Dynamic Routing

The data networks that we use in our everyday lives to learn, play, and work range from small, local networks to large, global internetworks. A home network may have a router and two or more computers. At work, an organization may have multiple routers and switches servicing the data communication needs of hundreds, or even thousands, of end devices.

Routers forward packets by using information in the routing table. Routes to remote networks can be learned by the router in two ways: static routes and dynamic routes. In a large network with numerous networks and subnets, configuring and maintaining static routes between these networks requires a great deal of administrative and operational overhead. This operational overhead is especially cumbersome when changes to the network occur, such as a failed link or implementing a new subnet. The use of dynamic routing protocols can ease the burden of configuration and maintenance tasks, and give the network infrastructure scalability.

This chapter introduces dynamic routing protocols. It explores the benefits of using dynamic routing protocols, how different routing protocols are classified, and the metrics routing protocols use to determine the best path for network traffic. In addition, the characteristics of dynamic routing protocols, and the differences between the various routing protocols, will be examined. Network professionals must understand the different routing protocols available in order to make informed decisions about when to use static routing, dynamic routing, or both. They also need to know which dynamic routing protocol is most appropriate in a particular network

environment.

Sections & Objectives

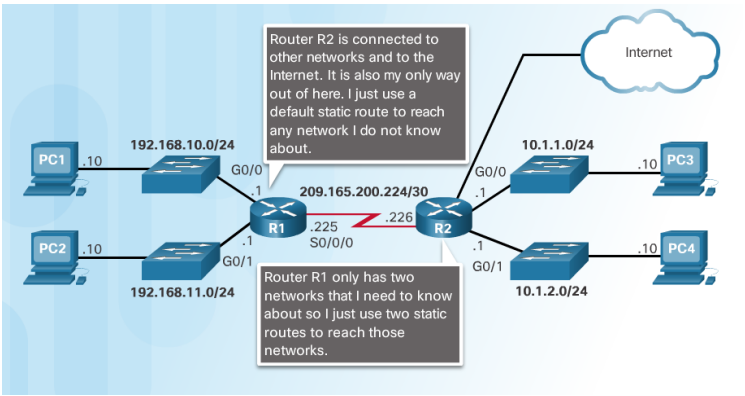
- Dynamic Routing Protocols
  - Explain the features and characteristics of dynamic routing protocols.
    - Compare the different types of routing protocols.
- Distance Vector Dynamic Routing
  - Explain how distance vector routing protocols operate.
    - Explain how dynamic routing protocols achieve convergence.
    - Describe the algorithm used by distance vector routing protocols to determine the best path.
    - Identify the types of distance-vector routing protocols.
- Link-State Dynamic Routing
  - Explain how link-state protocols operate.
    - Describe the algorithm used by link-state routing protocols to determine the best path.
    - Explain how the link-state routing protocol uses information sent in a link-state update.
    - Explain the advantages and disadvantages of using link-state routing protocols.

Dynamic Routing Protocols

Dynamic versus Static Routing

Static Routing Uses

- Networks often use both static and dynamic routing.
- Static Routing is used as follows:
  - For easy routing table maintenance in small networks.
  - Routing to and from a stub network.
  - Accessing a single default route.



Static Routing Uses

Before identifying the benefits of dynamic routing protocols, consider the reasons why network professionals use static routing. Dynamic routing certainly has several advantages over static routing; however, static routing is still used in networks today. In fact, networks typically use a combination of both static and dynamic routing. Static routing has several primary uses, including:

- Providing ease of routing table maintenance in smaller networks that are not expected to grow significantly.
- Routing to and from a stub network, which is a network with only one default route out and no knowledge of any remote networks.
- Accessing a single default route (which is used to represent a path to any network that does not have a more specific match with another route in the routing table).

The figure provides a sample scenario of static routing.

Dynamic versus Static Routing

Static Routing Advantages and Disadvantages

Advantages	Disadvantages
Easy to implement in a small network.	Suitable only for simple topologies or for special purposes such as a default static route.
Very secure. No advertisements are sent as compared to dynamic routing protocols.	Configuration complexity increases dramatically as network grows.
Route to destination is always the same.	Manual intervention required to re-route traffic.
No routing algorithm or update mechanism required; therefore, extra resources (CPU or RAM) are not required.	

Static Routing Advantages and Disadvantages

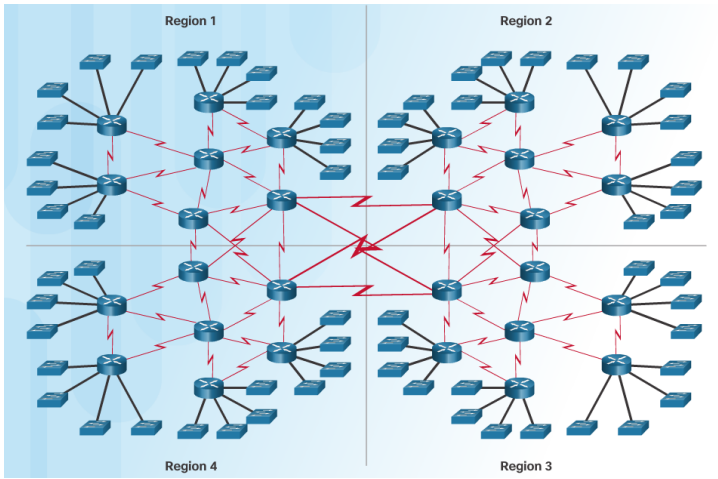
The table in the figure highlights the advantages and disadvantages of static routing. Static routing is easy to implement in a small network. Static routes stay the same, which makes them fairly easy to troubleshoot. Static routes do not send update messages; therefore, they require very little overhead.

The disadvantages of static routing include:

- They are not easy to implement in a large network.
- Managing the static configurations can become time consuming.
- If a link fails, a static route cannot reroute traffic.

Dynamic versus Static Routing

Dynamic Routing Protocols Uses



- Dynamic routing is the best choice for large networks
- Dynamic routing protocols help the network administrator manage the network:
  - Providing redundant paths
  - Automatically implementing the alternate path when a link goes down.

Dynamic Routing Protocols Uses

Dynamic routing protocols help the network administrator manage the time-consuming and exacting process of configuring and maintaining static routes.

Imagine maintaining the static routing configurations for the seven routers of the Region 1, in Figure.

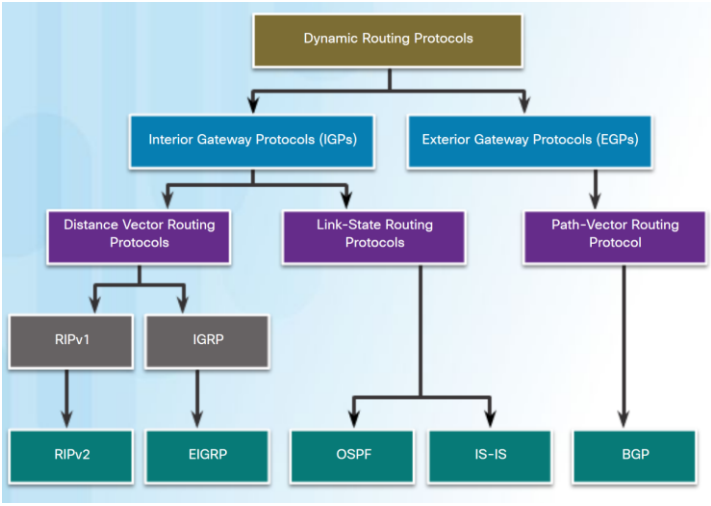
What if the company grew and now had four regions and 28 routers to manage, as shown in Figure? What happens when a link goes down? How do you ensure that redundant paths are available?

Dynamic routing is the best choice for large networks like the one shown.

Types of Routing Protocols

Classifying Routing Protocols

- The purpose of dynamic routing protocols includes:
  - Discovery of remote networks.
  - Maintaining up-to-date routing information.
  - Choosing the best path to destination networks.
  - Ability to find a new best path if current path is no longer available.



Classifying Routing Protocols

Dynamic routing protocols are used to facilitate the exchange of routing information between routers. A routing protocol is a set of processes, algorithms, and messages that are used to exchange routing information and populate the routing table with the routing protocol's choice of best paths. The purpose of dynamic routing protocols includes:

- Discovery of remote networks
- Maintaining up-to-date routing information
- Choosing the best path to destination networks
- Ability to find a new best path if the current path is no longer available

Routing protocols can be classified into different groups according to their characteristics. Specifically, routing protocols can be classified by their:

- **Purpose** - Interior Gateway Protocol (IGP) or Exterior Gateway Protocol (EGP)
- **Operation** - Distance vector protocol, link-state protocol, or path-vector protocol
- **Behavior** - Classful (legacy) or classless protocol

For example, IPv4 routing protocols are classified as follows:

- **RIPv1 (legacy)** - IGP, distance vector, classful protocol
- **IGRP (legacy)** - IGP, distance vector, classful protocol developed by Cisco (deprecated from 12.2 IOS and later)
- **RIPv2** - IGP, distance vector, classless protocol
- **EIGRP** - IGP, distance vector, classless protocol developed by Cisco

- **OSPF** - IGP, link-state, classless protocol
- **IS-IS** - IGP, link-state, classless protocol
- **BGP** - EGP, path-vector, classless protocol

The classful routing protocols, RIPv1 and IGRP, are legacy protocols and are only used in older networks. These routing protocols have evolved into the classless routing protocols, RIPv2 and EIGRP, respectively. Link-state routing protocols are classless by nature.

The figure displays a hierarchical view of dynamic routing protocol classification.

Dynamic Routing Protocol Overview

Dynamic Routing Protocol Overview

	Interior Gateway Protocols				Exterior Gateway Protocols
	Distance Vector		Link-State		Path Vector
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGP-MP

- RIP protocol was updated to RIPv2 to accommodate growth in the network environment
  - RIPv2 does not scale to current larger network implementations
- Routing Protocols developed to meet the need of larger networks include:
  - Open Shortest Path First (OSPF)
  - Intermediate System-to-Intermediate System (IS-IS).
  - Enhanced IGRP (EIGRP)
- Border Gateway Protocol (BGP) is used between Internet service providers (ISPs)

Dynamic Routing Protocol Evolution

Dynamic routing protocols have been used in networks since the late 1980s. One of the first routing protocols was RIP. RIPv1 was released in 1988, but some of the basic algorithms within the protocol were used on the Advanced Research Projects Agency Network (ARPANET) as early as 1969.

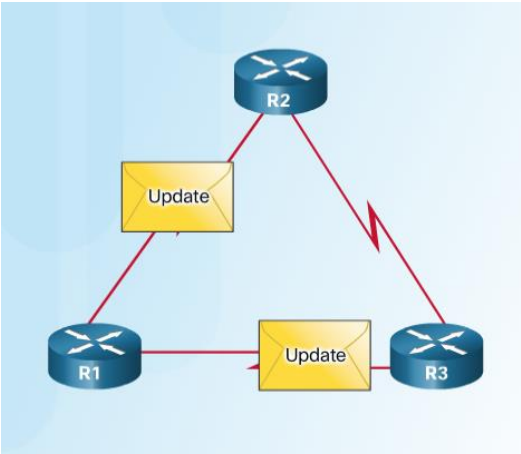
As networks evolved and became more complex, new routing protocols emerged. The RIP protocol was updated to RIPv2 to accommodate growth in the network environment. However, RIPv2 still does not scale to the larger network implementations of today. To address the needs of larger networks, two advanced 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.

With the advent of numerous consumer devices using IP, the IPv4 addressing space is nearly exhausted; thus, IPv6 has emerged. To support the communication based on IPv6, newer versions of the IP routing protocols have been developed, as shown in the IPv6 row in the Figure.

Dynamic Routing Protocol Overview

Dynamic Routing Protocol Components



- Purpose of dynamic routing protocols includes:
  - Discovery of remote networks
  - Maintaining up-to-date routing information
  - Choosing the best path to destination networks
  - Ability to find a new best path if the current path is no longer available
- The main components of dynamic routing protocols include:
  - Data structures - tables or databases kept in RAM.
  - Routing protocol messages - to discover neighboring routers, exchange routing information, and maintain accurate information about the network.
  - Algorithms – to facilitate learning routing information and for best path determination.

Dynamic Routing Protocol Components

Routing protocols are used to facilitate the exchange of routing information between routers. A routing protocol is a set of processes, algorithms, and messages that are used to exchange routing information and populate the routing table with the routing protocol's choice of best paths. The purpose of dynamic routing protocols includes:

- Discovery of remote networks
- Maintaining up-to-date routing information
- Choosing the best path to destination networks
- Ability to find a new best path if the current path is no longer available

The main components of dynamic routing protocols include:

- **Data structures -** Routing protocols typically use tables or databases for its operations. This information is kept in RAM.
- **Routing protocol messages -** Routing protocols use various types of messages to discover neighboring routers, exchange routing information, and other tasks to learn and maintain accurate information about the network.
- **Algorithm -** An algorithm is a finite list of steps used to accomplish a task. Routing protocols use algorithms for facilitating routing information and for best path determination.

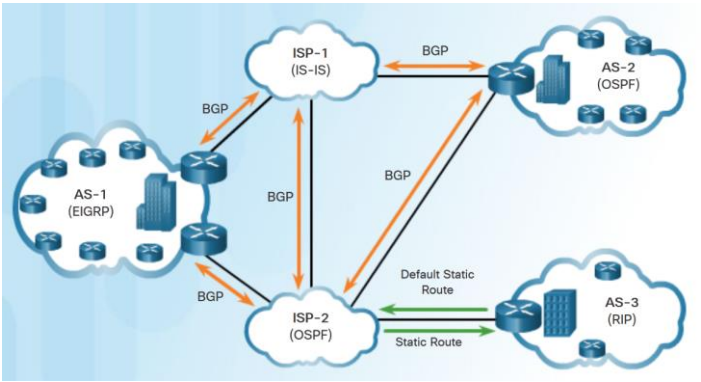
Routing protocols allow routers to dynamically share information about remote networks and automatically offer this information to their own routing tables. Click Play in the figure to see an animation of this process.

Routing protocols determine the best path, or route, to each network. That route is then offered to the routing table. The route will be installed in the routing table is there is not another routing source with a lower administrative distance. For example, a static route with an administrative distance of 1 will have precedence over the same network learned by a dynamic routing protocol. A primary benefit of dynamic routing protocols is that routers exchange routing information when there is a topology change. This exchange allows routers to automatically learn about new networks and also to find alternate paths when there is a link failure to a current network.

Types of Routing Protocols

IGP and EGP Routing Protocols

- Interior Gateway Protocols (IGP) - Used for routing within an Autonomous System (AS).
  - RIP, EIGRP, OSPF, and IS-IS.
- Exterior Gateway Protocols (EGP) - Used for routing between Autonomous Systems.
  - BGP



IGP and EGP Routing Protocols

An autonomous system (AS) is a collection of routers under a common administration such as a company or an organization. An AS is also known as a routing domain. Typical examples of an AS are a company's internal network and an ISP's network. The Internet is based on the AS concept; therefore, two types of routing protocols are required:

- **Interior Gateway Protocols (IGP)** - Used for routing within an AS. It is also referred to as intra-AS routing. Companies, organizations, and even service providers use an IGP on their internal networks. IGPs include RIP, EIGRP, OSPF, and IS-IS.
- **Exterior Gateway Protocols (EGP)** - Used for routing between ASes. It is also referred to as inter-AS routing. Service providers and large companies may interconnect using an EGP. The Border Gateway Protocol (BGP) is the only currently-viable EGP and is the official routing protocol used on the Internet.

Note: Because BGP is the only EGP available, the term EGP is rarely used; instead, most engineers simply refer to BGP.

The example in the figure provides simple scenarios highlighting the deployment of IGPs, BGP, and static routing:

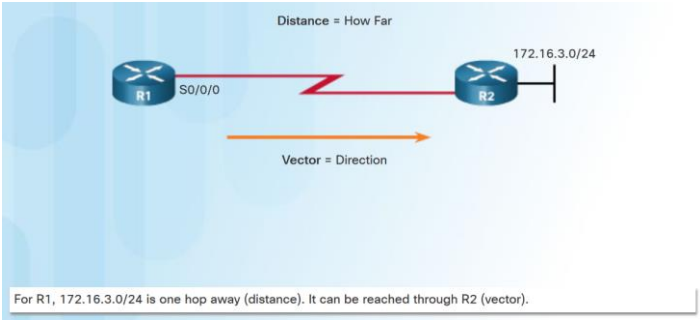
- **ISP-1** - This is an AS and it uses IS-IS as the IGP. It interconnects with other autonomous systems and service providers using BGP to explicitly control how traffic is routed.

- **ISP-2** - This is an AS and it uses OSPF as the IGP. It interconnects with other autonomous systems and service providers using BGP to explicitly control how traffic is routed.
- **AS-1** - This is a large organization and it uses EIGRP as the IGP. Because it is multihomed (i.e., connects to two different service providers), it uses BGP to explicitly control how traffic enters and leaves the AS.
- **AS-2** - This is a medium-sized organization and it uses OSPF as the IGP. It is also multihomed; therefore, it uses BGP to explicitly control how traffic enters and leaves the AS.
- **AS-3** - This is a small organization with older routers within the AS; it uses RIP as the IGP. BGP is not required because it is single-homed (i.e., connects to one service provider). Instead, static routing is implemented between the AS and the service provider.

Note: BGP is beyond the scope of this course and is not discussed in detail.

Types of Routing Protocols

Distance Vector Routing Protocols



- Distance vector means that routes are advertised by providing two characteristics:
  - Distance - Identifies how far it is to the destination network based on a metric such as hop count, cost, bandwidth, delay.
  - Vector - Specifies the direction of the next-hop router or exit interface to reach the destination.
- RIPv1 (legacy), RIPv2, IGRP Cisco proprietary (obsolete), EIGRP.

Distance Vector Routing Protocols

Distance vector means that routes are advertised by providing two characteristics:

Distance - Identifies how far it is to the destination network and is based on a metric such as the hop count, cost, bandwidth, delay, and more.

Vector - Specifies the direction of the next-hop router or exit interface to reach the destination.

For example, in the figure, R1 knows that the distance to reach network 172.16.3.0/24 is one hop and that the direction is out of the interface S0/0/0 toward R2.

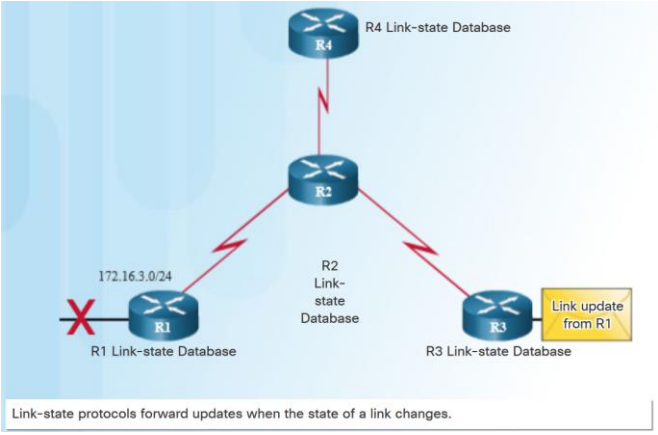
A router using a distance vector routing protocol does not have the knowledge of the entire path to a destination network. Distance vector protocols use routers as sign posts along the path to the final destination. The only information a router knows about a remote network is the distance or metric to reach that network and which path or interface to use to get there. Distance vector routing protocols do not have a map of the network topology like other types of routing protocols do.

There are four distance vector IPv4 IGPs:

- **RIPv1** - First generation legacy protocol
- **RIPv2** - Simple distance vector routing protocol
- **IGRP** - First generation Cisco proprietary protocol (obsolete and replaced by EIGRP)
- **EIGRP** - Advanced version of distance vector routing

Types of Routing Protocols

Link-State Routing Protocols



Link-state protocols forward updates when the state of a link changes.

- A link-State router uses the link-state information received from other routers:
  - to create a topology map.
  - to select the best path to all destination networks in the topology.
- Link-state routing protocols do not use periodic updates.
  - updates are only sent when there is a change in the topology
- OSPF and IS-IS

Link-State Routing Protocols

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 of the other routers.

To continue our analogy of sign posts, using a link-state routing protocol is like having a complete map of the network topology. The sign posts 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. Link-state routing protocols do not use periodic updates. In contrast, RIP-enabled routers send periodic updates of their routing information to their neighbors. After the routers have learned about all the required networks (achieved convergence), a link-state update is only sent when there is a change in the topology. For example, the link-state update in the animation is not sent until the 172.16.3.0 network goes down.

Link-state protocols work best in situations where:

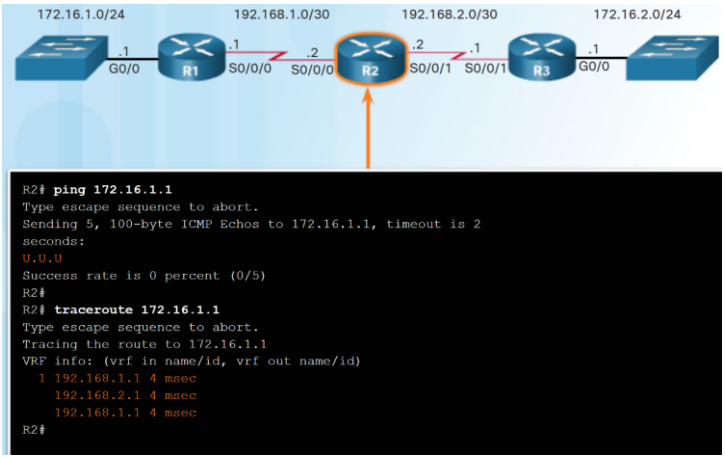
- The network design is hierarchical, usually occurring in large networks
- Fast adaptation to network changes is crucial
- The administrators are knowledgeable about the implementation and maintenance of a link-state routing protocol

There are two link-state IPv4 IGPs:
OSPF - Popular standards-based routing protocol
IS-IS - Popular in provider networks

Types of Routing Protocols

Classful Routing Protocols

- Classless routing protocols include subnet mask information in the routing updates.
- Classful routing protocols do not send subnet mask information in routing updates.
- Classful routing protocols cannot support variable-length subnet masks (VLSMs) and classless interdomain routing (CIDR).
- Classful routing protocols also create problems in discontiguous networks.



Classful Routing Protocols

The biggest distinction between classful and classless routing protocols is that classful routing protocols do not send subnet mask information in routing updates. Classless routing protocols include subnet mask information in the routing updates.

The two original IPv4 routing protocols developed were RIPv1 and IGRP. They were created when network addresses were allocated based on classes (i.e., class A, B, or C). At that time, a routing protocol did not need to include the subnet mask in the routing update, because the network mask could be determined based on the first octet of the network address.

Note: Only RIPv1 and IGRP are classful. All other IPv4 and IPv6 routing protocols are classless. Classful addressing has never been a part of IPv6.

The fact that RIPv1 and IGRP do not include subnet mask information in their updates means that they cannot provide variable-length subnet masks (VLSMs) and classless interdomain routing (CIDR).

Classful routing protocols also create problems in discontiguous networks. A discontiguous network is when subnets from the same classful major network address are separated by a different classful network address.

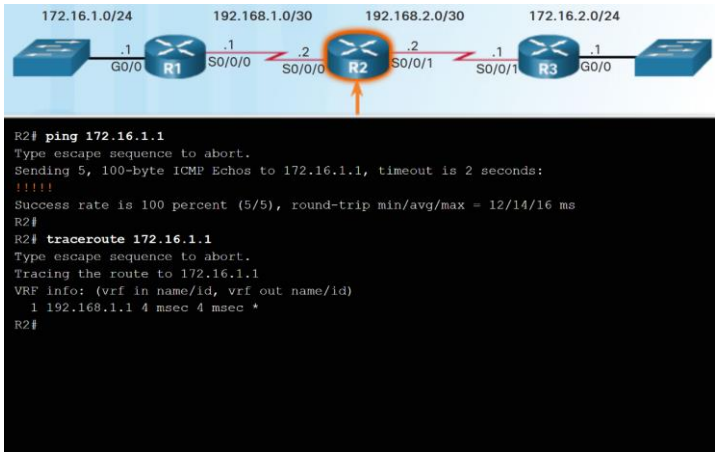
To illustrate the shortcoming of classful routing, refer to the topology in Figure. Notice that the LANs of R1 (172.16.1.0/24) and R3 (172.16.2.0/24) are both subnets of the same class B network (172.16.0.0/16). They are separated by different classful

subnets (192.168.1.0/30 and 192.168.2.0/30) of the same class C networks (192.168.1.0/24 and 192.168.2.0/24).
When R1 forwards an update to R2, RIPv1 does not include the subnet mask information with the update; it only forwards the class B network address 172.16.0.0. R2 receives and processes the update. It then creates and adds an entry for the class B 172.16.0.0/16 network in the routing table.
When R3 forwards an update to R2, it also does not include the subnet mask information and therefore only forwards the classful network address 172.16.0.0. R2 receives and processes the update and adds another entry for the classful network address 172.16.0.0/16 to its routing table. When there are two entries with identical metrics in the routing table, the router shares the load of the traffic equally among the two links. This is known as load balancing.
As shown in Figure, this has a negative effect on connectivity to a discontiguous network. Notice the erratic behavior of the **ping** and **traceroute** commands.

Types of Routing Protocols

Classless Routing Protocols

- Classless IPv4 routing protocols (RIPv2, EIGRP, OSPF, and IS-IS) all include the subnet mask information in routing updates.
- Classless routing protocols support VLSM and CIDR.
- IPv6 routing protocols are classless.



Classless Routing Protocols

Modern networks no longer use classful IP addressing, and therefore, the subnet mask cannot be determined by the value of the first octet. The classless IPv4 routing protocols (RIPv2, EIGRP, OSPF, and IS-IS) all include the subnet mask information with the network address in routing updates. Classless routing protocols support VLSM and CIDR.

IPv6 routing protocols are classless. The distinction of being classful or classless only applies to IPv4 routing protocols. All IPv6 routing protocols are considered classless because they include the prefix-length with the IPv6 address.

In this discontiguous network design, the classless protocol RIPv2 has been implemented on all three routers. When R1 forwards an update to R2, RIPv2 includes the subnet mask information with the update 172.16.1.0/24.

R2 receives, processes, and adds two entries in the routing table. The first line displays the classful network address 172.16.0.0 with the /24 subnet mask of the update. This is known as the parent route. The second entry displays the VLSM network address 172.16.1.0 with the exit and next-hop address. This is referred to as the child route. Parent routes never include an exit interface or next-hop IP address.

When R3 forwards an update to R2, RIPv2 includes the subnet mask information with the update 172.16.2.0/24.

R2 receives, processes, and adds another child route entry 172.16.2.0/24 under the parent route entry 172.16.0.0.

R2 is now aware of the subnetted networks.

Types of Routing Protocols

Routing Protocol Characteristics

- Routing protocols can be compared based on the characteristics in the chart.

	Distance Vector				Link State	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Speed of Convergence	Slow	Slow	Slow	Fast	Fast	Fast
Scalability - Size of Network	Small	Small	Small	Large	Large	Large
Use of VLSM	No	Yes	No	Yes	Yes	Yes
Resource Usage	Low	Low	Low	Medium	High	High
Implementation and Maintenance	Simple	Simple	Simple	Complex	Complex	Complex

Routing Protocol Characteristics

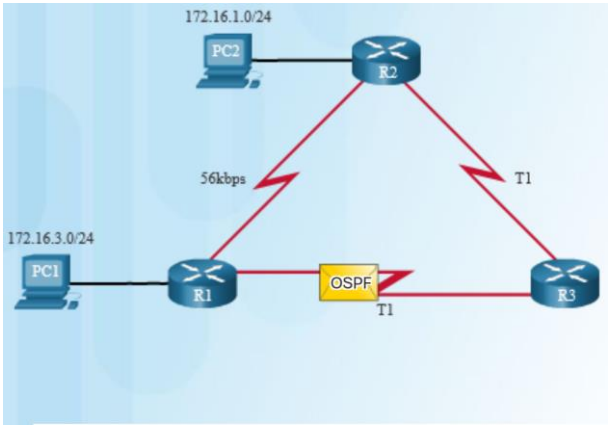
Routing protocols can be compared based on the following characteristics:

- **Speed of Convergence** - Speed of convergence defines how quickly the routers in the network topology share routing information and reach a state of consistent knowledge. The faster the convergence, the more preferable the protocol. Routing loops can occur when inconsistent routing tables are not updated due to slow convergence in a changing network.
- **Scalability** - Scalability defines how large a network can become, based on the routing protocol that is deployed. The larger the network is, the more scalable the routing protocol needs to be.
- **Classful or Classless (Use of VLSM)** - Classful routing protocols do not include the subnet mask and cannot support VLSM. Classless routing protocols include the subnet mask in the updates. Classless routing protocols support VLSM and better route summarization.
- **Resource Usage** - Resource usage includes the requirements of a routing protocol such as memory space (RAM), CPU utilization, and link bandwidth utilization. Higher resource requirements necessitate more powerful hardware to support the routing protocol operation, in addition to the packet forwarding processes.
- **Implementation and Maintenance** - Implementation and maintenance describes the level of knowledge that is required for a network administrator to implement and maintain the network based on the routing protocol deployed.

The table in the figure summarizes the characteristics of each routing protocol.

Types of Routing Protocols

Routing Protocol Metrics



RIP chooses best path based on hop count.
OSPF chooses best path based on bandwidth.

- A metric is a measurable value that is assigned by the routing protocol to different routes based on the usefulness of that route.
- Routing metrics are used to determine the overall "cost" of a path from source to destination.
- Best path is route with the lowest cost.
- Metrics used by various dynamic protocols:
  - RIP – Hop count
  - OSPF – Cost based on cumulative bandwidth
  - EIGRP - Bandwidth, delay, load, and reliability.

Routing Protocol Metrics

There are cases when a routing protocol learns of more than one route to the same destination. To select the best path, the routing protocol must be able to evaluate and decide between the available paths. This is accomplished through the use of routing metrics.

A metric is a measurable value that is assigned by the routing protocol to different routes based on the usefulness of that route. In situations where there are multiple paths to the same remote network, the routing metrics are used to determine the overall "cost" of a path from source to destination. Routing protocols determine the best path based on the route with the lowest cost.

Different routing protocols use different metrics. The metric used by one routing protocol is not comparable to the metric used by another. As a result, two different routing protocols might choose different paths to the same destination.

The following lists some dynamic protocols and the metrics they use:

- **Routing Information Protocol (RIP)** - Hop count
- **Open Shortest Path First (OSPF)** - Cisco's cost based on cumulative bandwidth from source to destination
- **Enhanced Interior Gateway Routing Protocol (EIGRP)** – Minimum bandwidth, delay, load, and reliability.

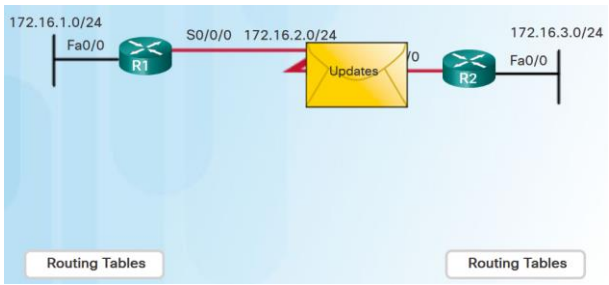
The figure shows that RIP would choose the path with the least amount of hops; whereas, OSPF would choose the path with the highest bandwidth.

Distance Vector Dynamic Routing

Distance Vector Fundamentals

Dynamic Routing Protocol Operation

- Operation of a dynamic routing protocol can be described as follows:
  - The router sends and receives routing messages on its interfaces.
  - The router shares routing messages and routing information with other routers using the same routing protocol.
  - Routers exchange routing information to learn about remote networks.
  - When a router detects a topology change, the routing protocol can advertise this change to other routers.



Dynamic Routing Protocol Operation

All routing protocols are designed to learn about remote networks and to quickly adapt whenever there is a change in the topology. The method that a routing protocol uses to accomplish this depends upon the algorithm it uses and the operational characteristics of that protocol.

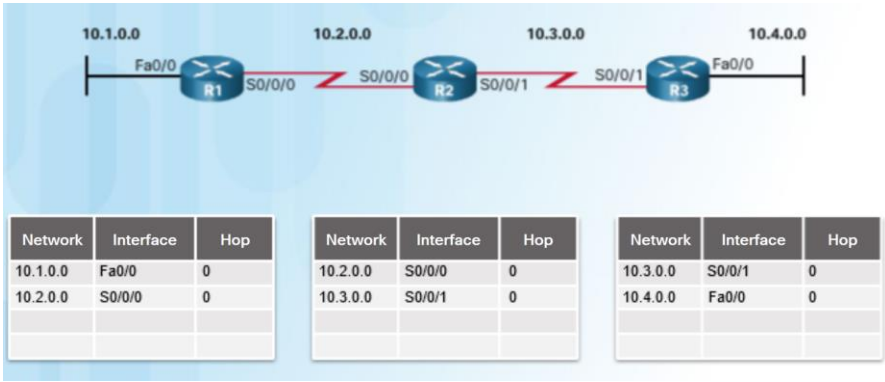
In general, the operations of a dynamic routing protocol can be described as follows:

1. The router sends and receives routing messages on its interfaces.
2. The router shares routing messages and routing information with other routers that are using the same routing protocol.
3. Routers exchange routing information to learn about remote networks.
4. When a router detects a topology change, the routing protocol can advertise this change to other routers.

Distance Vector Fundamentals

Cold Start

- After a router boots successfully it applies the saved configuration, then the router initially discovers its own directly connected networks.
  - It adds those directly connected interface IP addresses to its routing table



Cold Start

All routing protocols follow the same patterns of operation. To help illustrate this, consider the following scenario in which all three routers are running RIPv2.

When a router 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, then the router initially discovers its own directly connected networks.

Notice how the routers proceed through the boot up process and then discover any directly connected networks and subnet masks. This information is added to their routing tables as follows:

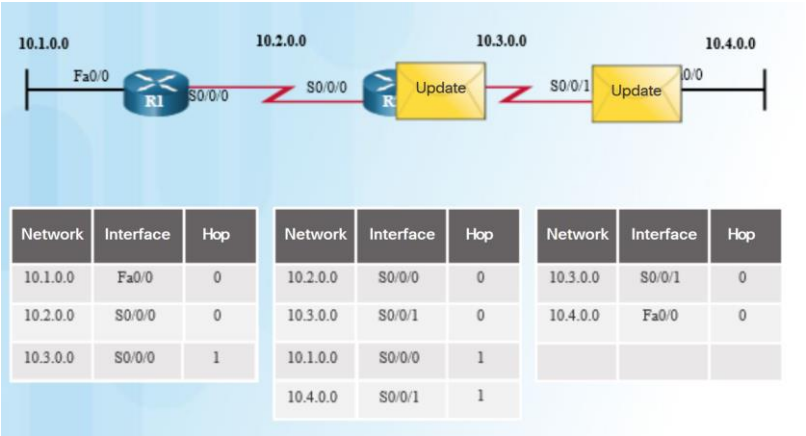
- R1 adds the 10.1.0.0 network available through interface FastEthernet 0/0 and 10.2.0.0 is available through interface Serial 0/0/0.
- R2 adds the 10.2.0.0 network available through interface Serial 0/0/0 and 10.3.0.0 is available through interface Serial 0/0/1.
- R3 adds the 10.3.0.0 network available through interface Serial 0/0/1 and 10.4.0.0 is available through interface FastEthernet 0/0.

With this initial information, the routers then proceed to find additional route sources for their routing tables.

Distance Vector Fundamentals

Network Discovery

- If a routing protocol is configured, the router exchanges routing updates to learn about any remote routes.
  - The router sends an update packet with its routing table information out all interfaces.
  - The router also receives updates from directly connected routers and adds new information to its routing table.



Network Discovery

After initial boot up and discovery, the routing table is updated with all directly connected networks and the interfaces those networks reside on.

If a routing protocol is configured, the next step is for the router to begin exchanging routing updates to learn about any remote routes.

The router sends an update packet out all interfaces that are enabled on the router. The update contains the information in the routing table, which currently is all directly connected networks.

At the same time, the router also receives and processes similar updates from other connected routers. Upon receiving an update, the router checks it for new network information. Any networks that are not currently listed in the routing table are added.

Refer to the figure for a topology setup between three routers, R1, R2, and R3 with RIPv2 enabled. Based on this topology, below is a listing of the different updates that R1, R2, and R3 send and receive during initial convergence.

R1:

- Sends an update about network 10.1.0.0 out the Serial0/0/0 interface
- Sends an update about network 10.2.0.0 out the FastEthernet0/0 interface
- Receives an update from R2 about network 10.3.0.0 and increments the hop count by 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
- Sends an update about network 10.2.0.0 out the Serial 0/0/1 interface
- Receives an update from R1 about network 10.1.0.0 and increments the hop count by 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 and increments the hop count by 1
- Stores network 10.4.0.0 in the routing table with a metric of 1

R3:

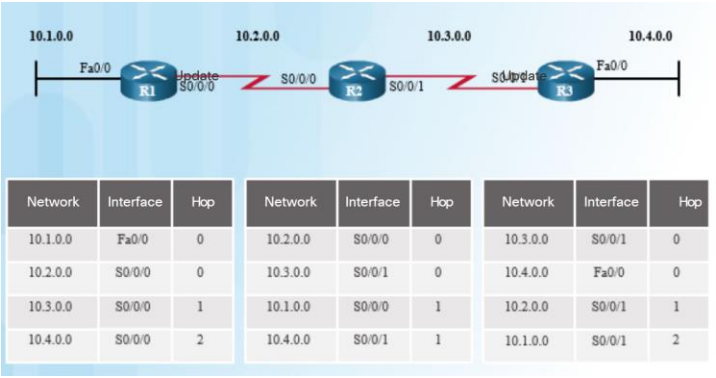
- Sends an update about network 10.4.0.0 out the Serial 0/0/1 interface
- Sends an update about network 10.3.0.0 out the FastEthernet0/0
- Receives an update from R2 about network 10.2.0.0 and increments the hop count by 1
- Stores network 10.2.0.0 in the routing table with a metric of 1

After this first round of update exchanges, each router knows about the connected networks of their directly connected neighbors. However, did you notice that R1 does not yet know about 10.4.0.0 and that R3 does not yet know about 10.1.0.0? Full knowledge and a converged network do not take place until there is another exchange of routing information.

Distance Vector Fundamentals

Exchanging the Routing Information

- Working toward convergence, the routers exchange the next round of periodic updates.
- Distance vector routing protocols use split horizon to avoid loops.
- Split horizon prevents information from being sent out the same interface from which it was received.



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	S0/0/1	2

Exchanging the 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.
Refer to the figure for a topology setup between three routers, R1, R2, and R3. After initial discovery is complete, each router continues the convergence process by sending and receiving the following updates.

R1:

- Sends an update about network 10.1.0.0 out the Serial 0/0/0 interface
- Sends an update about networks 10.2.0.0 and 10.3.0.0 out the FastEthernet0/0 interface
- Receives an update from R2 about network 10.4.0.0 and increments the hop count by 1
- 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 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 and 10.4.0.0 out of Serial 0/0/0 interface
- Sends an update about networks 10.1.0.0 and 10.2.0.0 out of Serial 0/0/1 interface

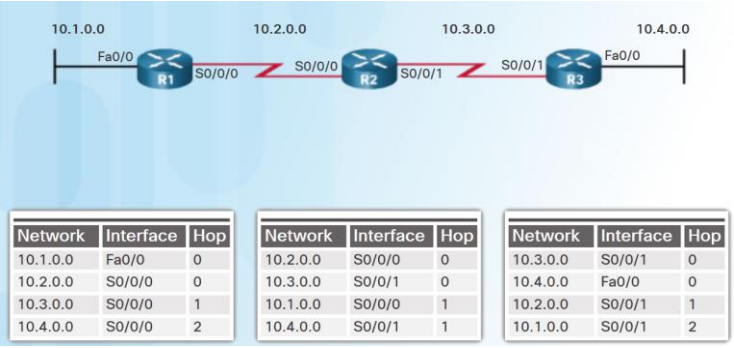
- Receives an update from R1 about network 10.1.0.0. There is no change; therefore, the routing information remains the same
- Receives an update from R3 about network 10.4.0.0. There is no change; therefore, the routing information remains the same

R3:
- Sends an update about network 10.4.0.0 out the Serial 0/0/1 interface
- Sends an update about networks 10.2.0.0 and 10.3.0.0 out the FastEthernet0/0 interface
- Receives an update from R2 about network 10.1.0.0 and increments the hop count by 1
- 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 with a metric of 1. There is no change; therefore, the routing information remains the same

Distance vector routing protocols typically implement a routing loop prevention technique known as split horizon. Split horizon prevents information from being sent out the same interface from which it was received. For example, R2 does not send an update containing the network 10.1.0.0 out of Serial 0/0/0, because R2 learned about network 10.1.0.0 through Serial 0/0/0.
After routers within a network have converged, the router can then use the information within the routing table to determine the best path to reach a destination. Different routing protocols have different ways of calculating the best path.

Distance Vector Fundamentals

Achieving Convergence



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	S0/0/1	2

- The network has converged when all routers have complete and accurate information about the entire network
- Convergence time is the time it takes routers to share information, calculate best paths, and update routing tables.
- Routing protocols can be rated based on the speed to convergence; the faster the convergence, the better the routing protocol.

Achieving Convergence

The network has converged when all routers have complete and accurate information about the entire network, as shown in the figure. 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.

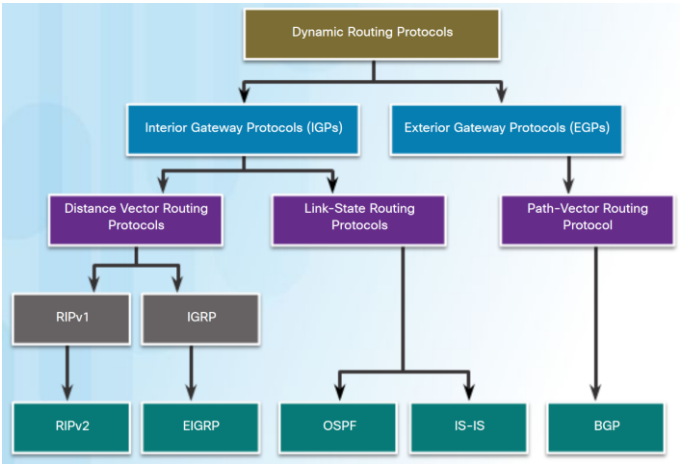
Convergence is both collaborative and independent. The routers share information with each other, but must independently calculate the impacts of the topology change on their own routes. Because they develop an agreement with the new topology independently, they are said to converge on this consensus.

Convergence properties include the speed of propagation of routing information and the calculation of optimal paths. The speed of propagation refers to the amount of time it takes for routers within the network to forward routing information.

Routing protocols can be rated based on the speed to convergence; the faster the convergence, the better the routing protocol. Generally, older protocols, such as RIP, are slow to converge, whereas modern protocols, such as EIGRP and OSPF, converge more quickly.

Distance Vector Routing Protocol Operation

Distance Vector Technologies



- Distance vector routing protocols share updates between neighbors.
- Routers using distance vector routing are not aware of the network topology.
- Some distance vector routing protocols send periodic updates.
  - RIPv1 sends updates as broadcasts 255.255.255.255.
  - RIPv2 and EIGRP can use multicast addresses to reach only specific neighbor routers.
  - EIGRP can use a unicast message to reach a specific neighbor router.
  - EIGRP only sends updates when needed, not periodically.

Distance Vector Technologies

Distance vector routing protocols share updates between neighbors. Neighbors are routers that share a link and are configured to use the same routing protocol. The router is only aware of the network addresses of its own interfaces and the remote network addresses it can reach through its neighbors. Routers using distance vector routing are not aware of the network topology.

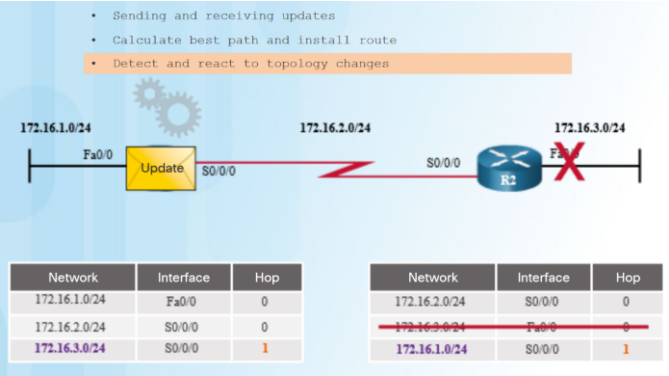
Some distance vector routing protocols send periodic updates. For example, RIP sends a periodic update to all of its neighbors every 30 seconds. RIP does this even if the topology has not changed. RIPv1 sends these updates as broadcasts to the all-hosts IPv4 address of 255.255.255.255.

The broadcasting of periodic updates is inefficient because the updates consume bandwidth and network device CPU resources. Every network device has to process a broadcast message. Instead of using broadcasts like RIP, RIPv2 and EIGRP can use multicast addresses to reach only specific neighbor routers. EIGRP can also use a unicast message to reach one specific neighbor router. Additionally, EIGRP only sends updates when needed, instead of periodically.

As shown in the figure, the two modern IPv4 distance vector routing protocols are RIPv2 and EIGRP. RIPv1 and IGRP are listed only for historical accuracy.

Distance Vector Routing Protocol Operation

Distance Vector Algorithm



- The distance vector algorithm 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
- RIP uses the Bellman-Ford algorithm as its routing algorithm.
- IGRP and EIGRP use the Diffusing Update Algorithm (DUAL) routing algorithm.

Distance Vector Algorithm

At the core of the distance vector protocol is the routing algorithm. The algorithm is used to calculate the best paths and then send that information to the neighbors. 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

In the figure, R1 and R2 are configured with the RIP routing protocol. 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. The algorithm on each router makes its calculations independently and updates the routing table with the new information. 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.

Different routing protocols use different algorithms to install routes in the routing table, send updates to neighbors, and make path determination decisions. For example:

RIP uses the Bellman-Ford algorithm as its routing algorithm. It is based on two algorithms developed in 1958 and 1956 by Richard Bellman and Lester Ford, Jr.

IGRP and EIGRP use the Diffusing Update Algorithm (DUAL) routing algorithm developed by Dr. J.J. Garcia-Luna-Aceves at SRI International.

Types of Distance Vector Routing Protocols

Routing Information Protocol

- The Routing Information Protocol (RIP)
  - Easy to confgure
  - Routing updates broadcasted (255.255.255.255) every 30 seconds
  - Metric is hop count
  - 15 hop limit
- RIPv2
  - **Classless routing protocol** - supports VLSM and CIDR
  - **Increased efficiency** – sends updates to multicast address 224.0.0.9
  - **Reduced routing entries** - supports manual route summarization
  - **Secure** - supports authentication

Characteristics and Features	RIPv1	RIPv2
Metric	Both use hop count as a simple metric. The maximum number of hops is 15.	
Updates Forwarded to Address	255.255.255.255	224.0.0.9
Supports VLSM	✗	✓
Supports CIDR	✗	✓
Supports Summarization	✗	✓
Supports Authentication	✗	✓

- RIPng
  - IPv6 enabled version of RIP
  - 15 hop limit and administrative distance is 120

Routing Information Protocol

The Routing Information Protocol (RIP) was a first generation routing protocol for IPv4 originally specified in RFC 1058. It is easy to configure, making it a good choice for small networks.

RIPv1 has the following key characteristics:

- Routing updates are broadcasted (255.255.255.255) every 30 seconds.
- The hop count is used as the metric for path selection.
- A hop count greater than 15 hops is deemed infinite (too far). That 15th hop router would not propagate the routing update to the next router.

In 1993, RIPv1 was updated to a classless routing protocol known as RIP version 2 (RIPv2). RIPv2 included the following improvements:

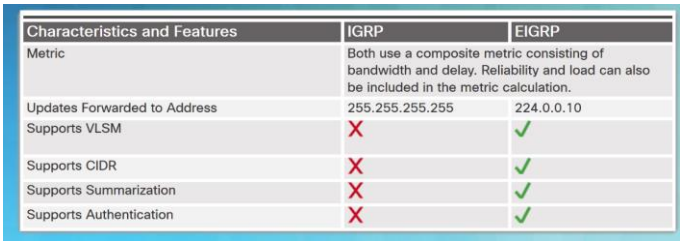
- **Classless routing protocol** - It supports VLSM and CIDR, because it includes the subnet mask in the routing updates.
- **Increased efficiency** - It forwards updates to multicast address 224.0.0.9, instead of the broadcast address 255.255.255.255.
- **Reduced routing entries** - It supports manual route summarization on any interface.
- **Secure** - It supports an authentication mechanism to secure routing table updates between neighbors.

The table in the figure summarizes the differences between RIPv1 and RIPv2.

RIP updates are encapsulated into a UDP segment, with both source and destination port numbers set to UDP port 520.
In 1997, the IPv6 enabled version of RIP was released. RIPng is based on RIPv2. It still has a 15 hop limitation and the administrative distance is 120.

Types of Distance Vector Routing Protocols

Enhanced Interior-Gateway Routing Protocol



Characteristics and Features	IGRP	EIGRP
Metric	Both use a composite metric consisting of bandwidth and delay. Reliability and load can also be included in the metric calculation.	
Updates Forwarded to Address	255.255.255.255	224.0.0.10
Supports VLSM	✗	✓
Supports CIDR	✗	✓
Supports Summarization	✗	✓
Supports Authentication	✗	✓

- EIGRP replaced IGRP in 1992. It includes the following features:
  - **Bounded triggered updates** – sends updates only to routers that need it.
  - **Hello keepalive mechanism** - Hello messages are periodically exchanged to maintain adjacencies.
  - **Maintains a topology table** - maintains all the routes received from neighbors (not only the best paths) in a topology table.
  - **Rapid convergence** – because it maintains alternate routes.
  - **Multiple network layer protocol support** – uses Protocol Dependent Modules (PDM) to support layer 3 protocols.

Enhanced Interior-Gateway Routing Protocol

The Interior Gateway Routing Protocol (IGRP) was the first proprietary IPv4 routing protocol developed by Cisco in 1984. It used the following design characteristics:
Bandwidth, delay, load, and reliability are used to create a composite metric.
Routing updates are broadcast every 90 seconds, by default.
Maximum limit of 255 hops
In 1992, IGRP was replaced by Enhanced IGRP (EIGRP). Like RIPv2, EIGRP also introduced support for VLSM and CIDR. EIGRP increases efficiency, reduces routing updates, and supports secure message exchange.
The table in the figure summarizes the differences between IGRP and EIGRP. EIGRP also introduced:

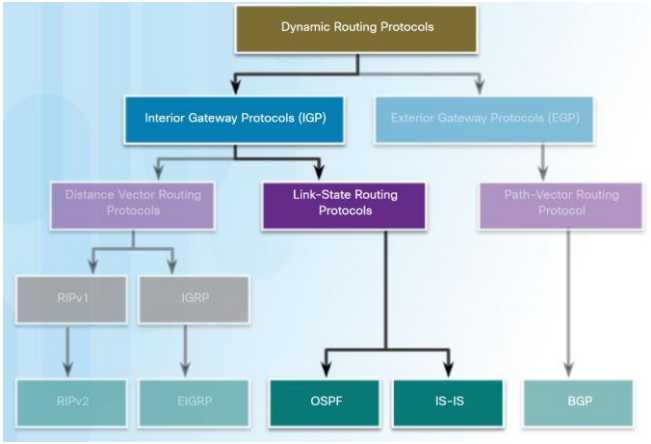
- **Bounded triggered updates** - It does not send periodic updates. Only routing table changes are propagated, whenever a change occurs. This reduces the amount of load the routing protocol places on the network. Bounded triggered updates means that EIGRP only sends to the neighbors that need it. It uses less bandwidth, especially in large networks with many routes.
- **Hello keepalive mechanism** - A small Hello message is periodically exchanged to maintain adjacencies with neighboring routers. This requires a very low usage of network resources during normal operation, as compared to periodic updates.
- **Maintains a topology table** - Maintains all the routes received from neighbors (not only the best paths) in a topology table. DUAL can insert backup routes into the EIGRP topology table.

- **Rapid convergence** - In most cases, it is the fastest IGP to converge because it maintains alternate routes, enabling almost instantaneous convergence. If a primary route fails, the router can use the already identified alternate route. The switchover to the alternate route is immediate and does not involve interaction with other routers.
- **Multiple network layer protocol support** - EIGRP uses Protocol Dependent Modules (PDM), which means that it is the only protocol to include support for protocols other than IPv4 and IPv6, such as legacy IPX and AppleTalk.

Link-State Dynamic Routing

Link-State Routing Protocol Operation

Shortest Path First Protocols



- Link-state routing protocols, also known as shortest path first protocols, are built around Edsger Dijkstra's shortest path first (SPF) algorithm.
- IPv4 Link-State routing protocols:
  - Open Shortest Path First (OSPF)
  - Intermediate System-to-Intermediate System (IS-IS)

Shortest Path First Protocols

Link-state routing protocols are also known as shortest path first protocols and are built around Edsger Dijkstra's shortest path first (SPF) algorithm. The SPF algorithm is discussed in more detail in a later section.

The IPv4 link-state routing protocols are shown in the figure:

- Open Shortest Path First (OSPF)
- Intermediate System-to-Intermediate System (IS-IS)

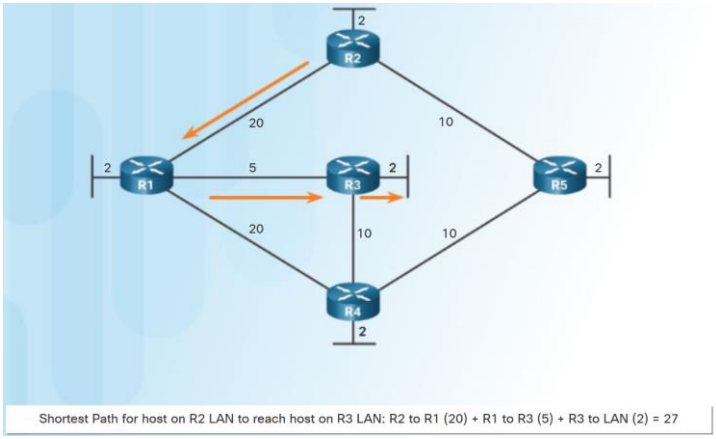
Link-state routing protocols have the reputation of being much more complex than their distance vector counterparts. However, the basic functionality and configuration of link-state routing protocols is equally straight-forward.

Just like RIP and EIGRP, basic OSPF operations can be configured using the:

- **router ospf** *process-id* global configuration command
- **network** command to advertise networks

Link-State Routing Protocol Operation

Dijkstra's Algorithm



- All link-state routing protocols apply Dijkstra's algorithm (also known as shortest path first (SPF)) to calculate the best path route:
  - Uses accumulated costs along each path, from source to destination.
  - Each router determines its own cost to each destination in the topology.

Dijkstra's Algorithm

All link-state routing protocols apply Dijkstra's algorithm to calculate the best path route. The algorithm is commonly referred to as the shortest path first (SPF) algorithm. This algorithm uses accumulated costs along each path, from source to destination, to determine the total cost of a route.

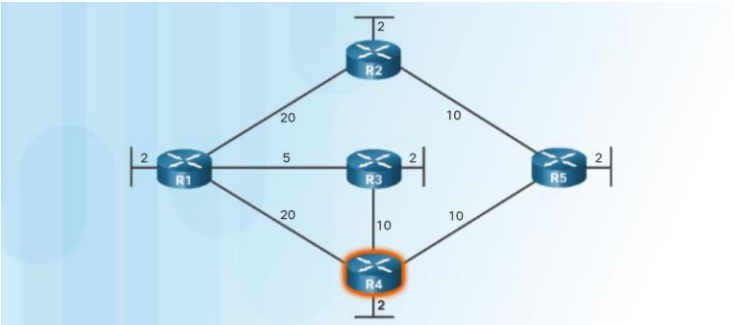
In the figure, each path is labeled with an arbitrary value for cost. The cost of the shortest path for R2 to send packets to the LAN attached to R3 is 27. Each router determines its own cost to each destination in the topology. In other words, each router calculates the SPF algorithm and determines the cost from its own perspective.

Note: The focus of this section is on cost, which is determined by the SPF tree. For this reason, the graphics throughout this section show the connections of the SPF tree, not the topology. All links are represented with a solid black line.

Link-State Routing Protocol Operation

SPF Example

- The table displays the shortest path and the accumulated cost to reach the identified destination networks from the perspective of R4.



Destination	Shortest Path	Cost
R1 LAN	R4 to R3 to R1	17
R2 LAN	R4 to R5 to R2	22
R3 LAN	R4 to R3	12
R5 LAN	R4 to R5	12

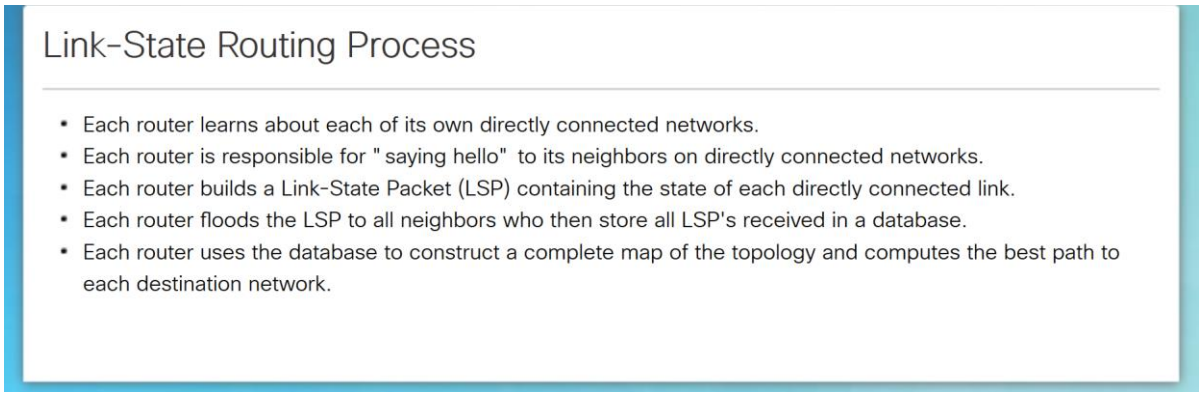
SPF Example

The table in Figure displays the shortest path and the accumulated cost to reach the identified destination networks from the perspective of R4.

The shortest path is not necessarily the path with the least number of hops. For example, look at the path to the R5 LAN. It might be assumed that R1 would send directly to R4 instead of to R3. However, the cost to reach R4 directly (22) is higher than the cost to reach R4 through R3 (17).

Link-State Updates

Link-State Routing Process



Note: This process is the same for both OSPF for IPv4 and OSPF for IPv6.

Link-State Routing Process

So exactly how does a link-state routing protocol work? With link-state routing protocols, a link is an interface on a router. Information about the state of those links is known as link-states.

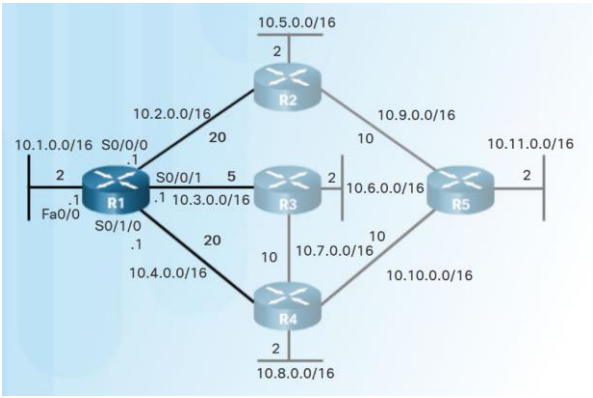
All routers in an OSPF area will complete the following generic link-state routing process to reach a state of convergence:

1. Each router learns about its own links and its own directly connected networks. This is done by detecting that an interface is in the up state.
2. Each router is responsible for meeting its neighbors on directly connected networks. Link state routers do this by exchanging Hello packets with other link-state routers on directly connected networks.
3. Each router builds a Link-State Packet (LSP) containing the state of each directly connected link. This is done by recording all the pertinent information about each neighbor, including neighbor ID, link type, and bandwidth.
4. Each router floods the LSP to all neighbors. Those neighbors store all LSPs received in a database. They then flood the LSPs to their neighbors until all routers in the area have received the LSPs. Each router stores a copy of each LSP received from its neighbors in a local database.
5. Each router uses the database to construct a complete map of the topology and computes the best path to each destination network. Like having a road map, the router now has a complete map of all destinations in the topology and the routes to reach them. The SPF algorithm is used to construct the map of the topology and to

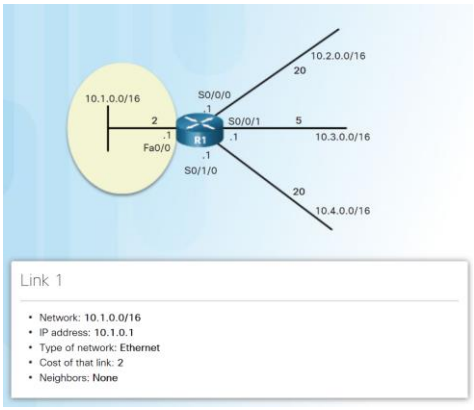
determine the best path to each network.
Note: This process is the same for both OSPF for IPv4 and OSPF for IPv6. The examples in this section will refer to OSPF for IPv4.

Link-State Updates

Link and Link-State



- The first step in the link-state routing process is that each router learns its own directly connected networks.



Link and Link-State

The first step in the link-state routing process is that each router learns about its own links, its own directly connected networks. When a router interface is configured with an IP address and subnet mask, the interface becomes part of that network.

Refer to the topology in Figure. For purposes of this discussion, assume that R1 was previously configured and had full connectivity to all neighbors. However, R1 lost power briefly and had to restart.

During boot up R1 loads the saved startup configuration file. As the previously configured interfaces become active, R1 learns about its own directly connected networks. Regardless of the routing protocols used, these directly connected networks are now entries in the routing table.

As with distance vector protocols and static routes, the interface must be properly configured with an IPv4 address and subnet mask, and the link must be in the up state before the link-state routing protocol can learn about a link. Also, like distance vector protocols, the interface must be included in one of the **network** router configuration statements before it can participate in the link-state routing process.

Figure shows R1 linked to four directly connected networks:

- FastEthernet 0/0 - 10.1.0.0/16
- Serial 0/0/0 - 10.2.0.0/16
- Serial 0/0/1 - 10.3.0.0/16
- Serial 0/1/0 - 10.4.0.0/16

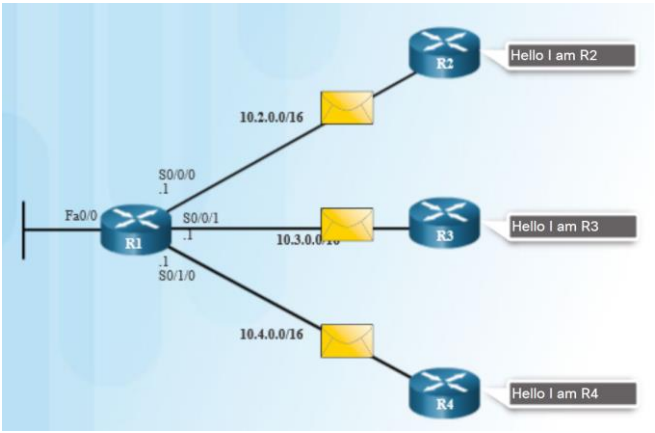
As shown in Figures 2, the link-state information includes:

- The interface's IPv4 address and subnet mask
- The type of network, such as Ethernet (broadcast) or Serial point-to-point link
- The cost of that link
- Any neighbor routers on that link

Note: Cisco’s implementation of OSPF specifies the OSPF routing metric as the cost of the link based on the bandwidth of the outgoing interface. For the purposes of this chapter, we are using arbitrary cost values to simplify the demonstration.

Link-State Updates

Say Hello



- The second step in the link-state routing process is that each router uses a Hello protocol to discover any neighbors on its links.
- When two link-state routers learn that they are neighbors, they form an adjacency.
- If a router stops receiving Hello packets from a neighbor, that neighbor is considered unreachable.

Say Hello

The second step in the link-state routing process is that each router is responsible for meeting its neighbors on directly connected networks.

Routers with link-state routing protocols use a Hello protocol to discover any neighbors on its links. A neighbor is any other router that is enabled with the same link-state routing protocol.

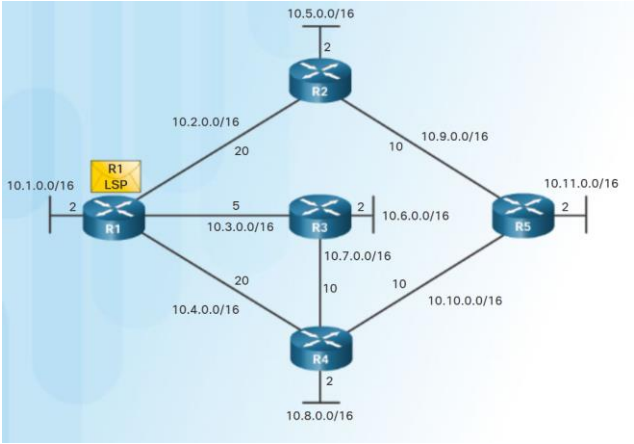
In the animation, R1 sends Hello packets out of its links (interfaces) to discover any neighbors. R2, R3, and R4 reply to the Hello packet with their own Hello packets because these routers are configured with the same link-state routing protocol. There are no neighbors out the FastEthernet 0/0 interface. Because R1 does not receive a Hello on this interface, it does not continue with the link-state routing process steps for the FastEthernet 0/0 link.

When two link-state routers learn that they are neighbors, they form an adjacency. These small Hello packets continue to be exchanged between two adjacent neighbors and serve as a keepalive function to monitor the state of the neighbor. If a router stops receiving Hello packets from a neighbor, that neighbor is considered unreachable and the adjacency is broken.

Link-State Updates

Building the Link-State Packet

- The third step in the link-state routing process is that each router builds a link-state packet (LSP) that contains the link-state information about its links.
- R1 LSP (in diagram) would contain:
  - R1; Ethernet network 10.1.0.0/16; Cost 2
  - R1 -> R2; Serial point-to-point network; 10.2.0.0/16; Cost 20
  - R1 -> R3; Serial point-to-point network; 10.3.0.0/16; Cost 5
  - R1 -> R4; Serial point-to-point network; 10.4.0.0/16; Cost 20



Building the Link-State Packet

The third step in the link-state routing process is that each router builds a link-state packet (LSP) containing the state of each directly connected link.

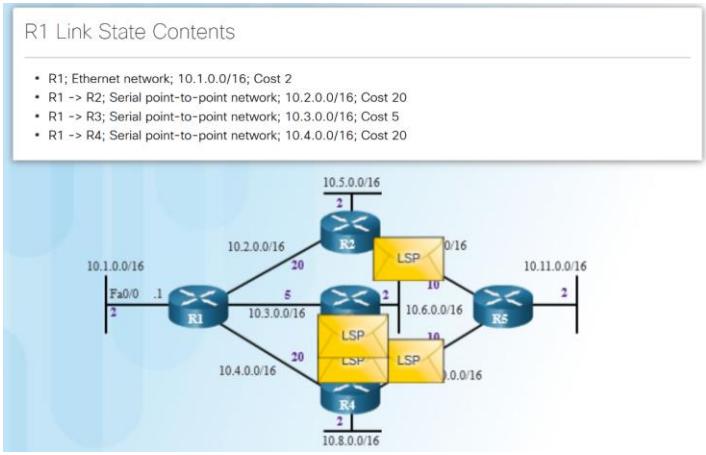
After a router has established its adjacencies, it can build its LSP that contains the link-state information about its links. A simplified version of the LSP from R1 displayed in the figure would contain the following:

1. R1; Ethernet network 10.1.0.0/16; Cost 2
2. R1 -> R2; Serial point-to-point network; 10.2.0.0/16; Cost 20
3. R1 -> R3; Serial point-to-point network; 10.3.0.0/16; Cost 5
4. R1 -> R4; Serial point-to-point network; 10.4.0.0/16; Cost 20

Link-State Updates

Flooding the LSP

- The fourth step in the link-state routing process is that each router floods the LSP to all neighbors.
- An LSP only needs to be sent:
  - During initial startup of the routing protocol process on that router (e.g., router restart)
  - Whenever there is a change in the topology (e.g., a link going down)
- An LSP also includes sequence numbers and aging information:
  - used by each router to determine if it has already received the LSP.
  - used to determine if the LSP has newer information.



Flooding the LSP

The fourth step in the link-state routing process is that each router floods the LSP to all neighbors, who then store all LSPs received in a database.

Each router floods its link-state information to all other link-state routers in the routing area. Whenever a router receives an LSP from a neighboring router, it immediately sends that LSP out all other interfaces except the interface that received the LSP. This process creates a flooding effect of LSPs from all routers throughout the routing area.

In the animation, notice how the LSPs are flooded almost immediately after being received without any intermediate calculations. Link-state routing protocols calculate the SPF algorithm after the flooding is complete. As a result, link-state routing protocols reach convergence very quickly.

Remember that LSPs do not need to be sent periodically. An LSP only needs to be sent:

- During initial startup of the routing protocol process on that router (e.g., router restart)
- Whenever there is a change in the topology (e.g., a link going down or coming up, a neighbor adjacency being established or broken)

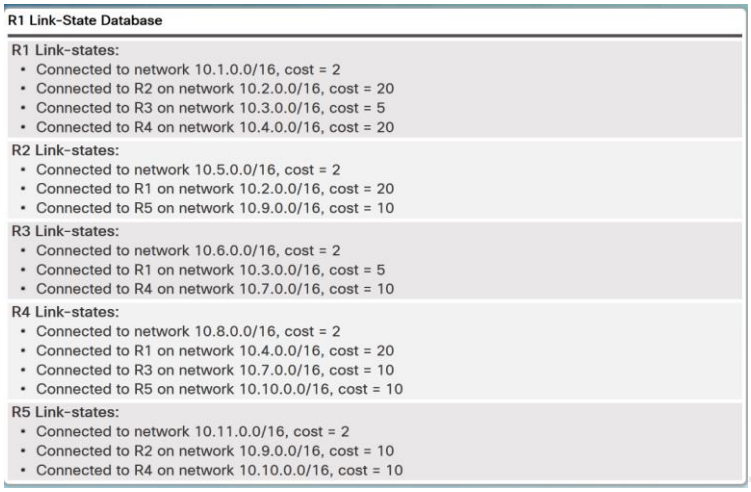
In addition to the link-state information, other information is included in the LSP, such as sequence numbers and aging information, to help manage the flooding process. This information is used by each router to determine if it has already received the LSP

from another router or if the LSP has newer information than what is already contained in the link-state database. This process allows a router to keep only the most current information in its link-state database.

Link-State Updates

Building the Link-State Database

- The final step in the link-state routing process is that each router uses the database to construct a complete map of the topology and computes the best path to each destination network.



Building the Link-State Database

The final step in the link-state routing process is that each router uses the database to construct a complete map of the topology and computes the best path to each destination network.

Eventually, all routers receive an LSP from every other link-state router in the routing area. These LSPs are stored in the link-state database.

The example in the figure displays the link-state database content of R1.

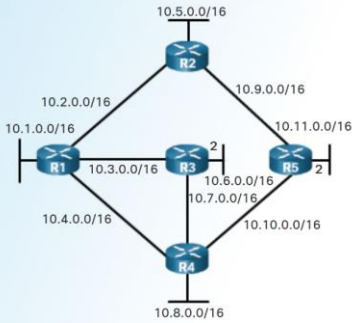
As a result of the flooding process, R1 has learned the link-state information for each router in its routing area. Notice that R1 also includes its own link-state information in the link-state database.

With a complete link-state database, R1 can now use the database and the shortest path first (SPF) algorithm to calculate the preferred path or shortest path to each network resulting in the SPF tree.

Link-State Updates

Building the SPF Tree

Destination	Shortest Path	Cost
10.5.0.0/16	R1 → R2	22
10.6.0.0/16	R1 → R3	7
10.7.0.0/16	R1 → R3	15
10.8.0.0/16	R1 → R3 → R4	17
10.9.0.0/16	R1 → R2	30
10.10.0.0/16	R1 → R3 → R4	25
10.11.0.0/16	R1 → R3 → R4 → R5	27



- Each router uses the link-state database and SPF algorithm to construct the SPF tree.
  - R1 identifies its directly connected networks and costs.
  - R1 adds any unknown networks and associated costs.
  - The SPF algorithm then calculates the shortest paths to reach each individual network resulting in the SPF tree shown in the diagram.
- Each router constructs its own SPF tree independently from all other routers.

Building the SPF Tree

Each router in the routing area uses the link-state database and SPF algorithm to construct the SPF tree.

For example, using the link-state information from all other routers, R1 can now begin to construct an SPF tree of the network. To begin, the SPF algorithm interprets each router's LSP to identify networks and associated costs.

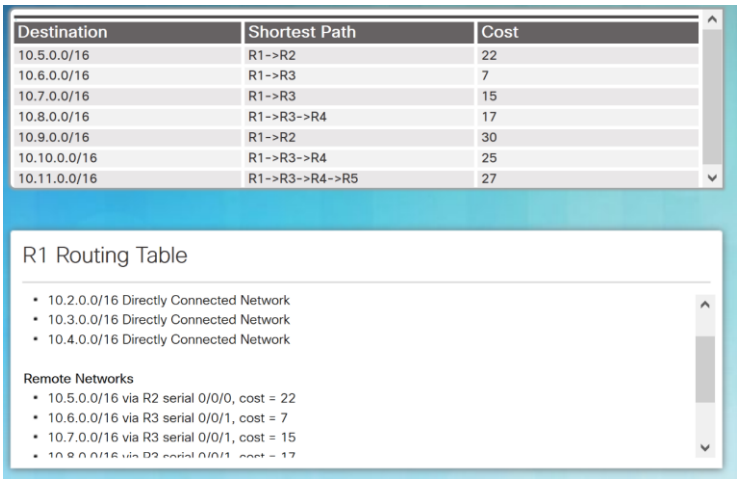
R1 identifies its directly connected networks and costs. R1 keeps adding any unknown network and associated costs to the SPF tree. Notice that R1 ignores any networks it has already identified.

The SPF algorithm then calculates the shortest paths to reach each individual network resulting in the SPF tree as shown in Figure. R1 now has a complete topology view of the link-state area.

Each router constructs its own SPF tree independently from all other routers. To ensure proper routing, the link-state databases used to construct those trees must be identical on all routers.

Link-State Updates

Adding OSPF Routes to the Routing Table



- Using the shortest path information determined by the SPF algorithm, these best paths are then added to the routing table.
- Directly connected routes and static routes are also included in the routing table.

Adding OSPF Routes to the Routing Table

Using the shortest path information determined by the SPF algorithm, these paths can now be added to the routing table. The figure shows the routes that have now been added to R1's IPv4 routing table.

The routing table also includes all directly connected networks and routes from any other sources, such as static routes. Packets are now forwarded according to these entries in the routing table.

Link-State Routing Protocol Benefits

Why Use Link-State Protocols?

Advantages of Link-State Routing Protocols

- Each router builds its own topological map of the network to determine the shortest path.
- Immediate flooding of LSPs achieves faster convergence.
- LSPs are sent only when there is a change in the topology and contain only the information regarding that change.
- Hierarchical design used when implementing multiple areas.

Why Use Link-State Protocols?

As shown in the figure, there are several advantages of link-state routing protocols compared to distance vector routing protocols.

Builds a Topological Map - Link-state routing protocols create a topological map, or SPF tree, of the network topology. Because link-state routing protocols exchange link-states, the SPF algorithm can build an SPF tree of the network. Using the SPF tree, each router can independently determine the shortest path to every network.

Fast Convergence - When receiving an LSP, link-state routing protocols immediately flood the LSP out all interfaces except for the interface from which the LSP was received. In contrast, RIP needs to process each routing update and update its routing table before flooding them out other interfaces.

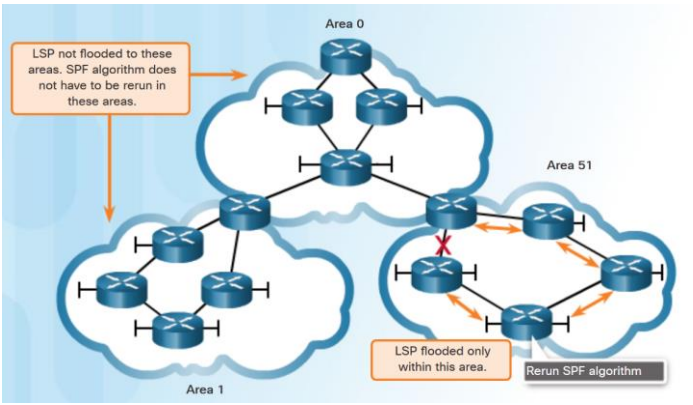
Event-driven Updates - After the initial flooding of LSPs, link-state routing protocols only send out an LSP when there is a change in the topology. The LSP contains only the information regarding the affected link. Unlike some distance vector routing protocols, link-state routing protocols do not send periodic updates.

Hierarchical Design - Link-state routing protocols use the concept of areas. Multiple areas create a hierarchical design to networks, allowing for better route aggregation (summarization) and the isolation of routing issues within an area.

Link-State Routing Protocol Benefits

Disadvantages of Link-State Protocols

- Disadvantages of Link-State protocols:
  - Memory Requirements - Link-state protocols require additional memory.
  - Processing Requirements - Link-state protocols can require more CPU processing.
  - Bandwidth Requirements - The flooding of link-state packets can adversely affect bandwidth.
- Using multiple areas can reduce the size of the link-state databases.
- Multiple areas can limit the amount of link-state information flooding and send LSPs only to those routers that need them.



Disadvantages of Link-State Protocols

Link-state protocols also have a few disadvantages compared to distance vector routing protocols:

- **Memory Requirements** - Link-state protocols require additional memory to create and maintain the link-state database and SPF tree.
- **Processing Requirements** - Link-state protocols can also require more CPU processing than distance vector routing protocols. The SPF algorithm requires more CPU time than distance vector algorithms such as Bellman-Ford, because link-state protocols build a complete map of the topology.
- **Bandwidth Requirements** - The flooding of link-state packets can adversely affect the available bandwidth on a network. This should only occur during initial startup of routers, but can also be an issue on unstable networks.

However, modern link-state routing protocols are designed to minimize the effects on memory, CPU, and bandwidth. The use and configuration of multiple areas can reduce the size of the link-state databases. Multiple areas can limit the amount of link-state information flooding in a routing domain and send LSPs only to those routers that need them. When there is a change in the topology, only those routers in the affected area receive the LSP and run the SPF algorithm. This can help isolate an unstable link to a specific area in the routing domain.

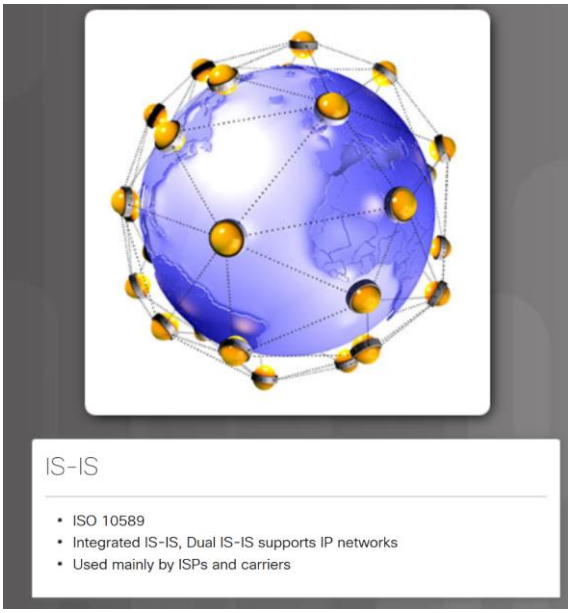
For example, in figure, there are three separate routing domains: area 1, area 0, and area 51. If a network in area 51 goes down, the LSP with the information about this downed link is only flooded to other routers in that area. Only those routers in area

51 need to update their link-state databases, rerun the SPF algorithm, create a new SPF tree, and update their routing tables. Routers in other areas learn that this route is down, but this is done with a type of LSP that does not cause them to rerun their SPF algorithm. Routers in other areas can update their routing tables directly.

Link-State Routing Protocol Benefits

Protocols that Use Link-State

- Two link-state routing protocols, OSPF and IS-IS.Open Shortest Path First (OSPF) - most popular implementation with two versions in use:
  - OSPFv2- OSPF for IPv4 networks (RFC 1247 and RFC 2328)
  - OSPFv3- OSPF for IPv6 networks (RFC 2740)
- Integrated IS-IS, or Dual IS-IS, includes support for IP networks.
- used mainly by ISPs and carriers.



Protocols that Use Link-State

There are only two link-state routing protocols, OSPF and IS-IS.

Open Shortest Path First (OSPF) is the most popular implementation. It was designed by the Internet Engineering Task Force (IETF) OSPF Working Group. The development of OSPF began in 1987 and there are two current versions in use:

- OSPFv2- OSPF for IPv4 networks (RFC 1247 and RFC 2328)
- OSPFv3- OSPF for IPv6 networks (RFC 2740)

Note: With the OSPFv3 Address Families feature, OSPFv3 includes support for both IPv4 and IPv6.

Intermediate System to Intermediate System (IS-IS) was designed by the International Organization for Standardization (ISO) and is described in ISO 10589. The first incarnation of this routing protocol was developed at Digital Equipment Corporation (DEC) and is known as DECnet Phase V. Radia Perlman was the chief designer of the IS-IS routing protocol.

IS-IS was originally designed for the OSI protocol suite and not the TCP/IP protocol suite. Later, Integrated IS-IS, or Dual IS-IS, included support for IP networks. Although IS-IS has been known as the routing protocol used mainly by ISPs and carriers, more enterprise networks are beginning to use IS-IS.

OSPF and IS-IS share many similarities, but also have several differences. There are pro-OSPF and pro-IS-IS factions who discuss and debate the advantages of one

routing protocol over the other. However, both routing protocols provide the necessary routing functionality for a large enterprise or ISP.
Note: Further study of IS-IS is beyond the scope of this course.

Chapter Summary

Conclusion

Dynamic Routing

- Explain the features and characteristics of dynamic routing protocols.
- Explain how distance vector routing protocols operate.
- Explain how link-state protocols operate.

Summary

Dynamic routing protocols are used by routers to facilitate the exchange of routing information between routers. The purpose of dynamic routing protocols includes: discovery of remote networks, maintaining up-to-date routing information, choosing the best path to destination networks, and the ability to find a new best path if the current path is no longer available. While dynamic routing protocols require less administrative overhead than static routing, they do require dedicating part of a router's resources for protocol operation, including CPU time and network link bandwidth.

Networks typically use a combination of both static and dynamic routing. Dynamic routing is the best choice for large networks and static routing is better for stub networks.

When there is a change in the topology routing protocols propagate that information throughout the routing domain. The process of bringing all routing tables to a state of consistency, where all of the routers in the same routing domain or area have complete and accurate information about the network, is called convergence. Some routing protocols converge faster than others.

Metrics are used by routing protocols to determine the best path or shortest path to reach a destination network. Different routing protocols may use different metrics. Typically, a lower metric means a better path. Metrics used by dynamic routing protocols include hops, bandwidth, delay, reliability, and load.

Routing protocols can be classified as either classful or classless, distance-vector or

link-state, and either an interior gateway protocol or an exterior gateway protocol. Distance vector protocols use routers as “sign posts” 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. Modern distance vector protocols are RIPv2, RIPng and EIGRP.

A router configured with a link-state routing protocol can create a complete view or topology of the network by gathering information from all of the other routers. This information is collected using link-state packets (LSPs).

Link-state routing protocols apply Dijkstra’s algorithm to calculate the best path route. The algorithm is commonly referred to as the shortest path first (SPF) algorithm. This algorithm uses accumulated costs along each path, from source to destination, to determine the total cost of a route. The link-state routing protocols are IS-IS and OSPF.

Dynamic Routing

New Terms and Commands

- best path
- Interior Gateway Protocol (IGP)
- Exterior Gateway Protocol (EGP)
- path-vector
- classless
- Routing Information Protocol version 1 (RIPv1)
- Interior Gateway Routing Protocol (IGRP
- Routing Information Protocol version 2 (RIPv2
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPF)
- Intermediate System to Intermediate System (IS-I
- Border Gateway Protocol (BGP)
- classless routing protocols
- autonomous system (AS)
- Distance
- metric
- cost
- periodic updates
- neighbors
- Variable-Length Subnet Mask (VLSM)
- Classless Inter-Domain Routing (CIDR)
- convergence
- route summarization
- Bellman-Ford algorithm
- Dijkstra's algorithm
- Shortest Path First (SPF) algorithm
- Diffusing Update Algorithm (DUAL)
- directly connected networks
- split horizon
- converge
- Convergence time

New Terms and Commands

Dynamic Routing

New Terms and Commands (Cont.)

- multicast addresses
- RIPng
- administrative distance
- SPF tree
- link state information
- OSPF area
- link-state routers
- Hello packets
- Link-State Packets (LSP)
- router ID
- All OSPF routers
- link-state database (LSDB)
- adjacency
- OSPFv2
- OSPFv3

New Terms and Commands


CISCO