

The University of Jordan, Comp. Eng. Dept.

Networks lab: Handout: Experiment 5

Dynamic Routing: Distance Vector Protocols (RIP: Theory and Practice)

Instructors: Prof. Khalid A. Darabkh and Eng. Muna Al-Akhras

Parts Included: Dynamic Routing Protocols, Routing Information Protocol (RIP), RIPv2 and Routing Information Protocol Next Generation (RIPng) Configuration Commands, and Practical Problems.

Part I: Dynamic Routing Protocols

Dynamic routing protocols play an important role in today's networks. The following sections describe several important benefits that dynamic routing protocols provide. In many networks, dynamic routing protocols are typically used with static routes.

A. The Evolution of Dynamic Routing Protocols

Dynamic routing protocols have been used in networks since the late 1980s. One of the first routing protocols was *Routing Information Protocol (RIP)*. RIP version 1 (RIPv1) was released in 1988. As networks evolved and became more complex, new routing protocols emerged. The RIP routing protocol was updated to accommodate growth in the network environment, into RIPv2. However, the newer version of RIP still does not scale to the larger network implementations of today. To address the needs of larger networks, two advanced routing protocols were developed: *Open Shortest Path First (OSPF)* and *Intermediate System-to-Intermediate System (IS-IS)*. Cisco developed the *Interior Gateway Routing Protocol (IGRP)* and *Enhanced IGRP (EIGRP)*, which also scales well in larger network implementations. Additionally, there was the need to connect different internetworks and provide routing between them. The *Border Gateway Protocol (BGP)* is now used between Internet service providers (ISPs). BGP is also used between ISPs and their larger private clients to exchange routing information. Figure 1 classifies the protocols.

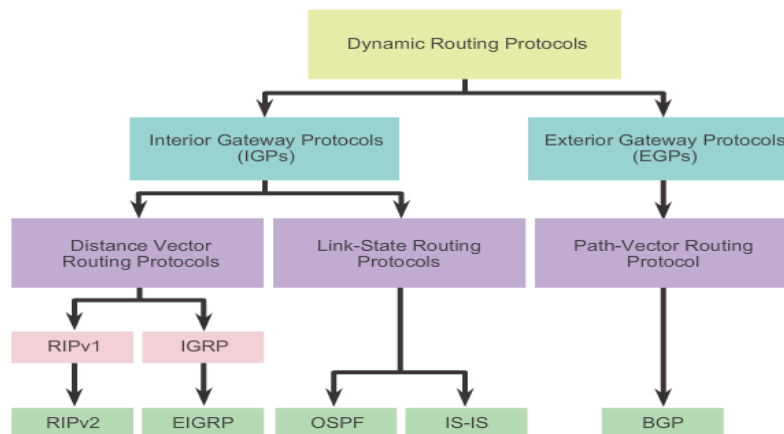


Figure 1. Classifications of dynamic routing protocols

Interestingly, **an autonomous system (AS)—otherwise known as a routing domain—is a collection of routers under a common administration. Typical examples are a company’s internal network and an ISP’s network.** Because the Internet is based on the autonomous system concept, two types of routing protocols are required: interior and exterior routing protocols. These protocols along with their summary are, which are also detailed in Figure 2:

- **Interior Routing Protocols**
 - Used within an autonomous system
 - Used within an area of administrative control
- **Exterior Routing Protocols**
 - Used between autonomous systems
 - Used to peer with networks in which you have no administrative control

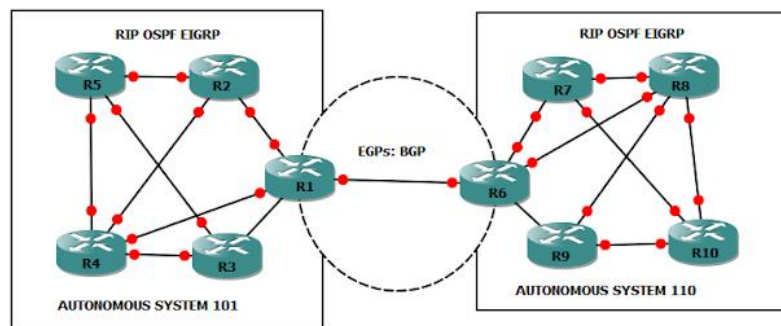


Figure 2. IGP Versus EGP Routing Protocols

B. Convergence, load balancing, and administrative distances

Convergence, is when the routing tables of all routers are at a state of consistency. **The network has converged when all routers have complete and accurate information about the network.** Convergence time is the time it takes routers to share information, calculate best paths, and update their routing tables. A network is not completely operable until the network has converged; therefore, most networks require short convergence times.

Load Balancing, you now know that individual routing protocols use metrics to determine the best route to reach remote networks. **But what happens when two or more routes to the same destination have identical metric values?** How will the router decide which path to use for packet forwarding? In this case, the router does not choose only one route. Instead, the router load-balances between these equal-cost paths. The packets are forwarded using all equal-cost paths. Figure 3 shows an example of load balancing, assuming that R2 load-balances traffic to PC5 over two equal-cost paths.

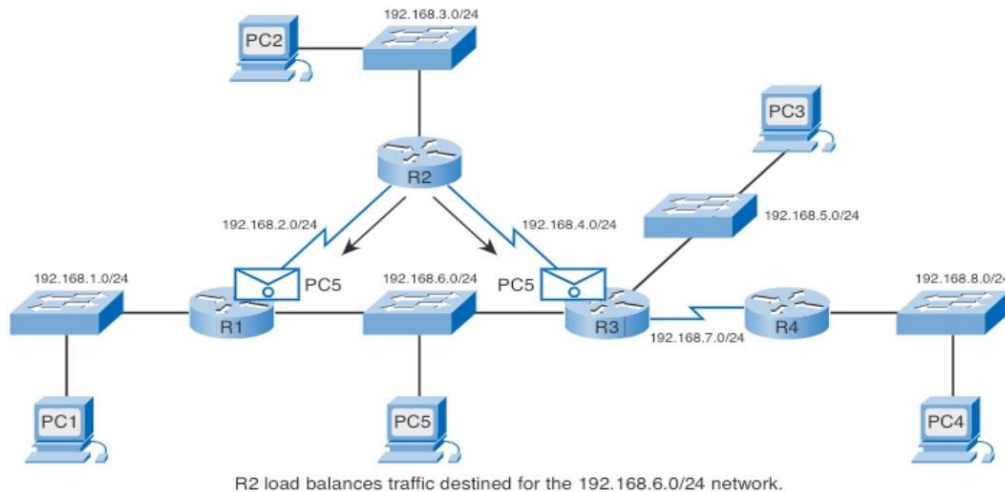


Figure 3. Load Balancing Across Equal-Cost Paths

Administrative distance (AD), defines the preference of a routing source (or the trustworthiness of a routing protocol). Each routing source—including specific routing protocols, static routes, and even directly connected networks—is prioritized in order of most to least preferable using an administrative distance value. Administrative distance is an integer value from 0 to 255. The lower the value, the more preferred the route source. An administrative distance of 0 is the most preferred. Only a directly connected network has an administrative distance of 0, which cannot be changed. An administrative distance of 255 means the router will not believe the source of that route, and it will not be installed in the routing table. Figure 4 shows a topology with R2 running both EIGRP and RIP. R2 is running EIGRP with R1 and RIP with R3.

The AD value is the first value in the brackets for a routing table entry. Notice, through Figure 5, that R2 has a route to the 192.168.6.0/24 network with an AD value of 90.

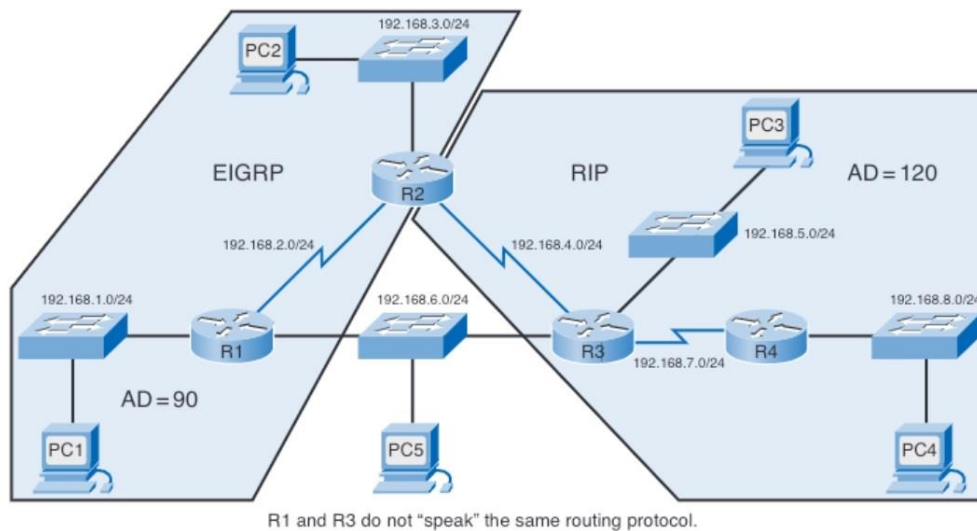


Figure 4. Different administrative distances

```
R2# show ip route

<output omitted>

Gateway of last resort is not set

D    192.168.1.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, Serial0/0/1
R    192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
D    192.168.6.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0
R    192.168.7.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
R    192.168.8.0/24 [120/2] via 192.168.4.1, 00:00:08, Serial0/0/1
```

Figure 5. Routing Table of R2

C. Routing Metrics and Costs

Routing metrics and costs are used for determining the best route to the destination. The factors used by the protocols to determine the shortest path; these factors are known as a metric. Metrics are the network variables used to determine the best route to the destination. For some protocols use the static metrics means that their value cannot be changed and for some other routing protocols use the dynamic metrics means that their value can be assigned by the system administrator.

The most common metric values are given below:

- **Hop count:** Hop count is defined as a metric that specifies the number of passes through internetworking devices such as a router, a packet must travel in a route to move from source to the destination. If the routing protocol considers the hop as a primary metric value, then the path with the least hop count will be considered as the best path to move from source to the destination.
- **Delay:** It is a time taken by the router to process, queue and transmit a datagram to an interface. The protocols use this metric to determine the delay values for all the links along the path end-to-end. The path having the lowest delay value will be considered as the best path.
- **Bandwidth:** The capacity of the link is known as a bandwidth of the link. The bandwidth is measured in terms of bits per second. The link that has a higher transfer rate like gigabit is preferred over the link that has the lower capacity like 56 kb. The protocol will determine the bandwidth capacity for all the links along the path, and the overall higher bandwidth will be considered as the best route.
- **Load:** Load refers to the degree to which the network resource such as a router or network link is busy. A Load can be calculated in a variety of ways such as CPU utilization, packets processed per second. If the traffic increases, then the load value will also be increased. The load value changes with respect to the change in the traffic.
- **Reliability:** Reliability is a metric factor may be composed of a fixed value. It depends on the network links, and its value is measured dynamically. Some networks go down more often than others. After network failure, some network links repaired more easily than other network links. Any reliability factor can be considered for the assignment of reliability ratings, which are generally numeric values assigned by the system administrator.

The list that follows defines the metric for each routing protocol:

- **RIP:** Hop count: Best path is chosen by the route with the lowest hop count.
- **IGRP and EIGRP:** Bandwidth, delay, reliability, and load: Best path is chosen by the route with the smallest composite metric value calculated from these multiple parameters. By default, only bandwidth and delay are used.
- **OSPF:** Cost: Best path is chosen by the route with the lowest cost. The Cisco implementation of OSPF uses bandwidth to determine the cost.

Referring to Figure 1, there are three distance vector routing protocols, which are summarized as follows:

- 1) Routing Information Protocol (RIP), which has the following specifications:
 - RFC 1058 (RIPv1), 1988
 - Classful, no support for VLSM
 - No support for authentication
 - RFC 2453(RIPv2), 1998
 - Classless, support for CIDR
 - Support for authentication
 - Uses hop count as routing metric
 - Slow to converge
 - Not very scalable
 - Limited to 15 hops
- 2) Interior Gateway Routing Protocol(IGRP), which has the following specifications:
 - Invented by Cisco to overcome limitations of RIP
 - Allows for hop count up to 255
 - Allows for multiple route metrics
 - Bandwidth
 - Delay
 - Load
 - Reliability
 - Classful, no support for VLSM
- 3) Enhanced Interior Gateway Routing Protocol(EIGRP)
 - Replaced IGRP
 - Maintains a Topology table
 - Successors, feasible successors
 - Allows for multiple route metrics
 - Classless, support for CIDR
 - Very fast to converge
 - Maintains neighbor relationships
 - Diffusing Update Algorithm (DUAL)

Part II: Routing Information Protocol (RIP)

A. Operation of Distance Vector Routing Protocols

Distance vector means that routes are advertised as vectors of distance and direction. Distance is defined in terms of a metric such as hop count, and direction is simply the next-hop router or exit interface. **Distance vector protocols typically use the Bellman-Ford algorithm for the best-path route determination.**

Some distance vector protocols like RIP periodically send complete routing tables to all connected neighbors. In large networks, these routing updates can become enormous, causing significant traffic on the links.

Although the Bellman-Ford algorithm eventually accumulates enough knowledge to maintain a database of reachable networks, **the algorithm does not allow a router to know the exact topology of an internetwork. The router only knows the routing information received from its neighbors. In a nutshell, the distance vector routing protocols do not have an actual map of the network topology.**

Distance vector protocols work best in the following situations: 1) The network is simple and flat and does not require a hierarchical design, 2) the administrators do not have enough knowledge to configure and troubleshoot link-state protocols, and 3) Worst-case convergence times in a network are not a concern.

It is worth mentioning that the Distance Vector (DV) protocols have the following specifications:

- Based on the Bellman-Ford algorithm
- Each router on the network compiles a list (or update) of the networks it can reach (in the form of a distance vector)
- **Exchange this list with its *neighboring routers* only, as shown in Figure 6, thereby making very slow convergence.**
- **Upon receiving vectors from each of its neighbors, the router computes its own *distance* to each neighbor, amend the distances, and update its routing table accordingly.**

Routing protocols allow routers to dynamically learn information about remote networks and automatically add this information to their own routing tables, as shown in Figure 6.

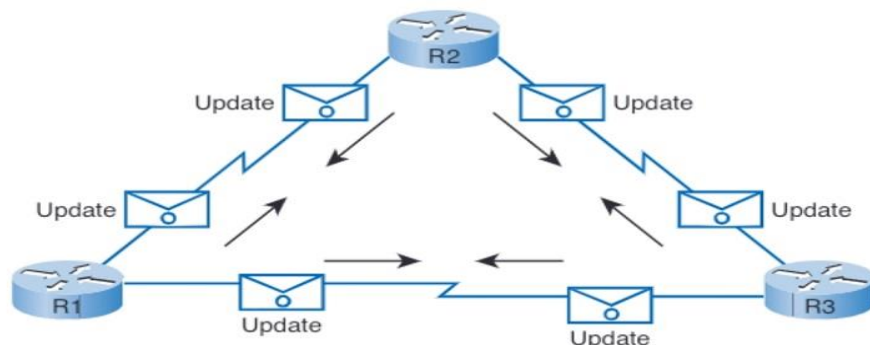


Figure 6. Routers Dynamically Pass Updates

B. RIP discussion

RIP uses hop count whereas the hop count refers to the number of routers a packet must cross to reach the destination network. For Router R3 in Figure 7, network 172.16.3.0 is two hops, or two routers, away. For Router R2, network 172.16.3.0 is one hop away, and for Router R1, it is 0 hops (because the network is directly connected).

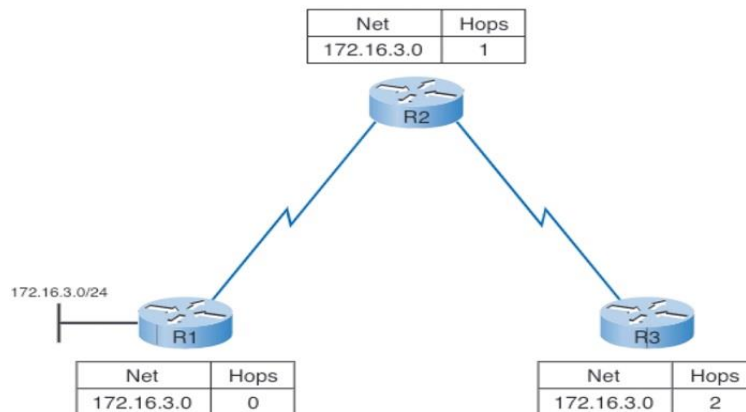


Figure 7. RIP Metrics

In Figure 8 (a), all the routers are using the RIP routing protocol. The metric associated with a certain route can be best viewed using the *show ip route* command. The metric value is the second value in the brackets for a routing table entry. In Figure 8 (b), R2 has a route to the 192.168.8.0/24 network that is two hops away. The highlighted 2 in the command output is where the routing metric is displayed.

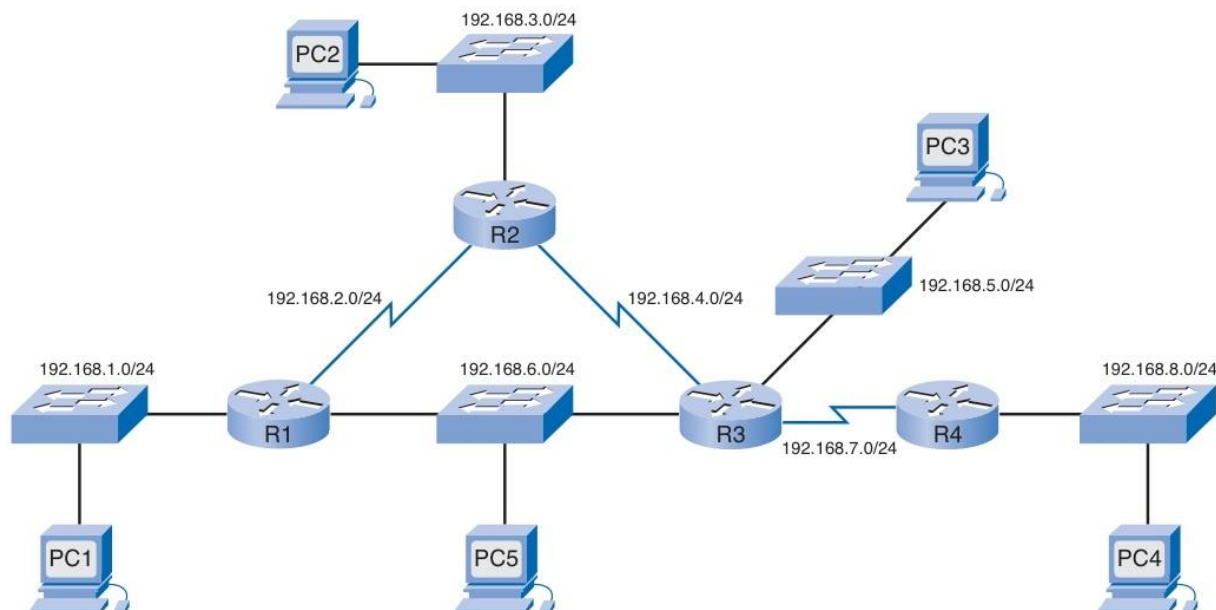


Figure 8 (a). Best Path Determined in a Network Using RIP

```
R2# show ip route
```

```
<output omitted>
```

```
Gateway of last resort is not set
```

```
R    192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:24, Serial0/0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, Serial0/0/1
R    192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:26, Serial0/0/1
R    192.168.6.0/24 [120/1] via 192.168.2.1, 00:00:24, Serial0/0/0
                                [120/1] via 192.168.4.1, 00:00:26, Serial0/0/1
R    192.168.7.0/24 [120/1] via 192.168.4.1, 00:00:26, Serial0/0/1
R    192.168.8.0/24 [120/2] via 192.168.4.1, 00:00:26, Serial0/0/1
```

Figure 8 (b). Routing Table of R2

C. RIP Main Timers

There are three main timers used in RIP, namely, **periodic update, route invalid timer, and route flush timer**. **They are detailed as follows:** the RIP routing update timer is generally set to 30 seconds, ensuring that each router **will send a complete copy of its routing table to all neighbors every 30 seconds**. The **route invalid timer** determines how much time must expire without a router having heard about a particular route before that route is considered invalid. When a route is marked invalid, neighbors are notified of this fact. This notification must occur prior to expiration of the **route flush timer**. When the route flush timer expires, the route is removed from the routing table. **Typical initial values for these timers are 90 seconds for the route invalid timer and 270 seconds for the route flush timer.**

D. Routing loops in RIP:

The main issue with distance vector routing protocols is *Routing Loops* since Bellman-Ford Algorithm cannot prevent loops. This routing loop in the DVR network causes the Count to Infinity Problem. Routing loops usually occur when an interface goes down or two routers send updates at the same time.

It is noteworthy to mention that a solution for the count to infinity problem is through defining a maximum. In other words, a limit is set on the number of hops to prevent counting for infinity, which is 16. Unfortunately, this solution will not prevent the occurrence of routing loops, but it stops it to propagate over 16. Interestingly, routing loops can occur in RIP due to mainly two possible cases:

- Due to having information in neighboring routers that conflict each other about the shortest distance to the destination. This may happen before, for example, reaching the steady state (convergence) in RIP protocol or EIGRP if we violate the feasibility condition (i.e., allowing those routes that have higher reported distances than the FD of current successor to be stored in the topology table bearing in mind using unequal-cost load balancing).
- Due to having Link-failures which may results in reaching count-to-infinity problem.

An example to show the occurrence of count to infinity (two-node instability) and routing loops is provided as follows. Consider a network topology as shown in Figure 9. Imagine for any reason the link to the C's local network (10.4.0.0, directly connected) got broken or failure. In this case, router C will update the cost to this local network to 16, which means infinity (i.e., unreachable). Now, two things can happen. The first one is that it is now C's turn to report its route (i.e., (send periodic update packet)) to B. In this case, everything goes fine (i.e., no routing loops). This is clearly shown in Figure 10. The other alternative is that B, which still has a route to 10.4.0.0, advertises it to C. Now, things start to go wrong, that are, packets to 10.4.0.0 are looped until their TTL expires, as shown in Figure 11. In particular, a packet is destined for network 10.4.0.0 arrives at router A. Accordingly to router A routing table, router A forwards the packet over interface S0. The packet arrives at router B, which forwards it out its interface S1, as indicated in its routing table. Router C receives that packet and checks or consults its routing table, which specify that the packet the packet should be forwarded out its interface S0. The packet arrives back at router B, which again forwards it to router C over interface S1. The packet loops between routers B and C indefinitely, as shown in Figure 11.

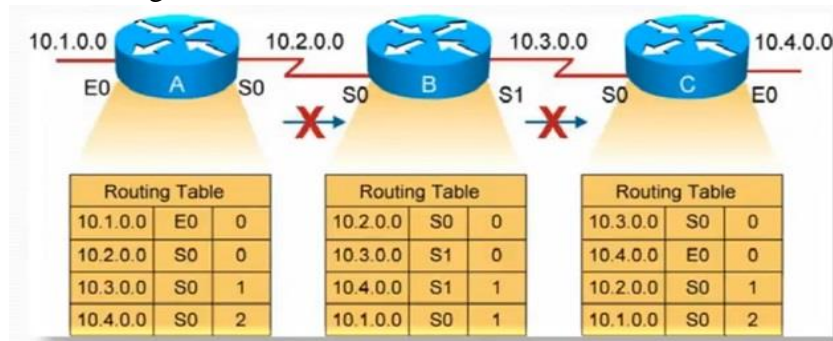


Figure 9. Routing loops: network topology

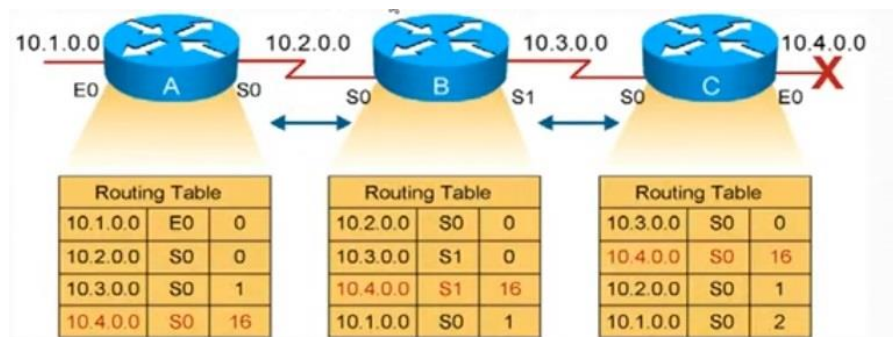


Figure 10. Routing loops: network topology – no loops

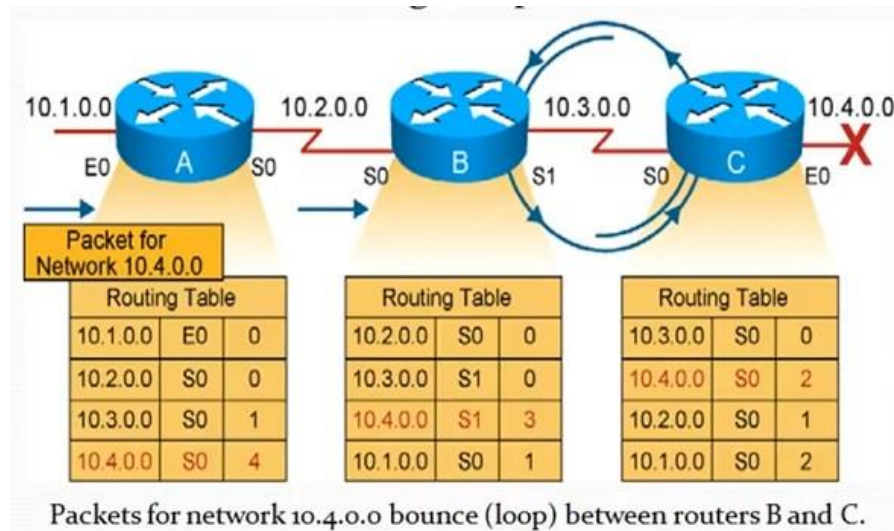


Figure 11. Routing loops: network topology –loops noticed!

To this end, it is good to stress on the point that avoiding count-to-infinity problem (i.e., having routing loops) means reducing the convergence time. As matter of fact, this can be done through getting use of many interesting solutions other than infinity (discussed earlier), namely, Split Horizon, Split Horizon with Poison Reverse, Triggered Updates, as well as Hold-down. They are detailed as follows:

- **Split Horizon**, do not send routes back over the same interface from which the route arrived. This helps in avoiding “mutual deception”: two routers tell each other they can reach a destination via each other.
 - ✓ One of the benefits of Split Horizon is decreasing the packet (update packet) size that leads to better bandwidth utilization.
 - ✓ Once again: the idea in the split horizon is as follows: *If a node A learns about the best route to a destination D from neighbor B, then A will not advertise its route for D back to B.*
 - ✓ It works great in single-path internetworks, that are, non-circular networks.
- **Split horizon with Poison Reverse**, differs from simple split horizon because it announces reverse directions. In other words, those networks learned in a given direction are announced with a hop count of 16, indicating that the network is unreachable. Referring to above example while illustrating the split horizon, one can further ensure that B will not use the route advertised by A by having A advertise a route to D with a *cost of INFINITY*, adhering to shortest path policy. This modification is called a *poison reverse*, because the node (A) is poisoning its route for D in its advertisement to B. Interestingly, in a single-path internetworks (or non-circular networks), split horizon with poison reverse has no benefit beyond split horizon. However, in a multipath internetwork (or circular networks), split horizon with poison reverse greatly reduces count-to-infinity (routing loops). Unfortunately, count-to-infinity can still occur in a multipath internetwork because routes to networks can be learned from multiple sources. Furthermore, poisoned reverse does have a disadvantage, that is, it increases the size of the routing messages.

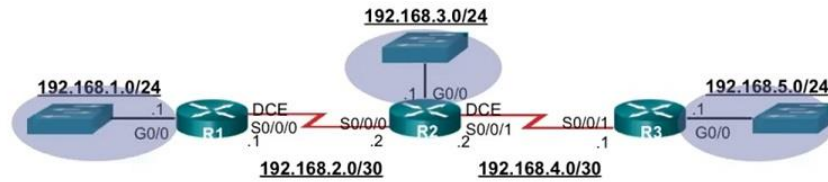
- **Triggered Updates**, allow a RIP router to announce changes in metric values almost immediately rather than waiting for the next periodic announcement. The trigger is a change to a metric in an entry in the routing table. For example, networks that become unavailable can be announced with a hop count of 16 through a triggered update.
 - ✓ If triggered updates were sent by all routers immediately, each triggered update could cause a cascade of broadcast traffic across the IP internetwork.
 - ✓ Triggered updates improve the convergence time of RIP internetworks but at the expense of additional broadcast traffic as the triggered updates are propagated.
 - ✓ Periodic announcement (every 30s) is still valid even adopting the idea of triggered updates.
- **Holddown Timers**, whenever a router learns about an unreachable route, it starts a timer. Until the time is up, the router discards any routing update that tells the unreachable route has become reachable. This protection ensures the router waits until the network is stable to modify its routing table.

E. Automatic Route Summarization

According to the classful, network specified, the subnets of that network are automatically identified and participate in the routing update. **By default, routing updates in RIP and EIGRP are summarized at network boundaries** to limit the number of routing advertisements and the size of routing tables. In other words, this is the definition of automatic route summarization, which allows a router to group networks together and advertises them as one large group using a single, summarized route of the aim of decreasing the number of entries in routing updates and reducing the number of entries in local routing tables. However, sometimes, automatic summarization leads to lose connectivity to networks that are contiguous and reach through different exit interfaces.

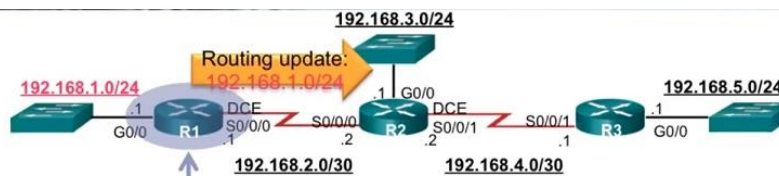
F. Passive Interfaces

At any time, you can manually stop broadcasting and receiving RIP and EIGRP updates from the LAN interfaces, these interfaces define as passive interfaces. This is done for two important purposes, which are, (i) to suppress unnecessary update traffic, such as when an interface is a LAN interface, with no other routers connected, (ii) to increase security controls, such as preventing unknown rogue routing devices from receiving RIP and EIGRP updates. Thus, the **passive-interface command** **allows a router to receive routing updates on an interface but not send updates via that interface.** To make the process clearer, Figures 12 (a) through (e) illustrate this feature along with its proper configuration through providing a certain topology and a detailed discussion **taking into account that in Figures 12(d) and (e), we consider that R3 has three LAN interfaces (G0/0, G0/1, and G0/3) and one serial interface (S0/0/1).**



- Sending out unneeded updates on a LAN:
 - Wastes Bandwidth
 - Wastes Resources
 - Security Risk
- The **passive-interface**
 - Stops routing updates out the specified interface.
 - The **network** that the specified interface belongs to is still advertised in routing updates that are sent out other interfaces.
 - Should be configured on interfaces which do not connect to other RIP routers.

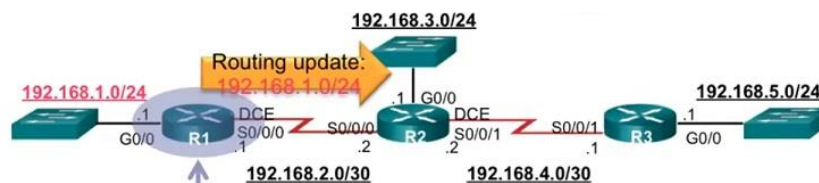
Figure 12 (a). RIP with Passive Interfaces Feature



```
R1(config)# router rip
R1(config-router)# passive-interface g0/0
R1(config-router)# end
R1#
```

- What about not configuring (or removing) the router rip command: **network 192.168.1.0**
- No. The router will no longer advertise the 192.168.1.0/24 network to R2

Figure 12 (b). RIP with Passive Interfaces Feature



```
R1# show ip protocols | begin Default
Default version control: send version 2, receive version 2
Interface          Send Recv Triggered RIP Key-chain
Serial0/0/0        2      2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  192.168.1.0
  192.168.2.0
Passive Interface(s):
  GigabitEthernet0/0
Routing Information Sources:
  Gateway          Distance    Last Update
  192.168.2.2      120        00:00:06
Distance: (default is 120)
```

Figure 12 (c). RIP with Passive Interfaces Feature


```

R2(config)# router rip
R2(config-router)# passive-interface g0/0
R2(config-router)# end
R2#
*Mar 10 16:33:32.391: %SYS-5-CONFIG_I: Configured from console by console
R2# show ip protocols | begin Default
Default version control: send version 2, receive version 2
  Interface      Send Recv Triggered RIP Key-chain
  Serial0/0/0    2     2
  Serial0/0/1    2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  192.168.2.0
  192.168.3.0
  192.168.4.0
Passive Interface(s):
  GigabitEthernet0/0
Routing Information Sources:
  Gateway        Distance    Last Update
  192.168.2.1     120        00:00:24
  Gateway        Distance    Last Update
  192.168.4.1     120        00:00:23
Distance: (default is 120)

```

Figure 12 (d). RIP with Passive Interfaces Feature

```

R3(config)# router rip
R3(config-router)# passive-interface default
R3(config-router)# no passive-interface s0/0/1
R3(config-router)# end
R3#
*Mar 10 16:34:28.899: %SYS-5-CONFIG_I: Configured from console by console
R3# show ip protocols | begin Default
Default version control: send version 2, receive version 2
  Interface      Send Recv Triggered RIP Key-chain
  Serial0/0/1    2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  192.168.4.0
  192.168.5.0
Passive Interface(s):
  GigabitEthernet0/0
  GigabitEthernet0/1
  GigabitEthernet0/3
Routing Information Sources:
  Gateway        Distance    Last Update
  192.168.4.2     120        00:00:23
Distance: (default is 120)

```

NOTE:

- As an alternative, all interfaces can be made passive using the **passive-interface default** command.
- Interfaces that should not be passive can be re-enabled using the **no passive-interface** command.

Figure 12 (e). RIP with Passive Interfaces Feature

G. Default Routes propagation command in RIP.

In the topology in Figure 13 (a), R1 is single-homed to a service provider. Therefore, all that is required for R1 to reach the Internet is a default static route going out of the Serial 0/0/1 interface. Similar default static routes could be configured on R2 and R3, but it is much more scalable to enter it one time on the edge router R1 and then have R1 propagate it to all other routers using RIP. To provide Internet connectivity to all other networks in the RIP routing domain, the default static route needs to be advertised to all other routers that use the dynamic routing protocol.

- To propagate a default route, the edge router must be configured with: A default static route using the **ip route 0.0.0.0 0.0.0.0 {exit-interface or /and next-hop-ip}** command.
- **The default-information originate router configuration command. This instructs R1 to originate default information, by propagating the static default route in RIP updates.**
- The example in Figure 13 (b) configures a fully specified default static route to the service provider, and then the route is propagated by RIP. Notice that R1 now has a Gateway of Last Resort and default route installed in its routing table.

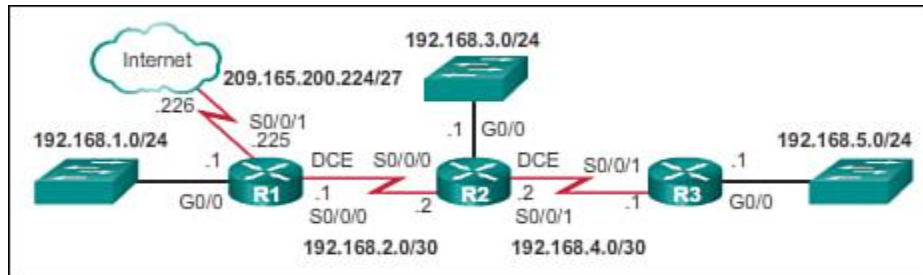


Figure 13 (a). Propagating a Default Route on R1

```
R1(config)# ip route 0.0.0.0 0.0.0.0 S0/0/1 209.165.200.226
R1(config)# router rip
R1(config-router)# default-information originate
R1(config-router)# ^z
R1#
*Mar 10 23:33:51.801: %SYS-5-CONFIG_I: Configured from console by
console
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.226 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 209.165.200.226, Serial0/0/1
  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.1.0/24 is directly connected, GigabitEthernet0/0
L   192.168.1.1/32 is directly connected, GigabitEthernet0/0
  192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.2.0/24 is directly connected, Serial0/0/0
L   192.168.2.1/32 is directly connected, Serial0/0/0
R   192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:08,
    Serial0/0/0
R   192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:08,
    Serial0/0/0
R   192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:08,
    Serial0/0/0
  209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C   209.165.200.0/24 is directly connected, Serial0/0/1
```

Figure 13 (b). Configuring and Verifying a Default Route on R1

Part IV: RIPv2 and RIPvng Commands:

A. RIP commands for IPv4:

- Configuring RIPv2 is a pretty straightforward process. Only three steps are required:
 - Enabling RIP on all routers by using the router rip global configuration command.

This command does not directly start the RIP process. Instead, it provides access to the router configuration mode where the RIP routing settings are configured. Routing updates are not sent until RIP is enabled using the network command in router configuration mode for the directly connected networks.

```
Router(config)# router rip
```

- Instructing the router to use RIPv2 by typing the version 2 command.

```
Router(config-router)# version 2
```

- Configuring the network addresses to be included in routing updates or specifying the interfaces to participate in routing updates. Thus, entering the network address for each directly connected network indicates that:

- Enabling RIP on all interfaces that belong to a specific network.
- Associated interfaces will now both send and receive RIP updates.
- **Advertising the specified network in RIP routing updates sent to other routers every 30 seconds. In order to have the directly connected networks of any router to be advertised in its periodic updates, the following command has to be considered:**

```
Router(config-router) # network {directly connected networks' ID}
```

- The first two commands are easy to comprehend, but the last command requires a little bit more thought. With the network command you specify which interfaces will participate in the routing process. Figure 2.1 shows the directly connected networks in both R1 and R2.

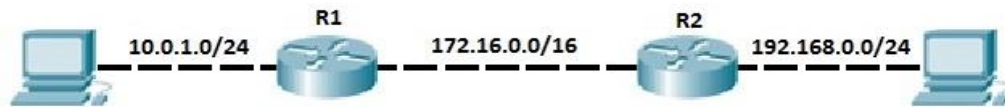


Figure 2.1. Directly connected networks to R1 and R2.

Therefore, the configuration on R1 should look like this:

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 10.0.1.0
R1(config-router)#network 172.16.0.0
```

The configuration on R2 looks similar, but with different network number for the directly connected subnet:

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 192.168.0.0
R2(config-router)#network 172.16.0.0
```

- The network command is used to specify the directly connected subnets on the router to be configured and that are intended to be included in the routing updates. This is a good time to point out that you still specify classful networks with the network command.
- In RIPv2 and EIGRP, this auto summarization behavior can be turned off (disabled) on all routers using the no auto-summary command. Moreover, manual summarization can be configured on a per interface level.

```
Router(config-router) # no auto-summary
```

- **The passive-interface command allows a router to receive routing updates on an interface but not send updates via that interface.**

```
Router(config-router) # passive-interface {interface name}
```

- **Default Routes propagation command in RIP.**

```
Router(config-router) # default-information originate
```

- After configuring RIP, we can verify routing table by typing the **show ip route** command:
 - **C** in the output indicates directly connected networks.
 - **R** in the output indicates the remote networks routes that discovered via RIP updates.
 - The legend lists **R** for all RIP routes in the routing table. Also note that the administrative distance of 120 is shown, together with the metric of 1.

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
      BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
      area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 1 subnets
C 10.0.1.0 is directly connected, FastEthernet0/0
C 172.16.0.0/16 is directly connected, FastEthernet0/1
R 192.168.0.0/24 [120/1] via 172.16.0.2, 00:00:25, FastEthernet0/1
Router#
```

- Table 2.1 presents a RIP Routing protocol configuration commands summary

Table 2.1 Summary of RIP configuration commands

Command	Description
Router(config)# router rip	Enable RIP routing protocol
Router(config-router)# network a.b.c.d	Add a.b.c.d network in RIP routing advertisement
Router(config-router)# no network a.b.c.d	Remove a.b.c.d network from RIP routing advertisement
Router(config-router)# version 2	Enable RIP routing protocol version two
Router(config-router)# no auto-summary	By default RIPv2 automatically summarize networks in their default classful boundary. This command will turn it off.
Router(config-router)# passive-interface s0/0/0	RIP will not broadcast routing update from this interface
Router(config-router) # default-information originate	propagate the static default route in RIP updates.
Router(config-router)# no ip split-horizon	Disable split horizon (Enable by default)
Router(config-router)# ip split-horizon	Enable split horizon
Router(config-router)# timers basic 30 90 180 270 360	Allow us to set RIP timer in seconds , 30 (routing update), 90 (invalid timer), 180 (Hold timer), 270 (Flush timer), 360 (sleep timer)
Router(config)# no router rip	Disable RIP routing protocol
Router# show ip rip database	Display RIP database including routes
Router# show ip route	Verify routing table
Router# show ip protocol	Verify all routing protocol status.

B. RIPng commands for IPv6:

RIPng is an extension of RIP developed for support of IPv6. The primary features of RIPng are the same as they were in IPv4. It's still a distance-vector protocol, has a maximum hop count of 15 and uses split horizon, poison reverse and other loop avoidance mechanisms. It uses hop count as the metric, sends updates every 30 seconds, RIPng messages use the UDP port 521 and the multicast address of FF02::9. But there are also some differences between the two versions. One of the most notable changes with RIPng (and all other IPv6 routing protocols), is that you enable network advertisement from interface configuration mode of a router instead of using network command in the global configuration mode. Table 2.2 summarizes the RIPng commands.

Table 2.2 Summary of RIPng configuration commands

Command	Description
Router(config)# ipv6 unicast-routing	Enables the forwarding of IPv6 unicast datagrams globally on the router.
Router(config)# ipv6 router rip <process name> <i>RIP v6</i>	Enable RIPng, the process name is used to differentiate between multiple RIP processes. It does not have to be the same on all routers in order to exchange routing information.
Router(config) # interface serial10/0/0	Moves to interface configuration mode.
Router(config-if) # ipv6 rip TOWER enable <i>↓</i> <i>RIP v6</i>	Creates the RIPng process named TOWER and enables RIPng on the interface. NOTE: Unlike RIPv1 and RIPv2, where you needed to create the RIP routing process with the router rip command and then use the network command to specify the interfaces on which to run RIP, the RIPng process is created automatically when RIPng is enabled on an interface with the ipv6 rip name enable command. TIP: Be sure that you do not misspell your process name. If you misspelled the name, you will inadvertently create a second process with the misspelled name. NOTE: Cisco IOS Software automatically creates an entry in the configuration for the RIPng routing process when it is enabled on an interface. NOTE: The ipv6 router rip process-name command is still needed when configuring optional features of RIPng.
Router(config)# ipv6 router rip TOWER	Creates the RIPng process named TOWER if it has not already been created and moves to router configuration mode.
Router(config-if) # ipv6 rip TOWER default-information originate	Announces the default route along with all other RIPng routes.
Router# show ipv6 interface	Displays the status of interfaces configured for IPv6.
Router# show ipv6 interface brief	Displays a summarized status of all interfaces along with assigned IPv6 addresses.
Router# show ipv6 neighbors	Displays IPv6 neighbor discovery cache information.
Router# show ipv6 protocols	Displays the parameters and the current state of the active IPv6 routing protocol processes.
Router# show ipv6 rip	Displays information about the current IPv6 RIPng process.
Router# show ipv6 rip database	Displays the RIPng process database. If more than one RIPng process is running, all are displayed with this command.
Router# show ipv6 route	Displays the current IPv6 routing table.
Router# show ipv6 route rip	Displays the current RIPng routes in the IPv6 routing table
Router# show ipv6 routers	Displays IPv6 router advertisement information received from other routers.

Part V: Configuring RIPv2 and RIPvng (Practical part):

A. IPv4 RIPv2 Configuration (Packet Tracer)

Consider the following scenario in Figure 2.2, which helps you practice configuring RIPv2 for IPv4 on routers, followed by the addressing table for each interface, as shown in Table 2.4.

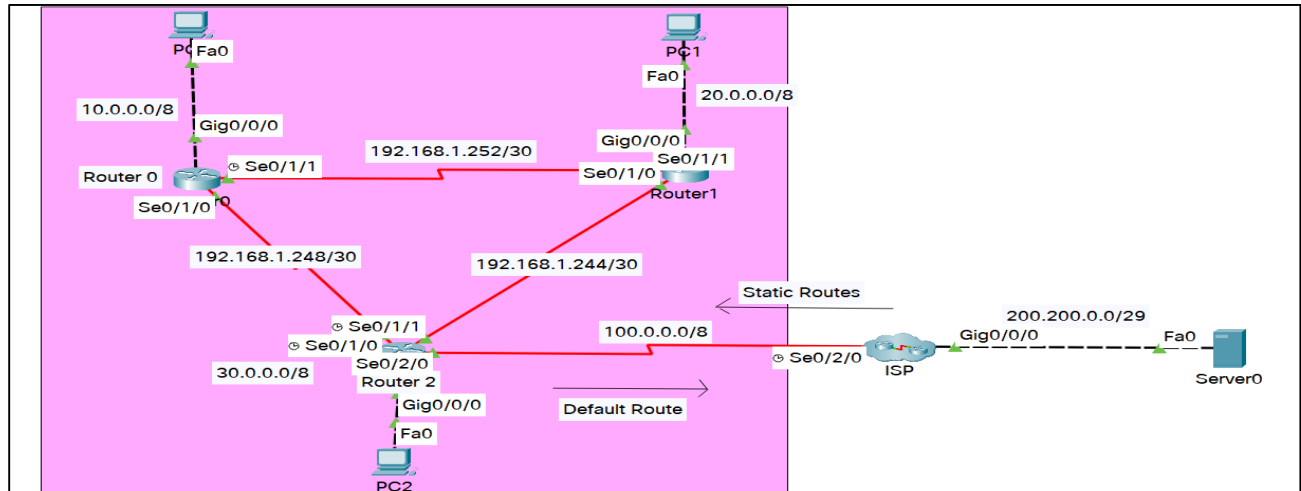


Figure 2.2. Network topology for RIPv2 routing protocol

Table 2.3. Initial IPv4 configuration

Device	Interface	IP configuration	Connected with	Default gateway
PC0	Fa 0	10.0.0.2/8	Router0' G0/0/0	10.0.0.1/8
PC1	Fa 0	20.0.0.2/8	Router1' G0/0/0	20.0.0.1/8
PC2	Fa 0	30.0.0.2/	Router2' G0/0/0	30.0.0.1/8
Server0	Fa 0	200.200.0.29	ISP' G0/0/0	200.200.0.1/29
Router 0	G0/0/0	10.0.0.1/8	PC0' Fa0	N/A
	S0/1/0	192.168.1.249/30	Router 2' S0/1/0	N/A
	S0/1/1	192.168.1.254/30	Router 1's S0/1/1	N/A
Router 1	G0/0/0	20.0.0.2/8	PC1's Fa0	N/A
	S0/1/0	192.168.1.245/30	Router'2 S0/1/1	N/A
	S0/1/1	192.168.1.253/30	Router0' S0/1/1	N/A
Router 2	G0/0/0	30.0.0.1/8	PC2's Fa0	N/A
	S0/1/0	192.168.1.250/30	Router 0' S0/1/0	N/A
	S0/1/1	192.168.1.246/30	Router 1' S0/1/0	N/A
ISP	G0/0/0	200.200.0.1/29	Server 0' Fa0	N/A
	S0/2/0	100.0.0.2/8	Router 2' S0/2/0	N/A

1. Assign IP addresses to PCs and server

Double-click **PC0**, click the **Desktop** menu item, and click **IP Configuration**. Assign the IP address 10.0.0.2/8 to PC0. Repeat the same process for PC1 and PC2 and assign the IP addresses 20.0.0.2/8 and 30.0.0.2/8, respectively. For server 0, assign the IP address 200.200.0.1/29.

2. Assign IP addresses to interfaces of routers

Double-click Router0, click CLI, and press the Enter key to access the command prompt for Router0. We need to configure an IP address and enable the interfaces before we can actually use

them for routing. To assign IP addresses, the interface mode is used, which can be accessed from the global configuration mode. **These steps are repeated for all routers.**

```
Router0>enable
Router0# configure terminal
Router0(config)#

Router0(config)#interface GigabitEthernet0/0/0
Router0(config-if)#ip address 10.0.0.1 255.0.0.0
Router0(config-if)#no shutdown
Router0(config-if)#exit

Router0(config)#interface Serial0/1/0
Router0(config-if)#ip address 192.168.1.249 255.255.255.252
Router0(config-if)#clock rate 64000
Router0(config-if)#no shutdown
Router0(config-if)#exit

Router0(config)#interface Serial0/1/1
Router0(config-if)#ip address 192.168.1.254 255.255.255.252
Router0(config-if)#clock rate 64000
Router0(config-if)#no shutdown
Router0(config-if)#exit
```

Now routers have information about the networks that they have on their own interfaces. Routers will not exchange this information between them on their own. We need to implement the RIP routing protocol, which will require them to share this information.

3. Configure RIP routing protocol

Configuration of the RIP protocol is much easier than you think. It requires only five steps to configure the RIP routing on Router 0, Router 1, and Router 2 (i.e., which appears in the pink rectangle area).

- Enable the RIP routing protocol from global configuration mode.
- Set the RIP version to 2.
- Tell the RIP which networks you want to advertise (directly connected networks).
- Disable the summarization of networks.
- Configure the LAN interface that contains no routers so that it does not send out any routing information (i.e., passive interface).

Only for router 2, we add two extra commands because it is connected to the ISP:

- Use the appropriate command to create a static default route on router 2 for all Internet traffic to exit the network through Serial0/2/0.
- Advertise the static default route configured in the previous step with other RIP routers using the "**default-information originate**" command.

The ISP router is configured with a summarized static route and LAN static routes.

Let's configure it in Router0:

```
Router0(config)#router rip
Router0(config-router)# version 2
Router0(config-router)# network 10.0.0.0
Router0(config-router)# network 192.168.1.252
```

```
Router0(config-router)# network 192.168.1.248
Router0(config-router)# no auto-summary
Router0(config-router)# passive-interface g0/0/0
```

That's all we need to configure the RIP. Follow the same steps on the remaining routers.

Let's configure it in Router1:

```
Router1(config)#router rip
Router1(config-router)# version 2
Router1(config-router)# network 20.0.0.0
Router1(config-router)# network 192.168.1.244
Router1(config-router)# network 192.168.1.252
Router1(config-router)# no auto-summary
Router1(config-router)# passive-interface g0/0/0
```

Let's configure it in Router2 :

- Note: This router is connected directly to the ISP router, so we need to add two extra commands, which are colored in red.

```
Router2(config)#router rip
Router2(config-router)# version 2
Router2(config-router)# network 30.0.0.0
Router2(config-router)# network 192.168.1.248
Router2(config-router)# network 192.168.1.244
Router2(config-router)# no auto-summary
Router2(config-router)# passive-interface g0/0/0
Router2(config-router)#default-information originate
Router2(config-router)#exit
Router2(config)#ip route 0.0.0.0 0.0.0.0 Serial0/2/0
```

Let's configure it in ISP:

- Note: This router uses static routing; we add the remote summarized networks and other remote networks (i.e., which are not summarized).

```
ISP>
ISP > enable
ISP # conf t
ISP(config)#ip route 192.168.1.240 255.255.255.240 s0/2/0
ISP(config)#ip route 10.0.0.0 255.0.0.0 s0/2/0
ISP(config)#ip route 20.0.0.0 255.0.0.0 s0/2/0
ISP(config)#ip route 30.0.0.0 255.0.0.0 s0/2/0
```

That's it. Our network is ready to take advantage of RIP routing.

4. Verify the configurations

To verify the setup, we will use the "ping" command to test the connectivity between two devices.

Step 1: View the routing tables of Router 0, Router 1, Router 2, and the ISP router.

- Use the appropriate command to show the routing table of **Router 2**. RIP (R) now appears with connected (C) and local (L) routes in the routing table, as shown in Figure 2.3. All networks have an entry. You also see a default route listed (S*).


```

Router2
Physical Config CLI Attributes
IOS Command Line Interface

Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

R 10.0.0.0/8 [120/1] via 192.168.1.249, 00:00:28, Serial0/1/0
R 20.0.0.0/8 [120/1] via 192.168.1.245, 00:00:19, Serial0/1/1
C 30.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 30.0.0.0/8 is directly connected, GigabitEthernet0/0/0
L 30.0.0.1/32 is directly connected, GigabitEthernet0/0/0
C 100.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 100.0.0.0/8 is directly connected, Serial0/2/0
L 100.0.0.1/32 is directly connected, Serial0/2/0
L 192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
C 192.168.1.244/30 is directly connected, Serial0/1/1
L 192.168.1.246/32 is directly connected, Serial0/1/1
C 192.168.1.248/30 is directly connected, Serial0/1/0
L 192.168.1.250/32 is directly connected, Serial0/1/0
R 192.168.1.252/30 [120/1] via 192.168.1.249, 00:00:28, Serial0/1/0
[120/1] via 192.168.1.245, 00:00:19, Serial0/1/1
S* 0.0.0.0/0 is directly connected, Serial0/2/0

```

Figure 2.3. The routing table of router 2 after configuring the RIP and static default route.

- View the routing tables for **Router 0**. Notice that, as presented in Figure 2.4, Router 0 has a full listing of all the directly connected networks and a default route. The **R* route** means that there is a default route that can be reached through Serial 0/1/0. The route source for this path is the RIP routing protocol.

```

Router0
Physical Config CLI Attributes
IOS Command Line Interface

Router>en
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 192.168.1.250 to network 0.0.0.0

C 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.0.0.0/8 is directly connected, GigabitEthernet0/0/0
L 10.0.0.1/32 is directly connected, GigabitEthernet0/0/0
R 20.0.0.0/8 [120/1] via 192.168.1.253, 00:00:02, Serial0/1/1
R 30.0.0.0/8 [120/1] via 192.168.1.250, 00:00:02, Serial0/1/0
R 192.168.1.0/24 [120/1] via 192.168.1.253, 00:00:02, Serial0/1/1
R 192.168.1.244/30 [120/1] via 192.168.1.250, 00:00:02, Serial0/1/0
C 192.168.1.246/32 is directly connected, Serial0/1/0
L 192.168.1.249/32 is directly connected, Serial0/1/0
C 192.168.1.252/30 is directly connected, Serial0/1/1
R* 0.0.0.0/0 [120/1] via 192.168.1.250, 00:00:02, Serial0/1/0
Router#

```

Figure 2.4. The routing table of router 2 after configuring the RIP and static default route.

- View the routing tables for the **ISP Router**. Notice that, as shown in Figure 2.5, each router has a full listing of all the directly connected networks and the static routes.

```

ISP
Physical Config CLI Attributes
IOS Command Line Interface

Router>en
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

S 10.0.0.0/8 is directly connected, Serial0/2/0
S 20.0.0.0/8 is directly connected, Serial0/2/0
S 30.0.0.0/8 is directly connected, Serial0/2/0
C 100.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 100.0.0.0/8 is directly connected, Serial0/2/0
L 100.0.0.2/32 is directly connected, Serial0/2/0
L 100.0.0.1/32 is directly connected, Serial0/2/0
S 192.168.1.240/28 is directly connected, Serial0/2/0
C 200.200.0.0/24 is variably subnetted, 2 subnets, 2 masks
C 200.200.0.0/29 is directly connected, GigabitEthernet0/0/0
L 200.200.0.1/32 is directly connected, GigabitEthernet0/0/0
Router#

```

Figure 2.5. The routing table of ISP after configuring static routes.

Step 2: Verify full connectivity to all destinations.

- Every device should now be able to ping every other device inside the network. In addition, all devices should be able to ping the Web Server, as shown in Figures 2.6 and 2.7.

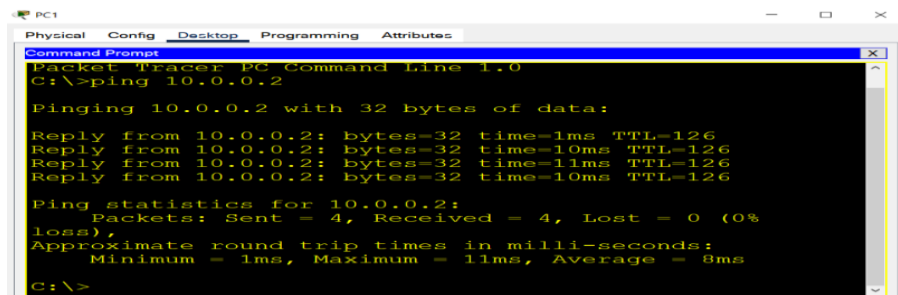


Figure 2.6. The successful ping results (Ping PC0 from PC2).

























Fire	Last Status	Source	Destination	Type	Color	Time(se	Periodic	Num	
	Successful	PC0	PC1	ICMP		0.000	N	0	
	Successful	PC0	PC2	ICMP		0.000	N	1	
	Successful	PC0	Server0	ICMP		0.000	N	2	
Fire	Last Status	Source	Destination	Type	Color	Time(se	Periodic	Num	
	Successful	PC1	PC0	ICMP		0.000	N	0	
	Successful	PC1	PC2	ICMP		0.000	N	1	
	Successful	PC1	Server0	ICMP		0.000	N	2	
Fire	Last Status	Source	Destination	Type	Color	Time(se	Periodic	Num	Edit
	Successful	PC2	PC0	ICMP		0.000	N	0	(edit)
	Successful	PC2	PC1	ICMP		0.000	N	1	(edit)
	Successful	PC2	Server0	ICMP		0.000	N	2	(edit)
Fire	Last Status	Source	Destination	Type	Color	Time(se	Periodic	Num	Edit
	Successful	Server0	PC0	ICMP		0.000	N	0	(edit)
	Successful	Server0	PC1	ICMP		0.000	N	1	(edit)
	Successful	Server0	PC2	ICMP		0.000	N	2	(edit)

Figure 2.7. The successful ping results for each device in the network.

B. Configuring IPv4 for any routing protocol (i.e., RIP) using CIDR:

Here, we can use a CIDR to configure any given routing protocol. In this example, for the network topology given in Figure 2.8, you have been given the following network address: 172.16.0.0/20. Consider that the default gateway IP addresses of the hosts (i.e., the routers' LAN interfaces) are included in the hosts' number. Moreover, Table 2.6 demonstrates the complete process of calculating the IP addresses.

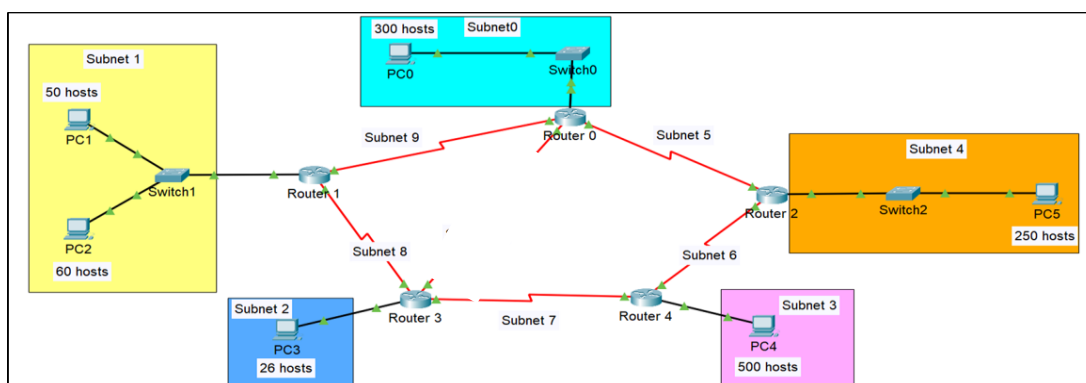


Figure 2.8. The network topology for the classless IP address.

Instructions to assign the IP address:

- For each **LAN** (Sub0, Sub1, Sub2, Sub3, and Sub4):
 - ✓ Assign the **last** valid host address in each subnet to the **LAN interface** of each Router.
 - ✓ Assign the **first** valid host address in each subnet to the **PC** in the corresponding subnet.
- For each **WAN** (Sub5, Sub6, Sub7, Sub8, and Sub9):
 - ✓ Assign the **first** valid host address in each subnet to **the WAN interface on the Router that has a smaller suffix number.**
 - ✓ Assign the **last** valid host address in each subnet **to the WAN interface on Router that has a higher suffix number.**
- ✓ For instance, Sub8 contains Route 1 and Router 3. Thus, the WAN interface of Router1 will be assigned the first valid host address, since Router 1 has a smaller suffix number, while the WAN interface of Router 3 will be assigned the last valid host address of Sub8.

Table 2.4. CIDR IP addressing configuration

Net #	# of hosts	# of required bits	# of required host	CIDR	Subnet mask	Network ID	Broadcast ID	Host Range
Subnet 3	500	9	512	23	255.255.254.0	172.16.0.0	172.16.1.255	172.16.0.1-172.16.1.254
Subnet 0	300	9	512	23	255.255.254.0	172.16.2.0	172.16.3.255	172.16.2.1-172.16.3.254
Subnet 4	250	8	256	24	255.255.255.0	172.16.4.0	172.16.4.255	172.16.4.1-172.16.4.254
Subnet 1	110	7	128	25	255.255.255.128	172.16.5.0	172.16.5.127	172.16.5.1-172.16.5.126
Subnet 2	26	5	32	27	255.255.255.224	172.16.5.128	172.16.5.159	172.16.5.129-172.16.5.158
Subnet 5	2	2	4	30	255.255.255.252	172.16.5.160	172.16.5.163	172.16.5.161-172.16.5.162
Subnet 6	2	2	4	30	255.255.255.252	172.16.5.164	172.16.5.167	172.16.5.165-172.16.5.166
Subnet 7	2	2	4	30	255.255.255.252	172.16.5.168	172.16.5.171	172.16.5.169-172.16.5.170
Subnet 8	2	2	4	30	255.255.255.252	172.16.5.172	172.16.5.175	172.16.5.173-172.16.5.174
Subnet 9	2	2	4	30	255.255.255.252	172.16.5.176	172.16.5.179	172.16.5.177-172.16.5.178

C. Configuring IPv6 RIPng (Practical part):

Figure 2.9 illustrates the network topology for the configuration that follows, which shows how to configure IPv6 and RIPng using the commands covered in this handout.

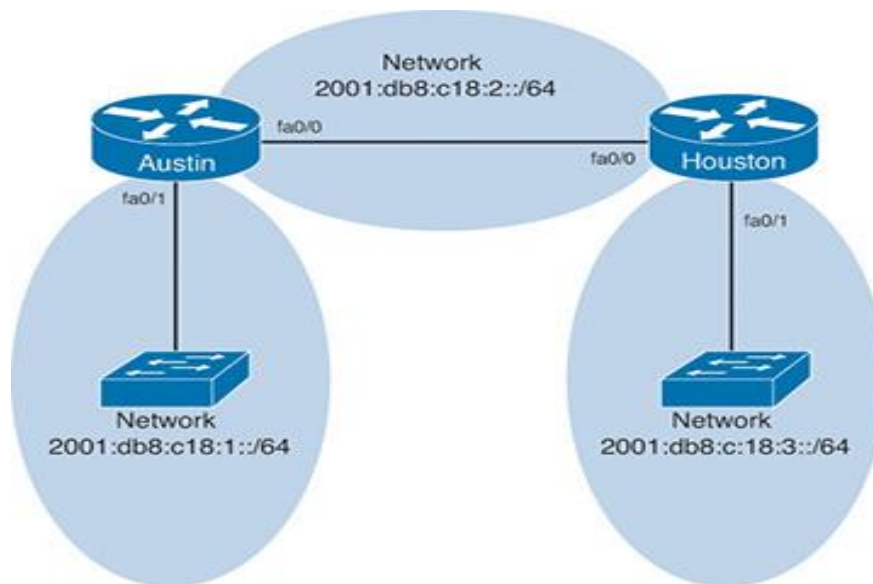


Figure 2.9. Network Topology for IPv6/RIPng Configuration Example

Austin Router configuration:

Router> enable	Moves to privileged mode
Router# configure terminal	Moves to global configuration mode
Router (config)# ipv6 unicast-routing	Enables the forwarding of IPv6 unicast datagrams globally on the router
Router (config)# interface fastethernet0/0	Enters interface configuration mode
Router (config-if)# ipv6 address 2001:db8:c18:2::/64 eui-64	Configures a global IPv6 address with an EUI-64 interface identifier in the low-order 64 bits of the IPv6 address
Router (config-if)# ipv6 rip TOWER enable	Creates the RIPng process named TOWER and enables RIPng on the interface
Router (config-if)# no shutdown	Activates the interface
Router (config-if)# interface fastethernet0/1	Enters interface configuration mode
Router (config-if)# ipv6 address 2001:db8:c18:1::/64 eui-64	Configures a global IPv6 address with an EUI-64 interface identifier in the low-order 64 bits of the IPv6 address
Router (config-if)# ipv6 rip TOWER enable	Creates the RIPng process named TOWER and enables RIPng on the interface
Router (config-if)# no shutdown	Activates the interface

Houston Router Configuration:

Router> enable	Moves to privileged mode
Router# configure terminal	Moves to global configuration mode
Router (config)# ipv6 unicast-routing	Enables the forwarding of IPv6 unicast datagrams globally on the router
Router (config)# interface fastethernet0/0	Enters interface configuration mode

Router (config-if)# ipv6 address 2001:db8:c18:2::/64 eui-64	Configures a global IPv6 address with an EUI-64 interface identifier in the low-order 64 bits of the IPv6 address
Router (config-if)# ipv6 rip TOWER enable	Creates the RIPng process named TOWER and enables RIPng on the interface
Houston(config-if)# no shutdown	Activates the interface
Router (config-if)# interface fastethernet 0/1	Enters interface configuration mode
Router (config-if)# ipv6 address 2001:db8:c18:3::/64 eui-64	Configures a global IPv6 address with an EUI-64 interface identifier in the low-order 64 bits of the IPv6 address
Router (config-if)# ipv6 rip TOWER enable	Creates the RIPng process named TOWER and enables RIPng on the interface
Router (config-if)# no shutdown	Activates the interface

Important Note: Some parts of this handout have been collected from several trustable sites, books, and published videos/slides and the other parts have been prepared and written by the instructors. As a matter of fact, this handout is made to be so straight forward, understandable, and so attractive whereas the students can do the required activities and solve the problems in a systematic and easy way, but still the instructors are expected to discuss some important material during the labs' sessions.