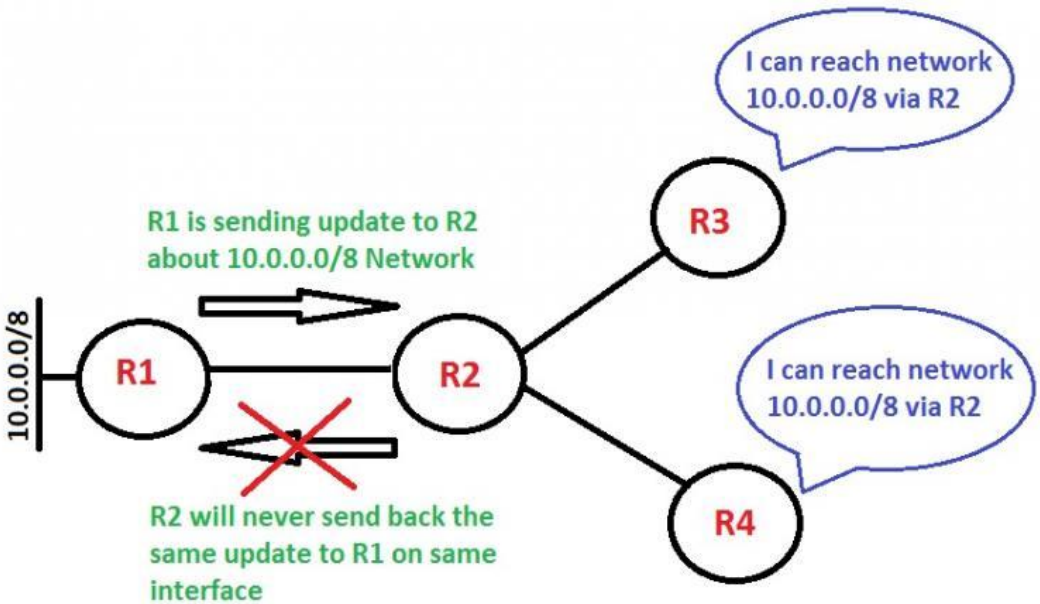
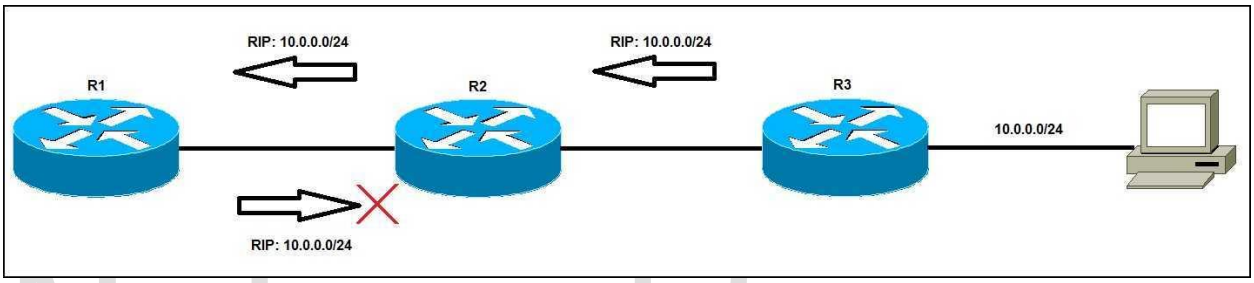

Networkforyou
Welcome
To
Network for you
Split Horizon
Networkforyou

What is the split-horizon?

- **Split-horizon is a feature that prevents a router from advertising a route back out the same interface where the router originally learned the route**. Routing protocols use this feature along with other features to remove routing loops.
- **Split horizon is a method used by distance vector protocols to prevent network routing loops. The basic principle is simple: Never send routing information back in the direction from which it was received.**
- Why do we need split horizon? Because distance vector protocols, such as Routing Information Protocol (RIP), are susceptible to routing loops, which occur when a data packet is caught in an endless circle and continuously routed through the same routers. To avoid these loops, the protocols often rely on split horizon. Other types of protocols, such as Open Shortest Path First, use different mechanisms to deter packet looping.
- When enabled, split horizon prevents a router from advertising a route back to the router from which it learned a route. In other words, if a router receives routing information from another router, the first router will not broadcast that information back to the second router, thus preventing routing loops from occurring.

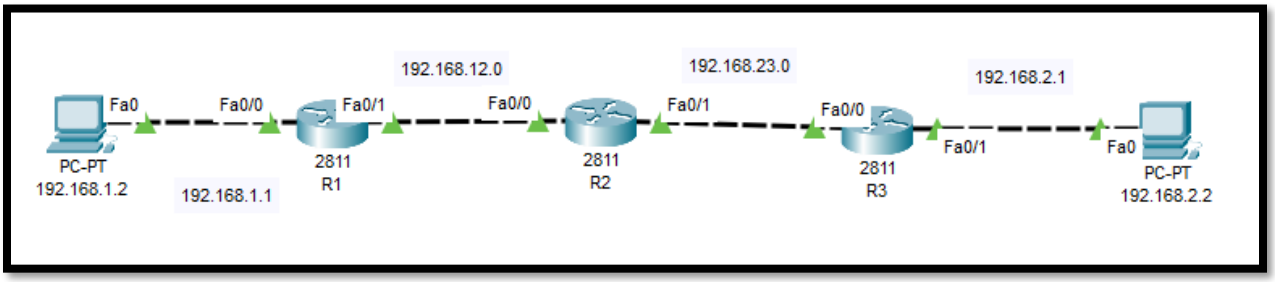


- Distance vector protocols are susceptible to routing loops. Routing loops occur when a packet is continually routed through the same routers over and over, in an endless circle. Because they can render a network unusable, distance vector routing protocols (such as RIP and EIGRP) employ several different mechanisms to prevent routing loops.
- Split horizon is one of the methods used by distance vector routing protocols to avoid routing loops. The principle is simple – a router will not advertise a route back onto the interface from which it was learned. Split horizon is enabled on interfaces by default.
- To consider what could happen without the split horizon mechanism, take a look at the following example:



- We have a network of three routers. All routers are running RIP, a distance vector protocol. R3 is directly connected to the 10.0.0.0/24 network and advertises that network using RIP to R2. R2 receives the routing update, places the route in its routing table and informs R1 about the 10.0.0.0/24. Because the split horizon mechanism is enabled by default on all interfaces, R1 will not advertise to R2 that it has the route to 10.0.0.0/24.
- Now consider what would happen if the split horizon mechanism didn't prevent R1 to advertise the route back to R2. R1 would advertise to R2 that it has a route to reach the 10.0.0.0/24. Let's say that the link between the R2 and R3 fails. Since R2 received a route to that network from R1, it will send all packets destined for the 10.0.0.0/24 network to R1. But R1 thinks that R2 has a route to reach that network (it doesn't know that the link between R2 and R3 failed) and sends the packets back to R2, thereby creating a routing loop.

Lab Time:



R1 Configuration:	**R2 Configuration:**
en config t hostname R1 int f0/0 ip add 192.168.1.1 255.255.255.0 no sh int f0/1 ip add 192.168.12.1 255.255.255.0 no sh router rip network 192.168.1.0 network 192.168.12.0	en config t hostname R2 int f0/0 ip add 192.168.12.2 255.255.255.0 no sh int f0/1 ip add 192.168.23.2 255.255.255.0 no sh router rip network 192.168.23.0 network 192.168.12.0
R3 Configuration:	
en config t hostname R3 int f0/1 ip add 192.168.2.1 255.255.255.0 no sh int f0/0 ip add 192.168.23.3 255.255.255.0 no sh router rip network 192.168.2.0	

network 192.168.23.0	

By default Split Horizon is enabling:

Disable Split Horizon
R1(config)#int range f0/0-1 R1(config-if-range)#no ip split-horizon

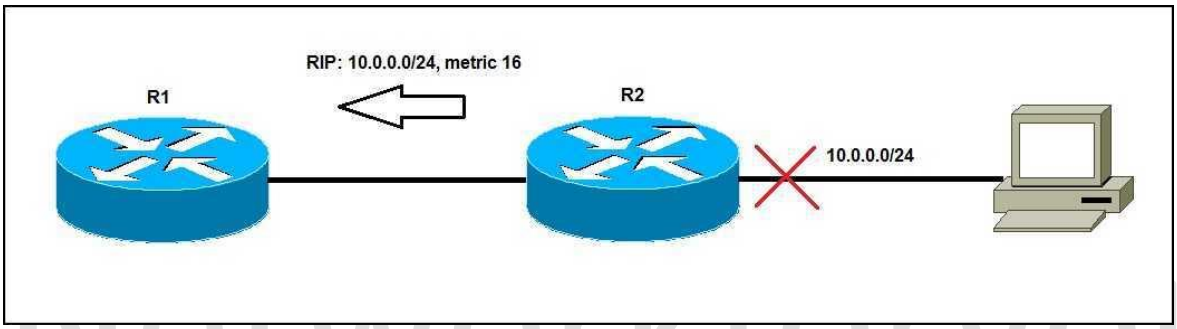
After Disabling Split Horizon we will have loop in network.

We can check in router R2 by enable **debug ip rip**.

```
RIP: sending  v1 update to 255.255.255.255 via FastEthernet0/1
(192.168.23.2)
RIP: build update entries
      network 192.168.1.0 metric 2
      network 192.168.2.0 metric 2
      network 192.168.12.0 metric 1
      network 192.168.23.0 metric 1
RIP: received v1 update from 192.168.23.3 on FastEthernet0/1
      192.168.1.0 in 3 hops
      192.168.2.0 in 1 hops
      192.168.12.0 in 2 hops
      192.168.23.0 in 1 hops
RIP: received v1 update from 192.168.12.1 on FastEthernet0/0
      192.168.1.0 in 1 hops
      192.168.2.0 in 3 hops
      192.168.12.0 in 1 hops
      192.168.23.0 in 2 hops
```

Route poisoning explained:

- Another method employed by distance vector routing protocols to prevent routing loops is route poisoning.
- When a router detects that one of its directly connected routes has failed, it will advertise a failed route with an infinite metric ("poisoning the route").
- Routers who receive the routing update will consider the route as failed and remove it from their routing tables.
- Each routing protocol has its own definition of an infinite metric. In the case of RIP the infinite metric is 16.



To better understand how route poisoning works, consider the following example:

We have a network of two routers. Both routers are running RIP. R2 has advertised the 10.0.0.0/24 network to R1. Now consider what happens when the network 10.0.0.0/24 fails:

1. R2 removes the route to 10.0.0.0/24 from its routing table.

2. R2 advertises the 10.0.0.0/24 network with an infinitive metric (16) to R1 ("route poisoning").

Route poisoning is a method used in computer networking to prevent routing loops. **A routing loop occurs when a packet is sent around a closed path in a network, never reaching its destination**. **Route poisoning is used to prevent this by advertising a route as unreachable to all other routers in the network.** This prevents the route from being used in routing calculations, and helps to prevent routing loops.

Route poisoning is typically used in distance-vector routing protocols, such as RIP. In these protocols, routers share routing information with each other. If a router learns about a route that is **unreachable**, it will poison the route by advertising it as unreachable to all other routers. This ensures that the route will not be used in routing calculations, and helps to prevent routing loops.

Tagging: This mechanism allows you to tag routes with a specific identifier. This can be used to filter routes or to prevent them from being poisoned.

Filtering: This mechanism allows you to block specific routes from being advertised to other routers. This can be used to prevent routing loops or to protect your network from unauthorized access. This can be done by configuring the ip access-list command on the router.