RIP Version 1 vs. RIP Version 2

RIP (Routing Information Protocol) is a distance-vector routing protocol used in small to medium-sized networks. There are two versions of RIP: RIP version 1 (RIPv1) and RIP version 2 (RIPv2). While both versions serve the same purpose of exchanging routing information between routers, they have differences in features, capabilities, and compatibility. Here's a comparison between RIP version 1 and RIP version 2:

1. **Routing Updates:**

- **RIPv1:** Sends routing updates as broadcast messages every 30 seconds.
- **RIPv2:** Supports both broadcast and multicast updates, allowing for more efficient use of network resources.

2. **Subnet Mask Support:**

- **RIPv1:** Does not support subnet masks in routing updates. It assumes that all subnets within a network have the same subnet mask.
- **RIPv2:** Supports Variable Length Subnet Mask (VLSM) and Classless Inter-Domain Routing (CIDR). It includes subnet mask information in routing updates, allowing for the use of different subnet masks within a network.

4. **Authentication:**

- **RIPv1:** Does not include authentication mechanisms, making it vulnerable to unauthorized route advertisements and spoofing attacks.
- **RIPv2:** Supports authentication using MD5 authentication, providing a level of security by ensuring that routing updates are only accepted from authenticated sources.

5. **Hop Count Limit:**

- **RIPv1:** Uses a maximum hop count of 15 to determine the maximum distance a route can traverse. Routes with a hop count greater than 15 are considered unreachable.
- **RIPv2:** Retains the maximum hop count of 15 but includes an option for setting a larger maximum hop count if needed, allowing for larger network topologies.

Below is a tabular comparison between RIPv1 and RIPv2:

Feature	**RIPv1**	**RIPv2**
Routing Updates	Broadcasts updates every 30 seconds.	Supports both broadcast and multicast updates.
Subnet Mask Support	Does not support subnet masks.	Supports Variable Length Subnet Mask (VLSM) and CIDR.
Route Tagging	Does not support route tagging.	Supports route tagging for additional information.
Authentication	Does not support authentication.	Supports MD5 authentication.

Feature	RIPv1	RIPv2
Hop Count Limit	Maximum hop count of 15.	Maximum hop count of 15, with an option for larger hop counts.
Broadcast Domain	Sends updates as broadcasts.	Supports multicast updates.
Summary Route Advertisement	Does not support summary route advertisement.	Supports advertisement of summary routes.
Compatibility	Widely supported by older devices.	Provides backward compatibility with RIPv1.

RIP commands

```
A(config)# router rip
A(config-router)# network 172.16.0.0
A(config-router)# passive-interface g0/0
A(config-router)# passive-interfacce g0/2
```

Enable Passive Interface:

```
passive-interface {interface_name}
```

This command prevents RIP updates from being sent or received on the specified interface.

Administrative Distance of Routing Protocols:

> Administrative Distance given on the basis of intellagence of routing protocols. Administrative distance is a value used by routers to select the best path when there are multiple routes to the same destination. The lower the administrative distance, the more preferred the route. Here's a table listing the administrative distances for various routing protocols:

Routing Protocol	Administrative Distance
Directly Connected	0
Static	1
eBGP	20
EIGRP	90
IGRP	100
OSPF (Open Shortest Path First)	110
IS-IS	115
RIP (Routing Information Protocol)	120

Routing Protocol	Administrative Distance
External EIGRP	170
Internal BGP (Border Gateway Protocol)	200
External BGP	20
Unknown	255

Route Selection Procedure of Router

The route selection procedure is a critical function performed by routers to ensure efficient data packet forwarding in computer networks. By examining routing table entries, comparing administrative distances and metrics, and selecting the best path based on predefined criteria, routers determine how to forward packets to their destinations. Understanding the route selection process is essential for network administrators to design, configure, and troubleshoot network infrastructures effectively.

1. **Longest Prefix Match:**
    - The router performs a longest prefix match to find the most specific route entry that matches the destination IP address.
    - If multiple entries match, the router selects the entry with the longest prefix (i.e., the most specific subnet mask).
2. **Administrative Distance Comparison:**
    - If there are multiple matching routes with the same prefix length, the router compares their administrative distances.
    - The route with the lowest administrative distance is preferred.
3. **Metric Comparison:**
    - If there are multiple routes with the same prefix length and administrative distance, the router compares their metrics.
    - The metric could be based on factors such as hop count, bandwidth, delay, reliability, or cost.
    - The router selects the route with the lowest metric as the best path.

Distance Vector vs Link-state

Distance Vector	Link-state
E.g. RIP	E.g. OSPF
Routing table	Routing table
	Link-state
	Neighbour table
Routing by Rummors	Link-state Database
Update 30 sec	hello packet 10/30sec

Distance Vector	Link-state
	LSA (No timer)
	DD (every 30 min)
Routing loops	Not having routing loops
conume more bandwidth	memory and processing power consuming
hop count (15)	each area 255 hops x 2^32
FLSM	VLSM and hierarchical addressing
255.255.255.255	multicast 224.0.0.5
	224.0.0.6
algorithm used Belmon and Ford	Dikikstra (SPF)
small networks	medium to large network

> still Link-state protocol used over Distance vector because it is very simple to configure.

OSPF Hierarchical Architecture

1. Backbone Area (Area 0):

- **Function:** The backbone area serves as the core of the OSPF network, connecting all other OSPF areas.
- **Area Identifier:** Area 0 (also known as the backbone area) is mandatory in OSPF. It must exist and interconnect all other areas.
- **Role:** All inter-area traffic passes through the backbone area, and routing information from other areas is summarized and propagated into the backbone.

2. ASBR (Autonomus System Border Routers):

- **Role:** ASBRs play a crucial role in integrating OSPF networks with external networks, enabling communication between OSPF domains and external destinations.
- **Function:** ASBRs help in maintaining network scalability and flexibility by allowing OSPF networks to grow and interconnect with external networks while maintaining efficient routing operations within the OSPF domain.
- **Connectivity:** ASBRs connect the OSPF routing domain to networks outside of the OSPF domain, such as other autonomous systems, Internet Service Providers (ISPs), or external networks.

3. ABRs (Area Border Routers):

- **Role:** ABRs connect multiple OSPF areas and maintain separate routing tables for each area.
- **Function:** They summarize routing information between areas, reducing the size of routing tables and optimizing routing efficiency.
- **Connectivity:** ABRs have interfaces in multiple areas, allowing them to route traffic between areas.

4. Internal Routers:

- **Role:** Internal routers play a vital role in maintaining intra-area connectivity and routing within OSPF areas.
- **Function:** They contribute to efficient routing operations by calculating shortest paths and maintaining routing tables for destinations within the OSPF area.
- **Connectivity:** Internal routers are responsible for intra-area communication within their respective OSPF areas.They maintain routing information for networks within the area and exchange routing updates with other routers within the same area.

Area Types:

- 1 **Backbone Area (Area 0):** The backbone area interconnects all other OSPF areas within the network. It acts as a central hub facilitating communication and routing between different OSPF areas.

- 2 **Stub Area:** A stub area does not receive external LSAs (Type 5 LSAs) from other areas. It uses a default route for external traffic.

> Stub area not for external area routers.

- 3 **Totally Stubby Area:** A totally stubby area does not receive any external LSAs or Type 3 LSAs from other areas. It uses a default route for all traffic outside the area

> Totally stubby area in not for external and internal area routers

- 4 **Not-So-Stubby Area (NSSA):** Similar to stub areas but allows ASBRs to inject external routes into the area using Type 7 LSAs, which are translated to Type 5 LSAs at the NSSA's boundary.

OSPF configuration.

For router A

```
A(config)# router ospf 1
here 1 is processi id locally significant
A(config-router)# network 172.16.10.0 0.0.0.255 area 0
A(config-router)# network 172.16.20.0 0.0.0.255 area 0
```

for router B

```
B(config-router)# ospf 2
B(config-router)# network 172.16.30.0 0.0.0.255 area 0
B(config-router)# network 172.16.20.0 0.0.0.255 area 0
```

syntax is

```
 A(config-router) network <ip address> <wild card mask> <area>
```

RID(Router ID)

- Highest of Loopback interfaces
- RID can chosen on basis of logical ID
- Ideal practice in OSPF to configure loopback ID
- If loopback is not present then consider Physical interface.

> Even if physical interface down then router OSPF works on logical interfaces.

```
A(config)# int lo 0
A(config-if)# no shut
A(confi-if)# ip address 1.1.1.1 255.255.255.255
```

Broadcast Multiaccess Network (BMA):

-A Broadcast Multiaccess Network (BMA) is a type of network topology where multiple nodes share a common communication medium and can communicate with each other through broadcasting. In a BMA network, each node can send data packets to all other nodes by broadcasting them onto the shared medium.

Designated Router (DR):

- **Purpose:** In OSPF multiaccess networks, such as Ethernet, the DR reduces the number of adjacencies and the amount of routing protocol traffic by representing the entire multiaccess network as a single router.
- **Function:** The DR is responsible for exchanging OSPF routing updates with other routers on the multiaccess network.
- **Advantages:**
  - Reduces the number of adjacencies: Instead of forming a full adjacency with each neighbor, routers only form adjacencies with the DR and BDR.
  - Decreases routing protocol traffic: OSPF updates are sent only to the DR and BDR, which then forward the updates to other routers on the network.
- **Selection Process:** The router with the highest OSPF priority becomes the DR. If multiple routers have the same priority, the router with the highest Router ID is selected as the DR.
- **Roles:** The DR forwards OSPF updates to all routers on the network, including the BDR, and participates in the OSPF routing process.
- **Backup:** In case the DR fails, the BDR takes over the responsibilities of the DR.

Backup Designated Router (BDR):

- **Purpose:** The BDR is a standby router that takes over the responsibilities of the DR in case the DR fails.
- **Function:** The BDR maintains a copy of the OSPF database and is ready to assume the role of the DR if the DR fails.
- **Advantages:** Ensures redundancy and fault tolerance in OSPF multiaccess networks by providing backup functionality.

- **Selection Process:** Similar to the DR election, the BDR is selected based on OSPF priority and Router ID.
- **Role:** The BDR remains in standby mode, ready to assume the role of the DR if necessary.

Designated Router Election:

- **Trigger:** The DR election process is triggered when OSPF routers on a multiaccess network first become adjacent.
- **Process:** Routers exchange OSPF Hello packets containing their Router ID and OSPF priority.
- **Selection Criteria:** The router with the highest OSPF priority becomes the DR, and the router with the second-highest priority becomes the BDR.
- **Priority Tiebreaker:** If multiple routers have the same priority, the router with the highest Router ID is selected as the DR.

> In router election router having highest priority elected first, if priority is same then router having highest RID elected first. defautl priority is 1 Priority range in between 0-255 There is election are always for BDR In neighbor table there is no DR only BDR then BDR assigns themselves as DR

Monitoring commands for OSPF

```
A(config-router)# show ip ospf database
A(config-router)# show ip ospf neighbor
A(config-router)# show ip route
```

EIGRP

- algrithm used DUAL
- parameter
    - Bandwidth
    - Delay
    - Load
    - Reliability
    - MTU

> In EIGRP have 2 packets i,e. Hello and Update packets Hello packets sends 5/60 sec. (1.544 Mbps) RTP is Reliable Transfer Protocol , all update happens in EIGRP through RTP. PDM (Protocol Dependent Module) makes descision about adding routes learned from other sources. Unqual Cost Load Balancing Default 4 path and maximum 6 path

EIGRP (Enhanced Interior Gateway Routing Protocol) is an advanced distance-vector routing protocol developed by Cisco Systems. It is designed to provide fast convergence, efficient bandwidth utilization, and scalability in large and complex networks. Here's an overview of EIGRP:

Key Features:

1. **Fast Convergence:**

- EIGRP uses the Diffusing Update Algorithm (DUAL) to calculate loop-free paths quickly and converge rapidly in response to network changes.
- It supports rapid convergence through features such as triggered updates and incremental updates.

2. **Efficient Bandwidth Utilization:**
    - EIGRP minimizes bandwidth usage by sending partial updates that include only the changes in network topology.
    - It uses Reliable Transport Protocol (RTP) to ensure reliable delivery of routing updates.
3. **Supports Multiple Network Layer Protocols:**
    - EIGRP can run over various network layer protocols, including IP, IPv6, and IPX.
    - It supports multiple address families, allowing for the simultaneous routing of different types of traffic.
4. **Advanced Features:**
    - EIGRP supports features such as Equal-Cost Multipath (ECMP), Load Balancing, and Route Summarization.
    - It provides features for network security, including authentication mechanisms and filtering capabilities.
5. **Support for VLSM and CIDR:**
    - EIGRP supports Variable Length Subnet Masking (VLSM) and Classless Inter-Domain Routing (CIDR), enabling efficient address space utilization.

EIGRP Components:

1. **Neighbor Discovery and Maintenance:**
    - EIGRP routers discover neighbors using Hello packets and maintain neighbor relationships.
    - Neighbor relationships allow routers to exchange routing updates and topology information.

EIGRP Operation:

1. **Initialization:** EIGRP routers send Hello packets to discover neighbors and establish neighbor relationships.
2. **Neighbor Discovery:** Routers exchange Hello packets and establish neighbor relationships with adjacent routers.
3. **Topology Exchange:** Routers exchange routing updates containing information about reachable networks and their associated metrics.
4. **Route Calculation:** Using the topology information received from neighbors, routers calculate loop-free paths and select the best routes to destination networks.
5. **Route Maintenance:** Routers monitor the reachability of destination networks and update routing tables in response to network changes.

Advantages of EIGRP:

- Fast convergence and efficient bandwidth utilization.

- Scalability in large and complex networks.
- Support for multiple network layer protocols and advanced features.
- Easy to configure and deploy in Cisco networks.
- Hierarchical design with route summarization capabilities.

Auto Summerization:

- It summerizes all network in one IP
- and sends IP to their corrosponding neighboring network.

Bandwidth Management:

- If link beyond one router down then the entire bandwidth will be full because of routing update so EIGRP uses only 50% bandwidth for routing update.

monitoring commands

```
A(config-router)# show ip eigrp topology
A(config-router)# show ip eigrp neighnor
```