Unit-6 - Application Layer.

-Ankit Pangeni

DATE

* Introduction and functions

It is a layer with the highest abstraction in TCP/IP model. It provides user interface ie. human Computer ~~se~~ interaction and Supports for services like emails, remote file access and transfer., & so on. This layer is implemented by network applications Eg Applications, Browsers, skype, Messengers.

Functions:

- Network virtual terminal : Allows user to log on to a remote host.
- File transfer and Management : Allows user to access files in a remote host.
- Mail Service:- Provides the basis for email forwarding & Storage facilities
- Directory service:- Provides access for global information about various services

* Web and HTTP

The World wide web (WWW), or simply web, is a repository for information spread all over the word & linked together. It is

DATE

all the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP). To use WWW, we need three components: a browser, a web server, and a protocol (HTTP).

The HTTP is a networking tool for distributed, collaborative, hypermedia information systems. It is the foundation of data communication for WWW. It functions as a request response protocol in the client-server computing protocol. It uses TCP (reliability) (used to acess data on WWW.). It transfers data in the form of plain text, hypertext, audio, video & so on.

→ HTTP message format

HTTP message is used to show how data is exchanged between the client & the server. It is based on client-server architecture & consists of an initial request line and an initial response line.

Format: HTTP_Message = Request | Response ; HTTP 1.1 message

- Initial Request line → It is different for the request and the response. A request line consists of 3 part: a method name, requested resource's local path, & the HTTP version being used. All these parts are separated by spaces: syntax: GET /path/to/file/index.html HTTP/1.0
- Initial response line: It is also known as the status line. It also has 3 parts: Http version, a response status code that gives the result of the request & the English reason phase describing status code.

Ex: HTTP/1.0 200 OK

PAGE

classmate

DATE

→ Non-persistent and Persistent connections

HTTP 1.1 specifies a persistent connection by default. Here, the connection is left open by the server for more requests after sending a response. The server can close the connection at the request of a client or if the time-out has been reached. The sender usually sends the length of the data with each response. In cases when sender doesn't know the length of the data, the server informs the client that the length is not known & closes the connection after sending the data so the client knows that the end of the data has been reached.

HTTP 1.0 specifies a non persistent connection. Here, one TCP connection is made for each request/response. The following lists the steps in this strategy:

1. The client opens a TCP connection & sends a request.
2. The server sends the response & closes the connection.
3. The client reads the data until it encounters an end-of-file marker; it then closes the connection.

Here, for N different pictures in N different files, the connection must be opened & closed N times. It imposes high overhead on the server.

DATE

* DNS and Query Types:-

The Domain Name System (DNS) is a supporting program that is used by the other program such as e-mail. It is a global system for translating IP addresses to human-readable domain names. When a user tries to access a web address like 'example.com' their web browser or application performs a DNS query against a DNS server, supplying the host name. The DNS server takes the hostname & resolves it into a numeric IP address, which the web browser can connect to.

→ Query types in DNS system:-

There are three types of queries in DNS system.

i) Recursive Query → Here, a DNS client provides a hostname, and the DNS resolver must provide an answer. DNS resolver responds with either a relevant source record, or an error message if it can't be found. The resolver starts a recursive query process, starting from the DNS root server, until it finds the authoritative Name Server that holds the IP address & other information for requested host name.

ii) Iterative Query → Here, a DNS client provides a hostname, & the DNS resolver returns the best answer it can. If the DNS resolver has the relevant DNS records in its cache, it returns them. If not, it refers the DNS client to the root server or another authoritative name Server which is nearest to the reqd DNS zone

DATE

iii) Non-recursive query :- Here, DNS resolver already knows the answer. It either immediately returns a DNS record or queries a DNS Name server which is authoritative for the record. In both cases, there is no need for additional rounds of queries, rather a response is immediately returned to the client.

→ Services provided by DNS

i) Host Aliasing → A host with a complicated hostname can have one or more alias names. DNS can be invoked by an application to obtain the canonical hostname for a supplied alias hostname as well as the ip address of the host.

ii) Mail Server Aliasing → It is highly desirable that e-mail address be easy to remember. Ex, If bob has an account with gmail, his email address must be as simple as bob@gmail.com. DNS can be invoked by a mail application to obtain the canonical hostname for a supplied alias hostname as well as Ip of host

iii) Load distribution → DNS is used to perform load distribution among replicated servers, such as replicated web servers. Busy sites such as cnn.com are replicated over multiple servers, with each running on a different end system & having a different Ip address. For replicated web servers a set of Ip addresses is thus associated with one cannonical hostname.

classmate

PAGE

DATE

Overview of how DNS works

DNS is a naming database in which internet domain names are located & translated into IP addresses. They translate what a user types into a browser into something the machine can use to find a webpage.

DNS is a client/server network communication. DNS clients send requests to the server while DNS servers send responses to the client. Client requests contain a domain name which is converted to IP address known as forward DNS lookups. DNS implements a distributed database to store the name of all the hosts available on the internet.

If a client, like a web browser sends a request containing a hostname, then a piece of software DNS resolver sends a request to dns server to obtain the IP address of a hostname. If the dns server doesn't contain the IP address associated with hostname, then it forwards the request to another DNS server. If the IP address has arrived at the resolver, it completes the request over the IP.

→ **DNS Records**

A DNS record is a database record used to map a URL into an IP address. They are stored in DNS servers & work to help users connect their sites to the outside world. Its main purpose is that people & applications don't have to remember big numbers to navigate to a domain. Ex: www.ankitpangeni.com has an IP of 104.161.23.62, so it is easier to remember a friendly name.

PAGE

classmate

DATE

Some different types of dns records are:

- A Record → Connects an Ip Address to a host name
- CNAME Record → Allows more than one DNS name for a host
- MX Record → Ensures email is delivered to the right location
- NS Record → Contains the name server info
- SRV Record → Finds computers that host specific services
- SPF Record → Used to help prevent against spam

→ DNS Messages.

DNS has two types of messages: query and response. Both types have the same format. The query message consists of a header & question records. & the response message consists of a header, question records, answer records, authoritative & additional records

- Header → Both query & response messages have the same header format with some fields set to zero for the query messages. Header is 12 bytes
- Question section → It consists of one or more question records. It is present in both query & record messages.
- Answer section → It consists of one or more resource records. It is present only on response messages & includes the answer from server to the client
- Authoritative section → This contains one or more resource records. It is present only on response messages. It gives information (domain name) about one or more authoritative servers for query

DATE

- Additional information section → It provides additional information that may help the resolver. Ex server may give the domain name of an authoritative server to the resolver in authoritative section & include the IP address of the same authoritative server in the addition information section.

✝ File Transfer & Email protocols

1. FTP

The File Transfer Protocol (FTP) is a standard communication protocol protocol used for the transfer of computer files from a server to a client on a computer network. It is built on a client-server model architecture using separate control & data connections between the client and the server. It basically refers to the rules that govern how computers transfer files from one system to another over the internet.

2. SFTP

SSH File Transfer Protocol is a secure file transfer protocol. It runs over the SSH protocol & supports the full security & authentication functionality of SSH. It is basically the FTP with added layer of security to the process. It also protects against password sniffing & integrity of data using encryption & cryptographic hash functions. It also authenticates both server & the user.

PAGE

classmate

DATE

3. SMTP

Simple Mail Transfer Protocol (SMTP) is an internet standard communication protocol for electronic mail transmission. It is a program used for sending messages to the other computers based on the e-mail addresses. It supports sending message to one or more recepients, message can include text, voice, video or graphics. Its main purpose is to set up communication rules between servers. The SMTP model is of two types: End-to-end & store-and-forward method. End-to-End model is used to communicate between different organizations whereas Store & forward is used within an organization.

4. IMAP

Internet Message Access Protocol, is a standard email retrieval protocol. It stores email messages on a mail server & enables the recipient to view & manipulate them as though they were stored locally on their device. It allows you to access your email wherever you are, from any device. When you read an email message using IMAP, you aren't actually downloading or storing it in your computer, instead you're reading from the email service.

5. POP3

Post office protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. POP3 allows us to download email messages on our local computer & read them even when we are offline. It works on two ports: 110 & 995. It only supports one-way email synchronization, allowing users to download emails from a server to a client.

DATE

Overview of Application server concepts

An application server enables a server to generate a dynamic, customized response to a client request. It is frequently viewed as a part of three-tier application, consisting of graphical user interface (GUI) server, an application server & a database & transaction server. It provides the business logic for an application program

1. Proxy

A proxy server is a computer system, router or which is a server application that acts as an intermediary (gateway) between a client requesting a resource & the server providing that resource. The word proxy means "to act on the behalf of other," and a proxy server acts on behalf of the user. All requests to the Internet go to the proxy server first, which evaluates the requests & forwards it to the internet. Likewise, responses come back to the proxy server & then to the user. It helps to prevent an attacker from invading a private network.

2. Web

A web server accepts & fulfills requests from clients for static content. (Ie. HTML pages, files, images, & videos) from a website. It is a computer where the web content is stored. Basically, web server is used to host the websites but there exists other web servers also, such as gaming, storage, FTP, email, etc. website is a collection of web pages while web server is a software that responds to the request for web resources.

PAGE

classmate

DATE

9. Mail.

A mail server also known as mail transfer agent is an application that receives incoming email from local users & forwards outgoing email for delivery. A computer dedicated to running such applications is called a mail server. Ex. gmail.

Mail servers can be broken down into two main categories:- Outgoing mail servers & incoming mail servers. Outgoing mail servers are known as SMTP servers and Incoming are called POP3 & IMap. IMap servers always store copies of messages on servers and POP3 servers are best known for storing sent & received messages locally.

* Network Management

Network management is the process of administering and managing computer networks. It is primarily focused on maintaining reliability, efficiency and overall performance of data transfer channels. The most common network management system is SNMP.

SNMP

SNMP stands for Simple Network Management Protocol. It is an Internet standard protocol for handling devices on a IP networks. Devices that typically provide SNMP include routers, switches, servers, workstations, printers, etc.

classmate

PAGE

DATE

SNMP is very simple, yet powerful. It helps the ability to manage your networks by.

-> provide read/write capabilities
-> Collect information on how much bandwidth is used.
-> Collect error reports into a log.
-> Email an alert when your server is low on disk space.

Components

- SNMP manager -> Used to communicate with SNMP agent on network devices. It is a software installed on a PC or a server to operate one or more network management systems. Functions: Queries agents, gets response from agents & sets variables in agents

- Managed devices -> It is the network element that requires some form of monitoring & management. Ex: routers, switches, servers, etc.

- SNMP agent -> It is a program that is packaged with the network element. It collects the management information database from the device & makes it available locally to the SNMP manager, when it is queried for

- Management Information Base (MIB) -> MIB files are the set of parameters that an SNMP manager can request the agent. Agent assembles these data locally & stores them as described in MIB.

Questions asked from this Chapter

DATE

Q. Why do we need a DNS system when we can directly use an IP address? What is domain name space? (2076 - 5 marks).

Q. Define DNS. Explain DNS records & DNS messages. (2068 - 5 marks) (2069 - 5 marks) (2075 - 5 marks).

Q. Explain the principles of application layer protocols. What do you mean by file transfer? (2067 - 5 marks).

Q. Explain working principle of DNS. (2069 - 5 marks) (2070 - 5 marks). (2071 - 2.5 marks) (2074 - 2.5 marks)