Routers

When a device in a Local Area Network needs to communicate with a device on another LAN, it must send that traffic to a specialized device connected to the LAN called a “router” whose purpose is to find the best path for the message to take to arrive at the intended target device, and to send the message along its way following that path.

In order to allow the billions of devices on the Internet to find each other, routers regularly need to communicate among themselves using protocols that enable them to share routing information so that, when a device needs to send a communication message to a target device, the routers work together to determine the best path for the message packet to use to arrive at the intended target device.

Each router port is configured with a specific routing protocol that is associated with that port's function. For example, a router port that connects to the Internet must learn how to efficiently route communication messages to destinations around the world. Protocols that facilitate this are called "gateway routing protocols" and have names such as the Border Gateway Protocol ("BGP") or Exterior Gateway Protocol ("EGP"). A router port that connects to an organization's internal networks must learn the how the organization's network is configured to efficiently route traffic throughout the organization. Protocols that serve this purpose are called "interior routing protocols" and have names such as Enhanced Interior Gateway Routing Protocol ("EIGRP"), Interior Gateway Routing Protocol ("IGRP"), Open Shortest Path First ("OSPF"), Routing Information Protocol I and II ("RIP"/"RIP II").

The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets. There are some popular companies that develop routers; such are **Cisco**, **3Com**, **HP**, **Juniper**, **D-Link**, **Nortel**, etc. Some important points of routers are given below:

- A router is used in **LAN** (Local Area Network) and **WAN** (Wide Area Network) environments. For example, it is used in **offices** for connectivity, and you can also establish the connection between distant networks such as from **Bhopal** to delhi.
- It shares information with other routers in networking.
- It uses the routing protocol to transfer the data across a network.
- Furthermore, it is more **expensive** than other networking devices like switches and hubs.

A router works on the **third layer** of the OSI model, and it is based on the IP address of a computer. It uses protocols such as ICMP to communicate between two or more networks. *It is also known as an **intelligent device** as it can calculate the best route to pass the network packets from source to the destination automatically.*

A virtual router is a software function or software-based framework that performs the same functions as a physical router. It may be used to increase the reliability of the network by virtual router redundancy protocol, which is done by configuring a virtual router as a default gateway. A virtual router runs on commodity servers, and it is packaged with alone or other network functions, like load balancing, firewall packet filtering, and wide area network optimization capabilities.

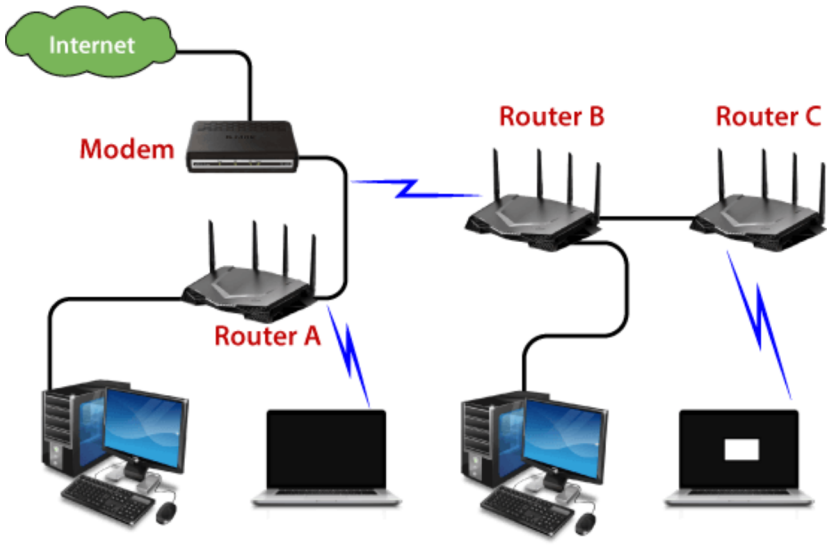
Why Routers?

A router is more capable as compared to other network devices, such as a hub, switch, etc., as these devices are only able to execute the basic functions of the network. For example, a hub is a basic networking device that is mainly used to forward the data between connected devices, but it cannot analyze or change anything with the transferring data. On the other hand, the router has the capability to analyze and modify the data while transferring it over a network, and it can send it to another network. For example, generally, routers allow sharing a single network connection between multiple devices.

How does Router work?

A router analyzes a destination IP address of a given packet header and compares it with the routing table to decide the packet's next path. The list of routing tables provides directions to transfer the data to a particular network destination. They have a set of rules that compute the best path to forward the data to the given IP address.

Routers use a **modem** such as a cable, fiber, or DSL modem to allow communication between other devices and the internet. Most of the routers have several ports to connect different devices to the internet at the same time. It uses the **routing tables** to determine where to send data and from where the traffic is coming.



A routing table mainly defines the default path used by the router. So, it may fail to find the best way to forward the data for a given packet. For example, the office router along a single default path instructs all networks to its internet services provider.

There are two types of tables in the router that are **static and dynamic**. The static routing tables are configured manually, and the dynamic routing tables are updated automatically by dynamic routers based on network activity.

Features of Router

- A router works on the 3rd layer (Network Layer) of the OSI model, and it is able to communicate with its adjacent devices with the help of IP addresses and subnet.
- A router provides high-speed internet connectivity with the different types of ports like gigabit, fast-Ethernet, and STM link port.
- It allows the users to configure the port as per their requirements in the network.
- Routers' main components are central processing unit (CPU), flash memory, RAM, Non-Volatile RAM, console, network, and interface card.
- Routers are capable of routing the traffic in a large networking system by considering the sub-network as an intact network.
- Routers filter out the unwanted interference, as well as carry out the data encapsulation and decapsulation process.
- Routers provide the redundancy as it always works in master and slave mode.
- It allows the users to connect several LAN and WAN.
- Furthermore, a router creates various paths to forward the data.

Applications of Routers

There are various areas where a router is used:

- Routers are used to connect hardware equipment with remote location networks like **BSC, MGW, IN, SGSN**, and other servers.
- It provides support for a fast rate of data transmission because it uses high STM links for connectivity; that's why it is used in both wired or wireless communication.
- Internet service providers widely use routers to send the data from source to destination in the form of e-mail, a web page, image, voice, or a video file. Furthermore, it can send data all over the world with the help of an IP address of the destination.
- Routers offer access restrictions. It can be configured in a way that allows for few users to access the overall data and allows others to access the few data only, which is defined for them.
- Routers are also used by software testers for WAN communications. For example, the software manager of an organization is located in Agra, and its executive is located at a different place like Pune or Bangalore. Then the router provides the executive the method to share his software tools and other applications with the manager with the help of routers by connecting their PCs to the router using WAN architecture.
- In wireless networks, by configuring VPN in routers, it can be used in the client-server model, which allows sharing the internet, video, data, voice, and hardware resources. As shown in the below picture:

In modern times, routers have the facility of inbuilt USB ports within the hardware. They have enough internal storage capacity. External storage devices can be used with routers to store and share data.

- Routers are used to set up the operation and maintenance center of an organization, which is known as the NOC center. All equipment at a distant location are connected by routers on optical cable at a central location, which also offer redundancy through the main link and protection link topology.

Types of Routers

There are various types of routers in networking; such are given below:

1. Wireless Router: Wireless routers are used to offer Wi-Fi connectivity to laptops, smartphones, and other devices with Wi-Fi network capabilities, and it can also provide standard ethernet routing for a small number of wired network systems.

Wireless routers are capable of generating a wireless signal in your home or office, and it allows the computers to connect with routers within a range, and use the internet. If the connection is indoors, the range of the wireless router is about 150 feet, and when the connection is outdoors, then its range is up to 300 feet.

Furthermore, you can make more secure wireless routers with a password or get your IP address. Thereafter, you can log in to your router by using a user ID and password that will come with your router.

2. Brouter: A brouter is a combination of the bridge and a router. It allows transferring the data between networks like a bridge. And like a router, it can also route the data within a network to the individual systems. Thus, it combines these two functions of bridge and router by routing some incoming data to the correct systems while transferring the other data to another network.

3. Core router: A core router is a type of router that can route the data within a network, but it is not able to route the data between the networks. It is a computer communication system device and the backbone of networks, as it helps to link all network devices. It is used by internet service providers (ISPs), and it also provides various types of fast and powerful data communication interfaces.

4. Edge router: An edge router is a lower-capacity device that is placed at the boundary of a network. It allows an internal network to connect with the external networks. It is also called as an access router. It uses an External BGP (Border Gateway Protocol) to provides connectivity with remote networks over the internet.

There are two types of edge routers in networking:

- **Subscriber edge router**
- **Label edge router**

The **subscriber edge router** belongs to an end-user organization, and it works in a situation where it acts on a border device.

The **label edge router** is used in the boundary of Multiprotocol Label Switching (MPLS) networks. It acts as a gateway between the LAN, WAN, or the internet.

5. Broadband routers: Broadband routers are mainly used to provide high-speed internet access to computers. It is needed when you connect to the internet through phone and use voice over IP technology (VOIP).

All broadband routers have the option of three or four Ethernet ports for connecting the laptop and desktop systems. A broadband router is configured and provided by the internet service provider (ISP). It is also known as a **broadband modem**, asymmetric digital subscriber line (**ADSL**), or digital subscriber line (**DSL**) modem.

Benefits of Router

There are so many benefits of a router, which are given below:

- **Security:** Router provides the security, as LANs work in broadcast mode. The information is transmitted over the network and traverses the entire cable system. Although the data is available to each station, but the station which is specifically addressed reads the data.
- **Performance enhancement:** It enhances the performance within the individual network. For example, if a network has 14 workstations, and all generate approximately the same volume of traffic. The traffic of 14 workstations runs through the same cable in a single

network. But if the network is divided into two sub-networks each with 7 workstations, then a load of traffic is reduced to half. As each of the networks has its own servers and hard disk, so fewer PCs will need the network cabling system.

- **Reliability:** Routers provide reliability. If one network gets down when the server has stopped, or there is a defect in the cable, then the router services, and other networks will not be affected. The routers separate the affected network, whereas the unaffected networks remain connected, without interrupting the work and any data loss.
- **Networking Range:** In networking, a cable is used to connect the devices, but its length cannot exceed 1000 meters. A router can overcome this limitation by performing the function of a repeater (Regenerating the signals). The physical range can be as per the requirement of a particular installation, as long as a router is installed before the maximum cable range exceeds.

Routing Protocols

Routing protocols specify a way for the router to identify other routers on the network and make dynamic decisions to send all network messages. There are several protocols, which are given below:

Open Shortest Path First (OSPF): It is used to calculate the best route for the given packets to reach the destination, as they move via a set of connected networks. It is identified by the Internet Engineering Task Force **(IETF)** as Interior Gateway Protocol.

Border Gateway Protocol (BGP): It helps manage how packets are routed on the internet via exchange of information between edge routers. It provides network stability for routers if one internet connection goes down while forwarding the packets, it can adapt another network connection quickly to send the packets.

Interior Gateway Routing Protocol (IGRP): It specifies how routing information will be exchanged between gateways within an independent network. Then, the other network protocols can use the routing information to determine how transmissions should be routed.

Enhanced Interior Gateway Routing Protocol (EIGRP): In this protocol, if a router is unable to find a path to a destination from the tables, it asks route to its neighbors, and they pass the query to their neighbors until a router has found the path. When the entry of routing table changes in one of the routers, it informs its neighbors only about the changes, but do not send the entire table.

Exterior Gateway Protocol (EGP): It decides how routing information can be exchanged between two neighbor gateway hosts, each of which has its own router. Additionally, it is commonly used to exchange routing table information between hosts on the internet.

Routing Information Protocol (RIP): It determines how routers can share information while transferring traffic among connected group of local area networks. The maximum number of hops that can be allowed for RIP is 15, which restricts the size of networks that RIP can support.

Difference between Bridge and Router

Bridge	Router
A bridge is a networking device that is used to connect two local area networks (LANs) by using media access control addresses and transmit the data between	A router is also a networking device that sends the data from one network to another network with the help of their IP addresses.

them.	
A bridge is able to connect only two different LAN segments.	A router is capable of connecting the LAN and WAN.
A bridge transfers the data in the form of frames.	A router transfers the data in the form of packets.
It sends data based on the MAC address of a device.	It sends data based on the IP address of a device.
The bridge has only one port to connect the device.	The router has several ports to connect the devices.
The bridge does not use any table to forward the data.	The router uses a routing table to send the data.

What is Routing Table in Router?

A routing table determines the path for a given packet with the help of an IP address of a device and necessary information from the table and sends the packet to the destination network. The routers have the internal memory that is known as Random Access Memory (RAM). All the information of the routing table is stored in RAM of routers.

For example:

Destination (Network ID)	Subnet mask	Interface
200.1.2.0	255.255.255.0	Eth0
200.1.2.64	255.255.255.128	Eth1
200.1.2.128	255.255.255.255	Eth2
Default		Eth3

A routing table contains the following entities:

- It contains an IP address of all routers which are required to decide the way to reach the destination network.
- It includes extrovert interface information.
- Furthermore, it is also contained IP addresses and subnet mask of the destination host.

Network Element in Router

There are two types of a network element in the router which are as follows:

Control plane: A router supports a routing table that determines which path and physical interface connection should be used to send the packet. It is done by using internal pre-configured directives, which are called static routes, or by learning routes with the help of routing protocol. A routing table stores the static and dynamic routes. Then the control-plane

logic eliminates the unnecessary directives from the table and constructs a forwarding information base that is used by the forwarding plane.

Forwarding plane: A router sends data packets between incoming and outgoing interface connections. It uses information stored in the packet header and matches it to entries in the FIB, which is supplied by the control plane; accordingly, it forwards the data packet to the correct network type. It is also called the user plane or data plane.

Routing Tables

A routing table is a set of rules, often viewed in table format, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables. See below a Routing Table:

Destination	Subnet mask	Interface
128.75.43.0	255.255.255.0	Eth0
128.75.43.0	255.255.255.128	Eth1
192.12.17.5	255.255.255.255	Eth3
default		Eth2

The entry corresponding to the *default* gateway configuration is a network destination of 0.0.0.0 with a network mask (netmask) of 0.0.0.0. The Subnet Mask of default route is always 255.255.255.255 .

Entries of an IP Routing Table:

A routing table contains the information necessary to forward a packet along the best path toward its destination. Each packet contains information about its origin and destination. Routing Table provides the device with instructions for sending the packet to the next hop on its route across the network.

Each entry in the routing table consists of the following entries:

1. **Network ID:**
   The network ID or destination corresponding to the route.
2. **Subnet Mask:**
   The mask that is used to match a destination IP address to the network ID.
3. **Next Hop:**
   The IP address to which the packet is forwarded
4. **Outgoing Interface:**
   Outgoing interface the packet should go out to reach the destination network.
5. **Metric:**
   A common use of the metric is to indicate the *minimum number of hops* (routers crossed) to the network ID.

Routing table entries can be used to store the following types of routes:

- Directly Attached Network IDs
- Remote Network IDs
- Host Routes
- Default Route

- Destination

*When a router receives a packet, it examines the destination IP address, and looks up into its **Routing Table** to figure out which interface packet will be sent out.*

How are Routing Tables populated?

There are ways to maintain Routing Table:

- Directly connected networks are added automatically.
- Using Static Routing.
- Using Dynamic Routing.

These Routing tables can be maintained manually or dynamically. In *dynamic routing*, devices build and maintain their routing tables automatically by using routing protocols to exchange information about the surrounding network topology. Dynamic routing tables allow devices to "listen" to the network and respond to occurrences like device failures and network congestion. Tables for *static network devices* do not change unless a network administrator manually changes them.

Route Determination Process (finding Subnet ID using Routing Table):

Consider a network is subnetted into 4 subnets as shown in the above picture. The IP Address of the 4 subnets are:

200.1.2.0 (Subnet a)
200.1.2.64 (Subnet b)
200.1.2.128 (Subnet c)
200.1.2.192 (Subnet d)

Then, **Routing table** maintained by the internal router looks like:

Destination	Subnet Mask	Interface
200.1.2.0	255.255.255.192	a
200.1.2.64	255.255.255.192	b
200.1.2.128	255.255.255.192	c
200.1.2.192	255.255.255.192	d
Default	0.0.0.0	e

To find its right subnet (subnet ID), router performs the bitwise ANDing of destination IP Address mentioned on the data packet and all the subnet masks one by one.

- If there occurs only one match, router forwards the data packet on the corresponding interface.
- If there occurs more than one match, router forwards the data packet on the interface corresponding to the longest subnet mask.

- If there occurs no match, router forwards the data packet on the interface corresponding to the default entry.

Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance vector routing protocol which has AD value 120 and works on the application layer of OSI model. RIP uses port number 520.

Hop Count :

Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the number of hopes allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and hop count of 16 is considered as network unreachable.

Features of RIP :

1. Updates of the network are exchanged periodically.
2. Updates (routing information) are always broadcast.
3. Full routing tables are sent in updates.
4. Routers always trust on routing information received from neighbor routers. This is also known as *Routing on rumours*.

RIP versions :

There are three vesions of routing information protocol – **RIP Version1**, **RIP Version2** and **RIPng**.

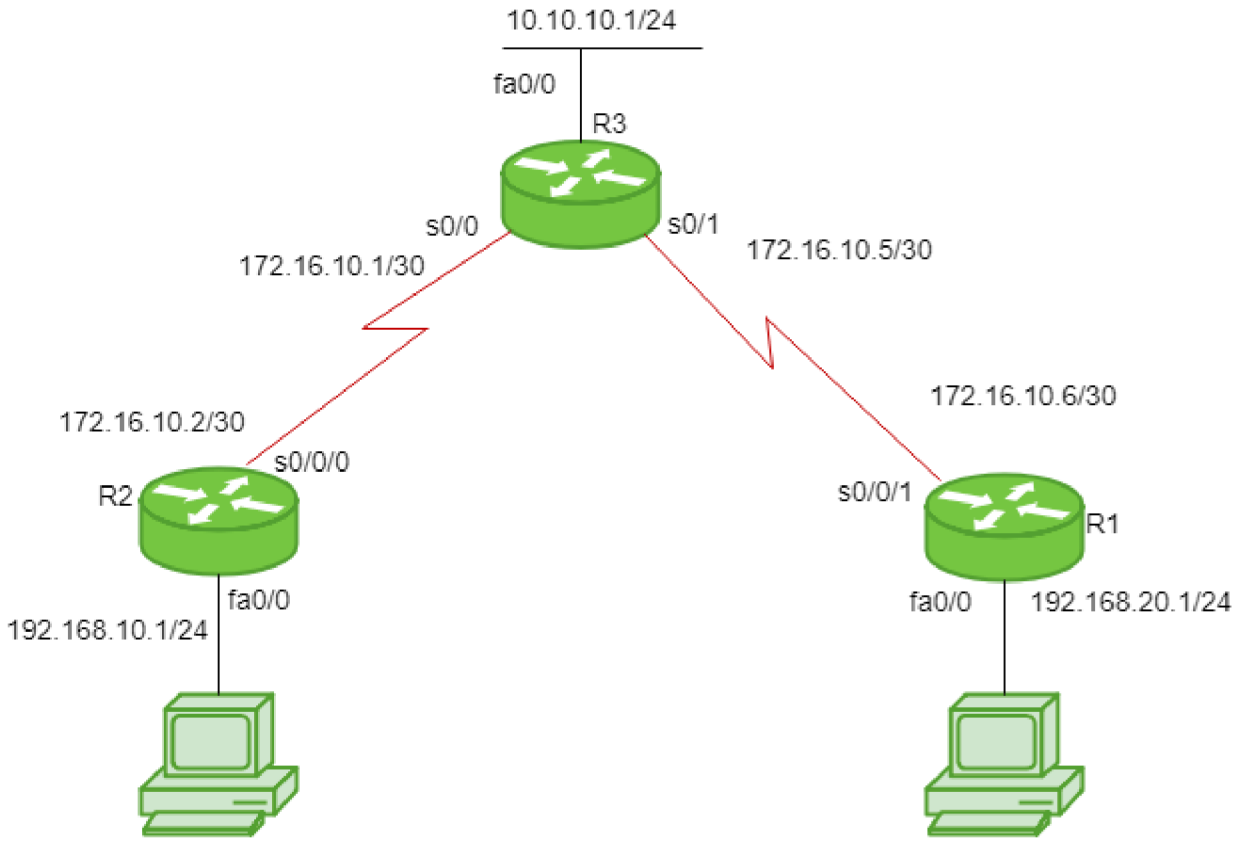
RIP v1	RIP v2	RIPng
Sends update as broadcast	Sends update as multicast	Sends update as multicast
Broadcast at 255.255.255.255	Multicast at 224.0.0.9	Multicast at FF02::9 (RIPng can only run on IPv6 networks)
Doesn't support authentication of update messages	Supports authentication of RIPv2 update messages	–
Classful routing protocol	Classless protocol, supports classful	Classless updates are sent

RIP v1 is known as *Classful* Routing Protocol because it doesn't send information of subnet mask in its routing update.

RIP v2 is known as *Classless* Routing Protocol because it sends information of subnet mask in its routing update.

>> Use debug command to get the details :
 # debug ip rip
>> Use this command to show all routes configured in router, say for router R1 :
***R1**# show ip route*
>> Use this command to show all protocols configured in router, say for router R1 :
***R1**# show ip protocols*

Configuration :



Consider the above given topology which has 3-routers R1, R2, R3. R1 has IP address 172.16.10.6/30 on s0/0/1, 192.168.20.1/24 on fa0/0. R2 has IP address 172.16.10.2/30 on s0/0/0, 192.168.10.1/24 on fa0/0. R3 has IP address 172.16.10.5/30 on s0/1, 172.16.10.1/30 on s0/0, 10.10.10.1/24 on fa0/0.
Configure RIP for R1 :
R1(config)# router rip
R1(config-router)# network 192.168.20.0
R1(config-router)# network 172.16.10.4
R1(config-router)# version 2
R1(config-router)# no auto-summary
Note : no auto-summary command disables the auto-summarisation. If we don't select no auto-summary, then subnet mask will be considered as classful in Version 1.
Configureg RIP for R2 :
R2(config)# router rip
R2(config-router)# network 192.168.10.0

R2(config-router)# network 172.16.10.0
R2(config-router)# version 2
R2(config-router)# no auto-summary
Similarly, Configure RIP for R3 :
R3(config)# router rip
R3(config-router)# network 10.10.10.0
R3(config-router)# network 172.16.10.4
R3(config-router)# network 172.16.10.0
R3(config-router)# version 2
R3(config-router)# no auto-summary

RIP timers :

- **Update timer :** The default timing for routing information being exchanged by the routers operating RIP is 30 seconds. Using Update timer, the routers exchange their routing table periodically.
- **Invalid timer:** If no update comes until 180 seconds, then the destination router consider it as invalid. In this scenario, the destination router mark hop count as 16 for that router.
- **Hold down timer :** This is the time for which the router waits for neighbour router to respond. If the router isn't able to respond within a given time then it is declared dead. It is 180 seconds by default.
- **Flush time :** It is the time after which the entry of the route will be flushed if it doesn't respond within the flush time. It is 60 seconds by default. This timer starts after the route has been declared invalid and after 60 seconds i.e time will be 180 + 60 = 240 seconds.

Note that all these times are adjustable. Use this command to change the timers :
R1(config-router)# timers basic
R1(config-router)# timers basic 20 80 80 90

Routing Information Protocol (RIP) V1 & V2
Routing Information Protocol (RIP) protocol are the intradomain (interior) routing protocol which is based on distance vector routing and it is used inside an autonomous system.Routers and network links are called node. The first column of routing table is destination address. The cost of metric in this protocol is hop count which is number of network which need to be passed to reach destination. Here infinity is defined by a fixed number which is 16 it means that using a Rip, network cannot have more than 15 hops.
RIP Version-1:
It is an open standard protocol means it works on the various vendors routers. It works on most of the router, it is classful routing protocol. Updates are broadcasted. Its administrative distance value is 120, it means it is not reliable, The lesser the administrative distance value the reliability is much more. Its metric is hop count and max hop count is 15. There will be total 16 router in the network. When there will be the same number of hop to reach destination, Rip starts to perform load balancing. Load balancing means if there are three ways to reach the destination and each way has same number of routers then packets will be sent to each path to reach the destination. This reduces traffic and also the load is balanced. It is used in small companies, in this protocol routing tables are updated in each 30 sec. Whenever link breaks rip trace out another path to reach the destination. It is one of the slowest protocol.
Advantages of RIP ver1 –

1. Easy to configure, static router are complex.
2. Less overhead
3. No complexity.

Disadvantage of RIP ver1 –

1. Bandwidth utilization is very high as broadcast for every 30 seconds.
2. It works only on hop count.
3. It is not scalable as hop count is only 15. If there will be requirement of more routers in the network it would be a problem .
4. Convergence is very slow, wastes a lot of time in finding alternate path.

RIP Version-2:

Due to some deficiencies in the original RIP specification, RIP version 2 was developed in 1993. It supports classless Inter-Domain Routing (CIDR) and has ability to carry subnet information, its metric is also hop count and max hop count 15 is same as rip version 1. It support authentication and does subnetting and multicasting. Auto summary can be done on every router. In RIPv2 Subnet masks are included in the routing update. RIPv2 multicasts the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast (255.255.255.255).

Advantages of RIP ver2 –

1. It's a standardized protocol.
2. It's VLSM compliant.
3. Provides fast convergence.
4. It sends triggered updates when the network changes.
5. Works with snapshot routing – making it ideal for dial networks.

Disadvantage of RIP ver2 – There lies some disadvantages as well:

1. Max hopcount of 15, due to the 'count-to-infinity' vulnerability.
2. No concept of neighbours.
3. Exchanges entire table with all neighbours every 30 seconds (except in the case of a triggered update).

RIP ver1 versus RIP ver2:

RIP Ver1	RIP Ver2
RIP v1 uses what is known as classful routing	RIP v2 is a classless protocol and it supports variable-length subnet masking (VLSM), CIDR, and route summarization
RIPv1 routing updates are broadcasted	RIP v2 routing updates are multicasted
RIPv1 has no authentication	RIP v2 supports authentication
RIP v1 does not carry mask in updates	RIP v2 does carry mask in updates, so it supports for VLSM

RIP v1 is an older, no longer much used routing protocol	IP v2 can be useful in small, flat networks or at the edge of larger networks because of its simplicity in configuration and usage

EIGRP fundamentals

Dynamic routing Protocol performs the same function as static routing Protocol does. In dynamic routing Protocol, if the destination is unreachable then an another entry, in the routing table, to the same destination can be used. One of the routing Protocol is EIGRP.

EIGRP:

Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing Protocol which is used to find the best path between any two layer 3 device to deliver the packet. EIGRP works on network layer Protocol of osi model and uses the protocol number 88.It uses metric to find out best path between two layer 3 device (router or layer 3 switch) operating EIGRP. Administrative Distance for EIGRP are:-

EIGRP routes	**AD values**
Summary Routes	5
Internal Routes	90
external routes	170

It uses some messages to communicate with the neighbour devices that operates EIGRP. These are :-

1. **Hello message-**These messages are keep alive messages which are exchanged between two devices operating EIGRP. These messages are used for neighbour discovery/recovery, if there is any device operating EIGRP or if any device(operating EIGRP) coming up again. These messages are used for neighbor discovery if multicast at 224.0.0.10. It contains values like AS number, k values etc.
   These messages are used as acknowledgment when unicast. A hello with no data is used as the acknowledgment.
2. **NULL update-**It is used to calculate SRTT(Smooth Round Trip Timer) and RTO(Retransmission Time Out).
   *SRTT:*The time is taken by a packet to reach neighboring router and the acknowledgment of the packet to reach to the local router.
   RTO: If a multicast fails then unicast are being sent to that router. RTO is the time for which the local router waits for an acknowledgment of the packet.
3. **Full Update –** After exchanging hello messages or after the neighbourship is formed, these messages are exchanged. This message contains all the best routes.
4. **Partial update-**These messages are exchanged when there is a topology change and new links are added. It contains only the new routes, not all the routes. These messages are multicast.
5. **Query message-**These messages are multicast when the device is declared dead and it has no routes to it in its topology table.

6. **Reply message –** These messages are the acknowledgment of the query message sent to the originator of the query message stating the route to the network which has been asked in the query message.
7. **Acknowledgement message**
   It is used to acknowledge EIGRP update, queries, and replies. Acks are hello packets that contain no data.
   Note:-Hello, and acknowledgment packets do not require any acknowledgment.
   Reply, query, update messages are reliable messages i.e requires acknowledgement.

Composite matrix-The EIGRP composite metric calculation can use up to 5 variables, but only 2 are used by default (K1 and K3). The composite metric values are :

K1 (bandwidth)
K2 (load)
K3 (delay)
K4 (reliability)
K5 (MTU)

The lowest bandwidth, load, delay, reliability, MTU along the path between the source and the destination is considered in the composite matrix in order to calculate the cost.

Note:- Generally, only k1 and k3 values are used for metric calculation by EIGRP. The values are 10100 for k1, k2, k3, k4, k5 respectively.

criteria To form EIGRP neighbourship, these criteria should be fulfilled:-

1. k values should match.
2. Autonomous system number should match. (AS is a group of networks running under a single administrative control) .
3. authentication should match (if applied). EIGRP supports MD5 authentication only.
4. subnet mask should be same.

Timers:-

Hello timer- The interval in which EIGRP sends a hello message on an interface. It is 5 seconds by default.

Dead timer- The interval in which the neighbor will be declared dead if it is not able to send the hello packet. It is 15 seconds by default.

Features of Enhanced Interior Gateway Routing Protocol (EIGRP)

Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco-proprietary hybrid routing protocol that contains features of distance-vector and link-state routing protocols. It is a network layer protocol which works on the protocol number 88.

Some of its features are:

1. **Rapid convergence –** EIGRP uses DUAL algorithm to support rapid convergence. If a route to a network goes down then another route(feasible successor) can be used. If there is no route present to that network in the topology table also then a query message is multicast to find out the alternative route to that network.
2. **Reduced bandwidth usage –** EIGRP doesn't send periodic updates like other distance vector routing protocol does.Distance Vector Routing protocol like RIP sends full routing table over

a period of time therefore consumes the available bandwidth needlessly but EIGRP uses partial updates if there is any change in the topology occurs i.e updates are triggered only if any event occurs therfore consuming the bandwidth when needed. Also, EIGRP updates are propagated to the routers only who requires it.

3. **Support all LAN and WAN data link protocols and topologies –** EIGRP supports multi-access network like fddi, token ring etc and all WAN topologies like leased line, point-to-point links. EIGRP doesn't require any additional configuration across layer 2 protocols like frame relay.
4. **Supports auto-summary –** In EIGRP, auto-summarization is enabled by default. Auto summarization is a feature which allows Routing Protocols to summarize its routes to their classful networks automatically i.e routers will receive summarised routes automatically. EIGRP. e.g-1.1.1.1 /24 will be automatically summarised to the classful 1.1.1.1/8
5. **Supports unequal cost load balancing –** Unequal cost load balancing is possible in EIGRP by changing the value of variance. By default, variance is 1 therfore supports equal cost load balancing but if we want to use unequal cost load balancing then we can change the value of variance according to the amount of traffic we want to divide across different paths. Feasible distance is multiplied in such a way that it becomes greater than the value of feasible distance of successor.
6. **Communication via Reliable Transfer Protocol (RTP) –** EIGRP depends upon proprietary protocol RTP to mange the communication between EIGRP speaking routers. EIGRP uses 224.0.0.10 as it's multicast address. For each multicast it sends, the router prepares and maintains a list of routers (speaking EIGRP). If no acknowledgement of multicast is received then same data is transmitted through 16 unicast messages. If no acknowledgement is received even after 16 unicast attempt then it is declared dead. This process is known as reliable multicast.
7. **Best path selection using DUAL –** EIGRP uses Diffusing Update Algorithm (DUAL) to find out the best path available to a network. EIGRP speaking routers maintains a topology table in which all the routes to the network are maintained. If the best path (successor) goes down, then second best path (feasible successor) is used from the topology table. If there is no path available in topology table then it sends a query message to resolve the query.

   It maintains 3 different tables mainly:
   (a) Neighbor table: It contains information about the routers with which neighbourship has been formed. It contains the SRTT, RTP. It also contains queue count value for the hello messages that are not being acknowledged.
   (b) Topology table: It contains all the routes available to a network (both feasible successor and successor).
   (c) Routing table: It contains all the routes which are being used to make current routing decisions. The routes in this table are considered as successor (best path) route.
8. **Traffic control –** Suppose if one of the interface of the router is connected to ISP then we don't want that interface to be part of EIGRP process. For this scenario, EIGRP provides a feature in which we can flag the interface as passive i.e not to take part in EIGRP process.
9. Support Variable Length Subnet Mask (VLSM).
10. Support for both IPv4 and IPv6.

Difference between IGRP and EIGRP:

S.NO	IGRP	EIGRP
1.	IGRP stands for Interior Gateway Routing Protocol.	EIGRP stands for Enhanced Interior Gateway Routing Protocol.
2.	Interior Gateway Routing Protocol is Classful routing technique.	While Enhanced Interior Gateway Routing Protocol is a classless routing technique.
3.	IGRP is a slow convergence.	While it is a fast convergence.
4.	In IGRP, Bellman ford algorithm is used.	While in this, Dual algorithm is used.
5.	IGRP needs more or high bandwidth.	While EIGRP needs low or less bandwidth.
6.	The least hop count in IGRP is 255.	While the least hop count in EIGRP is 256.
7.	It provides 24 bits for delay.	While it provides 32 bits for delay.

Open Shortest Path First (OSPF) Protocol fundamentals

Open shortest path first (OSPF) is a **link-state routing protocol** which 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 which 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 are 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. It is a **network layer protocol** which works on the protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router(DR)/Backup Designated Router (BDR).

Criteria –

To form neighbourship in OSPF, there is a criteria for both the routers:

1. It should be present in same area
2. Router I'd must be unique
3. Subnet mask should be same
4. Hello and dead timer should be same
5. Stub flag must match
6. Authentication must match

OSPF supports NULL, plain text, MD5 authentication.

Note – Both the routers (neighbors) should have same type of authentication enabled. e.g- if one neighbor has MD5 authentication enabled then other should also have MD5 authentication enabled.

OSPF messages –
OSPF uses certain messages for the communication between the routers operating OSPF.

- **Hello message –** These are keep alive messages used for neighbor discovery /recovery. These are exchanged in every 10 seconds. This include following information : Router I'd, Hello/dead interval, Area I'd, Router priority, DR and BDR IP address, authentication data.
- **Database Description (DBD) –** It is the OSPF routes of the router. This contains topology of an AS or an area (routing domain).
- **Link state request (LSR) –** When a router receive DBD, it compares it with its own DBD. If the DBD received has some more updates than its own DBD then LSR is being sent to its neighbor.
- **Link state update (LSU) –** When a router receives LSR, it responds with LSU message containing the details requested.
- **Link state acknowledgement –** This provides reliability to the link state exchange process. It is sent as the acknowledgement of LSU.
- **Link state advertisement (LSA) –** It is an OSPF data packet that contains link-state routing information, shared only with the routers to which adjacency has been formed.

Note – Link State Advertisement and Link State Acknowledgement both are different messages.
Timers –

- **Hello timer –** The interval in which OSPF router sends a hello message on an interface. It is 10 seconds by default.
- **Dead timer –** The interval in which the neighbor will be declared dead if it is not able to send the hello packet . It is 40 seconds by default.It is usually 4 times the hello interval but can be configured manually according to need.

OSPF supports/provides/advantages –

- Both IPv4 and IPv6 routed protocols
- Load balancing with equal cost routes for same destination
- VLSM and route summarization
- Unlimited hop counts
- Trigger updates for fast convergence
- A loop free topology using SPF algorithm
- Run on most routers
- Classless protocol

There are some disadvantages of OSPF like, it requires extra CPU process to run SPF algorithm, requires more RAM to store adjacency topology and more complex to setup and hard to troubleshoot.
Open Shortest Path First (OSPF) protocol States

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). 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. It is a network layer protocol which works on the protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router(DR)/Backup Designated Router (BDR).

OSPF terms –

1. **Router I'd –** It is the highest active IP address present on the router. First, highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.
2. **Router priority –** It is a 8 bit value assigned to a router operating OSPF, used to elect DR and BDR in a broadcast network.
3. **Designated Router (DR) –** It is elected to minimize the number of adjacency formed. DR distributes the LSAs to all the other routers. DR is elected in a broadcast network to which all the other routers shares their DBD. In a broadcast network, router requests for an update to DR and DR will respond to that request with an update.
4. **Backup Designated Router (BDR) –** BDR is backup to DR in a broadcast network. When DR goes down, BDR becomes DR and performs its functions.

DR and BDR election – DR and BDR election takes place in broadcast network or multi-access network. Here are the criteria for the election:

1. Router having the highest router priority will be declared as DR.
2. If there is a tie in router priority then highest router I'd will be considered. First, the highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.

OSPF states – The device operating OSPF goes through certain states. These states are:

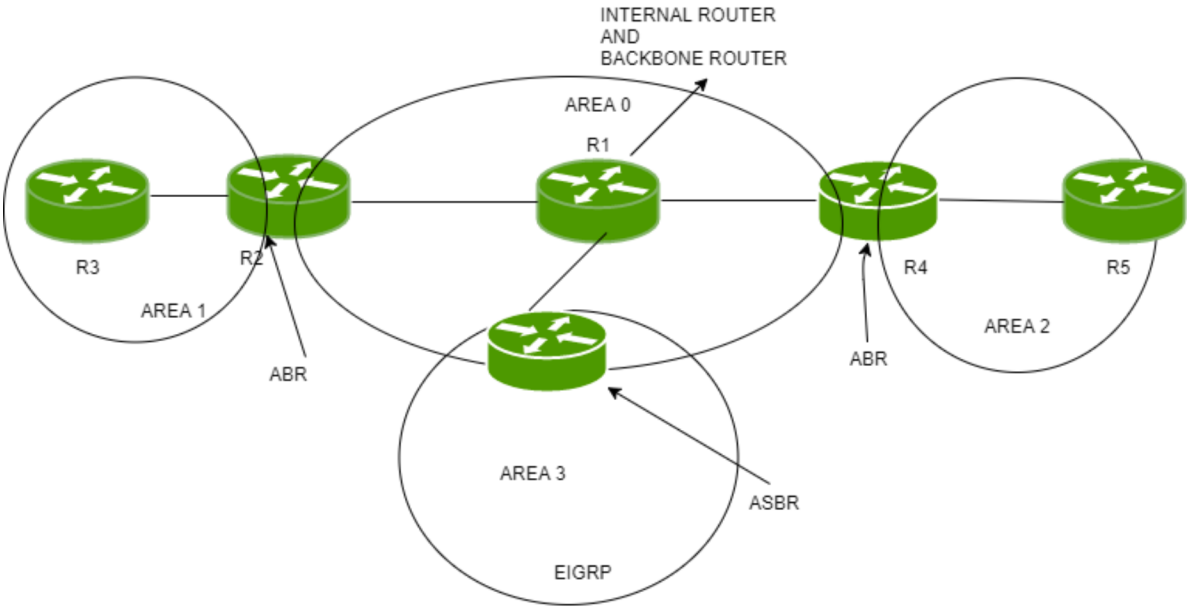
1. **Down –** In this state, no hello packet have been received on the interface.
   Note – The Down state doesn't mean that the interface is physically down. Here, it means that OSPF adjacency process has not started yet.
2. **INIT –** In this state, hello packet have been received from the other router.
3. **2WAY –** In the 2WAY state, both the routers have received the hello packets from other routers. Bidirectional connectivity has been established.
   Note – In between the 2WAY state and Exstart state, the DR and BDR election takes place.
4. **Exstart –** In this state, NULL DBD are exchanged.In this state, master and slave election take place. The router having the higher router I'd becomes the master while other becomes the slave. This election decides Which router will send it's DBD first (routers who have formed neighbourship will take part in this election).
5. **Exchange –** In this state, the actual DBDs are exchanged.
6. **Loading –** In this sate, LSR, LSU and LSA (Link State Acknowledgement) are exchanged.
   Important – When a router receives DBD from other router, it compares it's own DBD with the other router DBD. If the received DBD is more updated than its own DBD then the router will send LSR to the other router stating what links are needed. The other router replies with the LSU containing the updates that are needed. In return to this, the router replies with the Link State Acknowledgement.
7. **Full –** In this state, synchronization of all the information takes place. OSPF routing can begin only after the Full state.

Open shortest path first (OSPF) router roles and configuration

Open shortest path first (OSPF) is a link-state routing protocol which is used to find the best path between the source and the destination router using its own SPF algorithm.

Open shortest path first (OSPF) router roles –

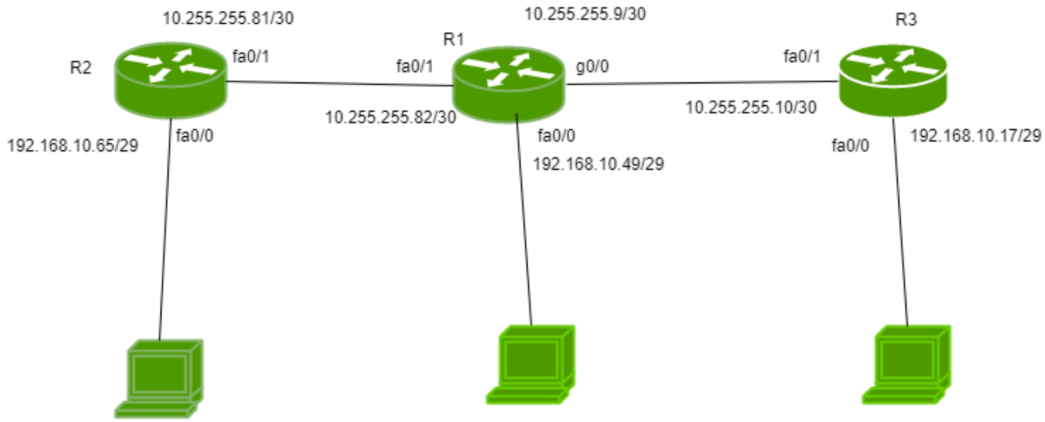
An area is a group of contiguous network and routers. Routers belonging to same area shares a common topology table and area I'd. The area I'd is associated with router's interface as a router can belong to more than one area. There are some roles of router in OSPF:



1. **Backbone router –** The area 0 is known as backbone area and the routers in area 0 are known as backbone routers. If the routers exists partially in the area 0then also it is a backbone router.
2. **Internal router –** An internal router is a router which have all of its interfaces in a single area.
3. **Area Boundary Router (ABR) –** The router which connects backbone area with another area is called Area Boundary Router. It belongs to more than one area. The ABRs therefore maintain multiple link-state databases that describe both the backbone topology and the topology of the other areas.
4. **4.Area Summary Border Router (ASBR) –** When an OSPF router is connected to a different protocol like EIGRP, or Border Gateway Protocol, or any other routing protocol then it is known as AS. The router which connects two different AS (in which one of the interface is operating OSPF) is known as Area Summary Border Router. These routers perform redistribution. ASBRs run both OSPF and another routing protocol, such as RIP or BGP. ASBRs advertise the exchanged external routing information throughout their AS.

Note – A router can be backbone router and Area Boundary Router at the same time i.e a router can perform more than one role at a time.

Configuration –



There is a small topology in which there are 3 routers namely R1, R2, R3 are connected. R1 is connected to networks 10.255.255.80/30 (interface fa0/1), 192.168.10.48/29 (interface fa0/0) and 10.255.255.8/30 (interface gi0/0)

Note – In the figure, IP addresses are written with their respected interfaces but as have to advertise networks therefore, you have to write network I'd. R2 is connected to networks 192.168.10.64/29 (interface fa0/0), 10.255.255.80/30 (interface fa0/1). R3 is connected to networks 10.255.255.8/30 (int fa0/1), 192.168.10.16/29 (int fa0/0).

Now, configuring OSPF for R1.

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.10.48 0.0.0.7 area 1
R1(config-router)#network 10.255.255.80 0.0.0.3 area 1
R1(config-router)#network 10.255.255.8 0.0.0.3 area 1
```

Here, 1 is the OSPF instance or process I'd. It can be same or different (doesn't matter). You have use wildcard mask here and area used is 1.

Now, configuring R2

```
R2(config)#router ospf 1
R2(config-router)#network 192.168.10.64 0.0.0.7 area 1
R2(config-router)#network 10.255.255.80 0.0.0.3 area 1
```

Similarly, for R3

```
R3(config)#router ospf 1
R3(config-router)#network 192.168.10.16 0.0.0.7 area 1
R3(config-router)#network 10.255.255.8 0.0.0.3 area 1
```

You can check the configuration by typing command

```
R3#show ip protocols
```