Interior Gateway Routing Protocols

- An Interior gateway routing protocol is used to determine how routing is performed within an autonomous system (AS). These routing protocols are also known as Intra-AS routing protocols.
- Two most popular routing protocols that have been used extensively for routing within an autonomous system in the Internet are :
- Routing Information Protocol (RIP), and
- Open Shortest Path First (OSPF).

Administrative Distance

- The administrative distance (AD) is used to rate the trustworthiness of routing information received on a router from a neighbor router.
- An administrative distance is an integer from 0 to 255, where 0 is the most trusted and 255 means no traffic will be passed via this route.
- If multiple routing protocols are configured (e.g. static route, RIP, EIGRP, OSPF) on a routers' interface and it receives two updates listing the same remote network, the first thing the router checks is the AD. If one of the advertised routes has a lower AD than the other, then the route with the lowest AD will be placed in the routing table.
- If both advertised routes to the same network have the same AD, then routing protocol metrics (such as hop count or bandwidth of the lines) will be used to find the best path to the remote network. The advertised route with the lowest metric will be placed in the routing table. But if both advertised routes have the same AD as well as the same metrics, then the routing protocol will load balance to the remote network (which means that it sends packets down each link).

Routing Information Protocol - Basics

- The Routing Information Protocol (RIP) was one of the first interior routing protocols used in TCP/IP. RIP is a distance vector protocol and uses Bellman Ford routing algorithm.
- In distance vector routing algorithm, each router passes complete routing table contents to neighboring routers, which then combine the received routing table entries with their own routing tables to complete the router's routing table.
- This is called routing by rumor because a router receiving an update from a neighbor router believes the information about remote networks without actually finding out for itself.
- RIP uses only hop count to determine the best path to a network. If RIP finds more than one link with the same hop count to the same remote network, it will automatically perform a round robin load balancing.
- RIP has a maximum allowable hop count of 15 by default, meaning that hop count of 16 is defined as infinity and considered as unreachable. Thus, RIP works well in small networks, but it's inefficient on large networks with a large number of routers installed.
- RIP version 1 uses only classful routing, which means that all devices in the network must use the same subnet mask. This is because RIP version 1 doesn't send updates with subnet mask information. RIP version 2 provides classless routing and does send subnet mask information with the route updates.
- Default AD of RIP is 120.

RIP Routing Information

- Like any routing protocol, the job of RIP is to provide a mechanism for exchanging information about routes so routers can keep their routing tables up to date.
- Each router in an RIP internetwork keeps track of all the networks in its routing table. For each network or host, following information is included:
  - The address of the network or host.
  - The distance from that router to the network or host.
  - The first hop for the route: the device to which datagrams must be sent first to eventually get to the destination network or host.
- Routing information is propagated between routers in RIP approximately every 30 seconds using a RIP response message. RIP response messages are also known as RIP advertisements.
- This RIP response message sent by a router specifies what networks it can reach, and how many hops to reach them. Other routers directly connected to it know that they can then reach those networks through that router at a cost of one additional hop.
- So if router A sends a message saying it can reach network X for a cost of N hops, each other router that connects directly to A can reach network X for a cost of $N + 1$ hops. It will put that information into its routing table, unless it knows of an alternate route through another router that has a lower cost.

RIP Timers

- RIP uses four different kinds of timers to regulate its performance:
- Route update timer - Sets the interval between periodic routing updates in which the router sends a complete copy of its routing table out to all neighbors.
- This process ensures that route information is regularly sent around the internet, so routers are always kept up to date about routes.
- The default value of update timer is 30 seconds.

RIP Timers

- Route invalid timer – When a router receives routing information and enters it into its routing table, that information cannot be considered valid indefinitely.
- Route invalid timer determines the length of time that must elapse before a router determines that a route has become invalid.
- Whenever the router receives a RIP Response with information about that route, the route is considered refreshed and its invalid timer is reset. As long as the route continues to be refreshed, the timer will never expire.
- If, however, RIP Responses containing that route stop arriving, the timer will eventually expire. When this happens, the route is marked for deletion, by setting the distance for the route to 16 (which indicates an unreachable network).
- It will come to this conclusion if it hasn't heard any updates about a particular route for that period. When that happens, the router will send out updates to all its neighbors letting them know that the route is invalid.
- The default value for the invalid timer is usually 180 seconds. This allows several periodic updates of a route to be missed before a router will conclude that the route is no longer reachable.

RIP Timers

- Route flush timer - When a route is marked for deletion, route flush timer is also started.
- This sets the time between a route becoming invalid and its removal from the routing table. The reason for using this two stage removal method is to give the router (that declared the route no longer reachable) a chance to propagate this information to other routers.
- Until the route flush timer expires, the router will include that route, with the unreachable metric of 16 hops, in its own RIP Responses, so other routers are informed of the problem with that route. When the timer expires the route is deleted.
- If during the route flush timer period, a new RIP Response for the route is received, then the deletion process is aborted, route flush timer is cleared, the route is marked as valid again, and a new invalid timer starts.
- The default value for this timer is 240(180+60) seconds. The value of the route invalid timer must be less than that of the route flush timer. This gives the router enough time to tell its neighbors about the invalid route before the local routing table is updated.

RIP Timers

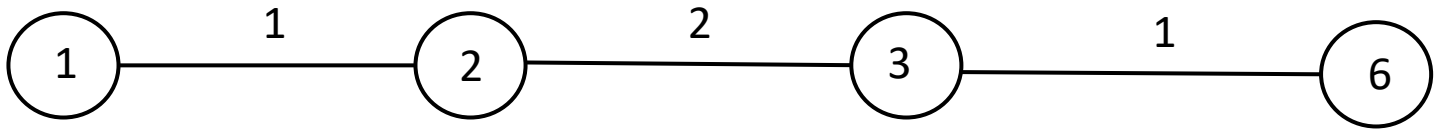
- Hold down timer - The hold down feature works by having each router start a timer when they first receive information about a network that is unreachable.
- This sets the amount of time during which routing information is suppressed. Routes will enter into the hold down state when an update packet is received that indicates the route is unreachable.
- This continues either until an update packet is received with a better metric, the original route comes back up, or the hold down timer expires.
- The default value for this timer is 180 seconds.

RIP Limitations & Problems

- The simplicity of the Routing Information Protocol is often considered as the main reason for its popularity but it also has some limitations and weakness. They are:
- Slow Convergence – In distance vector algorithm, all routers share all their routing information regularly so that all routers eventually end up with the same information about the location of networks and which are the best routes to use to reach them. This is called convergence.
- RIP algorithm is rather slow to achieve convergence. It takes a long time for all routers to get the same information, and in particular, it takes a long time for information about topology changes to propagate.
- Consider the worst case situation of two networks separated by 15 routers. Since routers send RIP Response messages only every 30 seconds, a change to one of this pair of networks might not be seen by the router nearest the other one until many minutes have elapsed.
- The slow convergence problem is even more pronounced when it comes to the propagation of route failures. Failure of a route is only detected through the expiration of the 180 second invalid timer, so that adds up to three minutes more delay before convergence can even begin.

RIP Limitations & Problems

- Consider the given example network
- Assume that all nodes are switched on at the same time $t = 0$
- Immediately after being switched on, each node informs its neighbors about its presence.
- Each node transmits its distance vector message every 60 seconds
- After receiving the distance vector messages the shortest path computations takes one second
- Calculate the time of convergence of this example network.

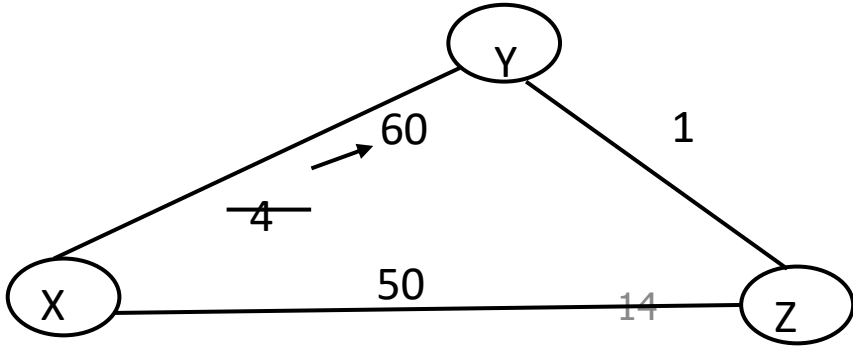


RIP Limitations & Problems

- The simplicity of the Routing Information Protocol is often considered as the main reason for its popularity but it also has some limitations and weakness. They are:
- Routing Loops - A routing loop occurs when in order to get to x, y routes through z, and z routes through y. (Ref. See Slide 16-17 Lecture 9-1)
- Larger loops can also exist: Router x says to send to y, which says to send to z, which says to send to t.
- Routing loops can occur in DV protocols e.g. after link failure or major increase in a link metric.
- RIP does not include any specific mechanism to detect or prevent routing loops; the best it can do is try to avoid them.

RIP Limitations & Problems

- The simplicity of the Routing Information Protocol is often considered as the main reason for its popularity but it also has some limitations and weakness. They are:
- Count to Infinity – Node z informs node y about its new cost (which is now 7) and subsequently node y re-calculates its cost to 8. Node y informs node z about its new cost (which is now 8) and subsequently node z re-calculates its cost to 9 and so on.
- The loop will persist i.e. message exchanges between y and z until z eventually computes the cost of its path to x via y to be greater than 50. At this point, z will determine that its least cost path to x is via its direct connection to x. y will then route to x via z.
- The result of the bad news about the increase in link cost has indeed traveled slowly. This problem is referred as count to infinity problem.

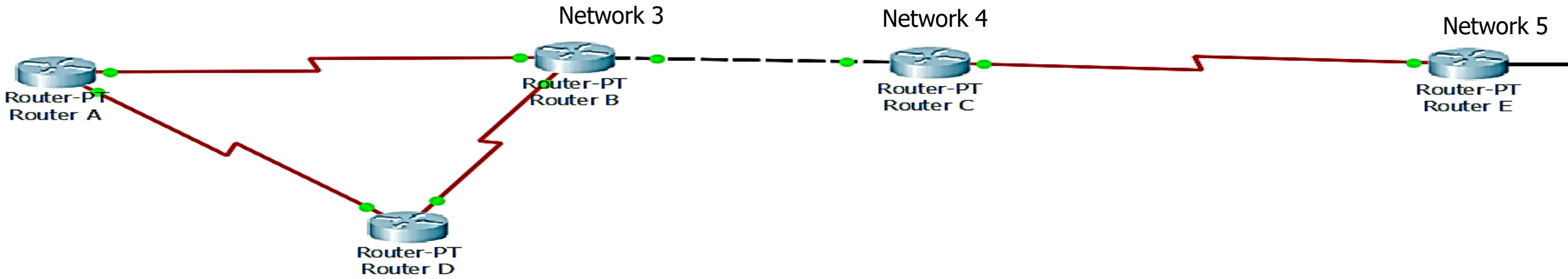


Techniques to Resolve RIP Problems

- Four techniques are used as a solution to problems that arise due to RIP. They are:
- Split Horizon – When a router sends out an RIP Response on any of the networks to which it is connected, it omits any route information that was originally learned from that network. This feature is called split horizon.
- This reduces incorrect routing information and routing overhead in a distance vector network.
- In other words, the routing protocol differentiates which interface a network route was learned on, and once this is determined, it won't advertise the route back out that same interface.
- This would have prevented Router z from sending the update information it received from Router y back to Router y.

Techniques to Resolve RIP Problems

- Split Horizon With Poisoned Reverse - This is an enhancement of the basic split horizon feature. Instead of omitting routes learned from a particular interface when sending RIP Response messages on that interface, we include those routes but set their metric to RIP infinity, 16.
- The poisoned reverse refers to the fact that we are poisoning the routes that we want to make sure routers on that interface don't use.
- For example, when Network 5 goes down, Router E initiates route poisoning by advertising Network 5 with a hop count of 16, or unreachable. This poisoning of the route to Network 5 keeps Router C from being susceptible to incorrect updates about the route to Network 5. When Router C receives a route poisoning from Router E, it sends an update, called a poison reverse, back to Router E. This ensures that all routers on the segment have received the poisoned route information.



Techniques to Resolve RIP Problems

- Triggered Updates – A routing loop occurs when in order to get to x, y routes through z, and z routes through y. Another aspect of the problem is that router had to wait up to 30 seconds until its next scheduled transmission time to tell other routers about the failure/link increase.
- For RIP to work well, whenever a router changes the metric for a route it is required to immediately send out an RIP Response to tell its immediate neighbor routers about the change. If these routers, seeing this change, update their routing information, they are in turn required to send out updates.
- Thus, the change of any network route information causes cascading updates to be sent throughout the internetwork, significantly reducing the slow convergence problem.

Techniques to Resolve RIP Problems

- Hold Down - Split horizon tries to solve the counting to infinity problem by suppressing the transmission of invalid information about routes that fail. For extra insurance, we can implement a feature that changes how devices receiving route information process it in the case of a failed route.
- The hold down feature works by having each router start a timer when they first receive information about a network that is unreachable.
- Until the timer expires, the router will discard any subsequent route messages that indicate the route is in fact reachable. A typical hold down timer runs for 180 seconds.
- The main advantage of this technique is that a router won't be confused by receiving spurious information about a route being accessible when it was just recently told that the route was no longer valid.
- Hold downs prevent routes from changing too rapidly by allowing time for either the downed route to come back up or the network to stabilize somewhat before changing to the next best route.