Government Polytechnic College, Jodhpur
Department of Computer Science (NBA Accredited)

Programme: Diploma **Class Test**: II **Session**: 2017-18
Course: Computer Network **Year**: IIIrd
Course CODE: CS-306 **Time:** 16:00 to 17:00
Max.Marks : 15 **Date:** 24-01-2018
Instructions to candidates: Attempt Any Three Questions

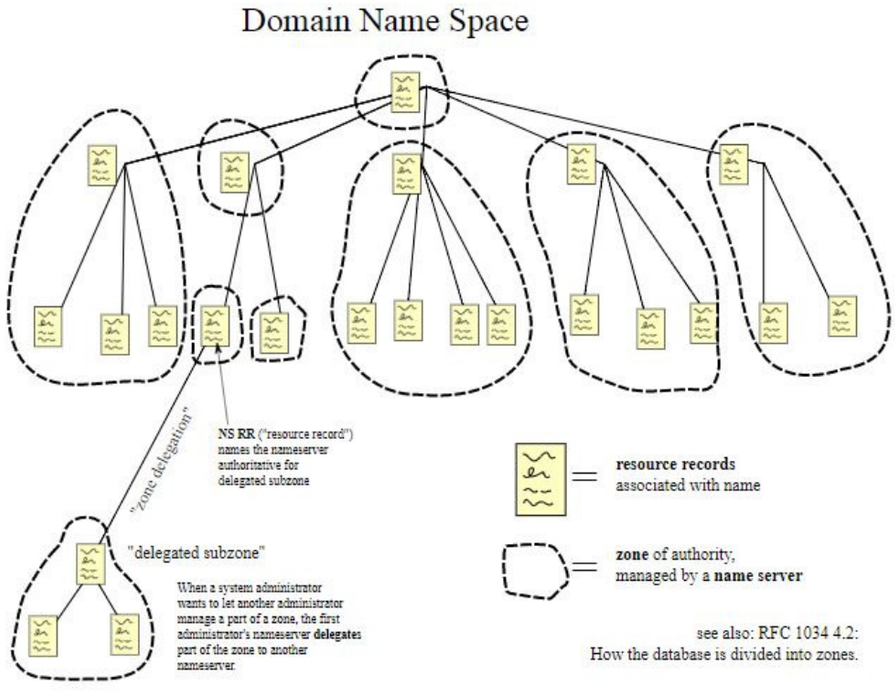
SI#	Question	Marks	CO MAPPING
1	Explain DNS.	5	CO4
2	Explain Simple Network Management Protocol.	5	CO4
3	Explain FTP.	5	CO4
4.	Explain the difference between POP and IMAP.	5	CO4

Ans.1 The **Domain Name System** (**DNS**) is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. By providing a worldwide, distributed directory service, the Domain Name System is an essential component of the functionality on the Internet, that has been in use since 1985.

The Domain Name System delegates the responsibility of assigning domain names and mapping those names to Internet resources by designating authoritative name servers for each domain. Network administrators may delegate authority over sub-domains of their allocated name space to other name servers. This mechanism provides distributed and fault tolerant service and was designed to avoid a single large central database.

The Domain Name System also specifies the technical functionality of the database service that is at its core. It defines the DNS protocol, a detailed specification of the data structures and data communication exchanges used in the DNS, as part of the Internet Protocol Suite. Historically, other directory services preceding DNS were not scalable to large or global directories as they were originally based on text files, prominently the hosts file.

To promote efficiency, servers can cache the answers they receive for a set amount of time. This allows them to respond more quickly the next time a request for the same lookup comes in. For example, if everyone in an office needs to access the same training video on a particular website on the same day, the local DNS server will ordinarily only have to resolve the name once, and then it can serve all the other requests out of its cache. The length of time the record is held -- the time to live -- is configurable; longer values decrease the load on servers, shorter values ensure the most accurate responses.



Ans 2 Simple Network Management Protocol (**SNMP**) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers, and more.[1]

SNMP is widely used in network management for network monitoring. SNMP exposes management data in the form of variables on the managed systems organized in a management information base (MIB) which describe the system status and configuration. These variables can then be remotely queried (and, in some circumstances, manipulated) by managing applications.

Three significant versions of SNMP have been developed and deployed. SNMPv1 is the original version of the protocol. More recent versions, SNMPv2c and SNMPv3, feature improvements in performance, flexibility and security.

SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.[2]

In typical uses of SNMP, one or more administrative computers called *managers* have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes a software component called an *agent* which reports information via SNMP to the manager.

An SNMP-managed network consists of three key components:

- Managed devices
- Agent – software which runs on managed devices
- Network management station (NMS) – software which runs on the manager

A *managed device* is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional (read and write) access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can be any type of device, including, but not limited to, routers, access servers, switches, cable modems, bridges, hubs, IP telephones, IP video cameras, computer hosts, and printers.

An *agent* is a network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP-specific form.

A *network management station* executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

In typical uses of SNMP, one or more administrative computers called *managers* have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes a software component called an *agent* which reports information via SNMP to the manager.

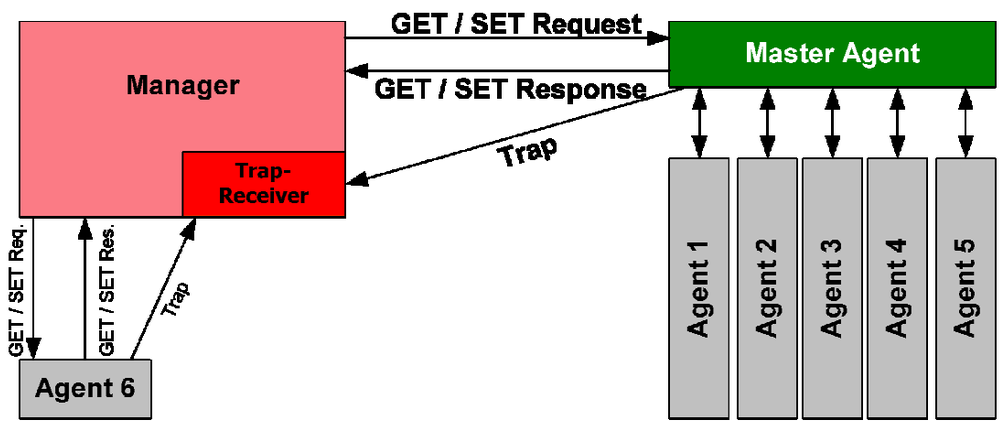
An SNMP-managed network consists of three key components:

- Managed devices
- Agent – software which runs on managed devices
- Network management station (NMS) – software which runs on the manager

A *managed device* is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional (read and write) access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can be any type of device, including, but not limited to, routers, access servers, switches, cable modems, bridges, hubs, IP telephones, IP video cameras, computer hosts, and printers.

An *agent* is a network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP-specific form.

A *network management station* executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

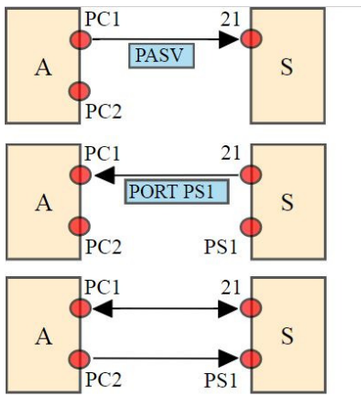


Ans 3.

The **File Transfer Protocol** (**FTP**) is a standard network protocol used for the transfer of computer files between a client and server on a computer network. FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server.[1]FTP users may

authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS). SSH File Transfer Protocol (SFTP) is sometimes also used instead; it is technologically different.

The first FTP client applications were command-line programs developed before operating systems had graphical user interfaces, and are still shipped with most Windows, Unix, and Linux operating systems.Many FTP clients and automation utilities have since been developed for desktops, servers, mobile devices, and hardware, and FTP has been incorporated into productivity applications, such as web page editors.



FTP may run in *active* or *passive* mode, which determines how the data connection is established. In both cases, the client creates a TCP control connection from a random, usually an unprivileged, port N to the FTP server command port 21.

- In active mode, the client starts listening for incoming data connections from the server on port M. It sends the FTP command PORT M to inform the server on which port it is listening. The server then initiates a data channel to the client from its port 20, the FTP server data port.
- In situations where the client is behind a firewall and unable to accept incoming TCP connections, *passive mode* may be used. In this mode, the client uses the control connection to send a PASV command to the server and then receives a server IP address and server port number from the server, which the client then uses to open a data connection from an arbitrary client port to the server IP address and server port number received.

Ans 4.

BASIS FOR COMPARISON	POP3	IMAP
Basic	To read the mail ithas to be downloaded first.	The mail content can be checked partially before downloading.
Organize	The user can not organize mails in the mailbox of the mail server.	The user can organize the mails on the server.
Folder	The user can not create, delete or rename mailboxes on a mail server.	The user can create, delete or rename mailboxes on the mail server.
Content	A user can not search the content of mail for prior downloading.	A user can search the content of mail for specific string of character before downloading.

BASIS FOR COMPARISON	POP3	IMAP
Partial Download	The user has to download the mail for accessing it.	The user can partially download the mail if bandwidth is limited.
Functions	POP3 is simple and has limited functions.	IMAP is more powerful, more complex and has more features over POP3.