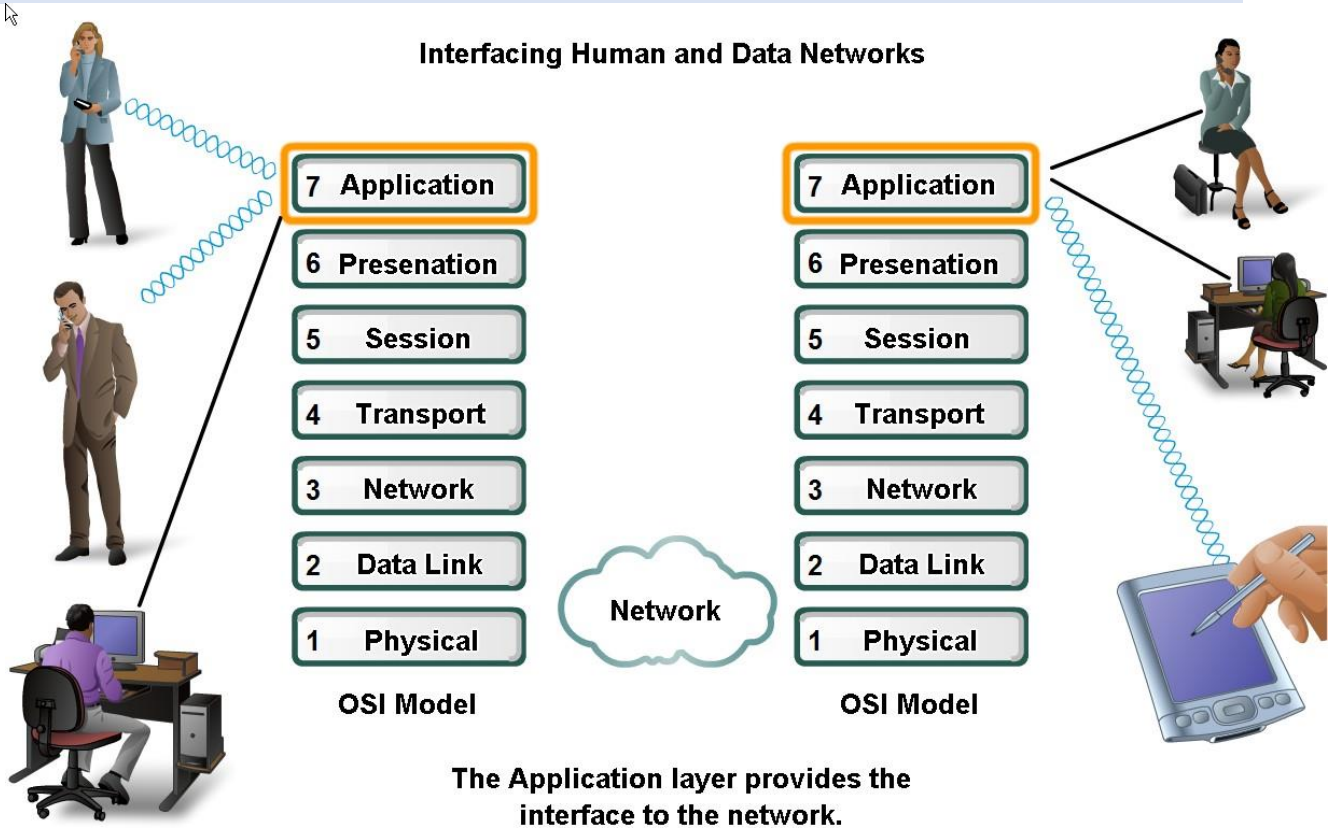
# Computer Networks Protocols

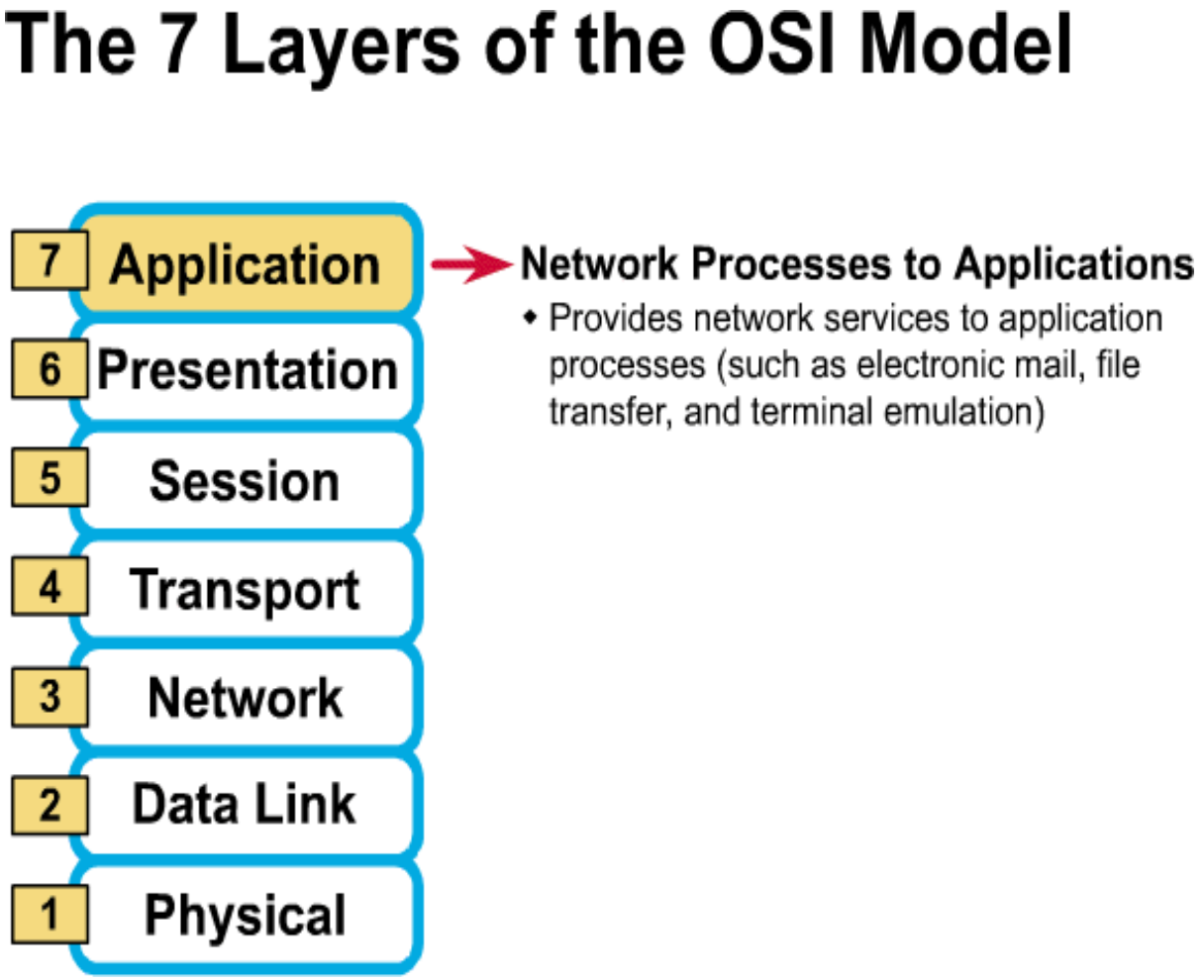
**2nd lecture**

Dr. Hasan Jawad



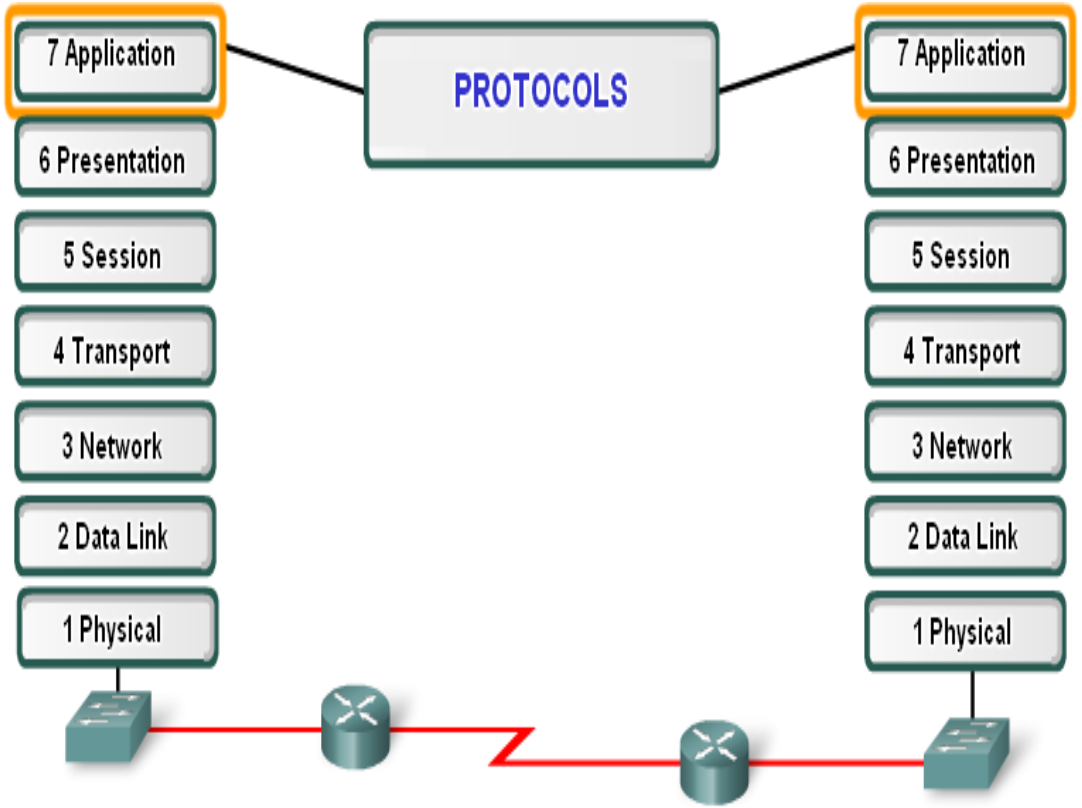
# 7. Application Layer

- Gives end-user applications access to network resources or allows users to interface with the network!



# Some of Applications layer protocols

- **DNS** – Matches domain names with IP addresses
- **HTTP** – Used to transfer data between clients/servers using a web browser
- **SMTP & POP3** – used to send email messages from clients to servers over the internet
- **FTP** – allows the download/upload of files between a client/server
- **Telnet** – allows users to login to a host from a remote location and take control as if they were sitting at the machine (virtual connection)
- **DHCP** – assigns IP addresses, subnet masks, default gateways, DNS servers, etc. To users as they login the network



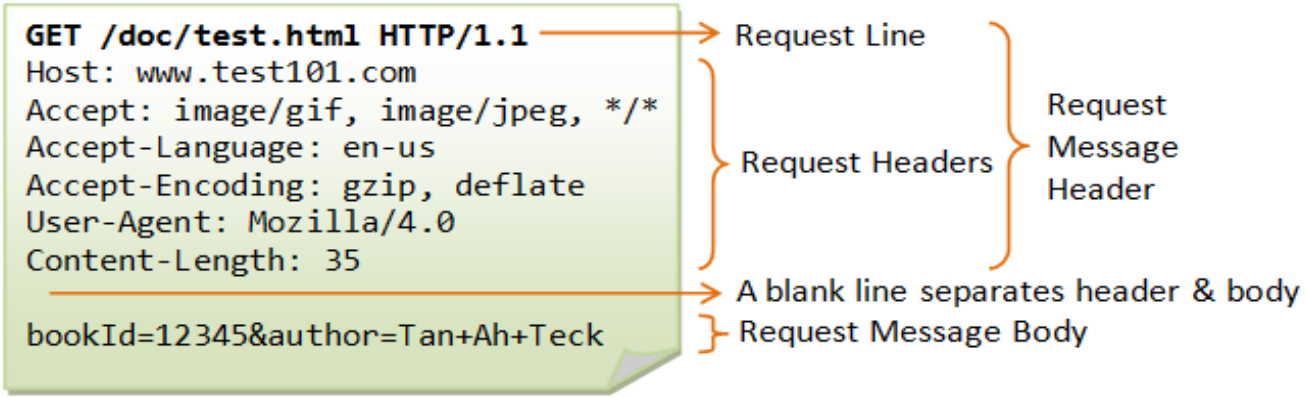

Application layer protocols provide the rules for communication between applications.

**Protocols:**

- Define processes on either end of the communication
- Define the types of messages
- Define the syntax of messages
- Define the meaning of any informational fields
- Define how messages are sent and the expected response
- Define interaction with the next lower layer

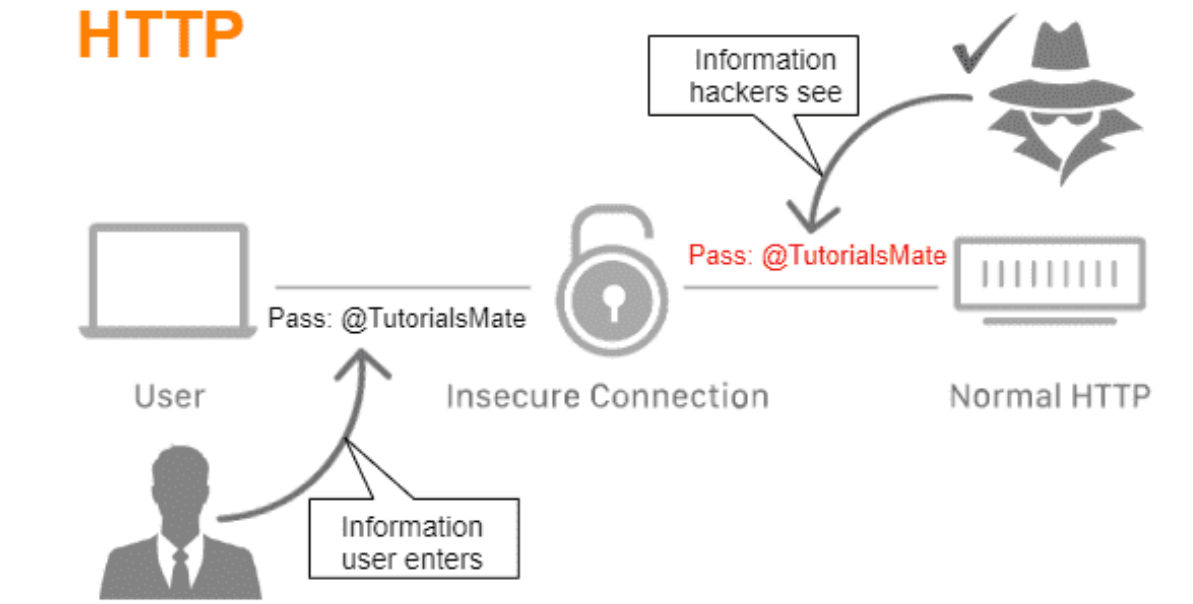
# Hypertext Transfer Protocol HTTP

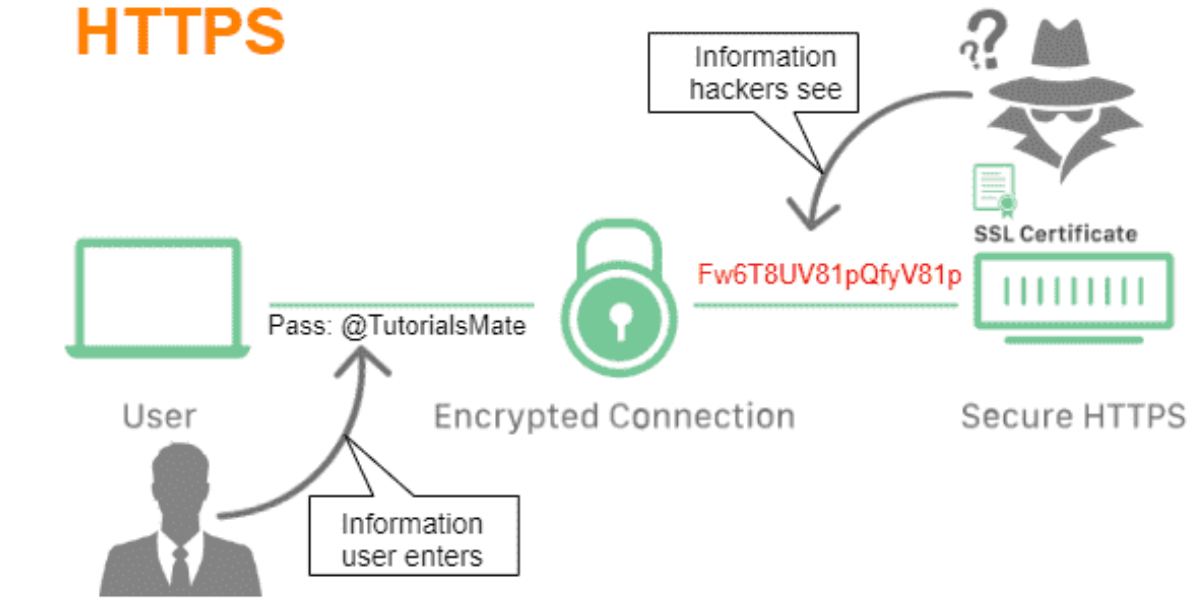
- HTTP is a simple request-response protocol that normally runs over TCP. It
- specifies what messages clients may send to servers and what responses they get back in return. The request and response headers are given in ASCII.
- HTTP is an application layer protocol because it runs on top of TCP and is closely associated with the Web.
- Because HTTP is an ASCII protocol, it is quite easy for a person at a terminal to directly talk to Web servers. All that is needed is a TCP connection to port 80 on the server.



# When HTTP is used over SSL, it is called **HTTPS** (**Secure HTTP**), even though it is the standard HTTP protocol.

- URL's beginning with HTTPS indicate that the connection is encrypted using Secure socket layer SSL.
- SSL builds a secure connection between two sockets, including
- *1. Parameter negotiation between client and s*
- *2. Authentication of the server by the client.*
- *3. Secret communication.*
- *4. Data integrity protection.*
- The new version of SSL is :**TLS** (**Transport Layer Security**)


HTTP
Information hackers see
Pass: @TutorialsMate
Pass: @TutorialsMate
User
Insecure Connection
Normal HTTP
Information user enters


HTTPS
Information hackers see
SSL Certificate
Fw6T8UV81pQfyV81p
Pass: @TutorialsMate
User
Encrypted Connection
Secure HTTPS
Information user enters

# File transfer protocol (FTP)

- It is the language that computers use to transfer files over a TCP/IP network.

FTP differs from other client-server applications in that it establishes two connections between the hosts. One connection is used for data transfer, the other for control information (commands and responses).

Separation of commands and data transfer makes FTP more efficient. The control connection uses very simple rules of communication. We need to transfer only a line of command or a line of response at a time. The data connection, on the other hand, needs more complex rules due to the variety of data types transferred. FTP uses two well-known TCP ports: Port 21 is used for the control connection, and port 20 is used for the data connection.

# E-mail

One of the most important services of internet is **electronic-mail.**
**Electronic mail**, commonly referred to as**e-mail**since1993,is a method of exchanging digital messages from a user to one or more recipients.
Some early email systems required both the users to be online at the same time.

## Post Office Protocol—Version 3 (POP3)

وكيل

POP3 is an extremely simple mail access protocol.
Because the protocol is so simple, its functionality is rather limited. POP3 begins when the user agent (the client) opens a TCP connection to the mail server on port 110. With the TCP connection established, POP3 progresses through three phases: **authorization, transaction, and update.**

Pop3 has two modes: keep mode and delete mode
In delete mode mail is deleted from mailbox after each retrieval.
In keep mode, mail remains in mailbox after each retrieval.

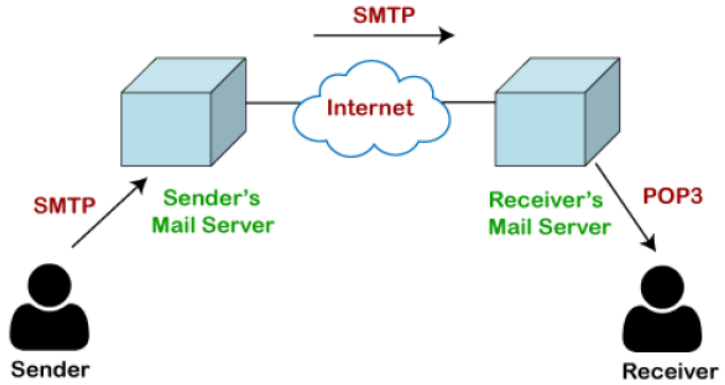
During the first phase, authorization, the user agent sends a username and a password to authenticate the user.

the user agent can mark messages for deletion, remove deletion marks, and obtain mail statistics.

The third phase, update, occurs after the client has issued the quit command, ending the POP3 session; at this time, the mail server deletes the messages that were marked for deletion.

Mail is usually downloaded to the user agent computer, instead of remaining on the mail server. This makes life easier on the server, but harder on the user. It is not easy to read mail on multiple computers, plus if the user agent computer breaks, all email may be lost permanently. Nonetheless, you will still find POP3 in use.

# Simple Mail Transfer Protocol (SMTP)




is at the heart of Internet electronic mail , SMTP transfers messages from senders' mail servers to the recipients' mail servers. SMTP is much older than HTTP.

SMTP is the principal **application-layer** protocol for Internet electronic mail. It uses the reliable data transfer service of TCP to transfer mail from the sender's mail server to the recipient's mail server.

SMTP has two sides: a client side, which executes on the sender's mail server, and a server side, which executes on the recipient's mail server. Both the client and server sides of SMTP run on every mail server. When a mail server sends mail to other mail servers, it acts as an SMTP client. When a mail server receives mail from other mail servers, it acts as an SMTP server.

**We now describe each of these components in the context of a sender, Alice, sending an e-mail message to a recipient, Bob.**

1. Alice invokes her user agent for e-mail, provides Bob's e-mail address (for example, `bob@someschool.edu`), composes a message, and instructs the user agent to send the message.

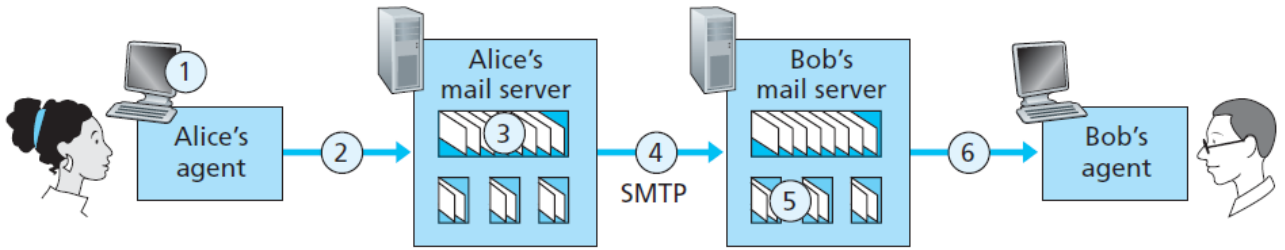
2. Alice's user agent sends the message to her mail server, where it is placed in a message queue.

3. The client side of SMTP, running on Alice's mail server, sees the message in the message queue. It opens a TCP connection to an SMTP server, running on Bob's mail server.

4. After some initial SMTP handshaking, the SMTP client sends Alice's message into the TCP connection.

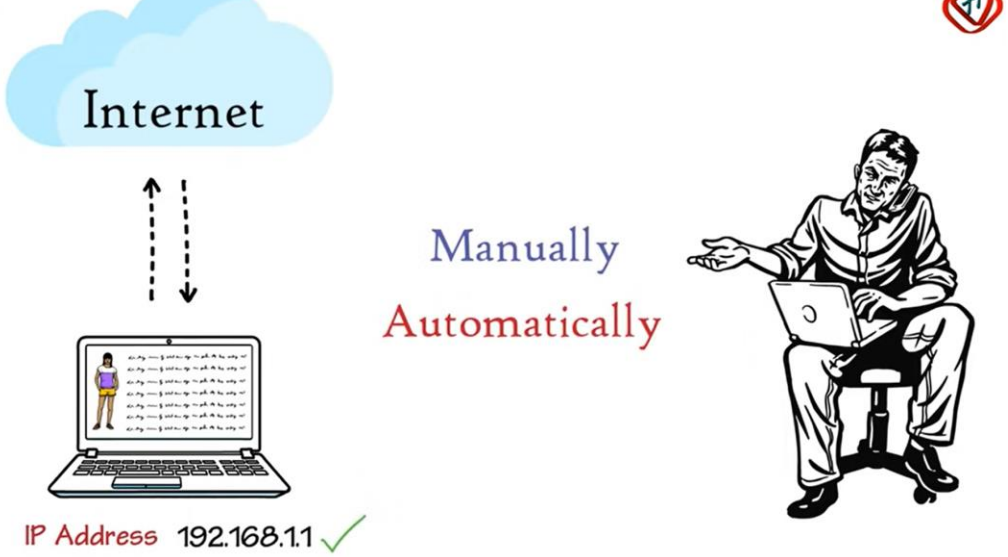
5. At Bob's mail server, the server side of SMTP receives the message, Bob's mail server then places the message in Bob's mailbox.

6. Bob invokes his user agent to read the message at his convenience.




Key:

# Dynamic Host Configuration Protocol (DHCP)




is an **application layer protocol**

- allows a host to obtain an IP address automatically. A network administrator can configure DHCP so that a given host receives the same IP address each time it connects to the network, or a host may be assigned a **temporary IP address** that will be different each time the host connects to the network.
- In addition to host IP address assignment, DHCP also allows a host to learn additional information, such as its subnet mask and default gateway.
- every network must have a DHCP server that is responsible for configuration.

# Benefits of DHCP

DHCP provides a range of benefits to network administrators:

1. **Reliable IP address configuration**

- You can't have two users with the same IP address because it would create a conflict where one or both devices could not connect to the network.

2 . **Reduced network administration**

- DHCP provides centralized and automated TCP/IP configuration. By deploying a DHCP relay agent, a DHCP server is not needed on every subnet.

3. **Mobility** – امكانية التنقل

- DHCP efficiently handles IP address changes for users on portable devices who move to different locations on wired or wireless networks.

4. **IP address optimization** – تحسين

- DHCP not only assigns addresses, it automatically takes them back and returns them to the pool when they are no longer being used.

5. **Efficient change management**

- DHCP makes it simple for an organization to change its IP address scheme from one range of addresses to another.

## Lease

The length of time for which a DHCP client holds the IP address information is known as the lease. When a lease expires, the client must renew it.

- **Controlling lease time**

- If all DHCP did was assign IP addresses permanently, it wouldn't be dynamic, it would be static. Static addresses are appropriate for some devices, such as network printers. However, under the DHCP protocol, every time the DHCP server assigns an address there is an associated lease time. When the lease expires, the client can no longer use the IP address and is essentially kicked off the network.

- The protocol is designed so active clients automatically contact the DHCP server halfway through the lease period to renew the lease. If the server doesn't respond immediately, the client continues to ask the DHCP server for a lease renewal until it is approved.

- Typically, when a host shuts down, the lease is automatically terminated, in order to free up its IP address so it can be used by another client on the network.