Chapter 5

Routing Information Protocol (RIP)

5.1 Basics of Dynamic Routing

Routing is the act of forwarding network packets from a source network to a destination network. This is a straightforward concept in principle. In practice, you must take into account a variety of considerations to insure the successful delivery of packets:

- When should you route?
- What is the best route?
- How is the best route determined?
- What if the network topology changes?
- What if there is a network fault?
- What if the destination does not exist?

Routing occurs when a packet must be forwarded off its originating network. Any packet with a destination network number that differs from the local network number is, by definition, destined for another network and must therefore be forwarded to the target network. A router is the designated networking device for forwarding packets between networks. Only a router has the internetwork information and the logic required to make the correct decision about how best to forward the packet.

TABLE I A simplified routing table

CODE	NETWORK, MASK	AD/METRIC	NEXT HOP	INTERFACE
O	10.0.0.0 /8	110/20	200.1.1.1	S0
O	172.16.0.0 /16	110/15	200.1.1.1	S0
O	192.168.1.0 /24	110/20	200.2.2.2	S1
C	210.1.1.4 /30	0/0	Directly connected	E0

A Simplified routing table is shown in Table I. There are six key elements to each routing entry:

- Code: An abbreviation indicating what process (directly connected, any protocol or static route) discovered the route.
- Network, Mask: Indicates the address of the destination network and its subnet mask.
- Administrative distance/Metric: Used to select the best route if more than one path to a network exists (covered in the next section).
- Next hop: IP address of the next router the packet will be forwarded to (specifically, the address of the interface of the next hop router that shares a network segment with an interface on the source router).
- Interface: The interface the packet will be forwarded out of.

Populating Route Tables

Route tables are populated through one of the following three sources:

- Directly connected networks
- Network paths statically (manually) entered into the route table
- Through one or more dynamic routing protocols

Directly Connected Networks

Any network directly connected to the interface of a router is automatically added to the route table. Whatever IP address and mask were configured for the interface are used to populate the table entry.

Static and Dynamic Routing

Aside from directly connected networks, route tables can only be populated with network paths in one of two ways: the route is manually entered by an administrator, or the router figures out network paths on its own by talking to other routers. A manually entered route is known as a static route. Such routing is suitable for very small networks. On the other hand, dynamic routes are routes a router learns from other routers via a routing protocol such as RIP, IGRP, EIGRP, OSPF, or BGP. Routing protocols run as processes on routers. They exchange information about the networks in the system and automatically populate route tables. Dynamic routing is suitable for networks of any size.

Task of dynamic routing protocols

Dynamic routing protocols are used by routers to share information about the reachability and status of remote networks. Dynamic routing protocols perform several activities, including the following:

■ Network discovery

■ Updating and maintaining routing tables

Automatic Network Discovery

Network discovery is a routing protocol's capability to share information about the networks it knows about with other routers that are also using the same routing protocol. Instead of configuring static routes to remote networks on every router, a dynamic routing protocol allows the routers to automatically learn about these networks from other routers. These networks and the best path to each network are added to the router's routing table and denoted as a network learned by a specific dynamic routing protocol.

Maintaining Routing Tables

After the initial network discovery, dynamic routing protocols will also update and maintain the networks in their routing tables. Dynamic routing protocols not only make a best-path determination to various networks but also determine a new best path if the initial path becomes unusable (or if the topology changes). For these reasons, dynamic routing protocols have an advantage over static routes. Routers that use dynamic routing protocols automatically share routing information with other routers and compensate for any topology changes without involving the network administrator.

Routing Table Principles

At times, this course refers to three principles regarding routing tables that will help you understand, configure, and troubleshoot routing issues. These principles are as follows:

- Every router makes its decision alone, based on the information it has in its own routing table.
- The fact that one router has certain information in its routing table does not mean that other routers have the same information.
- Routing information about a path from one network to another does not provide routing information about the reverse, or return, path.

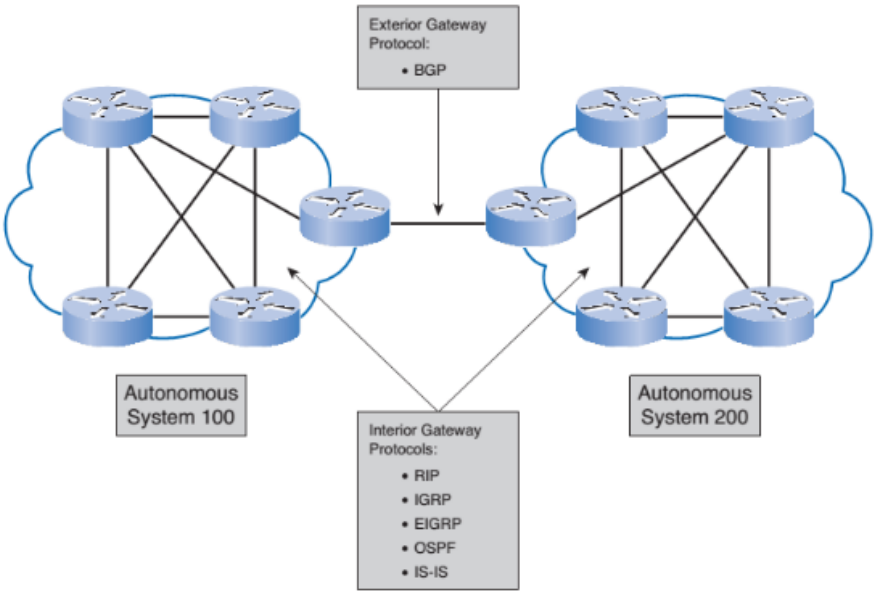


Fig. 5.1 IGP versus EGP routing protocols

Classifying Dynamic protocols

IGP and EGP

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 are

- *Interior gateway protocols (IGP):* Used for intra-autonomous system routing, that is, routing inside an autonomous system
- *Exterior gateway protocols (EGP):* Used for inter-autonomous system routing, that is, routing between autonomous systems

Fig. 5.1 is a simplified view of the difference between IGPs and EGPs. The autonomous system concept will be explained in more detail later in the chapter. Even though this is an oversimplification, for now, think of an autonomous system as an ISP.

Distance Vector and Link-State Routing Protocols

Interior gateway protocols (IGP) can be classified as two types:

- Distance vector routing protocols
- Link-state routing protocols

Distance Vector Routing Protocol Operation

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 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.

Distance vector protocols use routers as signposts along the path to the final destination. The only information a router knows about a remote network is the distance or metric to reach that network and which path or interface to use to get there. Distance vector routing protocols do not have an actual map of the network topology.

Distance vector protocols work best in situations where

- The network is simple and flat and does not require a hierarchical design.
- The administrators do not have enough knowledge to configure and troubleshoot linkstate protocols.
- Specific types of networks, such as hub-and-spoke networks, are being implemented.
- Worst-case convergence times in a network are not a concern.

Link-State Protocol Operation

In contrast to distance vector routing protocol operation, a router configured with a link-state routing protocol can create a "complete view," or topology, of the network by gathering information from all the other routers. Think of using a link-state routing protocol as having a complete map of the network topology. The signposts along the way from source to destination are not necessary, because all link-state routers are using an identical "map" of the network. A link-state router uses the link-state information to create a topology map and to select the best path to all destination networks in the topology.

With some distance vector routing protocols, routers send periodic updates of their routing information to their neighbors. Link-state routing protocols do not use periodic updates. After the network has converged, a link-state update is only sent when there is a change in the topology.

Link-state protocols work best in situations where

- The network design is hierarchical, usually occurring in large networks.
- The administrators have a good knowledge of the implemented link-state routing protocol.
- Fast convergence of the network is crucial.

TABLE II Default administrative distance of different protocols

Route Source	AD
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

Administrative Distance

Administrative distance (AD) defines the preference of a routing source. 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. Table II shows the default administrative distance of different routing protocols.

5.2 RIP

Routing Information Protocol (RIP) was originally specified in RFC 1058. It has the following key characteristics:

- Hop count is used as the metric for path selection.
- If the hop count for a network is greater than 15, RIP cannot supply a route to that network.
- Routing updates are broadcast or multicast every 30 seconds, by default.
- If for some reason, an update for a particular route is not received within a period of 180 seconds then that specific route is declared as invalid and the router which identified that, informs all its neighbors about this invalid route.

At the core of the distance vector protocol is the algorithm, which is used to calculate the best paths. Routers then send this information to neighboring routers. The algorithm used for the routing protocols defines the following processes:

- Mechanism for sending and receiving routing information
- Mechanism for calculating the best paths and installing routes in the routing table
- Mechanism for detecting and reacting to topology changes

Versions of RIP

RIP has two versions: version 1 and version 2. The version 1 is most elementary level dynamic routing protocol while the version 2 is free from many of the limitations of version 1. Differences between the two versions are given below:

1. RIPv1 uses classful addressing and fixed length subnet mask (FLSM) while RIPv2 supports classful addressing, FLSM and variable length subnet mask (VLSM).

2. Version 1 of RIP uses broadcasting (to 255.255.255.255) to send RIP messages to every neighbor. In this way, all the routers on the network receive the packets, as well as the hosts. RIP version 2, on the other hand, uses the all-router multicast address (224.0.0.9) to send the RIP messages only to RIP routers in the network.

3. RIPv2 sends and receives version 2 updates only. RIPv1 sends version 1 updates and receives both 1 and 2, however version 2 information is ignored.

4. RIPv2 ensure authentication, while RIPv1 does not.

Network Discovery

Network discovery is part of the process of the routing protocol algorithm that enables routers to first learn about remote networks.

Cold Start

When a router cold-starts or powers up, it knows nothing about the network topology. It does not even know that there are devices on the other end of its links. The only information that a router has is from its own saved configuration file stored in NVRAM. After a router boots successfully, it applies the saved configuration. If the IP addressing is configured correctly and active, the router will initially discover its own directly connected networks.

After a cold start and before the exchange of routing information, the routers initially discover their own directly connected networks and subnet masks. As shown in Fig. 5.2, this information is added to their routing tables:

- R1:
  - 10.1.0.0 available through interface FastEthernet 0/0
  - 10.2.0.0 available through interface Serial 0/0/0
- R2:
  - 10.2.0.0 available through interface Serial 0/0/0
  - 10.3.0.0 available through interface Serial 0/0/1
- R3:
  - 10.3.0.0 available through interface Serial 0/0/0
  - 10.4.0.0 available through interface FastEthernet 0/0

Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0

Fig.5.2 Network discovery: cold start

With this initial information, the routers start to exchange routing information.

Initial Exchange of Routing Information

If a routing protocol is configured, the routers begin exchanging routing updates, as shown in Fig. 5.3. Initially, these updates include information only about their directly connected networks. Upon receiving an update, the router checks it for new information. Any routes that are not currently in its routing table are added.

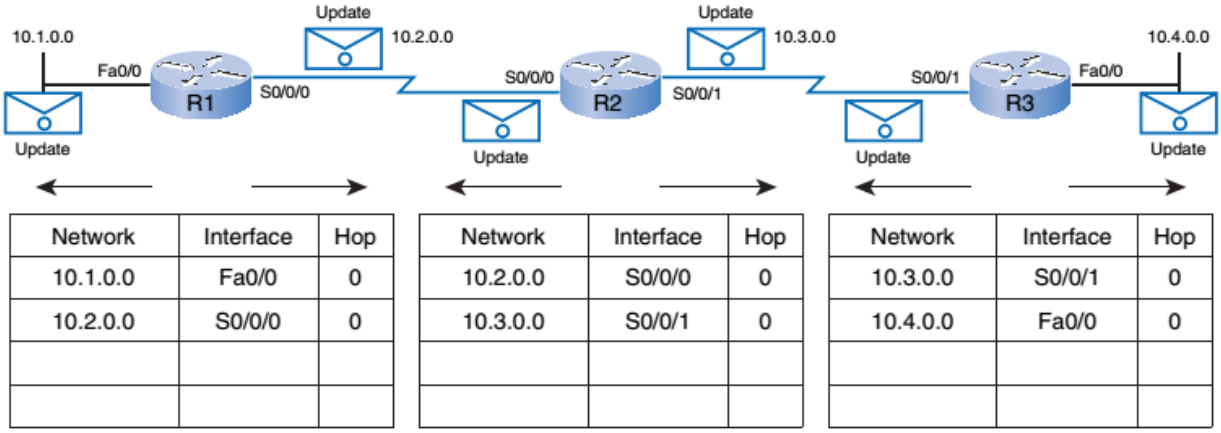


Fig.5.3 Network Discovery: Initial Exchange of Routing Updates

In Fig. 5.3, Routers R1, R2, and R3 start their initial exchange. All three routers send their routing tables to their neighbors, which at this point only contain the directly connected networks.

Each router processes updates in the following manner:

- R1:
  - Sends an update about network 10.1.0.0 out the Serial 0/0/0 interface with a metric of 1
  - Sends an update about network 10.2.0.0 out the FastEthernet 0/0 interface with a metric of 1
  - Receives an update from R2 about network 10.3.0.0 on Serial 0/0/0 with a metric of 1
  - Stores network 10.3.0.0 in the routing table with a metric of 1
- R2:
  - Sends an update about network 10.3.0.0 out the Serial 0/0/0 interface with a metric of 1
  - Sends an update about network 10.2.0.0 out the Serial 0/0/1 interface with a metric of 1
  - Receives an update from R1 about network 10.1.0.0 on Serial 0/0/0 with a metric of 1
  - Stores network 10.1.0.0 in the routing table with a metric of 1
  - Receives an update from R3 about network 10.4.0.0 on Serial 0/0/1 with a metric of 1
  - Stores network 10.4.0.0 in the routing table with a metric of 1

- R3:
  - Sends an update about network 10.4.0.0 out the Serial 0/0/1 interface with a metric of 1
  - Sends an update about network 10.4.0.0 out the FastEthernet 0/0 interface with a metric of 1
  - Receives an update from R2 about network 10.2.0.0 on Serial 0/0/1 with a metric of 1
  - Stores network 10.2.0.0 in the routing table with a metric of 1

As shown in Fig. 5.4, after this first round of update exchanges, each router knows about the connected networks of its directly connected neighbors.

Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

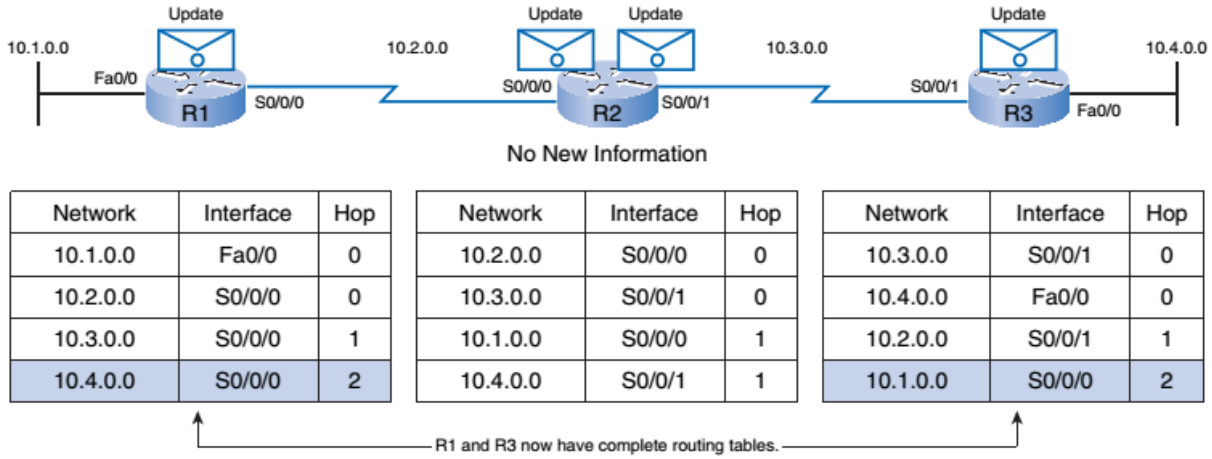
Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1

Fig. 5.4 Network Discovery: Updated Tables After Initial Exchange

Exchange of Routing Information

At this point, the routers have knowledge about their own directly connected networks and about the connected networks of their immediate neighbors. Continuing the journey toward convergence, the routers exchange the next round of periodic updates. Each router again checks the updates for new information.

In Fig. 5.5, R1, R2, and R3 send their latest routing tables to their neighbors.



Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/0	2

Fig. 5.5 Network Discovery—Next Update

Each router processes updates in the following manner:

- R1:
  - Sends an update about network 10.1.0.0 out the Serial 0/0/0 interface with a metric of 1.
  - Sends an update about networks 10.2.0.0 with a metric of 1 and 10.3.0.0 with a metric of 2 out the FastEthernet 0/0 interface.
  - Receives an update from R2 about network 10.4.0.0 on Serial 0/0/0 with a metric of 2.

- Stores network 10.4.0.0 in the routing table with a metric of 2.
- Same update from R2 contains information about network 10.3.0.0 on Serial 0/0/0 with a metric of 1. There is no change; therefore, the routing information remains the same.

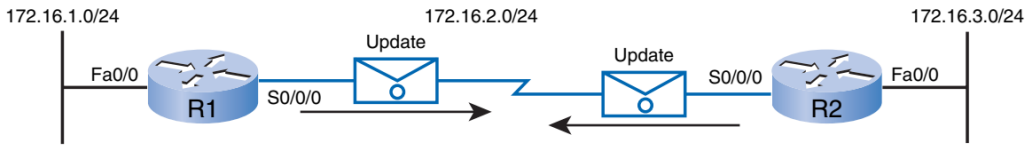
- R2:
  - Sends an update about networks 10.3.0.0 with a metric of 1 and 10.4.0.0 with a metric of 2 out the Serial 0/0/0 interface.
  - Sends an update about networks 10.1.0.0 with a metric of 2 and 10.2.0.0 with a metric of 1 out the Serial 0/0/1 interface.
  - Receives an update from R1 about network 10.1.0.0 on Serial 0/0/0. There is no change; therefore, the routing information remains the same.
  - Receives an update from R3 about network 10.4.0.0 on Serial 0/0/1. There is no change; therefore, the routing information remains the same.
- R3:
  - Sends an update about network 10.4.0.0 out the Serial0/0/1 interface.
  - Sends an update about networks 10.2.0.0 with a metric of 2 and 10.3.0.0 with a metric of 1 out the FastEthernet 0/0 interface.
  - Receives an update from R2 about network 10.1.0.0 on Serial 0/0/1 with a metric of 2.
  - Stores network 10.1.0.0 in the routing table with a metric of 2.
  - Same update from R2 contains information about network 10.2.0.0 on Serial 0/0/1 with a metric of 1. There is no change; therefore, the routing information remains the same.

Convergence

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.

In Fig. 5.6 R1 and R2 are configured with RIP. The algorithm sends and receives updates. Both R1 and R2 then glean new information from the update. In this case, each router learns about a new network, as shown in Fig. 5.7. The new networks are highlighted. The algorithm on each router makes its calculations independently and updates the routing table with the new information.

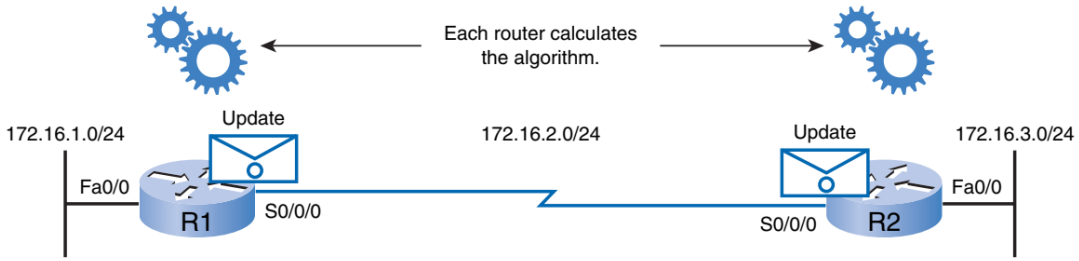
Fig. 5.8 illustrates what happens when there is a topology change. When the LAN on R2 goes down, the algorithm constructs a “triggered” update and sends it to R1. R1 then removes the network from the routing table.



Network	Interface	Hop
172.16.1.0/24	Fa0/0	0
172.16.2.0/24	S0/0/0	0

Network	Interface	Hop
172.16.2.0/24	S0/0/0	0
172.16.3.0/24	Fa0/0	0

Fig.5.6 Sending and receiving update

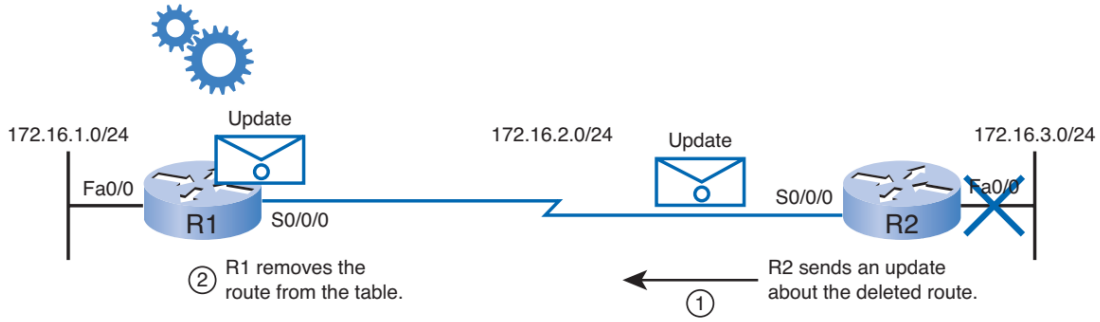


Network	Interface	Hop
172.16.1.0/24	Fa0/0	0
172.16.2.0/24	S0/0/0	0
172.16.3.0/24	S0/0/0	1

New routes are installed.

Network	Interface	Hop
172.16.2.0/24	S0/0/0	0
172.16.3.0/24	Fa0/0	0
172.16.1.0/24	S0/0/0	1

Fig. 5.7 Calculating the best path and installing routes



172.16.3.0/24 Down

Network	Interface	Hop
172.16.1.0/24	Fa0/0	0
172.16.2.0/24	S0/0/0	0
~~172.16.3.0/24~~	~~S0/0/0~~	~~1~~

Network	Interface	Hop
172.16.2.0/24	S0/0/0	0
~~172.16.3.0/24~~	~~Fa0/0~~	~~0~~
172.16.1.0/24	S0/0/0	1

Fig. 5.8 Detecting and reacting to topology changes

The speed of achieving convergence consists of

- How quickly the routers propagate a change in the topology in a routing update to their neighbors
- The speed of calculating best-path routes using the new routing information collected

A network is not completely operable until it has converged. Therefore, network administrators prefer routing protocols with shorter convergence times.