Chapter 6: Application Layer

Application Layer

- It focuses on protocols that provides process to process communication.
- It provides end user services using various protocols.
- Need of Application layer design
  - Think of different people/teams, working on the client and server programs.
    - Different programming languages.
    - Diverse hardware, operating systems.
  - Allow for future extensions
    - Leave room for additional data, meta-data

Functions of Application Layer

- File Transfer
  - It allows user to access, retrieve and manage files
- Mail Services
  - Basis for email forwarding and storage
- Directory Services
  - Distributed database for global information about various objects and services

Web and HTTP

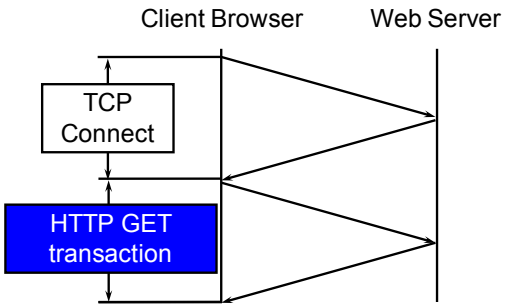
- Web is the repository of information spread all over the world and linked together.
- WWW or web is distributed client server service in which client using a browser can access a service from a server.
- To use www, we need 3 components
  - Browser
  - Web server
  - HTTP protocol

HTTP and HTTPS

- HTTP stands for Hyper Text Transfer Protocol
- HTTP is an application-level protocol for distributed, collaborative, hypermedia information systems.
- This is the foundation for data communication for the World Wide Web (ie. internet) since 1990
  - allows the transmitting and receiving of information across the Internet
- The S stands for "Secure" in HTTPS i.e., Secure hypertext transfer protocol
  - HTTPS is http using a Secure Socket Layer (SSL).

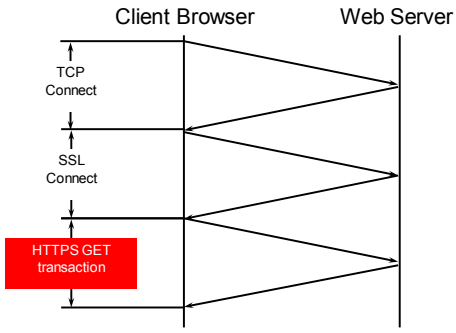
- Secure HTTP (HTTPS) is one of the popular protocols to transfer sensitive data over the Internet.
  - A secure socket layer is an encryption protocol invoked on a Web server that uses HTTPS.
  - Most implementations of the HTTPS protocol involve online purchasing or the exchange of private information.
- HTTPS is only slightly slower than HTTP

HTTP Transaction



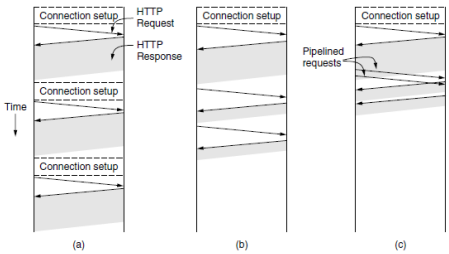
7

HTTPS Transaction



8

HTTP Connection



HTTP with (a) multiple connections and sequential requests. (b) A persistent connection and sequential requests. (c) A persistent connection and pipelined requests.

9

- Figure (a) shows non-persistent connections
  - Browser makes connection and request for each object
  - Server parses request, responds and closes connection
  - Performance problem
- Figure (b) shows persistent connections
  - On same TCP connection server parses request, responds, parses new request upon responds and so on
  - Improves performance
- Figure (c) shows pipelining with persistent connections
  - Send next request before previous response is received
  - Pipelining with persistent connection improves performance

10

HTTP Message

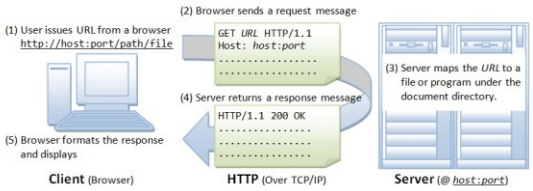
- The HTTP protocol is a request/response protocol.
- Client
  - A client sends a request to the server in the form of
    - ➢a request method
    - ➢URI, and
    - ➢protocol version
    - ➢followed by a MIME-like message containing
      - request modifiers
      - client information, and
      - possible body content over a connection with a server.

11

- Server
  - The server responds with
    - ➢a status line
    - ➢the message's protocol version and
    - ➢a success or error code,
    - ➢followed by a MIME-like message containing
      - server information,
      - entity meta information, and
      - possible entity-body content.

12

HTTP Example



DNS (Domain Name System)

- DNS is usually used to translate a host name into an IP address
  - automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites.
- Domain names comprise a hierarchy so that names are unique, yet easy to remember.
- DNS implements a distributed database to store this name and address information for all public hosts on the Internet.
- Most network operating systems support configuration of primary, secondary, and tertiary DNS servers, each of which can service initial requests from clients.

DNS Contd..

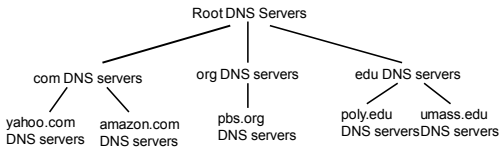
- Example :
  - Name used by human – www.example.com
  - translated to the addresses 93.184.216.119 (IPv4)
- Host name structure
  - Each host name is made up of a sequence of *labels* separated by periods.
    - Each label can be up to 63 characters
    - The total name can be at most 255 characters.
- Examples:
  - whitehouse.gov
  - Wikipedia.org
  - Kathford.edu.np
  - Iamtheproudownerofthelongestlongestlongestdomainnameinthisworld.com

DNS Query Types

- Recursive Query
  - A DNS client provides a hostname and DNS resolver must provide
    - ➢Either a relevant resource or
    - ➢An error message if it can't be found
- Iterative Query
  - A DNS client provides a hostname and DNS resolver returns the best answer.
    - ➢If DNS resolver has the relevant resource in cache, it returns them
    - ➢If not refers to the root server or another Authoritative Name Server

- Non-Recursive Query
  - In this case DNS resolver already knows the answer
  - It either directly returns the DNS record from cache or queries a DNS Name server which is authoritative for the record.

Distributed, Hierarchical Database



How DNS Works

- When a user tries to access a web address like ”example.com”, their web browser performs a DNS query
- The DNS server takes the hostname and resolve it into numeric IP address
- The DNS resolver is responsible for checking if the hostname is available in local cache,
  - If not contacts a series of DNS Name Servers, until it receives the IP of the service

19

DNS: Root name servers

- contacted by local name server that can not resolve name
- root name server:
  - contacts authoritative name server if name mapping not known
  - gets mapping
  - returns mapping to local name server

20

TLD and Authoritative Servers

- Top-level domain (TLD) servers:
  - Generic top level domains
    - responsible for .com, .org, .net, .edu, .gov, etc
  - Countries have a 2 letter top level domain
    - Example., uk, fr, np, ca, jp
- Authoritative DNS servers:
  - organization’s DNS servers,
  - providing authoritative hostname to IP mappings for organization’s servers (e.g., Web and mail)
    - Can be maintained by organization or service provider

21

Local Name Server

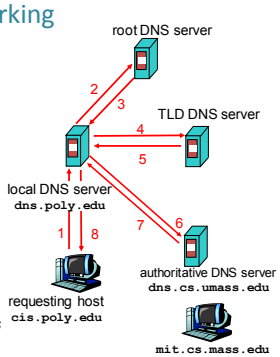
- Does not strictly belong to hierarchy
- Each ISP (residential ISP, company, university) has one.
  - Also called “default name server”
- When a host makes a DNS query, query is sent to its local DNS server
  - Acts as a proxy, forwards query into hierarchy.

22

Example of DNS Working

- Host at cis.poly.edu wants IP address for mit.cs.mass.edu

1. shows the query that is sent to the local name server.
2. start at the top of the name hierarchy by asking one of the root name servers.
3. name server for the *edu domain TLD*
4. sends the entire query to the *edu name server (mit.cs.mass.edu)*
5. *Returns the name server for authoritative DNS server*
6,7. *authoritative DNS server resolves the query to local DNS server*
8. Host at cis.poly.edu gets IP address for mit.cs.mass.edu



23

DNS Records

- DNS records are basically mapping files that tell the DNS server which IP address each domain is associated with, and how to handle requests sent to each domain.
- Various strings of letters are used as commands that dictate the actions of the DNS server, and these strings of commands are called DNS syntax.
- Some DNS records syntax that are commonly used in nearly all DNS record configurations are A, AAAA, CNAME, MX, PTR, NS, SOA, SRV, TXT, and NAPTR

24

DNS Resource Records

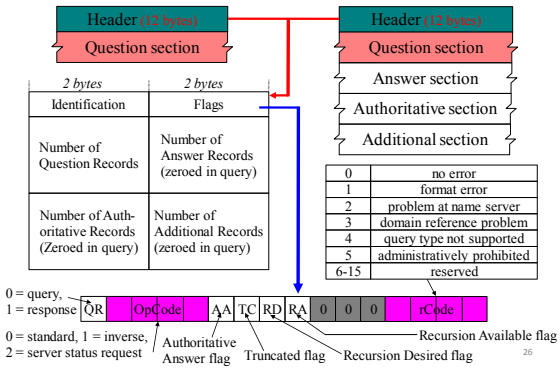
distributed db storing resource records (RR)

RR format: (name, value, type, ttl)

- Type=A
  - name is hostname
  - value is IP address
- Type=NS
  - **name** is domain (e.g. foo.com)
  - **value** is hostname of authoritative name server for this domain
- Type=CNAME
  - name is alias name for some "canonical" (the real) name www.ibm.com is really servereast.backup2.ibm.com
  - value is canonical name
- Type=MX
  - value is name of mailserver associated with name

25

DNS Message Format

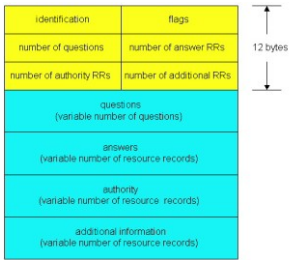


26

DNS protocol : *query* and *reply* messages, both with same *message format*

Message header

- Identification: 16 bit # for query, reply to query uses same #
- Flags:
  - Query or reply
  - Recursion desired
  - Recursion available
  - Reply is authoritative



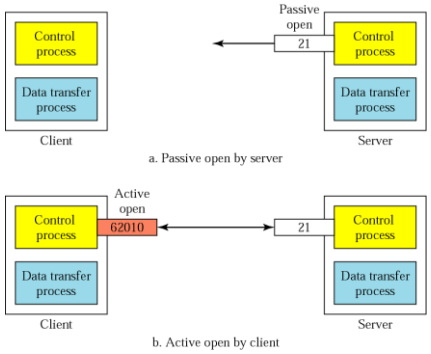
27

File Transfer Protocol : FTP

- Allows a user to copy files to/from remote hosts
- FTP uses the services of TCP
- It needs two TCP connections
  - The well-known port 21 is used for the control connection
  - and the well-known port 20 for the data connection
- Goal of FTP (Objective of FTP)
  - promote sharing of files
  - encourage indirect use of remote computers
  - shield user from variations in file storage
  - transfer data reliably and efficiently

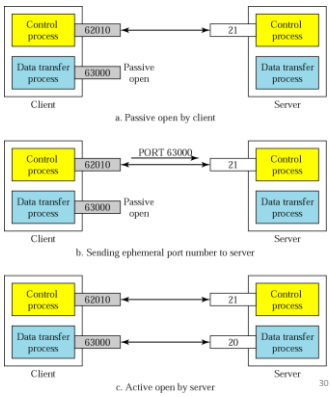
28

FTP Connections: The control connection



29

FTP : The data connection



30

The Data Connection

- Uses Server's well-known port 20
  - Client issues a passive open on an ephemeral port, say *x*.
  - Client uses PORT command to tell the server about the port number *x*.
  - Server issues an active open from port 20 to port *x*.
  - Server creates a child server/ephemeral port number to serve the client

31

Secure File Transfer Protocol (SFTP)

- Secure version of FTP
- Designed by IETF as an extension of the secure shell(SSH) protocol version 2.0 to provide secure file transfer capabilities
- SFTP requires that the client user must be authenticated by the server and data transfer must take place over a secure channel
- SFTP is designed to be platform independent and is available on most platform
- All the data is encrypted before sending on the network
- SFTP protect against password sniffing and other attacks
- It protects the integrity of the data

32

Electronic Mail

- It is one of the most widely used and popular internet applications.
- User can communicate with each other across the network
- Every user owns his own mailbox which he uses to send, receive and store messages from other users
  - Every user can be uniquely identified by his unique email address
- Mailbox principle
  - A sender does not require the receiver to be online nor the recipients to be present
  - A user's mailbox can be maintained anywhere in the internet on the server

33

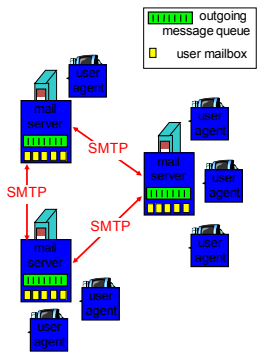
Electronic Mail Contd..

Three major components:

- user agents
- mail servers
- Simple Mail Transfer Protocol: SMTP

User Agent

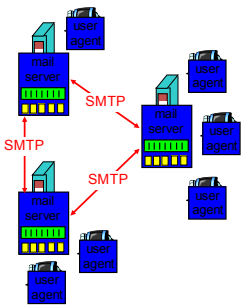
- "mail reader"
- composing, editing, reading mail messages
- e.g., Eudora, Outlook, elm, Netscape Messenger
- outgoing, incoming messages stored on server



34

Mail Servers

- mailbox contains incoming messages for user
- message queue of outgoing (to be sent) mail messages
- SMTP protocol between mail servers to send email messages
  - client: sending mail server
  - "server": receiving mail server



35

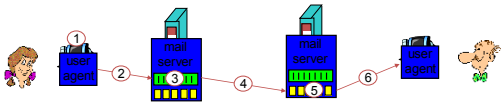
Electronic Mail: SMTP

- uses TCP to reliably transfer email message from client to server, port 25
- direct transfer: sending server to receiving server
- three phases of transfer
  - handshaking (greeting)
  - transfer of messages
  - Closure

36

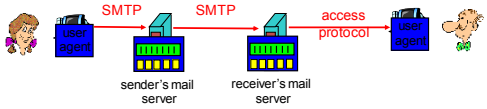
Scenario: Alice sends message to Bob

- Alice uses UA to compose message and send "to" bob@someschool.edu
- Alice's UA sends message to her mail server
  - message placed in message queue
- Client side of SMTP opens TCP connection with Bob's mail server
- SMTP client sends Alice's message over the TCP connection
- Bob's mail server places the message in Bob's mailbox
- Bob invokes his user agent to read message



37

Mail access protocols



- Mail access protocol: retrieval from server
  - POP: Post Office Protocol
    - authorization (agent <-->server) and download
  - IMAP: Internet Mail Access Protocol
    - more features (more complex)
    - manipulation of stored messages on server
  - HTTP: Hotmail , Yahoo! Mail, etc.

38

POP

- a protocol used to retrieve e-mail from a mail server
- Most e-mail applications (sometimes called an *e-mail client*) use the POP protocol
- Examples of native mail system
  - MS outlook, Lotus Notes, MS Exchange, Eudora
- There are two versions of POP
  - The first, called *POP2,* became a standard in the mid-80's and requires SMTP to send messages.
  - The newer version, POP3, can be used with or without SMTP
  - POP3 uses TCP/IP port 110

39

IMAP

- It is a method of accessing electronic mail messages that are kept on a possibly shared mail server.
- In other words, it permits a "client" email program to access remote message stores as if they were local.
- For example,
  - email stored on an IMAP server can be manipulated from a desktop computer
    - at home
    - a workstation at the office
    - and a notebook computer while travelling
- IMAP uses TCP/IP port 143

40

Feature	POP3	IMAP
Where is protocol defined?	RFC 1939	RFC 2060
Which TCP port is used?	110	143
Where is e-mail stored?	User's PC	Server
Where is e-mail read?	Off-line	On-line
Connect time required?	Little	Much
Use of server resources?	Minimal	Extensive
Multiple mailboxes?	No	Yes
Who backs up mailboxes?	User	ISP
Good for mobile users?	No	Yes
User control over downloading?	Little	Great
Partial message downloads?	No	Yes
Are disk quotas a problem?	No	Could be in time
Simple to implement?	Yes	No
Widespread support?	Yes	Growing

A comparison of POP3 and IMAP

41

Proxy Server

- Proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.
- Proxy server stores all the data it receives as a result of placing requests for information on the internet in it's *cache.*
  - Cache simply means memory
  - The cache is typically hard disk space, but it could be RAM
  - Caching documents means keeping a copy of internet documents so the server doesn't need to request them over again
  - With proxy caching, clients make requests to servers, but the requests first go through a proxy cache

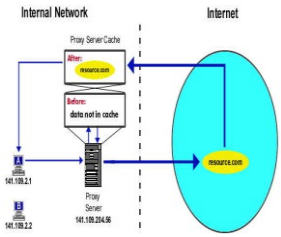
42

Advantages of Caching Documents

- Save users considerable time when they requested documents normally located out on the Internet.
- Save considerable network cost and connection time.
- Reduce the amount of disk space browsers use because many local browsers can use a single copy of a cached document.
- Caching is disk based; when you restart the server, documents that you cache are still available.
- Proxy caching is the most widely used method to improve Web performance

43

Caching a Document on a Proxy Server

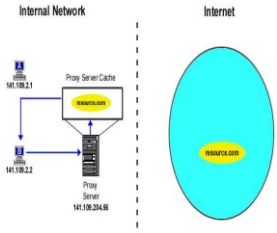


Scenario 1:

- user **A** request a web page
- the request goes to the proxy server
- the proxy server checks to see if the document is stored in cache
- the document is not in cache so the request is sent to the Internet
- the proxy server receives the request, stores (or caches) the page
- the page is sent to user **A** where is viewed

44

Retrieving Cached Documents



Scenario 2:

- user **B** request the same page as user **A** (ie. resource.com)
- the request goes to the proxy server
- the proxy server checks its cache for the page
- the page is stored in cache
- the proxy server sends the page to user **B** where it is viewed
- no connection to the Internet is required

45

Managing Cached Documents

- Many documents available on the Internet are "living" documents
- Determining when documents should be updated or deleted can be difficult task
  - Some documents can remain stable for a very long time and then suddenly change.
  - Other documents can change weekly or a daily basis.
- You need to decide carefully how often to refresh or delete the documents held in cache.

46

SNMP (Simple Network Management Protocol)

- an application layer protocol used to monitor network-attached devices.
- part of the TCP/IP protocol suite
- It allows Administrators to
  - manage network performance,
  - find and solve network problems, and
  - plan for network growth
- SNMP works as the manager/agent model.
  - Manager (the monitoring "client")
  - Agent (running on the equipment server)

47

SNMP Contd..

- The manager and agent use a Management Information Base (MIB) and a relatively small set of commands to exchange information.
  - MIBs are files defining the objects that can be queried, including:
    - Object name
    - Object description
    - Data type (integer, text, list)
  - The MIB is organized in a tree structure with individual variables, represented as leaves on the branches.
  - A long numeric tag or object identifier (OID) is used to distinguish each variable uniquely in the MIB and in SNMP messages.

48

How does it work?

- Basic commands
  - GET (manager -> agent)
    - Query for a value
  - GET-NEXT (manager -> agent)
    - Get next value (list of values for a table)
  - GET-RESPONSE (agent -> manager)
    - Response to GET/SET, or error
  - SET (manager -> agent)
    - Set a value, or perform action
  - TRAP (agent -> manager)
    - Spontaneous notification from equipment (line down, temperature above threshold, …)

Thank You!!!!!!