Unit - IV
Transport Layer

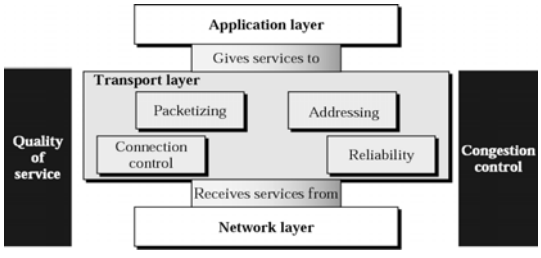
 U4.1

Learning Objective

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

 U4.2

Position of transport layer



 U4.3

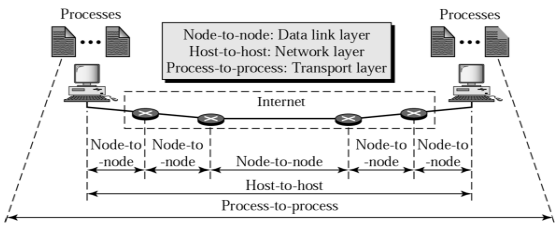
Transport Layer

Note:

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

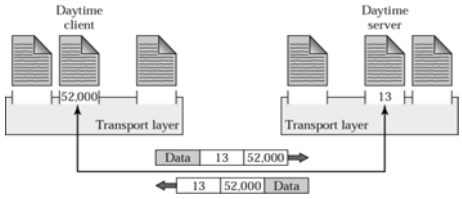
 U4.4

Transport Layer



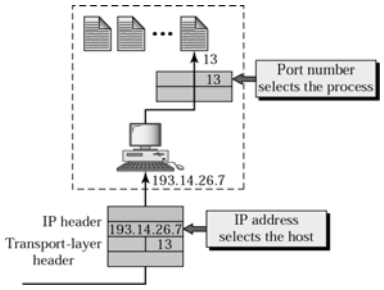
 U4.5

Port numbers



 U4.6

IP addresses versus port numbers

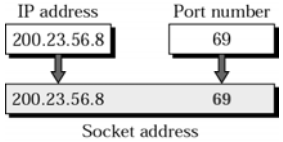


 U4.7

Cont ….

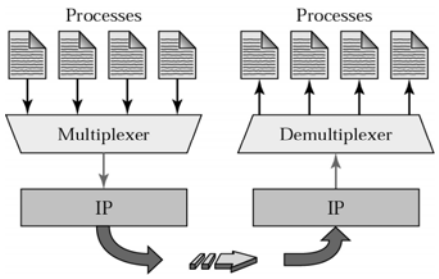
 U4.8

Socket address



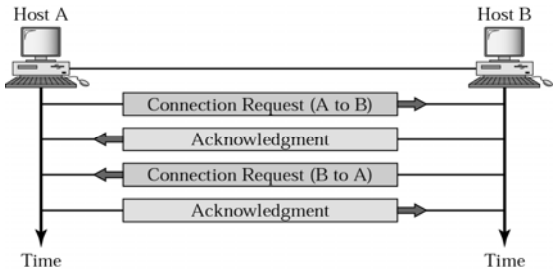
 U4.9

Multiplexing and demultiplexing



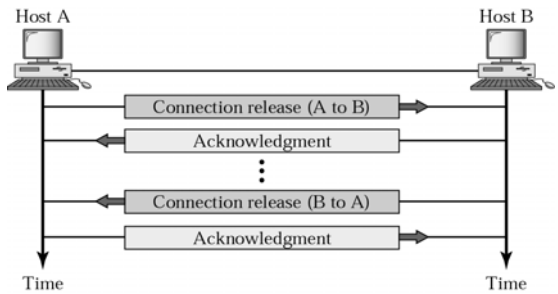
 U4.10

Connection establishment



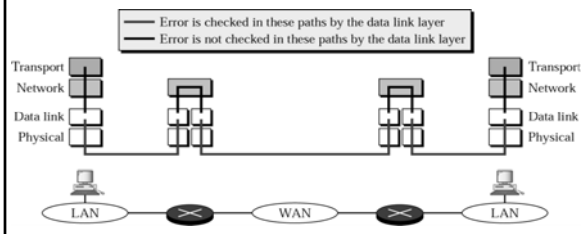
 U4.11

Connection termination



 U4.12

Error control



 U4.13

UDP

Port Numbers

User Datagram

Applications

 U4.14

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.

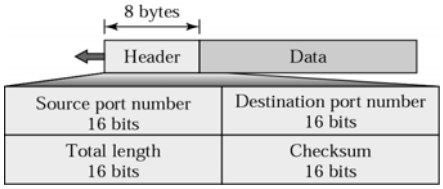
 U4.15

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)

 U4.16

User datagram format



 U4.17

Cont ….

Note:

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

 U4.18

Cont ….

Note:

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

 U4.19

TCP

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

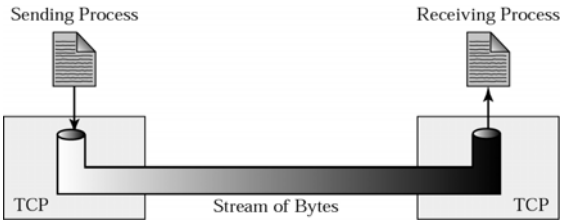
 U4.20

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

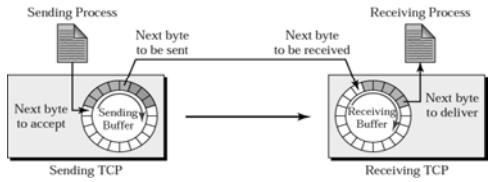
 U4.21

Stream delivery



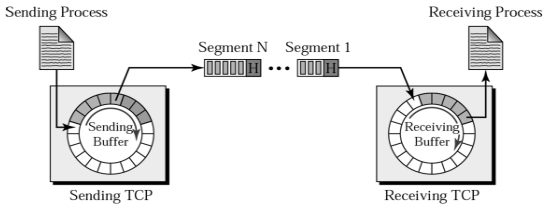
 U4.22

Sending and receiving buffers



 U4.23

TCP segments



 U4.24

Cont ….

Imagine a TCP connection is transferring a file of 6000 bytes. The first byte is numbered 10010. What are the sequence numbers for each segment if data are sent in five segments with the first four segments carrying 1000 bytes and the last segment carrying 2000 bytes?

Solution

The following shows the sequence number for each segment:
Segment 1 ==> sequence number: 10,010 (range: 10,010 to 11,009)
Segment 2 ==> sequence number: 11,010 (range: 11,010 to 12,009)
Segment 3 ==> sequence number: 12,010 (range: 12,010 to 13,009)
Segment 4 ==> sequence number: 13,010 (range: 13,010 to 14,009)
Segment 5 ==> sequence number: 14,010 (range: 14,010 to 16,009)

 U4.25

Cont ….

Note:

The bytes of data being transferred in each connection are numbered by TCP. The numbering starts with a randomly generated number.

 U4.26

Cont ….

Note:

The value of the sequence number field in a segment defines the number of the first data byte contained in that segment.

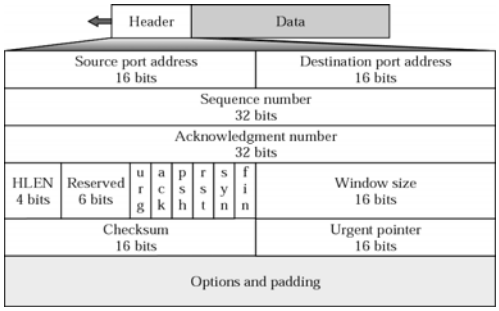
 U4.27

Cont ….

Note:

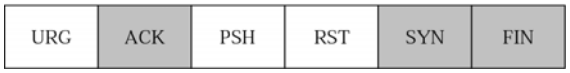
The value of the acknowledgment field in a segment defines the number of the next byte a party expects to receive. The acknowledgment number is cumulative.

TCP segment format



Control field

URG: Urgent pointer is valid	RST: Reset the connection
ACK: Acknowledgment is valid	SYN: Synchronize sequence numbers
PSH: Request for push	FIN: Terminate the connection

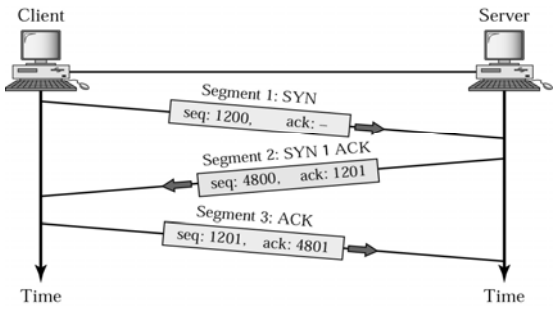


Description of flags in the control field

Flag	Description
URG	The value of the urgent pointer field is valid.
ACK	The value of the acknowledgment field is valid.
PSH	Push the data.
RST	The connection must be reset.
SYN	Synchronize sequence numbers during connection.
FIN	Terminate the connection.

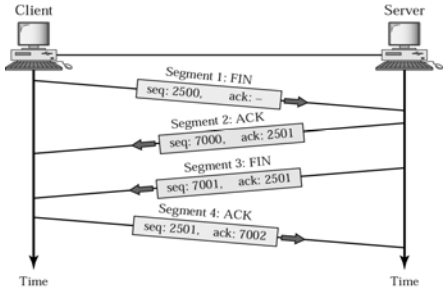
 U4.31

Three-step connection establishment



 U4.32

Four-step connection termination

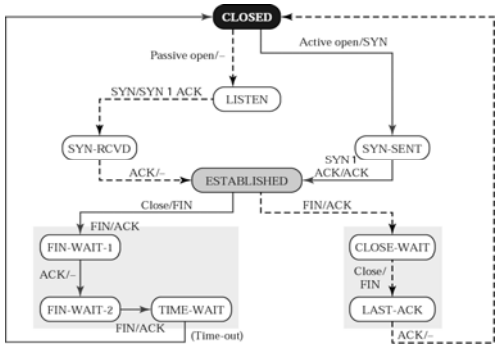


 U4.33

States for TCP

State	Description
CLOSED	There is no connection.
LISTEN	The server is waiting for calls from the client.
SYN-SENT	A connection request is sent; waiting for acknowledgment.
SYN-RCVD	A connection request is received.
ESTABLISHED	Connection is established.
FIN-WAIT-1	The application has requested the closing of the connection.
FIN-WAIT-2	The other side has accepted the closing of the connection.
TIME-WAIT	Waiting for retransmitted segments to die.
CLOSE-WAIT	The server is waiting for the application to close.
LAST-ACK	The server is waiting for the last acknowledgment.

State transition diagram



TCP

Flow Control

Flow control regulates the amount of data a source can send before receiving an acknowledgment from the destination. TCP defines a window that is imposed on the buffer of data delivered from the application program.

Sliding Window Protocol

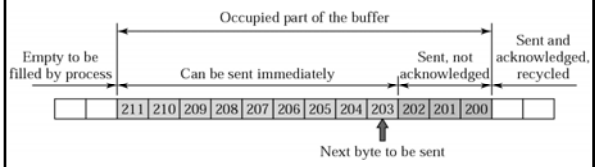
Cont ….

Note:

A sliding window is used to make transmission more efficient as well as to control the flow of data so that the destination does not become overwhelmed with data. TCP's sliding windows are byte-oriented.

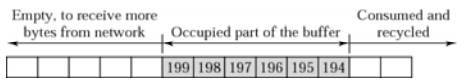
 U4.37

Sender buffer



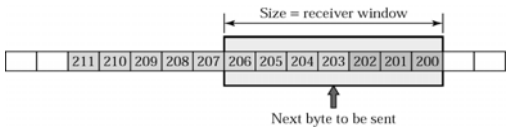
 U4.38

Receiver window

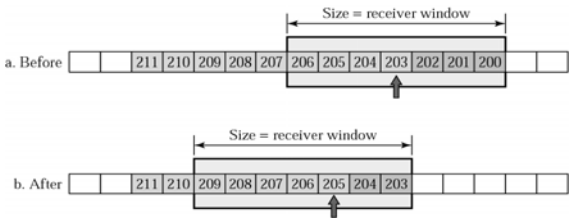


 U4.39

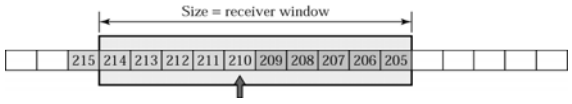
Sender buffer and sender window



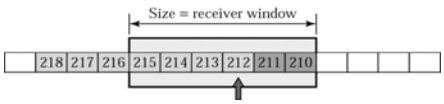
Sliding the sender window



Expanding the sender window



Shrinking the sender window



 U4.43

Cont ….

Note:

In TCP, the sender window size is totally controlled by the receiver window value (the number of empty locations in the receiver buffer). However, the actual window size can be smaller if there is congestion in the network.

 U4.44

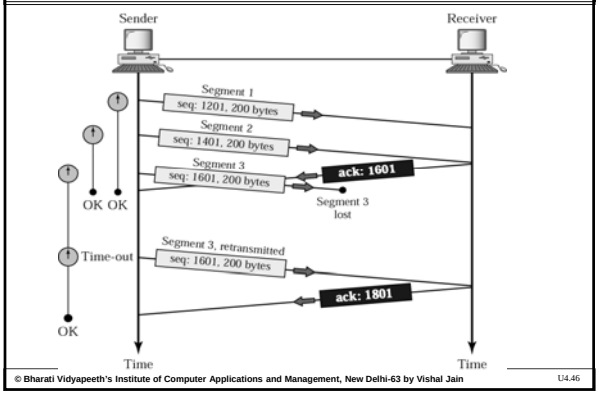
TCP

Error Control

TCP provides reliability using error control, which detects corrupted, lost, out-of-order, and duplicated segments. Error control in TCP is achieved through the use of the checksum, acknowledgment, and time-out.

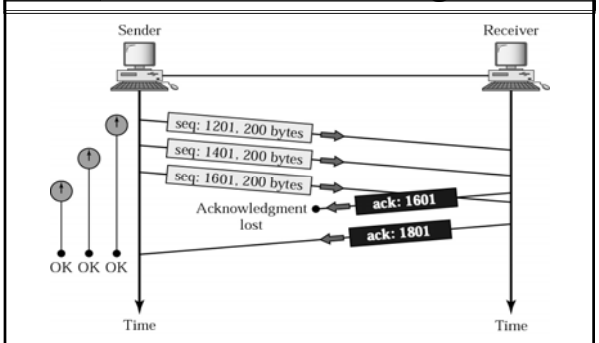
 U4.45

Lost segment



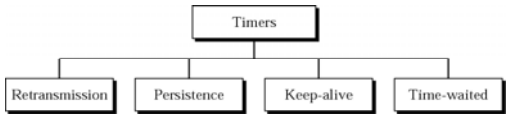
 U4.46

Lost acknowledgment



 U4.47

TCP timers



 U4.48

TCP timers

TCP maintains seven timers for each connection:-

Connection-establishment timer: starts when a SYN is sent to establish a new connection. If the sender doesn't receive an ACK within 75 seconds, the connection establishment is aborted.

Retransmission timer: is set when TCP sends data. If the other end does not acknowledge the data when this timer expires, TCP retransmits the data. This timer is calculated dynamically based on the RTT (round-trip time).

Delayed ACK timer: is set when TCP receives data that must be acknowledged but need not be acknowledged immediately. In Linux, this timer is set to 300ms.

TCP timers

Persist timer: is set when the other end of a connection advertise a zero window but it still has data to send. The sender keeps probing the closed window during a retransmission interval. Its value is calculated dynamically.

Keepalive timer: If the connection is idle for 2 hours, the keepalive timer expires and a special segment is sent to the other end. If other end is down, the sender will receive a RESET and the connection will be closed. If there is a segment exchange during 2 hours, the keepalive timer is set to 2 hours again.

TCP timers

FIN_WAIT_2 timer: is set to 10 minutes when a connection moves from the FIN_WAIT_1 state to the FIN_WAIT_2 state and the connection cannot receive any more data. When this timer expires it is reset to 75 seconds. When it expires, the connection is dropped.

2MSL timer: is set when the connection is actively closed. MSL (maximum segment lifetime) is the maximum amount of time any segment can exist in the network before being discarded. When TCP performs an active close, and sends the final acknowledgement, that connection must stay in the TIME_WAIT state for twice the MSL to let TCP resend the final ACK in case this ACK is lost.

TCP timers

The delayed ACK timer is different from the other six because when it is set a delayed ACK must be sent the next time TCP's 300-ms timer expires. But the other six timers are counters that are decremented by 1 every time TCP's 500-ms timer expires. When any one of the counters reaches 0, one of the following actions is taken:

· Drop the connection.
· Retransmit a segment.
· Send a keepalive probe.

 U4.52

DNS

- Introduction
- Namespace
- DNS in the Internet
- Resolution

 U4.53

DNS

- Domain Name System (DNS) is a Client /Server application programs used to help other application programs.

- DNS is used to map a host name in the application layer to an IP address in the network layer.

 U4.54

DNS

•Namespace

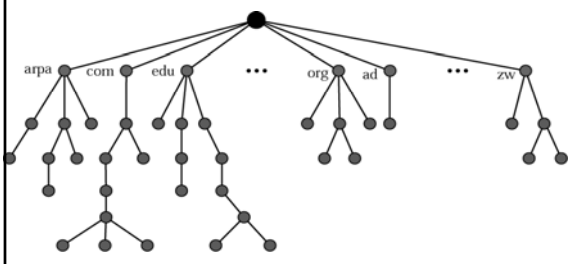
•The names assigned to machines must be unique because the addresses are unique. A name space that maps each address to a unique name can be organized in two ways: flat or hierarchical.

DNS

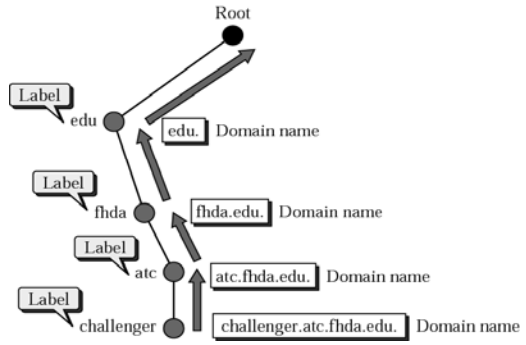
•Domain Namespace

•The domain name space is hierarchical in design. The names are defined in an inverted-tree structure with the root at the top. The tree can have 128 levels: level 0 (root) to level 127.

DNS



DNS



 U4.58

DNS

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

 U4.59

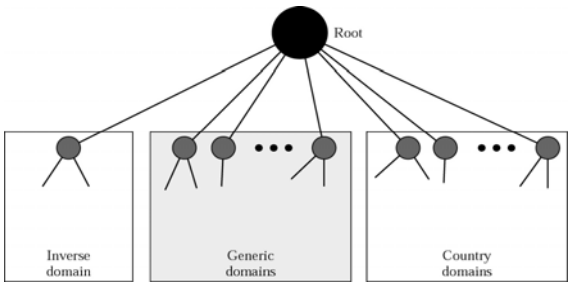
DNS

Domain Namespace in the Internet

The domain name space (tree) is divided into three different sections: generic domains, country domains, and the inverse domain.

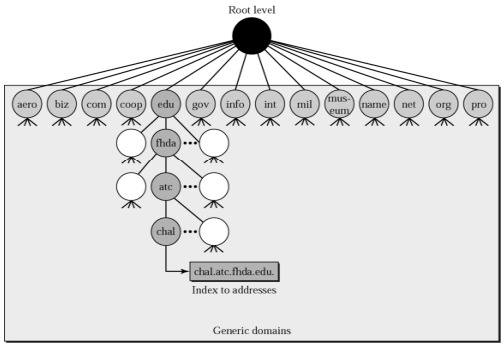
 U4.60

DNS



 U4.61

DNS



 U4.62

DNS

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

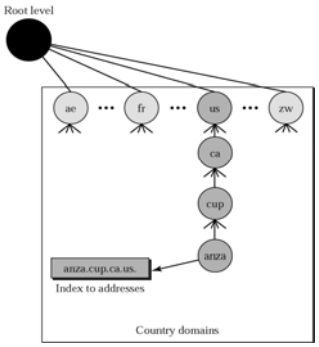
 U4.63

DNS

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

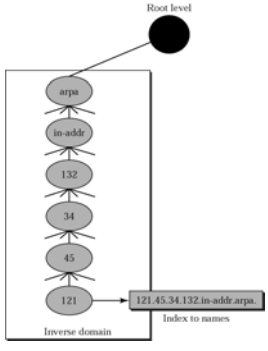
 U4.64

DNS



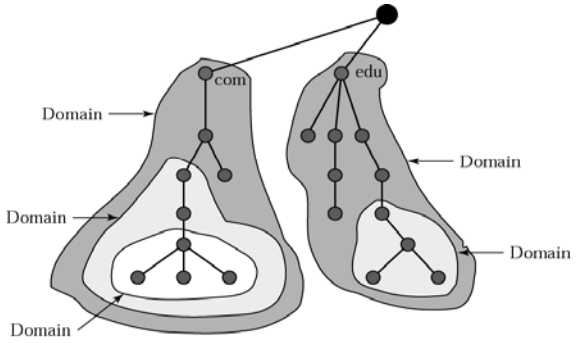
 U4.65

DNS



 U4.66

DNS



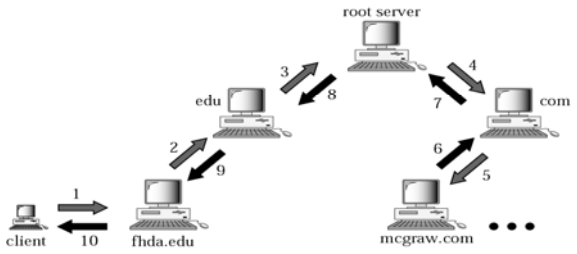
DNS

Resolution

Mapping a name to an address or an address to a name is called name-address resolution.

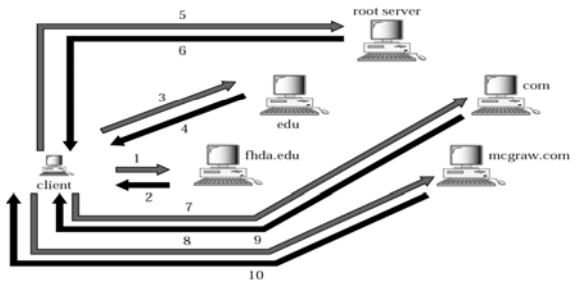
DNS

Recursive Resolution



DNS

Iterative Resolution



DNS

DNS can use the services of UDP or TCP using the well-known port 53.

E-Mail

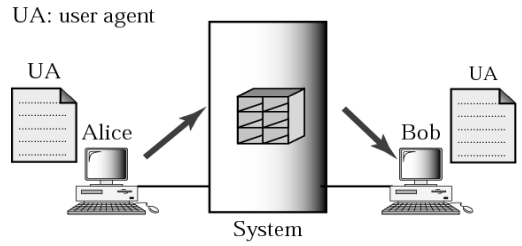
Electronic Mail: SMTP, POP, and IMAP

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

First Scenario
Second Scenario
Third Scenario
Fourth Scenario

E-Mail

First Scenario



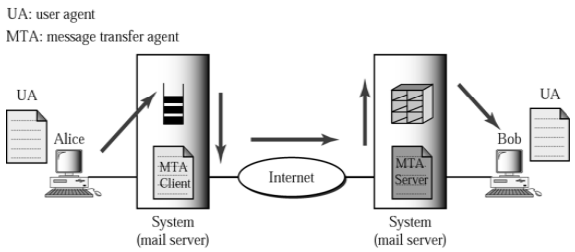
E-Mail

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



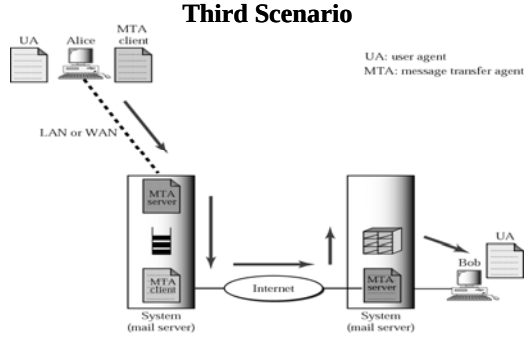
E-Mail

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



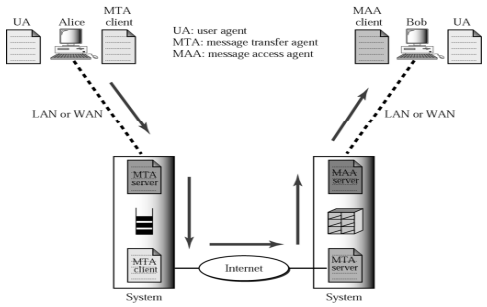
E-Mail

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

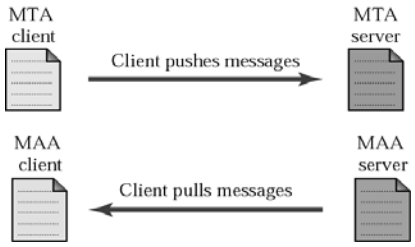
Fourth Scenario



 U4.79

E-Mail

Fourth Scenario



 U4.80

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.

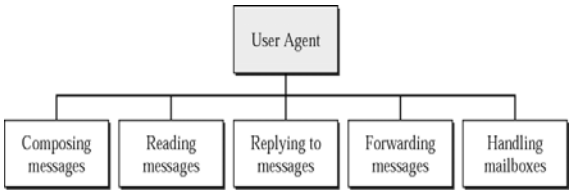
 U4.81

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

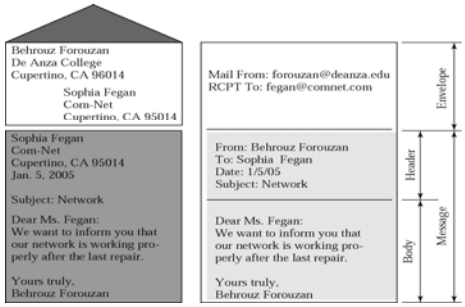
Some examples of command-driven user agents are mail, pine, and elm

E-Mail

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

E-Mail

Format of an E-mail

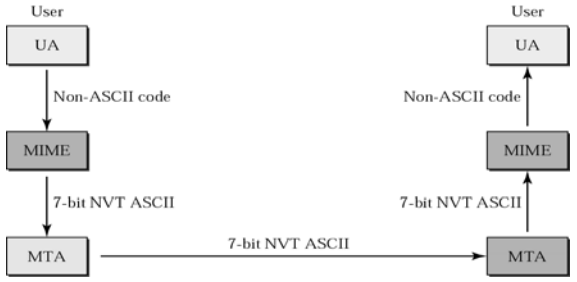


E-Mail

E-Mail Address

E-Mail

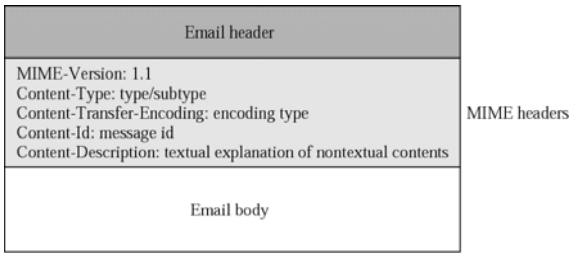
MIME



 U4.88

E-Mail

MIME Header



 U4.89

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

 U4.90

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)

 U4.91

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

 U4.92

E-Mail

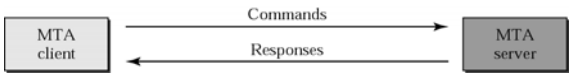
SMTP

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).

 U4.93

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

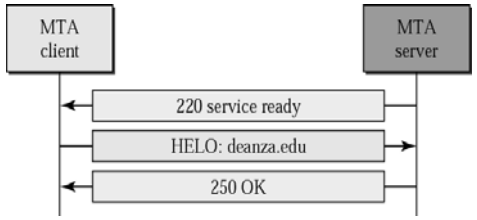
E-Mail

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

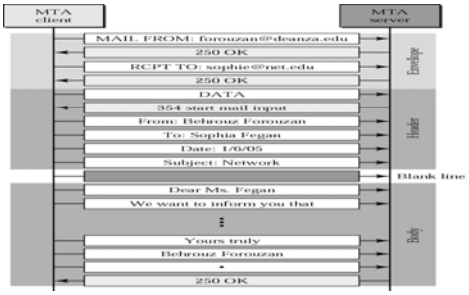
Connection establishment



 U4.97

E-Mail

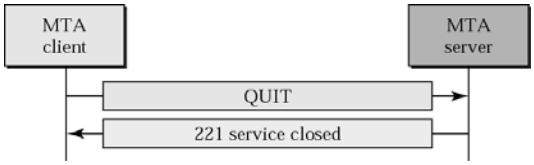
Message Transfer



 U4.98

E-Mail

Connection Termination



 U4.99

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.

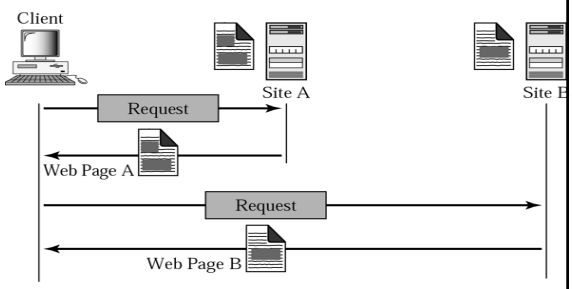
WWW

•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.

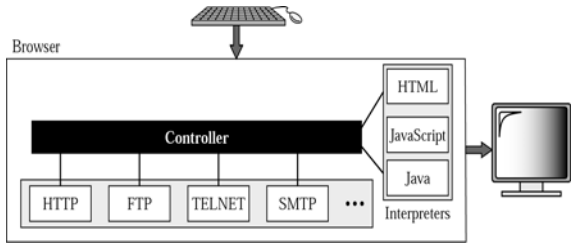
WWW

Architecture of WWW



WWW

Browser



 U4.103

WWW

URL

 U4.104

WWW

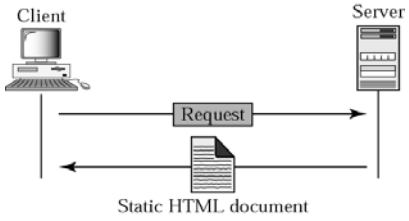
Web Documents

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.

 U4.105

WWW

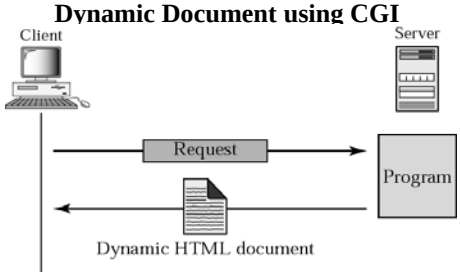
Static



 U4.106

WWW

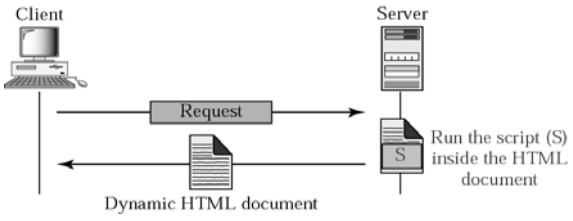
Dynamic Document using CGI



 U4.107

WWW

Dynamic Document using Server Side Script



 U4.108

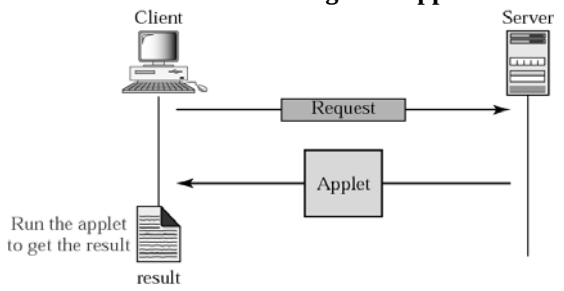
WWW

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

 U4.109

WWW

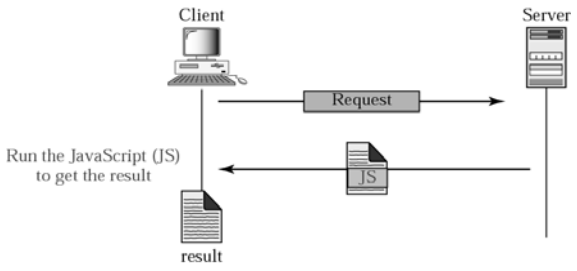
Active document using Java applet



 U4.110

WWW

Active document using Client-site script



 U4.111

WWW

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

WWW

HTTP

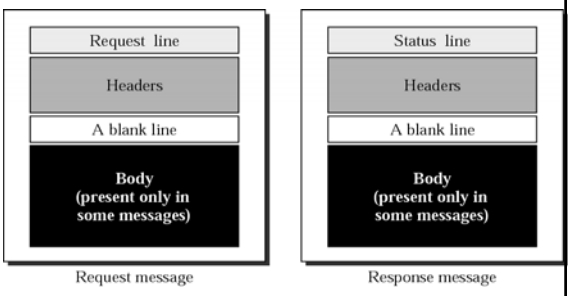
The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web. HTTP functions like a combination of FTP and SMTP.

WWW

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

WWW

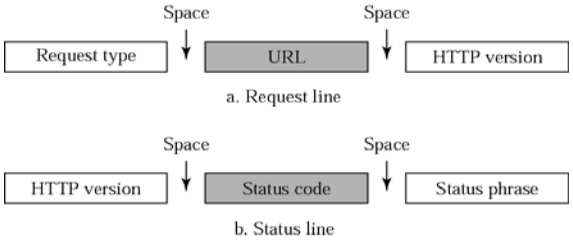
Request and Response Message



 U4.115

WWW

Request and Status Lines



 U4.116

WWW

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

 U4.117

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.

 U4.118

WWW

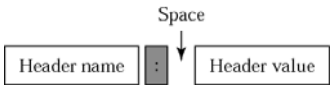
Status codes

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.

 U4.119

WWW

Header Format



 U4.120

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

 U4.121

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

 U4.122

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

 U4.123

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

 U4.124

WWW

HTTP version 1.1 specifies a persistent connection by default.

 U4.125

Summary

- www is a repository of information linked together from points all over the world.
- Hypertexts are document linked to one another through the concept of pointers.
- Browsers interpret and display a Web document.
- HTTP uses a TCP connection to transfer files.
- An HTTP message is similar in form to an SMTP message.
- HTTP, version 1.1 specifies a persistent connection.
- A proxy server keeps copies of responses to recent requests.

 U4.126

Network Security

Cryptography

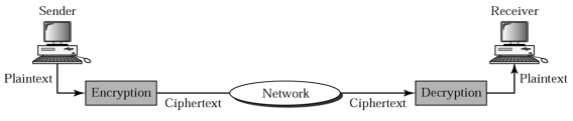
•Cryptography

•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

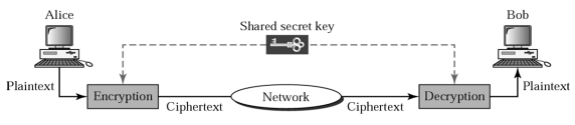
In cryptography, the encryption/decryption algorithms are public; the keys are secret.

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

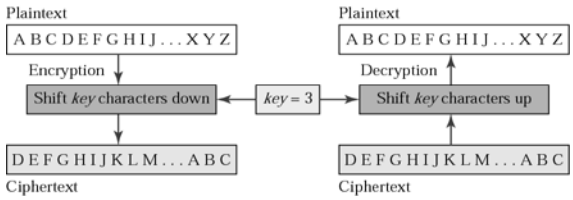


Cryptography

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

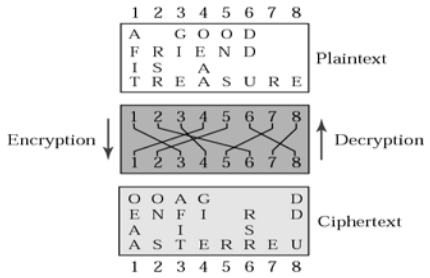
Cryptography

Caesar cipher



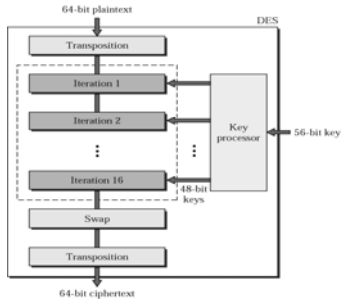
Cryptography

Transpositional cipher



Cryptography

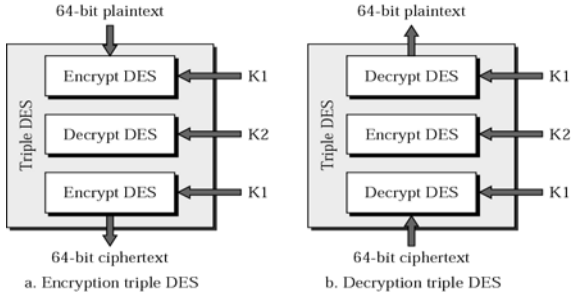
DES



 U4.136

Cryptography

Triple DES



 U4.137

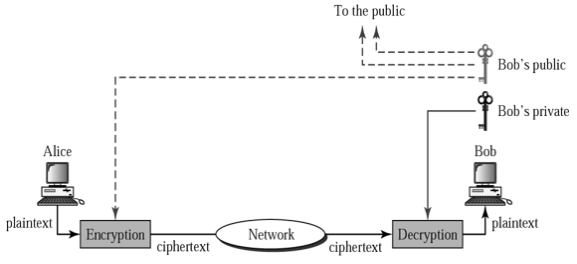
Cryptography

The DES cipher uses the same concept as the Caesar cipher, but the encryption/ decryption algorithm is much more complex.

 U4.138

Cryptography

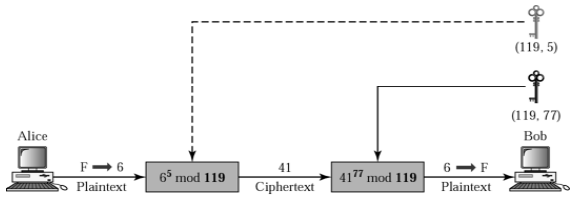
Public Key Cryptography



 U4.139

Cryptography

RSA



 U4.140

Cryptography

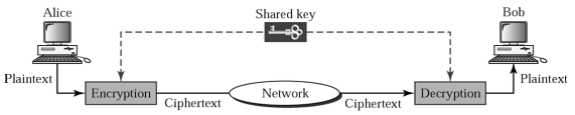
Symmetric-key cryptography is often used for long messages.

Asymmetric-key algorithms are more efficient for short messages.

 U4.141

Cryptography

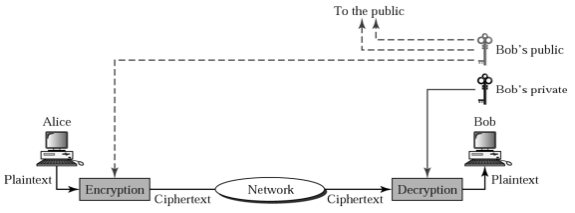
Privacy using symmetric-key encryption



 U4.142

Cryptography

Privacy using asymmetric-key encryption



 U4.143

Cryptography

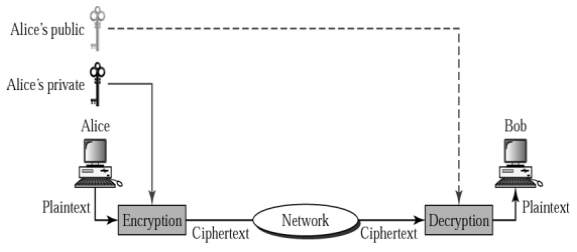
Digital Signature

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

 U4.144

Cryptography

Signing the Whole Document



 U4.145

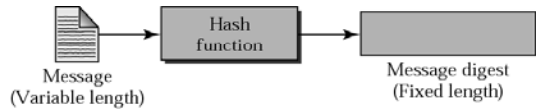
Cryptography

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

 U4.146

Cryptography

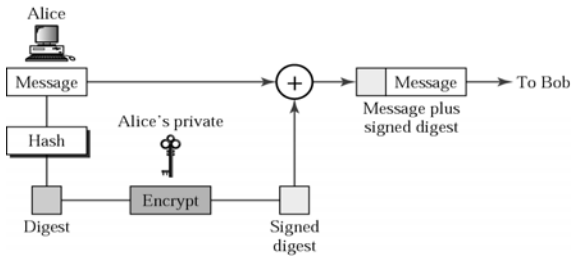
HASH Function



 U4.147

Cryptography

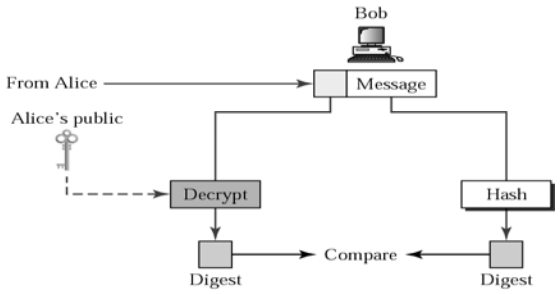
Sender Site



 U4.148

Cryptography

Receiver Site



 U4.149

IP Sec

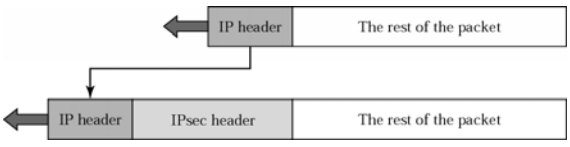
Security in the Internet

In this section we discuss a security method for each of the top 3 layers of the Internet model. At the IP level we discuss a protocol called IPSec; at the transport layer we discuss a protocol that "glues" a new layer to the transport layer; at the application layer we discuss a security method called PGP.

 U4.150

IP Sec

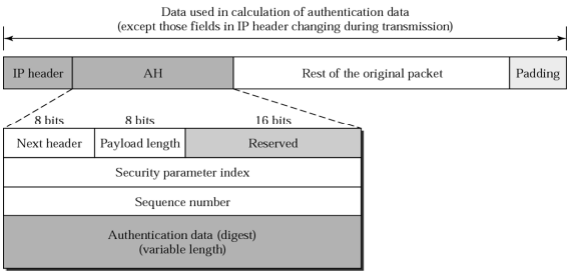
Transport mode



 U4.151

IP Sec

AH



 U4.152

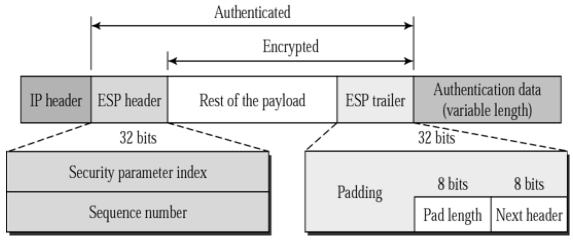
IP Sec

The AH protocol provides message authentication and integrity, but not privacy.

 U4.153

IP Sec

ESP



 U4.154

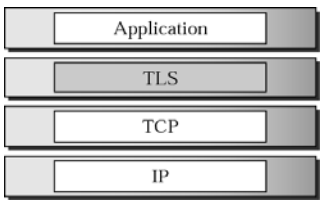
IP Sec

ESP provides message authentication, integrity, and privacy.

 U4.155

IP Sec

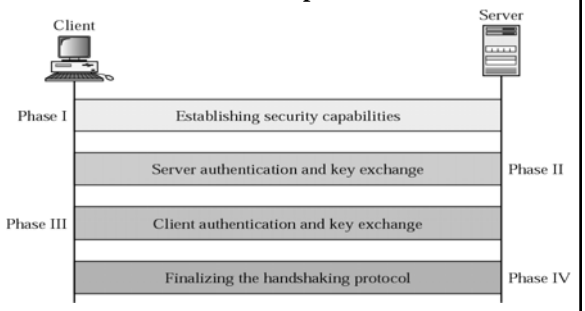
Position of TLS



 U4.156

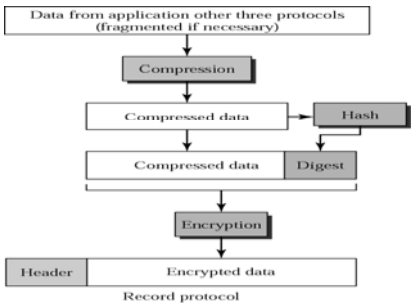
Cryptography

Handshake protocol



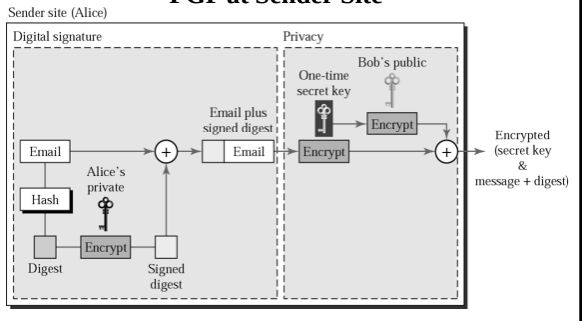
Cryptography

Record protocol



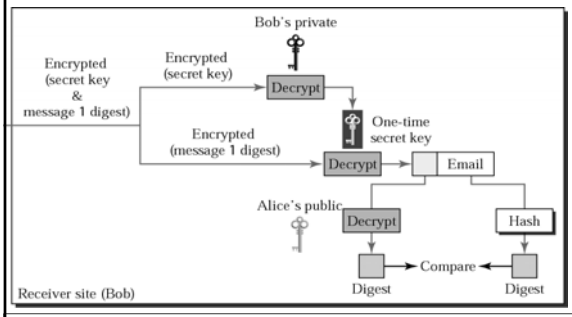
Cryptography

PGP at Sender Site



Cryptography

PGP at Receiver Site



Summary

- DNS is a client-server application that identifies each host on the Internet with a unique user-friendly name.
- DNS organizes the name space in a hierarchical structure to decentralize the responsibilities involved in naming.
- DNS can be pictured as an inverted hierarchical tree structure with one root node at the top and a maximum of 128 levels.
- Each node in a tree has a domain name.
- Domain name can be FQDN and PQDN
- FQDN – Fully qualified domain name
- PQDN – Partially qualified domain name

Review Questions (OBJ)

1. Which of the following functions does UDP perform?
A) process-to-process communication
B) host-to-host communication
C) end-to-end reliable data delivery
D) none of the above

2. When the IP layer of a receiving host receives a datagram, _____.
A) delivery is complete
B) a transport layer protocol takes over
C) a header is added
D) none of the above

Review Questions (OBJ)

3. A port address in UDP is _____bits long.
A) 8
B) 16
C) 32
D) any of the above

4. Which of the following does UDP guarantee?
A) flow control
B) connection-oriented delivery
C) flow control
D) none of the above

 U4.163

Review Questions (OBJ)

5. The combination of an IP address and a port number is called a _____.
A) transport address
B) network address
C) socket address
D) none of the above

6. To use the services of UDP, we need _____ socket addresses.
A) four
B) two
C) three
D) none of the above

 U4.164

Review Questions (OBJ)

7. UDP packets are called _____.
A) user datagrams
B) segments
C) frames
D) none of the above

8. UDP packets have a fixed-size header of _____ bytes.
A) 16
B) 8
C) 40
D) none of the above

 U4.165

Review Questions (OBJ)

9. TCP is a _____protocol.
A) stream-oriented
B) message-oriented
C) block-oriented
D) none of the above

10. TCP is a _____ protocol.
A) connection-oriented
B) connectionless
C) both a and b
D) none of the above

Review Questions (Short)

1. Name various Congestion prevention policies on various layers.
2. Explain various timers in TCP.
3. Draw state transition diagram for TCP.
4. How is internetworking implemented in virtual circuits
5. What is silly window syndrome in TCP ?Explain use of Nagle's algorithm
6. Explain Token Bucket Algorithm.
7. Explain how congestion is controlled in TCP
8. Explain Distance vector routing in TCP.

Review Questions (Short)

9. How is congestion controlled through choke packets.
10. What is Clark's algorithm and what role it plays in silly window syndrome in TCP

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

Review Questions

1. In the _____ protocol we avoid unnecessary transmission by sending only frames that are corrupted.

A) Stop-and-Wait ARQ
B) Go-Back-N ARQ
C) Selective-Repeat ARQ
D) none of the above

1. Both Go-Back-N and Selective-Repeat Protocols use a _____.

A) sliding frame
B) sliding window
C) sliding packet
D) none of the above

Review Questions

1. In the _____ protocol we avoid unnecessary transmission by sending only frames that are corrupted.

A) Stop-and-Wait ARQ
B) Go-Back-N ARQ
C) Selective-Repeat ARQ
D) none of the above

1. Both Go-Back-N and Selective-Repeat Protocols use a _____.

A) sliding frame
B) sliding window
C) sliding packet
D) none of the above

Review Questions

1. In the _____ protocol we avoid unnecessary transmission by sending only frames that are corrupted.

A) Stop-and-Wait ARQ
B) Go-Back-N ARQ
C) Selective-Repeat ARQ
D) none of the above

1. Both Go-Back-N and Selective-Repeat Protocols use a _____.

A) sliding frame
B) sliding window
C) sliding packet
D) none of the above

 U4.172

Review Questions

1. In the _____ protocol we avoid unnecessary transmission by sending only frames that are corrupted.

A) Stop-and-Wait ARQ
B) Go-Back-N ARQ
C) Selective-Repeat ARQ
D) none of the above

1. Both Go-Back-N and Selective-Repeat Protocols use a _____.

A) sliding frame
B) sliding window
C) sliding packet
D) none of the above

© Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi-63 by Vishal Jain U4.173

Review Questions

1. In the _____ protocol we avoid unnecessary transmission by sending only frames that are corrupted.

A) Stop-and-Wait ARQ
B) Go-Back-N ARQ
C) Selective-Repeat ARQ
D) none of the above

1. Both Go-Back-N and Selective-Repeat Protocols use a _____.

A) sliding frame
B) sliding window
C) sliding packet
D) none of the above

© Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi-63 by Vishal Jain U4.174