[Notes on Unit-V]: Computer Networks]

Syllabus:-Unit-V

- Application Layer - File Transfer, Access and Management,
- Electronic mail.
- Virtual Terminals,
- Other applications.
- Example Networks - Internet and Public Networks.

Possible Conceptual Questions:-

Question No-(1): What are various responsibilities of Application Layer?
Answer:- Responsibilities of Application Layer:
Application layer is basically responsible for providing the Interface to users so that network may be accessed. Other responsibilities of the application layer may be defined as below:-

- Identifying and establishing the availability of intended communication partners
- Synchronizing cooperating applications
- Establishing agreement on procedures for error recovery
- Controlling data integrity

Application Layer Examples: Following are the common examples of the Application Layer protocols:

- Domain Name System
- File Transfer Protocol
- Hypertext Transfer Protocol
- Simple Mail Transport Protocol
- Simple Network Management Protocol
- Telnet

Question No-(2): What do you understand by File Transfer Protocol? Explain at least 10 Commands of FTP? How FTP is different from TFTP?
Answer: - File Transfer Protocol:- File Transfer Protocol**(**FTP) is an important Application Layer protocol. It is a reliable, connection-oriented service that uses TCP to transfer files between systems.

FTP and TFTP

- FTP is connection-oriented service that uses TCP.
- TFTP can be treated as LAN version of FTP.
- TFTP is a connectionless service that uses User Datagram Protocol (UDP).
- TFTP is used on routers to transfer configuration files and Cisco IOS images.
- TFTP is designed to be small and easy to implement.

FTP Commands: The FTP (**F**ile **T**ransfer **P**rotocol) utility program is commonly used for copying files to and from other computers. These computers may be at the same site or at different sites thousands of miles apart..

To connect your local machine to the remote machine, type

```
ftp machinename
```

where machinename is the full machine name of the remote machine, e.g., dbitdoon.com. If the name of the machine is unknown, you may type

```
ftp machinennumber
```

where machinennumber is the net address of the remote machine, e.g., 129.82.45.181. In either case, this command is similar to logging onto the remote machine. If the remote machine has been reached successfully,

FTP responds by asking for a loginname and password.

When you enter your own loginname and password for the remote machine, it returns the prompt

```
ftp>
```

and permits you access to your own home directory on the remote machine. You should be able to move around in your own directory and to copy files to and from your local machine using the FTP interface commands given on the following page.

Anonymous FTP

At times you may wish to copy files from a remote machine on which you do not have a login name. This can be done using anonymous FTP.

When the remote machine asks for your loginname, you should type in the word anonymous. Instead of a password, you should enter your own electronic mail address. This allows the remote site to keep records of the anonymous FTP requests.

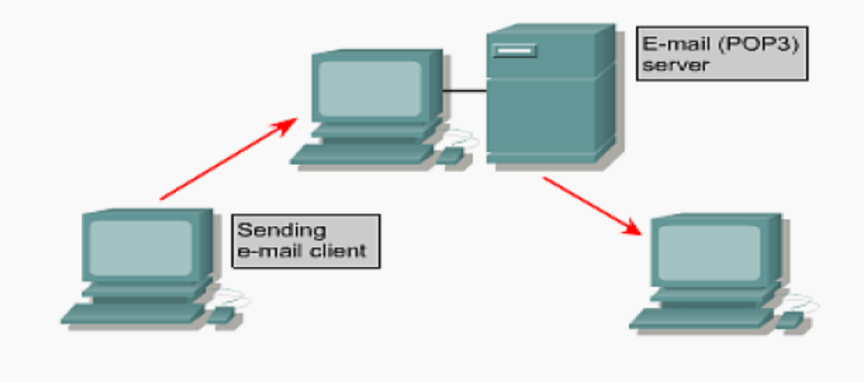
Once you have been logged in, you are in the anonymous directory for the remote machine. This usually contains a number of public files and directories. Again you should be able to move around in these directories. However, you are only able to copy the files from the remote machine to your own local machine; you are not able to write on the remote machine or to delete any files there.

Other Common FTP Commands

?	to request help or information about the FTP commands
ascii	to set the mode of file transfer to ASCII (this is the default and transmits seven bits per character)
binary	to set the mode of file transfer to binary (the binary mode transmits all eight bits per byte and thus provides less chance of a transmission error and must be used to transmit files other than ASCII files)
bye	to exit the FTP environment (same as quit)
cd	to change directory on the remote machine
close	to terminate a connection with another computer
close brubeck	closes the current FTP connection with brubeck, but still leaves you within the FTP environment.
delete	to delete (remove) a file in the current remote directory (same as rm in UNIX)
get	to copy one file from the remote machine to the local machine

get ABC DEF	copies file ABC in the current remote directory to (or on top of) a file named DEF in your current local directory.
get ABC	copies file ABC in the current remote directory to (or on top of) a file with the same name, ABC, in your current local directory.
help	to request a list of all available FTP commands
lcd	to change directory on your local machine (same as UNIX cd)
ls	to list the names of the files in the current remote directory
mkdir	to make a new directory within the current remote directory
mget	to copy multiple files from the remote machine to the local machine; you are prompted for a y/n answer before transferring each file
mget *	copies all the files in the current remote directory to your current local directory, using the same filenames. Notice the use of the wild card character, *.
mput	to copy multiple files from the local machine to the remote machine; you are prompted for a y/n answer before transferring each file
open	to open a connection with another computer
put	to copy one file from the local machine to the remote machine
pwd	to find out the pathname of the current directory on the remote machine
quit	to exit the FTP environment (same as bye)
rmdir	to to remove (delete) a directory in the current remote directory

Question No-(3): Explain working of E-mail System with the help of suitable diagrams?
Answer: Working of an Email System: - Email system is based on the working of two protocols viz. SMTP and POP3.



When sending an e-mail message, the process that is followed is to send the letter to the post office where the user belongs. The user then picks up the e-mail from the post office.

SMTP is a relatively simple, text-based protocol, in which one or more recipients of a message are specified (and in most cases verified to exist) along with the message text and possibly other encoded objects. The message is then transferred to a remote server using a procedure of queries and responses between the client and server.

An email client knows the *outgoing mail* SMTP server from its configuration. A relaying server typically determines which SMTP server to connect to by looking up the each recipient's domain name (the part of the email address to the right of the **at** (**@**) sign).

The SMTP client initiates a TCP connection to server's port 25 (unless overridden by configuration). SMTP is a "push" protocol that does not allow one to "pull" messages from a remote server on demand. To do this a mail client must use POP3 through port No 110.

However E-mail servers communicate with each other using the Simple Mail Transport Protocol (SMTP) to send and receive mail.

Question No-(4): What do you understand by Virtual Terminals? What is the use of Virtual Terminals?

Answer: Virtual Terminals: Virtual Terminal refers to an application service that :-

(a) Allows host terminals on a multi-user network to interact with other hosts regardless of hardware, terminal type and characteristics

(b) Allows remote log-on by local-area-network managers for the purpose of management,

(c) Allows users to access information from another host processor for transaction processing, and

(d) Serves as a backup facility.

This is a software in user's computer that emulates a particular type of hardware terminal in order to access a server. When personal computers began to proliferate in the late 1980s, virtual terminals enabled users to access the corporate minicomputers and mainframes from their PCs without having to use dedicated terminals. These provide access to a database or an information system via a common interface such as a Web browser on any user's computer.

Virtual terminal protocol based on the OSI application layer protocols has been defined. However, the virtual terminal protocol is not widely used on the Internet.

Following three terms are used in Virtual Termianal:-

- **Terminal emulator:-** An application program that provides access to virtual terminals
- **Pseudo terminal:-** The software interface that provides access to virtual terminals
- **Virtual console:-** An analogous concept that provides several *local* consoles to remote devices and services.

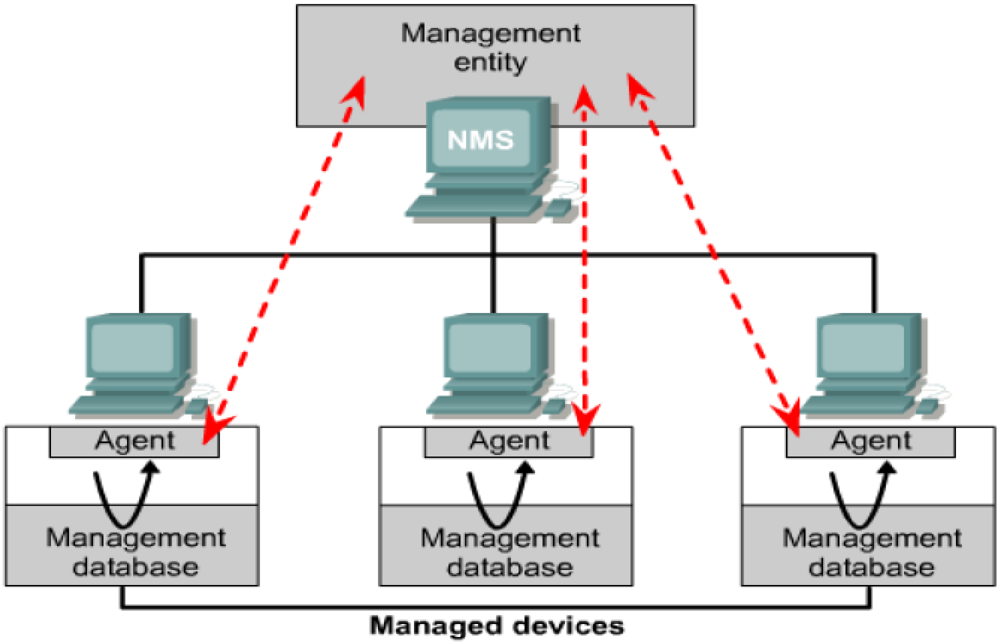
Question No-(5): What do you understand by SNMP? Explain how networks are managed by SNMP? Highlight terms used in SNMP?

Answer:-**SNMP (Simple Network Management Protocol):-** The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices.

Following terms need to be defined to explain the working of SNMP.

- **Network elements – (Sometimes called managed devices):**- network elements are hardware devices such as computers, routers, and terminal servers that are connected to networks and are being managed.

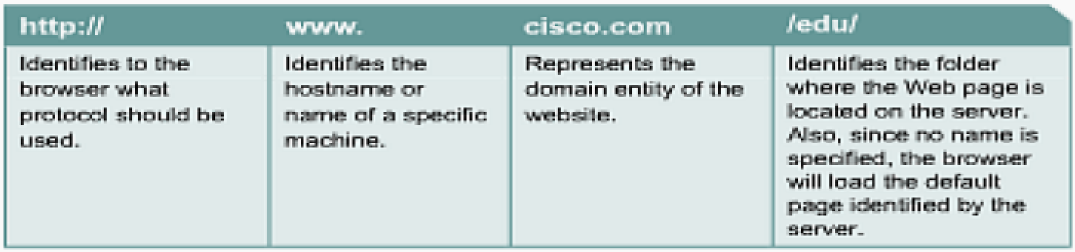
- **Network Managing Agents** -- Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.
- **Managed object** -- A managed object is a characteristic of something that can be managed. For example, a list of currently active TCP circuits in a particular host computer is a managed object. Managed objects differ from variables, which are particular object instances. Using our example, an object instance is a single active TCP circuit in a particular host computer. Managed objects can be scalar (defining a single object instance) or tabular (defining multiple, related instances).
- **Management information base (MIB)** -- A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules.
- **Structure of Management Information (SMI)** -- The SMI defines the rules for describing management information. The SMI is defined using ASN(Abstract Syntax Notations).
- **Syntax notation** -- A syntax notation is a language used to describe a MIB's managed objects in a machine-independent format. Consistent use of a syntax notation allows different types of computers to share information. Internet management systems use a subset of the International Organization for Standardization's (ISO's) Open System Interconnection (OSI) Abstract Syntax Notation (ASN.1) to define both the packets exchanged by the management protocol and the objects that are to be managed
- **Network management stations (NMSs)** -- Sometimes called consoles, these devices execute management applications that monitor and control network elements. Physically, NMSs are usually engineering workstation-caliber computers with fast CPUs, megapixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.
- **Parties** -- Newly defined in SNMPv2, a party is a logical SNMPv2 entity that can initiate or receive SNMPv2 communication. Each SNMPv2 party comprises a single, unique party identity, a logical network location, a single authentication protocol, and a single privacy protocol. SNMPv2 messages are communicated between two parties. An SNMPv2 entity can define multiple parties, each with different parameters. For example, different parties can use different authentication and/or privacy protocols.
- **Management protocol** -- A management protocol is used to convey management information between agents and NMSs. SNMP is the Internet community's de facto standard management protocol.



<u>Question No-(6):</u> What do you understand by URL? What are various portions of the URL?
<u>Answer</u>:- **<u>URL(Uniform Resource Locator)</u>**:- URL refers to the direct link to a particular file of portion of the file if that file is accessible over the Internet. Using URL one can access the file directly.
URL has its standard portion:-
First Portion defines the protocol based on which that particular site or file is developed.
e.g. http://   ftp://   etc.
Second portion identifies the name of the computers on which the file exist.
Further extension is also possible: -
e.g.:- http://www.dbitdoon.com:80/CS/IT/index.html#point1

In above URL protocol is http(hyper text transfer protocol), System name is www.dbitdoon.com .point1 portion of file Index.html is being accessed through the port no 80 of this machine. Index.html residing inside the IT folder that in turn resides inside CS folder.

Computer name also can be interpreted as below:-



http://	www.	cisco.com	/edu/
Identifies to the browser what protocol should be used.	Identifies the hostname or name of a specific machine.	Represents the domain entity of the website.	Identifies the folder where the Web page is located on the server. Also, since no name is specified, the browser will load the default page identified by the server.

This figure identifies the parts of a standard Uniform Resource Locator (URL) address.

Question No-(7): What do you understand by DNS? How DNS maps names into ip-address?

Answer: -The **Domain Name System** (DNS) associates various information with domain names; most importantly, it serves as the "phone book" for the Internet by translating human-readable computer hostnames, e.g. *www.example.com*, into IP addresses, e.g. *208.77.188.166*, which networking equipment needs to deliver information. It also stores other information such as the list of mail servers that accept email for a given domain. In providing a worldwide keyword-based redirection service, the Domain Name System is an essential component of contemporary Internet use.

•A domain is a group of computers that are associated by their geographical location or their business type.
•There are more than 200 top-level domains on the Internet, examples of which include the following:
us – United States
.uk – United Kingdom
.edu – educational sites
.com – commercial sites
.gov – government sites
.org – non-profit sites
.net – network service

How DNS works in theory : DNS working may be understood with the help of following terms:-

The domain name space :-The domain name space consists of a tree of domain names. Each node or leaf in the tree has zero or more *resource records*, which hold information associated with the domain name. The tree sub-divides into *zones* beginning at the root zone. A DNS zone consists of a collection of connected nodes authoritatively served by an *authoritative DNS nameserver*. (Note that a single nameserver can host several zones.)

When a system administrator wants to let another administrator control a part of the domain name space within the first administrator's zone of authority, control can be delegated to the second administrator. This splits off a part of the old zone into a new zone, which comes under the authority of the second administrator's nameservers. The old zone ceases to be authoritative for the new zone.

Parts of a domain name

A domain name usually consists of two or more parts (technically a **label**), which is conventionally written separated by dots, such as example.com.

- The rightmost label conveys the top-level domain (for example, the address www.example.com has the top-level domain **com**).
- Each label to the left specifies a subdivision, or subdomain of the domain above it. Note: "subdomain" expresses relative dependence, not absolute dependence. For example: example.com comprises a subdomain of the com domain, and www.example.com comprises a subdomain of the domain **example.com**. In theory, this subdivision can go down 127 levels. Each label can contain up to 63 characters. The whole domain name does not exceed a total length of 253 characters.
- A hostname refers to a domain name that has one or more associated IP addresses; ie: the 'www.example.com' and 'example.com' domains are both hostnames, however, the 'com' domain is not.

DNS servers

The Domain Name System consists of a hierarchical set of DNS servers. Each domain or subdomain has one or more authoritative DNS servers that publish information about that domain and the name servers of any domains "beneath" it. The hierarchy of authoritative DNS servers matches the hierarchy of domains. At the top of the hierarchy stand the root nameservers: the servers to query when looking up (*resolving*) a top-level domain name

DNS resolvers

A resolver looks up the resource record information associated with nodes. A resolver knows how to communicate with name servers by sending DNS queries and heeding DNS responses.
A DNS query may be either a recursive query or a non-recursive query:

- A non-recursive query is one where the DNS server may provide a partial answer to the query (or give an error). DNS servers must support non-recursive queries.
- A recursive query is one where the DNS server will fully answer the query (or give an error). DNS servers are not required to support recursive queries.

The resolver (or another DNS server acting recursively on behalf of the resolver) negotiates use of recursive service using bits in the query headers.
Resolving usually entails iterating through several name servers to find the needed information. However, some resolvers function simplistically and can communicate only with a single name server. These simple resolvers rely on a recursive query to a recursive name server to perform the work of finding information for them.

Address resolution mechanism

In practice, full host names will frequently consist of just three segments (e.g. www.*inadomain.example*).
For querying purposes, software interprets the name segment by segment, from right to left, using an iterative search procedure. At each step along the way, the program queries a corresponding DNS server to provide a pointer to the next server which it should consult.

A DNS recursor consults three nameservers to resolve the address www.dbitdoon.com
As originally envisaged, the process was as simple as:

1. the local system is pre-configured with the known addresses of the root servers in a file of *root hints*, which need to be updated periodically by the local administrator from a reliable source to be kept up to date with the changes which occur over time.
2. query one of the root servers to find the server authoritative for the next level down (so in the case of our simple hostname, a root server would be asked for the address of a server with detailed knowledge of the *example* top level domain).
3. querying this second server for the address of a DNS server with detailed knowledge of the second-level domain (*inadomain.example* in our example).
4. repeating the previous step to progress down the name, until the final step which would, rather than generating the address of the next DNS server, return the final address sought.

Question No-(8): What do you mean by public network? Make a note on Internet?

Answer :- (Students must prepare a good short note on Internet.)