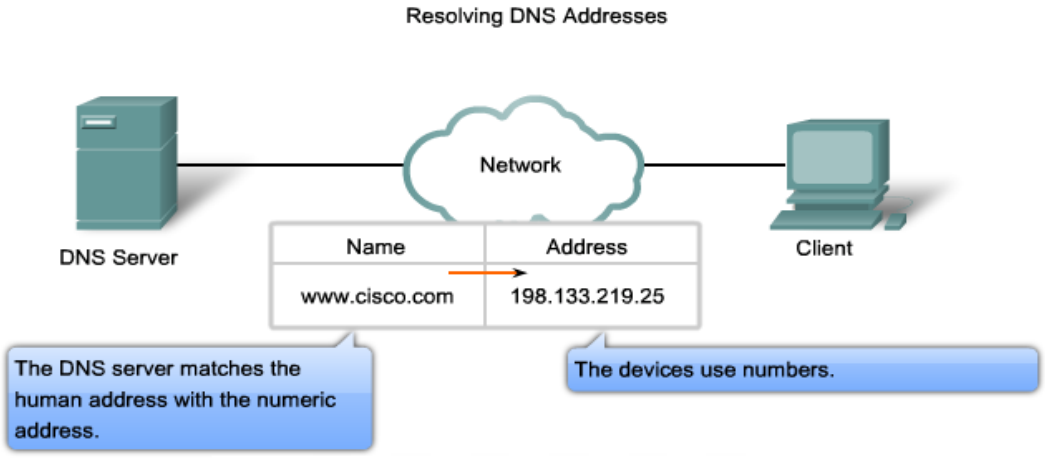
Application Layer

Domain Name Service (DNS)

- DNS is a client-server application that identifies each host on the Internet with a **unique user-friendly name.**
- The names must be unique because the addresses are unique.
- DNS Servers resolve names to IP addresses. It would be difficult to remember the IP address of every website we like to visit, but we can remember names.



HOW DNS Work?

- One DNS server can't response to all of the demands that coming from all over the world.
- The problem is how we can **distribute the traffic among** more DNS servers, this problem solved by Domain Name Space.

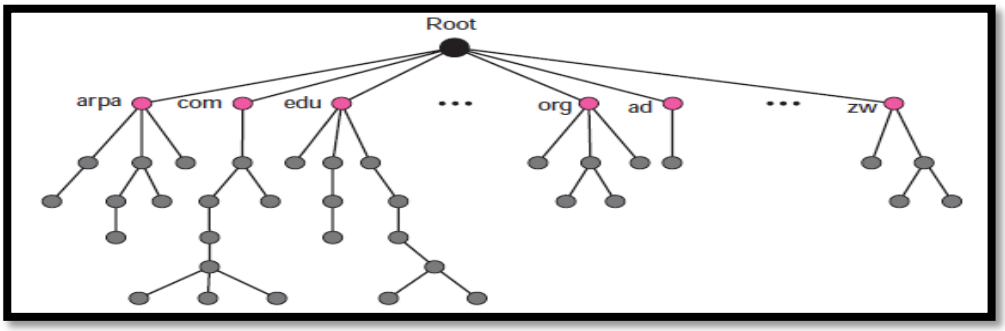
Types of Domain Name Space

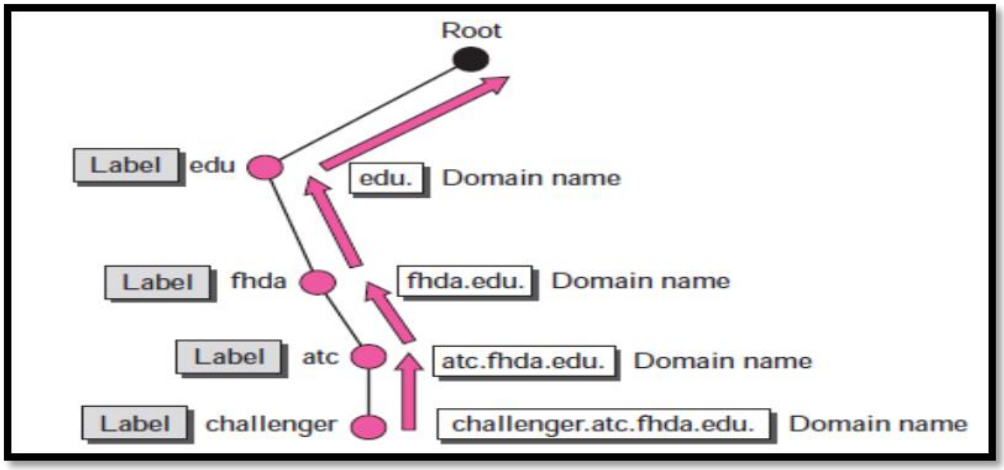
1. **Flat name space**: a name is assigned to an address. A name in this space is a sequence of characters without structure. **Don't use in Internet because there is no centrally controlled.**
2. **Hierarchical name space: each name is made of several parts.** The first part can define the nature of the organization, the second part can define the name of an organization, and the third part can define departments in the organization. **Used at internet.**

Hierarchical Domain name space(structure)

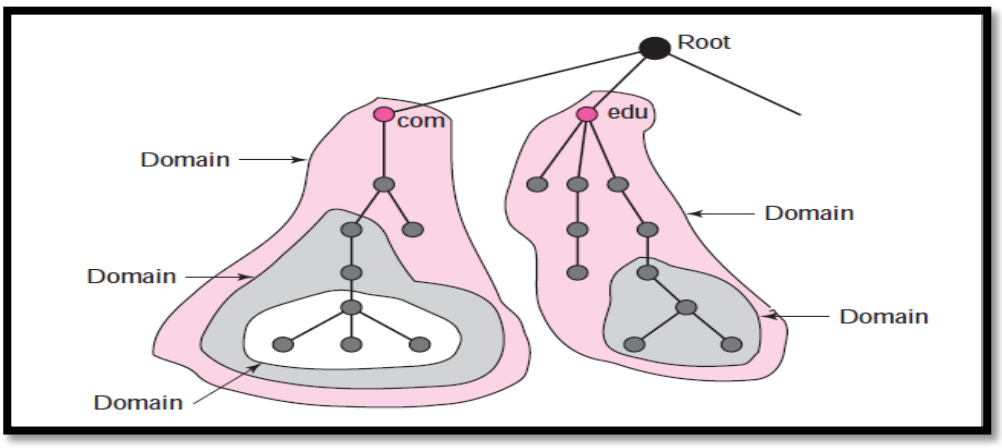
- DNS organizes the name space in a **hierarchical** structure to **decentralize** the responsibilities involved in naming. Distributed the traffic between more than one DNS server.
- hierarchical tree structure with **one root**

- The tree can have only 128 levels: level 0 (root) to level 127.

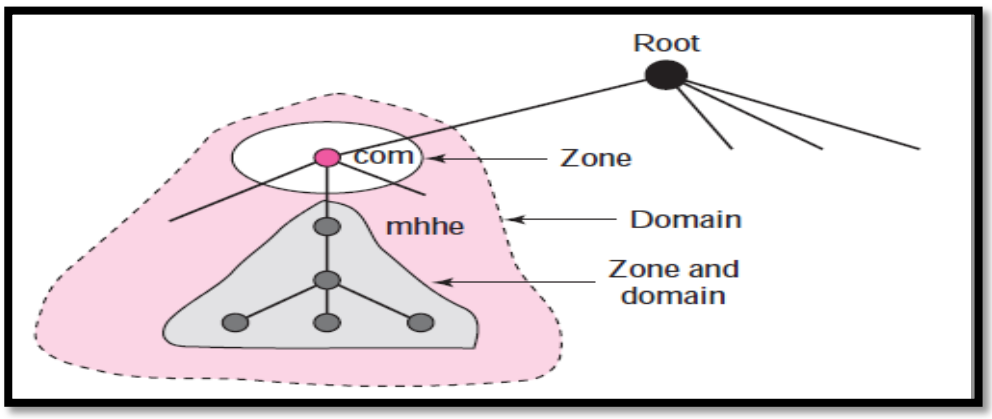




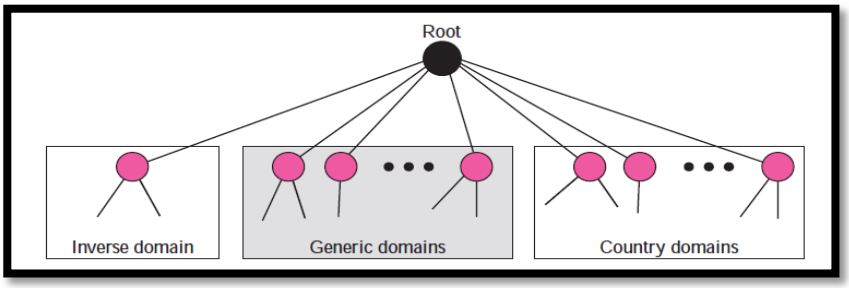
- **A domain** is a sub tree of the domain name space.



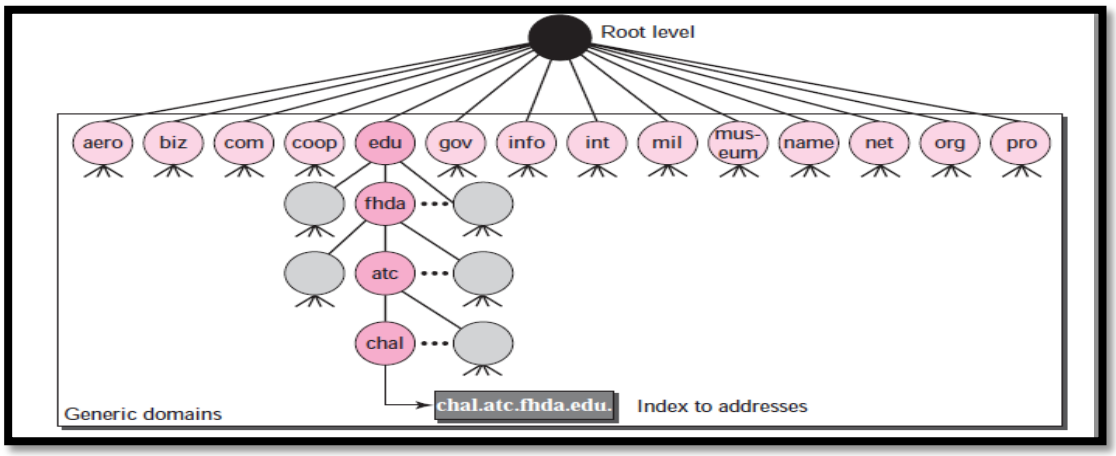
- **Zone in name space**



- **DNS In The Internet**

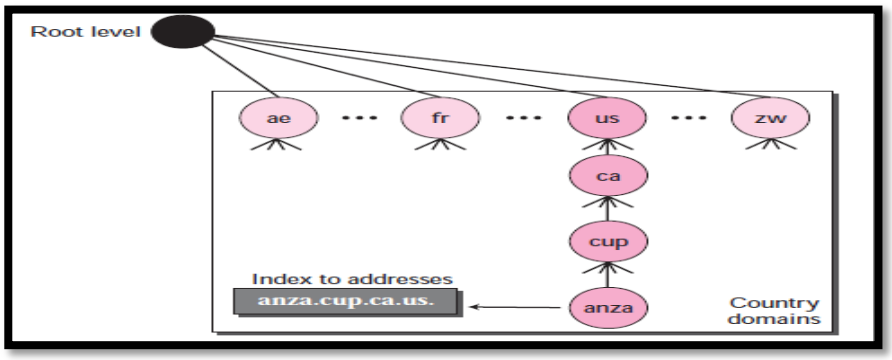


- **<u>Generic domains</u>: There** are fourteen generic domains, each specifying an organization type.



Label	*Description*
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
museum	Museums and other non-profit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

- **Country domains** (uses **two character** country abbreviations, Second labels can be organizational and so on)



E-mail Services and SMTP/POP protocols

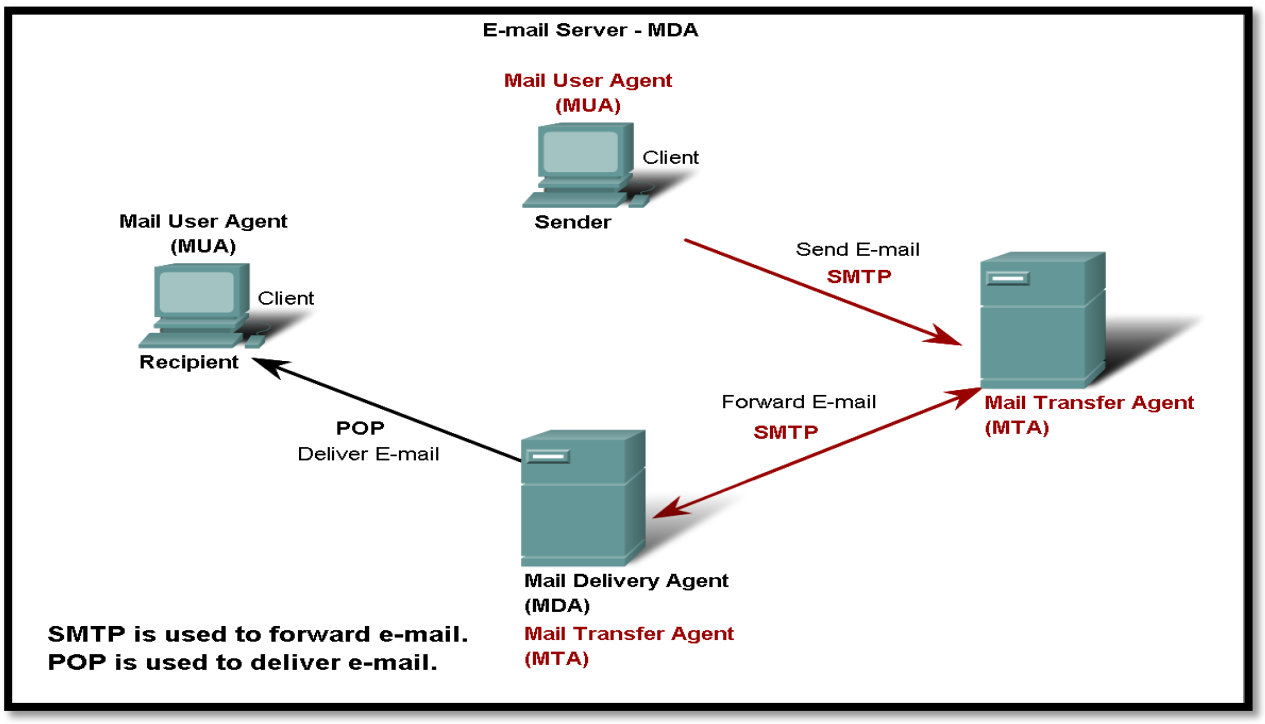
- E-mail is the most popular network **service.**
- E-mail **client** (when people compose e-mail) is called Mail User Agent (**MUA**)
- MUA **allows** messages to be **sent/retrieved** to and from your mailbox
- Requires several applications and services:
  - **POP or POP3** – deliver email from server to client (incoming messages) post office prot.
  - **SMTP** – handles outbound messages from clients

E-mail Services and SMTP/POP protocols

What do servers require?

1) Must be running SMTP.
2) Also operates
   - Mail Transfer Agent (**MTA**) – used to forward email
   - Receives email from the clients **MUA**
   - Uses SMTP to **route email** between SERVERS
   - Passes email to the **MDA** for final delivery

3) For two e-mail servers to talk – MUST run SMTP and MTA in order to transfer mail between the 2 servers!

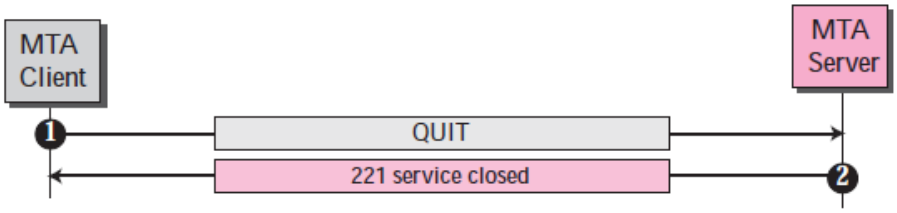


Commands and Responses

- SMTP uses **commands and responses** to transfer messages between an MTA client and an MTA server.
- The mail server is called an ***SMPT client when sending message*** and ***SMPT server when receiving message***.

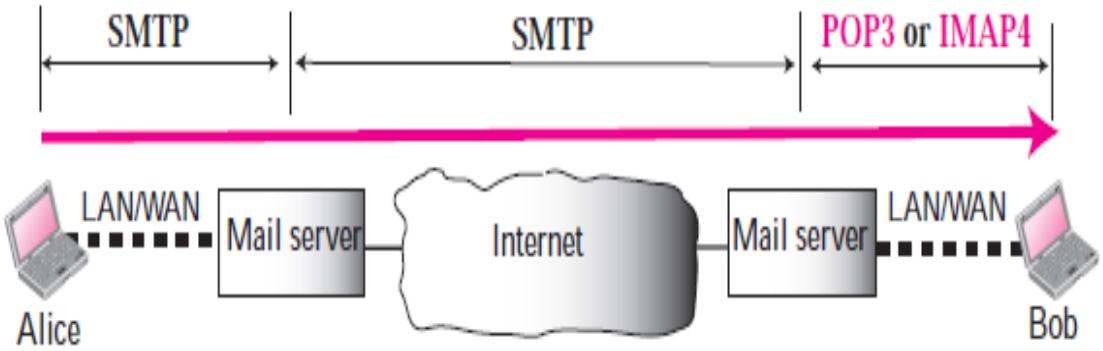
- **Commands are sent from the client to the server.**
  1. **HELO.**
  2. **MAIL FROM.**
  3. **RCPT TO.**
  4. **DATA.**
  5. **QUIT.**

- **Connection Termination**



Message Access Agent: POP and IMAP

As shown in the figure bellow, the **first** and the **second** stages of mail delivery use **SMTP**. However, **SMTP is not involved in the third stage** because **SMTP is a push protocol**; **it pushes the message from the client to the server**.

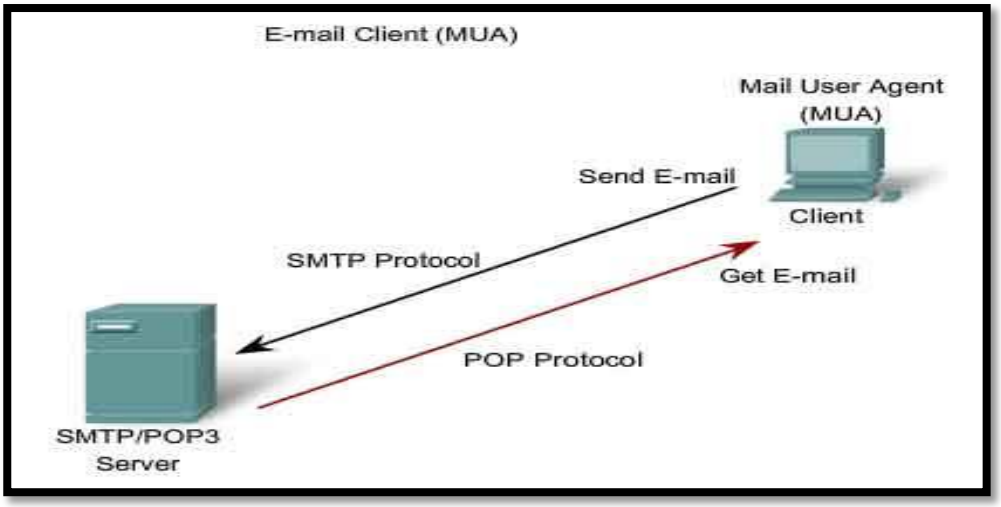


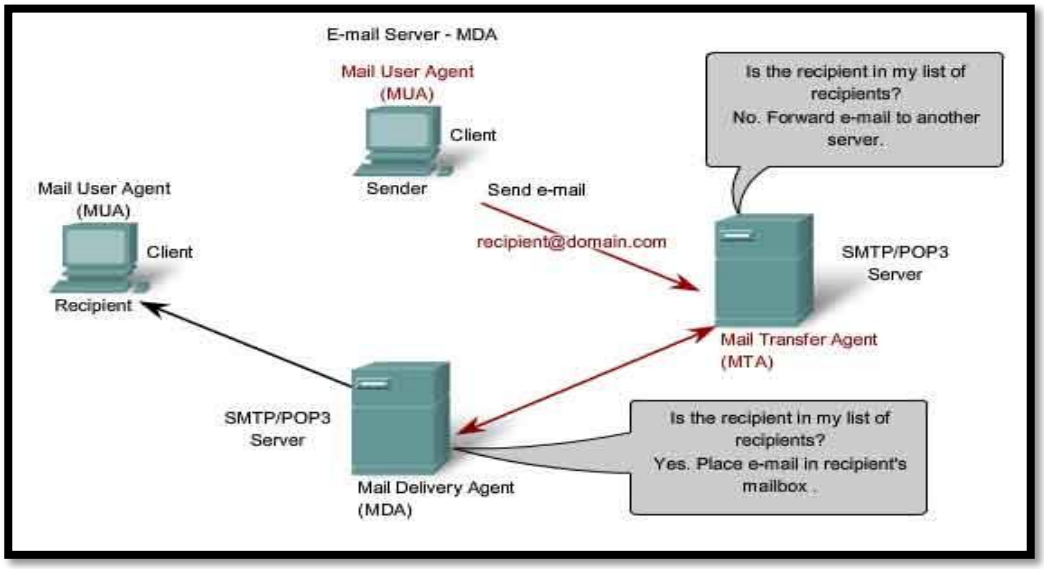
E-mail Server Processes - MTA and MDA and the SMTP protocol

The e-mail server operates two separate processes:

1. Mail Transfer Agent (MTA)
2. Mail Delivery Agent (MDA)

- The **Mail Transfer Agent (MTA)** process is used to **forward e-mail**.
- The MTA receives messages from the **MUA (client)** or from another MTA on another e-mail server.
- Based on the message header, it determines how a message has to be forwarded to reach its destination.
- **If the mail is addressed to a user whose mailbox is on the local server, the mail is passed to the MDA (POP or IMAP). If the mail is for a user not on the local server, the MTA routes the e-mail to the MTA on the appropriate server.**





File Transfer Protocol (FTP)

- Commonly used application layer protocol
- Used for the **transfer of files between clients/servers** model architecture.
- **Requires two connections to the server**
    1. **Control connection**: control connection is used for opening / closing an FTP session and for transferring commands from client to server uses TCP port 21(This connection is kept alive as long as the client keeps FTP session active).
    2. **Data Connection:** The data connection is used for transferring individual files between client and server uses TCP port 20 (This connection is kept alive for the duration of one file transfer).

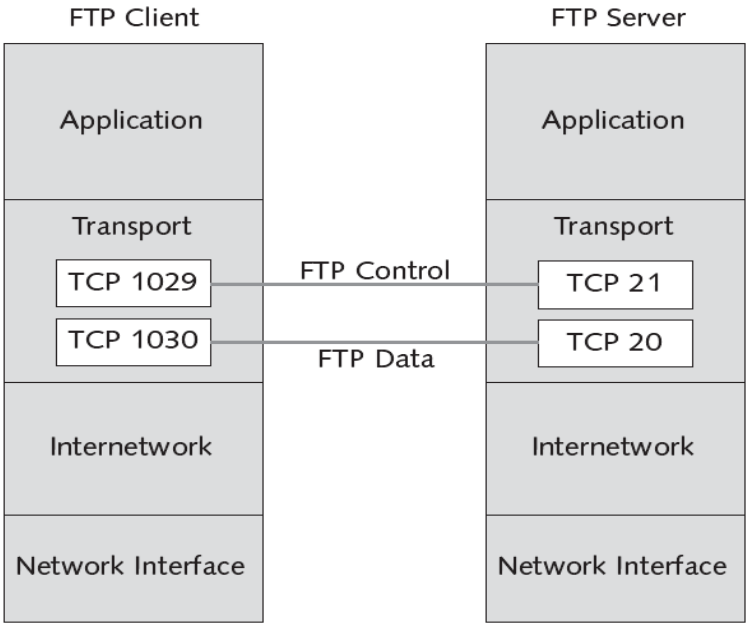
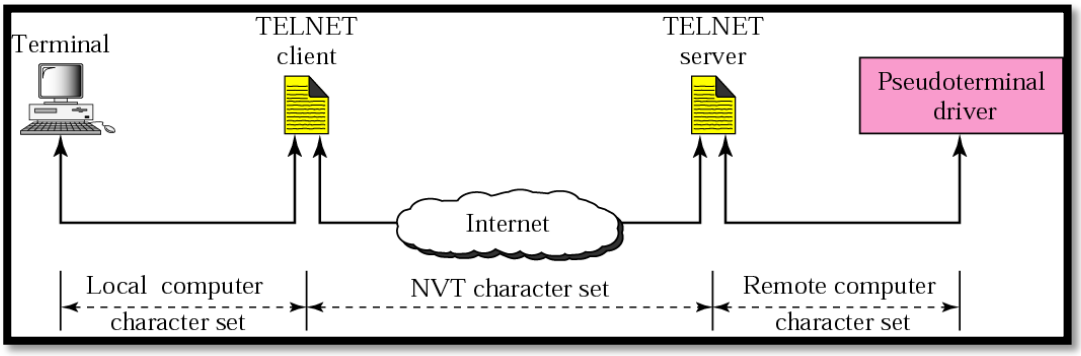


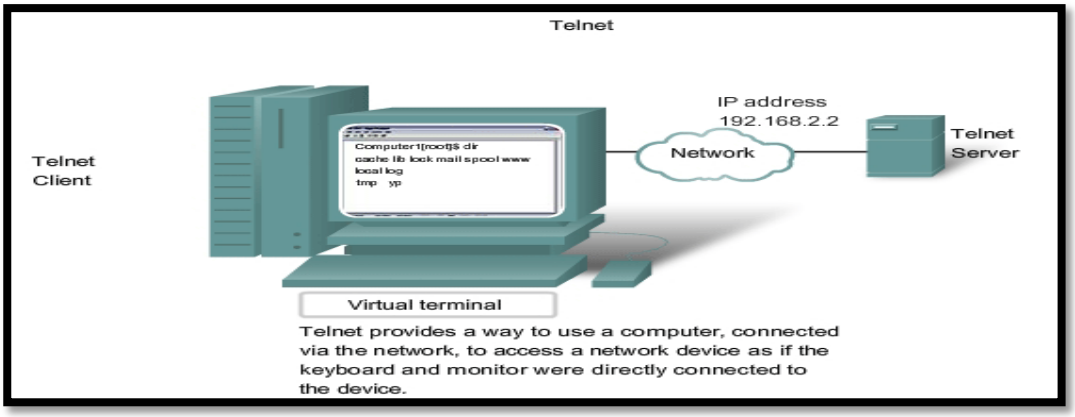
Figure 3-2 TCP port usage in FTP communications

Telnet

TELNET is a protocol allowing you to **connect to remote computers**. TELNET uses a client/server model. It has the following features:

- **Allows users to emulate text-based terminal devices over the network using software**.
- A connection is known as a **Network Virtual Terminal** session.
- Can be **run from the command prompt** on a PC.
- You can use the device as if you were sitting there with all the **rights and priorities** that you username will offer you.
- **Disadvantages: Doesn't support encryption like SSH. All data is transferred as plain text. It can be easily intercepted and understood.**
- If security is a concern, you should use Secure Shell (SSH) protocol. Provides for remote logins with stronger authentication than telnet.

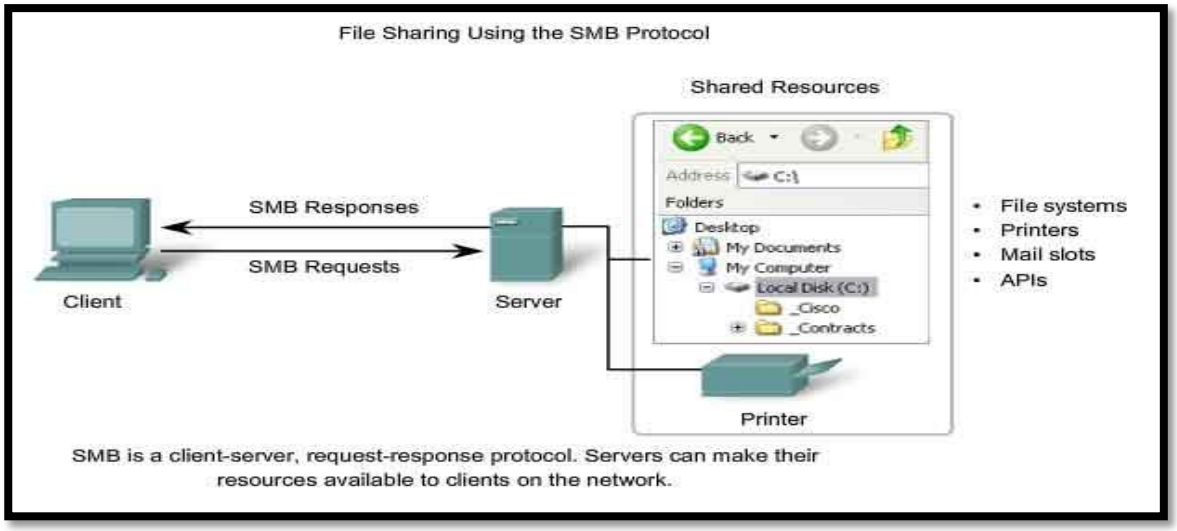




File Sharing Services and SMB Protocol

- The Server Message Block (SMB) is a **client/server file sharing protocol**.
- SMB has become a mainstay of Microsoft networking, even more so since the introduction of Windows 2000 software.

- **Allows servers to share their resources with clients.**
- Linux and UNIX also share with Microsoft networks using a version of SMB called SAMBA.
- Apple also supports sharing resources using an SMB protocol
- What can SMB do?
    1. **Start, authenticate, and terminate sessions.**
    2. **Control file and printer access.**
    3. **Allow applications to send/receive messages to/from another device.**



Secure Shell Protocol (SSH)

- The Secure Shell (SSH) protocol is a method for **secure remote login** from one computer to another.
- It protects the communications with strong encryption.
- SSH, **like** TELNET, uses TCP as the underlying transport protocol, but SSH is **more secure** and provides **more services** than TELNET. These services are:
    1. Covers authentication, encryption.
    2. Solve the security issues at remote login of Telnet.
    3. Solve the security issues during file transfer at FTP

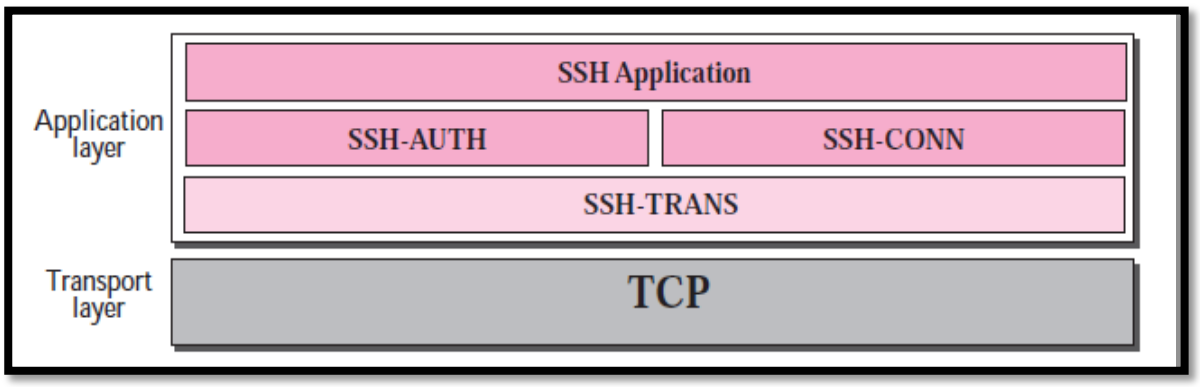
- There are two versions of SSH: **SSH-1** and **SSH-2**, which are totally incompatible.
- The first version, SSH-1 is now deprecated because of security problems in it.
- SSH is a proposed application-layer protocol with four components.

Q/ Compare between SSL and SSH?

SSL	SSH
is **TCP**-based and always used in **WEB applications**, with HTTP.	is **TCP**-based and always used with **Telnet** and **FTP**

SSH-2 Components

SSH is organized as three protocols (**components**) that typically run on top of TCP, these are:



SSH Transport-Layer Protocol (SSH-TRANS)

This protocol is responsible about:

- Privacy or confidentiality of the message exchanged.
- Data integrity.
- Server authentication.
- Compression of the messages that improve the efficiency of the system and make attack more difficult.

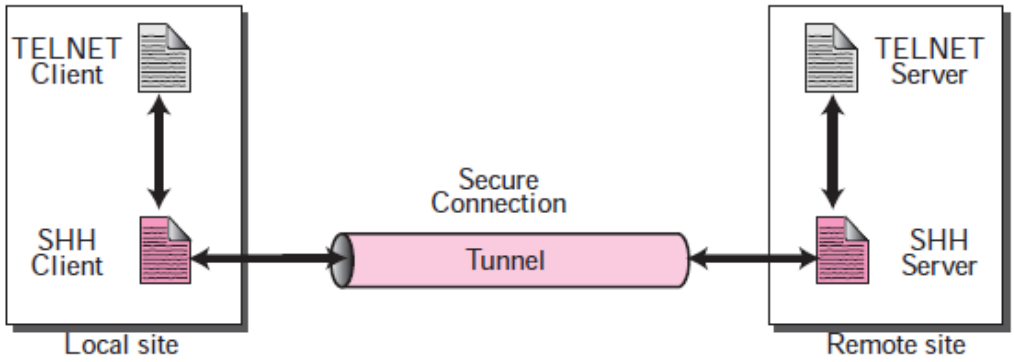
SSH Authentication Protocol (SSH-AUTH)

- After a secure channel is established between the client and the server, **the server is authenticated for the client**, SSH can call software that can authenticate the client for the server.
- **The Connection Protocol [SSH-CONNECT]:** multiplexes the encrypted tunnel into several logical channels. It runs over the user authentication protocol.

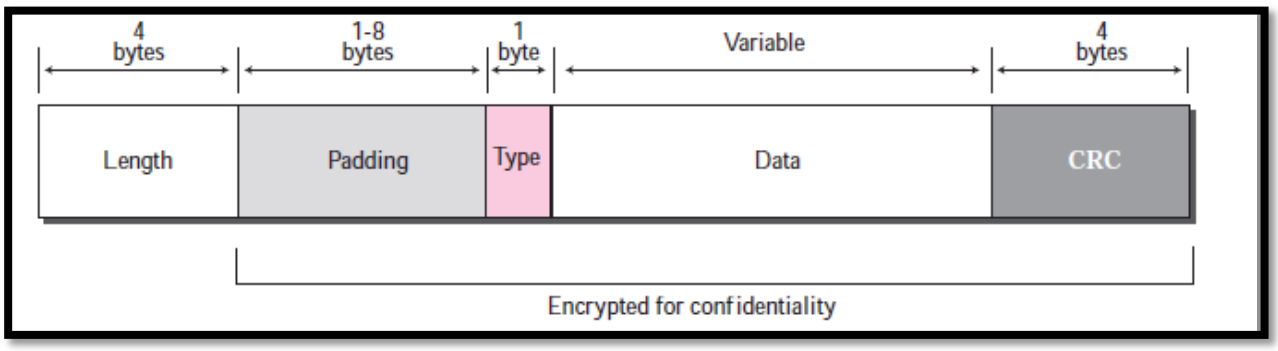
SSH Applications

- Remote login
- file transfer

Port Forwarding



Format of the SSH Packets



- **Length:** This 4-byte field defines the length of the packet including the type, the data, and the CRC field, but not the padding and the length field.
- **Padding**: One to eight bytes of padding is added to the packet to make the attack on the security provision more difficult.
- **Type:** This one-byte field defines the type of the packet used by SSH protocols.
- **CRC:** The cyclic redundancy check filed is used for **error detection**.