Introduction to Data Communications and Networks

(CYB 204)

Application Layer

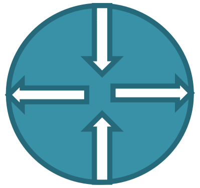
Egena Onu, Ph.D.

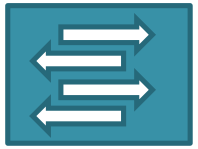
Department of Computer Science

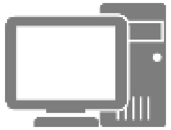
Bingham University

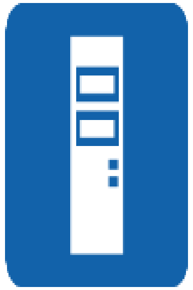
Karu.

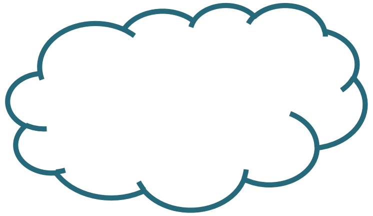
Icons

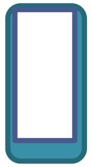

Router


Switch

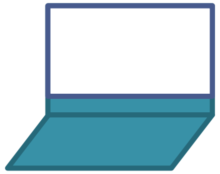

Desktop Computer


Server


Internet/Cloud


Mobile Device

Clock


Laptop

Introduction

- The application layer is the highest layer in the protocol suite.
- The application layer provides services to the user.
- Communication is provided using a logical connection, which means that the two application layers assume that there is an imaginary direct connection through which they can send and receive messages.
- The application layer is the only layer that provides services to the Internet user
- The application layer exchange messages with their peers on other machines
- Applications need their own protocols. These applications are part of network protocol.

Network Application Software

- A network application is a software program or service that relies on network resources to perform specific functions, enabling communication, information sharing, and collaboration among devices connected to a network.

- Network applications are distributed in the sense that their complete functionality depends on the co-operation of many separate devices that can be in different locations.

- These applications leverage the power of networks, whether local area networks (LANs), wide area networks (WANs), or the internet, to provide various services and functionalities.

- Network applications use network protocols and communication standards to transmit and receive data, making them integral to modern computing.

- Whether you’re browsing the web, sending emails, sharing files, or engaging in video conferences, you’re likely using network applications that seamlessly bridge the gap between your device and the broader networked world.

- Network applications can be written in any programming language, such as C++, C, C#, Python, Java, etc.

- An application is also called a process.

Network Application Software

- Types of Network Applications
  - There are several types of network applications, each designed to serve specific purposes and meet diverse communication and data-sharing needs:

1. Web Browsers:
   - Google Chrome, Mozilla Firefox, Microsoft Edge
   - Web browsers allow users to access and navigate websites and web-based applications over the internet. They use network protocols such as HTTP and HTTPS to retrieve web content.

2. Email Clients:
   - Microsoft Outlook, Apple Mail, Gmail
   - Email clients facilitate the sending, receiving, and management of email messages over email servers, typically using protocols like SMTP, IMAP, and POP3.

3. File Transfer Protocols:
   - FTP (File Transfer Protocol), SFTP (Secure File Transfer Protocol)
   - These applications enable the transfer of files between devices and servers. FTP and SFTP ensure secure and efficient file exchange over networks.

Network Application Software

- Types of Network Applications

4. Messaging Apps:
   - Applications such as WhatsApp, Slack, Microsoft Teams are considered as messaging appliations.
   - Messaging applications allow real-time text, voice, and video communication between individuals and groups, enhancing collaboration and connectivity.

5. Video Conferencing Tools:
   - Zoom, Microsoft Teams, Cisco Webex
   - Video conferencing applications enable virtual meetings, webinars, and remote collaboration through live video and audio communication.

6. Remote Desktop Applications:
   - TeamViewer, AnyDesk, Remote Desktop Protocol (RDP)
   - These applications allow users to access and control remote computers over a network, facilitating technical support, troubleshooting, and remote work.

Network Application Software

- Importance of Network Applications
- Network applications play a pivotal role in today's interconnected world for several reasons:

1. Enhanced Connectivity:
   - Network applications enable individuals and organizations to connect and communicate seamlessly, bridging geographical distances and fostering collaboration.

2. Data Sharing and Accessibility:
   - They facilitate the sharing and access of data and resources, promoting efficient information exchange and decision-making.

3. Streamlined Workflow:
   - Network applications automate processes, reducing manual tasks and enhancing productivity across various industries.

Network Application Software

- Importance of Network Applications

4. Improved Communication
   - These applications offer real-time communication channels, supporting video conferencing, instant messaging, and email, which are essential for business operations and personal interactions.

5. Remote Work and Flexibility
   - Network applications empower remote work by providing secure access to corporate resources, enabling businesses to adapt to changing work environments.

6. Scalability and Growth
   - As businesses expand, network applications can scale to accommodate increased demands, ensuring they remain effective tools for communication and collaboration.

Network Application Software

- Network Application Architecture
  - Application architecture is different from the network architecture.
  - The network architecture is fixed and provides a set of services to applications.
  - The application architecture, on the other hand, is designed by the application developer and defines how the application should be structured over the various end systems.
  - There are two types of application architecture:
    - Client-Server
    - Peer-to-Peer (P2P)

Network Application Software

- Network Application Architecture
  - Client-server architecture
    - An application program running on the local machine that sends a request to another application program is known as a client, and a program that serves a request is known as a server.
    - For example, when a web server receives a request from the client host, it responds to the request to the client host.

Network Application Software

- Network Application Architecture
  - Characteristics of Client-server architecture:
    - In Client-server architecture, clients do not directly communicate with each other. For example, in a web application, two browsers do not directly communicate with each other.
    - A server is a fixed, well-known address known as IP address because the server is always on while the client can always contact the server by sending a packet to the sender's IP address
  - Disadvantage Of Client-server architecture
    - It is a single-server based architecture which is incapable of holding all the requests from the clients. For example, a social networking site can become overwhelmed when there is only one server.

Network Application Software

- Network Application Architecture
  - P2P (peer-to-peer) Architecture
    - In P2P architecture, there is no dedicated server in a data center.
    - The peers are the computers which are not owned by the service provider. Most of the peers reside in the homes, offices, schools, and universities.
    - The peers communicate with each other without passing the information through a dedicated server, this architecture is known as peer-to-peer architecture.
    - The applications based on P2P architecture includes file sharing and internet telephony.

Network Application Software

- Network Application Architecture
  - Features of P2P architecture
    - Self scalability: In a file sharing system, although each peer generates a workload by requesting the files, each peer also adds a service capacity by distributing the files to the peer.
    - Cost-effective: It is cost-effective as it does not require significant server infrastructure and server bandwidth.

Network Application Software

- Network Application Architecture
  - Hybrid Architecture
    - Some network applications do not need the totality of client-server or P2P architecture. The utilise both architectures for efficiency.
    - The combination of both client-server and P2P is know as the hybrid application architecture.

Network Application Software

- Network Application Architecture
  - Hybrid Architecture
    - Consider the following examples:
      - Skype
        - Internet telephony app
        - Finding address of remote party: centralized server(s)
        - Client-client connection is direct (not through server)
      - Instant messaging
        - Chatting between two users is P2P
        - Presence detection/location centralized:
          - User registers its IP address with central server when it comes online
          - User contacts central server to find IP addresses of buddies

Application Layer Protocols

- Application-layer protocols define how applications running on different computing devices exchange messages. Application-layer protocols define the following:
  - Types of messages exchanged between applications
  - The syntax and semantics of fields in the messages
  - Rules for governing how messages are exchanged between applications running on different devices

- The application layer protocols used to make communication between sender and receiver faster, more efficient, reliable, and secure.

- These protocols include:
  - Hyper Text Transfer Protocol (HTTP)
  - Domain Name Service (DNS)
  - File Transfer Protocl (FTP)
  - Simple Mail Transfer Protocol (SMTP)
  - Multipurpose Internet Mail Extensions (MIME)
  - Post Office Protocol (POP)
  - Terminal Network (TELNET)

Application Layer Protocols

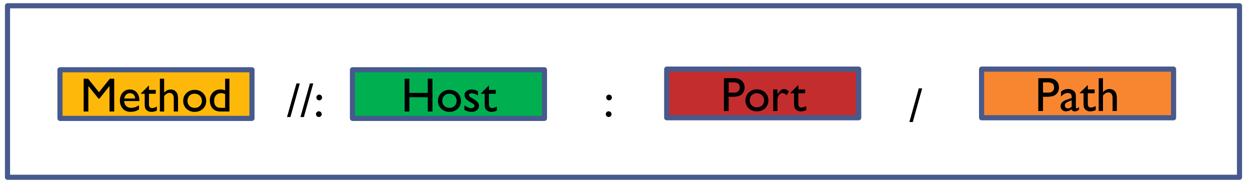
- Hyper Text Transfer Protocol (HTTP)
  - Web server and browser
    - In the Web, there are two distinct applications that communicate with each other:
      - The browser program running in the user's host (desktop, laptop, tablet, smartphone, and so on) and
      - The Web server program running in the Web server host. A Web browser is the client program that requests services from the Web server.
    - Popular Web browsers include Microsft Internet Explorer, Google Chrome, Mozilla and Onion.
    - Popular Web servers include Apache and Microsoft Internet Information Server. The Web server hosts resources in the form of Web pages.

Application Layer Protocols

- Hyper Text Transfer Protocol (HTTP)
  - Web page
    - A Web page is a collection of one or more files in a particular format.
    - A file format can be text, JPEG image or video clip.
    - The most common file format is HTML.
  - HTML
    - HTML files are text files created using the Hypertext Mark-up Language (HTML), which marks up the text and other content of a document in such a way as to describe the appearance when displayed in a Web browser.
    - Most Web pages consist of a base HTML file linked to other HTML files or other files such as image files, which can be on the same server or on a different one.
    - In this way, the contents of the World Wide Web are stored on the numerous Web servers scattered across the world, where those contents are linked together to form a single 'web'.

Application Layer Protocols

- Hyper Text Transfer Protocol (HTTP)
  - URL
    - Web pages on Web servers are addressed by Uniform Resource Locators (URLs). A URL has the form: http://<host name>/<file path name> or https://<host name>/<file path name>



Method //: Host : Port / Path

    - Method is the protocol used to retrieve the document from a server. For example, HTTP.
    - Host is the computer where the information is stored, and the computer is given an alias name. Web pages are mainly stored in the computers and the computers are given an alias name that begins with the characters "www". This field is not mandatory.
    - The URL can also contain the **port** number of the server, but it's an optional field. If the port number is included, then it must come between the host and path and it should be separated from the host by a colon.
    - Path: Path is the pathname of the file where the information is stored. The path itself contain slashes that separate the directories from the subdirectories and files.

Application Layer Protocols

- Hyper Text Transfer Protocol (HTTP)
    - The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. HTTP has been in use by the World-Wide Web global information initiative since 1990.
    - The World-Wide Web is based on a simple protocol called HTTP that allows browser programs such as Google Chrome and Internet Explorer, to fetch files from remote server programs, for example apache, and to view them.
    - HTTP is the protocol used to communicate between a client and a server. The protocol defines what characters can be sent along the socket stream connection.
    - The basic protocol is **request** and **response**.
    - The server accepts a connection and the client sends a request command line, various optional MIME lines and then a blank. The server must then send a response line giving a success or failure code, followed by additional optional lines, then the blank line and finally, if a file was successfully requested, the file contents (whether HTML, GIF or whatever).

Application Layer Protocols

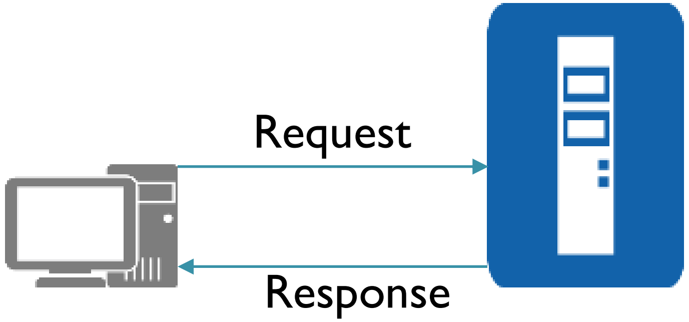
- Hyper Text Transfer Protocol (HTTP)
  - This protocol is known as Hypertext Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
  - HTTP is used to carry the data in the form of MIME-like format.

Application Layer Protocols

- Hyper Text Transfer Protocol (HTTP)
  - Features of HTTP
    - Connectionless protocol
      - HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server.
      - When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection.
      - The connection between client and server exist only during the current request and response time only.
    - Media independent
      - HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content.
      - It is required for both the client and server to specify the content type in MIME-type header.
    - Stateless
      - HTTP is a stateless protocol as both the client and server know each other only during the current request.
      - Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

Application Layer Protocols

- Hyper Text Transfer Protocol (HTTP)
  - HTTP Transactions
    - HTTP transactions are carried out in two simple messages: request and response.



    - The client initiates a transaction by sending a request message to the server. The server replies to the request message by sending a response message.

Application Layer Protocols

- Hyper Text Transfer Protocol (HTTP)
  - HTTP Transactions
    - Request Message
      - The request message is sent by the client that consists of a request line, headers, and sometimes a body.

Request
Request Header: value
Body (optional)

      - The first line in a request message is called a request line.
      - After the request line, we can have zero or more request header lines.
      - The body is an optional one. It contains the comment to be sent or the file to be published on the website when the method is PUT or POST.

Application Layer Protocols

- Hyper Text Transfer Protocol (HTTP)
  - HTTP Transactions
    - Request Message
      - Request Line
        - There are three fields in this request line - Method, URL and Version.
        - The Method field defines the request types.
        - The URL field defines the address and name of the corresponding web page.
        - The Version field gives the version of the protocol; the most current version of HTTP.
        - Some of the Method types are:

Method	Action
GET	Requests a document from the server.
HEAD	Requests information about a document but not the document itself.
PUT	Sends a message from the client to the server.
POST	Sends some information from the client to the server.
TRACE	Echoes the incoming request.
DELETE	Removes the webpage.
CONNECT	Reserved
OPTIONS	Inquires about available options.

Application Layer Protocols

- Hyper Text Transfer Protocol (HTTP)
  - HTTP Transactions
    - Request Header
      - Each request header line sends additional information from the client to the server.
      - Each header line has a header name, a colon, a space, and a header value.
      - The value field defines the values associated with each header name.
      - Headers defined for request message include

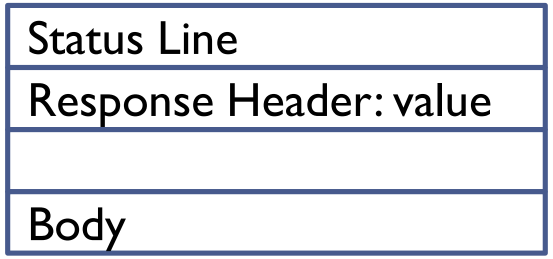
Header	Description
User-Agent	Identifies the client program
Accept	Shows the media format the client can accept
Accept-charset	Shows the character set the client can handle
Accept-lencoding	Shows the encoding scheme the client can handle
Accept-language	Shows the language the client can accept
Authorisation	Shows what permissions the client has.
Host	Shows the host and port number of the client
Date	Shows the current date
Upgrade	Specifies the preferred communication protocol
Cookie	Returns the cookie to the server
If-Modified-Since	If the file is modified since a specific date

Application Layer Protocols

- Hyper Text Transfer Protocol (HTTP)
  - HTTP Transactions
    - Request Message
      - Body
        - The body can be present in a request message. It is optional.
        - Usually, it contains the comment to be sent or the file to be published on the website when the method is PUT or POST.
      - Conditional Request
        - A client can add a condition in its request.
        - In this case, the server will send the requested web page if the condition is met or inform the client otherwise.
        - One of the most common conditions imposed by the client is the time and date the web page is modified.
        - The client can send the header line If-Modified-Since with the request to tell the server that it needs the page only if it is modified after a certain point in time.

Application Layer Protocols

- Hyper Text Transfer Protocol (HTTP)
  - HTTP Transactions
    - Response Message
      - The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.



Status Line

Response Header: value

Body

      - The first line in a request message is called a status line.
      - After the request line, we can have zero or more response header lines.
      - The body is an optional one. The body is present unless the response is an error message

Application Layer Protocols

- Hyper Text Transfer Protocol (HTTP)
  - HTTP Transactions
    - Response Message
      - Status Line
        - The Status line contains three fields - HTTP version , Status code, Status phrase
        - The first field defines the version of HTTP protocol, currently 1.1.
        - The status code field defines the status of the request. It classifies the HTTP result. It consists of three digits:

          1xx–Informational, 2xx– Success, 3xx–Redirection,

          4xx–Client error, 5xx–Server error
        - The Status phrase field gives brief description about status code in text form.
        - Some of the Status codes are

Application Layer Protocols

- Hyper Text Transfer Protocol (HTTP)
  - HTTP Transactions
    - Response Message
      - Status Line
        - The Status line contains three fields - HTTP version , Status code, Status phrase.
        - The first field defines the version of HTTP protocol, currently /1.1 to /3.
        - The status code field defines the status of the request. It classifies the HTTP result. It consists of three digits:

          1xx–Informational, 2xx– Success, 3xx–Redirection,

          4xx–Client error, 5xx–Server error
        - The Status phrase field gives brief description about status code in text form.

Application Layer Protocols

- Hyper Text Transfer Protocol (HTTP)
  - HTTP Transactions
    - Response Message
      - Some of the status code includes:

Code	Phrase	Description
100	Continue	Initial request received, client to continue process
200	Ok	Request is successful
301	Moved permanently	Request URL is no longer in use
404	Not found	Document not found
500	Internal server error	An error such as a crash, at the server site

Application Layer Protocols

- Hyper Text Transfer Protocol (HTTP)
  - HTTP Transactions
    - Response Message
      - Response Header
        - Each header provides additional information to the client.
        - Each header line has a header name, a colon, a space, and a header value.
        - Some of the response headers are:

Response Header	Description
Content-type	Specifies the MIME type
Expires	Date and time up to which the document is valid
Last-modified	Date and time when the document was last updated
Location	Specifies location of the created or moved document

Application Layer Protocols

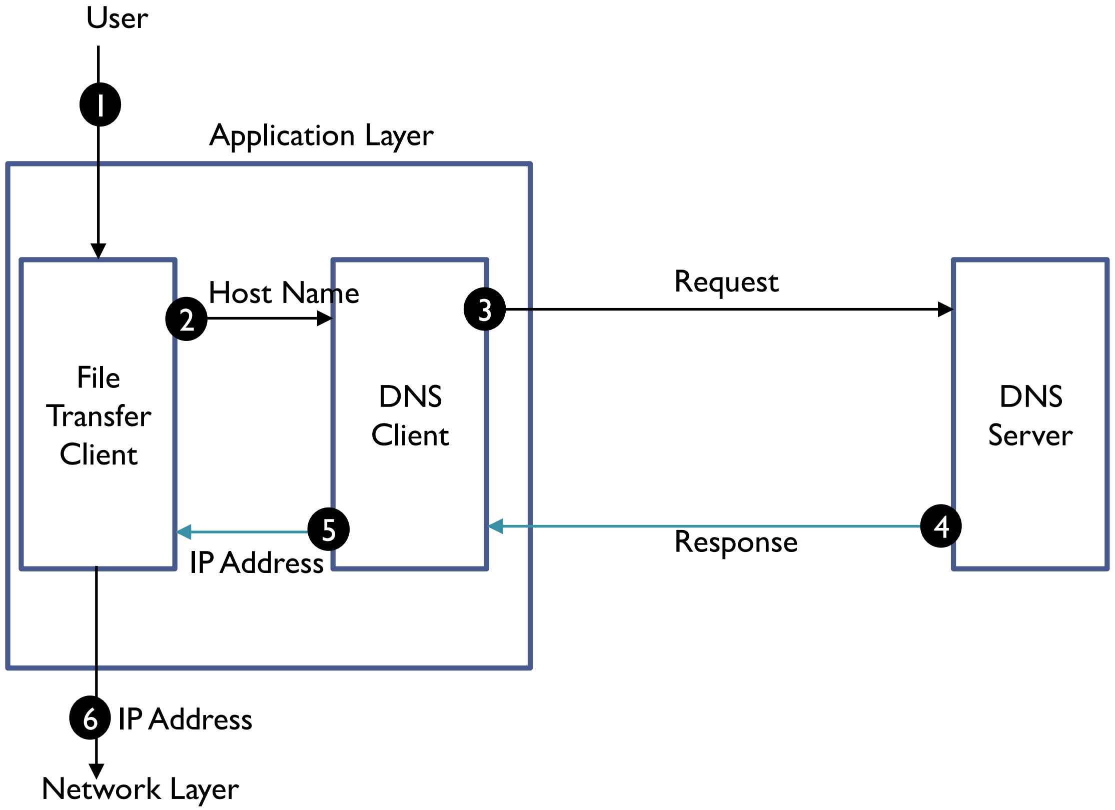
- Hyper Text Transfer Protocol (HTTP)
  - HTTP Transactions
    - Response Message
      - Body
        - The body contains the document to be sent from the server to the client.
        - The body is present unless the response is an error message.

Application Layer Protocols

- Domain Name Service (DNS)
  - Domain Name System was designed in 1984.
  - DNS is used for name-to-address mapping.
  - The DNS provides the protocol which allows clients and servers to communicate with each other.
  - For example: a host name like www.yahoo.com is translated into numerical IP addresses like 207.174.77.131
  - Domain Name System (DNS) is a distributed database used by TCP/IP to map between hostnames and IP addresses and to provide electronic mail routing information.
  - Each site maintains its own database of information and runs a server program that other systems across the Internet can query.

Application Layer Protocols

- Domain Name Service (DNS)
  - How DNS Works
    - The following six steps shows the working of a DNS. It maps the host name to an IP address:
      1. The user passes the host name to the file transfer client.
      2. The file transfer client passes the host name to the DNS client.
      3. Each computer, after being booted, knows the address of one DNS server. The DNS client sends a message to a DNS server with a query that gives the file transfer server name using the known IP address of the DNS server.
      4. The DNS server responds with the IP address of the desired file transfer server.
      5. The DNS server passes the IP address to the file transfer client.
      6. The file transfer client now uses the received IP address to access the file transfer server.



Application Layer Protocols

- Domain Name Service (DNS)
  - Name Space
    - Name space is a set of domain names contained in the DNS. These names are organized into a flat or hierarchical tree-like structure.
    - To be unambiguous, the names assigned to machines must be carefully selected from a name space with complete control over the binding between the names and IP address.
    - The names must be unique because the addresses are unique.
    - A name space that maps each address to a unique name can be organised in two ways:
      - Flat
      - Hierarchical.

Application Layer Protocols

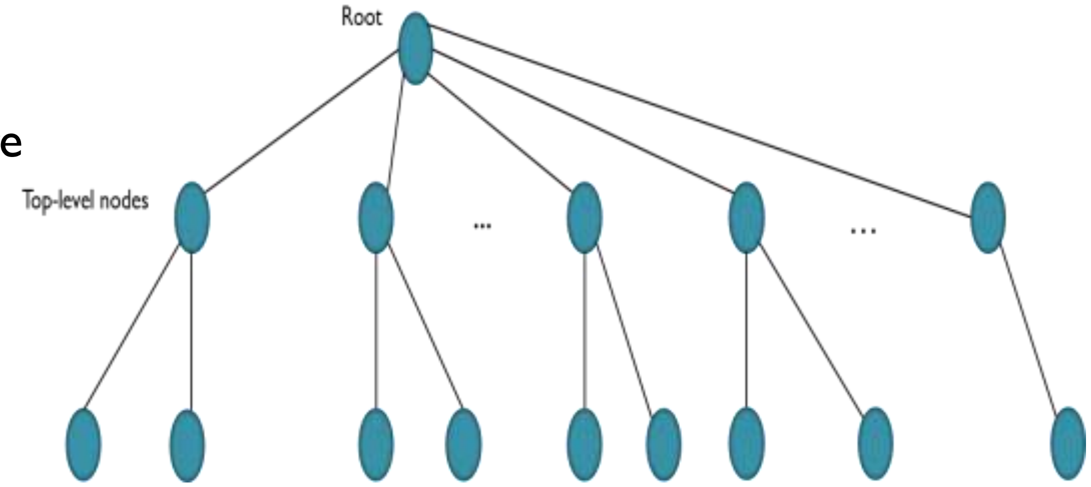
- Domain Name Service (DNS)
  - Name Space
    - Flat Name Space
      - In a flat name space, a name is assigned to an address.
      - A name in this space is a sequence of characters without structure.
      - The disadvantage of a flat name space is that it cannot be used in a large system such as Internet because it must be centrally controlled to avoid ambiguity and duplication.

Application Layer Protocols

- Domain Name Service (DNS)
  - Name Space
    - Hierarchical Name Space
      - In a hierarchical name space, each name is made of several parts. The first part can define the organization, the second part can define the name, the third part can define departments, and so on.
      - In this case, the authority to assign and control the name spaces can be decentralized.
      - A central authority can assign the part of the name that defines the nature of the organization and the name. The responsibility for the rest of the name can be given to the organization itself. Suffixes can be added to the name to define host or resources.
      - The management of the organization need not worry that the prefix chosen for a host is taken by another organization because even if part of an address is the same, the whole address is different.
      - The names are unique without the need to be assigned by a central authority. The central authority controls only part of the name, not the whole name.

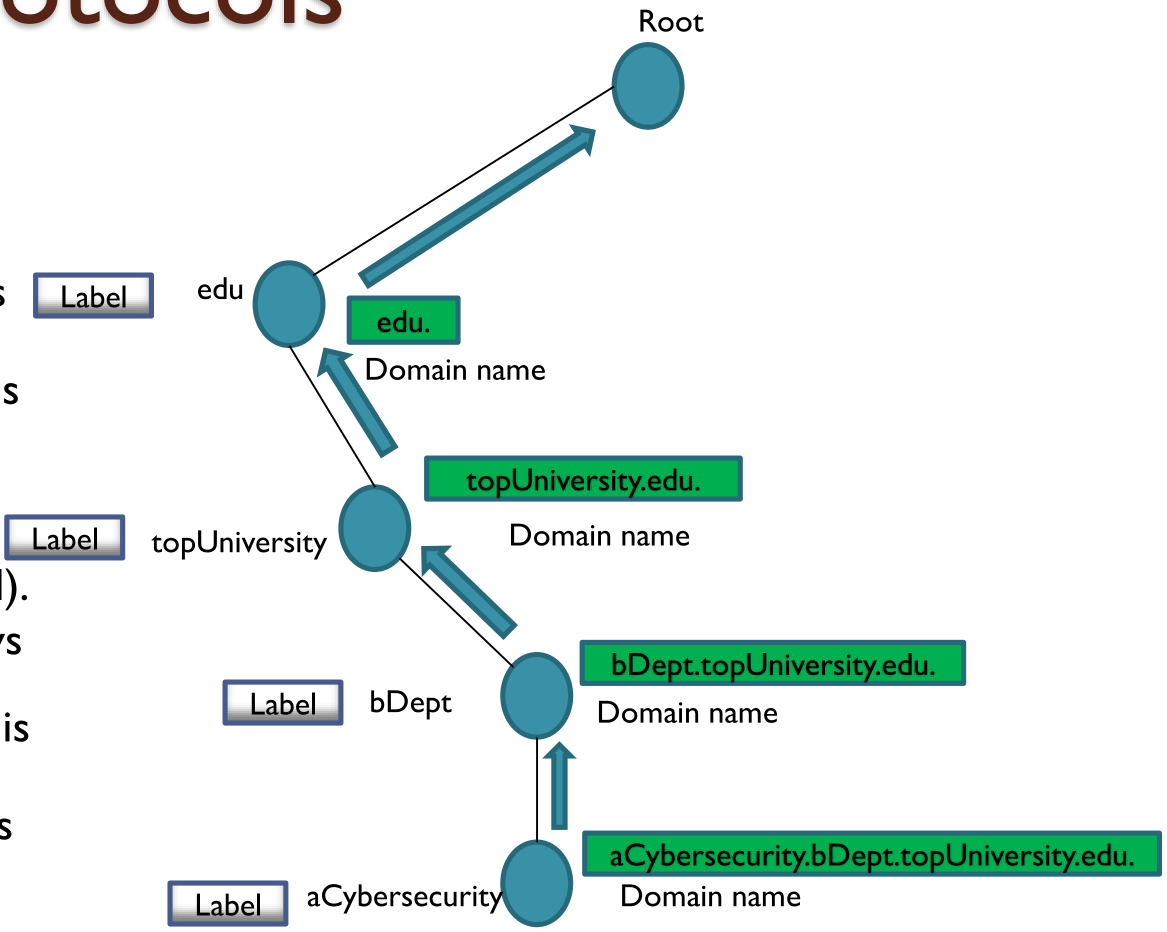
Application Layer Protocols

- Domain Name Service (DNS)
  - Domain Name Space
    - To have a hierarchical name space, a domain name space was designed. In this design, the names are defined in an inverted-tree structure with the root at the top.
    - Each node in the tree has a label, which is a string with a maximum of 63 characters.
    - The root label is a null string.
    - DNS requires that children of a node have different labels, which guarantees the uniqueness of the domain names.



Application Layer Protocols

- Domain Name Service (DNS)
  - Domain Name
    - Each node in the tree has a label called as domain name.
    - A full domain name is a sequence of labels separated by dots (.)
    - The domain names are always read from the node up to the root.
    - The last label is the label of the root (null).
    - This means that a full domain name always ends in a null label, which means the last character is a dot because the null string is nothing.
    - If a label is terminated by a null string, it is called a fully qualified domain name (FQDN).
    - If a label is not terminated by a null string, it is called a partially qualified domain name (PQDN).



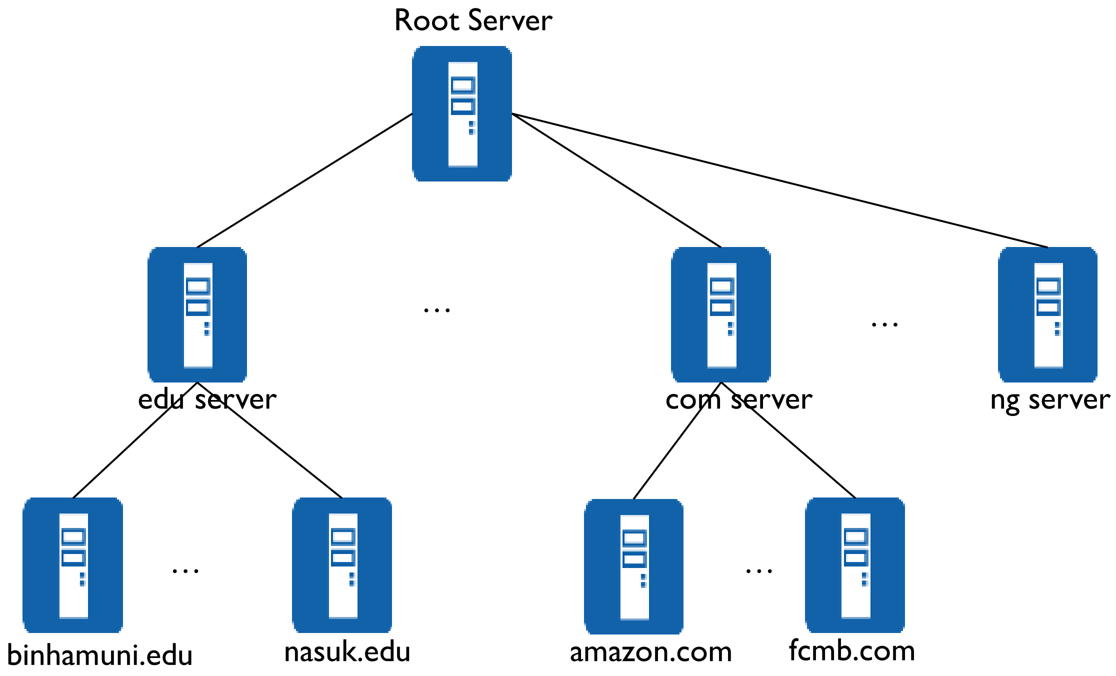
Application Layer Protocols

- Domain Name Service (DNS)
  - Domain
    - A domain is a subtree of the domain name space.
    - The name of the domain is the domain name of the node at the top of the subtree.
    - A domain may itself be divided into domains.

  - Distribution of Name Space
    - The information contained in the domain name space must be stored.
    - But it is very inefficient and also not reliable to have just one computer store such a huge amount of information.
    - It is inefficient because responding to requests from all over the world, places a heavy load on the system.
    - It is not reliable because any failure makes the data inaccessible.
    - The solution to these problems is to distribute the information among many computers called DNS servers.

Application Layer Protocols

- Domain Name Service (DNS)
  - Hierarchy of Name Servers
    - The way to distribute information among DNS servers is to divide the whole space into many domains based on the first level.
    - Let the root stand-alone and create as many domains as there are first level nodes.
    - Because a domain created this way could be very large,
    - DNS allows domains to be divided further into smaller domains.
    - Thus we have a hierarchy of servers in the same way that we have a hierarchy of names.



Application Layer Protocols

- Domain Name Service (DNS)
  - Zone
    - What a server is responsible for, or has authority over, is called a zone.
    - The server makes a database called a zone file and keeps all the information for every node under that domain.
    - If a server accepts responsibility for a domain and does not divide the domains into smaller domains, the domain and zone refer to the same thing.
    - But if a server divides its domain into sub domains and delegates parts of its authority to other servers, domain and zone refer to different things.
    - The information about the nodes in the sub domains is stored in the servers at the lower levels, with the original server keeping some sort of references to these lower level servers.
    - But still, the original server does not free itself from responsibility totally.
    - It still has a zone, but the detailed information is kept by the lower level servers.

Application Layer Protocols

- Domain Name Service (DNS)
  - Root Server
    - A root sever is a server whose zone consists of the whole tree.
    - A root server usually does not store any information about domains but delegates its authority to other servers, keeping references to those servers.
    - Currently there are more than 13 root servers, each covering the whole domain name space.
    - The servers are distributed all around the world.

Application Layer Protocols

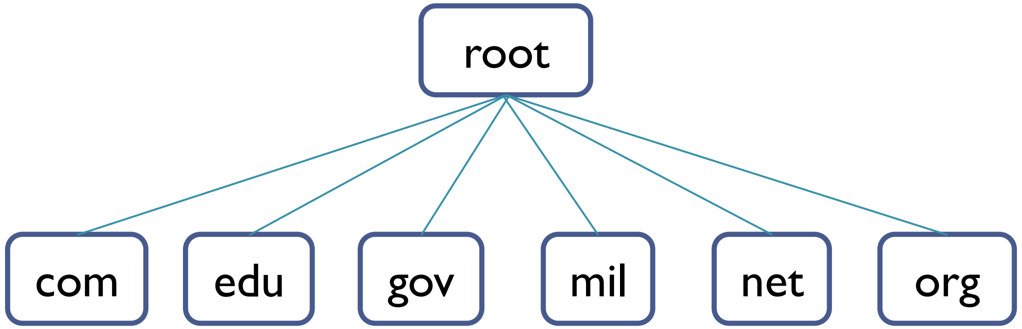
- Domain Name Service (DNS)
  - Primary and Secondary Servers
    - DNS defines two types of servers: primary and secondary.
    - A Primary Server is a server that stores a file about the zone for which it is an authority.
    - Primary Servers are responsible for creating, maintaining, and updating the zone file.
    - Primary Server stores the zone file on a local disc.
    - A secondary server is a server that transfers the complete information about a zone from another server (Primary or Secondary) and stores the file on its local disc.
    - If updating is required, it must be done by the primary server, which sends the updated version to the secondary.
    - A primary server loads all information from the disk file; the secondary server loads all information from the primary server.

Application Layer Protocols

- Domain Name Service (DNS)
  - DNS in the Internet
    - DNS is a protocol that can be used in different platforms.
    - In the Internet, the domain name space (tree) is divided into three different sections:
      - Generic domains
      - Country domains
      - Inverse domain.

Application Layer Protocols

- Domain Name Service (DNS)
  - DNS in the Internet
    - Generic Domains
      - The generic domains define registered hosts according to their generic behavior.
      - Each node in the tree defines a domain, which is an index to the domain name space database.
      - The first level in the generic domains section allows seven possible three character levels.
      - These levels describe the organization types as listed in following table.



.com	commercial organisations
.edu	educational institutions
.gov	government institutions
.mil	military groups
.net	major network support centres
.org	non-profit ornanisations

Application Layer Protocols

- Domain Name Service (DNS)
  - DNS in the Internet
    - Country Domains
      - The country domains section follows the same format as the generic domains but uses two characters for country abbreviations (e.g.; ng for Nigeria, us for United States etc.,) in place of the three character organizational abbreviation at the first level.
      - Second level labels can be organizational, or they can be more specific, national designation.
      - Nigeria for example, may choose to use state abbreviations as a subdivision of the country domain (e.g., be.in.)

Application Layer Protocols

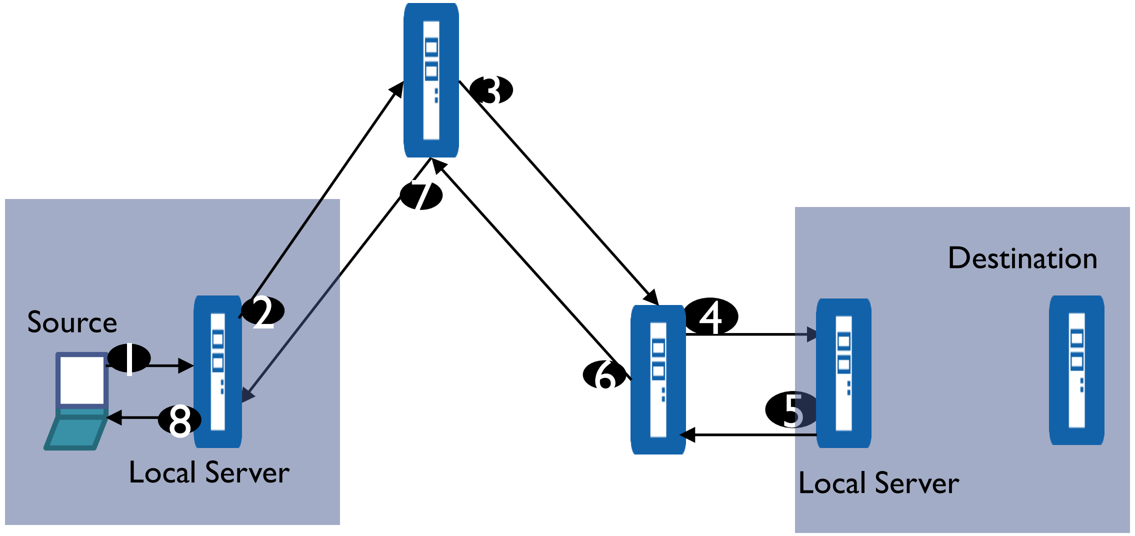
- Domain Name Service (DNS)
  - DNS in the Internet
    - Inverse Domains
      - Mapping an address to a name is called Inverse domain.
      - The client can send an IP address to a server to be mapped to a domain name and it is called PTR(Pointer) query.
      - To answer queries of this kind, DNS uses the inverse domain

Application Layer Protocols

- Domain Name Service (DNS)
  - DNS Resolution
    - Mapping a name to an address or an address to a name is called name address resolution.
    - DNS is designed as a client server application.
    - A host that needs to map an address to a name or a name to an address calls a DNS client named a Resolver.
    - The Resolver accesses the closest DNS server with a mapping request.
    - If the server has the information, it satisfies the resolver; otherwise, it either refers the resolver to other servers or asks other servers to provide the information.
    - After the resolver receives the mapping, it interprets the response to see if it is a real resolution or an error and finally delivers the result to the process that requested it.
    - A resolution can be either ***recursive*** or ***iterative***.

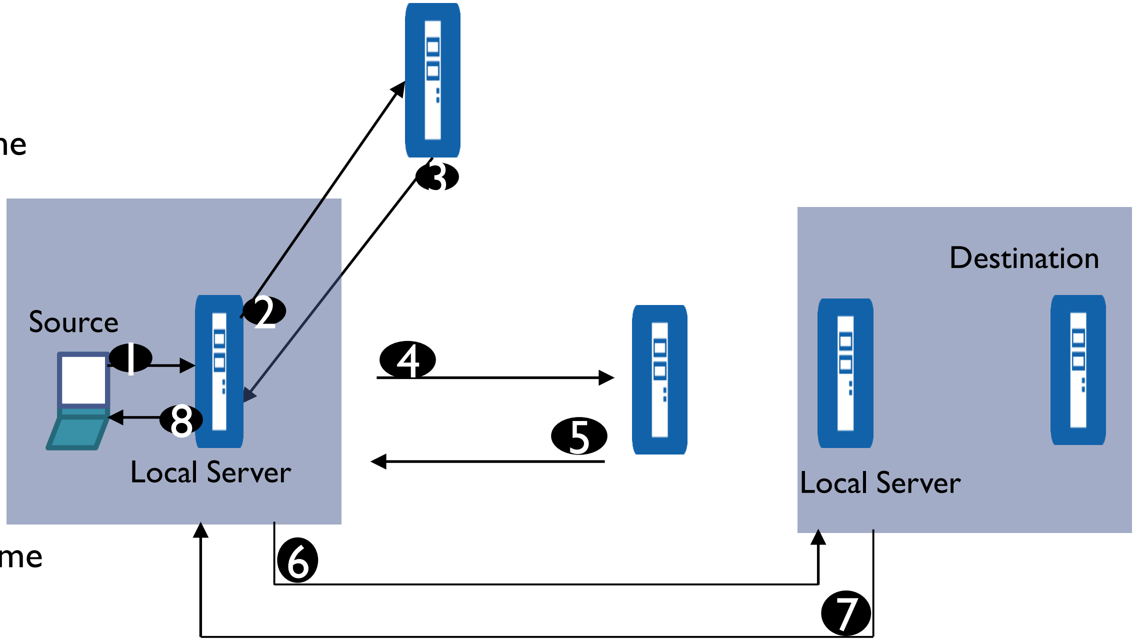
Application Layer Protocols

- Domain Name Service (DNS)
  - DNS Resolution
    - Recursive Resolution
      - The application program on the source host calls the DNS resolver (client) to find the IP address of the destination host. The resolver, which does not know this address, sends the query to the local DNS server of the source (Event 1)
      - The local server sends the query to a root DNS server (Event 2)
      - The Root server sends the query to the top-level-DNS server(Event 3)
      - The top-level DNS server knows only the IP address of the local DNS server at the destination. So it forwards the query to the local server, which knows the IP address of the destination host (Event 4)
      - The IP address of the destination host is now sent back to the top-level DNS server(Event 5) then back to the root server (Event 6), then back to the source DNS server, which may cache it for the future queries (Event 7), and finally back to the source host (Event 8).



Application Layer Protocols

- Domain Name Service (DNS)
  - DNS Resolution
    - Iterative Resolution
      - In iterative resolution, each server that does not know the mapping, sends the IP address of the next server back to the one that requested it.
      - The iterative resolution takes place between two local servers.
      - The original resolver gets the final answer from the destination local server.
      - The messages shown by Events 2, 4, and 6 contain the same query.
      - However, the message shown by Event 3 contains the IP address of the toplevel domain server.
      - The message shown by Event 5 contains the IP address of the destination local DNS server
      - The message shown by Event 7 contains the IP address of the destination.
      - When the Source local DNS server receives the IP address of the destination, it sends it to the resolver (Event 8).



Application Layer Protocols

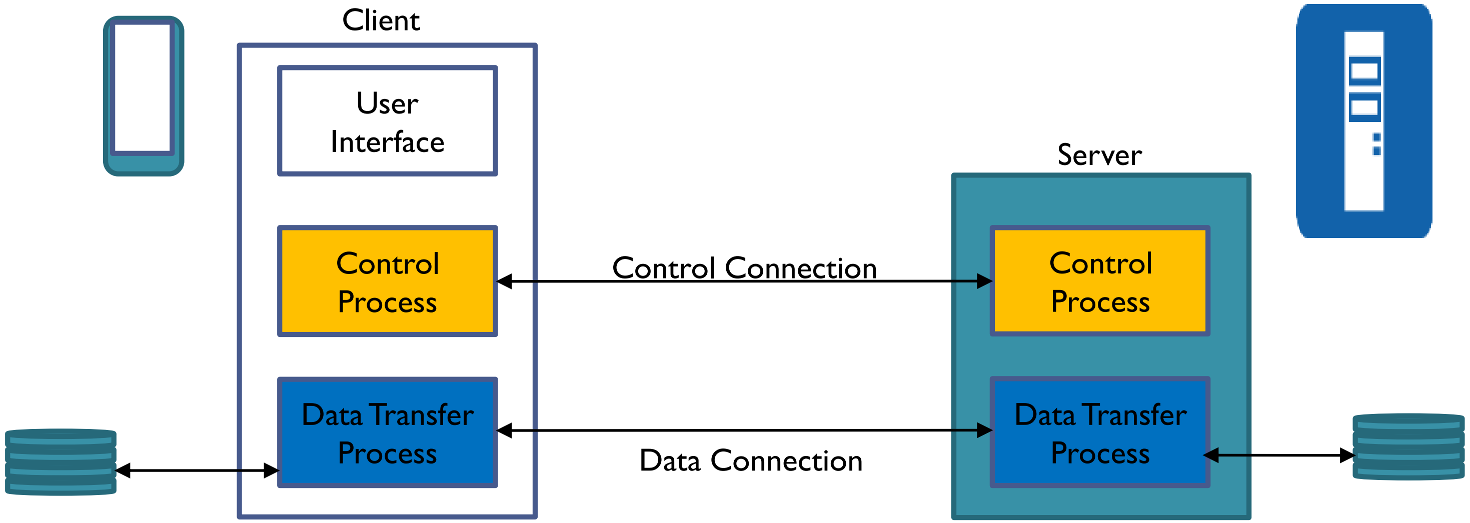
- File Transfer Protocol (FTP)
  - FTP is a standard internet protocol that is used for transmitting files from one host to another.
  - It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
  - It is also used for downloading files to computer from other servers.
  - Although we can transfer files using HTTP, FTP is a better choice to transfer large files or to transfer files using different formats.

Application Layer Protocols

- File Transfer Protocol (FTP)
    - FTP Objectives
        - It provides the sharing of files.
        - It is used to encourage the use of remote computers.
        - It transfers the data more reliably and efficiently.

Application Layer Protocols

- File Transfer Protocol (FTP)
  - FTP Mechanism
    - This figure shows the basic model of the FTP.



- The FTP client has three components:
  - User interface, control process, and data transfer process.
- The server has two components:
  - Server control process and server data transfer process.

Application Layer Protocols

- File Transfer Protocol (FTP)
  - FTP CONNECTIONS
    - There are two types of connections in FTP:
      - Control Connection and Data Connection.
    - The two connections in FTP have different lifetimes.
    - The control connection remains connected during the entire interactive FTP session.
    - The data connection is opened and then closed for each file transfer activity. When a user starts an FTP session, the control connection opens.
    - While the control connection is open, the data connection can be opened and closed multiple times if several files are transferred.
    - FTP uses two well-known TCP ports:
      - Port 21 is used for the control connection
      - Port 20 is used for the data connection.

Application Layer Protocols

- File Transfer Protocol (FTP)
  - FTP CONNECTIONS
    - Control Connection:
      - The control connection uses very simple rules for communication.
      - Through control connection, we can transfer a line of command or line of response at a time.
      - The control connection is made between the control processes.
      - The control connection remains connected during the entire interactive FTP session.
    - Data Connection:
      - The Data Connection uses very complex rules as data types may vary.
      - The data connection is made between data transfer processes.
      - The data connection opens when a command comes for transferring the files and closes when the file is transferred.

Application Layer Protocols

- File Transfer Protocol (FTP)
  - FTP Communication
    - FTP Communication is achieved through commands and responses.
    - FTP Commands are sent from the client to the server
    - FTP responses are sent from the server to the client.
    - FTP Commands are in the form of ASCII uppercase, which may or may not be followed by an argument.
    - Some of the most common commands are:

Command	Description
ABOR	Abort the previous command
CDUP	Change a parent directory
DELE	Delete a file
LIST	List subdirectories of files
MKD	Create a directory
PASS	Password
PASV	Server chooses a port
PORT	Client chooses a port
PWD	Display name of current directory
QUIT	Log out of the system
RETR	Retrieve files; file are transferred from server to client
RMD	Delete a directory
RNFR	Identify a file to be renamed
RNTO	Rename the file
STOR	Store files; files are transferred from client to server
STRU	Define data organisation (F: file, R: record, or P: page)
TYPE	Default file type (A: ASCII, E: EBCDIC, I: image)
USER	User information
MDE	Define transmission mode (S: stream, B: block, or C: compressed)

Application Layer Protocols

- File Transfer Protocol (FTP)
  - FTP Communication
    - Every FTP command generates at least one response.
    - A response has two parts: a three-digit number followed by text.
    - The numeric part defines the code; the text part defines needed parameter.

Code	Description
125	Data connection open
150	File status OK
200	Command OK
220	Service ready
221	Service closing
225	Data connection open
226	Closing data connection
230	User login
250	Request file action OK
331	User name OK; password is needed
425	Cannot open data connection
450	File action not taken; file not available
452	Action Aborted; insufficient storage
500	Syntax error; unrecognised command
501	Syntax error in parameters or arguments
530	User not logged in

Application Layer Protocols

- File Transfer Protocol (FTP)
  - FTP File Type
    - FTP can transfer one of the following file types across the data connection:
      - ASCII file, EBCDIC file, or image file.
  - FTP Data Structure
    - FTP can transfer a file across the data connection using one of the following data structure : file structure, record structure, or page structure.
    - The file structure format is the default one and has no structure. It is a continuous stream of bytes.
    - In the record structure, the file is divided into records. This can be used only with text files.
    - In the page structure, the file is divided into pages, with each page having a page number and a page header. The pages can be stored and accessed randomly or sequentially.

Application Layer Protocols

- File Transfer Protocol (FTP)
  - FTP Transmission Mode
    - FTP can transfer a file across the data connection using one of the following three transmission modes: stream mode, block mode, or compressed mode.
      - The stream mode is the default mode; data are delivered from FTP to TCP as a continuous stream of bytes.
      - In the block mode, data can be delivered from FTP to TCP in blocks.
      - In the compressed mode, data can be compressed and delivered from FTP to TCP.
  - FTP File Transfer
    - File transfer occurs over the data connection under the control of the commands sent over the control connection.
    - File transfer in FTP means one of three things:
      - Retrieving a file (server to client)
      - Storing a file (client to server)
      - Directory listing (server to client).

Application Layer Protocols

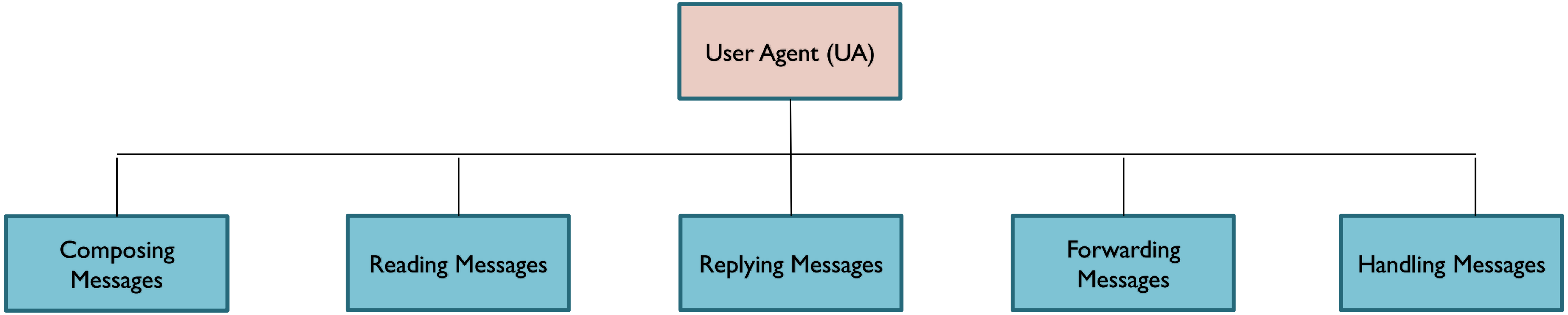
- File Transfer Protocol (FTP)
  - FTP Security
    - FTP requires a password. The password is sent in plaintext which is unencrypted. This means it can be intercepted and used by an attacker.
    - The data transfer connection also transfers data in plaintext, which is insecure.
    - To be secure, one can add a Secure Socket Layer between the FTP application layer and the TCP layer. In this case FTP is called SSL-FTP.

Application Layer Protocols

- Electronic Mail
  - One of the most popular Internet services is electronic mail (E-mail).
  - Email is one of the oldest network applications.
  - Sending emails across the networks is achieved using a few application layer protocols:
    - Simple Mail Transfer Protocols (SMTP)
    - Multipurpose Internet Message Extension (MIME)
    - Internet Mail Access Protocol (IMAP)
  - The components of an Email are:
    1. User Agent (UA)
    2. Message Transfer Agent (MTA) – SMTP
    3. Message Access Agent (MAA) - IMAP , POP

Application Layer Protocols

- Electronic Mail
  - Components of an eMail
    - User Agent (UA)
      - The first component of an electronic mail system is the user agent (UA).
      - It provides service to the user to make the process of sending and receiving a message easier.
      - A user agent is a software package that composes, reads, replies to, and forwards messages. It also handles local mailboxes on the user computers.



Application Layer Protocols

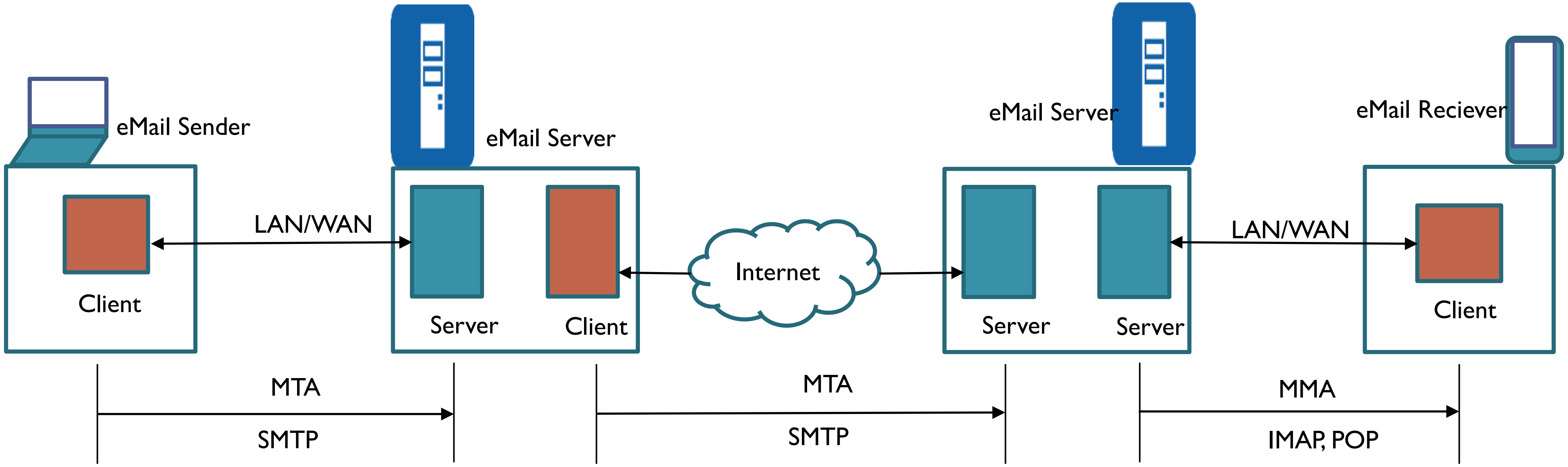
- Electronic Mail
  - Components of an eMail
    - There are two types of user agents: Command-driven and GUI-based.
    - Command driven
      - Command driven user agents belong to the early days of electronic mail.
      - A command-driven user agent normally accepts a one character command from the keyboard to perform its task.
      - Some examples of command driven user agents are mail, pine, and elm.
    - GUI-based
      - Modern user agents are GUI-based.
      - They allow the user to interact with the software by using both the keyboard and the mouse.
      - They have graphical components such as icons, menu bars, and windows that make the services easy to access.
      - Some examples of GUI-based user agents are Eudora and Outlook.

Application Layer Protocols

- Electronic Mail
  - Components of an eMail
    - Message Transfer Agent (MTA)
      - The actual mail transfer is done through message transfer agents (MTA).
      - To send mail, a system must have the MTA client, and to receive mail, a system must have a MTA server.
      - The formal protocol that defines the MTA client and server in the Internet is called Simple Mail Transfer Protocol (SMTP).
    - Message Access Agent (MAA)
      - MAA is a software that pulls messages out of a mailbox.
      - POP3 and IMAP4 are examples of MAA.

Application Layer Protocols

- Electronic Mail



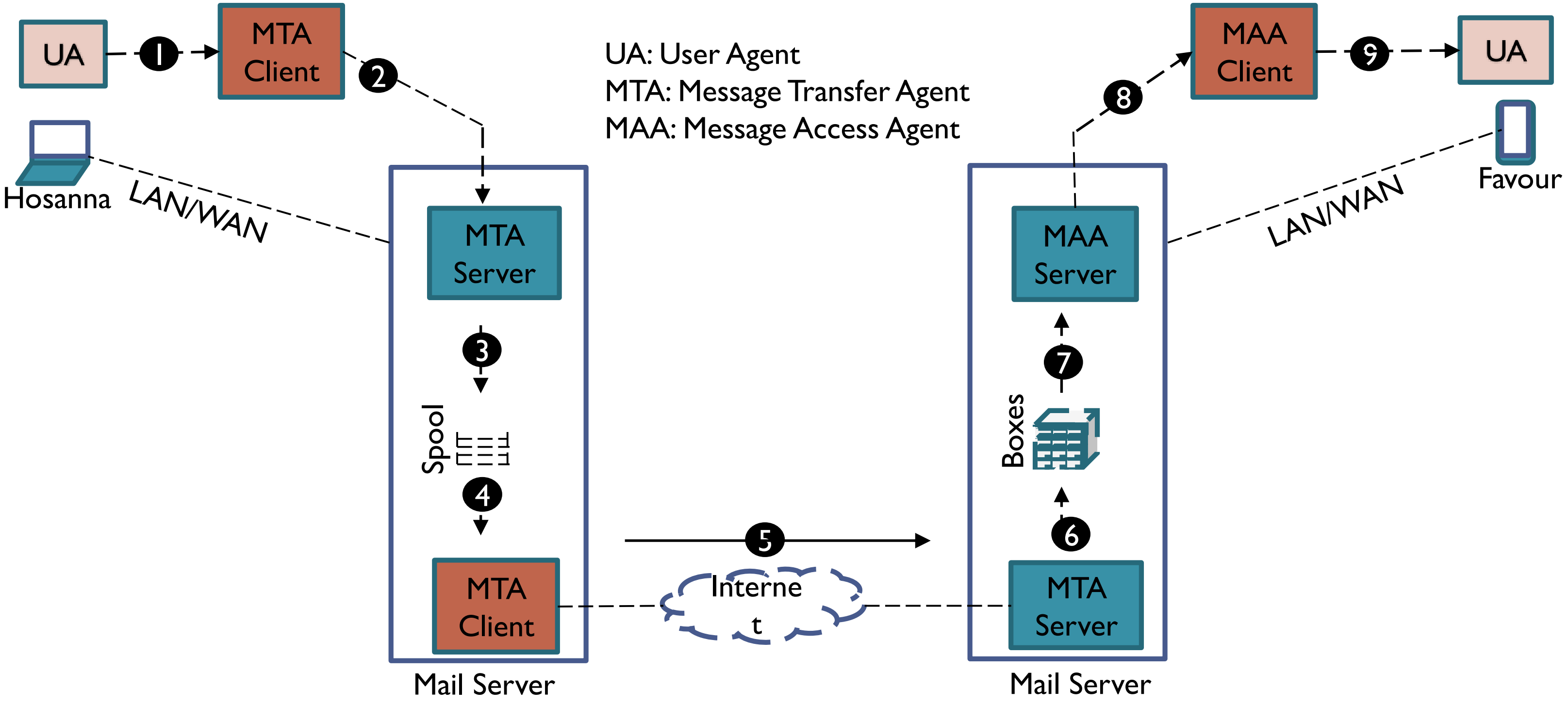
Components of an eMail

  - When the sender and the receiver of an e-mail are on the same system, we need only two User Agents and no Message Transfer Agent

  - When the sender and the receiver of an e-mail are on different system, we need two UA, two pairs of MTA (client and server), and two MAA (client and server).

Application Layer Protocols

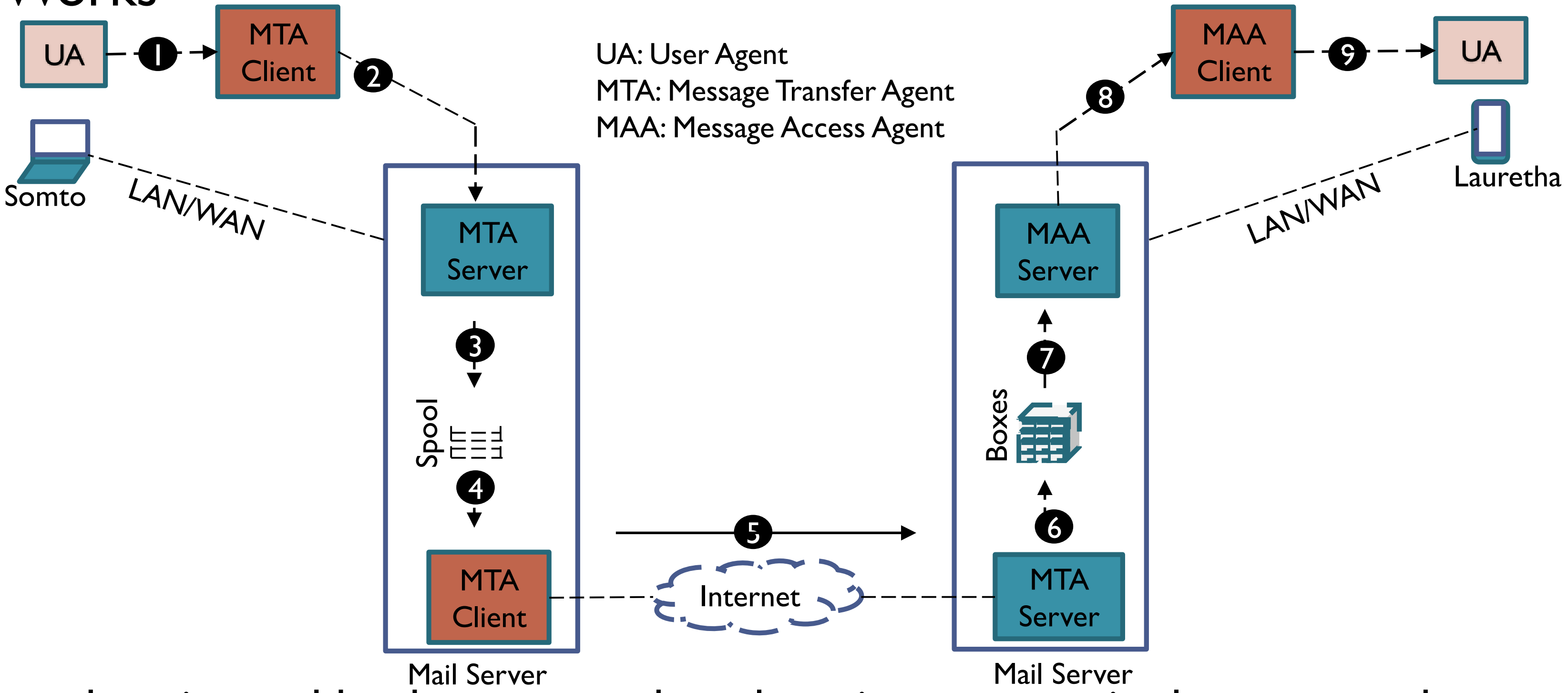
- Electronic Mail
  - How eMail Works



- When Hosanna needs to send a message to Favour, she runs a UA program to prepare the message and send it to her mail server.
- The mail server at her site uses a queue (spool) to store messages waiting to be sent. The message, however, needs to be sent through the Internet from Hosanna's site to Favour's site using an MTA.
- Here two message transfer agents are needed: one client and one server.
- The server needs to run all the time because it does not know when a client will ask for a connection.

Application Layer Protocols

- Electronic Mail
  - How eMail Works



- The client can be triggered by the system when there is a message in the queue to be sent.
- The user agent at the Favour’s site allows Favour to read the received message.
- Favour later uses an MAA client to retrieve the message from an MAA server running on the second server.

Application Layer Protocols

- Electronic Mail
  - Simple Mail Transfer Protocol (SMTP)
    - SMTP is the standard protocol for transferring mail between hosts in the TCP/IP protocol suite.
    - SMTP is not concerned with the format or content of messages themselves.
    - SMTP uses information written on the envelope of the mail (message header), but does not look at the contents (message body) of the envelope.
    - SMTP operates as client-server protocol consisting of an SMTP client and SMPT server.

Application Layer Protocols

- Electronic Mail
  - Simple Mail Transfer Protocol (SMTP)
    - SMTP clients and servers have two main components
      - User Agents(UA) – Prepares the message, encloses it in an envelope.
      - Mail Transfer Agent (MTA) – Transfers the mail across the internet
    - SMTP Commands and Responses
      - The operation of SMTP consists of a series of commands and responses exchanged between the SMTP sender and SMTP receiver.
      - The initiative is with the SMTP sender, who establishes the TCP connection.
      - Once the connection is established, the SMTP sender sends commands over the connection to the receiver.
      - The command is from an MTA client to an MTA server; the response is from an MTA server to the MTA client.

Application Layer Protocols

Keyword	Argument(s)	Description
HELLO	Sender's host name	Identifies itself
MAIL FROM	Sender of the message	Identifies sender of the message
RCPT TO	Intended recipient	Identifies recipient of the message
DATA	Body of the message	Sends the actual message
QUIT		Terminates the message
RSET		Aborts the current mail transaction
VRFY	Name of recipient	Verifies the address of the recipient
NOOP		Checks the address of the recipient
TURN		Switches the sender and the recipient
EXPN	Mailing list	Asks the recipient to expand the mailing list
HELP	Command name	Asks the recipient to send information about the command sent as an argument
SEND FROM	Intended recipient	Specifies that the mail be delivered only to the terminal of the recipient, and no the mail box
SMOL FROM	Intended recipient	Specifies that the mail be deliver to the terminal or the mail box of the recipient
SMAL FROM	Intended recipient	Specifies that the mail be delivered to terminal and the mail box of the recipient

Code	Description
Positive Completion Reply	
211	System status or help reply
214	Help message
220	Service delay
221	Service closing transmission channel
250	Request command completed
251	User not local; the message will be forwarder
Positive Intermediate Reply	
354	Start mail input
Transient Negative Completion Reply	
421	Service not available
450	Mailbox not available
451	Command aborted: local error
452	Command aborted: insufficient usage

Code	Description
Permanent Negative Completion Reply	
500	Syntax error: unrecognised command
501	Syntax error in parameters or argument
502	Command not implemented
503	Bad sequence of commands
504	Command temporarily not implemented
550	Command is not executed; mail box unavailable
551	User not local
552	Requested action aborted; exceeded storage location
553	Requested action not taken; mailbox name not allowed
554	Transaction failed

Application Layer Protocols

- Electronic Mail
  - Simple Mail Transfer Protocol (SMTP)
    - SMTP Operations
      - Basic SMTP operation occurs in three phases:
        1. Connection Setup
        2. Mail Transfer
        3. Connection Termination

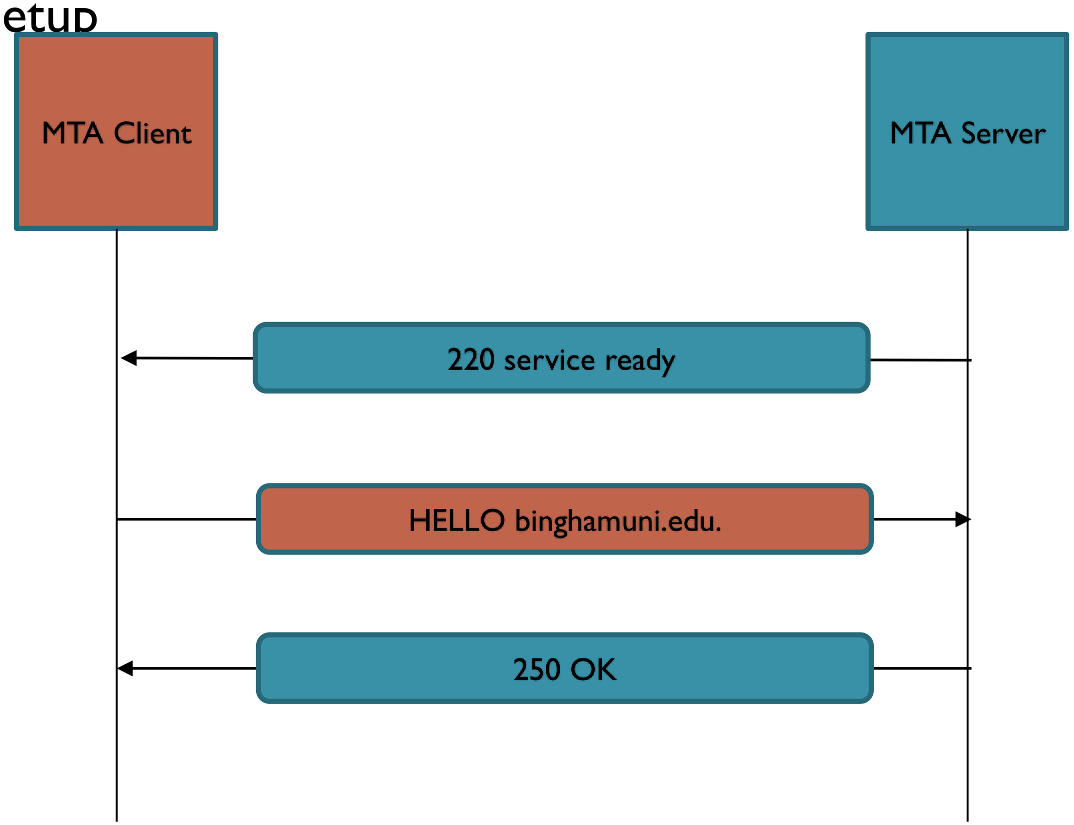
Application Layer Protocols

- Electronic Mail
  - Simple Mail Transfer Protocol (SMTP)
    - SMTP Operations
      - Connection Setup
        - An SMTP sender will attempt to set up a TCP connection with a target host when it has one or more mail messages to deliver to that host.
        - The sequence is quite simple:

1. The sender opens a TCP connection with the receiver.
2. Once the connection is established, the receiver identifies itself with
3. "Service Ready".
4. 3.The sender identifies itself with the HELO command.
5. 4.The receiver accepts the sender's identification with "OK".
6. 5. If the mail service on the destination is unavailable, the destination host returns a "Service Not Available" reply in step 2, and the process is terminated.

Application Layer Protocols

- Electronic Mail
  - Simple Mail Transfer Protocol (SMTP)
    - SMTP Operations
      - Connection Setup

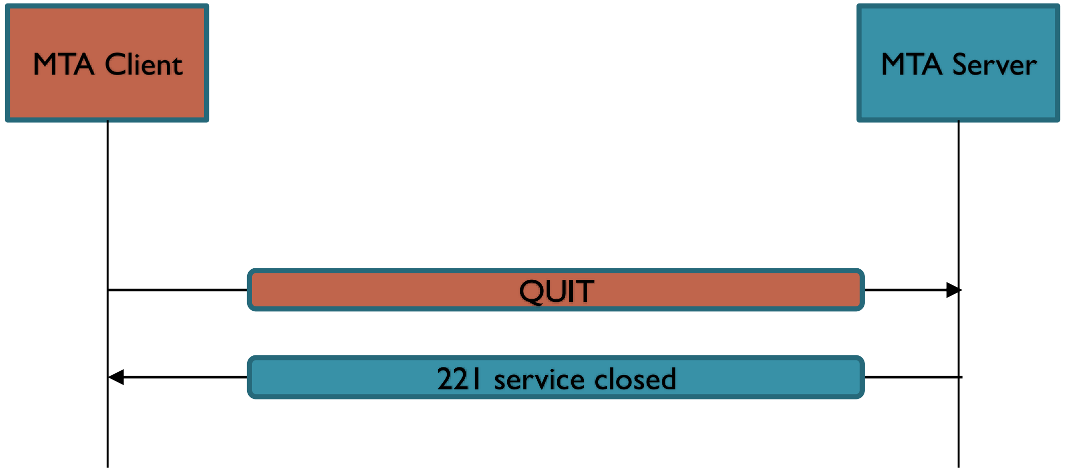


Application Layer Protocols

- Electronic Mail
  - Simple Mail Transfer Protocol (SMTP)
    - SMTP Operations
      - Mail Transfer
        - Once a connection has been established, the SMTP sender may send one or more messages to the SMTP receiver.
        - There are three logical phases to the transfer of a message:
          1. A MAIL command identifies the originator of the message.
          2. One or more RCPT commands identify the recipients for this message.
          3. A DATA command transfers the message text.

Application Layer Protocols

- Electronic Mail
  - Simple Mail Transfer Protocol (SMTP)
    - SMTP Operations
      - Connection Termination
        - The SMTP sender closes the connection in two steps.
        - First, the sender sends a QUIT command and waits for a reply.
        - The second step is to initiate a TCP close operation for the TCP connection.
        - The receiver initiates its TCP close after sending its reply to the QUIT command.



Application Layer Protocols

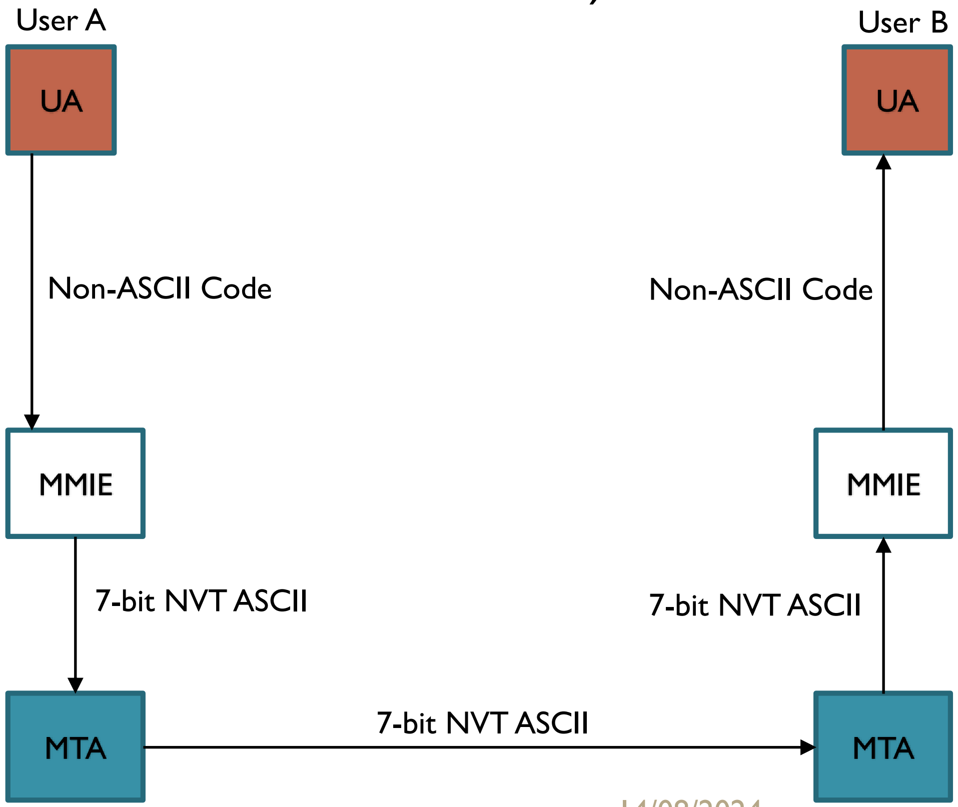
- Electronic Mail
  - Simple Mail Transfer Protocol (SMTP)
    - Limitations of Smtp
      - SMTP cannot transmit executable files or other binary objects.
      - SMTP cannot transmit text data that includes national language characters, as these are represented by 8-bit codes with values of 128 decimal or higher, and SMTP is limited to 7-bit ASCII.
      - SMTP servers may reject mail message over a certain size.
      - SMTP gateways that translate between ASCII and the character code EBCDIC do not use a consistent set of mappings, resulting in translation problems.
      - Some SMTP implementations do not adhere completely to the SMTP standards defined.
      - Common problems include the following:
        1. Deletion, addition, or recording of carriage return and linefeed.
        2. Truncating or wrapping lines longer than 76 characters.
        3. Removal of trailing white space (tab and space characters).
        4. Padding of lines in a message to the same length.
        5. Conversion of tab characters into multiple-space characters.

Application Layer Protocols

- Electronic Mail
  - Multipurpose Internet Mail Extension (MIME)
    - SMTP provides a basic email service, while MIME adds multimedia capability to SMTP.
    - MIME is an extension to SMTP and is used to overcome the problems and limitations of SMTP.
    - Email system was designed to send messages only in ASCII format.
    - Languages such as French, Chinese, etc., are not supported.
    - Image, audio and video files cannot be sent.
    - MIME adds the following features to email service:
      - Be able to send multiple attachments with a single message;
      - Unlimited message length;
      - Use of character sets other than ASCII code;
      - Use of rich text (layouts, fonts, colors, etc)
      - Binary attachments (executables, images, audio or video files, etc.), which may be divided if needed.

Application Layer Protocols

- Electronic Mail
  - Multipurpose Internet Mail Extension (MIME)
    - MIME is a protocol that converts non-ASCII data to 7-bit NVT(Network Virtual Terminal) ASCII and vice-versa.

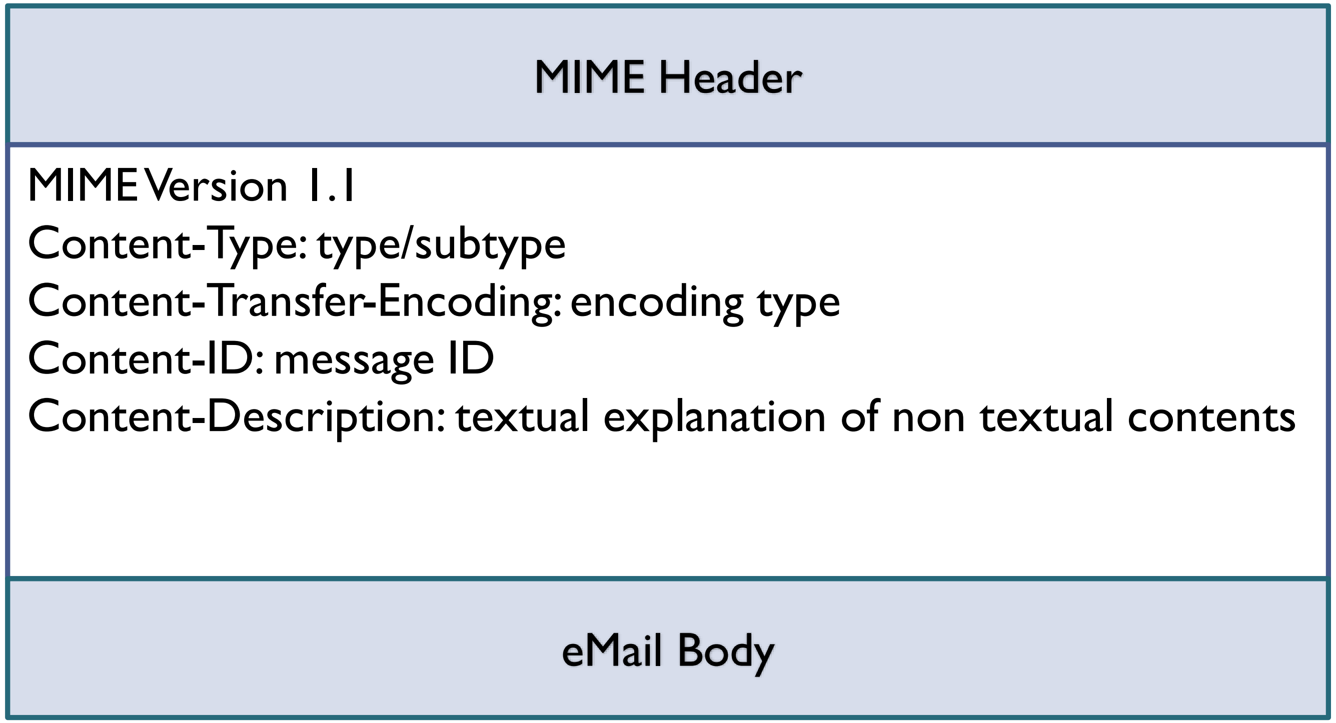


Application Layer Protocols

- Electronic Mail
  - Multipurpose Internet Mail Extension (MIME)
    - MIME Headers
      - Using headers, MIME describes the type of message content and the encoding used.
      - Headers defined in MIME are:
      - MIME-Version- current version, i.e., 1.1
      - Content-Type - message type (text/html, image/jpeg, application/pdf)
      - Content-Transfer-Encoding - message encoding scheme (eg base64).
      - Content-Id - unique identifier for the message.
      - Content-Description - describes type of the message body.

Application Layer Protocols

- Electronic Mail
  - Multipurpose Internet Mail Extension (MIME)
    - MIME Headers



MIME Header

MIME Version 1.1
Content-Type: type/subtype
Content-Transfer-Encoding: encoding type
Content-ID: message ID
Content-Description: textual explanation of non textual contents

eMail Body

Application Layer Protocols

- Electronic Mail
  - Multipurpose Internet Mail Extension (MIME)
    - MIME Content Types
      - There are seven different major types of content and a total of 14 subtypes.
      - In general, a content type declares the general type of data, and the subtype specifies a particular format for that type of data.
      - MIME also defines a multipart type that says how a message carrying more than one data type is structured.
      - This is like a programming language that defines both base types (e.g., integers and floats) and compound types (e.g., structures and arrays).
      - One possible multipart subtype is mixed, which says that the message contains a set of independent data pieces in a specified order.
      - Each piece then has its own header line that describes the type of that piece.

Ap

- E

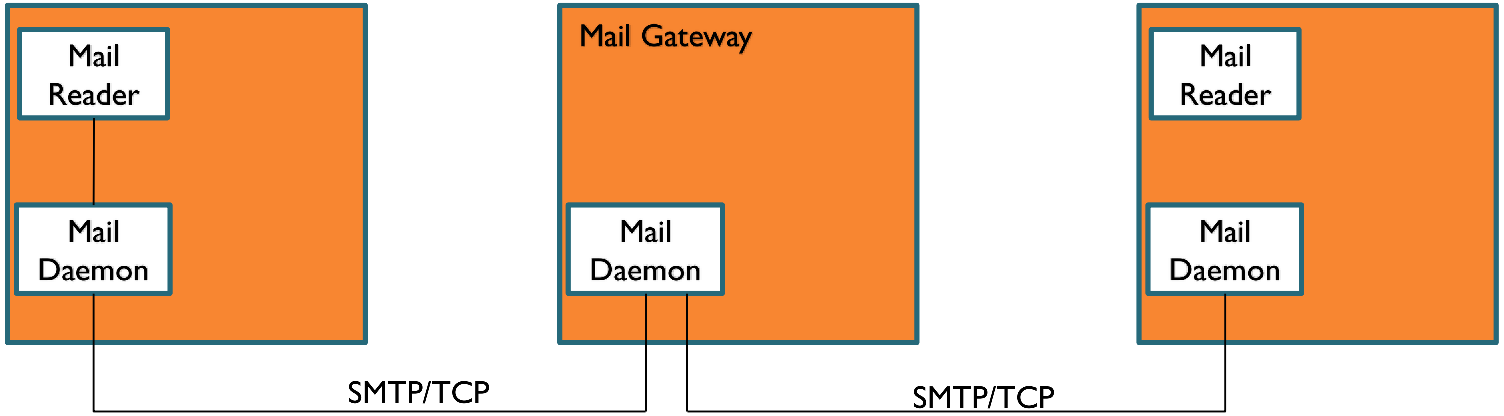
Type	Subtype	Description
Text	Plain	Unformatted
	HTML	HTML format
Multipart	Mixed	Body contains ordered parts of different data types
	Parallel	Same as in mixed but no order
	Digest	Similar to mixed subtypes, but the default is message/RFC822
	Alternative	Parts are different versions of the same message
Message	RFC822	Body is an encapsulated message
	Partial	Body is a fragment of a bigger message
	External-Body	Body is a reference to another message
Image	JPEG	Image is in JPEG format
	GIF	Image is in GIF format
Video	MPEG	Video is in MPEG format
Audio	Basic	Single-channel encoding of voice at kHz
Application	PostScript	Adobe PostScript
	Octect-stream	General binary data (8-bit bytes)

Application Layer Protocols

- Electronic Mail
  - Multipurpose Internet Mail Extension (MIME)
    - Encoding Formats of Mime
      - MIME uses various encoding formats to convert binary data into the ASCII character set.
      - To transfer binary data, MIME offers five encoding formats which can be usedin the header transfer-encoding:
        - **7-bit**: 7-bit text format (for messages without accented characters);
        - **8-bit**: 8-bit text format;
        - **quoted-printable**: Quoted-Printable format, recommended for messages which use a 7-bit alphabet (such as when there are accent marks);
        - **base-64**: Base 64, for sending binary files as attachments;
        - **binary**: binary format; not recommended.
      - Since MIME is very open, it can use third-party encoding formats such as:
        - **BinHex**: A proprietary format belonging to Apple
        - **Uuencode**: for UNIX-to-UNIX encoding
        - **Xencode**: for binary-to-text encoding

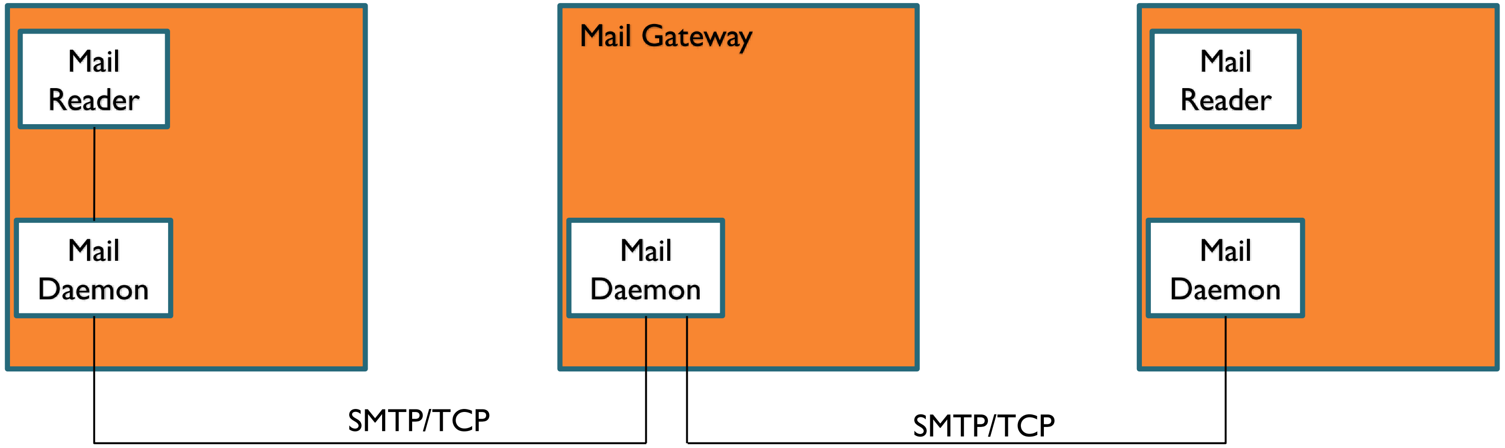
Application Layer Protocols

- Electronic Mail
  - Multipurpose Internet Mail Extension (MIME)
    - Message Transfer In MIME
      - MTA is a mail daemon (sendmail) active on hosts having mailbox, used to send an email.
      - Mail passes through a sequence of gateways before it reaches the recipient mail server.
      - Each gateway stores and forwards the mail using Simple mail transfer protocol (SMTP).



Application Layer Protocols

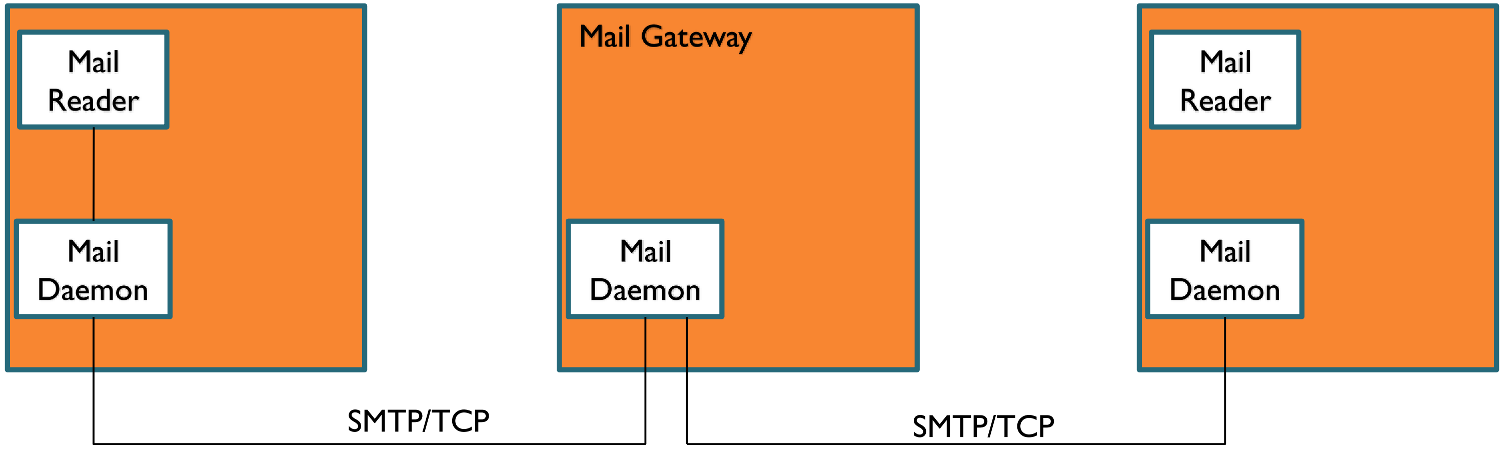
- Electronic Mail
  - Multipurpose Internet Mail Extension (MIME)
    - Message Transfer In MIME



- SMTP defines communication between MTAs over TCP on port 25.
- In an SMTP session, sending MTA is client and receiver is server. In each exchange:
- Client posts a command (HELO, MAIL, RCPT, DATA, QUIT,VRFY, etc.)
- Server responds with a code (250, 550, 354, 221, 251 etc) and an explanation.
- Client is identified using HELO command and verified by the server

Application Layer Protocols

- Electronic Mail
  - Multipurpose Internet Mail Extension (MIME)
    - Message Transfer In MIME



- Client forwards message to server, if server is willing to accept.
- Message is terminated by a line with only single period (.) in it.
- Eventually client terminates the connection.

Application Layer Protocols

- Electronic Mail
  - Internet Mail Access Protocol (IMAP)
    - IMAP is an Application Layer Internet protocol that allows an e-mail client to access e-mail on a remote mail server.
    - It is a method of accessing electronic mail messages that are kept on a possibly shared mail server.
    - IMAP is a more capable wire protocol.
    - IMAP is similar to SMTP in many ways.
    - IMAP is a client/server protocol running over TCP on port 143.

Application Layer Protocols

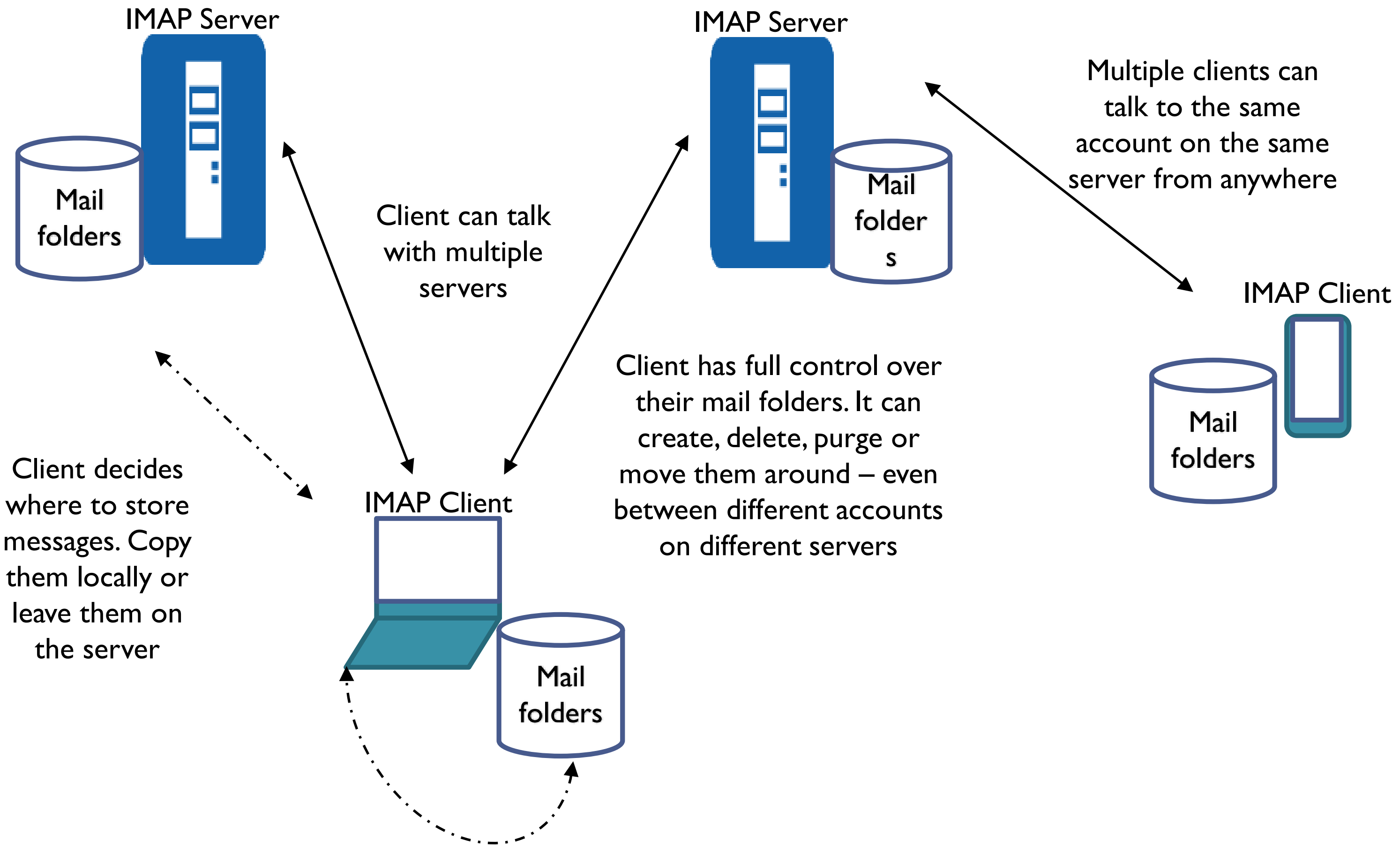
- Electronic Mail
  - Internet Mail Access Protocol (IMAP)
    - IMAP allows multiple clients simultaneously connected to the same mailbox, and through flags stored on the server, different clients accessing the same mailbox at the same or different times can detect state changes made by other clients.
    - In other words, it permits a "client" email program to access remote message stores as if they were local.
    - For example, email stored on an IMAP server can be manipulated from a desktop computer at home, a workstation at the office, and a notebook computer while travelling, without the need to transfer messages or files back and forth between these computers.

Application Layer Protocols

- Electronic Mail
  - Internet Mail Access Protocol (IMAP)
    - IMAP can support email serving in three modes:
      - Offline
      - Online
        - Users may connect to the server, look at what email is available, and access it online. This looks to the user very much like having local spool files, but they're on the mail server.
      - Disconnected Operation
        - A mail client connects to the server, can make a "cache" copy of selected messages, and disconnects from the server. The user can then work on the messages offline, and connect to the server later and resynchronize the server status with the cache.

Application Layer Protocols

- Electronic Mail
  - Internet Mail Access Protocol (IMAP)



Client can talk with multiple servers

Multiple clients can talk to the same account on the same server from anywhere

Client has full control over their mail folders. It can create, delete, purge or move them around – even between different accounts on different servers

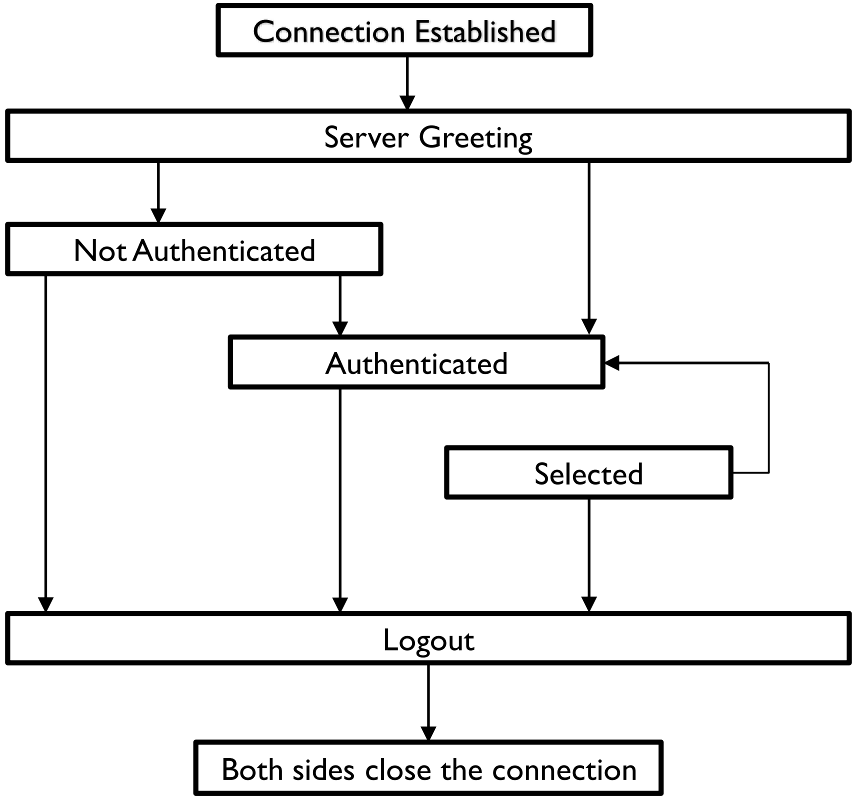
Client decides where to store messages. Copy them locally or leave them on the server

Application Layer Protocols

- Electronic Mail
  - Internet Mail Access Protocol (IMAP)
    - OPERATION OF IMAP
      - The mail transfer begins with the client authenticating the user and identifying the mailbox they want to access.
      - Client Commands: LOGIN, AUTHENTICATE, SELECT, EXAMINE, CLOSE, and LOGOUT
      - Server Responses: OK, NO (no permission), BAD (incorrect command),
      - When user wishes to FETCH a message, server responds in MIME format.
      - Message attributes such as size are also exchanged.
      - Flags are used by client to report user actions: SEEN, ANSWERED, DELETED, RECENT

Application Layer Protocols

- Electronic Mail
  - Internet Mail Access Protocol (IMAP)



Connection Established

Server Greeting

Not Authenticated

Authenticated

Selected

Logout

Both sides close the connection

IMAP Operation

1. Connection without pre-authentication (OK greeting)
2. Pre-authenticated connection (PREAUTH greeting)
3. Rejected connection (BYE greeting)
4. Successful LOGIN or AUTHENTICATION command
5. Successful SELECT or EXAMINE command
6. CLOSE command or failed SELECT or EXAMINE commar
7. LOGOUT command, server shutdown, or connection clos

Application Layer Protocols

- Electronic Mail
  - Internet Mail Access Protocol (IMAP)
    - IMAP4
      - The latest version is IMAP4. IMAP4 is more powerful and more complex.
      - IMAP4 provides the following extra functions:
      - A user can check the e-mail header prior to downloading.
      - A user can search the contents of the e-mail for a specific string of characters prior to downloading.
      - A user can partially download e-mail. This is especially useful if bandwidth is limited and the e-mail contains multimedia with high bandwidth requirements.
      - A user can create, delete, or rename mailboxes on the mail server.
      - A user can create a hierarchy of mailboxes in a folder for e-mail storage.

Application Layer Protocols

- Electronic Mail
  - Internet Mail Access Protocol (IMAP)
    - Advantages of IMA
      - With IMAP, the primary storage is on the server, not on the local machine.
      - Email being put away for storage can be foldered on local disk, or can be foldered on the IMAP server.
      - The protocol allows full user of remote folders, including a remote folder hierarchy and multiple inboxes.
      - It keeps track of explicit status of messages, and allows for user-defined status.
      - Supports new mail notification explicitly.
      - Extensible for non-email data, like Netnews, document storage, etc.
      - Selective fetching of individual MIME body parts.
      - Server-based search to minimize data transfer.
      - Servers may have extensions that can be negotiated.

Application Layer Protocols

- Electronic Mail
  - Post Office Protocol (POP3)
    - Post Office Protocol (POP3) is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.
    - There are two versions of POP.
      - i. The first, called POP2, became a standard in the mid-80's and requires SMTP to send messages.
      - ii. The current version, POP3, can be used with or without SMTP. POP3 uses TCP/IP port 110.
    - POP is a much simpler protocol, making implementation easier.
    - POP supports offline access to the messages, thus requires less internet usage time
    - POP does not allow search facility.
    - In order to access the messages, it is necessary to download them.
    - It allows only one mailbox to be created on server.
    - It is not suitable for accessing non mail data.
    - POP mail moves the message from the email server onto the local computer, although there is usually an option to leave the messages on the email server as well.

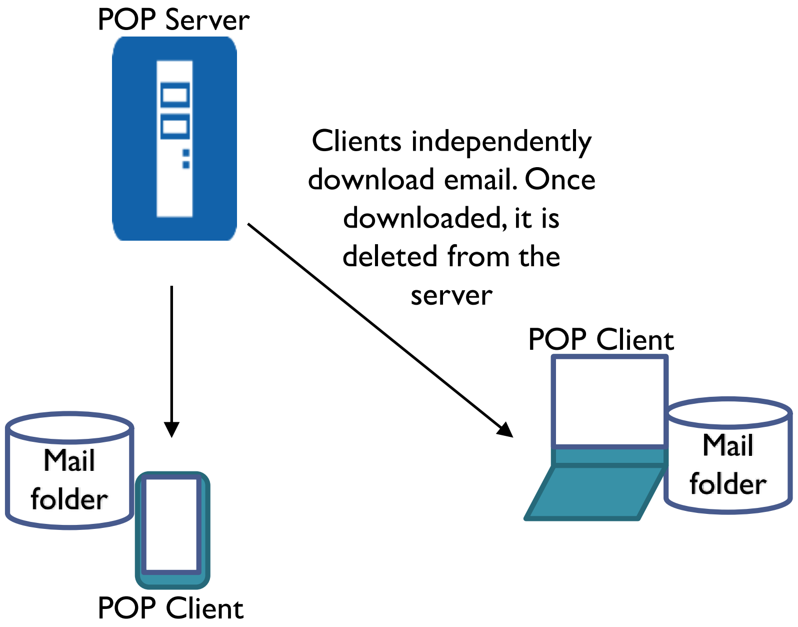
Application Layer Protocols

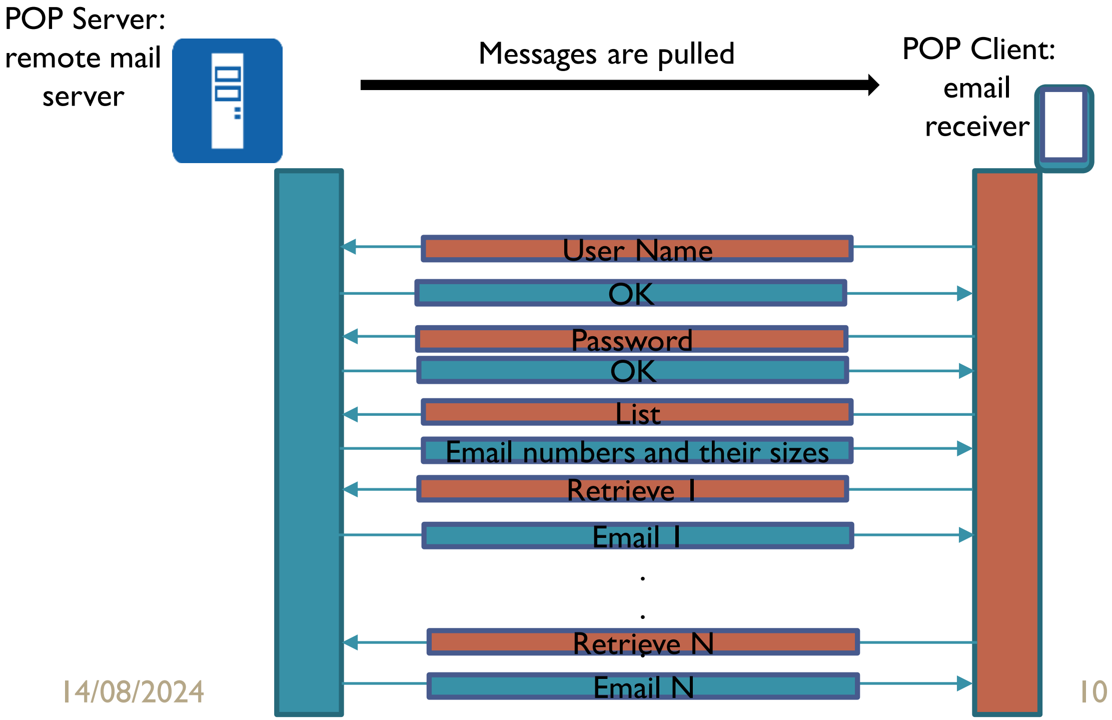
- Electronic Mail
  - Post Office Protocol (POP3)
    - POP treats the mailbox as one store, and has no concept of folders.
    - POP works in two modes namely, delete and keep mode.
      - **Delete Mode:** In delete mode, mail is deleted from the mailbox after retrieval. The delete mode is normally used when the user is working at their permanent computer and can save and organize the received mail after reading or replying.

      - **Keep Mode:** In keep mode, mail after reading is kept in mailbox for later retrieval. The keep mode is normally used when the user accesses her mail away from their primary computer.

Application Layer Protocols

- Electronic Mail
  - Post Office Protocol (POP3)
    - POP3 client is installed on the recipient computer and POP server on the mail server.
    - Client opens a connection to the server using TCP on port 110.
    - Client sends username and password to access mailbox and to retrieve messages.


POP Server
Clients independently download email. Once downloaded, it is deleted from the server
POP Client
Mail folder
Mail folder
POP Client


POP Server: remote mail server
Messages are pulled
POP Client: email receiver
User Name
OK
Password
OK
List
Email numbers and their sizes
Retrieve 1
Email 1
.
.
Retrieve N
Email N

Application Layer Protocols

- Electronic Mail
  - Post Office Protocol (POP3)
    - POP3 Commands
      - POP commands are generally abbreviated into codes of three or four letters
      - The following describes some of the POP commands:

i. UID - This command opens the connection

ii. STAT - It is used to display number of messages currently in the mailbox

iii. LIST - It is used to get the summary of messages

iv. RETR -This command helps to select a mailbox to access the messages

v. DELE - It is used to delete a message

vi. RSET - It is used to reset the session to its initial state

vii. QUIT - It is used to log off the session

Application Layer Protocols

- Electronic Mail
  - Post Office Protocol (POP3)

Difference between POP and IMAP		
	POP	IMAP
	Generally used to support single client.	Designed to handle multiple clients.
	Messages are accessed offline.	Messages are accessed online although it also supports offline mode.
	POP does not allow search facility.	IMAP offers ability to search emails.
	All the messages have to be downloaded.	It allows selective transfer of messages to the client.
	Only one mailbox can be created on the server.	Multiple mailboxes can be created on the server.
	Not suitable for accessing non-mail data.	Suitable for accessing non-mail data i.e., attachment.
	POP commands are generally abbreviated into codes of three or four letters. Eg., STAT.	IMAP commands are not abbreviated, they are full. Eg. STATUS.
	It requires minimum use of server resources.	Clients are totally dependent on server.
	Mails once downloaded cannot be accessed from some other location.	Allows mails to be accessed from multiple locations.
	The e-mails are not downloaded automatically	Users can view the headings and sender of e-mails and then decide to

Application Layer Protocols

- Electronic Mail
  - Post Office Protocol (POP3)
    - Advantages of IMAP over POP
      - IMAP is more powerful and more complex than POP.
      - User can check the e-mail header prior to downloading.
      - User can search e-mail for a specific string of characters prior to downloading.
      - User can download partially, very useful in case of limited bandwidth.
      - User can create, delete, or rename mailboxes on the mail server.

Application Layer Protocols

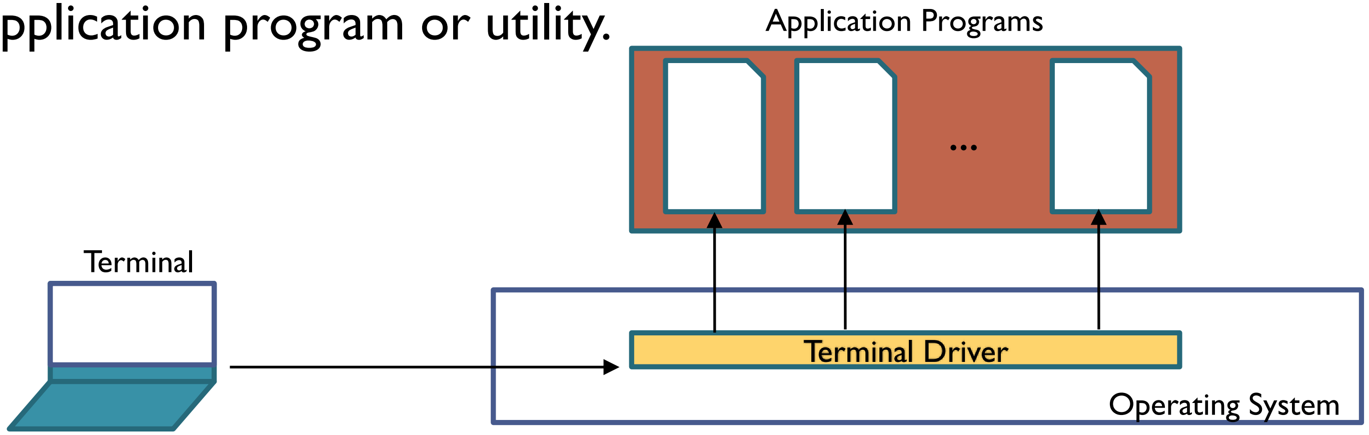
- Terminal Network (TELNET)
  - TELNET is the original remote logging protocol, based on client-server program.
  - Telnet provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side.
  - TELNET allows us to explain the issues and challenges related to the concept of remote logging.
  - Network administrators often use TELNET for diagnostic and debugging purposes.
  - TELNET requires a logging name and password.
  - It is vulnerable to hacking because it sends all data including the password in plaintext (not encrypted).
  - A hacker can eavesdrop and obtain the logging name and password. Because of this security issue, the use of TELNET has diminished.

Application Layer Protocols

- Terminal Network (TELNET)
  - Types of TELNET Logging
  - There are two types of TELNET logging:
    - Local Logging
    - Remote Logging

Application Layer Protocols

- Terminal Network (TELNET)
  - Types of TELNET Logging
    - Local Logging
      - When a user logs into a local system, it is called local logging.
      - As a user types at a terminal or at a workstation running a terminal emulator, the keystrokes are accepted by the terminal driver.
      - The terminal driver passes the characters to the operating system.
      - The operating system, in turn, interprets the combination of characters and invokes the desired application program or utility.

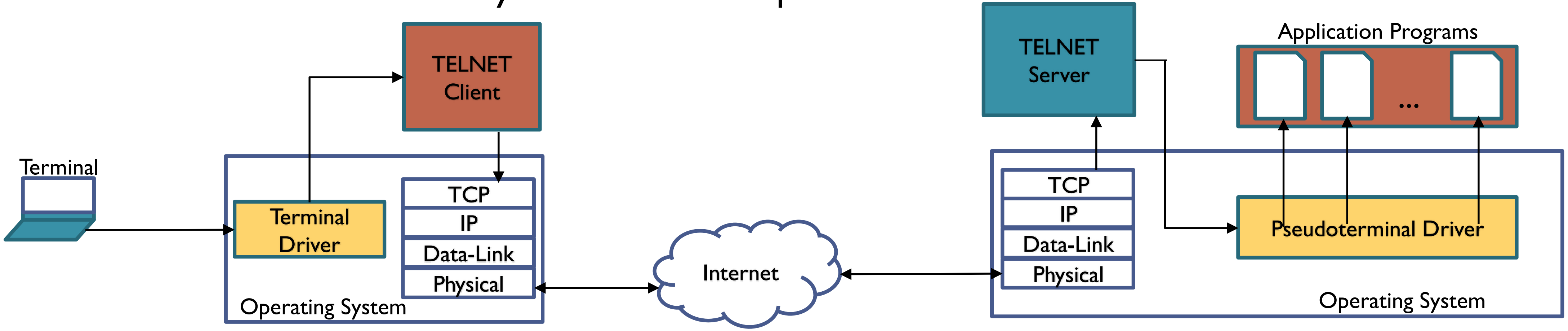


Application Layer Protocols

- Terminal Network (TELNET)
  - Types of TELNET Logging
    - Remote Logging
      - When a user wants to access an application program or utility located on a remote machine, they perform remote logging.
      - Remote Logging uses TELNET client and TELENT server programs.
      - The user sends the keystrokes to the terminal driver where the local operating system accepts the characters but does not interpret them.
      - The characters are sent to the TELNET client, which transforms the characters into a universal character set called Network Virtual Terminal (NVT) characters and delivers them to the local TCP/IP stack.

Application Layer Protocols

- Terminal Network (TELNET)
  - Types of TELNET Logging
    - Remote Logging
      - The commands or text, in NVT form, travel through the Internet and arrive at the TCP/IP stack at the remote machine.
      - The characters are delivered to the operating system and passed to the TELNET server, which changes the characters to the corresponding characters understandable by the remote computer.



Application Layer Protocols

- Terminal Network (TELNET)
  - Types of TELNET Logging
    - Remote Logging
      - The characters cannot be passed directly to the operating system because the remote operating system is not designed to receive characters from a TELNET server; it is designed to receive characters from a terminal driver.
      - A piece of software called pseudoterminal driver, is added to this, which pretends that the characters are coming from a terminal.
      - The operating system then passes the characters to the appropriate application program.

Application Layer Protocols

- Terminal Network (TELNET)
  - TELENT Options
    - TELNET lets the client and server negotiate options before or during the use of the service.
    - Options are extra features available to a user with a more sophisticated terminal.
    - Users with simpler terminals can use default features.

Application Layer Protocols

- Terminal Network (TELNET)
  - TELNET Commands

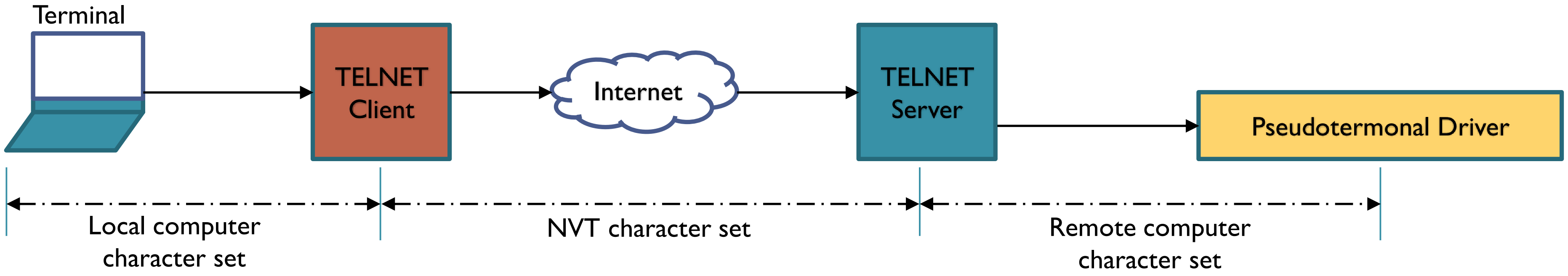
Command	Meaning
open	Connect to a remote computer
close	Close the connection
display	Show the operating parameters
mode	Change to line or character mode
set	Set the operating parameters
status	Display the status information
send	Send special characters
quit	Exit TELNET

Application Layer Protocols

- Terminal Network (TELNET)
  - Network Virtual Terminal (NVT)
    - The mechanism to access a remote computer is complex.
    - We are dealing with heterogeneous systems.
    - This is because every computer and its operating system accepts a special combination of characters as tokens.
    - For example, the end-of-file token in a computer running the DOS operating system is Ctrl+z, while the UNIX operating system recognizes Ctrl+d.
    - If we want to access any remote computer in the world, we must first know what type of computer we will be connected to, and we must also install the specific terminal emulator used by that computer.

Application Layer Protocols

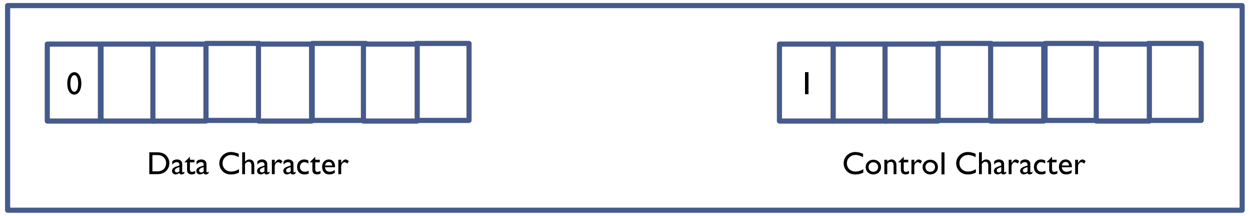
- Terminal Network (TELNET)
  - Network Virtual Terminal (NVT)
  - TELNET solves this problem by defining a universal interface called the Network Virtual Terminal (NVT) character set.
  - Via this interface, the client TELNET translates characters (data or commands) that come from the local terminal into NVT form and delivers them to the network.



  - The server TELNET, on the other hand, translates data and commands from NVT form into the form acceptable by the remote computer.

Application Layer Protocols

- Terminal Network (TELNET)
  - NVT Character Format
    - NVT uses two sets of characters, one for data and one for control.
    - For data, NVT normally uses what is called NVT ASCII. This is an 8-bit character set in which the seven lowest order bits are the same as ASCII and the highest order bit is 0.
    - To send control characters between computers , NVT uses an 8-bit character set in which the highest order bit is set to 1.



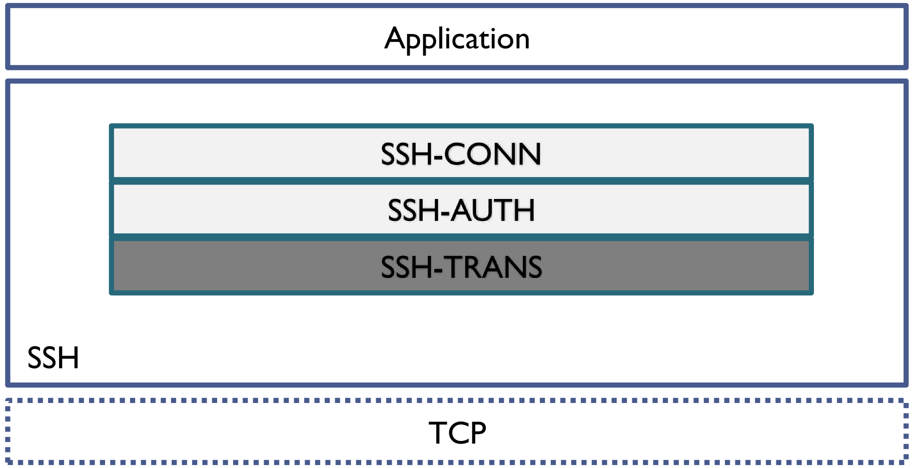
NVT Character Format

Application Layer Protocols

- Secure Shell (SSH)
  - Secure Shell (SSH) is a secure application program that can be used today for several purposes such as remote logging and file transfer, it was originally designed to replace TELNET.
  - 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 flaws in it.

Application Layer Protocols

- Secure Shell (SSH)
  - Components of SSH
    - SSH protocol has three components:
      1. SSH Transport-Layer Protocol (SSH-TRANS)
      2. SSH Authentication Protocol (SSH-AUTH)
      3. SSH Connection Protocol (SSH-CONN)



Application Layer Protocols

- Secure Shell (SSH)
  - Components of SSH
    - SSH Connection Protocol (SSH-CONN)
      - After the secured channel is established and both server and client are authenticated for each other, SSH can call a piece of software that implements the third protocol, SSH-CONN.
      - One of the services provided by the SSH-CONN protocol is multiplexing.
      - SSH-CONN takes the secure channel established by the two previous protocols and lets the client create multiple logical channels over it.
      - Each channel can be used for a different purpose, such as remote logging, file transfer, and so on.

Application Layer Protocols

- Secure Shell (SSH)
  - Components of SSH
    - SSH Authentication Protocol (SSH-AUTH)
      - After a secure channel is established between the client and the server and the server is authenticated for the client.
      - SSH can call another procedure that can authenticate the client for the server.
      - This layer defines a number of authentication tools similar to the ones used in SSL.
      - Authentication starts with the client, which sends a request message to the server.
      - The request includes the user name, server name, the method of authentication, and the required data.
      - The server responds with either a success message, which confirms that the client is authenticated, or a failed message, which means that the process needs to be repeated with a new request message.

Application Layer Protocols

- Secure Shell (SSH)
  - Components of SSH
    - SSH Transport-Layer Protocol (SSH-TRANS)
      - SSH first uses a protocol that creates a secured channel on top of the TCP.
      - This new layer is an independent protocol referred to as SSH-TRANS.
      - When the procedure implementing this protocol is called, the client and server first use the TCP protocol to establish an insecure connection.
      - Then they exchange several security parameters to establish a secure channel on top of the TCP.

Application Layer Protocols

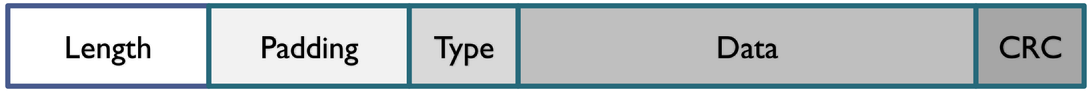
- Secure Shell (SSH)
  - Application of SSH
    - SSH is a general-purpose protocol that provides a secure connection between a client and server.
      - SSH for Remote Logging
        - Several free and commercial applications use SSH for remote logging.
        - Among them, we can mention PuTTy, by Simon Tatham, which is a client SSH
        - program that can be used for remote logging.
        - Another application program is Tectia, which can be used on several platforms.
      - SSH for File Transfer
        - One of the application programs that is built on top of SSH for file transfer is the Secure File Transfer Program (sftp).
        - The sftp application program uses one of the channels provided by the SSH to transfer files.
        - Another common application is called Secure Copy (scp).
        - This application uses the same format as the UNIX copy command, cp, to copy files.

Application Layer Protocols

- Secure Shell (SSH)
  - Application of SSH
    - Port Forwarding
      - One of the interesting services provided by the SSH protocol is port forwarding.
      - We can use the secured channels available in SSH to access an application program that does not provide security services.
      - Applications such as TELNET and Simple Mail Transfer Protocol (SMTP), can use the services of the SSH port forwarding mechanism.
      - The SSH port forwarding mechanism creates a tunnel through which the messages belonging to other protocols can travel.
      - For this reason, this mechanism is sometimes referred to as SSH tunneling.

Application Layer Protocols

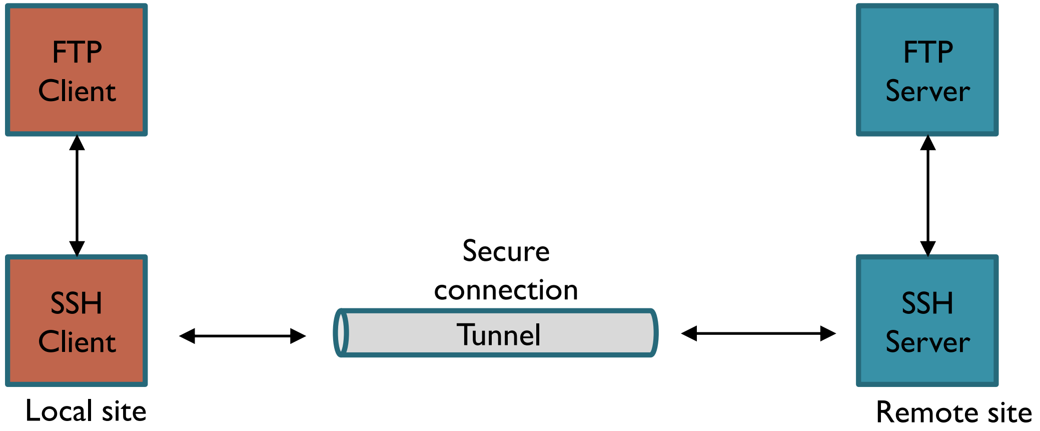
- Secure Shell (SSH)
  - SSH Packet Format
    - The length field defines the length of the packet but does not include the padding.
    - The Padding field is added to the packet to make the attack on the security provision more difficult.
    - The type field designates the type of the packet used in different SSH protocols.
    - The data field is the data transferred by the packet in different protocols.
    - The CRC field is used for error detection.



Length	Padding	Type	Data	CRC

Application Layer Protocols

- Secure Shell (SSH)
  - Securing FTP Applications Using SSH
    - The FTP client can use the SSH client on the local site to make a secure connection with the SSH server on the remote site.
    - Any request from the FTP client to the FTP server is carried through the tunnel provided by the SSH client and server.
    - Any response from the FTP server to the FTP client is also carried through the tunnel provided by the SSH client and server.



Questions!