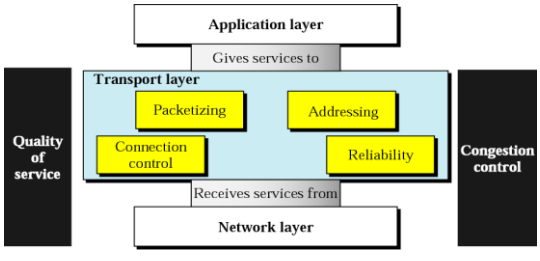
Unit - IV

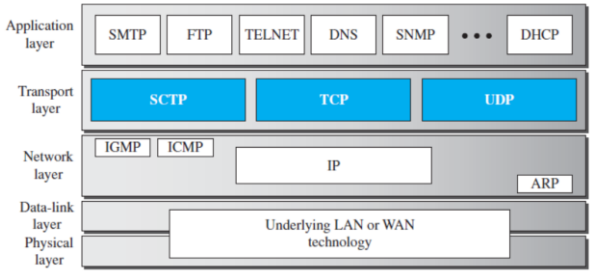
Learning Objective

- ***Client-Server Paradigm***
- ***Addressing***
- ***Multiplexing and Demultiplexing***
- ***Connectionless/Connection-Oriented***
- ***Reliable/Unreliable***

Position of transport layer



Position of transport layer

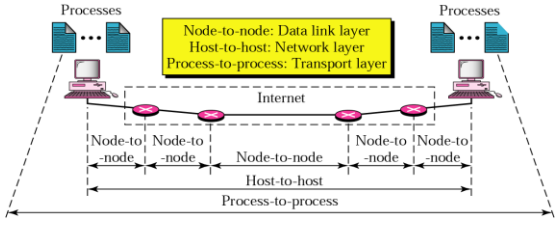


Transport Layer

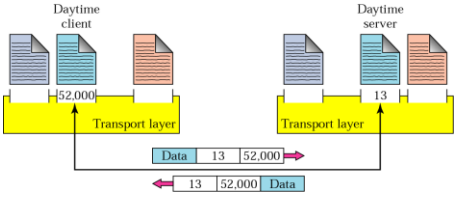
Note:

The transport layer is responsible for process-to-process delivery.

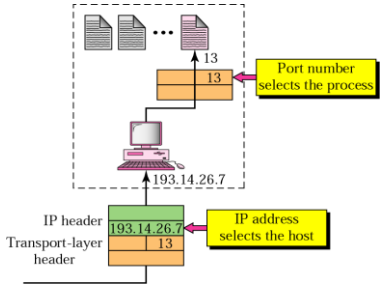
Transport Layer



Port numbers



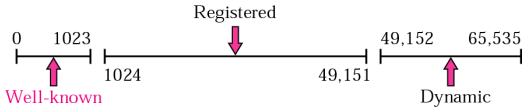
IP addresses versus port numbers



Port numbers

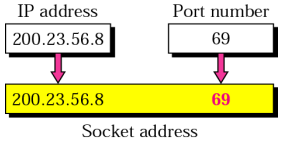
- Well-known port:
  - The ports ranging from 0 to 1023 are assigned and controlled by ICANN.
- Registered ports:
  - The ports ranging from 1024 to 49,151 are not assigned or controlled by ICANN.
  - They can only be registered with ICANN to prevent duplication.
- Dynamic ports:
  - The ports ranging from 49,152 to 65,535 are neither controlled nor registered.
  - They can be used as temporary or private port numbers.

Cont ….

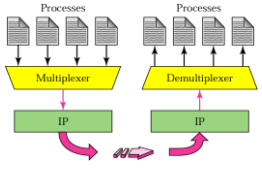


Socket address

- A transport-layer protocol in the TCP suite needs both the IP address and the port number, at each end, to make a connection.
- The combination of an IP address and a port number is called a socket address.

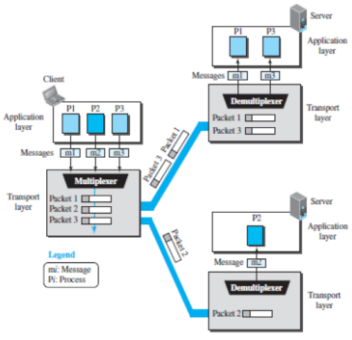


Multiplexing and demultiplexing



- Whenever an entity accepts items from more than one source, this is referred to as multiplexing (many to one);
- Whenever an entity delivers items to more than one source, this is referred to as demultiplexing (one to many).

Multiplexing and demultiplexing



Pushing or Pulling

- If the sender delivers items whenever they are produced, without a prior request from the consumer, the delivery is referred to as pushing.
- If the producer delivers the items after the consumer has requested them, the delivery is referred to as pulling.

Pushing or Pulling

When the producer pushes the items, the consumer may be overwhelmed and there is a need for flow control.

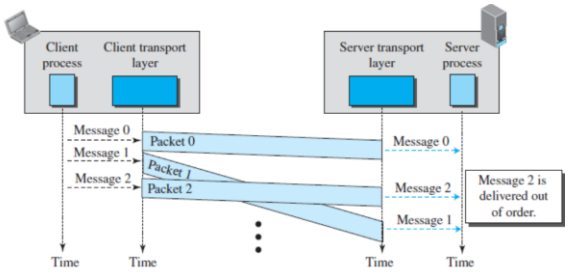
When the consumer pulls the items, it requests them when it is ready. In this case, there is no need for flow control.

Connectionless and Connection-Oriented

- Connectionless Service:
  - In a connectionless service, the source process (application program) needs to divide its message into chunks of data of the size acceptable by the transport layer and deliver them to the transport layer one by one.
  - The transport layer treats each chunk as a single unit without any relation between the chunks.
  - Packets may arrive out of order at the destination and will be delivered out of order to the server process
  - No flow control, error control, or congestion control can be effectively implemented in a connectionless service

 U4.16

Connectionless and Connection-Oriented



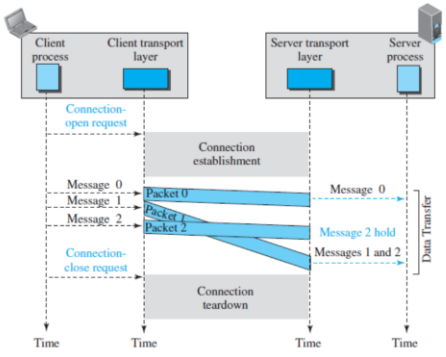
 U4.17

Connectionless and Connection-Oriented

- Connection-Oriented Service:
  - The client and the server first need to establish a logical connection between themselves.
  - The data exchange can only happen after the connection establishment.
  - After data exchange, the connection needs to be torn down
  - We can implement flow control, error control, and congestion control in a connection-oriented protocol.

 U4.18

Connectionless and Connection-Oriented



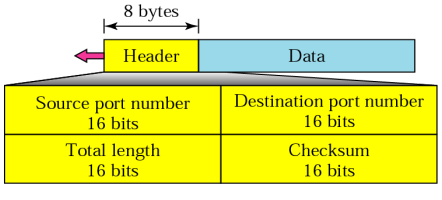
UDP

Port Numbers

User Datagram

Applications

User datagram format



Cont ….

Note:

The calculation of checksum and its inclusion in the user datagram are optional.

Cont ….

Note:

UDP is a connectionless, unreliable protocol that has no flow and error control. It uses port numbers to multiplex data from the application layer.

Cont ….

Note:

UDP is a convenient transport-layer protocol for applications that provide flow and error control. It is also used by multimedia applications.

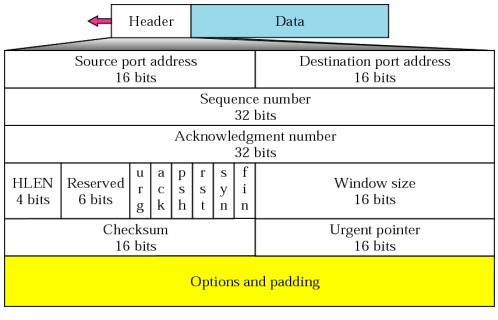
Well-known ports used by UDP

Port	Protocol	Description
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
53	Nameserver	Domain Name Service
67	Bootps	Server port to download bootstrap information
68	Bootpc	Client port to download bootstrap information
69	TFTP	Trivial File Transfer Protocol
111	RPC	Remote Procedure Call
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management Protocol
162	SNMP	Simple Network Management Protocol (trap)

TCP

- *Port Numbers*
- *Services*
- *Sequence Numbers*
- *Segments*
- *Connection*
- *Transition Diagram*
- *Flow and Error Control*
- *Silly Window Syndrome*

TCP segment format

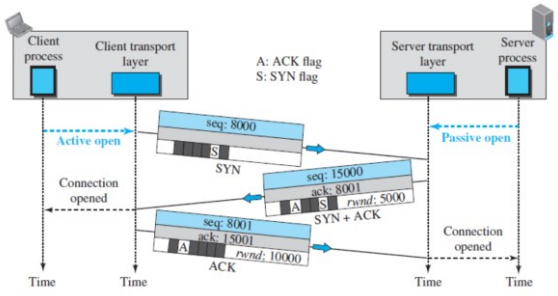


Well-known ports used by TCP

Port	Protocol	Description
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
20	FTP, Data	File Transfer Protocol (data connection)
21	FTP, Control	File Transfer Protocol (control connection)
23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

 U4.28

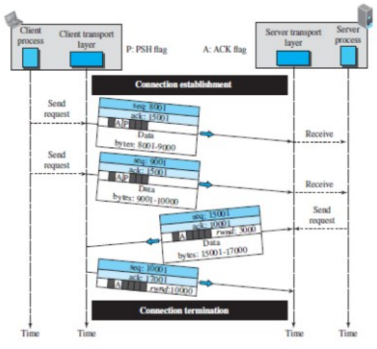
Connection Establishment Using Three-way Handshaking



rwnd: receive window size

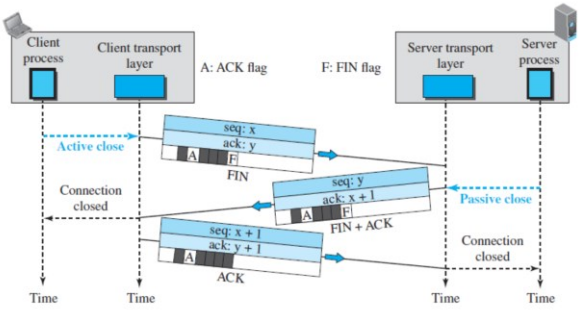
 U4.29

Data Transfer in TCP

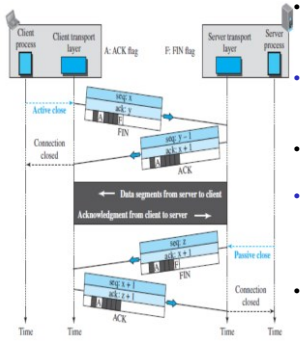


 U4.30

Connection Termination Using Three-way Handshaking

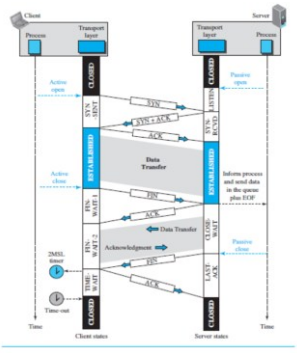


Half Close



- Client sends the all data to the server and request for connection close.
- Server sends the acknowledgement to client to close connection.
- But, server is still open. (Half Close)
- After processing the data, server send the data to the client and after that server gets acknowledgment from client.
- After finishing all the processes, the server send the connection close request to client

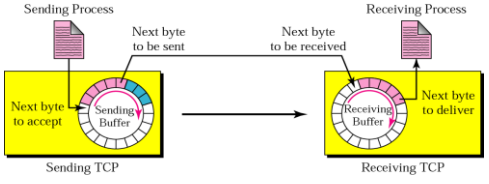
Time-line Diagram for a Common Scenario



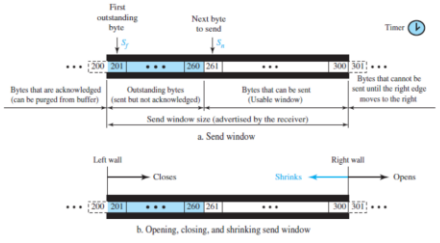
Flow Control

- Flow Control basically means that TCP will ensure that a sender is not overwhelming a receiver by sending packets faster than it can consume.
- TCP stores the data it needs to send in the send buffer, and the data it receives in the receive buffer.
- To control the amount of data that TCP can send, the receiver will advertise its Receive Window (rwnd), that is, the spare room in the receive buffer.
- Transmission Control Protocol (TCP) uses a sliding window for flow control.

Sending and receiving buffers

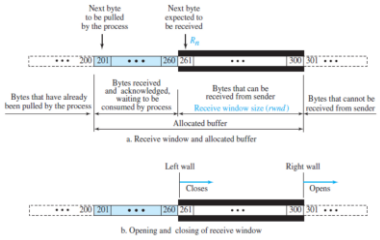


Send Window in TCP



- The opening window process allows more data to be in the buffer that can be sent.
- The closing window process indicates some sent data bytes have been acknowledged.
- The shrinking windows process denotes the decrement in the window size.
- The receiver can open or close the window but shrinking window is not recommended.

Receive Window in TCP



- The opening window process allows more data to be in the buffer that can be sent.
- The closing window process indicates some sent data bytes have been acknowledged.

rwnd = buffer size - number of waiting bytes to be pulled

Flow Control

- TCP on the sending system must wait to send more data until all bytes in the current send buffer are acknowledged by TCP on the receiving system.
- On the receiving system, TCP stores received data in a receive buffer.
- TCP acknowledges receipt of the data, and advertises (communicates) a new receive window to the sending system.
- If the receive buffer is full, the receiving system advertises a receive window size of zero, and the sending system must wait to send more data.

Flow Control

- After the receiving application retrieves data from the receive buffer, the receiving system can then advertise a receive window size that is equal to the amount of data that was read.
- TCP on the sending system can resume sending data.

Silly Window Syndrome

- Window Shutdown:
  - The receiver can temporarily shut down the window by sending a *rwnd* of 0.
- Probing:
  - Even when the window is shut down by an order from the receiver, the sender can always send a segment with 1 byte of data.
- A serious problem can arise in the sliding window operation when either the sending application program creates data slowly or the receiving application program consumes data slowly, or both.

Silly Window Syndrome

- For example,
  - If TCP sends segments containing only 1 byte of data, it means that a 41-byte datagram (20 bytes of TCP header and 20 bytes of IP header) transfers only 1 byte of user data.
  - Here the overhead is 41/1.
  - If we include the overhead of DLL and Physical Layer, it could be worse.
  - This indicates that we are using the capacity of the network very inefficiently.
  - This problem is called the Silly Window Syndrome

Silly Window Syndrome

- Syndrome Created by the Sender
  - The sending TCP may create a silly window syndrome if it is serving an application program that creates data slowly, for example, 1 byte at a time.
- Syndrome Created by the Receiver
  - The receiving TCP may create a silly window syndrome if it is serving an application program that consumes data slowly, for example, 1 byte at a time.

Error Control

- TCP provides reliability using error control.
- Error control includes mechanisms for
  - Detecting and resending corrupted segments,
  - Resending lost segments,
  - Storing out-of-order
  - Segments until missing segments arrive,
  - And detecting and discarding duplicated segments.

Error Control

- Error control in TCP is achieved through
  - Checksum
    - ✓If a segment is corrupted, as detected by an invalid checksum, the segment is discarded by the destination TCP and is considered as lost
    - ✓TCP uses a 16-bit checksum that is mandatory in every segment.
  - Acknowledgment
    - ✓TCP uses acknowledgments to confirm the receipt of data segments.
    - ✓Control segments that carry no data, but consume a sequence number, are also acknowledged.
    - ✓ACK segments are never acknowledged.

Error Control

- Error control in TCP is achieved through
  - Checksum
    - ✓If a segment is corrupted, as detected by an invalid checksum, the segment is discarded by the destination TCP and is considered as lost
    - ✓TCP uses a 16-bit checksum that is mandatory in every segment.
  - Acknowledgment
    - ✓TCP uses acknowledgments to confirm the receipt of data segments.
    - ✓Control segments that carry no data, but consume a sequence number, are also acknowledged.
    - ✓ACK segments are never acknowledged.

Error Control

- Acknowledgment
  - ✓Cumulative Acknowledgment (ACK):
    - The receiver acknowledges that it correctly received a packet, message, or segment in a stream which implicitly informs the sender that the previous packets were received correctly
  - ✓Selective Acknowledgment (SACK):
    - TCP may experience poor performance when multiple packets are lost from one window of data with Cumulative Acknowledgement.
    - SACKs allow a receiver to acknowledge non-consecutive data, so that the sender can retransmit only what is missing at the receiver's end.
    - Since there is no provision in the TCP header for adding this type of information, SACK is implemented as an option at the end of the TCP header.

Error Control

- Retransmission:
  - ✓When a segment is sent, it is stored in a queue until it is acknowledged at sender side.
  - ✓When the retransmission timer expires or when the sender receives three duplicate ACKs for the first segment in the queue, that segment is retransmitted.
    - Retransmission after RTO:
      - The sending TCP maintains one retransmission time-out (RTO) for each connection.
      - When the timer matures, i.e. times out, TCP resends the segment in the front of the queue (the segment with the smallest sequence number) and restarts the timer.
      - The value of RTO is dynamic in TCP and is updated based on the round-trip time (RTT) of segments.

Error Control

- Retransmission:
  - Retransmission after Three Duplicate ACK Segments:
    - If RTO is large, more time is needed to get confirmation about whether a segment has been delivered or not.
    - If three or more duplicate ACKs are received in a row, it is a strong indication that a segment has been lost.
    - To expedite service throughout the Internet, when three duplicate ACKs received, the missing segment immediately without waiting for the time-out
- Out-of-Order Segments:
  - ✓TCP do not discard out-of-order segments.
  - ✓They store them temporarily and flag them as out-of-order segments until the missing segments arrive.

Data may arrive out of order and be temporarily stored by the receiving TCP, but TCP guarantees that no out-of-order data are delivered to the process.

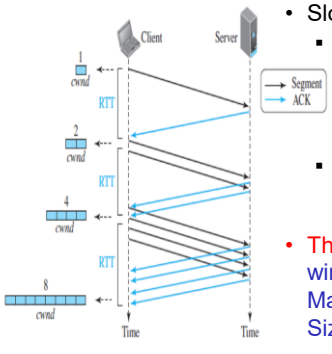
Congestion Control

- To control the number of segments to transmit, TCP uses another variable called a congestion window, *cwnd*, whose size is controlled by the congestion situation in the network.
- The *cwnd* variable and the *rwnd* variable together define the size of the send window in TCP.
- Actual window size = minimum (rwnd, cwnd)

Congestion Control

- TCP's general policy for handling congestion consists of following three phases-
  - Slow Start
  - Congestion Avoidance
  - Congestion Detection

Congestion Control

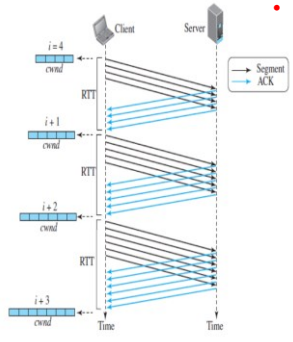


- Slow Start:
  - The sender sends the packet and gradually increases the number of packets until it reaches a threshold.
  - The size of congestion window increases exponentially.
- Threshold= (Receiver window size / Maximum Segment Size) / 2

Congestion Control

For each ACK, the cwnd is increased by only 1. Hence, if two segments are acknowledged cumulatively, the size of the cwnd increases by only 1, not 2. The growth is still exponential, but it is not a power of 2.

Congestion Control



- Congestion Avoidance: Additive Increase
  - Sender increases the congestion window size linearly to avoid the congestion
  - On receiving each acknowledgement, sender increments the congestion window size by 1.
  - Congestion window size = Congestion window size + 1

Congestion Control

In the congestion-avoidance algorithm, the size of the congestion window increases additively until congestion is detected

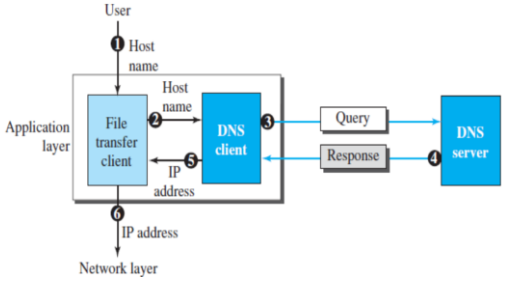
Congestion Control

- Congestion Detection
  - When sender detects the loss of segments, it reacts in different ways depending on how the loss is detected
  - There're two conditions when TCP detects congestion.
    - ✓When there is no acknowledgment received for a packet sent by the sender within an estimated time.
      - Start a new slow start phase
    - ✓The second condition occurs when the receiver gets three duplicate acknowledgments.
      - Begin a new congestion avoidance phase

Domain Name System

- To identify an entity, TCP/IP protocols use the IP address, which uniquely identifies the connection of a host to the Internet.
- People prefer to use names instead of numeric addresses.
- Therefore, the Internet needs to have a directory system that can map a name to an address.
- A better solution is to distribute the information among many computers in the world.
- The host that needs mapping can contact the closest computer holding the needed information.
- This method is called Domain Name System.

Domain Name System



Domain Name System

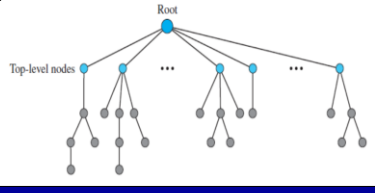
- The names must be unique because the addresses are unique.
- A name space that maps each address to a unique name can be organized in two ways
  - Flat
    - ✓A name in this space is a sequence of characters without structure
    - ✓It cannot be used in a large system such as the Internet because it must be centrally controlled to avoid ambiguity and duplication.

Domain Name System

- Hierarchical.
  - ✓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, the third part can define departments in the organization, and so on.

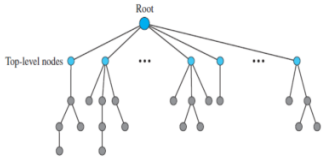
Domain Name Space

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



Domain Name Space

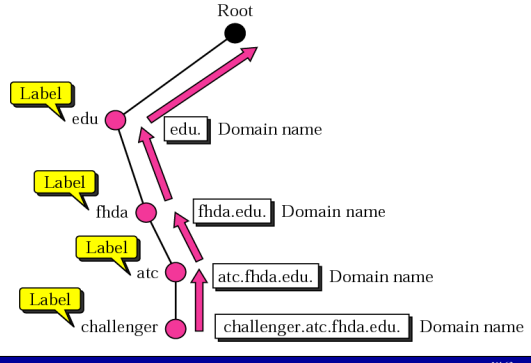
- Label:
  - Each node in the tree has a label, which is a string with a maximum of 63 characters
  - The root label is a null string (empty string).
  - DNS requires that children of a node (nodes that branch from the same node) have different labels, which guarantees the uniqueness of the domain names.



Domain Name Space

- Domain Name:
  - Each node in the tree has a 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.
  - 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.

Domain Name Space

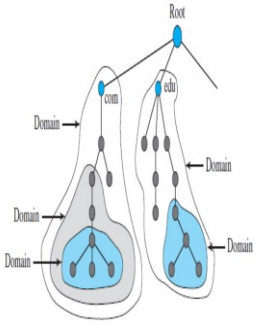


Domain Name Space

- 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).

FQDN	PQDN
challenger.atc.fhda.edu. cs.hmme.com. www.funny.int.	challenger.atc.fhda.edu cs.hmme www

Domain Name Space



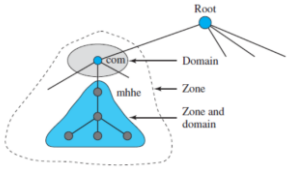
- A domain is a subtree of the domain name space.
- The name of the domain is the name of the node at the top of the subtree.
- A domain may itself be divided into domains.

Domain Name Space

- Distribution of Name Space
  - The information contained in the domain name space must be stored.
  - 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.

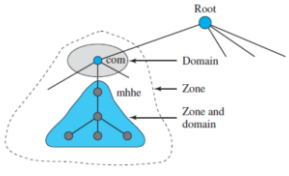
Domain Name Space

- Zone
  - Since the complete domain name hierarchy cannot be stored on a single server, it is divided among many servers.
  - What a server is responsible for or has authority over is called a zone.



Domain Name Space

- Zone
  - if a server divides its domain into subdomains and delegates part of its authority to other servers, "domain" and "zone" refer to different things.
  - Otherwise, Zone and Domain are same.



Domain Name Space

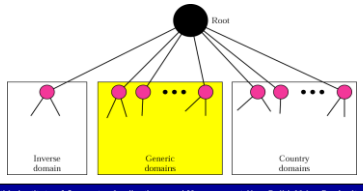
- Root Server
  - A root server is a server whose zone consists of the whole tree.
  - Root server usually does not store any information about domains but delegates its authority to other servers, keeping references to those servers.
    - ✓Primary Servers
      - A primary server is a server that stores a file about the zone for which it is an authority.
      - It is responsible for creating, maintaining, and updating the zone file.
      - It stores the zone file on a local disk.

Domain Name Space

- Root Server
  - ✓Secondary Servers
    - 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 disk.
    - The secondary server neither creates nor updates the zone files.
    - If updating is required, it must be done by the primary server, which sends the updated version to the secondary.

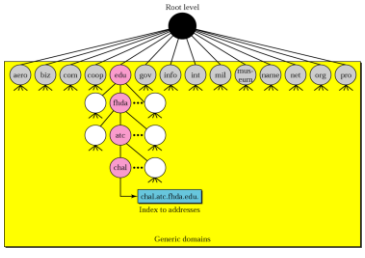
Domain Name Space

- DNS on the Internet
  - On the Internet, the domain name space (tree) was originally divided into three different sections:
  - Generic domains,
  - Country domains,
  - The inverse domains.



Domain Name Space

- The generic domains define registered hosts according to their generic behavior



Domain Name Space

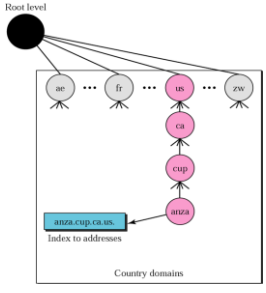
Label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers

Domain Name Space

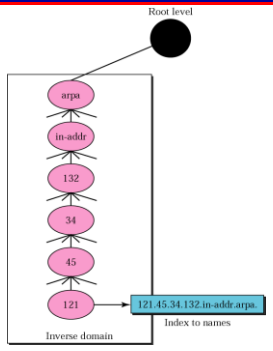
Label	Description
int	International organizations
mil	Military groups
museum	Museums and other non-profit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

Domain Name Space

- The country domains section uses two-character country abbreviations



Domain Name Space



Domain Name Space

- Resolution
  - Mapping a name to an address is called name-address resolution.
  - A host that needs to map an address to a name or a name to an address calls a DNS client called 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.

Domain Name Space

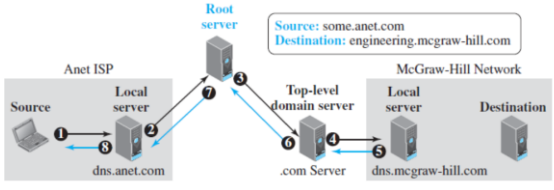
- Resolution
  - Recursive Resolution
  - Iterative Resolution

Domain Name Space

- 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
    - ✓If local DNS Server does not know this address, it sends the query to a root DNS server
    - ✓The root server the send the query to the top-level-domain server
    - ✓If top-level-server does not know the address, it forwards the query to the local DNS server, where the address is available

Domain Name Space

- Resolution
  - Recursive Resolution

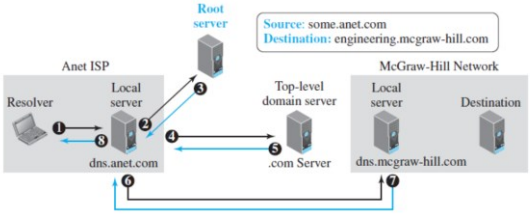


Domain Name Space

- Resolution
  - 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.
    - ✓Normally the iterative resolution takes place between two local servers; the original resolver gets the final answer from the local server.

Domain Name Space

- Resolution
  - Iterative Resolution



  - Note that the messages shown by events 2, 4, and 6 contain the same query.

Domain Name Space

- Caching
  - When a server asks for a mapping from another server and receives the response, it stores this information in its cache memory before sending it to the client.
  - If the same or another client asks for the same mapping, it can check its cache memory
  - To inform the client that the response is coming from the cache memory and not from an authoritative source, the server marks the response as unauthoritative.

Domain Name Space

- Caching
  - Problem:
    - ✓If a server caches a mapping for a long time, it may send an outdated mapping to the client.
    - ✓DNS requires that each server keep a TTL counter for each mapping it caches.
    - ✓The cache memory must be searched periodically and those mappings with an expired TTL must be purged.

E-Mail

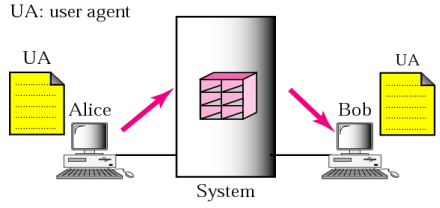
Electronic Mail: SMTP, POP, and IMAP

To explain the architecture of email, there are following Scenario :

First Scenario
Second Scenario
Third Scenario
Fourth Scenario

E-Mail

First Scenario



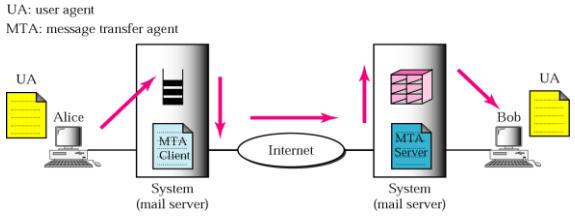
E-Mail

First Scenario

When the sender and the receiver of an email are on the same system, we need only two user agents.

E-Mail

Second Scenario



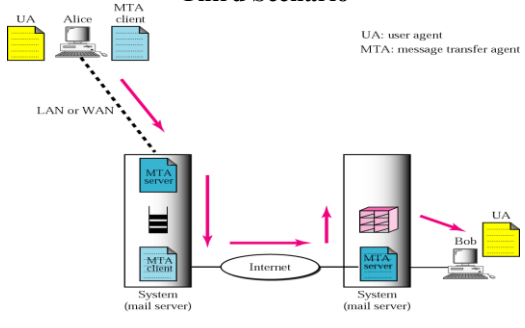
E-Mail

Second Scenario

When the sender and the receiver of an email are on different systems, we need two UAs and a pair of MTAs (client and server).

E-Mail

Third Scenario



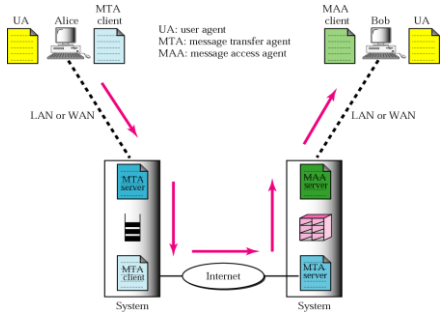
E-Mail

Third Scenario

When the sender is connected to the mail server via a LAN or a WAN, we need two UAs and two pairs of MTAs (client and server).

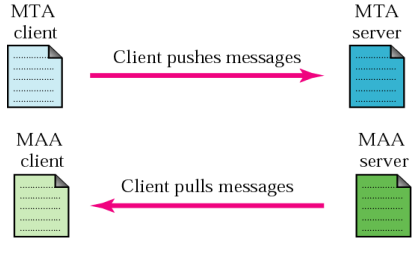
E-Mail

Fourth Scenario



E-Mail

Fourth Scenario



E-Mail

Fourth Scenario

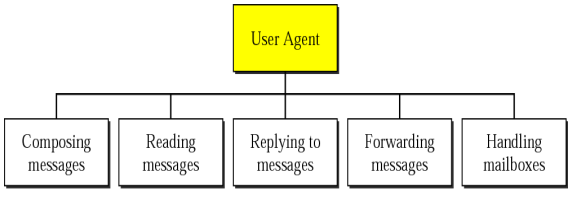
When both sender and receiver are connected to the mail server via a LAN or a WAN, we need two UAs, two pairs of MTAs (client and server), and a pair of MAAs (client and server). This is the most common situation today.

E-Mail

User Agent

The user agent (UA) provides service to the user to make the process of sending and receiving a message easier.

E-Mail



E-Mail

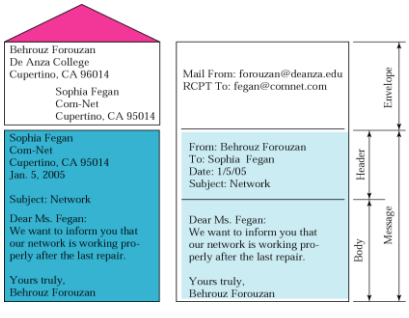
Some examples of command-driven user agents are mail, pine, and elm

E-Mail

Some examples of GUI-based user agents are Eudora, Outlook, and Netscape.

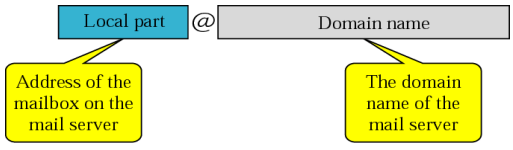
E-Mail

Format of an E-mail



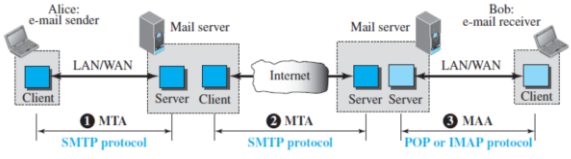
E-Mail

E-Mail Address



E-Mail

- Protocols used in Email



E-Mail

- SMTP (Simple Message Transfer Protocol):
  - SMTP simply defines how commands and responses must be sent back and forth.
    - ✓Commands are sent from the client to the server.
    - ✓Responses are sent from the server to the client.
      - A response is a three-digit code that may be followed by additional textual information

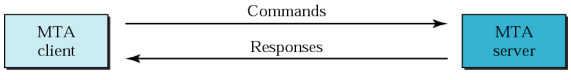
E-Mail

SMTP

The actual mail transfer requires message transfer agents (MTAs). The protocol that defines the MTA client and server in the Internet is called Simple Mail Transfer Protocol (SMTP).

E-Mail

Command and Responses



E-Mail

Commands

Keyword	*Argument(s)*
HELO	Sender's host name
MAIL FROM	Sender of the message
RCPT TO	Intended recipient of the message
DATA	Body of the mail
QUIT	
RSET	
VRFY	Name of recipient to be verified
NOOP	
TURN	
EXPN	Mailing list to be expanded
HELP	Command name
SEND FROM	Intended recipient of the message
SMOL FROM	Intended recipient of the message
SMAL FROM	Intended recipient of the message

E-Mail

Responses

Code	Description
	Positive Completion Reply
211	System status or help reply
214	Help message
220	Service ready
221	Service closing transmission channel
250	Request command completed
251	User not local; the message will be forwarded
	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 storage

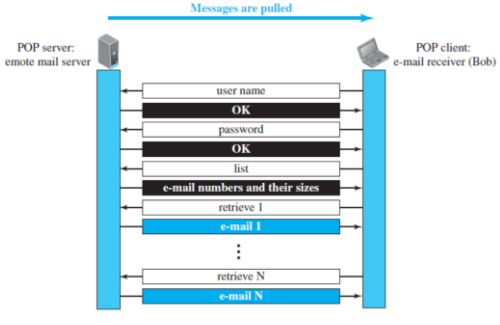
E-Mail

Post Office Protocol (POP)

- The client POP3 software is installed on the recipient computer
- The server POP3 software is installed on the mail server.
- Mail access starts with the client when the user needs to download its e-mail from the mailbox on the mail server.
- The client opens a connection to the server on TCP port 110 and provide username and password.

E-Mail

Post Office Protocol (POP)



E-Mail

Post Office Protocol (POP)

- POP3 has two modes: the delete mode and the keep mode.
  - In the delete mode, the mail is deleted from the mailbox after each retrieval.
  - In the keep mode, the mail remains in the mailbox after retrieval.

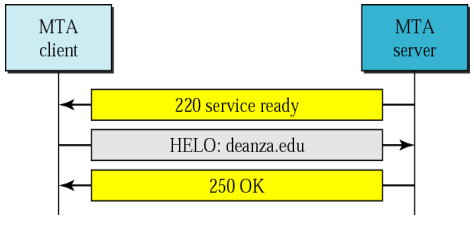
E-Mail

Internet Mail Access Protocol (IMAP)

- IMAP4 is similar to POP3, but it has more features
  - 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. (Sometimes email contains bulky multimedia files)
  - 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

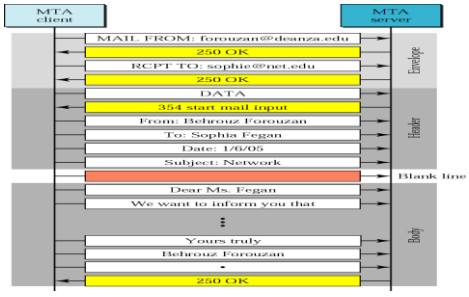
E-Mail

Connection establishment



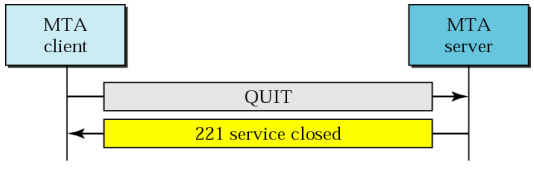
E-Mail

Message Transfer



E-Mail

Connection Termination



E-Mail

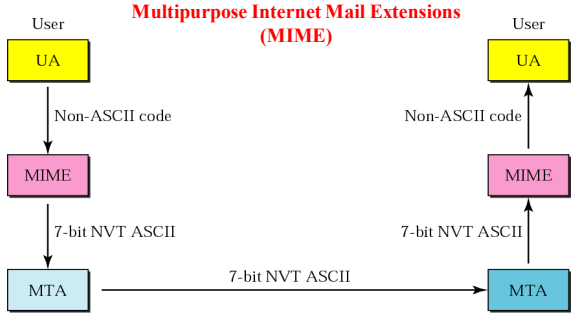
Multipurpose Internet Mail Extensions (MIME)

- Electronic mail has a simple structure.
- It can send messages only in NVT 7-bit ASCII format.
- It cannot be used for languages other than English (such as French, German, Hebrew, Russian, Chinese, and Japanese).
- It cannot be used to send binary files or video or audio data.

NVT: Network Virtual Terminal

E-Mail

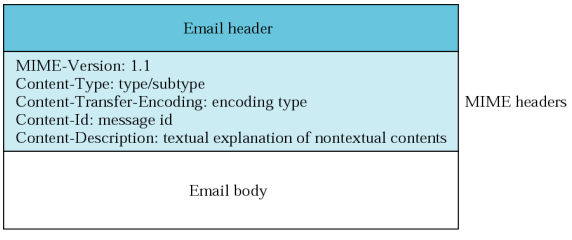
Multipurpose Internet Mail Extensions (MIME)



NVT: Network Virtual Terminal

E-Mail

MIME Header



E-Mail

Data Types and Sub Types in MIME

Type	*Subtype*	*Description*
Text	Plain	Unformatted
	HTML	HTML format (see Chapter 22)
Multipart	Mixed	Body contains ordered parts of different data types
	Parallel	Same as above, but no order
	Digest	Similar to Mixed, but the default is message/RFC822
	Alternative	Parts are different versions of the same message

E-Mail

Data Types and Sub Types in MIME

Type	*Subtype*	*Description*
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 8 KHz
Application	PostScript	Adobe PostScript
	Octet-stream	General binary data (eight-bit bytes)

 U4.118

E-Mail

Content Transfer Encoding

Type	*Description*
7bit	NVT ASCII characters and short lines
8bit	Non-ASCII characters and short lines
Binary	Non-ASCII characters with unlimited-length lines
Base64	6-bit blocks of data are encoded into 8-bit ASCII characters
Quoted-printable	Non-ASCII characters are encoded as an equal sign followed by an ASCII code

 U4.119

Summary

- The UA prepares the message, creates the envelope, and puts the message in the envelope.
- The mail address consists of two parts : local part (user mail box) and domain name. localpart@domainname
- MIME allows the transfer of multimedia messages.
- MTA transfers the mail across the Internet.
- SMTP uses commands and responses to transfer messages between an MTA client and an MTA server.

 U4.120

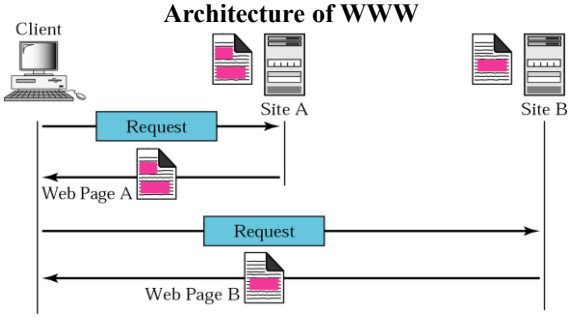
WWW

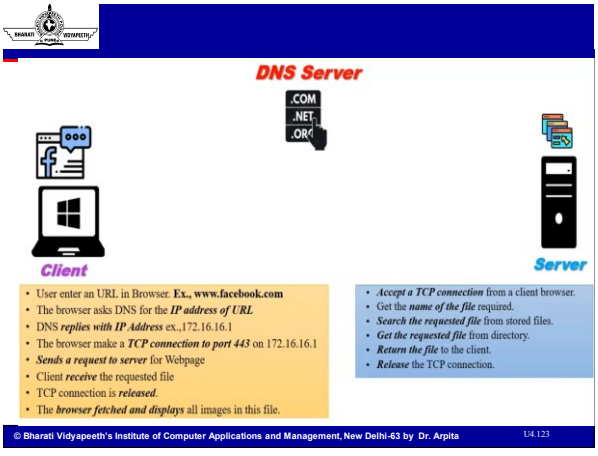
•World Wide web

The WWW is a distributed client-server service, in which a client using a browser can access a service using a server. The service provided is distributed over many locations called sites.

WWW

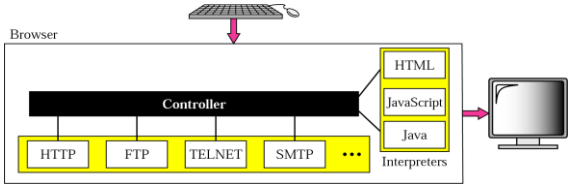
Architecture of WWW





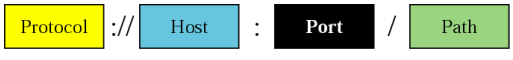
WWW

Browser



WWW

URL



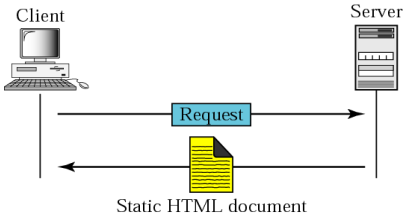
WWW

Web Documents

The documents in the WWW can be grouped into three broad categories: static, dynamic, and active. The category is based on the time the contents of the document are determined.

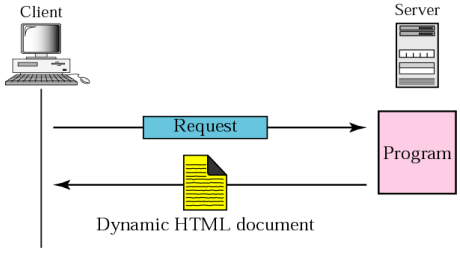
WWW

Static



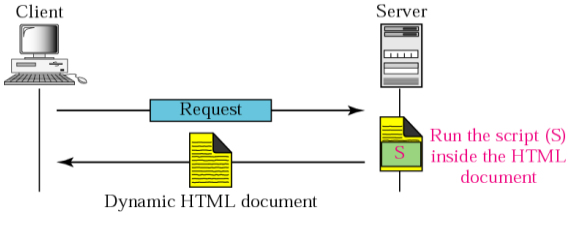
WWW

Dynamic Document using CGI (Common Gateway Interface)



WWW

Dynamic Document using Server Side Script

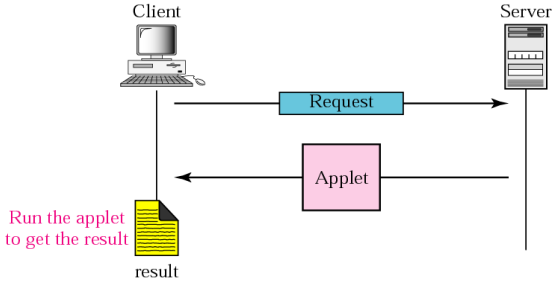


WWW

Dynamic documents are sometimes referred to as server-site dynamic documents.

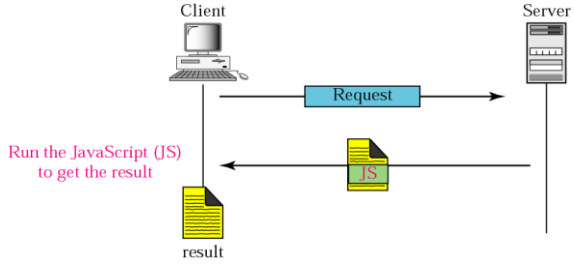
WWW

Active document using Java applet



WWW

Active document using Client-site script



WWW

Active documents are sometimes referred to as client-site dynamic documents.

WWW

HTTP

The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web. HTTP functions like a combination of FTP and SMTP.

WWW

HTTP uses the services of TCP on well-known port 80.

WWW

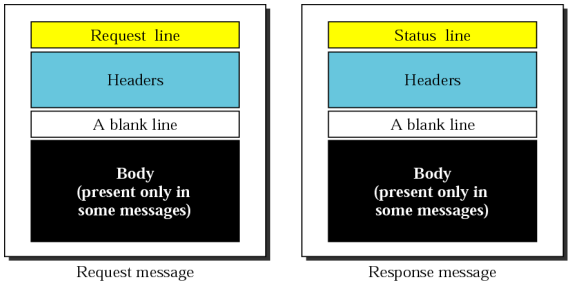
- An HTTP request is made by a client, to a named host, which is located on a server.
- The aim of the request is to access a resource on the server.
- A correctly composed HTTP request contains the following elements:
  - A request line.
  - A series of HTTP headers, or header fields.
  - A message body, if needed.

WWW

- An HTTP response is made by a server to a client.
- The aim of the response is to provide the client with the resource it requested, or inform the client that the action it requested has been carried out;
- Otherwise, to inform the client that an error occurred in processing its request.
- An HTTP response contains:
  - A status line.
  - A series of HTTP headers, or header fields.
  - A message body, which is usually needed.

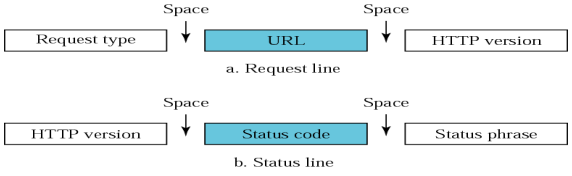
WWW

Request and Response Message



WWW

Request and Status Lines




```
GET /fee-structure HTTP/1.1
HTTP/1.1 200 OK  (text/html)
```


WWW

Request Methods

Method	*Action*
GET	Requests a document from the server
HEAD	Requests information about a document but not the document itself
POST	Sends some information from the client to the server
PUT	Sends a document from the server to the client
TRACE	Echoes the incoming request
CONNECT	Reserved
OPTION	Enquires about available options

WWW

Status codes

Code	*Phrase*	*Description*
	Informational	
100	Continue	The initial part of the request has been received and the client may continue with its request.
101	Switching	The server is complying with a client request to switch protocols defined in the upgrade header.
	Success	
200	OK	The request is successful.
201	Created	A new URL is created.
202	Accepted	The request is accepted, but it is not immediately acted upon.
204	No content	There is no content in the body.

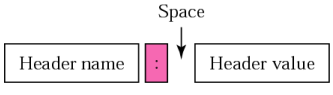
WWW

Status codes

Code	Phrase	Description
	Redirection	
301	Multiple choices	The requested URL refers to more than one resource.
302	Moved permanently	The requested URL is no longer used by the server.
304	Moved temporarily	The requested URL has moved temporarily.
	Client Error	
400	Bad request	There is a syntax error in the request.
401	Unauthorized	The request lacks proper authorization.
403	Forbidden	Service is denied.
404	Not found	The document is not found.
405	Method not allowed	The method is not supported in this URL.
406	Not acceptable	The format requested is not acceptable.
	Server Error	
500	Internal server error	There is an error, such as a crash, at the server site.
501	Not implemented	The action requested cannot be performed.
503	Service unavailable	The service is temporarily unavailable, but may be requested in the future.

WWW

Header Format



WWW

General Header

Header	Description
Cache-control	Specifies information about caching
Connection	Shows whether the connection should be closed or not
Date	Shows the current date
MIME-version	Shows the MIME version used
Upgrade	Specifies the preferred communication protocol

WWW

Request Header

Header	Description
Accept	Shows the media format the client can accept
Accept-charset	Shows the character set the client can handle
Accept-encoding	Shows the encoding scheme the client can handle
Accept-language	Shows the language the client can accept
Authorization	Shows what permissions the client has
From	Shows the e-mail address of the user
Host	Shows the host and port number of the client
If-modified-since	Send the document if newer than specified date
If-match	Send the document only if it matches given tag
If-non-match	Send the document only if it does not match given tag
If-range	Send only the portion of the document that is missing
If-unmodified-since	Send the document if not changed since specified date
Referrer	Specifies the URL of the linked document
User-agent	Identifies the client program

 U4.145

WWW

Response Header

Header	Description
Accept-range	Shows if server accepts the range requested by client
Age	Shows the age of the document
Public	Shows the supported list of methods
Retry-after	Specifies the date after which the server is available
Server	Shows the server name and version number

 U4.146

WWW

Entity Header

Header	Description
Allow	Lists valid methods that can be used with a URL
Content-encoding	Specifies the encoding scheme
Content-language	Specifies the language
Content-length	Shows the length of the document
Content-range	Specifies the range of the document
Content-type	Specifies the media type
Etag	Gives an entity tag
Expires	Gives the date and time when contents may change
Last-modified	Gives the date and time of the last change
Location	Specifies the location of the created or moved document

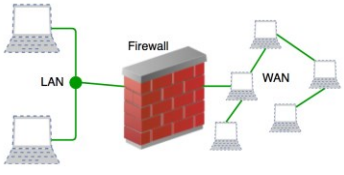
 U4.147

WWW

HTTP version 1.1 specifies a persistent connection by default.

Firewall

- A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- A firewall typically set up a barrier between a trusted network and an untrusted network.



Types of Firewall

- First Generation- Packet Filtering Firewall :
  - Packet filtering firewall is used to control network access by monitoring outgoing and incoming packet and allowing them to pass or stop based on source and destination IP address, protocols and ports.
  - It analyses traffic at the transport protocol layer
  - They have no ability to tell whether a packet is part of an existing stream of traffic.
  - Packet filtering firewall maintains a filtering table which decides whether the packet will be forwarded or discarded.

https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/

Firewall

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Sample Packet Filter Firewall Rule

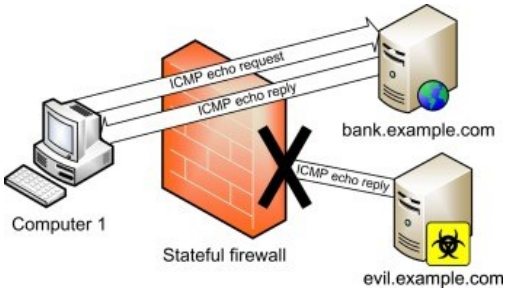
https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/

Types of Firewall

- Second Generation- Stateful Inspection Firewall:
  - Stateful firewalls (performs Stateful Packet Inspection) can determine the connection state of packet.
  - It keeps track of the state of networks connection travelling across it.
  - It monitors all activity from the opening of a connection until it is closed.
  - The filtering decisions would not only be based on defined rules, but also on packet's history in the state table.

https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/

Types of Firewall



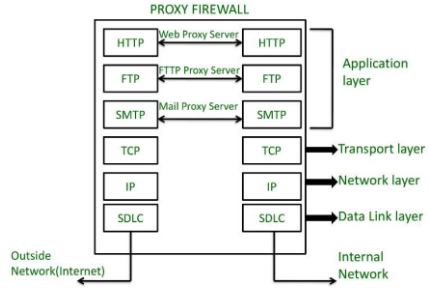
https://www.sciencedirect.com/topics/computer-science/stateful-firewall

Types of Firewall

- Third Generation- Application Layer Firewall :
  - Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer.
  - Application layer firewalls are hosts that run proxy servers.
  - A proxy firewall prevents the direct connection between either side of the firewall.
  - Each packet has to pass through the proxy

https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/

Types of Firewall



https://media.geeksforgeeks.org/wp-content/cdn-uploads/20210910181506/gfg7.png

Types of Firewall

- Next Generation Firewalls (NGFW) :
  - Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks.
  - Firewalls to block modern threats such as advanced malware and application-layer attacks.
  - Firewall should provide a holistic view of activity and full contextual awareness to see:
    - ✓Threat activity across users, hosts, networks, and devices.
    - ✓Where and when a threat originated
    - ✓Communications between virtual machines, file transfers, and more

https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/

Types of Firewall

- Software Firewall :
  - Software firewall is a special type of computer software runs on a computer/server.
  - It's main purpose is to protect your computer/server from outside attempts to control or gain access.
  - It protects the one system at a time.
- Hardware Firewall :
  - It is physical piece of equipment planned to perform firewall duties.
  - Hardware firewall are incorporated into the router that is situated between the computer and the internet gateway.
  - It protects a whole network at a time.

https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/

Cryptography

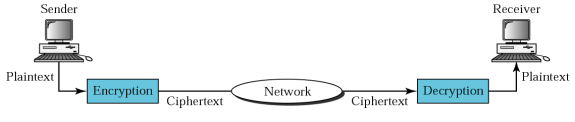
Cryptography

The word cryptography in Greek means "secret writing." The term today refers to the science and art of transforming messages to make them secure and immune to attacks. Two Types of Cryptography:

- **Symmetric-Key Cryptography**
- **Asymmetric-Key Cryptography**

Cryptography

Cryptography Components



Cryptography

In cryptography, the encryption/decryption algorithms are public; the keys are secret.

Cryptography

In symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.

Cryptography

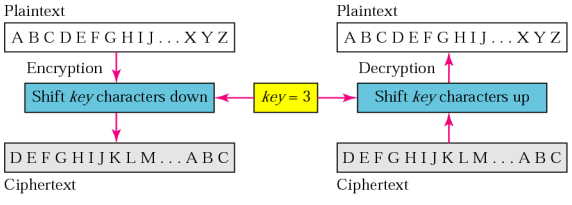
Symmetric-Key Cryptography

Cryptography

In symmetric-key cryptography, the same key is used in both directions.

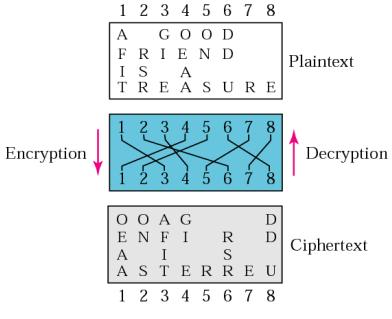
Cryptography

Caesar cipher



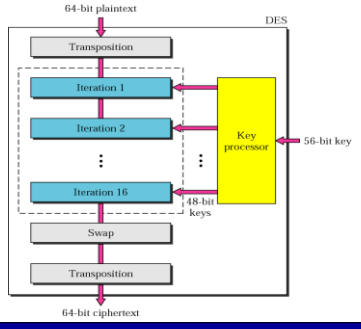
Cryptography

Transpositional cipher



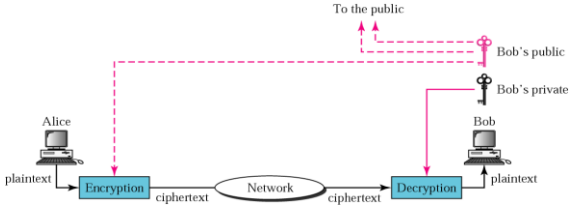
Cryptography

DES



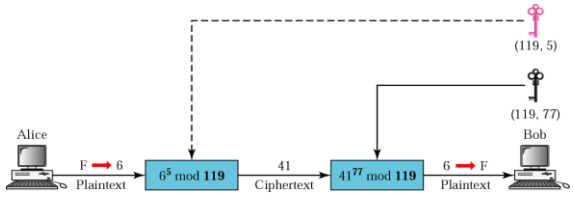
Cryptography

Public Key Cryptography



Cryptography

RSA(Rivest–Shamir–Adleman)



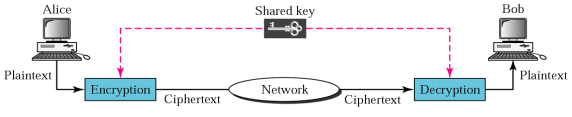
Cryptography

Symmetric-key cryptography is often used for long messages.

Asymmetric-key algorithms are more efficient for short messages.

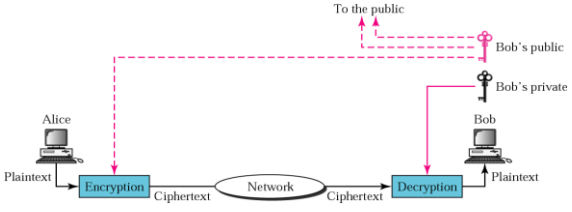
Cryptography

Privacy using symmetric-key encryption



Cryptography

Privacy using asymmetric-key encryption



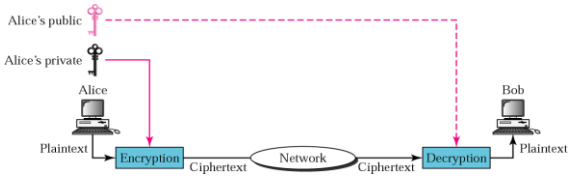
Cryptography

Digital Signature

Digital signature can provide authentication, integrity, and nonrepudiation for a message.

Cryptography

Signing the Whole Document

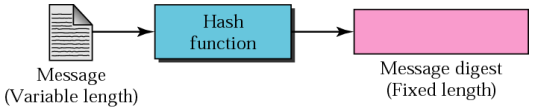


Cryptography

Digital signature does not provide privacy. If there is a need for privacy, another layer of encryption/decryption must be applied.

Cryptography

HASH Function



 U4.175

Recommended reading

1. Forouzun, Data Communication and Networking, TMH
2. Tanenbaum , A computer Networks: Prentice Hall
3. Stallings , High speed Networks :Printice Hall
4. Comer D. Computer Networks: Printice hall
5. Kurose, J and ross , Computer Networking : Addison Wesley

 U4.176