Over the years, routing protocols have evolved to meet the increasing demands of complex networks. The first protocol used was Routing Information Protocol (RIP). RIP still enjoys popularity because of its simplicity and widespread support.

Understanding RIP is important to your networking studies for two reasons. First, RIP is still in use today. You may encounter a network implementation that is large enough to need a routing protocol, yet simple enough to use RIP effectively. Second, familiarity with many of the fundamental concepts of RIP will help you to compare RIP with other protocols. Understanding how RIP operates and its implementation will make learning other routing protocols easier.

RIP Historical Impact

RIP is the oldest of the distance vector routing protocols. Although RIP lacks the sophistication of more advanced routing protocols, its simplicity and continued widespread use is a testament to its longevity. RIP is not a protocol "on the way out." In fact, an IPv6 form of RIP called RIPng (next generation) is now available.

RIP evolved from an earlier protocol developed at Xerox, called Gateway Information Protocol (GWINFO). With the development of Xerox Network System (XNS), GWINFO evolved into RIP. It later gained popularity because it was implemented in the Berkeley Software Distribution (BSD) as a daemon named routed (pronounced "route-dee", not "rout-ed"). Various other vendors made their own, slightly different implementations of RIP. Recognizing the need for standardization of the protocol, Charles Hedrick wrote RFC 1058 in 1988, in which he documented the existing protocol and specified some improvements. Since then, RIP has been improved with RIPv2 in 1994 and with RIPng in 1997.

RIP Characteristics

As discussed in "Distance Vector Routing Protocols," RIP has the following key characteristics:

RIP is a distance vector routing protocol.

RIP uses hop count as its only metric for path selection.

Advertised routes with hop counts greater than 15 are unreachable.

Messages are broadcast every 30 seconds.

The data portion of a RIP message is encapsulated into a UDP segment, with both source and destination port numbers set to 520. The IP header and data link headers add broadcast destination addresses before the message is sent over RIP

Message Format: RIP Header

Three fields are specified in the four byte header. The Command field specifies the message type, discussed in more detail in the next section. The Version field is set to 1 for RIP version 1. The third field is labeled Must be zero. "Must be zero" fields provide room for future expansion of the protocol.

RIP Message Format: Route Entry

The route entry portion of the message includes three fields with content: Address family identifier (set to 2 for IP unless a router is requesting a full routing table, in which case the field is set to zero), IP address, and Metric. This route entry portion represents one destination route with its associated metric. One RIP update can contain up to 25 route entries. The maximum datagram size is 504 bytes, not including the IP or UDP headers.

Why are there so many fields set to zero?

RIP was developed before IP and was used for other network protocols (like XNS). BSD also had its influence. Initially, the extra space was added with the intention of supporting larger address spaces in the future. As we will see in Chapter 7, RIPv2 has now used most of these empty fields.

RIP Request/Response Process

RIP uses two message types specified in the Command field: Request message and Response message.

Each RIP-configured interface sends out a request message on startup, requesting that all RIP neighbors send their complete routing tables. A response message is sent back by RIP-enabled neighbors. When the requesting router receives the responses, it evaluates each route entry. If a route entry is new, the receiving router installs the route in the routing table. If the route is already in the table, the existing entry is replaced if the new entry has a better hop count. The startup router then sends a triggered update out all RIP-enabled interfaces containing its own routing table so that RIP neighbors can be informed of any new routes.

RIP is a classful routing protocol. As you may have realized from the previous message format discussion, RIPv1 does not send subnet mask information in the update. Therefore, a router either uses the subnet mask configured on a local interface, or applies the default subnet mask based on the address class. Due to this limitation, RIPv1 networks cannot be discontiguous nor can they implement VLSM.

As you know from Chapter 3, "Introduction to Dynamic Routing Protocols," administrative distance (AD) is the trustworthiness (or preference) of the route source. RIP has a default administrative distance of 120. When compared to other interior gateway protocols, RIP is the least-preferred routing protocol. IS-IS, OSPF, IGRP, and EIGRP all have lower default AD values.

To enable a dynamic routing protocol, enter the global configuration mode and use the router command.If you type a space followed by a question mark, a list of all the available routing protocols supported by the IOS displays.

To enter the router configuration mode for RIP, enter router rip at the global configuration prompt. Notice that the prompt changes from a global configuration prompt to the following:

R1(config-router)#

This command does not directly start the RIP process. Instead, it provides access to configure routing protocol settings. No routing updates are sent.

If you need to completely remove the RIP routing process from a device, negate the command with no router rip. This command stops the RIP process and erases all existing RIP configurations.

By entering the RIP router configuration mode, the router is instructed to run RIP. But the router still needs to know which local interfaces it should use for communication with other routers, as well as which locally connected networks it should advertise to those routers. To enable RIP routing for a network, use the network command in the router configuration mode and enter the classful network address for each directly connected network.

Router(config-router)#network directly-connected-classful-network-address

The network command:

Enables RIP on all interfaces that belong to a specific network. Associated interfaces will now both send and receive RIP updates.

Advertises the specified network in RIP routing updates sent to other routers every 30 seconds.

Note: If you enter a subnet address, the IOS automatically converts it to a classful network address. For example, if you enter the command network 192.168.1.32, the router will convert it to network 192.168.1.0.

In the figure, the network command is configured on all three routers for the directly connected networks. Notice that only classful networks were entered.

What happens if you enter a subnet address or interface IP address instead of the classful network address when using the network command for RIP configurations?

R3(config)#router rip

R3(config-router)#network 192.168.4.0

R3(config-router)#network 192.168.5.1

In this example, we entered an interface IP address instead of the classful network address. Notice that the IOS does not give an error message. Instead, the IOS corrects the input and enters the classful network address. This is proven with the verification below.

R3#show running-config

!

router rip

network 192.168.4.0

network 192.168.5.0

!

Powerful Troubleshooting Commands

To verify and troubleshoot routing, first use show ip route and show ip protocols. If you cannot isolate the problem using these two commands, then use debug ip rip to see exactly what is happening. These three commands are discussed in a suggested order that you might use to verify and troubleshoot a routing protocol configuration. Remember, before you configure any routing - whether static or dynamic - make sure all necessary interfaces are "up" and "up" with the show ip interface brief command.

The show ip route command verifies that routes received by RIP neighbors are installed in a routing table. An R in the output indicates RIP routes. Because this command displays the entire routing table, including directly connected and static routes, it is normally the first command used to check for convergence. Routes may not immediately appear when you execute the command because networks take some time to converge. However, once routing is correctly configured on all routers, the show ip route command will reflect that each router has a full routing table, with a route to each network in the topology.

nterpreting show ip protocols Output

If a network is missing from the routing table, check the routing configuration using show ip protocols. The show ip protocols command displays the routing protocol that is currently configured on the router. This output can be used to verify most RIP parameters to confirm that:

RIP routing is configured

The correct interfaces send and receive RIP updates

The router advertises the correct networks

RIP neighbors are sending updates

This command is also very useful when verifying the operations of other routing protocols, as we will see later with EIGRP and OSPF.

Interpreting debug ip rip Output

Most RIP configuration errors involve an incorrect network statement configuration, a missing network statement configuration, or the configuration of discontiguous subnets in a classful environment. As shown in the figure, an effective command used to find issues with RIP updates is the debug ip rip. This command displays RIP routing updates as they are sent and received. Because updates are periodic, you need to wait for the next round of updates before seeing any output.

Unnecessary RIP Updates Impact Network

As you saw in the previous example, R2 is sending updates out FastEthernet0/0 even though no RIP device exists on that LAN. R2 has no way of knowing this and, as a result, sends an update every 30 seconds. Sending out unneeded updates on a LAN impacts the network in three ways:

1. Bandwidth is wasted transporting unnecessary updates. Because RIP updates are broadcast, switches will forward the updates out all ports.

2. All devices on the LAN must process the update up to the Transport layers, where the receiving device will discard the update.

3. Advertising updates on a broadcast network is a security risk. RIP updates can be intercepted with packet sniffing software. Routing updates can be modified and sent back to the router, corrupting the routing table with false metrics that misdirect traffic.

Stopping Unnecessary RIP Updates

You might think you could stop the updates by removing the 192.168.3.0 network from the configuration using the no network 192.168.3.0 command, but then R2 would not advertise this LAN as a route in updates sent to R1 and R3. The correct solution is to use the passive-interface command, which prevents the transmission of routing updates through a router interface but still allows that network to be advertised to other routers. Enter the passive-interface command in router configuration mode.

Router(config-router)#passive-interface interface-type interface-number

This command stops routing updates out the specified interface. However, the network that the specified interface belongs to will still be advertised in routing updates that are sent out other interfaces.

In the figure, R2 is first configured with the passive-interface command to prevent routing updates on FastEthernet0/0 because no RIP neighbors exist on the LAN. The show ip protocols command is then used to verify the passive interface. Notice that the interface is no longer listed under Interface, but under a new section called Passive Interface(s). Also notice that the network 192.168.3.0 is still listed under Routing for Networks, which means that this network is still included as a route entry in RIP updates that are sent to R1 and R3.

Rules for Processing RIPv1 Updates

The following two rules govern RIPv1 updates:

If a routing update and the interface on which it is received belong to the same major network, the subnet mask of the interface is applied to the network in the routing update.

If a routing update and the interface on which it is received belong to different major networks, the classful subnet mask of the network is applied to the network in the routing update.

Advantages of Automatic Summarization

As we saw with R2 in the previous figure, RIP automatically summarizes updates between classful networks. Because the 172.30.0.0 update is sent out an interface (Serial 0/0/1) on a different classful network (192.168.4.0), RIP sends out only a single update for the entire classful network instead of one for each of the different subnets. This process is similar to what we did when summarized several static routes into a single static route. Why is automatic summarization an advantage?

Smaller routing updates sent and received, which uses less bandwidth for routing updates between R2 and R3.

R3 has a single route for the 172.30.0.0/16 network, regardless of how many subnets there are or how it is subnetted. Using a single route results in a faster lookup process in the routing table for R3.

Is there a disadvantage to automatic summarization? Yes, when there are discontiguous networks configured in the topology.

Disadvantage of Automatic Summarization

As you can see in the figure, the addressing scheme has been changed. This topology will be used to show a main disadvantage with classful routing protocols like RIPv1 - their lack of support for discontiguous networks.

Classful routing protocols do not include the subnet mask in routing updates. Networks are automatically summarized across major network boundaries since the receiving router in unable to determine the mask of the route. This is because the receiving interface may have a different mask than the subnetted routes.

Notice that R1 and R3 both have subnets from the 172.30.0.0/16 major network, whereas R2 does not. Essentially, R1 and R3 are boundary routers for 172.30.0.0/16 because they are separated by another major network, 209.165.200.0/24. This separation creates a discontiguous network, as two groups of 172.30.0.0/24 subnets are separated by at least one other major network. 172.30.0.0/16 is a discontiguous network.

Adding Internet Access to the Topology

RIP was the first dynamic routing protocol and was used extensively in early implementations between customers and ISPs, as well as between different ISPs. But in today's networks, customers do not necessarily have to exchange routing updates with their ISP. Customer routers that connect to an ISP do not need a listing for every route on the Internet. Instead, these routers have a default route that sends all traffic to the ISP router when the customer router does not have a route to a destination. The ISP configures a static route pointing to the customer router for addresses inside the customer's network.

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. You could configure a static default route on R1 pointing to R2, but this technique is not scalable. With every router added to the RIP routing domain, you would have to configure another static default route. Why not let the routing protocol do the work for you?

In many routing protocols, including RIP, you can use the default-information originate command in router configuration mode to specify that this router is to originate default information, by propagating the static default route in RIP updates. In the figure, R2 has been configured with the default-information originate command. Notice from the debug ip rip output that it is now sending a "quad-zero" static default route to R1.