Theory:

CAT 5, CAT 6, and CAT 7

CAT 5, CAT 6, and CAT 7 are different generations of Ethernet cables, each with varying characteristics. Following are the key differences between them:

1) Speed and Bandwidth:
CAT 5: It supports data transfer speeds up to 100 Mbps (Megabits per second) with a maximum bandwidth of 100 MHz. CAT 5 cables are considered outdated and are rarely used for new installations.
CAT 6: It supports data transfer speeds up to 10 Gbps (Gigabits per second) with a maximum bandwidth of 250 MHz. CAT 6 cables are commonly used for home and small office networks.
CAT 7: It offers higher performance with data transfer speeds up to 10 Gbps and beyond, reaching up to 40 Gbps. It has a higher bandwidth capacity of 600 MHz. CAT 7 is designed for more demanding applications and larger network infrastructures.

2) Shielding:
CAT 5: It is typically an unshielded twisted pair (UTP) cable, meaning it does not have any shielding to protect against electromagnetic interference (EMI) or crosstalk.
CAT 6: It can be either unshielded twisted pair (UTP) or shielded twisted pair (STP) cable. Shielded variants have additional shielding to reduce EMI and crosstalk.
CAT 7: It features additional shielding known as individually shielded pairs (S/FTP or S/STP). This shielding provides better protection against EMI and crosstalk, leading to improved signal quality and reduced interference.

3) Connectors and Backward Compatibility:
CAT 5: It commonly uses RJ-45 connectors, which are the standard connectors for Ethernet cables. CAT 5 cables are backward compatible with newer Ethernet standards like CAT 5e, CAT 6, and CAT 7.
CAT 6: It also uses RJ-45 connectors, and CAT 6 cables are backward

compatible with CAT 5 and CAT 5e.
CAT 7: It uses specialized RJ-45 connectors with stricter specifications to ensure better signal integrity at higher frequencies. CAT 7 cables are backward compatible with older Ethernet standards as well.

4) Distance:
CAT 5: It is suitable for shorter distances within a network, typically up to 100 meters (328 feet).
CAT 6: It can also reach up to 100 meters for 10 Gbps speeds but may have reduced performance at longer distances.
CAT 7: It can achieve 10 Gbps speeds at longer distances, typically up to 100 meters (328 feet).

Aim: Configure IP static routing

Theory:

1) Static routing method is most trusted by a router.
2) Static routing is not really a routing protocol.
3) Static routes do not dynamically adapt to network changes, are not particularly scalable, and require manual updating to reflect changes.

Static routing has the following advantages

1) There is no bandwidth usage between routers, which means you could possibly save money on WAN links.
2) There is no overhead on the router CPU, which means you could possibly buy a cheaper router than you would use if you were using dynamic routing.
3) It adds security because the administrator can choose to allow routing access to certain networks only.

Static routing has the following disadvantages

1) Static routes don't dynamically adapt to network change.
2) If a network is added to the internetwork, the administrator has to add a route to it on all routers—by hand.
3) It's not feasible in large networks because maintaining it would be a full- time job in itself.
4) With static routing, as your network grows, it can be difficult just keep adding static routes makes sure everybody can still get everything.
5) The administrator must really understand the internetwork and how each router is connected in order to configure routes correctly.

Practical 5
Configure IP routing using RIP

Aim: Configure IP routing using Routing Information Protocol (RIP)

Theory:

RIP (Routing Information Protocol) is a standardized Distance Vector protocol, designed for use on smaller networks. RIP was one of the first true Distance Vector routing protocols, and is supported on a wide variety of systems. RIP adheres to the following Distance Vector characteristics:

- RIP sends out periodic routing updates (every 30 seconds)
- RIP sends out the full routing table every periodic update
- RIP uses a form of distance as its metric (in this case, hopcount)
- RIP uses the Bellman-Ford Distance Vector algorithm to determine the best "path" to a particular destination Other characteristics of RIP include:
- RIP supports IP and IPX routing.
- RIP utilizes UDP port 520 • RIP routes have an administrative distance of 120.
- RIP has a maximum hopcount of 15 hops. Any network that is 16 hops away or more is considered unreachable to RIP, thus the maximum diameter of the network is 15 hops. A metric of 16 hops in RIP is considered a poison route or infinity metric.

Practical 6
Configuring Simple and multi-area OSPF

Aim: Configuring Simple and multi-area OSPF

Theory:

Open shortest path first (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own shortest path first (SPF) algorithm. A link-state routing protocol is a protocol that uses the concept of triggered updates, i.e., if there is a change observed in the learned routing table then the updates are triggered only, not like the distance-vector routing protocol where the routing table is exchanged at a period of time.

Open shortest path first (OSPF) is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e., the protocol which aims at moving the packet within a large autonomous system or routing domain.

OSPF advantages –

1) Both IPv4 and IPv6 routed protocols
2) Load balancing with equal-cost routes for the same destination
3) Unlimited hop counts
4) Trigger updates for fast convergence
5) A loop-free topology using SPF algorithm
6) Run-on most routers
7) Classless protocol

There are some disadvantages of OSPF

1) It requires an extra CPU process to run the SPF algorithm
2) Requiring more RAM to store adjacency topology, and
3) Being more complex to set up and hard to troubleshoot

b) Configure DNS

DNS stands for Domain Name System. It is a fundamental part of the internet infrastructure and serves as a decentralized system for translating human-readable domain names into IP addresses, which are used by computers to identify each other on the internet.

When we type a website's domain name into your web browser (e.g., www.ismile.com), the DNS comes into play. The DNS acts as a phonebook for the internet, converting the domain name into the corresponding IP address (e.g., 192.0.2.1) that represents the actual location of the website's server on the internet.

Configuring server and client

Aim: Configure the following Servers using a suitable topology

a) Configure DHCP
b) Configure DNS
c) Configure HTTP
d) Configure Telnet
e) Configure FTP

a) Configure DHCP

DHCP, which stands for Dynamic Host Configuration Protocol, is a standardized network protocol used to automatically assign and manage IP addresses and other network configuration parameters to devices on a network. It is an essential component of most modern computer networks, including local area networks (LANs) and larger networks such as the Internet.

The primary purpose of DHCP is to simplify the process of configuring IP addresses and related network settings for devices, such as computers, smartphones, tablets, and other network-enabled devices. Without DHCP, network administrators would need to manually assign unique IP addresses to each device on the network, which could be time-consuming and prone to errors.

Configure SMTP, POP3, IMAP and MIME

SMTP (SIMPLE MAIL TRANSFER PROTOCOL)

The actual mail transfer is done through message transfer agents (MTAs). To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA. The formal protocol that defines the MTA client and server in the Internet is called **Simple Mail Transfer Protocol (SMTP).**
SMTP is used two times, between the sender and the sender's mail server and between the two mail servers. Another protocol is needed between the mail server and the receiver.
SMTP simply defines how commands and responses must be sent back and forth.

POP3 (POST OFFICE PROTOCOL)

Post Office Protocol, version 3 (POP3) is simple and limited in functionality. The client POP3 software is installed on the recipient computer; the server POP3 software is installed on the mail server. Mail access starts with the client when the user needs to download its e-mail from the mailbox on the mail server. The client opens a connection to the server on TCP port 110. It then sends its user name and password to access the mailbox. The user can then list and retrieve the mail messages, one by one

IMAP4 (Internet Mail Access Protocol)

Another mail access protocol is **IMAP4.** IMAP4 is similar to POP3, but it has more features; IMAP4 is more powerful and more complex. POP3 is deficient in several ways. It does not allow the user to organize her mail on the server; the user cannot have different folders on the server. In addition, POP3 does not allow the user to partially check the contents of the mail before downloading. IMAP4 provides some extra functions as compared to POP3 which are as follows

1) A user can search the contents of the e-mail for a specific string of characters prior to downloading.
2) A user can partially download e-mail. This is especially useful if bandwidth is limited and the e-mail contains multimedia with high bandwidth requirements.
3) A user can create, delete, or rename mailboxes on the mail server.