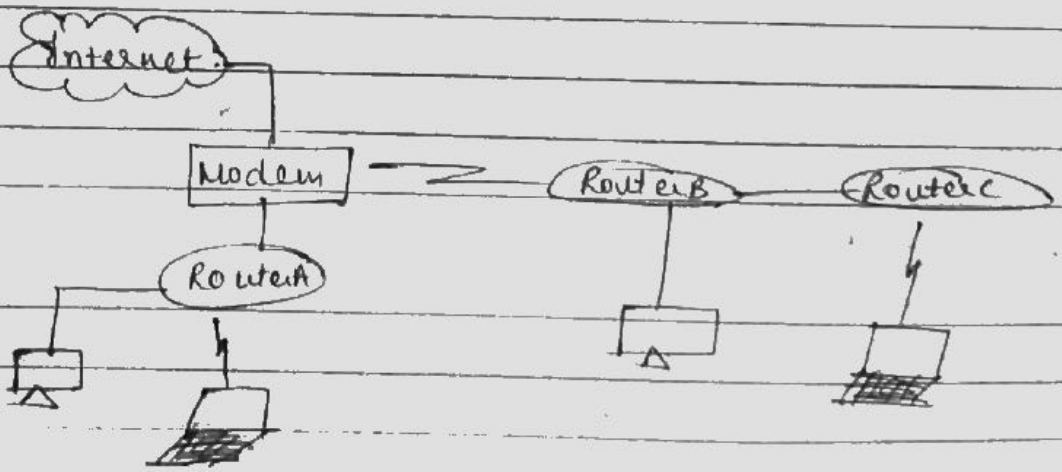
NRA Unit 4

4.1. Routers:

→ When a device in a LAN needs to communicate with a device on another LAN, it must send that traffic to a specialized device connected to LAN called Router.
→ The purpose of router is to find the best path for the message.
→ In order to allow billions of devices to find each other, routers need to regularly communicate among themselves.
→ The routers work together to determine the best paths for the message packet.
→ Each router port is configured with a specific protocol that is associated with that port's function.
→ Router is designed to recieve, analyze and forward data packets b/w computer networks.
→ It examines the destination IP address and uses headers and forwarding tables to decide the best way.
→ It is used in LAN & WAN enviornments.
→ It shares information with other routers in Networking.
→ It is more expensive than switches / hubs, etc.
→ It works on third layer of OSI model.
→ It is known as an intelligent device.
→ It allows users to configure ports as per requirements.
→ It uses a modem to allow communication between other devices.



(*) Application of Routers:

→ Used to connect Hardware equipment with remote location n/ws
→ Supports fast rate of data transmission.
→ Can send data all over the world with the help of IP address of destination.
→ It can be configured in a way that it allows access to other users for some data only which is defined for them.
→ Also used for WAN communications.

(*) - Types of Routers:

① Wireless Routers: → Used to offer wifi connectivity to laptops, smartphones, etc.
→ Capable of generating wireless signals.
→ If the connection is indoor, the range is about 150 ft and when the connection is outdoor, the range is up to 300 ft.
→ It can be secured with the help of passwords.

② Brouter: → It is the combination of a bridge and a router.
→ Allows transferring the data b/w n/ws like a bridge.
→ It can route data within a n/w.
→ It routes the incoming data to correct systems and transfer the other data to another n/w.

③ Core router: → Routes the data within a n/w.
→ Not able to route data between the networks.
→ Helps to link all network devices.
→ Provides various types of fast and powerful data communication interfaces.

④ Edge Router: → lower capacity device that is placed at the boundary of a n/w.
→ Allows internal n/w to connect with external n/ws.
→ Also called access routers.

→ It uses BGP to provide connectivity.
→ Two types: ⓐ. Subscriber edge Router: belongs to end-user organization
ⓑ. Label edge Router: Acts as a gateway b/w LAN, WAN or the Internet.

③. Broadband Routers: → Mainly used to provide high speed internet access to computers.
→ Needed when you connect to internet through phone and use voice over IP.
→ They have the option of 3 or 4 ethernet ports for connecting laptop and desktop systems.

(*). Benefits of Router:
(a). Security.
(b). Performance enhancement.
(c). Reliability: If the n/w gets down or there is a defect in the cable, other n/ws will not get affected.
(d). Networking Range: The physical range can be as per the requirement of a particular installation.

(*). Routing protocols:
(a). OSPF
(b). BGP
(c). IGRP
(d). EIGRP
(e). EGP
(f). RIP.

(*). Bridge

① Used to connect 2 LANs.
② It only connects 2 LAN segments.
③ Transfers data in the form of frames.
④ Sends data based on MAC address of device.
⑤ Has only one port.
⑥ Does not use any table to forward data.

Router

① Sends data from one N/w to another N/w.
② Capable of connecting LAN & WAN.
③ Transfers data in the form of packets.
④ Sends data based on IP Address of device.
⑤ Has several ports.
⑥ Uses a routing table to send data.

(*). Routing Table:

→ It determines the path for a given packet with the help of IP address of device.
→ The info. of Routing tables is stored in RAM of routers.
→ Routing table contains following entities:
(a). IP address of all the routers.
(b). Includes extrovert interface information.
(c). IP address and subnet mask of destination host.
→ Network Element in a router:

(a). Control Plane ↓

CP logic eliminates unnecessary directives from the table and constructs a forwarding information

(b). forwarding Plane.

forwards the data packet to correct N/w type. Also called user plane or data plane.

→ Routing tables is a set of rules that is used to determine where data packets are travelling over an IP N/w.

Entries of Routing Table: Each packet contains information about its origin and destination. Each entry consists of.

(a). Network ID
(b). Subnet Mask: Mask that is used to match destination IP & Network ID not
(c). Next Hop: IP address to which packet is forwarded
(d). Outgoing Interface
(e). Metric: Indicates minimum no. of hops.

→ Ways to maintain a routing table:
(a) Directly connected nlws are added automatically.
(b). Using static Routing.
(c). Using Dynamic Routing. → devices maintain their routing tables automatically using routing Protocols.

(+). Routing Information Protocol (RIP)

→ Dynamic Routing Protocol.
→ Uses Hop count as a routing metric to find best path.
→ It is a distance vector routing protocol.
→ Administrative Distance (AD) value is 120.
→ Works on application layer of OSI Model.
→ Uses port number 520.
(*). Hop count → No. of routers occuring b/w source & destination.
→ Path with lowest hop count is considered to be the best path.
→ RIP prevents routing loops by limiting the number of hops allowed in path from source to destination.
→ Max. hop count allowed for RIP is 15. Hop count of 16 means network unreachable.

(*) Features of RIP:
→ Updates of nlw are exchanged periodically.
→ Updates are always broadcasted.
→ Full routing tables are sent in updates.
→ Routers always trust on routing information received by neighbour routers. Also known as Routing on Rumours.

(*) RIP Version: 3 versions:

(a) RIP version 1: → Sends update as broadcast.
→ Broadcasts at 255.255.255.255
→ Doesn't support authentication of update messages.
→ Classful Routing Protocol.
→ Doesn't send information of subnet mask in its routing ~~tett~~ update.
→ Intradomain based on distance vector Routing.

(b) RIP version 2: → Sends update as multicast.
→ Multicasts at 224.0.0.9
→ Supports authentication of RIP V_2 update messages.
→ Classless protocol, supports classful.

(c) RIP Version 3: → Sends updates as multicast.
→ Multicasts at FF02::9
→ Classless updates are sent.

(*) RIP timers:
(a) Update timer: default time is 30 sec. Routers exchange their routing table periodically every 30 sec..
(b) Invalid timer: If no update come till 180 sec, the destination router considers it as invalid. The destination Router marks hop count 16 in this case.

c. Hold down timer: The time for which the router waits for the neighbour router to respond. If the router doesn't respond within a given time, it is declared dead. It is 180 sec. by default.

d. Flush timer: 60 sec by default. The time after which the entry of the route will be flushed if it doesn't respond within the flush time.

Q. RIP V1

→ Open standard protocol. Classful Routing Protocol, works on most of the router.
→ AD value is 120 which means that it is not reliable.
→ Lesser AD value, reliability is much more.
→ Max hop count is 15. Max routers in the n/w will be 16
→ When there will be same no. of hops to reach destination, the router will perform load balancing. (Load balancing means that if there are 3 paths with same no. of routers, packets will be sent to each path to reduce traffic.)
→ Slowest protocol.
→ Whenever link breaks, RIP traces another path.

Advantages:

→ Easy to configure, static routers are complex.
→ Less overhead
→ No complexity.

Disadvantages:

→ High bandwidth utilization.
→ It works only on hop count
→ It is not scalable. If there is a requirement of more than 15 routers, then it would be a problem.
→ Convergence is slow, wastes a lot of time in finding alternate path.

(*) RIP V2

→ Supports classless Inter-Domain Routing. It does subnetting & multicasting
→ metric = hop count (max 15)

Advantages:
→ It is a standardized protocol.
→ It is VLSM compliant.
→ Provides fast convergence.
→ Sends triggered updates.
→ Works with snapshot routing - making it ideal for dial networks.

Disadvantages:
→ Max hop count of 15.
→ NO concept of neighbours.
→ Exchanges entire table with all neighbours every 30 sec.

RIP V1	RIP V2
① Uses classful routing	① Classless protocol. Supports VLSM, CIDR, etc.
② Updates are broadcasted	② Updates are multicasted.
③ Older, no longer much used	③ Useful in small nws or at the edge of large nws.
④ Has no authentication	④ Supports authentication.

(*) EIGRP

→ Dynamic Routing Protocol. Performs same function as Static R.P. does.
→ Enhanced Interior Gateway Routing Protocol
→ used to find best path between any two layer 3 devices to deliver packet.
→ Works on nw layer of OSI model.
→ AD values: Summary Routes → 5
Internal Routes → 90
External Routes → 170

→ EIGRP messages:

● Hello Message: → Keep alive messages which are exchanged b/w 2 devices operating EIGRP.
→ These messages are used for neighbours discovery / recovery (multicast)
→ Used as acknowledgement when multicast. A hello with no data is used as acknowledgement.

② · NULL update → Used to calculate Smooth Round Trip Timer and Retransmission time out (RTO).
→ SRTT: time taken for a packet to reach neighbouring router and acknowledgement of packet.
→ RTO: RTO is the timer for which the local router waits for Acknowledgement.

③ · FULL Update - After exchanging Hello messages, these messages are exchanged. They contain best routes.

④ · Partial update - These messages are exchanged when there is topology change and new links are added. It contains only new routes, not all routes.

⑤ · Query Message: → Message is multicast when the device is declared dead.

⑥ · Reply Message → Acknowledgement of Query messages.

⑦ · ACKNOWLEDGEMENT message: → Used to acknowledge EIGRP update, queries & replies. Hello packets that do not contain data.

→ Composite Matrix: EIGRP composite metric can use upto 5 variables, but only 2 are used by default (K1 and K3). Composite metric values are:
K1 (bandwidth)
K2 (load)
K3 (delay)
K4 (Reliability)
K5 (MTU)
The lowest value are considered in the composite matrix in order to calculate the cost.

* To perform EIGRP neighbourship:
(a) K values should match.
(b) Autonomous System number should match.
(c) Authentication should match.
(d) Subnet mask should be same.

(*) Timers: default
→ Hello timer: The interval in which EIGRP sends hello message. - 5 sec. by
→ Dead timer: The interval in which neighbour will be declared dead if no hello packet is received. 15 sec. by default.

(*) Features of EIGRP:
(a) Rapid Convergence: If a route to a nw goes down, then another route can be used.
(b) Reduced bandwidth usage: Doesn't send periodic updates. EIGRP uses partial updates if there is any change in topology.
(c) Supports all LAN & WAN data link protocols & topologies.
(d) Supports auto-summary: allows Routing Protocols to summarize its routes to their classful nws automatically.
(e) Supports unequal cost load balancing: by changing value of variance. In case of equal LB, value is 1, we can change it for unequal LB.
(f) Communication via RTP (Reliable Transfer Protocol):
(g) Best path selection using DUAL (Diffusing Update Algorithm).

It mainly maintains 3 tables, namely: (after establishing connection)
(a) Neighbour table → contains info of neighbour routers
(b) Topology table → contains all the routes available to a nw.
(c) Routing table → contains all the routes which are being used to make current routing decisions.
(d) Traffic control:

⑩. It supports VLSM.
⑪. Support for both IPV4 and IPV6.

IGRP	EIGRP
①. Interior Gateway R.P	①. Enhanced Interior Gateway RP.
②. Classful routing.	②. Classless routing.
③. Slow convergence	③. fast convergence.
④. Bellman ford Algo is used.	④. DUAL algo is used.
⑤. Needs more/high bandwidth.	⑤. Needs less/low bandwidth.
⑥. Hop count is 255 (least).	⑥. Hop count is 256 (least)
⑦. provides 24 bits for delay.	⑦. 32 bits for delay.

* OSPF (Open shortest path first)
→ It is a link state Routing Protocol used to find best path bet source and destination router.
→ The whole routing table is not exchanged.
→ Nlw layer protocol.
→ AD value 110.
To form neighbourship,
(a). It should be present in same area.
(b). Router ID must be unique.
(c). Subnet mask should be same.
(d). Hello & dead timer should be same.
(e). Stub flag must match.
(f). Authentication must match.

(*) OSPF messages:
(a). Hello Message → Keep alive messages used for neighbour discovery/recovery. Exchanged every 10 sec.

(b). Database Description (DBD): Contains topology of an AS or an area.
(c) Link-state Request (LSR): When a router receives DBD, it compares with its own DBD. If the DBD received has some more updates, then LSR is being sent to its neighbour.
(d). Link State Update (LSU) → when a router receives LSR, it responds with LSU.
(e) Link State Acknowledgement: Provides reliability to link state exchange process. Sent as Acknowledgement of LSU.
(f). Link State Advertisement: An OSPF data packet that contains info shared only with the routers to which Adjacency has been formed.

Timers

(a). Hello Timer: Interval in which OSPF sends Hello message. 10 sec default.
(b) Dead Timer: Interval in which neighbour will be declared dead if it is not able to send hello packet. 40 sec. by default.

Advantages:

→ supports both IPV4 and IPV6 routed protocols.
→ Provides load balancing with equal cost routes for same destination.
→ supports VLSM and Route summarization.
→ Provides unlimited hop counts.
→ Provides triggered updates for fast convergence.
→ Provides a loop free topology using SPF algo.
→ Runs on most Routers.
→ Classless protocol.

Disadvantages → Requires extra CPU process to run SPF algo, Requires more RAM, more complex setup, hard to troubleshoot.

OSPF terms:

(a). Router id: Highest active IP address present on router. (First highest loopback address is considered. If not, then Highest Active IP).

(b). Router Priority: 8 bit value assigned to a router operating ospf. not

(c). Designated Router (DR): Elected to minimize the no. of adjacency formed. It is the router having highest priority.

(d). Backup Designated Router (BDR): Back up to DR in a broadcast ing nlw. When DR goes down, BDR becomes DR and performs its functions.

→ If there is a tie in router priority, then Router ID will be considered. (First the highest loopback address).

OSPF states:

(a) Down - No Hello packets have been received.

(b). INIT - Hello packets have been received from other router.

(c). 2WAY - Both routers have received hello packets from other routers. Bidirectional connectivity has been established.

(d). Exsart - NULL DBD are exchanged. Master and slave election takes place.

(e). Exchange - Actual DBDs are exchanged.

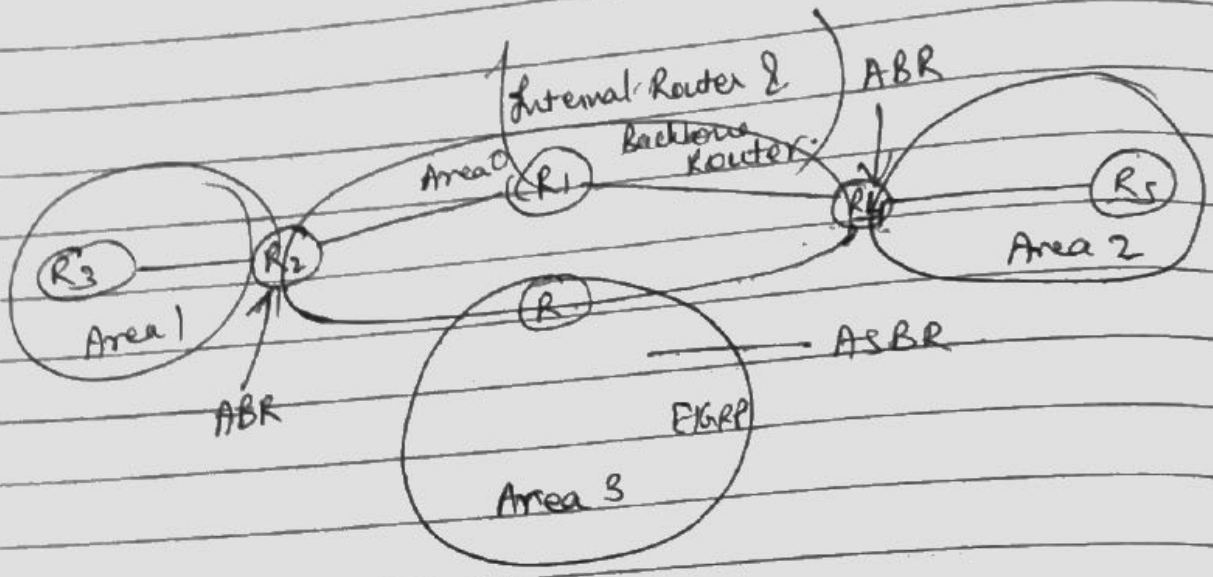
(f). Loading - LSR, LSU and LSA are exchanged.

(g). Full → Synchronization of all info takes place. OSPF routing can begin only after full state.

OSPF router roles:

(1). Backbone Routers: Area 0 is known as backbone area and routers in area 0 are backbone Routers. If routers exist partially in area 0, then also it is a backbone Router.

② Internal Router: Has all of its interfaces in a single area.
③ Area Boundary Router (ABR): Connects backbone area with other area. It belongs to more than 1 area.
④ Area summary Border Router (ASBR): When OSPF router is connected to different protocol like EIGRP, or BGP, then it is known as AS. The router which connects two AS is known as ASBR. These routers perform redistribution.



(*) Integrated IS-IS:
→ Routers are referred to as ~~Integrated~~ Intermediate Systems. Thus, Intermediate Systems to Intermediate Systems means router to router.
→ IS-IS runs directly over layer 2 protocols.
→ Provides traffic engineering capabilities (extended).

Key features:

→ Areas: Provides 2 level n/w hierarchy. Routers in backbone area are called L2 routers and Internal routers are called L1 router. A router is entirely within an area, unlike OSPF where routers can sit on the borders b/w two areas.
→ Addressing in IS-IS: Addressing is based on OSI-NSAP addres

IS-IS for IP networks uses NET addressing.

→ PSEUDONODES And NONPSEUDONODES: IS-IS allows handling of different ntw types. A broadcast ntw is treated as a pseudonode, where one of the routers serve as the pseudonode. For links that are not for broadcast ntws but are for point-to-point ntws a pseudonode is created.

→ SHORTEST PATH CALCULATION: Based on Dijkstra's Algorithm. Once the router receives a new LSP, it waits for 5 sec. before running shortest path calculation. There is a 10 sec. Hold down timer.

IS-IS defines defines four categories of protocol packets / protocol Data units (PDUs):

(a) Hello packet
(b) Link State PDUs (LSP)
(c) Complete sequence number PDUs (CSNP)
(d) partial sequence number PDUs (PSNP)

Similarities b/w IS-IS and OSPF:

→ Both provide ntw hierarchy through two level areas.
→ Both use Hello packets to establish connection & ~~maintain~~ continue & maintain them.
→ Both have the ability to do address summarization b/w areas.
→ Both maintain link state database, shortest path computation using Dijkstra's Algo.
→ Both have the provision to elect a designated Router for representing a broadcast n/w.

Differences b/w IS-IS and OSPF:

→ In OSPF an area border routers can sit on the boundary while in ISIS, router has to be inside the area.

→ OSPF packets are encapsulated in IP datagrams, IS-IS packets are directly encapsulated in link layer frames.
→ OSPF dimensionless link metric value is in b/w 1 to 65535
IS-IS metric value ranges 0-63 (narrow metric), which has been extended to 0-16777215 (wide metric).
→ IS-IS safer than OSPF.
→ IS-IS keepalives can be used for MTU Detection.
→ IS-IS allows overload declaration.

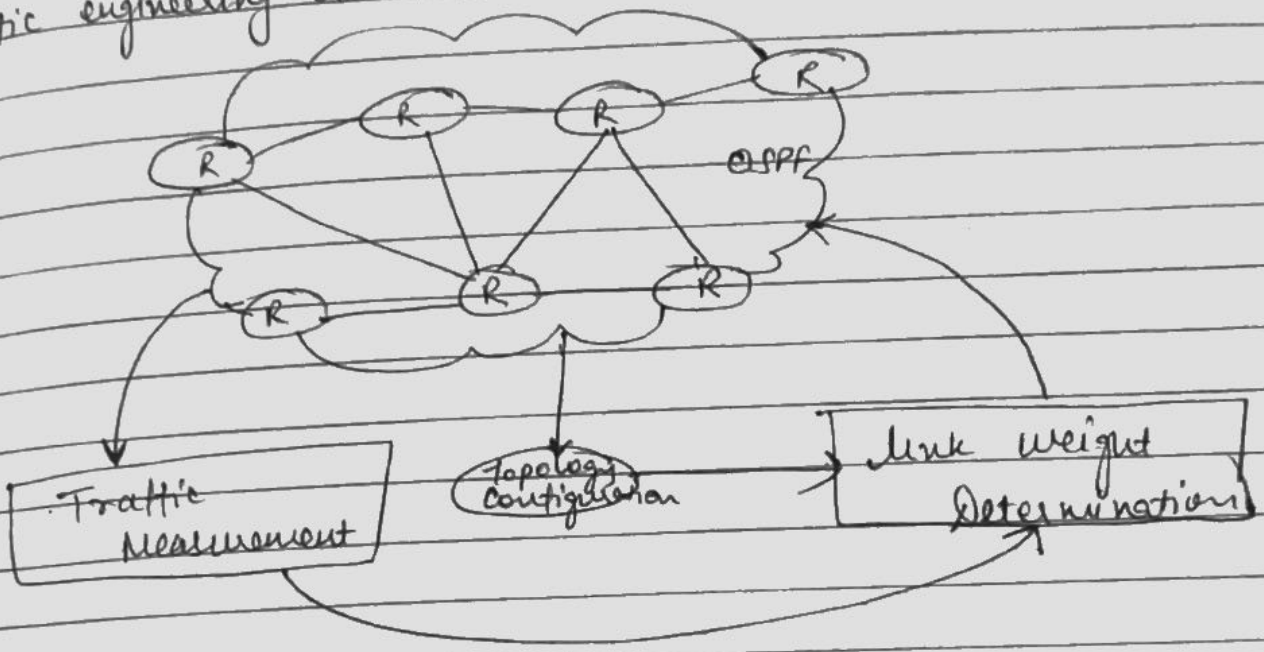
(*). IP Traffic Engineering: Traffic, stochasticity, delay & Utilization

IP N/w Traffic:
→ An IP n/w provides many services such as web & email.
→ In current IP n/w the predominant traffic is due to applications that use TCP for transport layer.
→ On a backbone link, approximately 90% of the traffic is TCP based
→ A message content created by applications is broken into smaller TCP pieces, called TCP segments by including TCP header Information
→ Traffic in an IP n/w is IP datagrams generated by various applications, without wondering which among the applications it is for.

(b) Traffic Engineering: An Architectural Framework:

→ Since a n/w consists of a number of routers it is important to estimate source-destination traffic volume to obtain a traffic matrix that can be used for traffic engineering.

→ Traffic engineering occurs outside the actual n/w.



→ From the actual n/w, traffic measurements are collected to estimate traffic matrix.

→ topology and configuration are also obtained from the n/w.

→ Based on topology and configuration & traffic matrix, a link weight determination process determines link weights.

→ The computed link weight is injected into the n/w.

→ Each router receives metrics for its outgoing link through this external process.

→ Once the router receives link metrics, it then spreads the information.

→ This means that if no new link weights are obtained from the traffic engineering system, the router will generate a new LSA by continuing to use the previous link metric value.