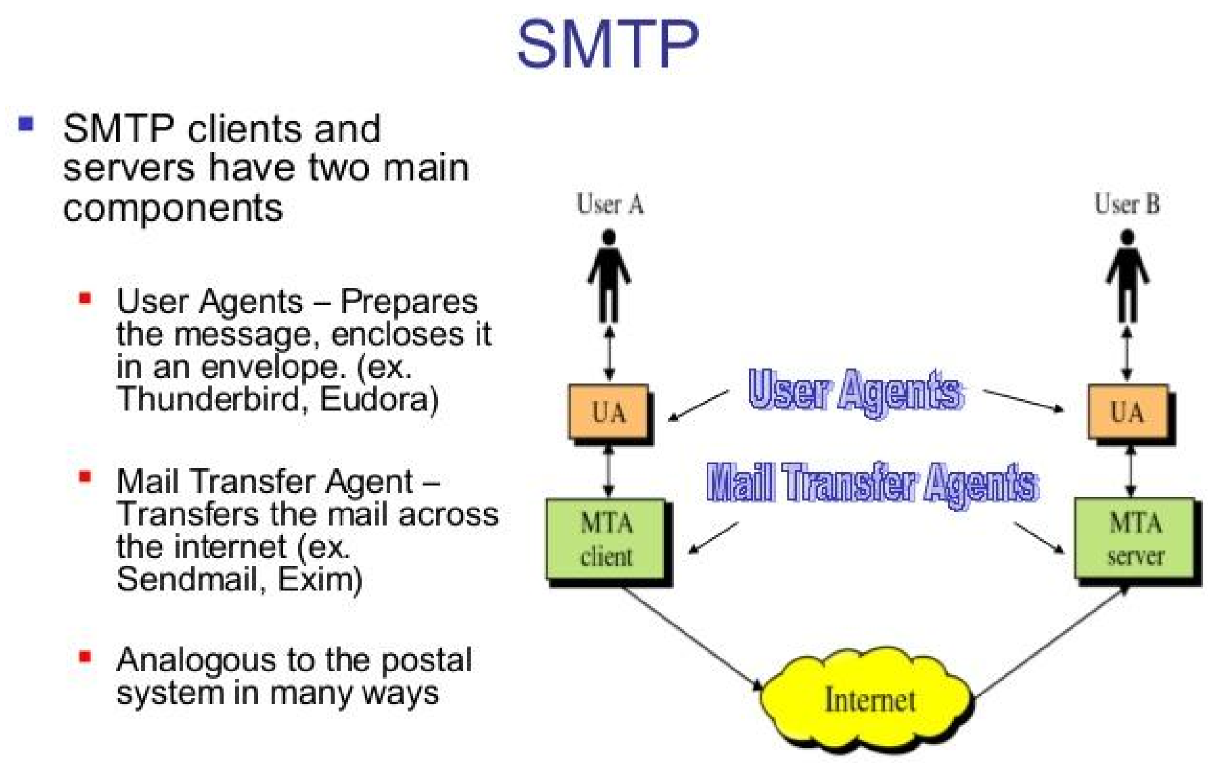
- ➢ **Standard protocol for email service on TCP/IP n/w.**
- ➢ **Application layer protocol that enables transmission and deliver of email over internet.**
- ➢ **Also known as RFC 821 & RFC 2821.**
- ➢ **SMTP works by intiating a session b/w user and server, where as MTA & MDA provide searching & local delivery services.**

COMPONENTS

- √ **Local user/client utility known as Mail User Agent (MVA).**
- √ **Server known as Mail Submission Agent (MSA).**
- √ **Mail Transfer Agent (MTA).**
- √ **Mail Delivery Agent (MDA).**

Port 25 is for SMTP relay.
Port 587 is Default port for SMTP submission of modren web.
Port 465 is registered for SMTPS (SMTP over SSL).
Port 2525 is not official SMTP port, used as alternative for 587.

PORT NUMBER: 25 & 465 & 587 & 2525



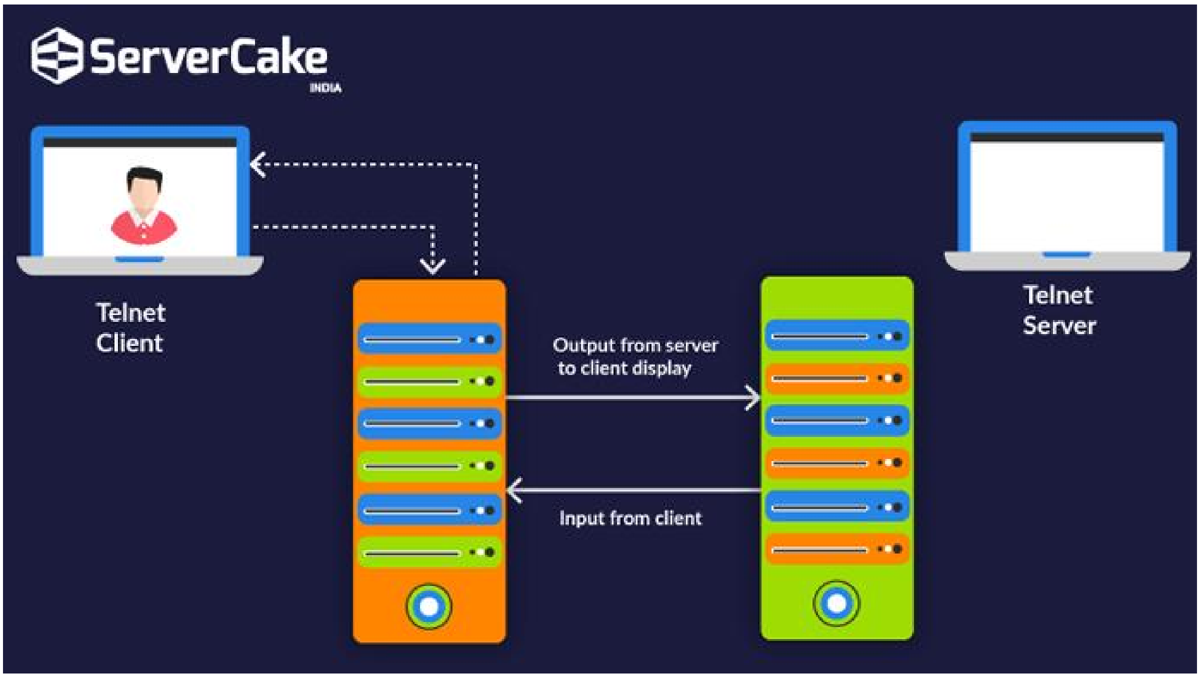
SMTP

- SMTP clients and servers have two main components
  - User Agents – Prepares the message, encloses it in an envelope. (ex. Thunderbird, Eudora)
  - Mail Transfer Agent – Transfers the mail across the internet (ex. Sendmail, Exim)
  - Analogous to the postal system in many ways

Telenet

- ➢ **Telenet is a n/w protocol used to virtually access a computer & to provide a two-way collaborative and test - based communication channel b/w two machines.**
- ➢ **Client-Server protocol used to open a command line on a remote computer.**
- ➢ **Used to ping a port.**
- ➢ **Not secure & unencrypted.**
- ➢ **SSH, Putty are alternatives of telenet which provides secured connection.**

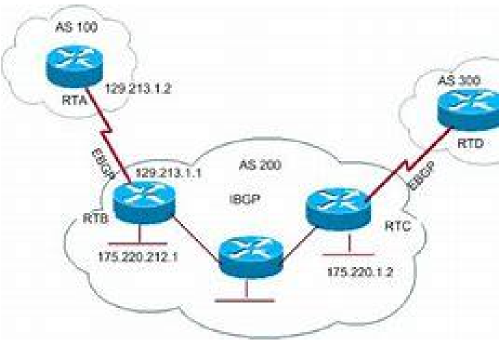
PORT NUMBER: 23



Broder Gateway Protocol (BGP)

- ➢ Used to exchange routing information for internet.
- ➢ Provide communication b/w two autonomous s/m's.
- ➢ Runs over TCP, supports CIDR, supports security.

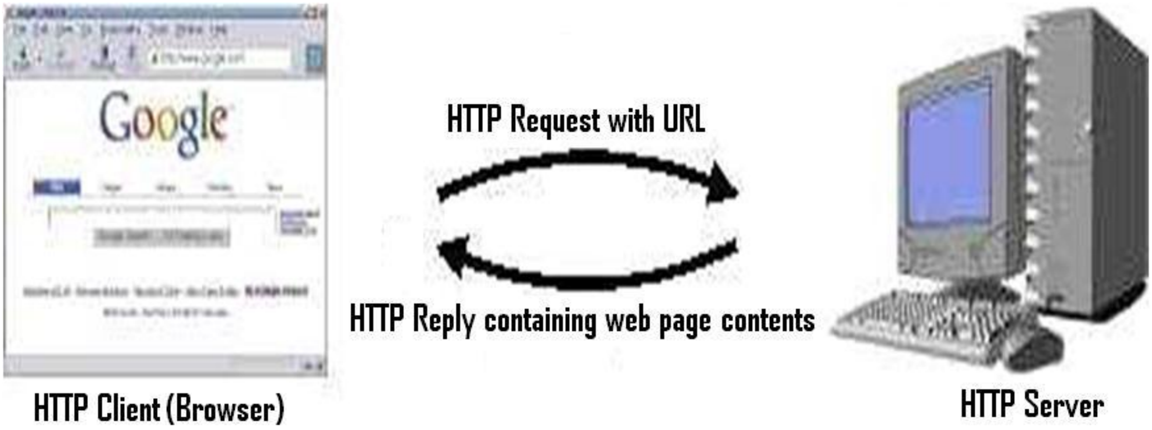
PORT NUMBER: 179



Hyper Text Transfer Protocol (HTTP)

- ➢ Application layer protocol for distributed, collaborative, hypermedia information s/m's.
- ➢ Plain text data transfer and unsecure.

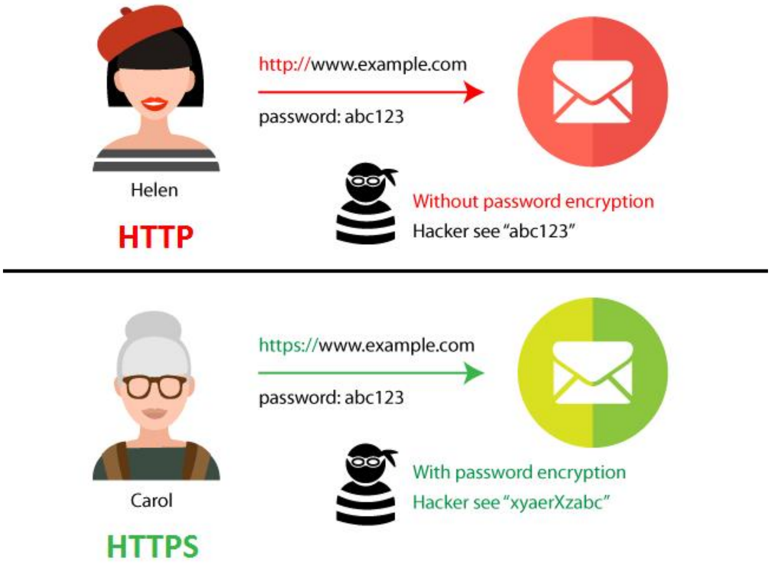
PORT NUMBER: 80



Hyper Transfer Text Protocol Secure (HTTPS)

- Highly advanced & secure version of HTTP.
- Encrypts communication with SSL.
- Combination of SSL/TLS & HTTP.
- Transport layer protocol.

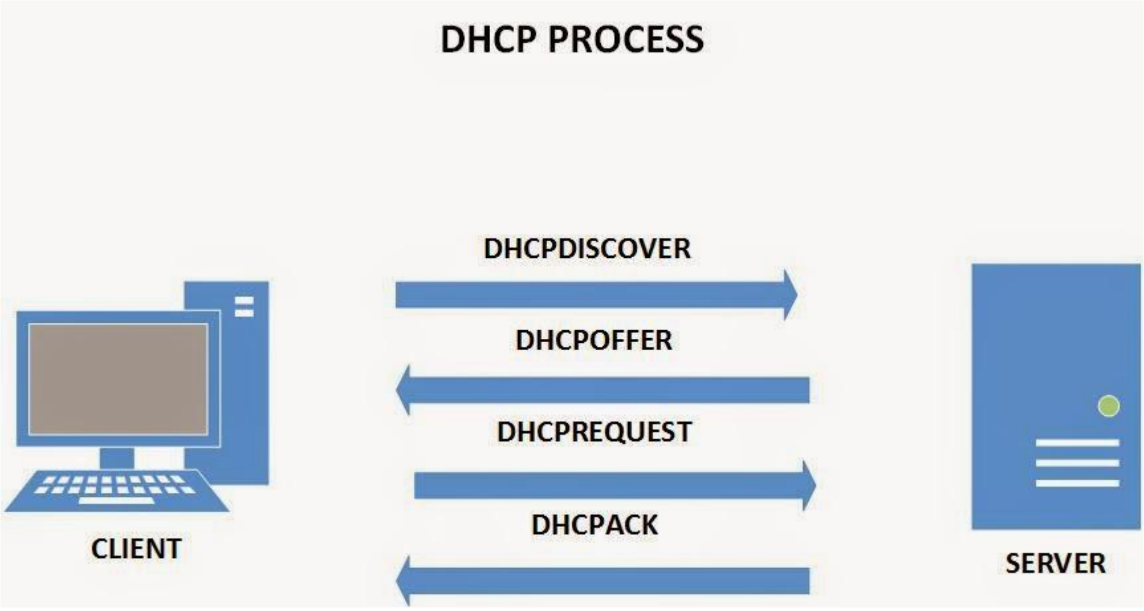
PORT NUMBER: 443



Dynamic Host Control Protocol (DHCP)

- N/W management protocol used on IP local area n/w's.
- A DHCP server must present on device.
- Device connected to n/w request IP address from DHCP server using DHCP protocol.

PORT NUMBER: 67 (Server Port) & 68 (Client Port)

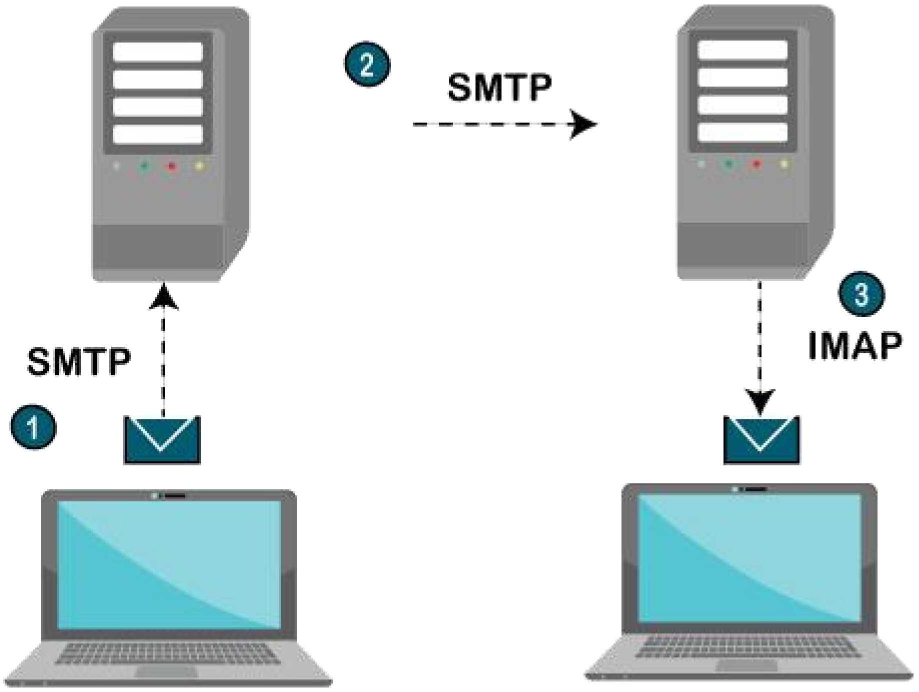


Internet Message Access Protocol (IMAP)

- Standard protocol for accessing email on a remote server from local client.
- Uses application layer protocol using underlying transport layer to establish host-host communication for applications.
- Also know as

  Interactive Mail Access Protocol OR
  Internet Mail Access Protocol OR
  Iterin Mail Access Protocol.

PORT NUMBER: 143



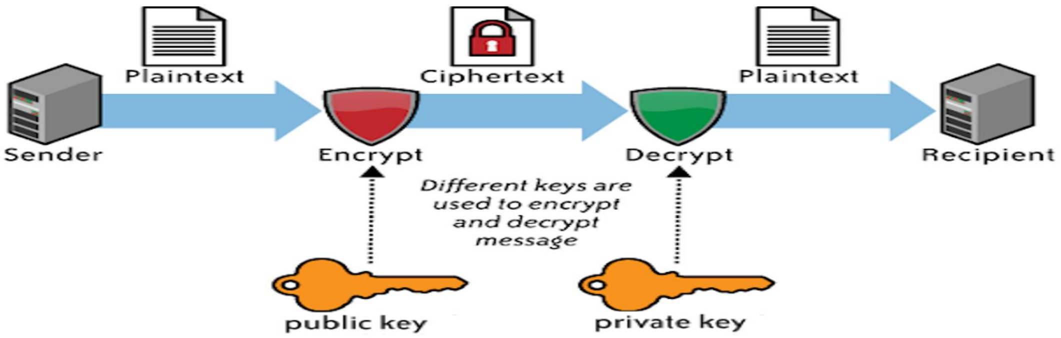
Secure Sockets Layer (SSL)

- Security protocol that provides privacy, authentication & integrity to internet connectivity.
- Eventually evolved into Transport Layer Security (TLS).
- Encryption based internet security protocol.
- Provides high privacy by encrypting data.
- Uses handshake b/w devices as authentication process.
- Digitally signs to provide data integrity & verify data is not tampered before receiving receiver.

http://domain.com
SSL
https://domain.com

Transport Layer Security (TLS)

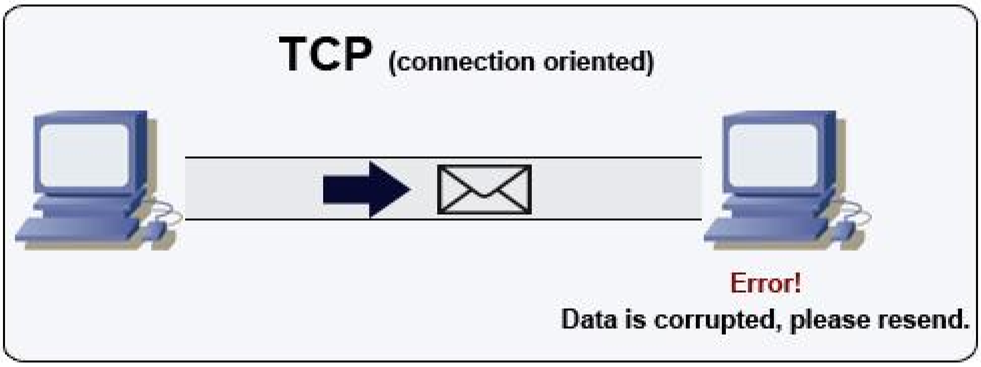
- Cryptographic protocol that provides end-end security of data sent b/w applications over internet.
- Implemented on top of TCP in order to encrypt application layer protocols such as HTTP, FTP, SMTP, IMAP.
- Also be implemented on DCP, DCCP, SCTP as well.
- Symmetric cryptography encrypts and decrypts data with a secret key that is known to sender and receiver.
- Typically uses 128 bit but 256 bit is preferable (less than 80 bit is unsecure).
- Assymetric cryptography uses public key & private key.
- Minimum key length is 1024 bit & 2048 bit is preferred.

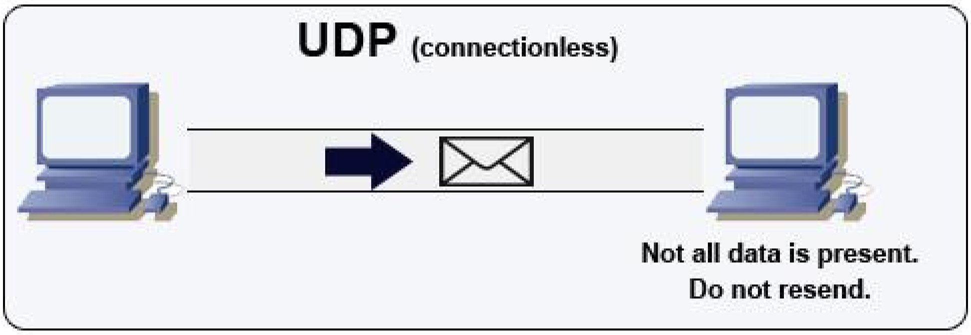


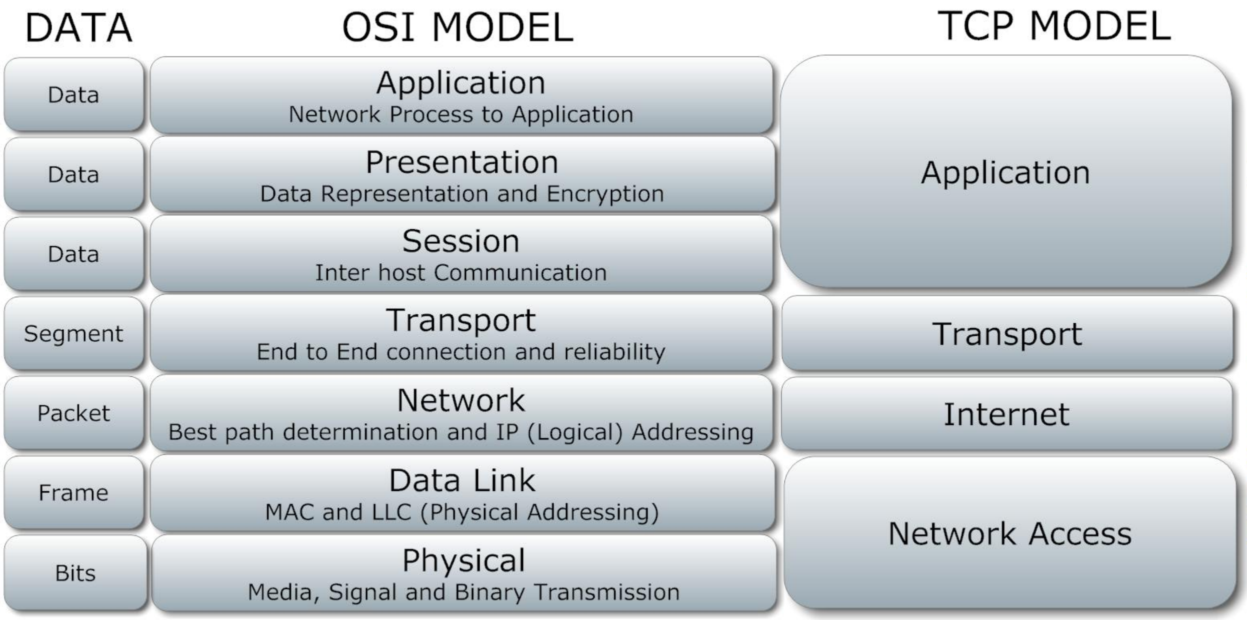
User Datagram Protocol (UDP)

- Part of Internet Protocol Suite referred as UDP/IP suite.
- Unreliable & connectionless protocol.
- No need to establish connection prior to data transfer.
- Used for real-time services like computer gaming, voice or video conference etc.
- Drop packets instead of processing delayed packets.
- More efficient interms of latency bandwidth.

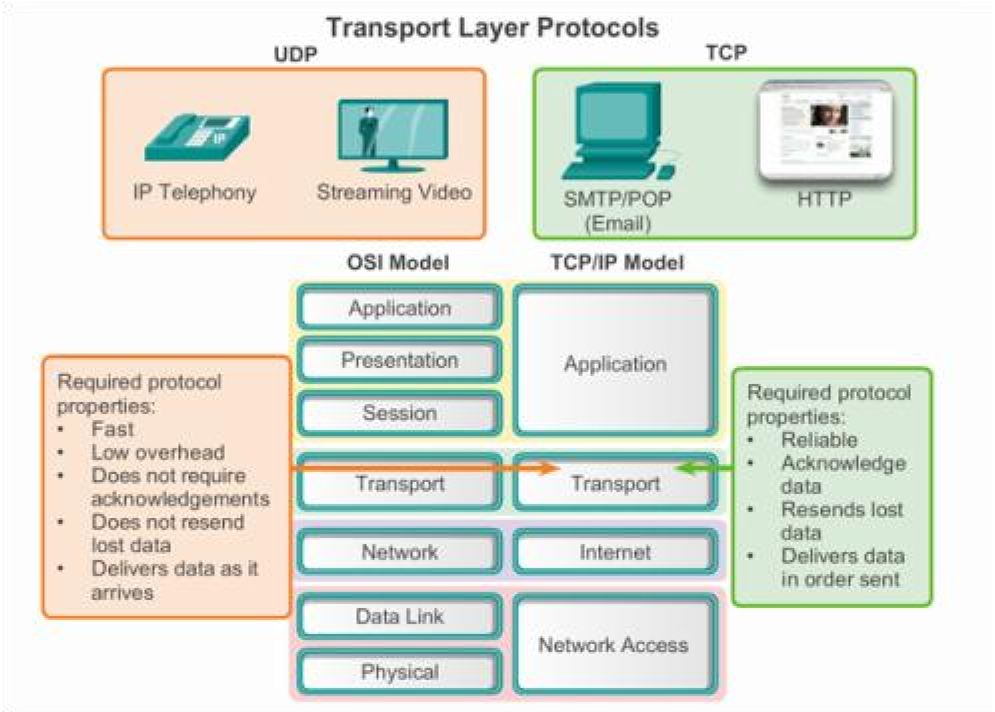
PORT NUMBER: 0 - 1023

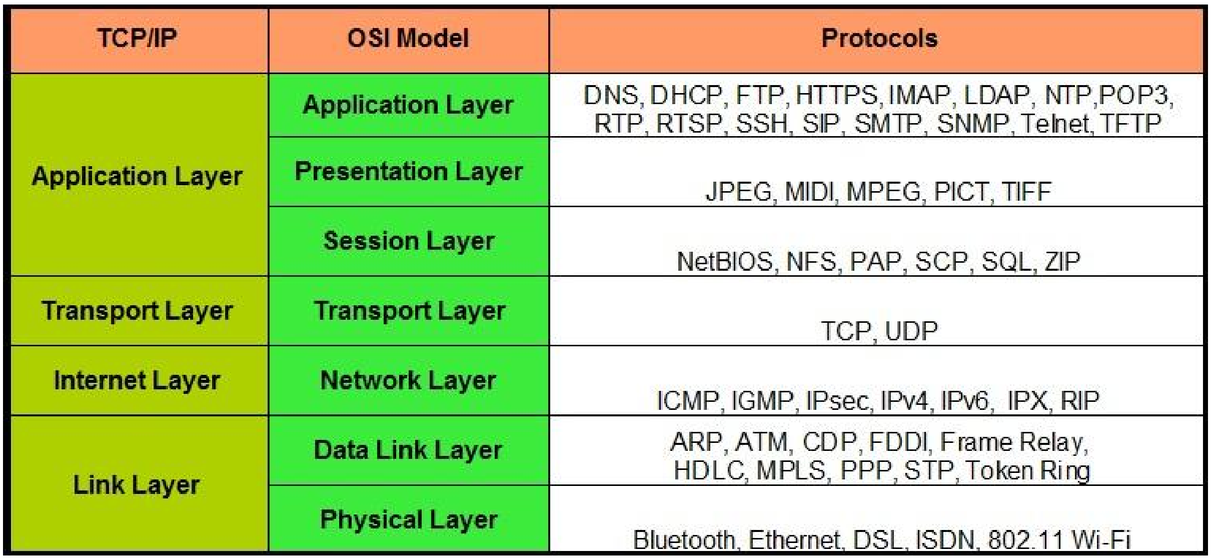






DATA	OSI MODEL	TCP MODEL
Data	Application Network Process to Application	Application
Data	Presentation Data Representation and Encryption	
Data	Session Inter host Communication	
Segment	Transport End to End connection and reliability	Transport
Packet	Network Best path determination and IP (Logical) Addressing	Internet
Frame	Data Link MAC and LLC (Physical Addressing)	Network Access
Bits	Physical Media, Signal and Binary Transmission	

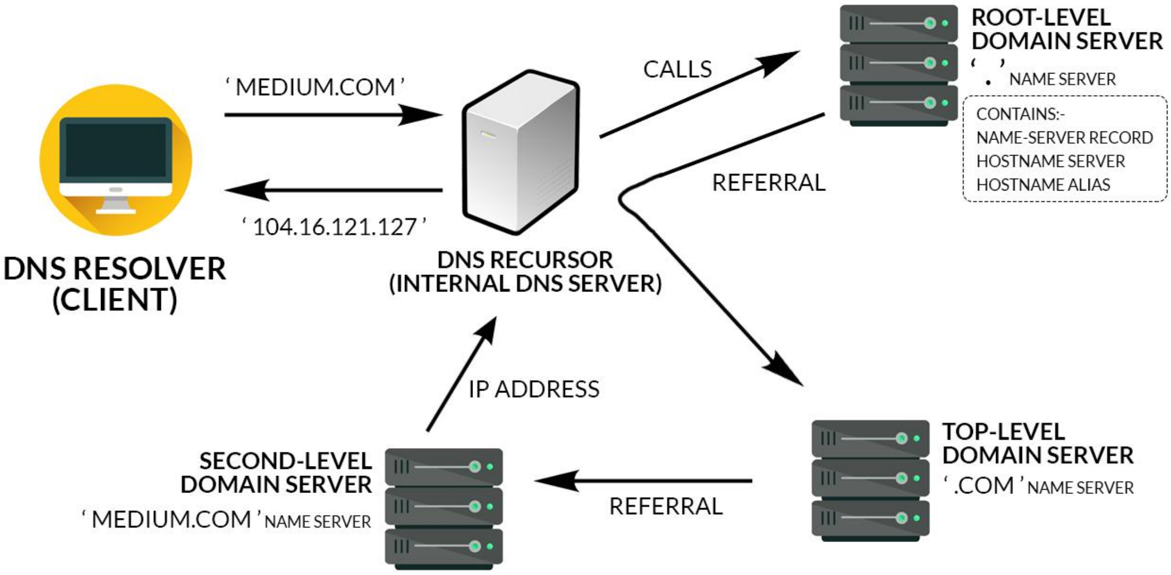




TCP/IP	OSI Model	Protocols
Application Layer	Application Layer	DNS, DHCP, FTP, HTTPS, IMAP, LDAP, NTP,POP3, RTP, RTSP, SSH, SIP, SMTP, SNMP, Telnet, TFTP
	Presentation Layer	JPEG, MIDI, MPEG, PICT, TIFF
	Session Layer	NetBIOS, NFS, PAP, SCP, SQL, ZIP
Transport Layer	Transport Layer	TCP, UDP
Internet Layer	Network Layer	ICMP, IGMP, IPsec, IPv4, IPv6, IPX, RIP
Link Layer	Data Link Layer	ARP, ATM, CDP, FDDI, Frame Relay, HDLC, MPLS, PPP, STP, Token Ring
	Physical Layer	Bluetooth, Ethernet, DSL, ISDN, 802.11 Wi-Fi

Domain Name Service (DNS)

www.xyz.com -> searches for default domain server -> searches domain name in domain name server -> when domain name is found -> locates ip address -> DNS return back ip address -> system uses ip address to fetch html page from location to download -> after downloading done -> web page is displayed in web browser.



Bare Metal

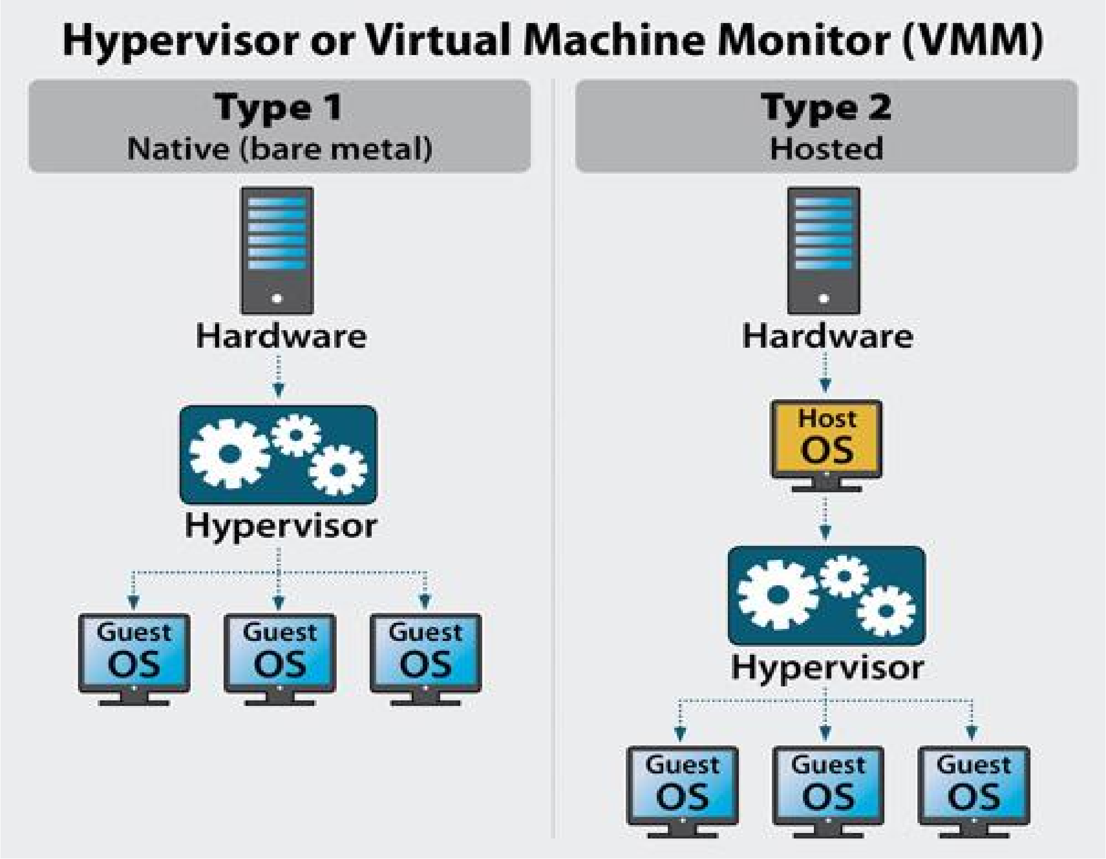
A bare-metal server is a computer server that hosts one tenant, or consumer, only. The term is used for distinguishing between servers that can host multiple tenants and which utilize virtualisation and cloud hosting. Such servers are used by a single consumer and are not shared between consumers. Each server may run any amount of work for a user, or have multiple simultaneous users, but they are dedicated entirely to the entity who is renting them. Unlike servers in a data center, they are not being shared between multiple customers. Bare-metal servers are physical servers. Each server offered for rental is a distinct physical piece of hardware that is a functional server on its own. They are not virtual servers running in multiple pieces of shared hardware.

Hypervisor

A hypervisor is a hardware virtualization technique that allows multiple guest operating systems (OS) to run on a single host system at the same time. The guest OS shares the hardware of the host computer, such that each OS appears to have its own processor, memory and other hardware resources.

Type 1: Also known as native or bare-metal hypervisors, these run directly on the host computer's hardware to control the hardware resources and to manage guest operating systems. Examples of Type 1 hypervisors include VMware ESXi, Citrix XenServer and Microsoft Hyper-V hypervisor.

Type 2: Also known as hosted hypervisors, these run within a formal operating system environment. In this type, the hypervisor runs as a distinct second layer while the operating system runs as a third layer above the hardware.



Web Error Codes

- 404 - Not Found
  -> Resource no longer available.
- 403 - Forbidden
  -> Access to resource is forbidden.
- 500 - Internal Server Error
  -> Server side error codes.
- 404 - Service Unavailable
  -> Web Server isn't available.
- 404 - Gateway Timeout
  -> Communication b/w proxy server & web server timeout.

HTTP and its associated secure HTTPS are the primary protocols for browsing on the web. Each web request results in a response with an associated status code.

Status codes fall into classes:

Informational Responses	**->**	**100 - 199**
Success responses	**->**	**200 - 299**
Redirection Responses	**->**	**300 - 399**
Client Error Responses	**->**	**400 - 499**
Server Error Responses	**->**	**500 - 599**