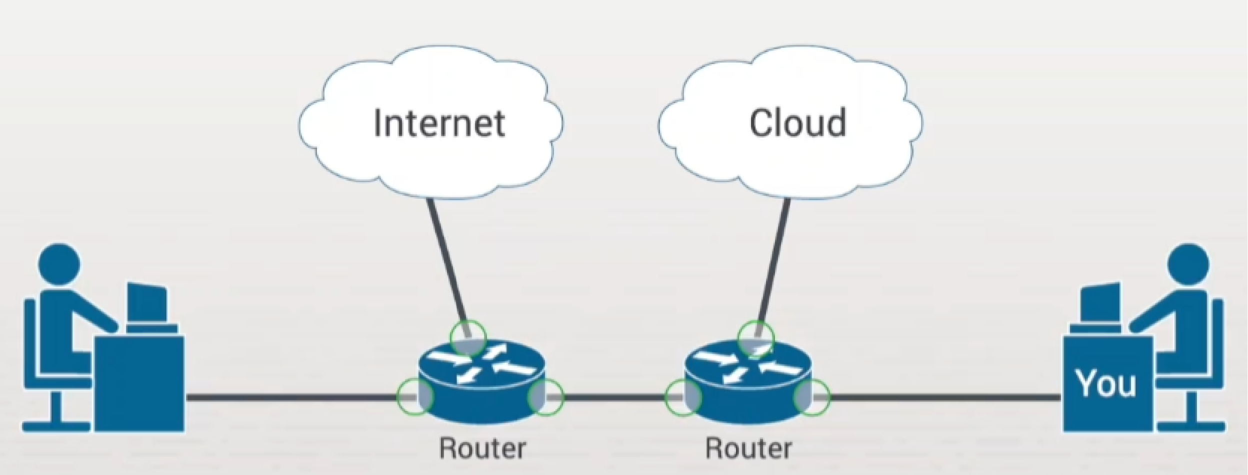
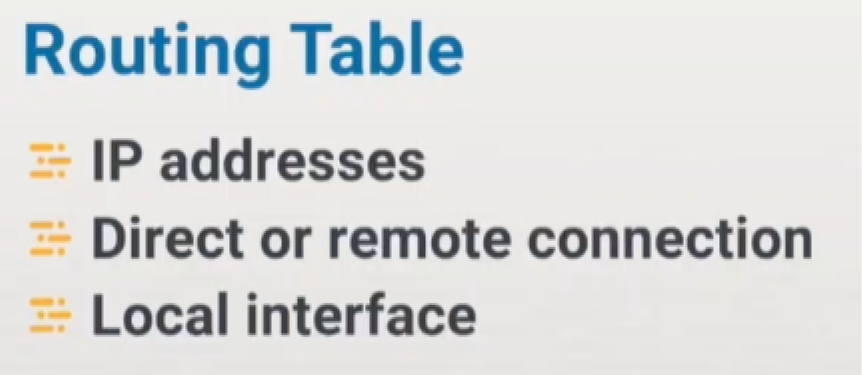
IPv4 Routing Overview



Best Path Determination

Router gathers information from connected devices and stores in routing table.

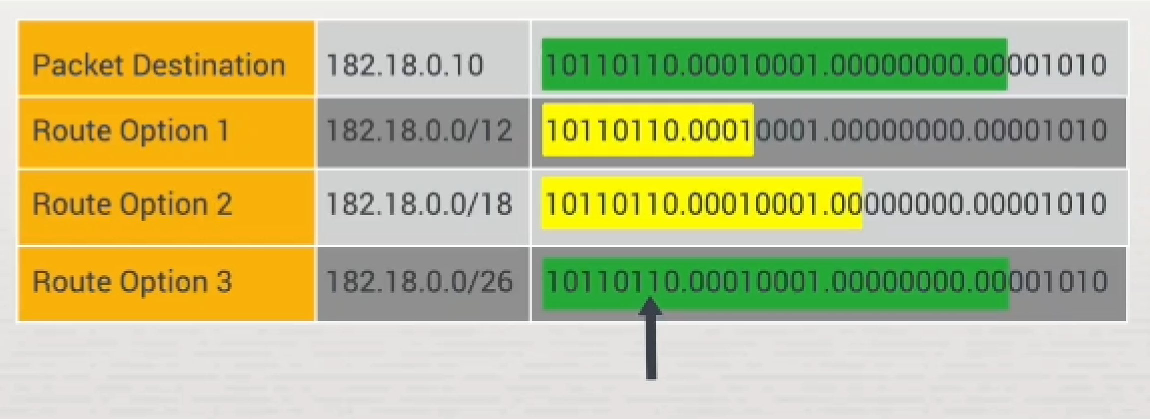


Routing Table

- IP addresses
- Direct or remote connection
- Local interface

The Longest Match

The best match is called the longest match. When comparing routes to the packet's destination IP address, the route with the most left-matching bits, or the longest match, is the preferred route.



Packet Destination	182.18.0.10	10110110.00010001.00000000.00001010
Route Option 1	182.18.0.0/12	10110110.00010001.00000000.00001010
Route Option 2	182.18.0.0/18	10110110.00010001.00000000.00001010
Route Option 3	182.18.0.0/26	10110110.00010001.00000000.00001010

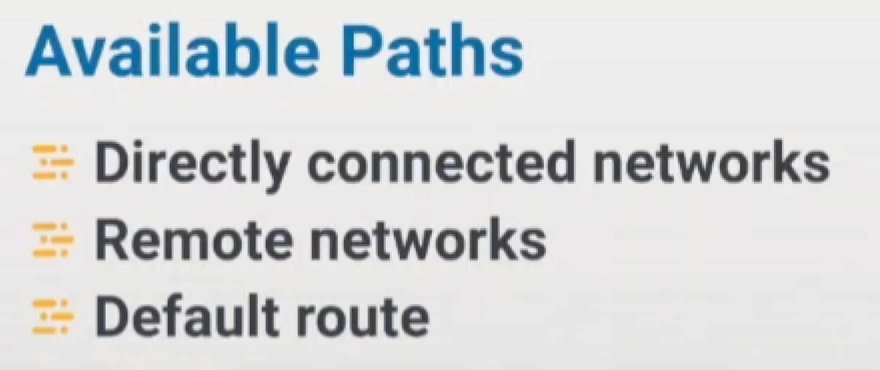
For example, let's say that the destination IP address is 182.18.0.10. Here, you see the IP address in both decimal and binary formats. The router finds three possible routes.

All of them have at least one octet in common. However, since 182.16.0.0/26 has the longest matching IP packet destination, it'll provide the best path.

Once the router has calculated the best path, it sends the packets one of three ways.

If the routing table indicates that the destination device is on a connected network, the router will forward the packet to a directly connected device on that network. For a router to be added to the routing table, the local interface needs to be configured with an IP address and a subnet mask; the interface must also be active.

If the destination is on a remote network, the router will forward the packet to a next hop router. Remote routes can be added to the routing table manually or dynamically. Manually added routes are called static routes. They don't update automatically and must be updated as the network layout changes. Dynamic routes are added to the routing table when the routing protocols learn about the remote network. Dynamic routes update automatically.



Available Paths

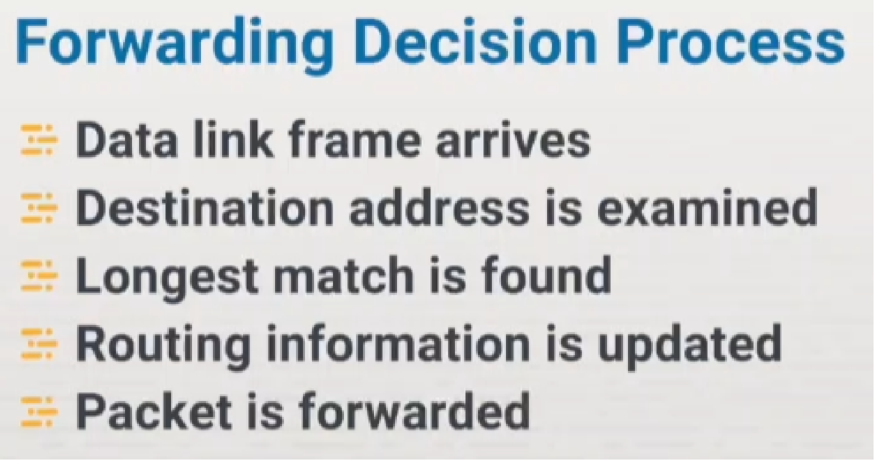
- Directly connected networks
- Remote networks
- Default route

Default Route

If there's no match found in the routing table, the packet will be dropped. You can avoid this by setting a default route in hopes that the next device will have more information on the intended destination. Default routes can be entered manually or can be obtained via the Dynamic Routing Protocols.

Forwarding Decision Process

The main purpose of packet forwarding is to embed packets with the correct data link frame type for the outgoing device. Routers use the forwarding decision process to determine what to do with a packet. After the data link frame arrives with an encapsulated IP address, the router examines the destination address and refers to its routing table. Next, the router finds the longest match. The packet is then encapsulated in a frame with the updated routing information and sent on its way. If no matching route entry is found, the packet is dropped.

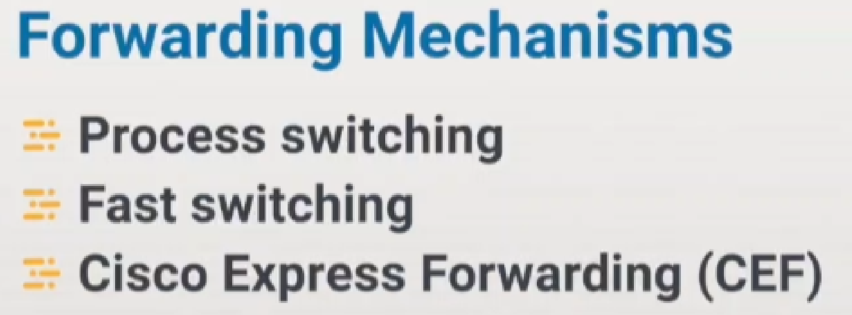


Forwarding Decision Process

- Data link frame arrives
- Destination address is examined
- Longest match is found
- Routing information is updated
- Packet is forwarded

Forwarding Mechanisms

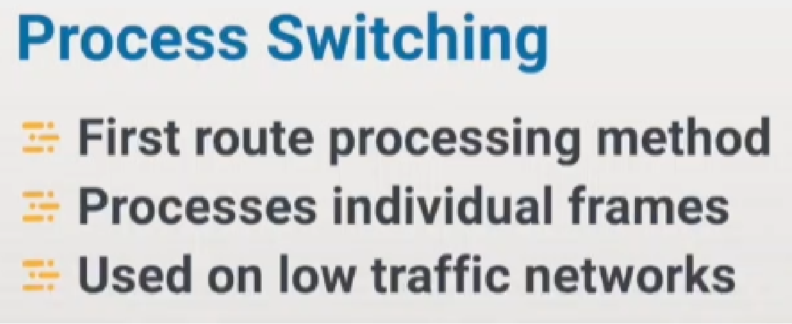
The more efficiently a router can forward packets, the better it is at keeping up with demand. To help with this efficiency, Cisco routers support three packet forwarding mechanisms: process switching, fast switching, and Cisco Express Forwarding, or CEF.



Forwarding Mechanisms

- Process switching
- Fast switching
- Cisco Express Forwarding (CEF)

Process switching was the earliest Cisco route processing implementation. It requires the router to individually process each received frame. That means that packets are individually matched to a routing table and assigned an exit interface. If the routing table is small or if network traffic is minimal, process switching functions well. But in environments where the routing table is large or network traffic is heavy, process switching performs poorly.

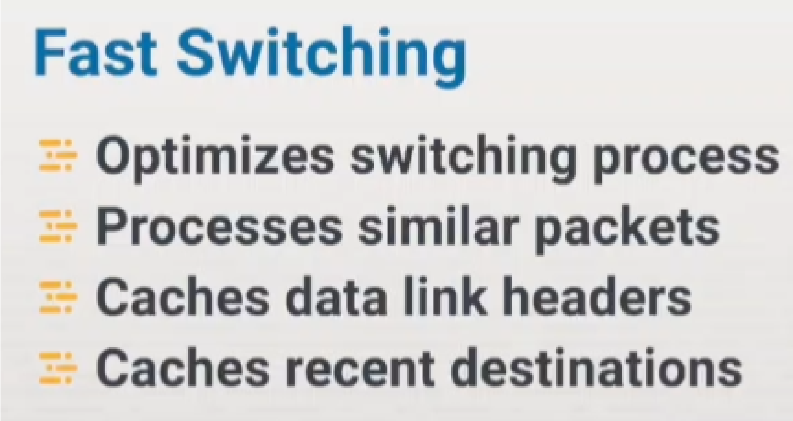


Process Switching

- First route processing method
- Processes individual frames
- Used on low traffic networks

Fast Switching

Fast switching was the next process to come into use. Fast switching processes packets in the same manner as process switching. But it incorporates several mechanisms designed to optimize the process. The key idea behind fast switching is that packets addressed to the same destination can be processed in an identical way. Instead of processing each packet individually, fast switching caches frequently used data link headers and recently used destinations. As additional packets arrive with the same destination address, the next hop information can be reused without you needing to re-evaluate every packet.

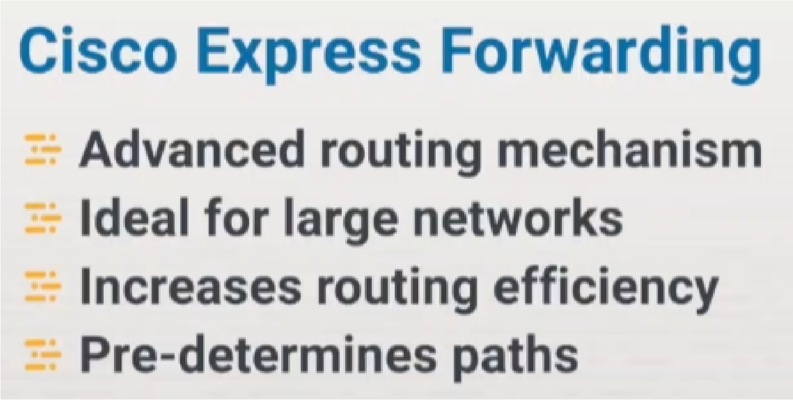


Fast Switching

- Optimizes switching process
- Processes similar packets
- Caches data link headers
- Caches recent destinations

CEF Cisco Express Forwarding

And then we have CEF. CEF is an advanced routing mechanism designed to optimize packet processing in very large networks. CEF increases packet switching speed and reduces the overhead introduced by other routing techniques. It maintains a Forwarding Information Base (or FIB) and an adjacency table to pre-determine forwarding paths.



Cisco Express Forwarding

- Advanced routing mechanism
- Ideal for large networks
- Increases routing efficiency
- Pre-determines paths

Routing Table Facts

There are many technologies working together to ensure that when you click something on a website, you get a quick response. Routers are probably the most important technology at work here because a router transfers traffic from one network to the next.

Routing Table

A routing table is a list of routes to known networks. This information is gathered from directly connected networks, static routes, and dynamic routing protocols. When configuring static routes and dynamic protocols, it is important to remember the following principles:

- Each router makes a decision based on the information that it has in its routing table.
- A routing table will not always match the routing table of another router.
- Routing information does not provide information about a return route.

The router uses the routing table to determine where to send packets. When a packet is received, the router compares the destination IP address contained in the packet with all known routes in the routing table. Keep in mind:

- The destination address is compared to the networks in the routing table in order to find a match.
- A match is made when the destination IP address is on the same subnet as indicated by the route in the routing table.
- The IP address might match more than one route in the routing table. If that is the case, the most specific routing table entry is used. That is the network with the subnet mask that has the greatest number of significant bits.
- When a match is found, the packet is sent out the specified router interface to the next hop router address.
- If no match is found, the packet is dropped (not forwarded).

The routing table includes the following components:

Component	Description
Route source	The route source is indicated using one of the following codes: • L indicates the address of a local router interface • C indicates a directly connected network • S indicates a static route used to reach a certain network • P indicates a dynamic network learned using the OSPF routing protocol • R indicates a dynamic network learned using the RIP routing protocol

Prefix and prefix length	The network address and subnet address for the destination route.
Administrative distance	The administrative distance is a description of the trustworthiness or preferability of a route. It is learned from a specific source. Each source type (such as each routing protocol) is given an administrative distance value. A lower number indicates a more preferred route.
Metric	The metric identifies how far away the destination is, either in distance or time. The lower the metric, the higher the preference of the route.
Next-hop	The next-hop is the IP address of the next router that the packet will be forwarded to.
Route timestamp	The route timestamp indicates how much time has passed since the route was learned.
Exit interface	The interface used for sending packets to their destination.

Longest Match

When a router receives a packet, it reviews the routing table to decide the best path to take. The best match is referred to as the longest match. When comparing routes to the packet's destination IP address, the route with the most left matching bits, the longest match, will be the preferred route.

The routing table entries include a prefix and a prefix length/subnet mask. See the example below:

Route Entry	Prefix and Prefix Length	IP Address in Binary
Route Entry 1	182.17.0.0/12	**10110110.0001**0001.00000000.00001010
Route Entry 2	182.17.0.0/18	**10110110.00010001.00000000.00**001010
Route Entry 3	182.17.0.0/26	**10110110.00010001.00000000.00**001010

Let’s say that the destination IP address is 182.17.0.10. Since 182.17.0.0/26 has the longest matching IP packet destination, it would provide the best path.

Packet Destination	182.17.0.10	**10110110.00010001.00000000.00**001010

Available Paths

Once the router has calculated the best path, it will do one of three things:

Action	Description
Directly connected networks	If the routing table indicates that the destination device is on a connected network, the router will forward the packet to the directly connected device on that network. In order for a router to be added to the routing table, the local interface must be active and configured with an IP address and a subnet mask.
Remote networks	If the destination is on a remote network, the router will forward the packet to a next-hop router. Remote routes can be added to the routing table manually or dynamically. Manually added routes are referred to as static routes. Static routes will not update automatically and must be updated as network layout changes. Dynamic routes are added to the routing table when the associated routing protocols learn about the remote network. Dynamic routes update automatically.
Default route	If there is no match found in the routing table, the packet will be dropped. This can be avoided by setting a default route in hopes that the next device will have more information on the intended destination. Default routes can be entered manually or can be obtained via dynamic routing protocols.

Packet Forwarding

The main purpose of packet forwarding is to place packets into the correct data link frame type for the outgoing device. Routers use the following packet forwarding decision process:

1. The data link frame arrives with an encapsulated IP address.
2. The router examines the destination address and refers to its routing table.
3. The router finds the longest match in the routing table.
4. The router encapsulates the packet in a frame with the updated routing information.
5. If there is no matching route entry, the packet is dropped.

The more efficiently a router can forward packets, the better it will be at keeping up with demand. To help with this efficiency, Cisco routers support three packet forwarding mechanisms:

Mechanism	Description
Process switching	Process switching was the earliest Cisco route processing implementation. Process switching required the router to process each received frame individually using the steps outlined above. If the routing table is small or if network traffic is minimal, process switching functions adequately. However, in environments with large routing tables or heavy network traffic, process switching performs poorly.
Fast switching	Fast switching processes packets in the same manner as process switching; however, it incorporates several mechanisms designed to optimize the process. The key idea behind fast switching is that packets addressed to the same destination can be processed in an identical manner. Instead of processing each packet individually, fast switching caches frequently used data link headers and recently used destinations.
Cisco Express Forwarding (CEF)	CEF is an advanced routing mechanism designed to optimize packet processing in very large networks. CEF increases packet switching speed and reduces the overhead introduced by other routing techniques. CEF maintains a Forwarding Information Base (FIB) and an adjacency table to pre-determine forwarding paths.

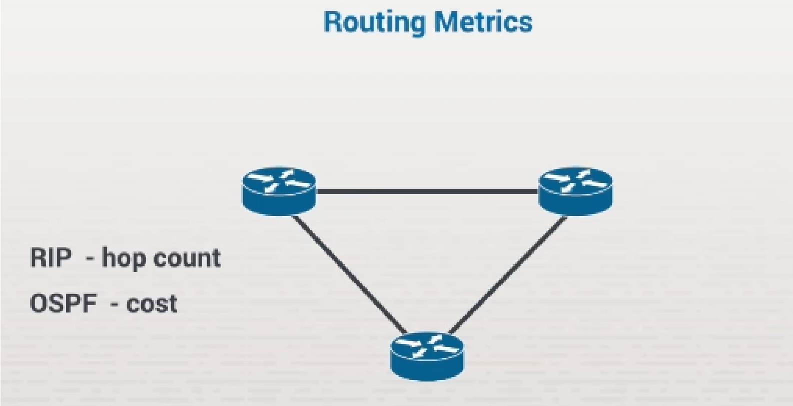
Cisco express forwarding (CEF) maintains adjacency tables, which contain Layer 2 information linked to a particular entry in the forwarding information base (FIB). This reduces the need to send ARP requests before forwarding packets, which increases the speed of the routing process. CEF builds the adjacency table using information from the ARP table.

The FIB maintains a mirror image of the forwarding information contained in the IP routing table, specifying the next-hop address for a particular IP route. Both CEF and fast switching cache frequently used data link headers, allowing them to be copied instead of reconstructed from scratch every time a packet is forwarded. Likewise, both CEF and fast switching cache recently used destinations, requiring the router to consult the routing table only if a packet's destination address is not in the cache.

Routing Metrics

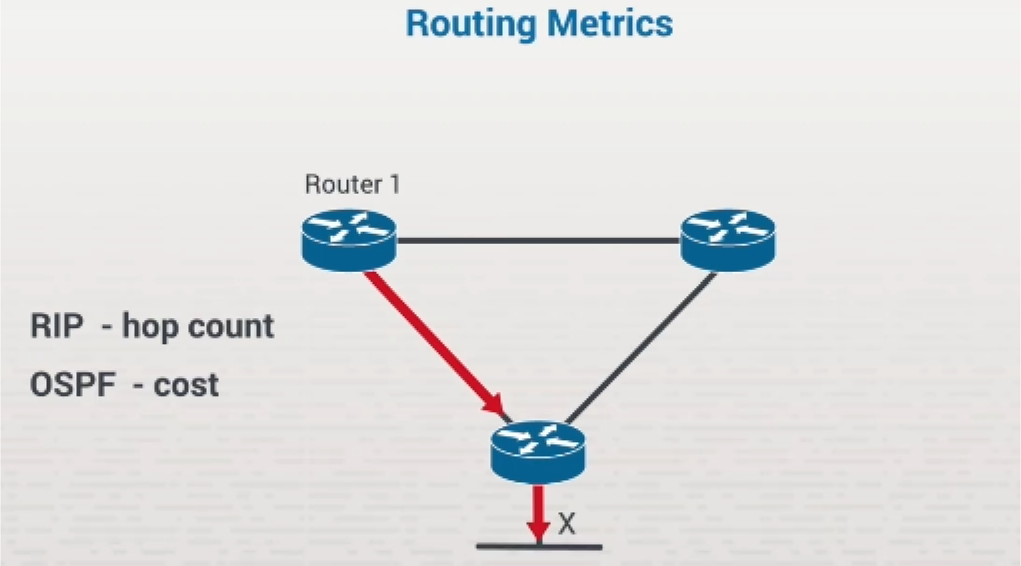
Routing protocols use metrics to decide which path to take when there's more than one way to get to a remote network.

Routing protocols use different factors for metrics. For example, RIP, the Routing Information Protocol, uses something called hop count to determine the best path. OSPF, the Open Shortest Path First Protocol, is smarter and more efficient; it uses something called cost. Let's compare the two.



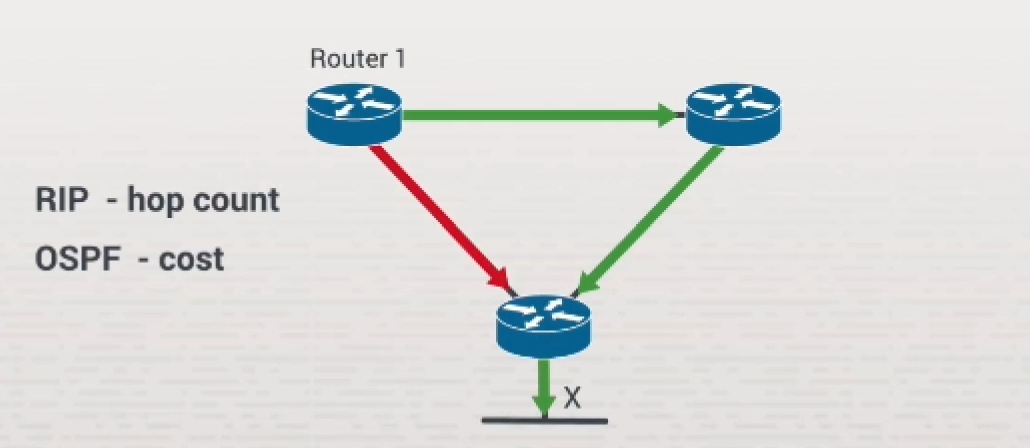
Routing Information Protocol

RIP is only concerned with hops, or the number of routers we have to cross to get to the destination network. From Router 1's perspective, there are clearly two ways to get to Network X. We could take the path down this left side and jump over or get routed by this router, and now, I'm on X.



That represents a one-hop path. We could take the other route, go off to the right hop, get routed, go down to the router on the bottom, hop again, get routed, and land on X. The path down the left side is a single hop. X is one hop away from Router 1.

If we go around the right side, we have to jump over two routers to get to X, so that's a hop count of two.

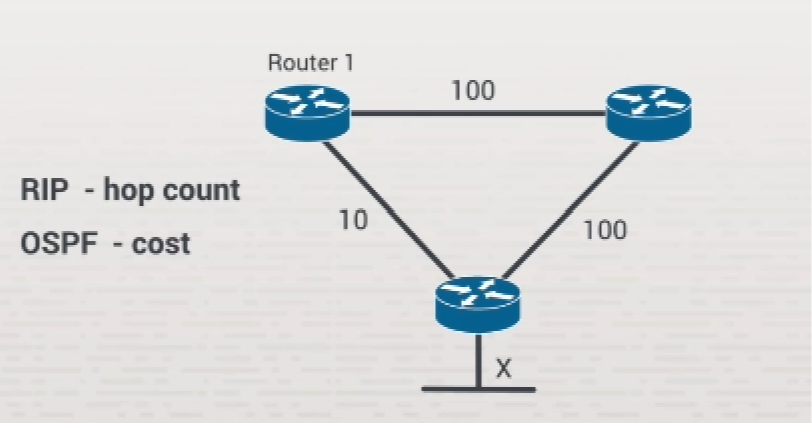


The lower the metric, the better the path. So, in this case, Router 1 would choose the left path, down the left, for all traffic destined for X. Any packet that Router 1 receives intended for network X will traverse down this left side. In fact, it won't use this other pathway at all unless something happens to the path on the left. In that case, Router 1 will fail over to the only remaining route to X at that time.

As you can see, RIP doesn't consider the bandwidth of the connections at all. It doesn't consider speed, delay, or anything related to performance. It just looks at the number of routers there are to jump over, and the lowest hop count wins.

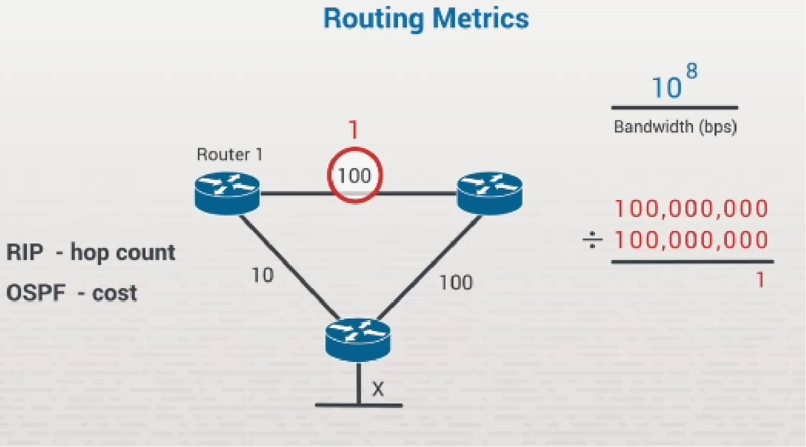
Open Shortest Path First (OSPF)

Let's compare that to OSPF. OSPF uses a metric called cost, and cost is factored into the bandwidth of the connections.



To demonstrate this, we need to know the bandwidth values of these connections. At the top we have a 100-megabit-per-second link. The next link is the same. And this third link is a 10-megabit-per-second link.

OSPF cost is calculated based on this formula: 10 to the 8th divided by the bandwidth of the link in bits per second. It calculates based on each link it has to cross to get to the destination network. Let's consider the 100-megabit-per-second links first. 10 to the 8th is a 1 with eight 0s behind it. 100 megabits per second is one million bits per second, so it's the same number in this case. One divided by the other equals 1. The OSPF cost of that link on top is 1.



Routing Metrics

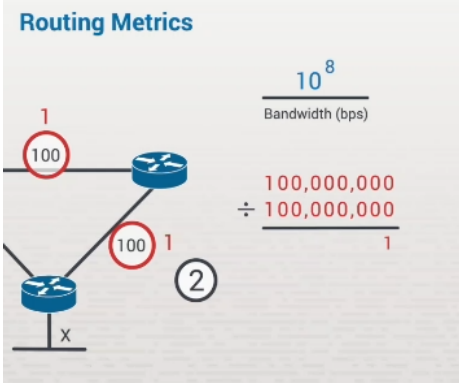
RIP - hop count

OSPF - cost

$$\frac{10^8}{\text{Bandwidth (bps)}}$$

$$\begin{array}{r} 100{,}000{,}000 \\ \div\ 100{,}000{,}000 \\ \hline 1 \end{array}$$

The same is true over here. If Router 1 took the path through both of those links, its cumulative cost, or metric, would be 2.



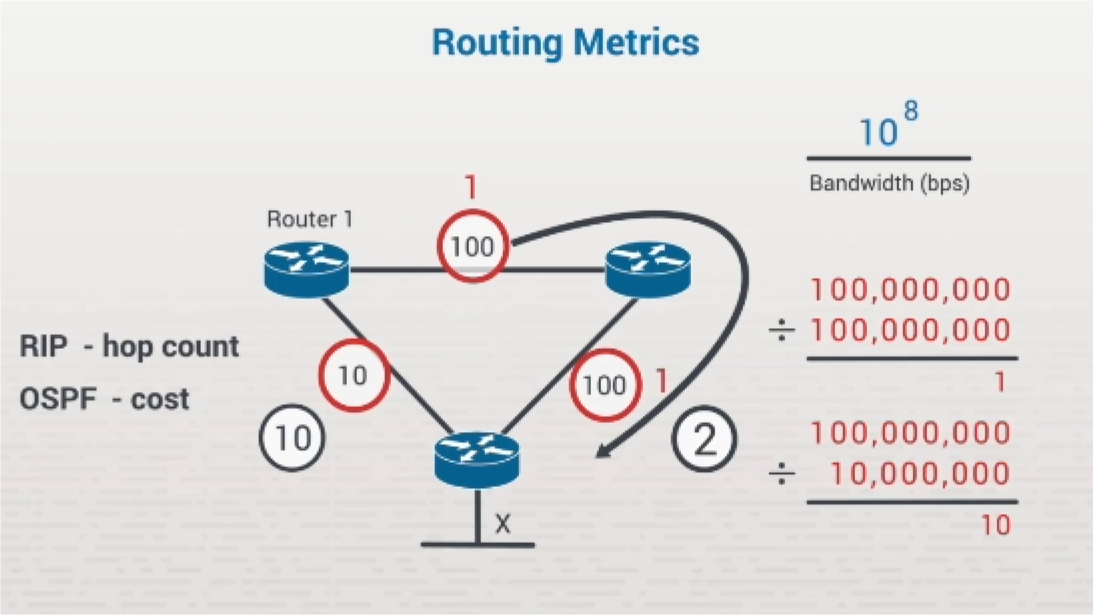
Routing Metrics

$$\frac{10^8}{\text{Bandwidth (bps)}}$$

$$\begin{array}{r} 100{,}000{,}000 \\ \div\ 100{,}000{,}000 \\ \hline 1 \end{array}$$

Let's take a look at the 10-megabit-per-second connection now. It's the same formula: 10 to the 8th divided by 10 million bits per second, and that comes up with 10. The cost of this path to OSPF is going 10. Just like in RIP, the lowest metric wins. Two is lower than 10, so all traffic in this case.

OSPF is smart enough to recognize that it's going to be faster to send data around this--what appeared to be a longer path to X--than it would be to go over the single link on the left because of its lower speed.



RIP was based only on hop counts, so it didn't have the intelligence to recognize that the 10 megabit-per-second link on the left is actually a slower connection, and that going the other direction is faster. Like we saw with RIP, something broke in this pathway that OSPF had selected. And then, of course, OSPF would start sending data down this slower connection. At that point, it would be the only remaining path.

Administrative Distance (AD)

Routers use AD when there are multiple sources of information about remote networks. It helps them determine which source is most trustworthy and which routing protocol or source will actually populate the routing table.

Now, remember that different routers use different factors to determine the best path to a network number. Here, we have a simple network with three routers, and we're going to focus on the segment on the bottom. I'm going to label it Network X. And we also have RIP (Routing Information Protocol) and OSPF (Open Shortest Path First Protocol) using different metrics to determine the best path.

From Router 1's perspective, we learned that RIP would always prefer this path to get to Network X because there's only one hop to the next network. The other connection would require two hops.

While RIP values hop counts, OSPF values bandwidth. In this scenario, OSPF would actually prefer the long way around to get to Network X because of the faster connection speed. There are two 100-megabit-per-second links, which actually results in a lower metric than if I had used this slower 10-megabit-per-second link.

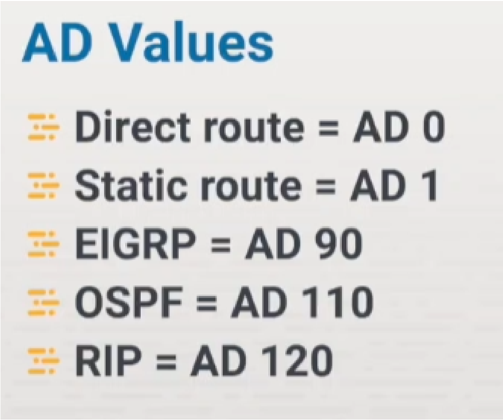
So, let's say that you have both RIP and OSPF active on each of these three devices. If RIP prefers this path, but OSPF prefers this path, Router 1 has to make a choice. RIP is saying, "Hey, I think we should send all the traffic down this path to get to Network X." OSPF says, "I have a better idea. Let's send all the data around this faster path because of the better bandwidth." Which information does Router 1 actually trust? That's where administrative distance comes in handy.

Administrative Distance

Sources of information, such as routing protocols, have default AD values associated with them. If I have multiple sources of information feeding me data, I trust the one with the lowest AD.
A directly connected route is always the most trustworthy source of information. So, this means that two types of ports will always give us the lowest AD: an Ethernet port and a Wide Area Network, or WAN port. Both will have an AD of 0. That's the most trusted value.

A statically defined route is the next lowest. Those have an AD of 1. Because you need to enter a static route manually, the router assumes that if you took the time to type it in, then it must be trustworthy.

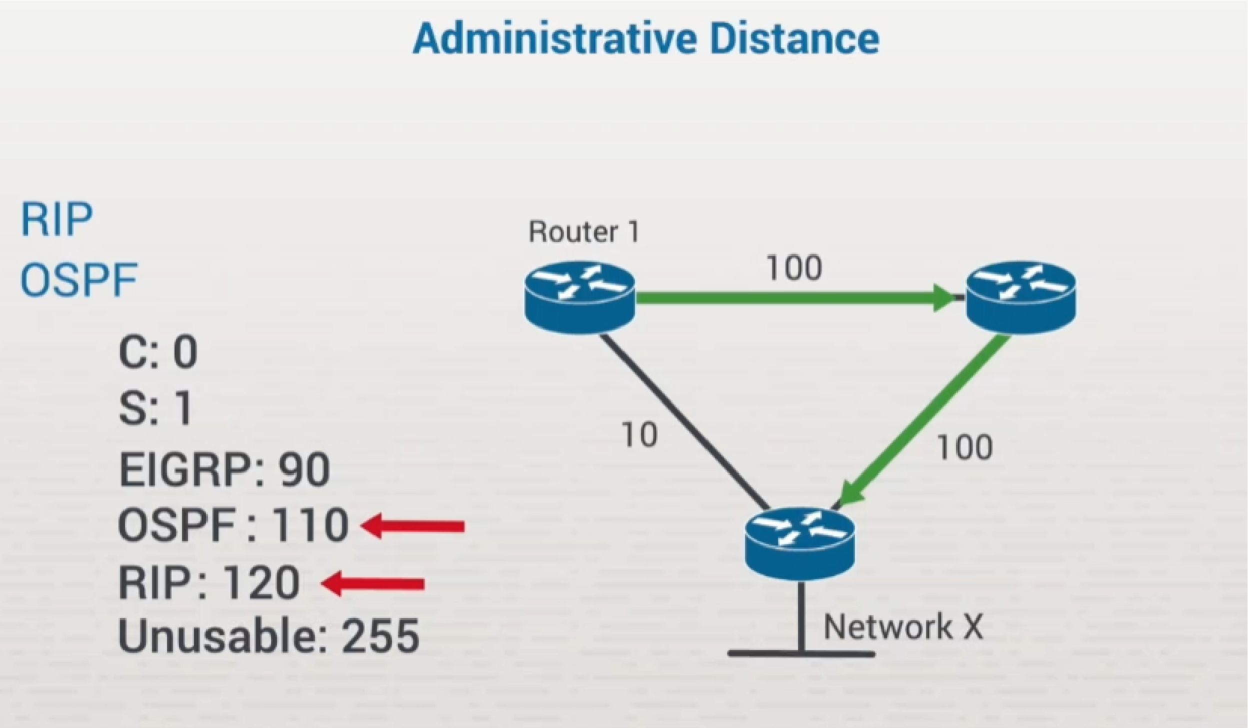
What about the routing protocols? Each protocol has a default starting value that you can override, depending on your network needs. Enhanced Interior Gateway Routing Protocol (EIGRP) is set at 90 by default. OSPF defaults to 110. RIP has a default value of 120. The highest AD value you'll ever see is 255, which is considered unusable.



AD Values

- Direct route = AD 0
- Static route = AD 1
- EIGRP = AD 90
- OSPF = AD 110
- RIP = AD 120

Knowing this, let's look at our example again. Router 1 is getting information from both RIP and OSPF. Which one is it going to trust? Since OSPF is 110 and the RIP value is 120, OSPF is considered the more trustworthy source. For this reason, the OSPF route is inserted into Router 1's routing table, but the RIP route is not. All traffic intended for Network X will follow the pathway set by OSPF. If OSPF weren't running, then, obviously, the RIP route would be installed in the routing table instead.


Administrative Distance

RIP
OSPF

C: 0
S: 1
EIGRP: 90
OSPF : 110
RIP: 120
Unusable: 255

Administrative Distance Facts

Administrative distance (AD) is a value used to rank route sources, such as a static route or a specific routing protocol. Routers use administrative distance to determine the best path when there are multiple sources of information about remote networks. It is not uncommon for routers to be configured with a combination of static routes and multiple routing protocols. As a result, there may be more than one route source for the same remote network. The AD determines the trustworthiness of the route source.

AD helps routers determine which source is most trustworthy and which routing protocol or source will populate the routing table. Routing protocols use metrics to determine the path to take when there's more than one way to get to a remote network. Each routing protocol uses different factors for metrics. For example, RIP focuses on the hop count metric. The hop count is the number of routers data will be routed through to get to the destination network. OSPF is a more efficient protocol that relies on a metric called cost. The cost is determined based on the bandwidth of the available connections. EIGRP considers bandwidth, delay, load, and reliability.

Assuming that two routes are available to the same location, the router will use the following criteria for choosing between these routes:

- If a static route is available, it will be selected.
- If a router learns of two routes to a remote network through different routing protocols (such as RIP and OSPF), it will choose the route with the lowest administrative distance; OSPF in this example.
- If a router learns of two routes through the same protocol (for example two routes through EIGRP), the router will choose the route that has the best cost as

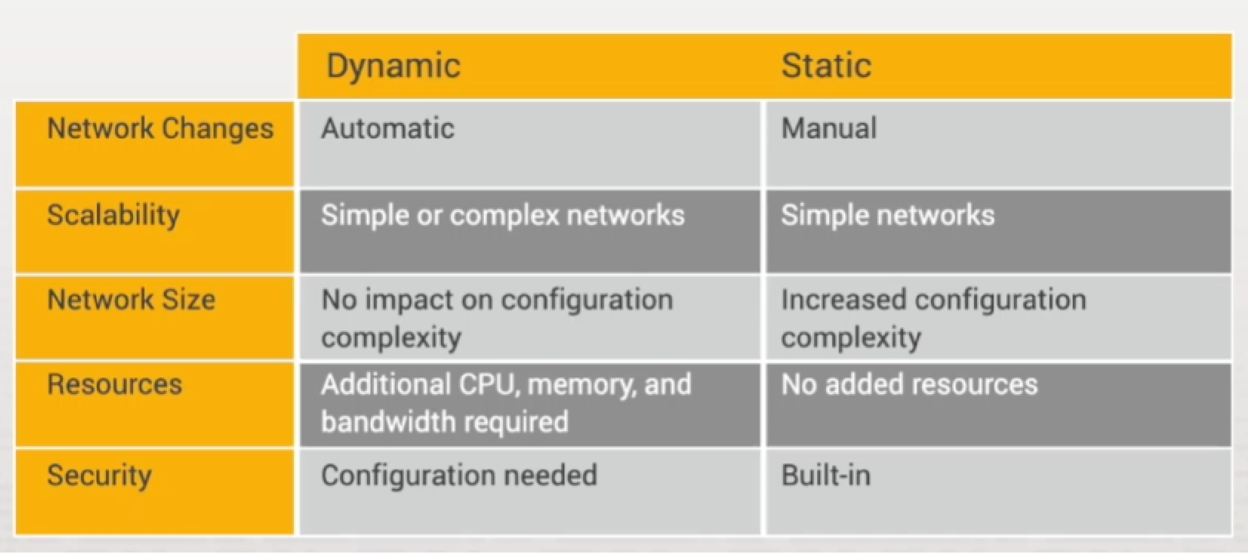
defined by the routing metric. For EIGRP, the link with the highest bandwidth and least delay will be used.

You can modify how routes are selected by modifying the administrative distance associated with a source. The route with the lowest AD is chosen.

The following table lists the various route sources and their administrative distances:

Route Source	Description
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

Static vs. Dynamic Routing



	Dynamic	Static
Network Changes	Automatic	Manual
Scalability	Simple or complex networks	Simple networks
Network Size	No impact on configuration complexity	Increased configuration complexity
Resources	Additional CPU, memory, and bandwidth required	No added resources
Security	Configuration needed	Built-in

*Most networks use a combination of both

There are four types of static routes:

- Standard Static Route
- Default Static Route
- Summary Static Route
- Floating Static Route

Route Type	Description
Standard static route	Standard static routes can be used when connecting to a remote network. If data is frequently exchanged between networks, there's no need to use a dynamic routing protocol. Instead, an administrator can configure a direct route between the two networks, saving resources each time data is exchanged.

Default static route	Default static routes are used in two instances: ● If there is only one router on your network, you can set up a default static route to direct to the ISP, packets with IP addresses not in the routing table. ● Similarly, in a larger network, a default route can be used when the IP address does not match an entry in the routing table. In the event that packets are destined to a destination outside of an organization, the packets are sent through an edge router to the company's internet service provider. Be aware of the following default route details: ● Default routes work best when only one path exists to a part of the network. ● One default route in the routing table could replace hundreds of static entries in the routing table. ● When the default route is not set, the router discards packets that do not match a route in the routing table.
Summary static route	A summary static route is used to minimize the number of routing table entries. Multiple static routes can be combined into one static route if the networks are touching or use the same next-hop address.
Floating static route	Floating static routes are backup routes. If one link fails, the floating route is to be used. This is accomplished by setting a higher administrative distance to the backup route. By default, the administrative distance of a static route is 1, but the distance can be increased to ensure that it serves as a backup route.

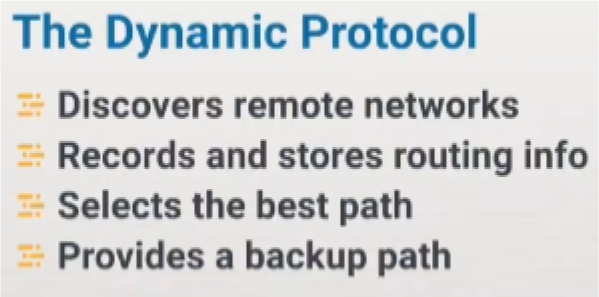
Dynamic Routing Overview

- **Routing Information Protocol (RIP)** is a distance-vector protocol that uses hop count as its primary metric.
- **RIP** - was first dynamic routing protocol. Still used for smaller networks.

Four Main Responsibilities of Routing Protocols

Routing protocols are used to share routing information between devices. These protocols have four main responsibilities:

- discovering remote networks,
- recording and storing current routing information,
- selecting the best path to each destination,
- and providing a backup path to use if the preferred path becomes unavailable.



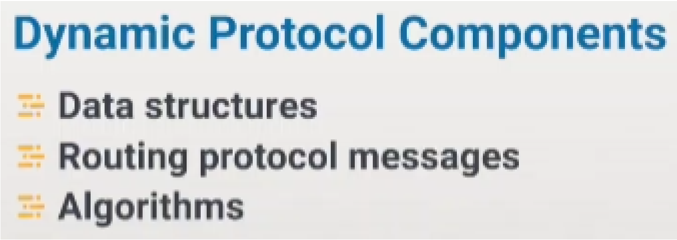
The Dynamic Protocol

- Discovers remote networks
- Records and stores routing info
- Selects the best path
- Provides a backup path

Dynamic Protocol Components

Dynamic routing protocols have three main components.

- First, there are data structures. Routing protocols maintain structured databases in the system RAM.
- Second, routing protocol messages are used to obtain and maintain information about a network. These messages aid in the discovery and exchange of information with nearby routers.
- Lastly, algorithms are finely detailed lists that routing protocols use to manage routing information and determine the best paths. Once a route is selected, it's added to the routing table--if there isn't a better route available to the same destination.



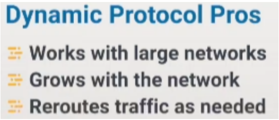
Dynamic Protocol Components

- Data structures
- Routing protocol messages
- Algorithms

Once a route is selected, it's added to the routing table--if there isn't a better route available to the same destination.

Dynamic Protocol Pros

These protocols are useful for larger networks, especially networks that have multiple routers. They continue to work despite network growth. And they automatically adapt to reroute traffic as needed.

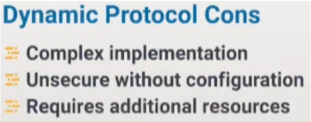


Dynamic Protocol Pros

- Works with large networks
- Grows with the network
- Reroutes traffic as needed

Dynamic Protocol Cons

First, their implementation is fairly complex. Because the router is continuously advertising information about the network to neighboring devices, dynamic protocols aren't secure without additional configuration. And the ongoing communication, processing, and storage increase the amount of processing power, memory, and bandwidth that's needed.



Dynamic Protocol Cons

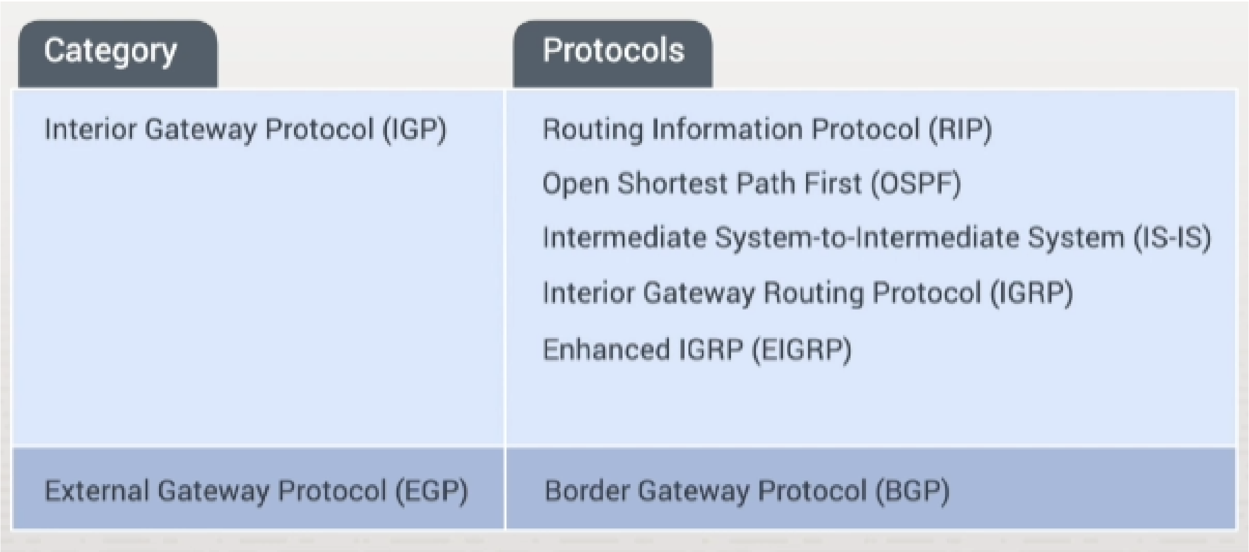
- Complex implementation
- Unsecure without configuration
- Requires additional resources

Internal Routing vs External Routing

Each organization that's assigned a network address from an ISP is considered an autonomous system, or AS. The organization is free to create one large network or to divide the network into segments. Each autonomous system is identified by an AS number. This number is either locally administered or registered if it's connected to the internet.

- Routers are used within an autonomous system to segment the network. They're also used to connect multiple autonomous systems together.

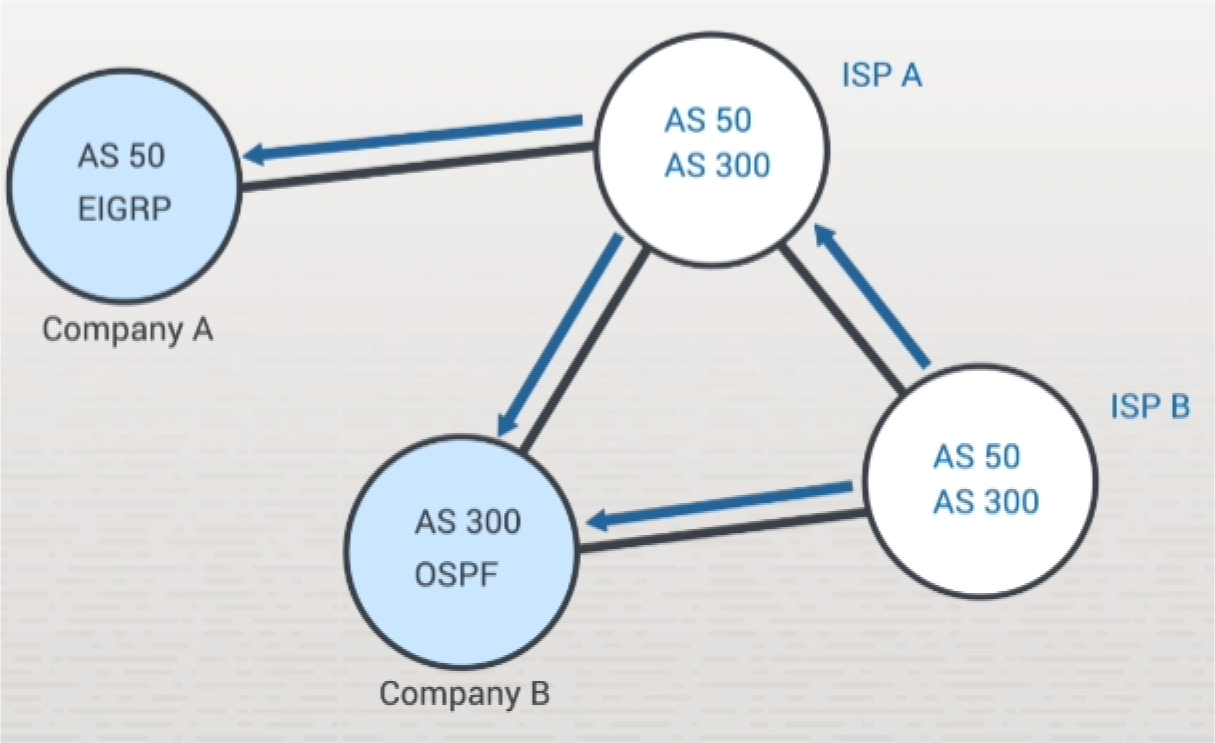
- **Routing protocols can be classified based on whether they're routing traffic within or between autonomous systems**.
  - **Internal routing protocols**, also known as interior gateway protocols, are used to send information between devices in an organization's routing domain. A few examples are RIP, OSPF, IS-IS, IGRP, and Enhanced IGRP, or EIGRP for short.
  - **External routing protocols.** They're also known as external gateway protocols, or EGPs for short. ISPs use them to send packets across the internet from one internal network to another. BGP is the only external protocol



Category	Protocols
Interior Gateway Protocol (IGP)	Routing Information Protocol (RIP) Open Shortest Path First (OSPF) Intermediate System-to-Intermediate System (IS-IS) Interior Gateway Routing Protocol (IGRP) Enhanced IGRP (EIGRP)
External Gateway Protocol (EGP)	Border Gateway Protocol (BGP)

BGP Example

In this scenario, we have two companies. Each company is connected to a single ISP. Each of these balloons forms an exterior gateway protocol perspective. Company A could be AS 50. Company B could be AS 300. Company A might be using EIGRP as their internal routing protocol, while company B might be using OSPF as its routing protocol. Or both organizations might be using a combination of dynamic protocols and static routes.



BGP is an external routing protocol that's only concerned with delivering data to the front door of your autonomous system. What happens after it's delivered to your front door is determined by your internal routing processes. BGP routing tables are, fundamentally, a list of AS numbers across the internet and the next hop required to get closer to them. The other protocols – RIP, OSPF, and EIGRP – are interior protocols that are used to route traffic within a single autonomous system.

Dynamic Routing Facts

Routing protocols share routing information between devices. These protocols have four main responsibilities:

- Discover remote networks
- Record and store current routing information
- Select the best path to each destination
- Provide a backup path

This lesson covers the following topics:

- RIP vs. dynamic routing
- Internal vs. external routing
- Load balancing
- Best path determination
- Protocols used by IP version

RIP vs. Dynamic Routing Protocols

As computer networks became more complex and more widespread, Routing Information Protocol (RIP) was improved, but it just wasn't enough to keep up with the demands larger networks. Although RIP is still used for smaller networks, additional protocols have been designed to support larger networks. Dynamic protocols are now most commonly used, especially for larger networks.

Dynamic routing protocols have three main components:

- Data structures
- Routing protocol messages
- Algorithms

Dynamic protocols are useful for any network with multiple routers. These protocols work well to accommodate network growth. Additionally, dynamic protocols automatically adapt to reroute traffic when needed. Because the router is continuously advertising information about the network to neighboring devices, dynamic protocols are not secure without additional configuration. When considering dynamic routing, keep in mind that it's complex to implement and has increased CPU, RAM, and bandwidth requirements for ongoing communication, processing, and storage.

Internal vs. External Routing

Each organization with an assigned network address from an ISP is considered an autonomous system (AS). The AS is free to create one large network or divide the network into segments (subnets). Each autonomous system is identified by an AS number. This number can be either locally administered or registered if the AS is connected to the internet.

Routers are used within an autonomous system to segment the network. In addition, autonomous systems are used to connect multiple autonomous systems together. Internal routing protocols, also known as Interior Gateway Protocols (IGPs), are used to send information between devices within an organization's routing domain. An external routing protocol, External Gateway Protocol (EGP), is used by ISPs to send packets across the internet from one network to another. The following table identifies protocols classified as IGPs and EGPs.

Classification	Protocols
Interior Gateway Protocols (IGPs)	IGPs include the following: • Routing Information Protocol (RIP) • Open Shortest Path First (OSPF) • Interior Gateway Routing Protocol (IGRP) • Intermediate System-to-Intermediate System (IS-IS) • Enhanced IGRP (EIGRP)

Exterior Gateway Protocols (EGP)	Border Gateway Protocol (BGP) is an EGP.

BGP is an external routing protocol that coordinates routing between autonomous systems on the internet. BGP routing tables are a list of AS numbers across the internet and the next hop required to get to them. Once the BGP delivers data from the internet to your network, interior gateway protocols (RIP, OSPF, and EIGRP) are used to route traffic within the AS that is your network.

Load Balancing

In the event a router has more than one path to the same destination with the same cost metric, the router will forward the packets using both paths. This process is called *equal cost load balancing*. The routing table has one destination but uses a different exit interface to forward packets on each of the equal cost paths. Load balancing is automatically implemented by dynamic routing protocols and can improve network performance.

Best Path Determination

Routing protocols consider various routes to a destination and select a route based on the distance to that network. The best path is the path with the lowest metric. Each protocol has a different method for setting metrics as shown in the following table:

Routing Protocol	Metric
Routing Information Protocol (RIP)	RIP considers hop count. *Hop count* is determined by the number of routers along a path. Each router equals one hop count. No more than 15 hop counts are permitted for a route.
Open Shortest Path First (OSPF)	OSPF considers the cost. Cost is determined by the total bandwidth available from origination to destination. Better bandwidth gets a lower cost. Slower bandwidth gets a higher cost.
Enhanced Interior Gateway Routing Protocol (EIGRP)	EIGRP uses a metric that considers the slowest bandwidth, dependability of a path, load, and delay values.

There are three primary algorithms used to determine the best path:

- Distance vector
- Link state
- Path vector

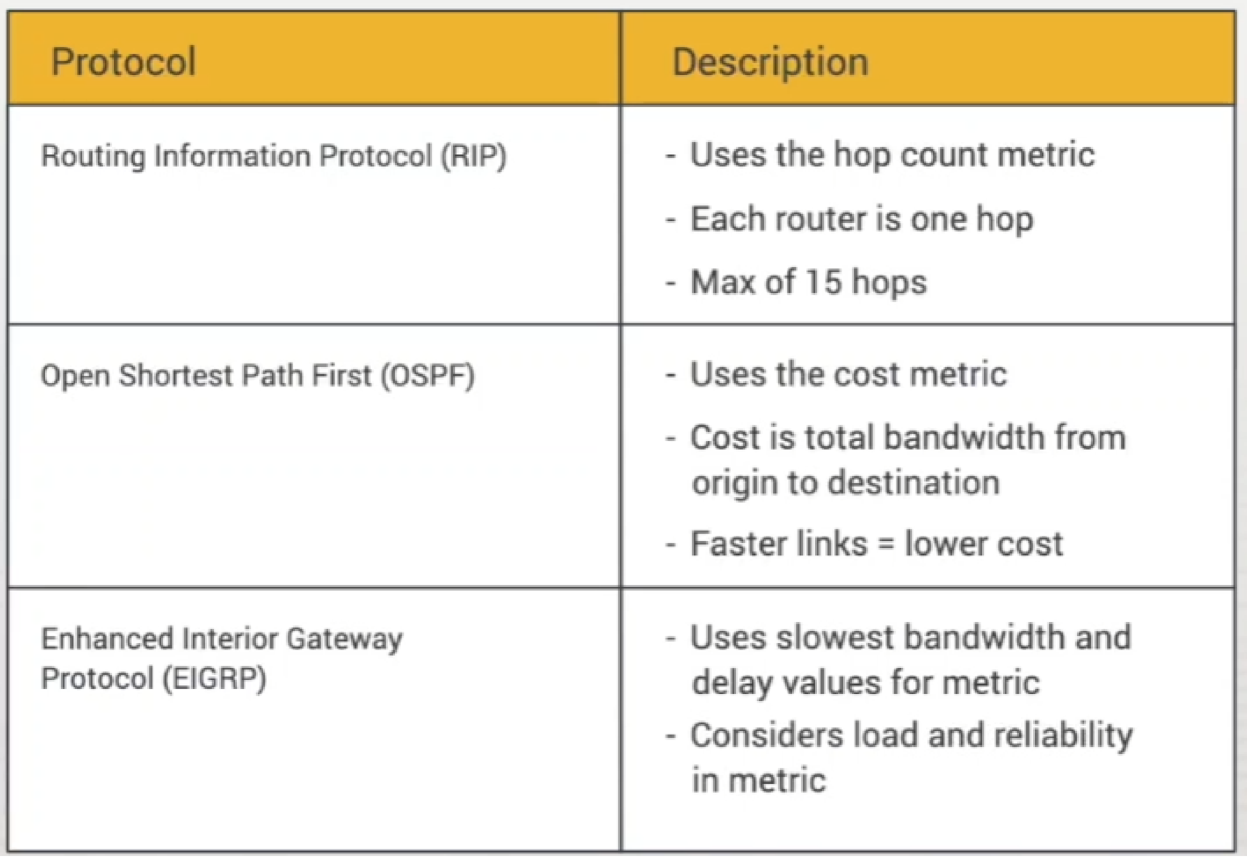
Protocols Used by IP Version

The following table identifies protocols used by IPv4 and IPv6:

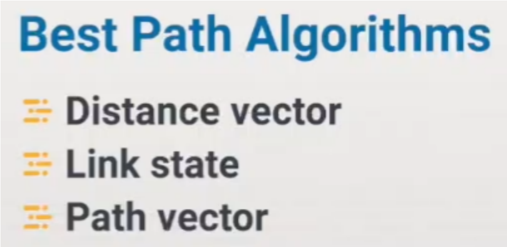
IP Version	Distance Vector	Link-State	Path Vector
IPv4	RIPv2 EIGRP	OSPFv2 IS-IS	BGP-4
IPv6	RIPng EIGRP for IPv6	OSPFv3 IS-IS for IPv6	BGP-MP

Best Path Determination

Protocol methods for determining metric.
RIP, OSPF, EIGRP



Protocol	Description
Routing Information Protocol (RIP)	- Uses the hop count metric - Each router is one hop - Max of 15 hops
Open Shortest Path First (OSPF)	- Uses the cost metric - Cost is total bandwidth from origin to destination - Faster links = lower cost
Enhanced Interior Gateway Protocol (EIGRP)	- Uses slowest bandwidth and delay values for metric - Considers load and reliability in metric



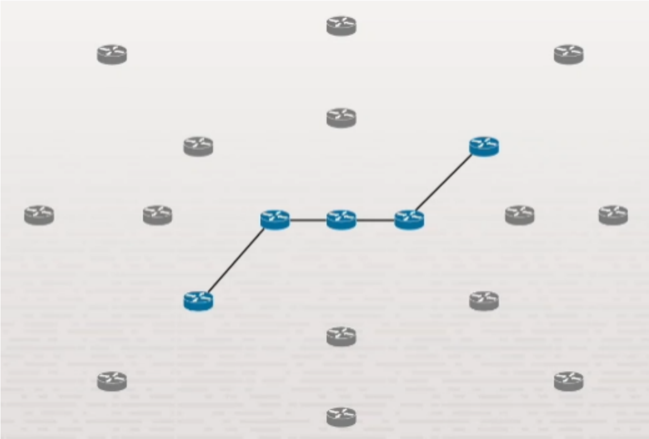
Best Path Algorithms

- Distance vector
- Link state
- Path vector

Distance vector protocols

Distance vector protocols slow convergence. Convergence is how quickly the network realizes that a change has occurred and that the routing tables are stable again. All the routers have to update if a new network comes up, or an existing network number goes down. This happens via routing protocols, but it takes longer for distance vector protocols to actually make that happen. The result is slower convergence. That's one of the negatives. You also have a greater potential for routing loops. Basically, a routing loop is when routers are confused as to what direction to send a packet. The packets end up being bounced back and forth aimlessly between different routers. The positive aspect of routing this way is that it's very easy to configure. In the case of RIP, you pretty much just activate the protocol on the routers and you're done.

Routers running distant vector protocols don't have a global view of the network. They're aware of directly connected networks. They know there are networks beyond their neighboring routers, but they have no idea where those networks actually are.

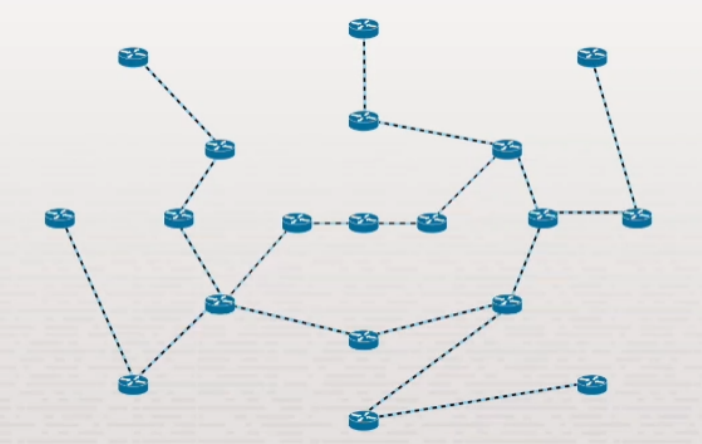


For that reason, these routers have to keep broadcasting their routing tables, every 30 seconds in RIP's case, to pick up anything that might've changed. Basically, these routers have to check in to find out what's going on around them. As you can imagine, this isn't very efficient.

Link state routing protocols

Link state routing protocols offer a much faster convergence and better efficiency. Once the routing tables converge, they don't send as much data across the network. They're also more scalable, meaning that there is minimal impact on performance as the network grows. They're also less subject to loops. Of course, there are a few downsides. Link state routing is more complex. So, the larger you network grows, the more time you have to spend managing the OSPF solution.

Link state routing is demanding on the random access memory, the RAM, and the Central Processing Unit, the CPU. This is because link state protocols maintain an entire map of your network. They don't just know their neighbors, like distance vector routing protocols.

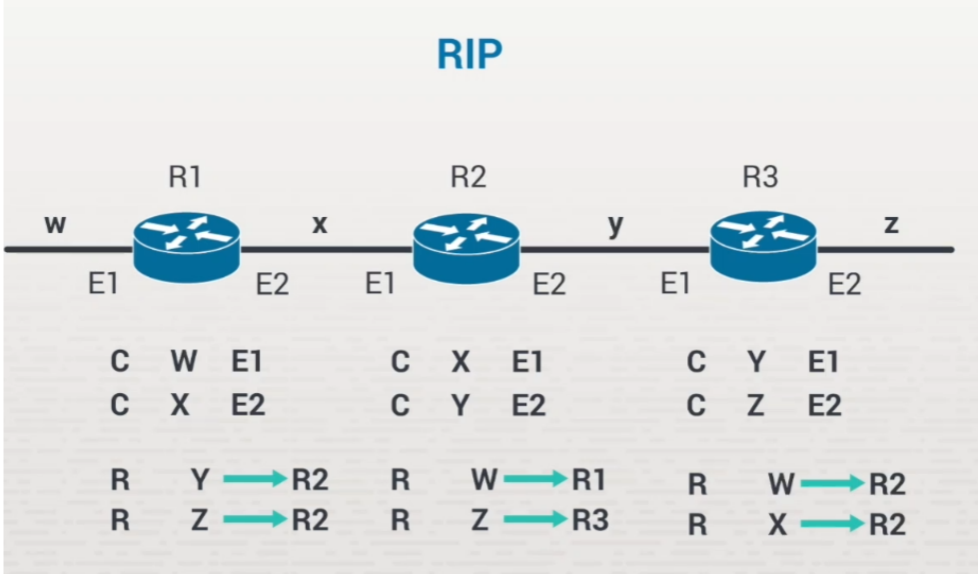


Overall though, you have more configuration and design options with link state routing than you do with distance vector routing.

Distance Vector Routing Operation

Let's talk about distance vector routing and how it works. Routers send updates to their neighboring routers. These updates include the router's entire routing table. These tables are then sent at regular intervals, determined by the router's configuration. They're updated based on information received from their neighbors.

RIP



C	W	E1	C	X	E1	C	Y	E1
C	X	E2	C	Y	E2	C	Z	E2
R	Y	→ R2	R	W	→ R1	R	W	→ R2
R	Z	→ R2	R	Z	→ R3	R	X	→ R2

The routing advertisements sent by routers configured for RIP—or any distance vector routing protocol—are the entire routing table. In fact, this continues after these tables have converged.

Converged means that the routing tables have been updated. You can see that all of the routing tables are complete.

Every certain number of seconds – in RIP's case, it's 30 by default – these routers re-advertise those tables just in case something changed. They add any missed networks to the table. Imagine routing tables with 400 routes. Advertising every 30 seconds would become a burden on your network.

Because of the limited view of the network, distance vector routers are also very slow to converge. Compared to link-state protocols, distance vector protocols are inefficient. They aren't preferred in today's enterprise networks.

More information online https://www.routerfreak.com/understanding-network-routing-protocols/

Distance Vector Facts

Distance vector routing uses the number of hops to the destination to determine the routing path. It was developed in the early 1980's, prior to the development of link-state protocols. Distance vector routing uses the Bellman-Ford algorithm to determine the best path for a particular route.

Routers running distant vector protocols don't have a global view of the network. They're aware of directly connected networks; they're also aware that there are networks beyond their neighboring routers. But, they have no idea where those networks reside.

Convergence defines how quickly the network can update routing tables after a change to the network. This happens via routing protocols. It takes longer for distance vector protocols to propagate a change, resulting in slower convergence. For that reason, distance vector protocols broadcast their route tables frequently. The frequent broadcasting reduces the resources available for transmitting data.

Keep in mind the following principles about the distance vector method:

- Routers send updates only to their neighbor routers.
- Routers send their entire routing table.
- Tables are sent at regular intervals. Each router is configured to specify its own update interval.
- Routers modify their tables based on information received from their neighbors.

Because routers using the distance vector method send their entire routing table at specified intervals, they are susceptible to a condition known as a routing loop, also called a count-to-infinity condition. Like a bridging loop, a routing loop occurs when two routers have different information in the routing table. The following table identifies methods you can use to minimize the effects of a routing loop.

Method	Characteristics
Split horizon	Using the split horizon method, also called best information, routers keep track of where the information about a route came from. Routers do not report route information to the routers on that path. In other words, routers do not report information back to the router from which their information originated.
Split horizon with poison reverse	The split horizon with poison reverse method is also called poison reverse or route poisoning. In this method, routers continue to send information about routes back to the next hop router but advertise the path as unreachable. If the next hop router notices that the route is still reachable, it ignores the information. If, however, the path timeout has been reached, the route is immediately set to unreachable (16 hops for RIP). Convergence happens faster with poison reverse than with split horizon. However, it results in more network traffic because the entire table is broadcast each time an update is sent.
Triggered updates	With the triggered update method, also known as a flash update, routers that receive updated information broadcast those changes immediately rather than waiting for the next reporting interval. With this method, periodic regular router broadcast are punctuated by special broadcasts if conditions change. This method reduces the convergence time.
Hold-down s	With the hold-down method, routers will hold, for a period of time, an update that reinstates an expired link. The time period typically reflects the time required to attain convergence on the network. The hold-down timer is reset when the timer runs out or when a network change occurs.

The distance vector method has the following advantages:

- Stable and proven method. Distance vector was the original routing algorithm.
- Easy to implement and administer.
- Bandwidth requirements are negligible for a typical LAN environment.
- Less hardware and processing power than other routing methods.

Distance vector has the following disadvantages:

- Relatively long time to reach convergence. Updates are sent at specified intervals.
- Routers must recalculate their routing tables before forwarding changes.
- Susceptible to routing loops (count-to-infinity).
- Bandwidth requirements can be too great for WAN or complex LAN environments.

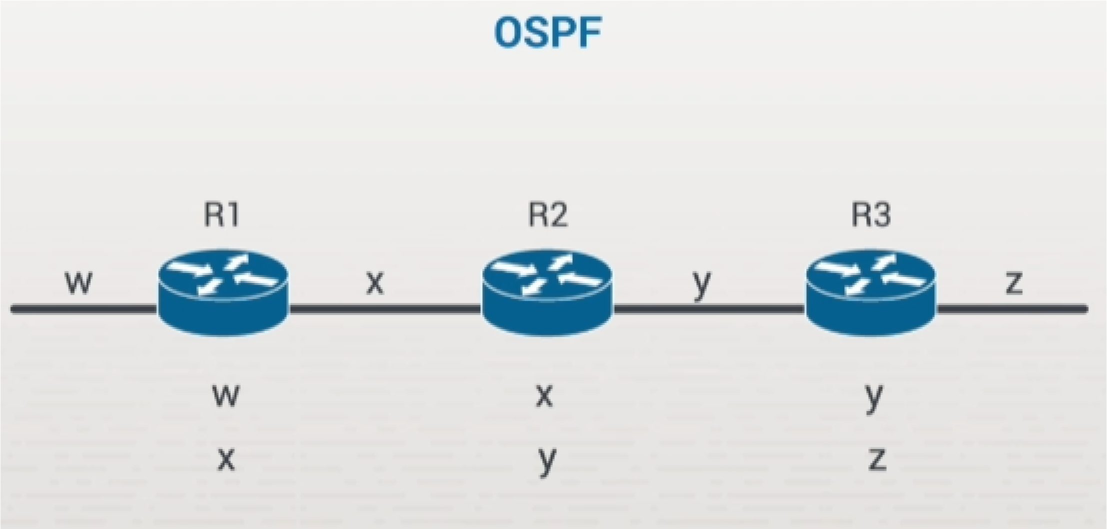
Link State Routing Operation

Link-state routing provides a better solution for larger networks. The most common link-state routing protocol is Open Shortest Path First, or the OSPF Protocol.

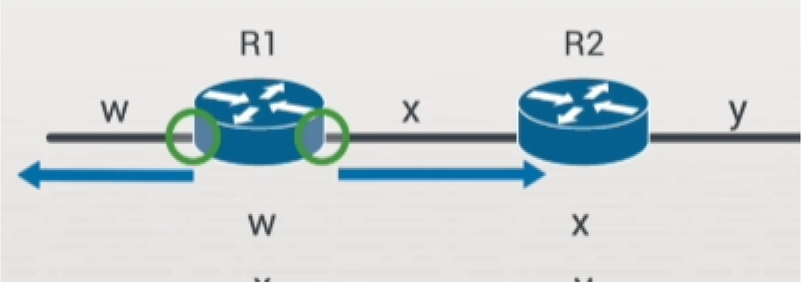
The benefits of link-state protocols are that they offer faster convergence and they're more efficient than distance vector protocols, or DVR protocols. Once the routing tables have converged, they don't send as much data on the network. This means they're more scalable.

If you had to identify a negative to link-state protocols, it would be that they're more demanding on the routers themselves. They have higher random access memory, or RAM requirements. They're also heavier on the central processing unit, or the CPU. This is because they maintain a link-state database—also known as a topology database—that contains an entire map of the network.

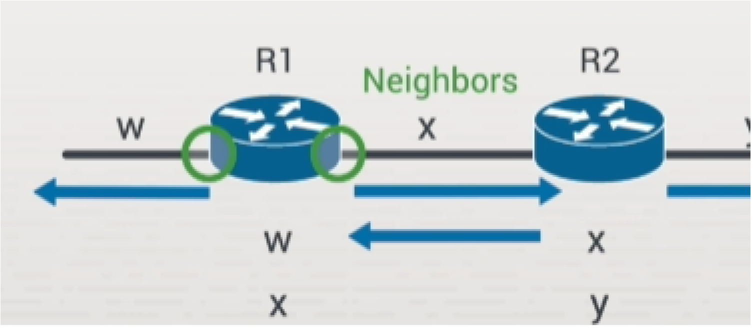
Example 1



When you activate OSPF on a router, the first thing it does is to send out hello packets from each of its configured interfaces. If you activate OSPF in Router 1 and tell it to run on both of these interfaces—connected to Networks W and X—it'll start sending out the packets in both directions. OSPF tries to detect other neighboring routers that are also running OSPF.



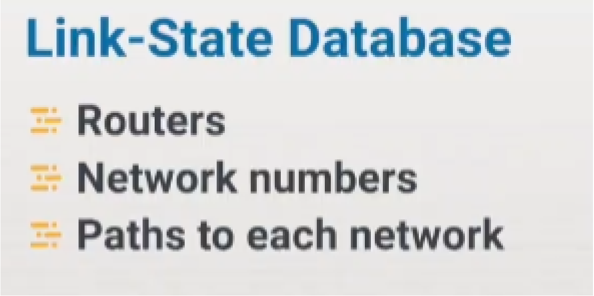
For now, we won't get a response to these hellos from Router 2. It hasn't been configured yet with OSPF. As soon as you activate OSPF on Router 2, it'll start sending out its own hellos. Now Routers 1 and 2 see each other's hello packets and they're now neighbors.



OSPF routers never send their entire routing table. Instead, they send out link-state advertisements, or LSAs. Router 1 has to tell Router 2 that Network W is out here. Then an LSA is sent to Router 2 that contains information about Network W. LSAs will continue to be sent by Router 1 until all information has been conveyed to Router 2. Router 2 does the same thing. They keep exchanging LSAs back and forth until all three routers are aware of each network number in your organization.

Link-State Database

Every router will have a complete link-state database—an LSDB—once all of the LSAs have been sent, received, and absorbed. This table is a full view of your entire network, including routers, network numbers, and paths. Each LSDB on your network is identical.



Link-State Database

- Routers
- Network numbers
- Paths to each network

Once the databases are complete, each router creates a routing table based on its location on the map. Unlike the LSDB, each routing table is different because each router is located at a different point on the network.

Once the routing tables have been built, they'll go quiet. They don't periodically advertise their routing tables. Instead, they continue to send hellos back and forth to verify that the neighbor is still there. If they don't get a reply, they assume the neighbor is gone. All the networks that were reachable through that neighbor are purged. A notice is sent out to other routers, which lets them know that the topology map has changed. There will also be increased network traffic anytime a router is brought up for the first time. This is because all tables are being converged.

Link State Routing Facts

In link-state routing, each network node maintains data to identify which nodes are connected to which other nodes. Each node determines the best route to every node in the network.

Link-State Routing Protocols

Link-state routing protocols offer faster convergence and better efficiency because once the routing tables have converged, they don't send as much data across the network. They are also more scalable, meaning there is minimal impact on performance as the network grows. They are also less subject to loops.

Of course, there are a few downsides. Link-state routing is more complex. The larger your network grows, the more time you must spend designing the OSPF solution to make sure it's operating as efficiently as it could be. Link-state routing is demanding on the RAM and CPU because instead of knowing only the neighbors, like distance vector routing protocols, link-state protocols maintain an entire map of your network. Overall, you have more configuration options and design capabilities with link-state routing than you do with distance vector routing.

Keep in mind the following information about the link-state method:

- Routers broadcast Link-State Packets (LSPs) to all routers. This process is known as flooding.
- Routers send information about their own links.
- Link-state protocols send hello packets to discover new neighbors.
- LSPs are sent at regular intervals when there is a new neighbor, a neighbor has gone down, or the cost to a neighbor has changed.
- Neighboring routers exchange link-state advertisements (LSAs) to construct a topological database.
- The shortest path first (SPF) algorithm is applied to the topological database to create an SPF tree from which a table of routing paths and associated ports is built.
- Routers use LSPs to build their tables and calculate the best route.
- Routers use the SPF algorithm to select the shortest route.
- Network administrators have greater flexibility in setting the metrics used to calculate routes.

Advantages of Link-State Routing

The link-state method has the following advantages over the distance vector method:

- Less convergence time (because updates are forwarded immediately)
- Not susceptible to routing loops
- Less susceptible to erroneous information (because only firsthand information is broadcast)
- Negligible bandwidth requirements for a typical LAN environment

Disadvantages of Link-State Routing

Although more stable than the distance vector method, the link-state method has the following problems:

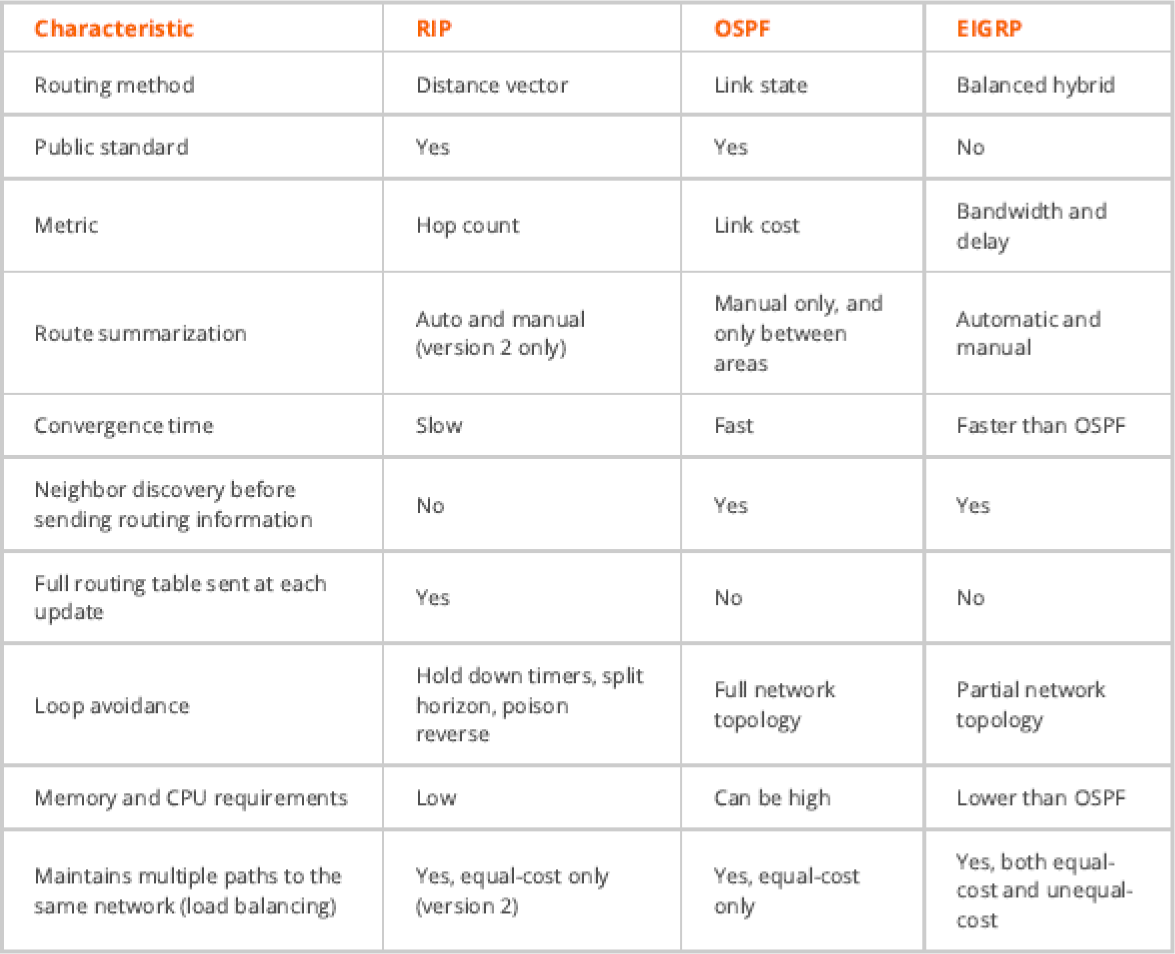
- Because the algorithm re-creates the exact topology of the network for route computation, the link-state algorithm requires greater CPU and memory capability to calculate the network topology and select the route.
- It generates a high amount of traffic when LSPs are initially flooded through the network or when the topology changes. However, after the initial configuration occurs, the traffic from the link-state method is smaller than that from the distance vector method.
- It is possible for LSPs to get delayed or lost, resulting in an inconsistent view of the network. This is particularly a problem for larger networks and is also a problem if parts of the network come online at different times or if the bandwidth between links varies. For example, LSPs travel faster through some parts of the network than through others.

Routing Protocol Comparison Facts

Routing protocols facilitate network connectivity in a number of ways. Router protocols perform tasks such as, enable routers to communicate with each other; create and maintain routing databases; determine the best routes; and avoid routing loops. The following table compares various features of the routing protocols you should be familiar with:

Characteristic	RIP	OSPF	EIGRP
Routing method	Distance vector	Link state	Balanced hybrid
Public standard	Yes	Yes	No
Metric	Hop count	Link cost	Bandwidth and delay
Route summarization	Auto and manual (version 2 only)	Manual only, and only between areas	Automatic and manual
Convergence time	Slow	Fast	Faster than OSPF

Neighbor discovery before sending routing information	No	Yes	Yes
Full routing table sent at each update	Yes	No	No
Loop avoidance	Hold down timers, split horizon, poison reverse	Full network topology	Partial network topology
Memory and CPU requirements	Low	Can be high	Lower than OSPF
Maintains multiple paths to the same network (load balancing)	Yes, equal-cost only (version 2)	Yes, equal-cost only	Yes, both equal-cost and unequal-cost



Characteristic	RIP	OSPF	EIGRP
Routing method	Distance vector	Link state	Balanced hybrid
Public standard	Yes	Yes	No
Metric	Hop count	Link cost	Bandwidth and delay
Route summarization	Auto and manual (version 2 only)	Manual only, and only between areas	Automatic and manual
Convergence time	Slow	Fast	Faster than OSPF
Neighbor discovery before sending routing information	No	Yes	Yes
Full routing table sent at each update	Yes	No	No
Loop avoidance	Hold down timers, split horizon, poison reverse	Full network topology	Partial network topology
Memory and CPU requirements	Low	Can be high	Lower than OSPF
Maintains multiple paths to the same network (load balancing)	Yes, equal-cost only (version 2)	Yes, equal-cost only	Yes, both equal-cost and unequal-cost