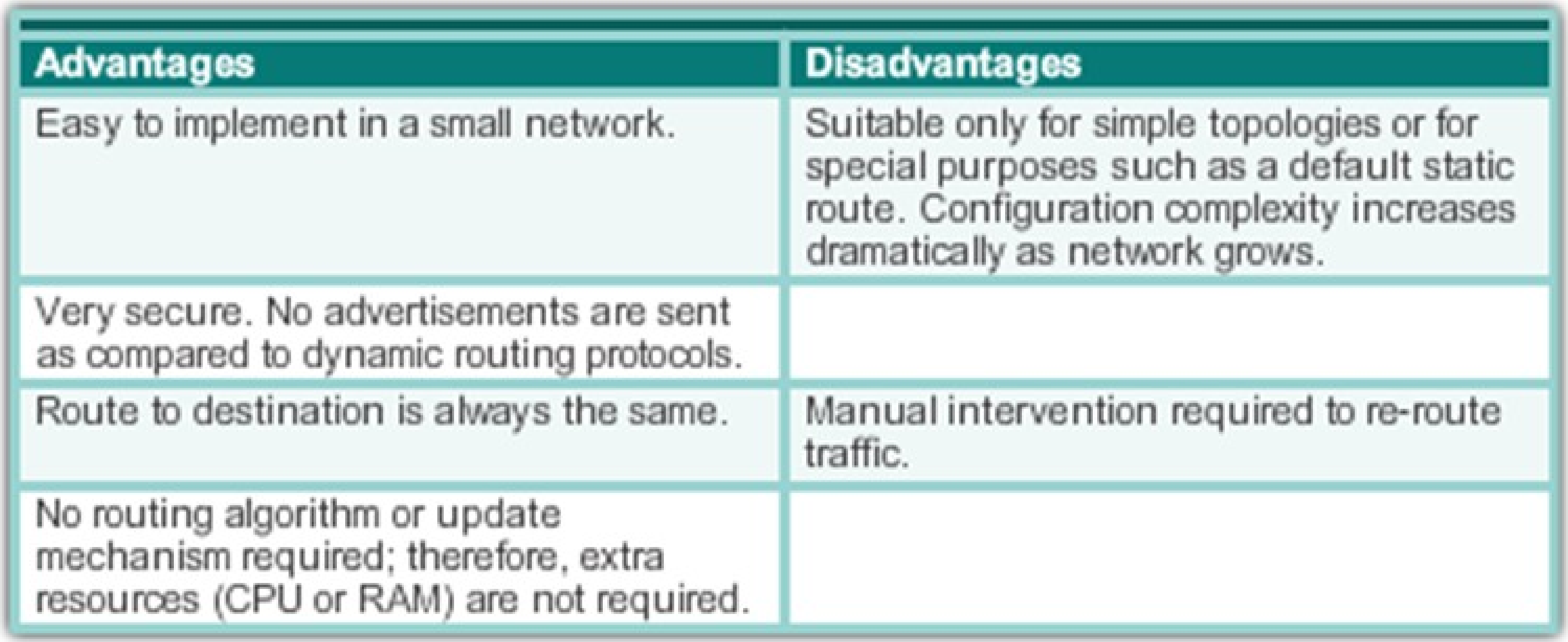
Static and Dynamic Routing

Reach Remote Networks

A router can learn about remote networks in one of two ways:

- **Manually** - Remote networks are manually entered into the route table using static routes.
- **Dynamically** - Remote routes are automatically learned using a dynamic routing protocol.

Static Routing



Advantages	Disadvantages
Easy to implement in a small network.	Suitable only for simple topologies or for special purposes such as a default static route. Configuration complexity increases dramatically as network grows.
Very secure. No advertisements are sent as compared to dynamic routing protocols.	
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.	

Use of Static Routes

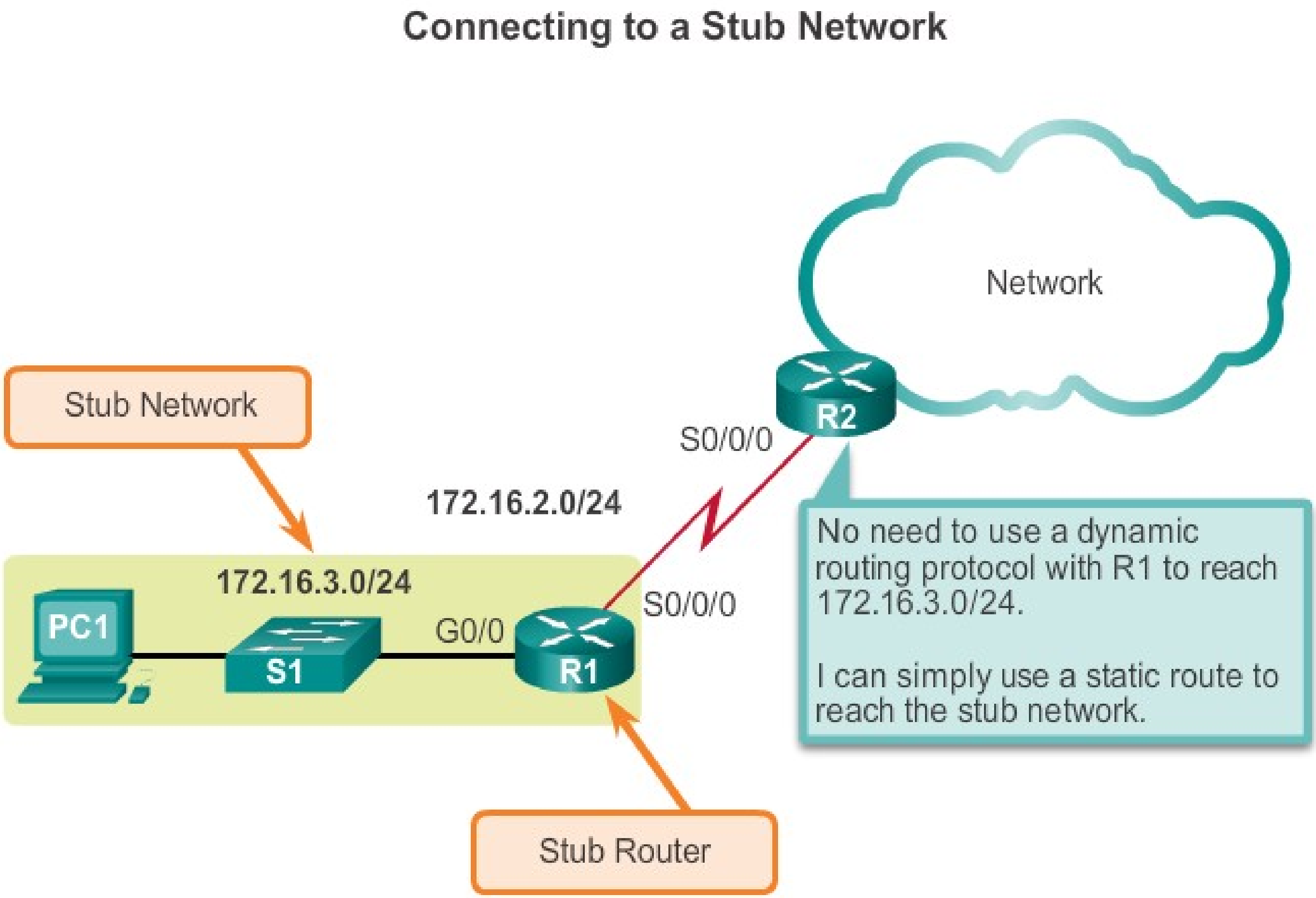
- Providing ease of routing table maintenance in smaller networks that are not expected to grow significantly.
- Routing to and from stub networks. A stub network is a network accessed by a single route, and the router has no other neighbors.
- Using a single default route : Default routes are used to send traffic to any destination beyond the next upstream router.

Static Route Applications

Static Routes are often used to:

- Connect to a specific network.
- Provide a Gateway of Last Resort for a stub network.
- Reduce the number of routes advertised by summarizing several contiguous networks as one static route.
- Create a backup route in case a primary route link fails.

Standard Static Route



No need to use a dynamic routing protocol with R1 to reach 172.16.3.0/24.

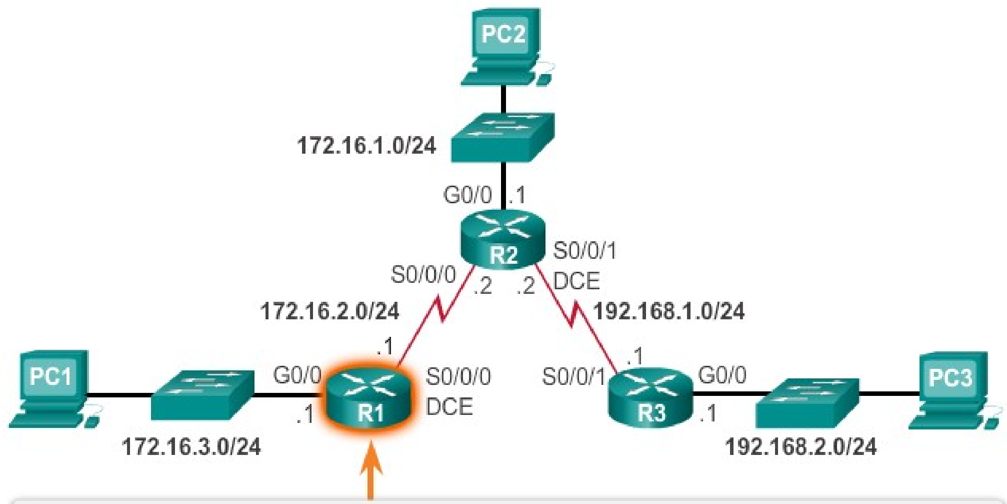
I can simply use a static route to reach the stub network.

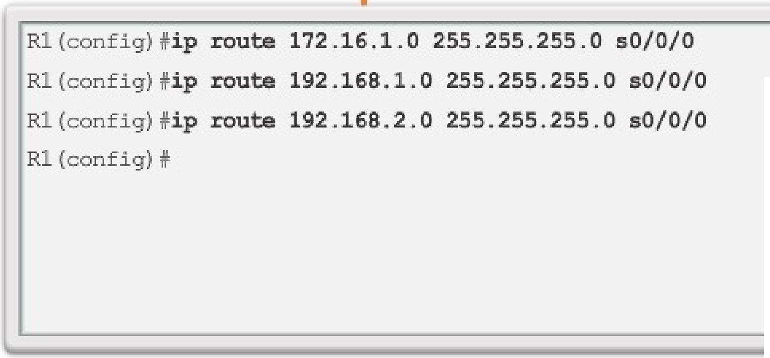
Default Static Route

- A default static route is a route that matches all packets.
- A default route identifies the gateway IP address to which the router sends all IP packets that it does not have a learned or static route.
- A default static route is simply a static route with 0.0.0.0/0 as the destination IPv4 address.

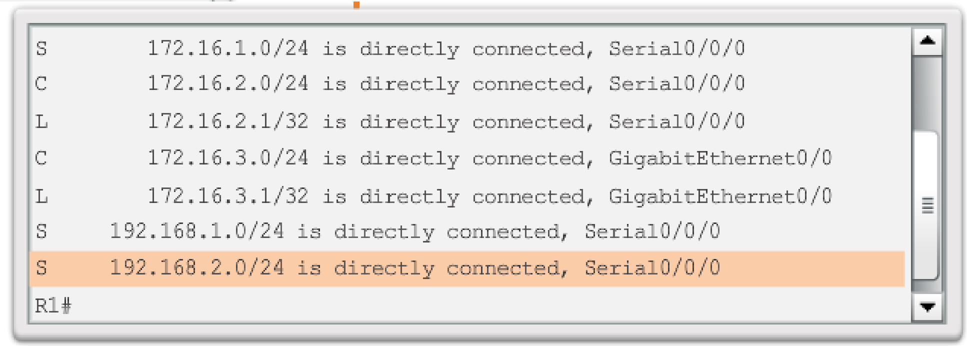
Configure Static Route

Configure Directly Attached Static Routes on R1



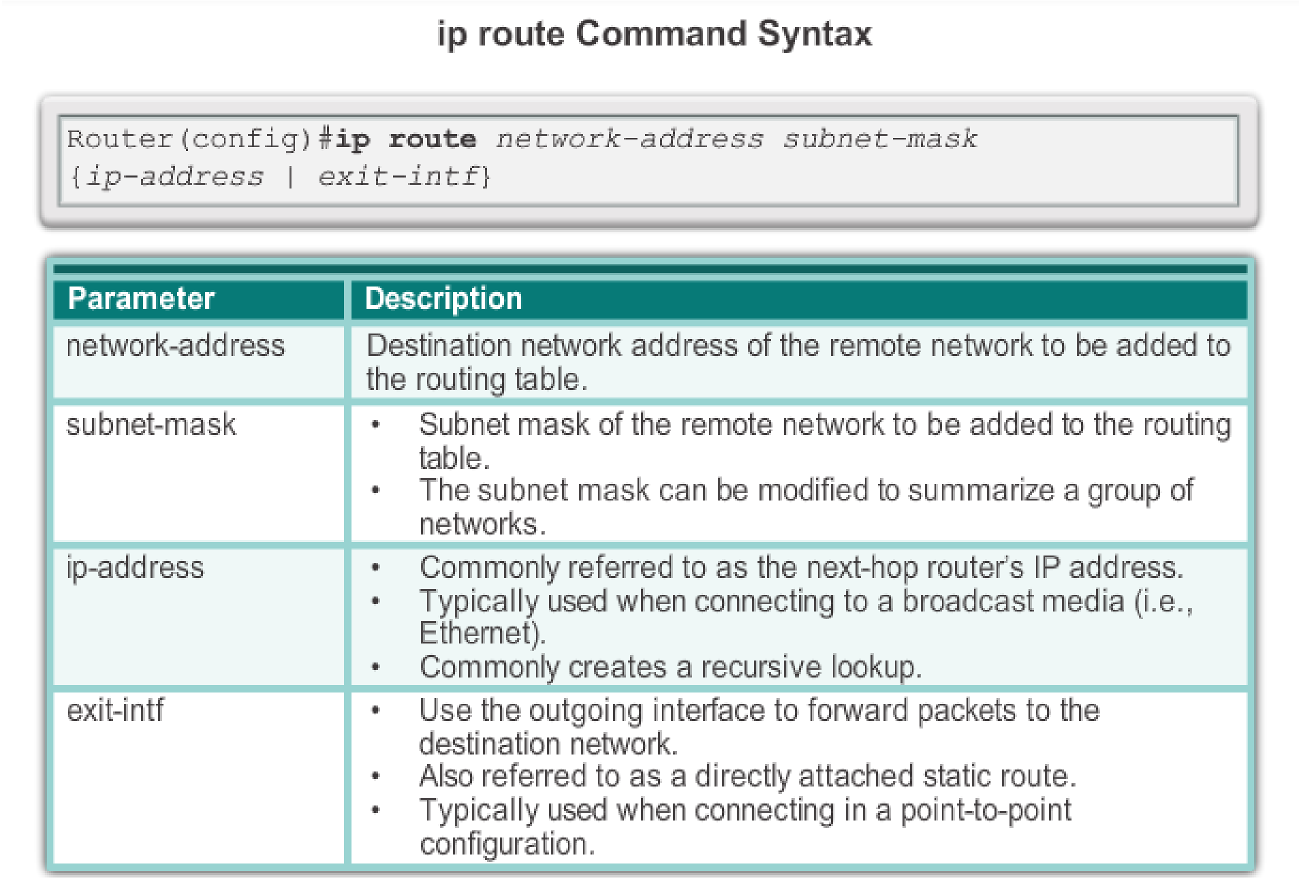


```
R1(config)#ip route 172.16.1.0 255.255.255.0 s0/0/0
R1(config)#ip route 192.168.1.0 255.255.255.0 s0/0/0
R1(config)#ip route 192.168.2.0 255.255.255.0 s0/0/0
R1(config)#
```



```
S       172.16.1.0/24 is directly connected, Serial0/0/0
C       172.16.2.0/24 is directly connected, Serial0/0/0
L       172.16.2.1/32 is directly connected, Serial0/0/0
C       172.16.3.0/24 is directly connected, GigabitEthernet0/0
L       172.16.3.1/32 is directly connected, GigabitEthernet0/0
S    192.168.1.0/24 is directly connected, Serial0/0/0
S    192.168.2.0/24 is directly connected, Serial0/0/0
R1#
```

ip route Command to configure



ip route Command Syntax

```
Router(config)#ip route network-address subnet-mask
{ip-address | exit-intf}
```

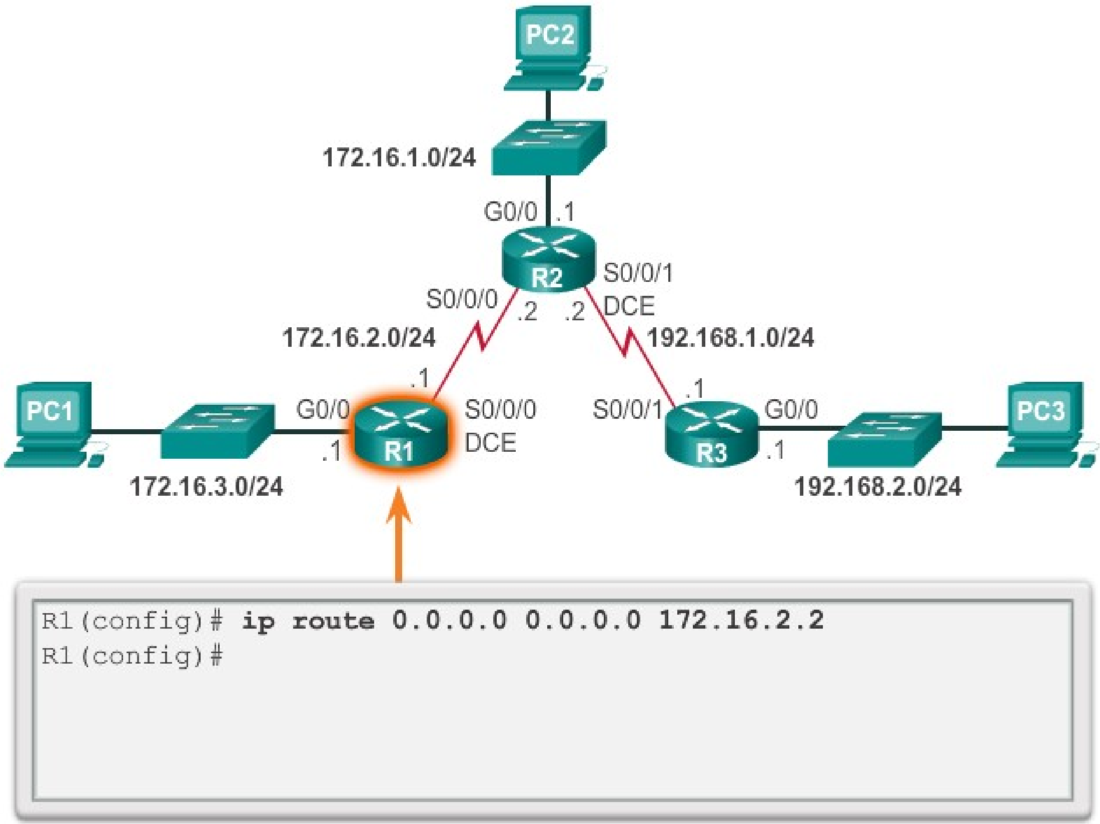
Parameter	Description
network-address	Destination network address of the remote network to be added to the routing table.
subnet-mask	• Subnet mask of the remote network to be added to the routing table. • The subnet mask can be modified to summarize a group of networks.
ip-address	• Commonly referred to as the next-hop router's IP address. • Typically used when connecting to a broadcast media (i.e., Ethernet). • Commonly creates a recursive lookup.
exit-intf	• Use the outgoing interface to forward packets to the destination network. • Also referred to as a directly attached static route. • Typically used when connecting in a point-to-point configuration.

Verify a Static Route

Along with **`ping`** and **`traceroute`**, useful commands to verify static routes include:

- **`show ip route`**
- **`show ip route static`**
- **`show ip route`** `network`

Configure a Default Static Route

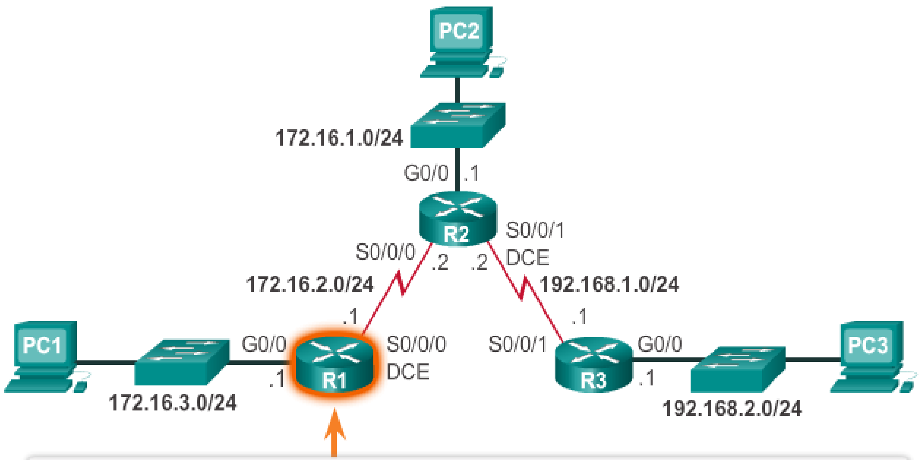


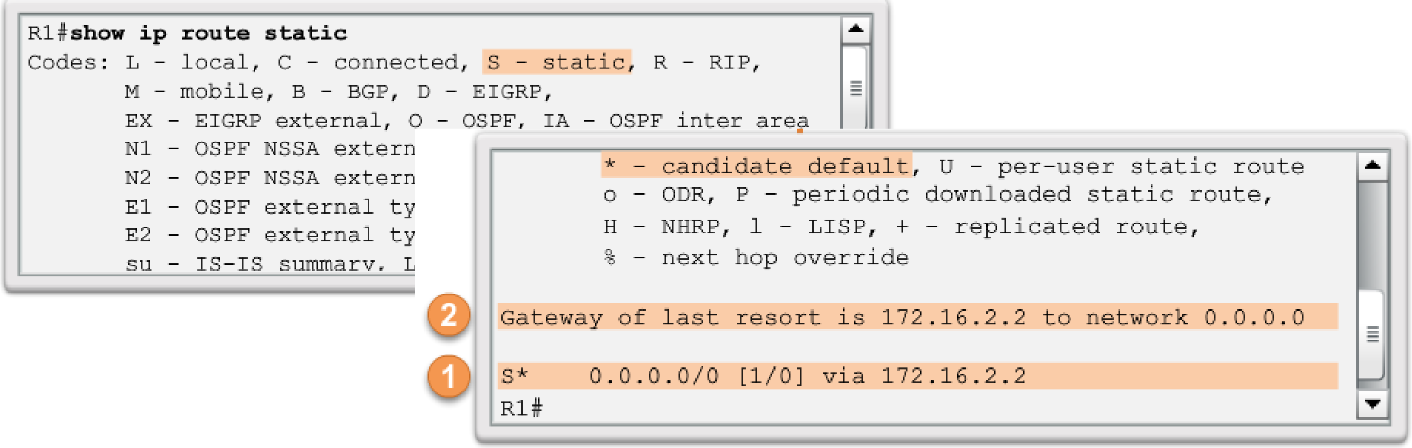
Configuring a Default Static Route

```
R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2
R1(config)#
```

Verify a Default Static Route

Verifying the Routing Table of R1

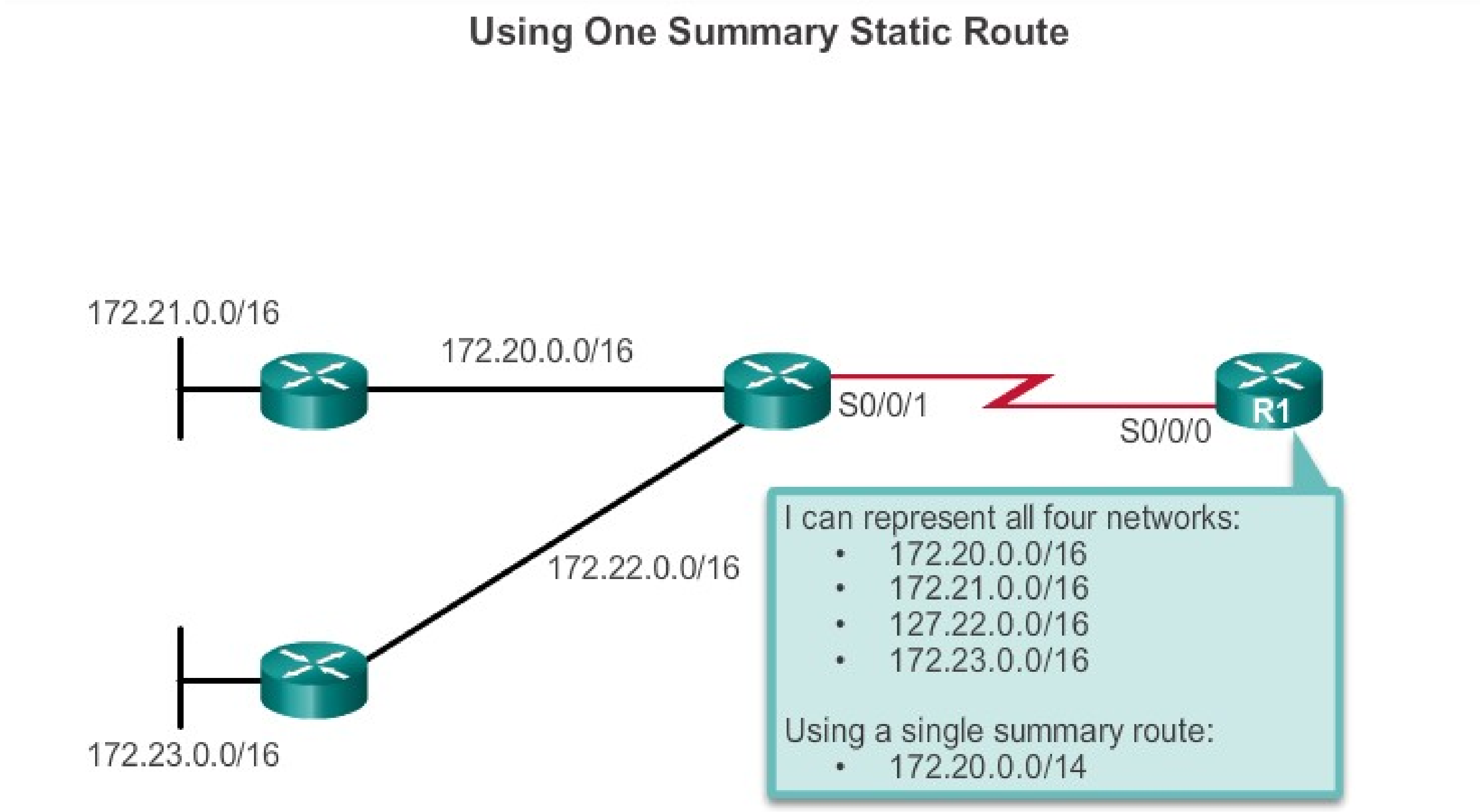




```
R1#show ip route static
Codes: L - local, C - connected, S - static, R - RIP,
       M - mobile, B - BGP, D - EIGRP,
       EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA extern
       N2 - OSPF NSSA extern
       E1 - OSPF external ty
       E2 - OSPF external ty
       su - IS-IS summary, L
```

```
       * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route,
       H - NHRP, l - LISP, + - replicated route,
       % - next hop override

Gateway of last resort is 172.16.2.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.2.2
R1#
```

Summary Static Route



Using One Summary Static Route

I can represent all four networks:

- 172.20.0.0/16
- 172.21.0.0/16
- 127.22.0.0/16
- 172.23.0.0/16

Using a single summary route:

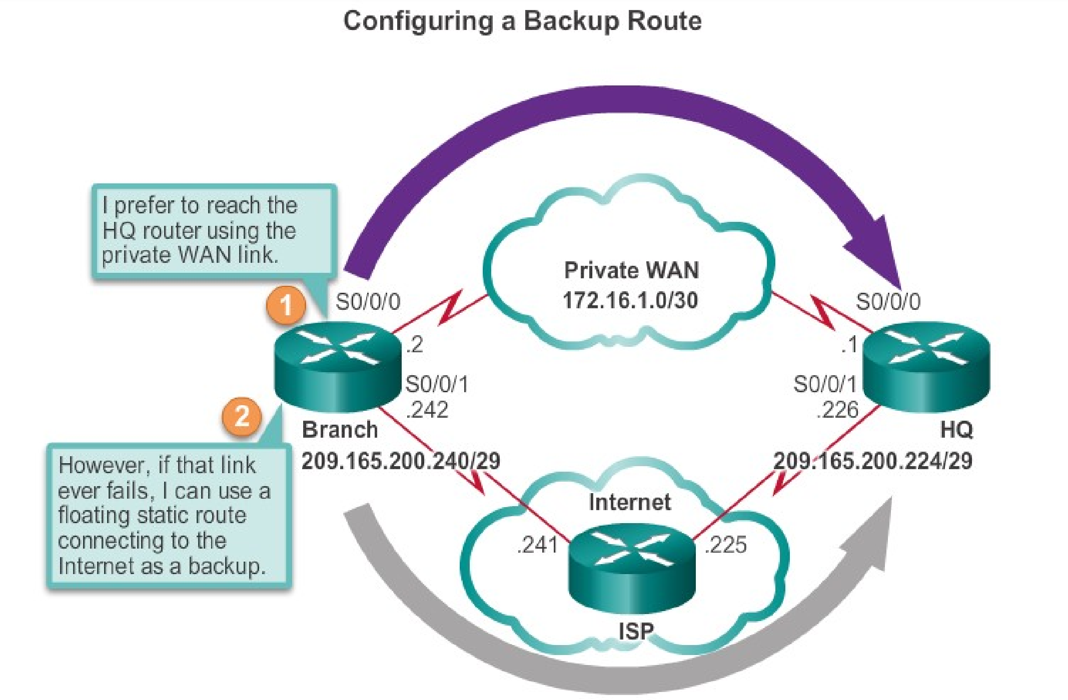
- 172.20.0.0/14

Floating Static Routes

- Floating static routes are static routes that have an administrative distance greater than the administrative distance of another static route or dynamic routes:
- The administrative distance of a static route can be increased to make the route less desirable than that of another static route or a route learned through a dynamic routing protocol.
- In this way, the static route “floats” and is not used when the route with the better administrative distance is active.
- However, if the preferred route is lost, the floating static route can take over, and traffic can be sent through this alternate route.

Floating Static Route

- Floating static routes are static routes that are used to provide a backup path to a primary static or dynamic route, in the event of a link failure.
- The floating static route is only used when the primary route is not available.
- To accomplish this, the floating static route is configured with a higher administrative distance than the prima route.

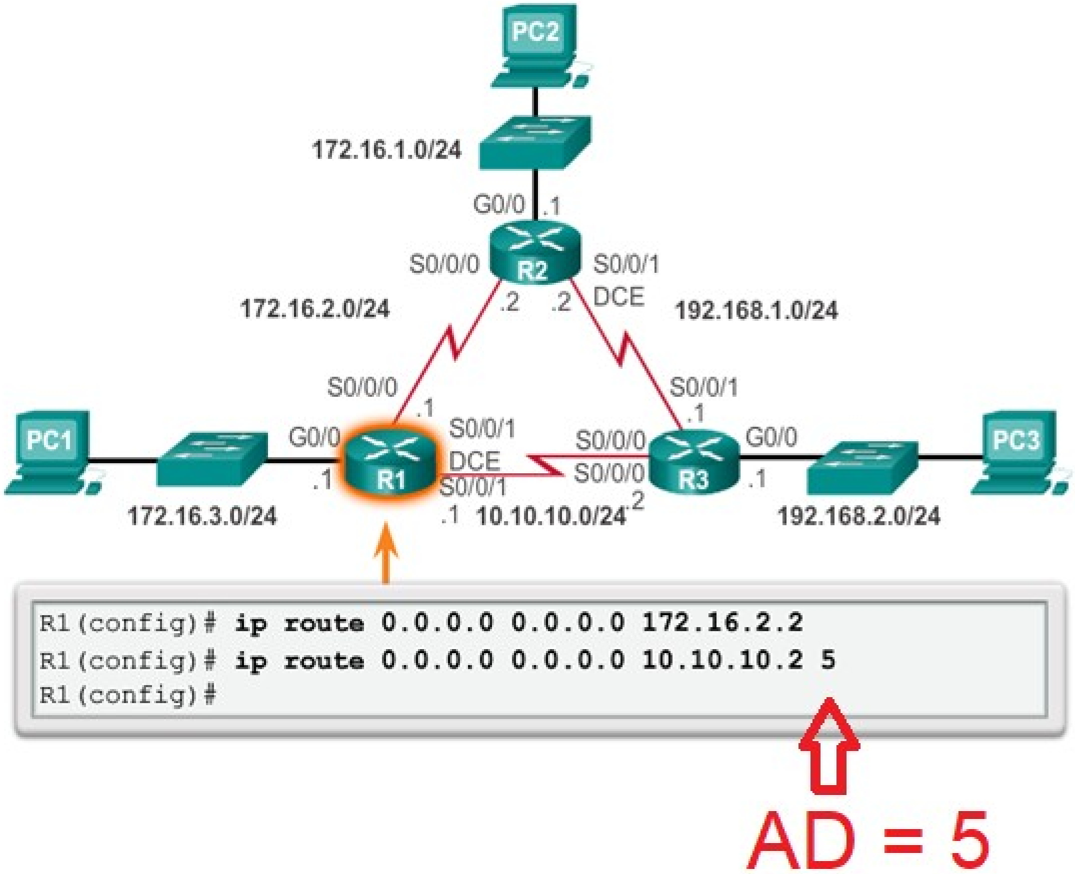


Configuring a Backup Route

① I prefer to reach the HQ router using the private WAN link.

② However, if that link ever fails, I can use a floating static route connecting to the Internet as a backup.

Configure a Floating Static Route



```
R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2
R1(config)# ip route 0.0.0.0 0.0.0.0 10.10.10.2 5
R1(config)#
```

AD = 5

Dynamic Routing Protocols

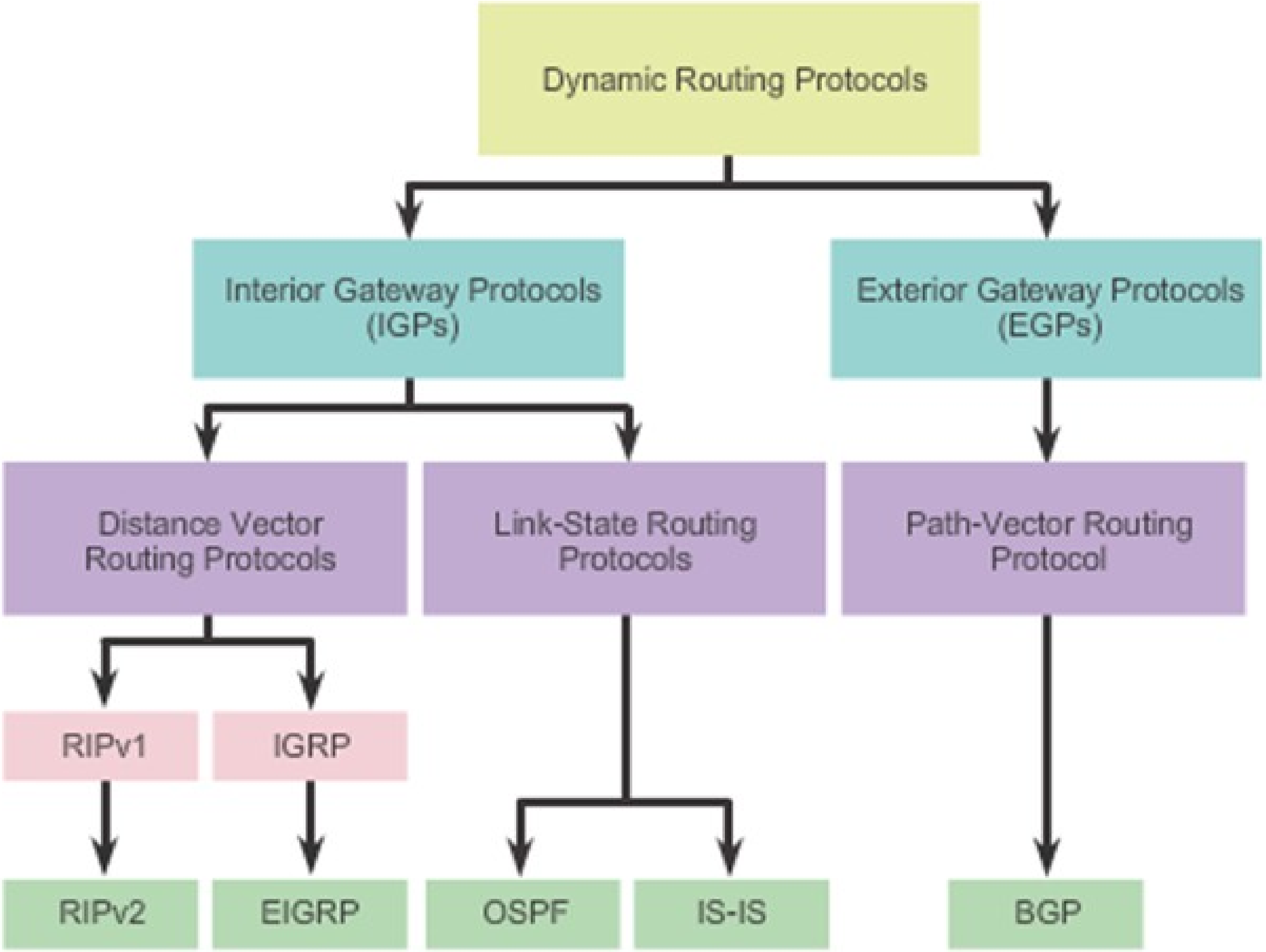
Purpose of Dynamic Routing Protocols

Routing Protocols are used to facilitate the exchange of routing information between routers.

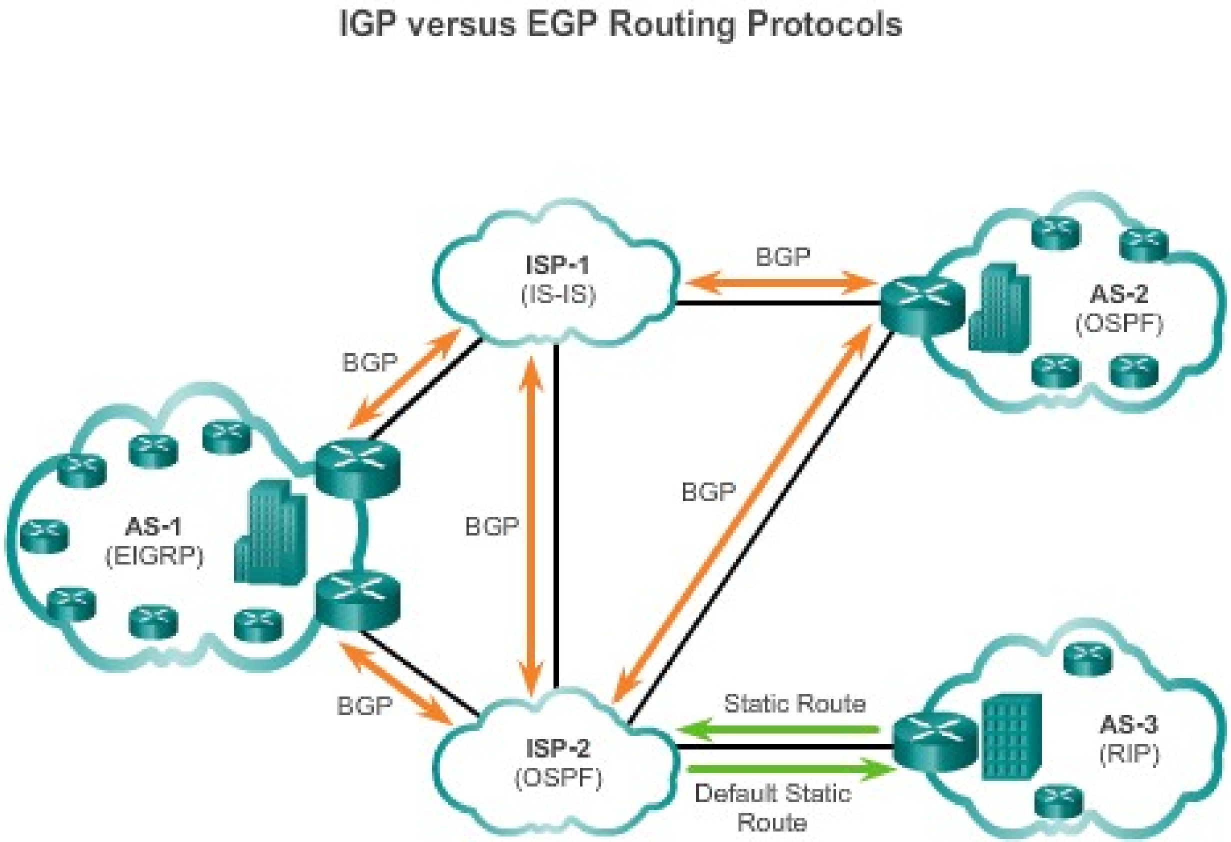
The purpose of dynamic routing protocols includes:

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

Classifying Routing Protocols



IGP and EGP Routing Protocols



Interior Gateway Protocols (IGP) -

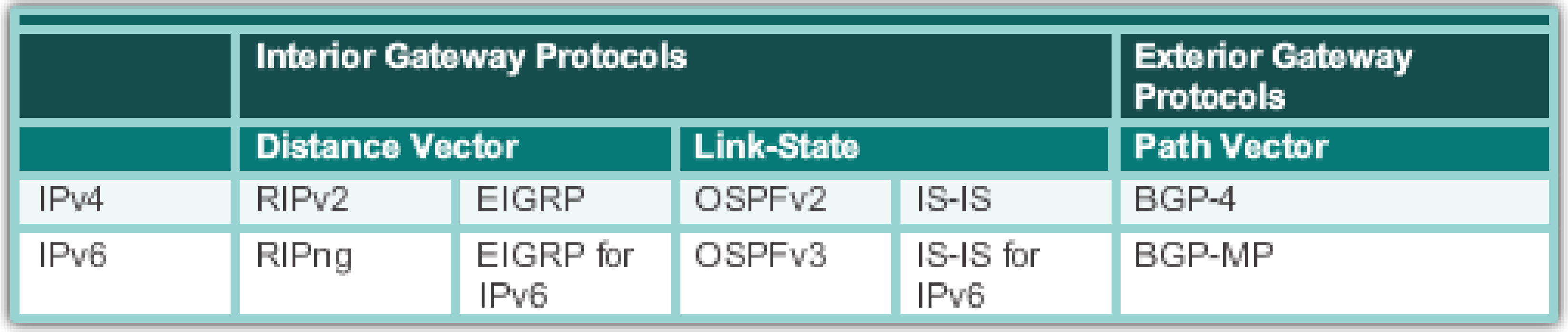
- Used for routing within an AS
- Include RIP, EIGRP, OSPF, and IS-IS

Exterior Gateway Protocols (EGP) -

- Used for routing between AS
- Official routing protocol used by the Internet

Dynamic Routing Protocols

- Dynamic routing protocols used in networks since the late 1980s
- Newer versions support the communication based on IPv6



	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

Components of Dynamic Routing Protocols

- **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 -** Routing protocols use algorithms for facilitating routing information for best path determination.

The Role of Dynamic Routing Protocols

Advantages

- Automatically share information about remote networks
- Determine the best path to each network and add this information to their routing tables
- Compared to static routing, dynamic routing protocols require less administrative overhead
- Help the network administrator manage the time-consuming process of configuring and maintaining static routes

Disadvantages :

- Part of a router’s resources are dedicated for protocol operation, including CPU time and network link bandwidth
- Times when static routing is more appropriate

Dynamic Routing Protocol Operation

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.

Routing Protocol Metrics

A metric is a measurable value that is assigned by the routing protocol to different routes based on the usefulness of that route:

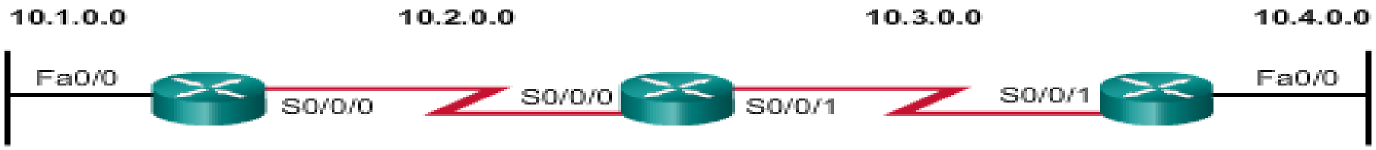
- Used to determine the overall “cost” of a path from source to destination.
- Routing protocols determine the best path based on the route with the lowest cost.

- RIP: Hop count is the metric
- OSPF: Bandwidth

Routing Protocol Operating Fundamentals

Cold Start

Directly Connected Networks Detected



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

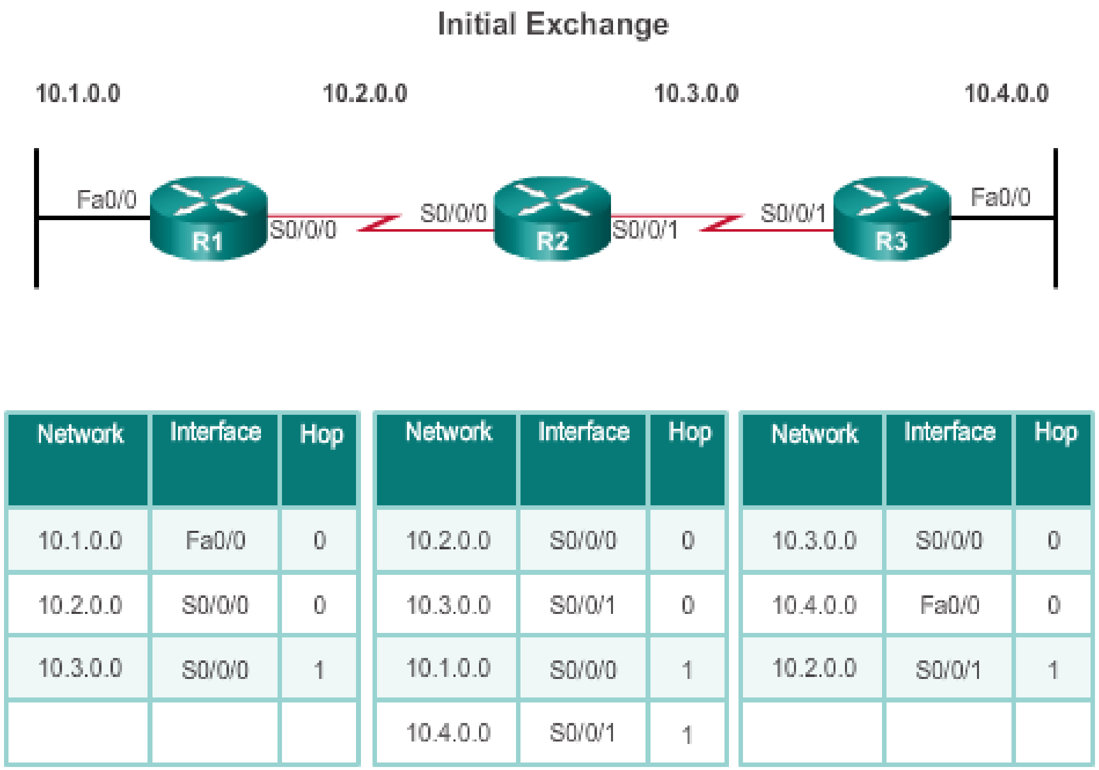
Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0

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

Routers running RIPv2

- All routers have the information of their own interfaces which are directly connected

Network Discovery



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

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

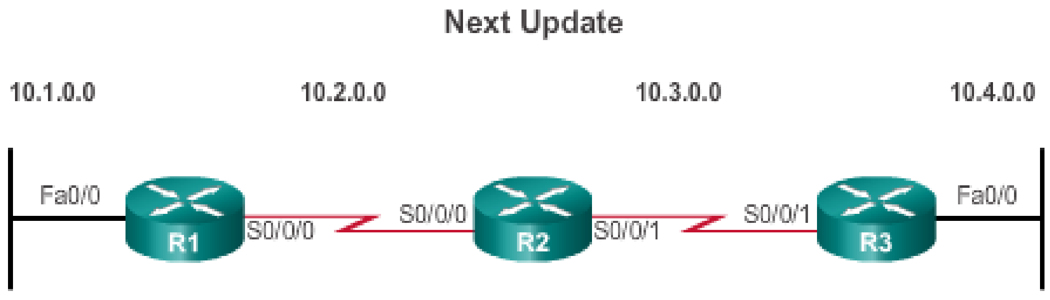
Network	Interface	Hop
10.3.0.0	S0/0/0	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1

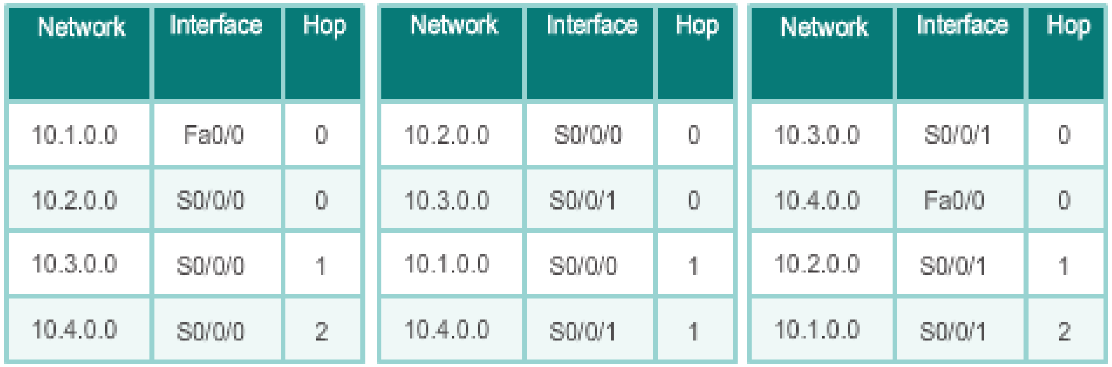
Routers running RIPv2

Router 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 update from R2 about network 10.3.0.0 with a metric of 1
- Stores network 10.3.0.0 in the routing table with a metric of 1

Exchanging the Routing Information





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

Routers running RIPv2

Router R1:

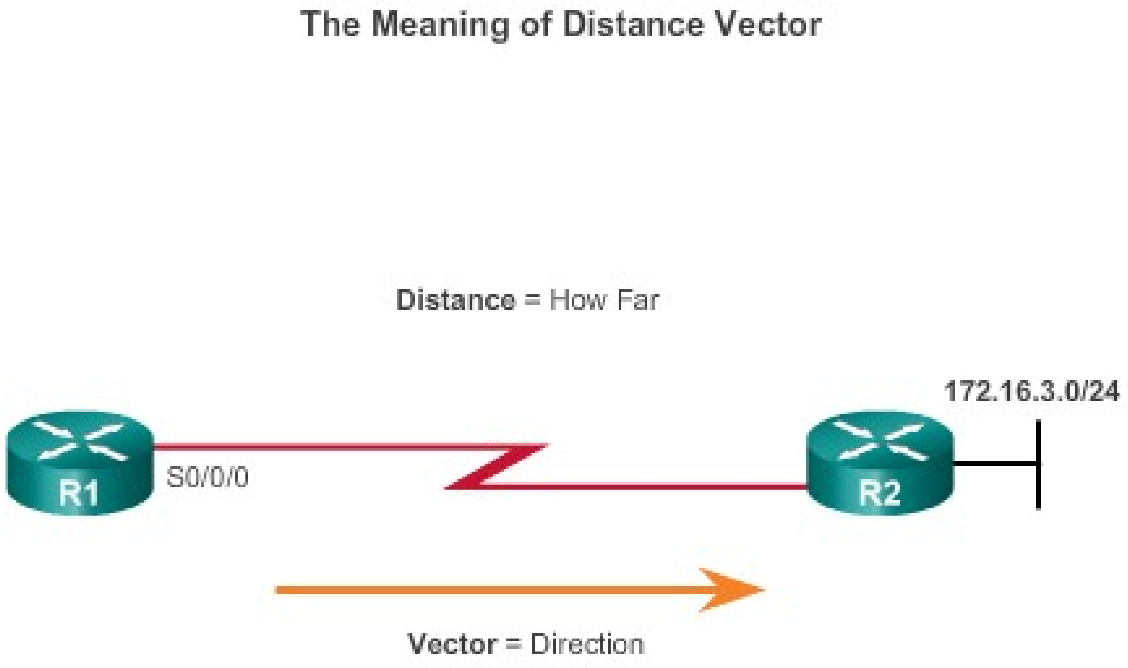
- Sends an update about network 10. 1. 0. 0 out the Serial 0/0/0 interface
- Sends an update about networks 10. 2. 0. 0 and 10. 3. 0. 0 out the FastEthernet0/0 interface
- Receives an update from R2 about network 10. 4. 0. 0 with a metric of 2
- Stores network 10. 4. 0. 0 in the routing table with a metric of 2
- Same update from R2 contains information about network 10. 3. 0. 0 with a metric of 1. There is no change; therefore, the routing information

Achieving Convergence

The network is 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 their routing tables.
- A network is not completely operable until the network has converged.
- 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.
- Generally, older protocols, such as RIP, are slow to converge, whereas modern protocols, such as EIGRP and OSPF, converge more quickly.

Distance Vector Routing Protocols: Examples

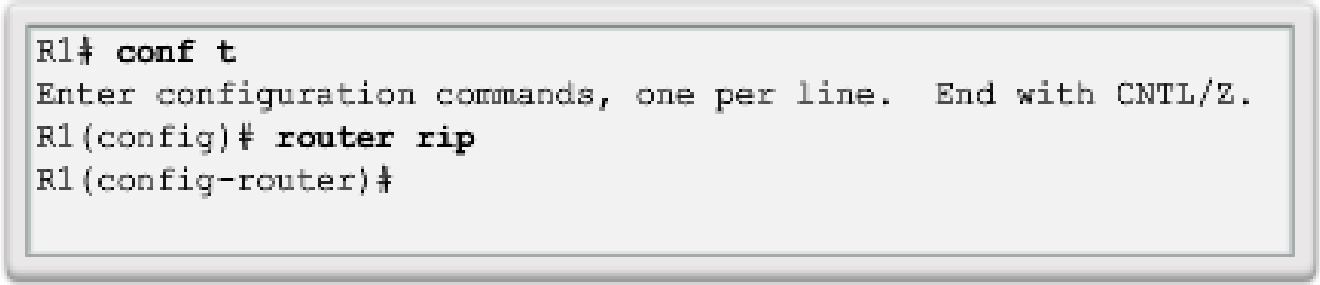


For R1, 172.16.3.0/24 is one hop away (distance). It can be reached through R2 (vector).

Distance vector IPv4 IGPs:

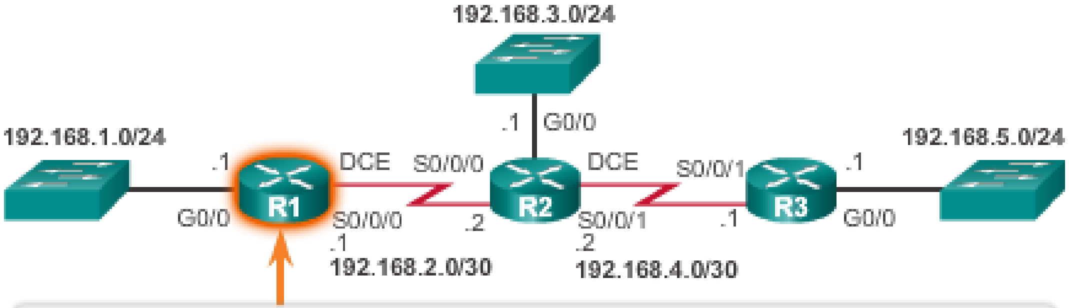
- **RIPv1** - First generation legacy protocol
- **RIPv2** - Simple distance vector routing protocol
- **IGRP** - First generation Cisco proprietary protocol (obsolete)
- **EIGRP** - Advanced version of distance vector routing

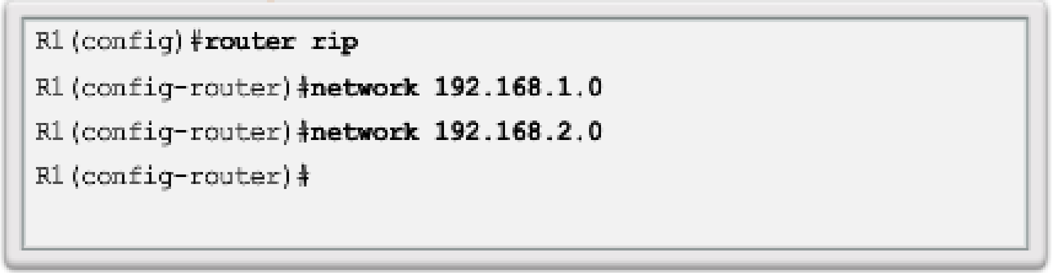
Router RIP Configuration



```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# router rip
R1(config-router)#
```

Advertising the R1 Networks



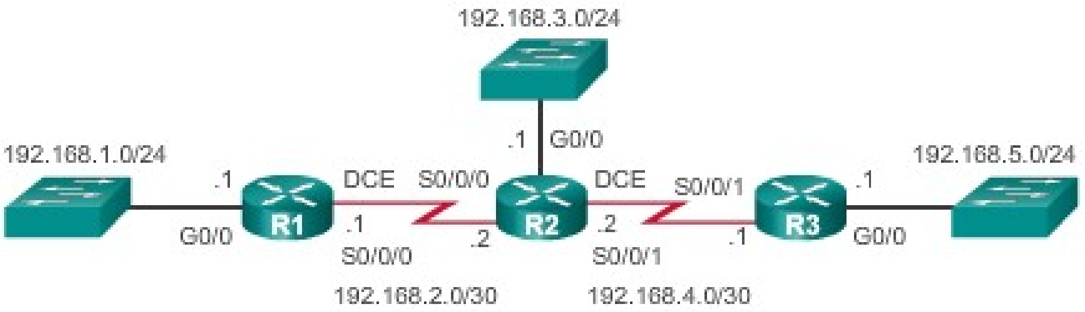


```
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0
R1(config-router)#
```

Configuring the RIP Protocol

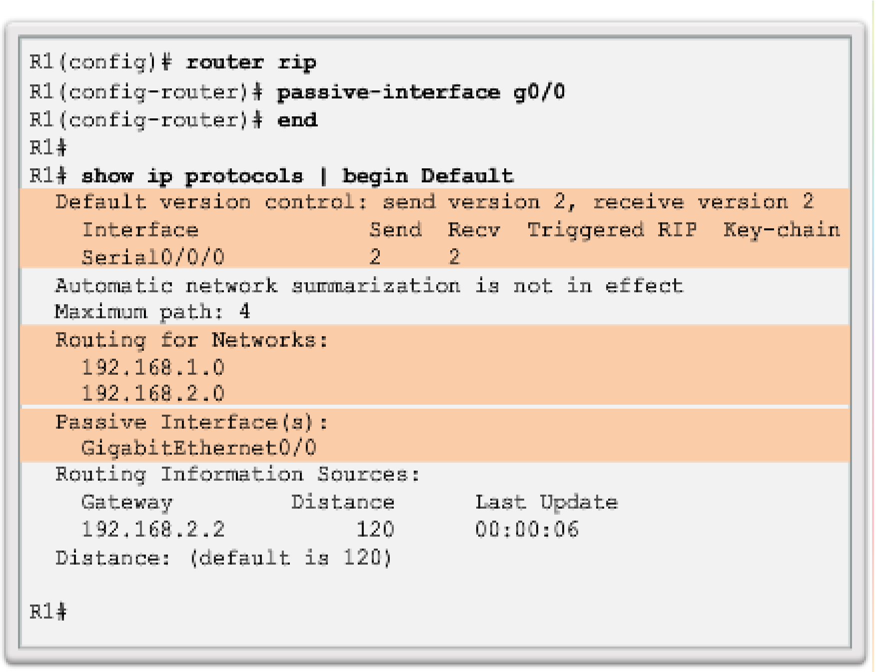
Configuring Passive Interfaces

Configuring Passive Interfaces on R1



Sending out unneeded updates on a LAN impacts the network in three ways:

- Wasted Bandwidth
- Wasted Resources
- Security Risk

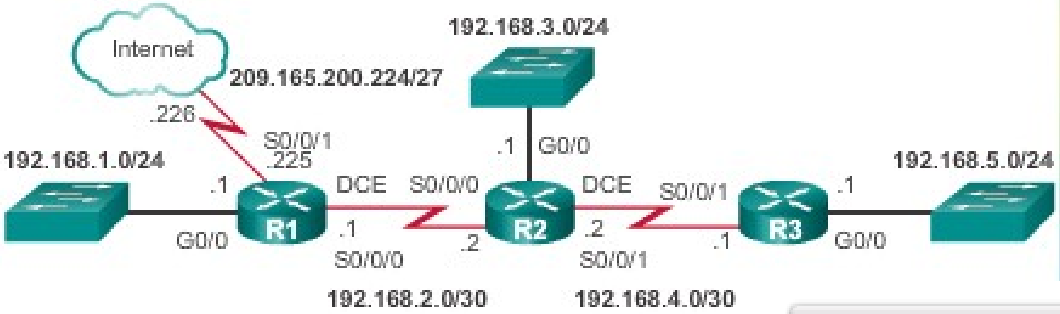


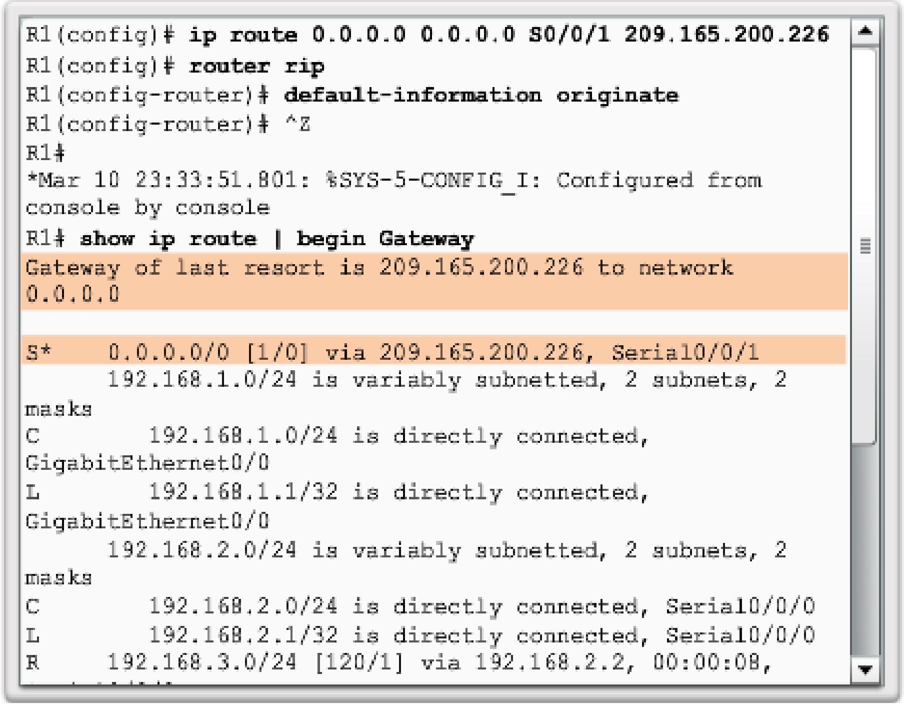
```
R1(config)# router rip
R1(config-router)# passive-interface g0/0
R1(config-router)# end
R1#
R1# show ip protocols | begin Default
  Default version control: send version 2, receive version 2
    Interface             Send  Recv  Triggered RIP  Key-chain
    Serial0/0/0           2     2
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    192.168.1.0
    192.168.2.0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.2          120      00:00:06
  Distance: (default is 120)

R1#
```

Configuring the RIP Protocol

Propagating a Default Route

Propagating a Default Route on R1



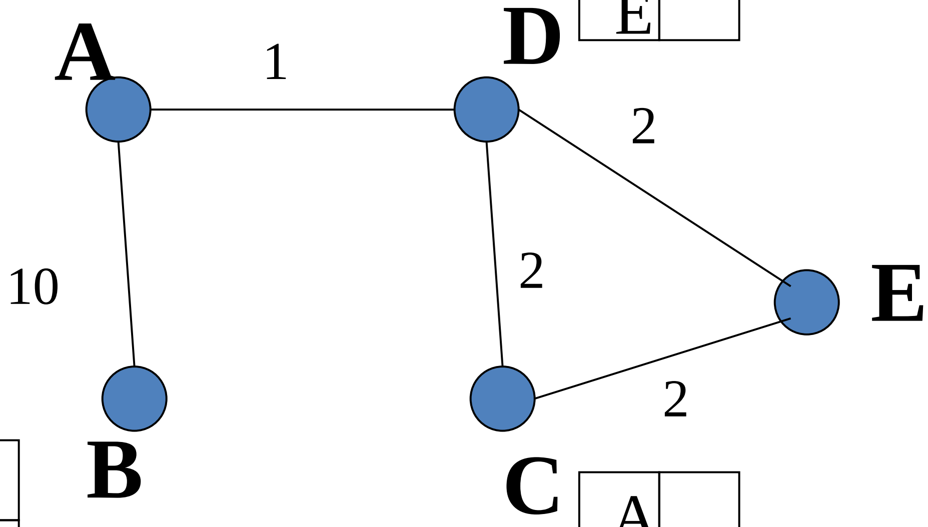


```
R1(config)# ip route 0.0.0.0 0.0.0.0 S0/0/1 209.165.200.226
R1(config)# router rip
R1(config-router)# default-information originate
R1(config-router)# ^Z
R1#
*Mar 10 23:33:51.801: %SYS-5-CONFIG_I: Configured from
console by console
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.226 to network
0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.226, Serial0/0/1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2
masks
C        192.168.1.0/24 is directly connected,
GigabitEthernet0/0
L        192.168.1.1/32 is directly connected,
GigabitEthernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2
masks
C        192.168.2.0/24 is directly connected, Serial0/0/0
L        192.168.2.1/32 is directly connected, Serial0/0/0
R     192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:08,
```

Example: DV routing

A	0
B	
C	
D	
E	

A	
B	
C	
D	0
E	

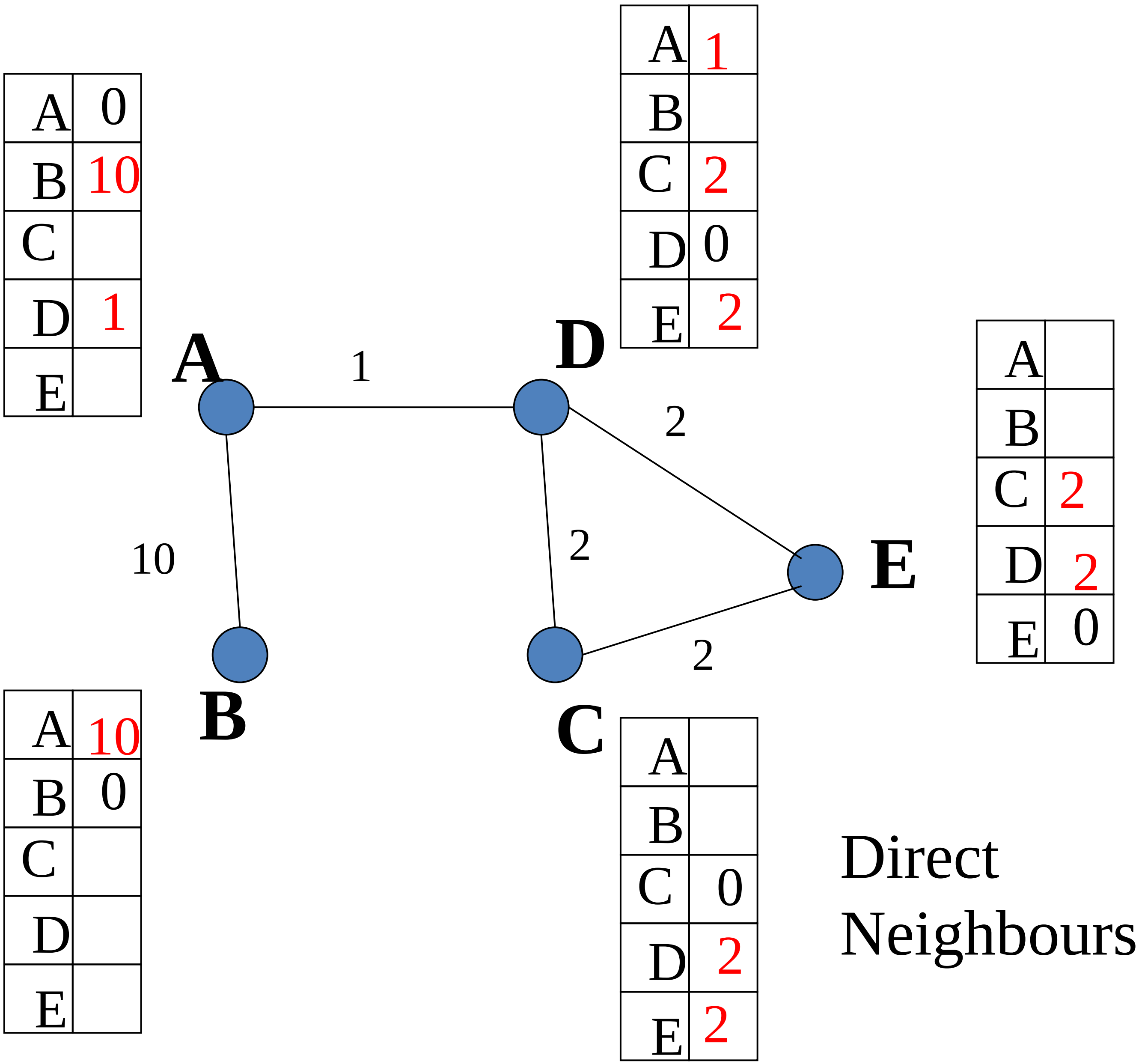


A	
B	
C	
D	
E	0

A	
B	0
C	
D	
E	

A	
B	
C	0
D	
E	

Initialization



A	0
B	10
C	
D	1
E	

A	1
B	
C	2
D	0
E	2

A	
B	
C	2
D	2
E	0

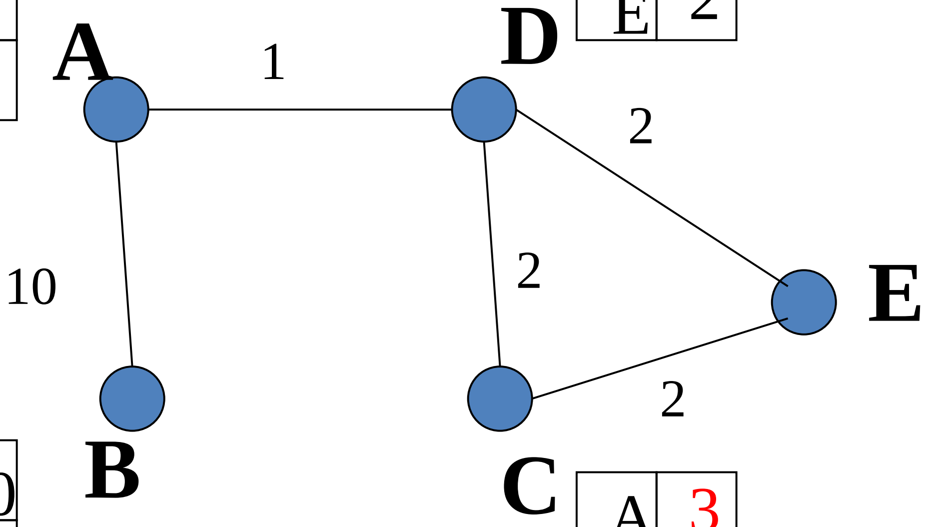
A	10
B	0
C	
D	
E	

A	
B	
C	0
D	2
E	2

Direct Neighbours

A	0
B	10
C	3
D	1
E	3

A	1
B	11
C	2
D	0
E	2



A	3
B	
C	2
D	2
E	0

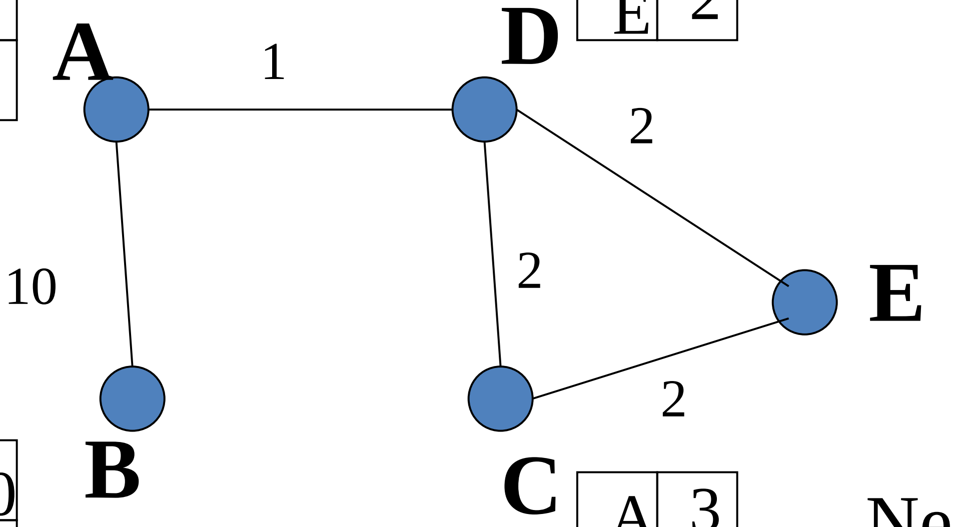
A	10
B	0
C	
D	11
E	

A	3
B	
C	0
D	2
E	2

Neighbours
of neighbours

A	0
B	10
C	3
D	1
E	3

A	1
B	11
C	2
D	0
E	2

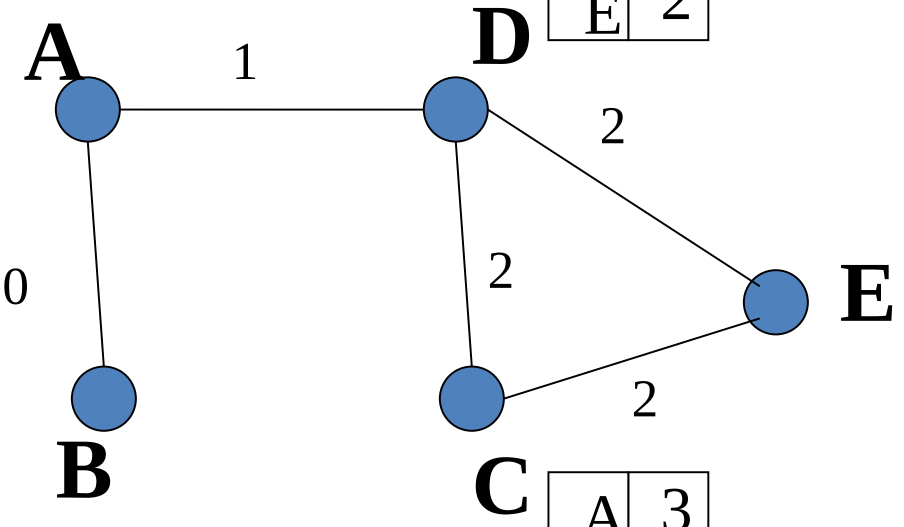


A	3
B	13
C	2
D	2
E	0

A	10
B	0
C	13
D	11
E	13

A	3
B	13
C	0
D	2
E	2

Neighbours
of neighbours
of neighbours



A	0
B	10
C	3
D	1
E	3

A	1
B	11
C	2
D	0
E	2

A	3
B	13
C	2
D	2
E	0

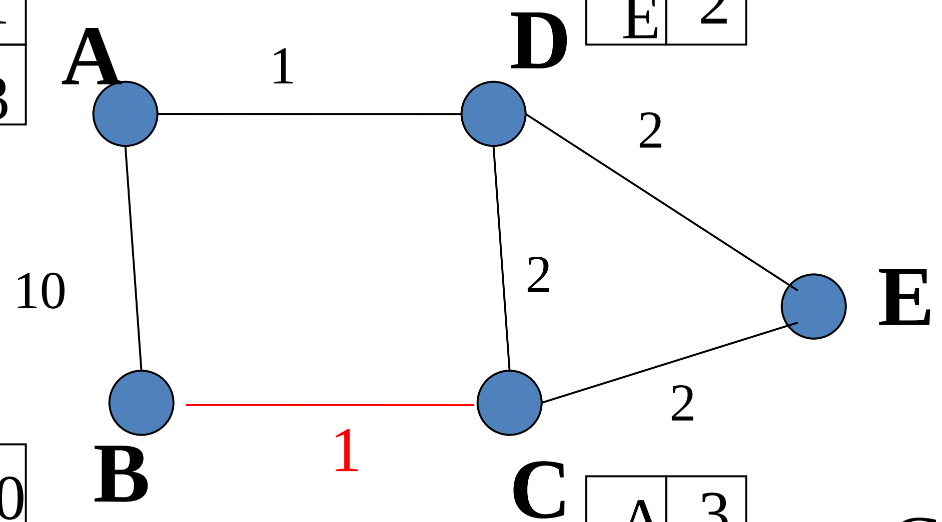
A	10
B	0
C	13
D	11
E	13

A	3
B	13
C	0
D	2
E	2

Stable convergence

A	0
B	10
C	3
D	1
E	3

A	1
B	11
C	2
D	0
E	2

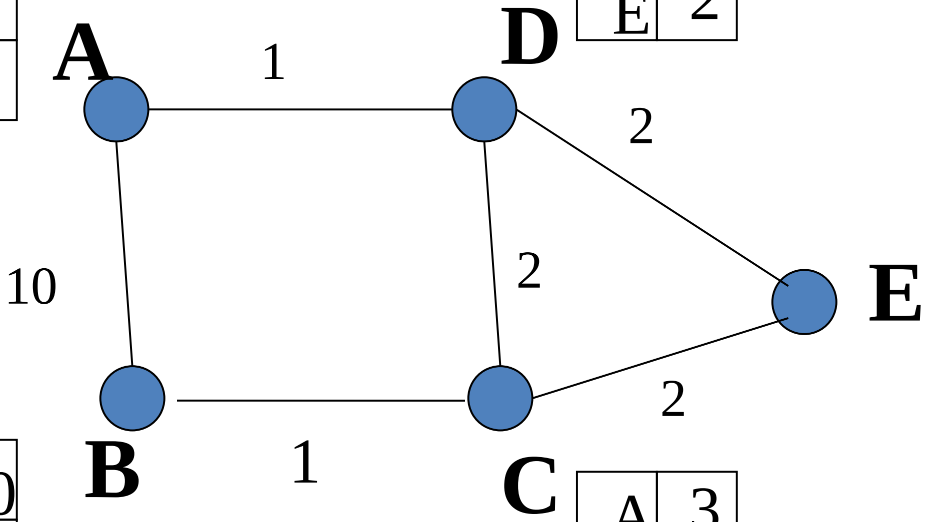


A	3
B	13
C	2
D	2
E	0

A	10
B	0
C	13
D	11
E	13

A	3
B	13
C	0
D	2
E	2

Good news:
A new link!



A	0
B	10
C	3
D	1
E	3

A	1
B	11
C	2
D	0
E	2

A	3
B	13
C	2
D	2
E	0

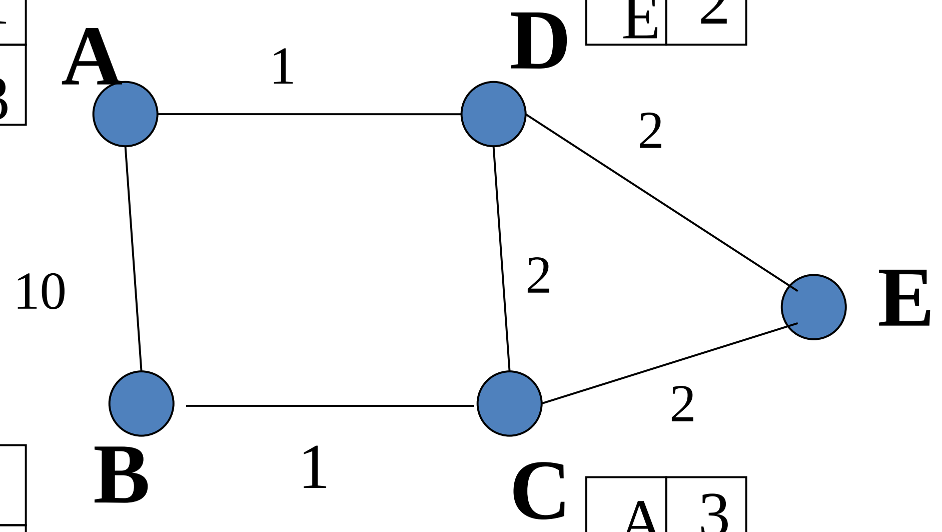
A	10
B	0
C	1
D	11
E	13

A	3
B	1
C	0
D	2
E	2

Direct endpoints know

A	0
B	10
C	3
D	1
E	3

A	1
B	3
C	2
D	0
E	2



A	3
B	3
C	2
D	2
E	0

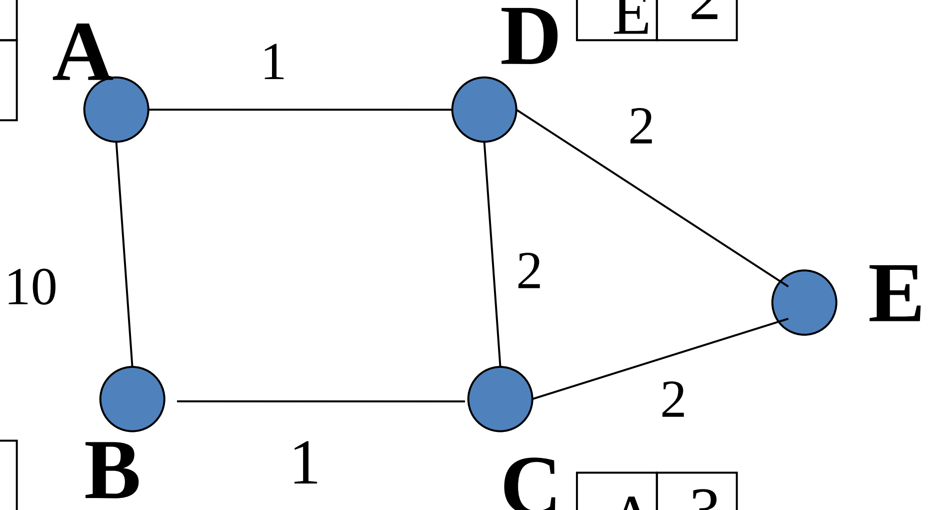
A	4
B	0
C	1
D	3
E	3

A	3
B	1
C	0
D	2
E	2

Neighbours know

A	0
B	4
C	3
D	1
E	3

A	1
B	3
C	2
D	0
E	2



A	3
B	3
C	2
D	2
E	0

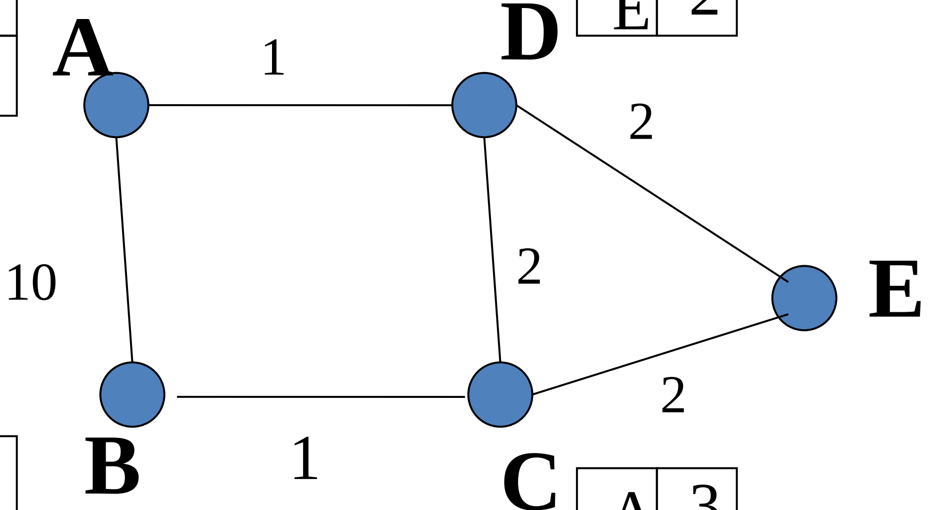
A	4
B	0
C	1
D	3
E	3

A	3
B	1
C	0
D	2
E	2

Neighbours of neighbours know

A	0
B	4
C	3
D	1
E	3

A	1
B	3
C	2
D	0
E	2

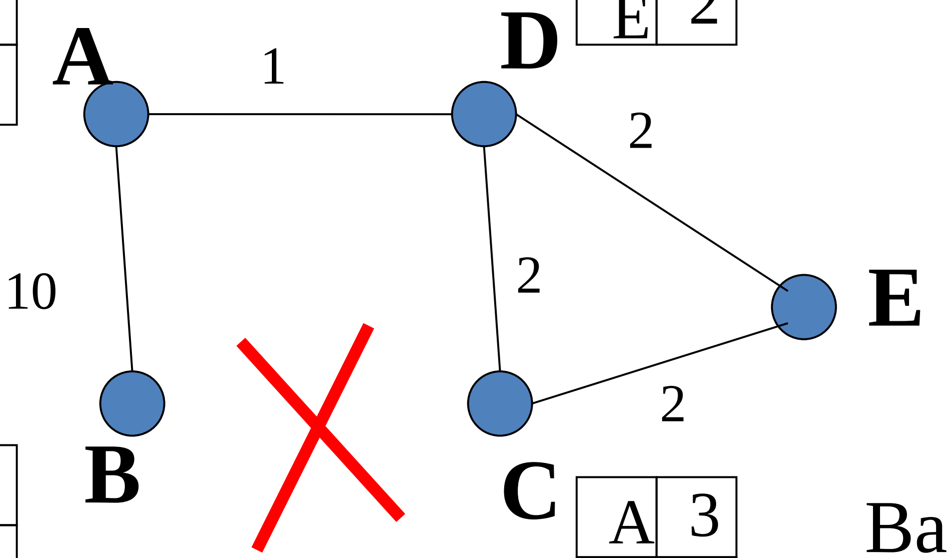


A	3
B	3
C	2
D	2
E	0

A	4
B	0
C	1
D	3
E	3

A	3
B	1
C	0
D	2
E	2

A happy and stable network



A	0
B	4
C	3
D	1
E	3

A	1
B	3
C	2
D	0
E	2

A	3
B	3
C	2
D	2
E	0

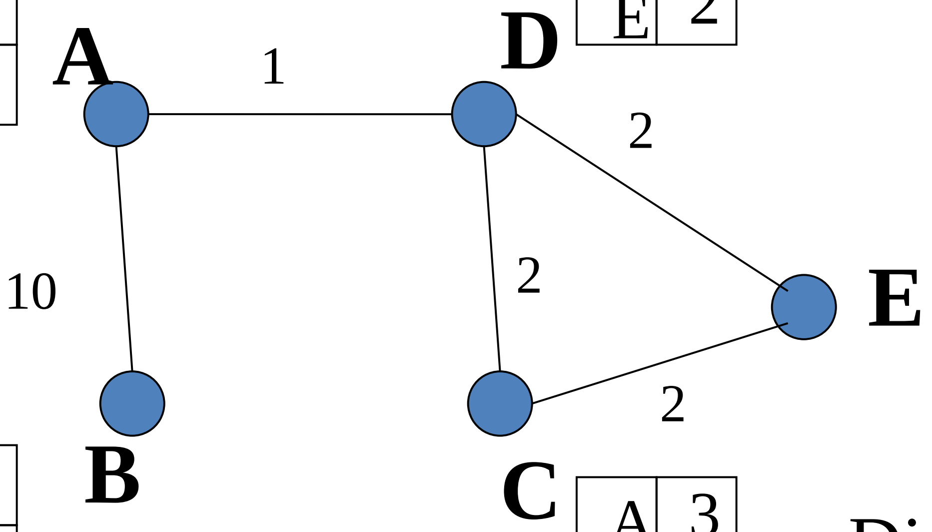
A	4
B	0
C	1
D	3
E	3

A	3
B	1
C	0
D	2
E	2

Bad news:
Link crash!!

A	0
B	4
C	3
D	1
E	3

A	1
B	3
C	2
D	0
E	2



A	3
B	3
C	2
D	2
E	0

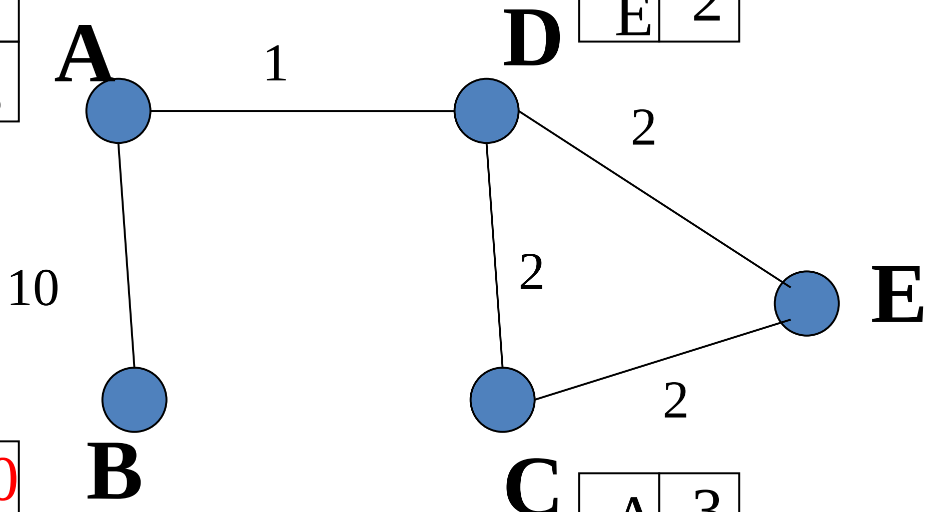
A	
B	0
C	
D	
E	

A	3
B	
C	0
D	2
E	2

Direct endpoints know

A	0
B	4
C	3
D	1
E	3

A	1
B	3
C	2
D	0
E	2



A	3
B	3
C	2
D	2
E	0

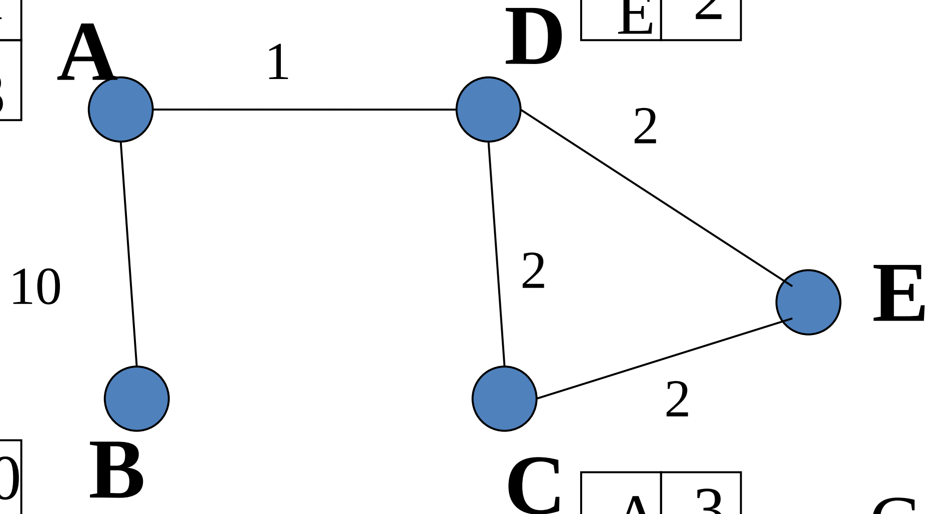
A	10
B	0
C	
D	
E	

A	3
B	
C	0
D	2
E	2

A	0
B	4
C	3
D	1
E	3

A	1
B	3
C	2
D	0
E	2

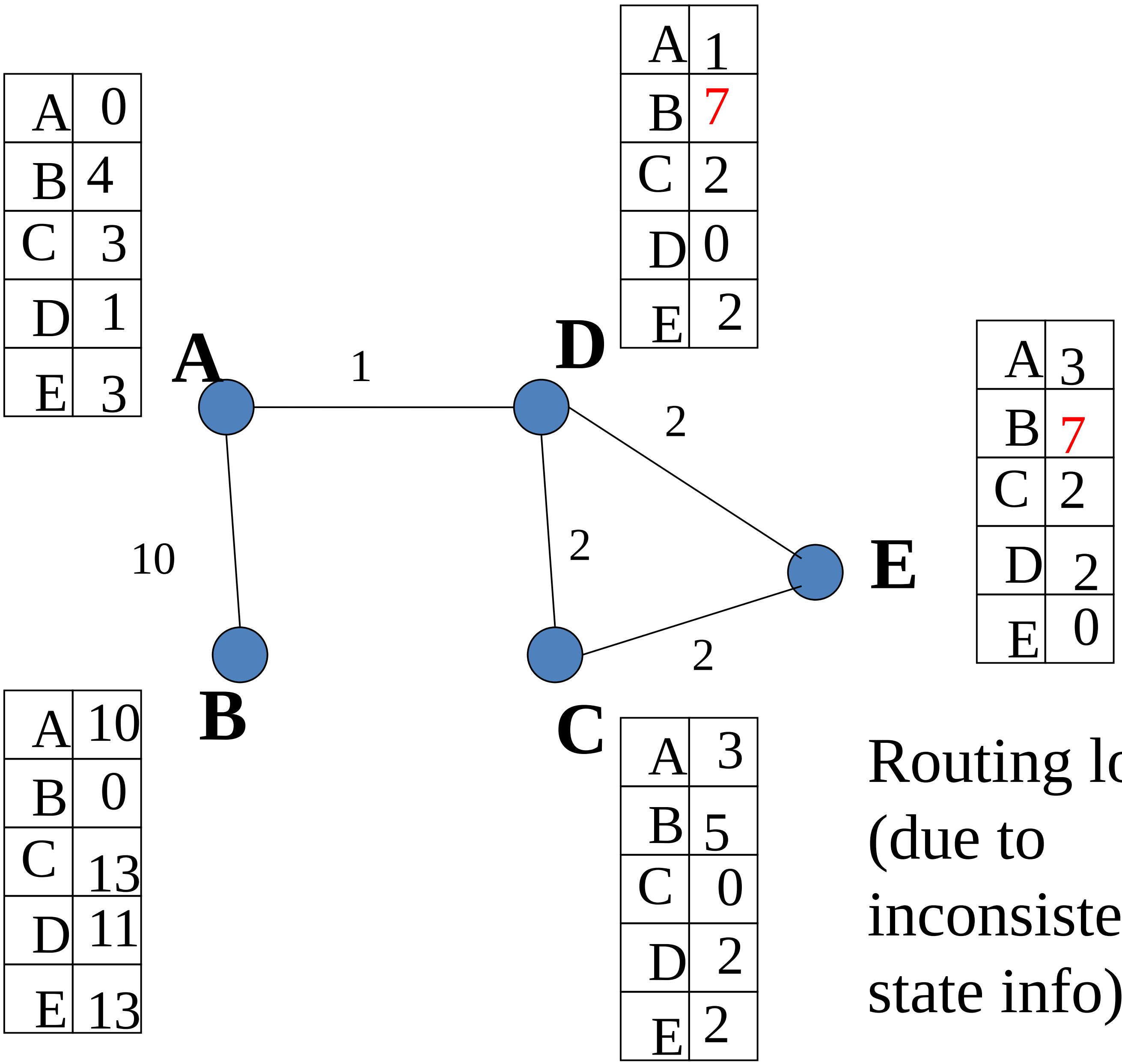
A	3
B	3
C	2
D	2
E	0



A	10
B	0
C	13
D	11
E	13

A	3
B	5
C	0
D	2
E	2

Get help from neighbours



A	0
B	4
C	3
D	1
E	3

A	1
B	7
C	2
D	0
E	2

A	3
B	7
C	2
D	2
E	0

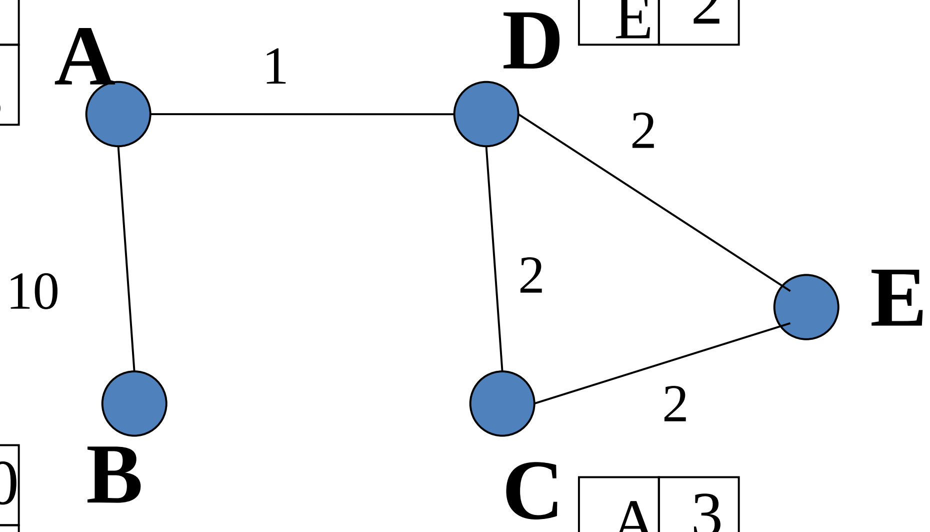
A	10
B	0
C	13
D	11
E	13

A	3
B	5
C	0
D	2
E	2

Routing loop (due to inconsistent state info)

Problem of DV Routing: Count-to-Infinity

- Count-to-Infinity problem
- **Counting to infinity** is just another name for a routing loop.
- In distance vector routing, routing loops usually occur when an interface goes down.
- It can also occur when two routers send updates to each other at the same time.



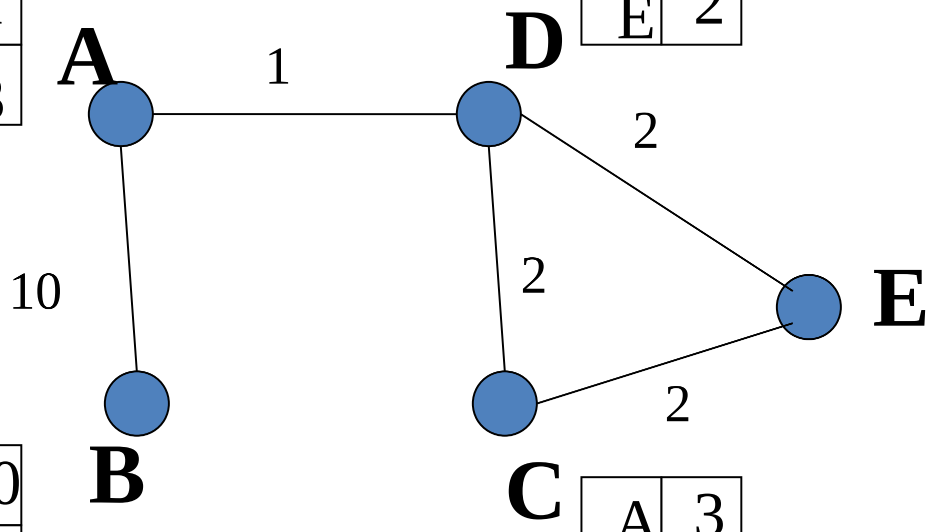
A	0
B	8
C	3
D	1
E	3

A	1
B	7
C	2
D	0
E	2

A	3
B	7
C	2
D	2
E	0

A	10
B	0
C	13
D	11
E	13

A	3
B	9
C	0
D	2
E	2



A	0
B	8
C	3
D	1
E	3

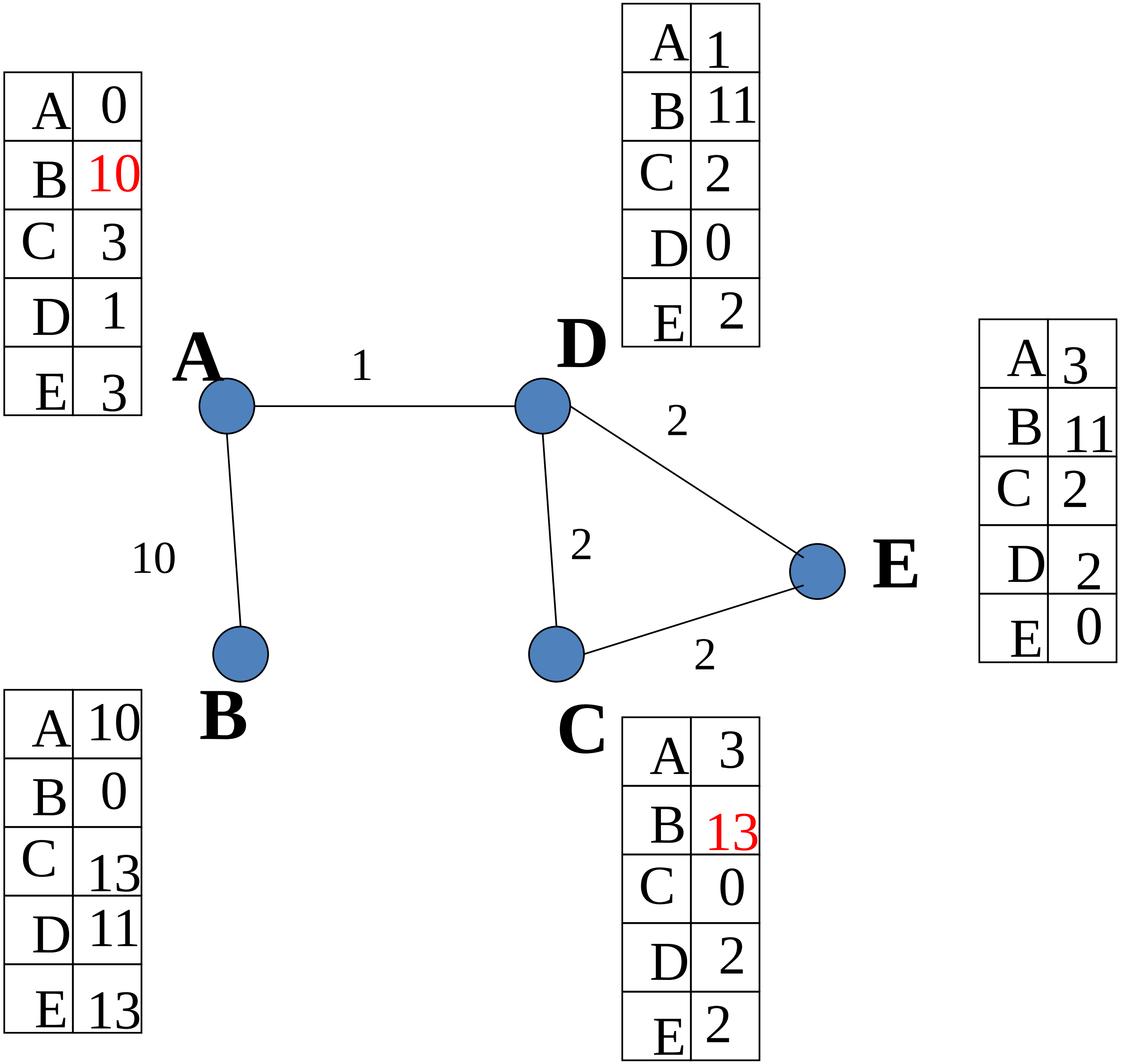
A	1
B	11
C	2
D	0
E	2

A	3
B	11
C	2
D	2
E	0

A	10
B	0
C	13
D	11
E	13

A	3
B	9
C	0
D	2
E	2

Counting
to infinity…



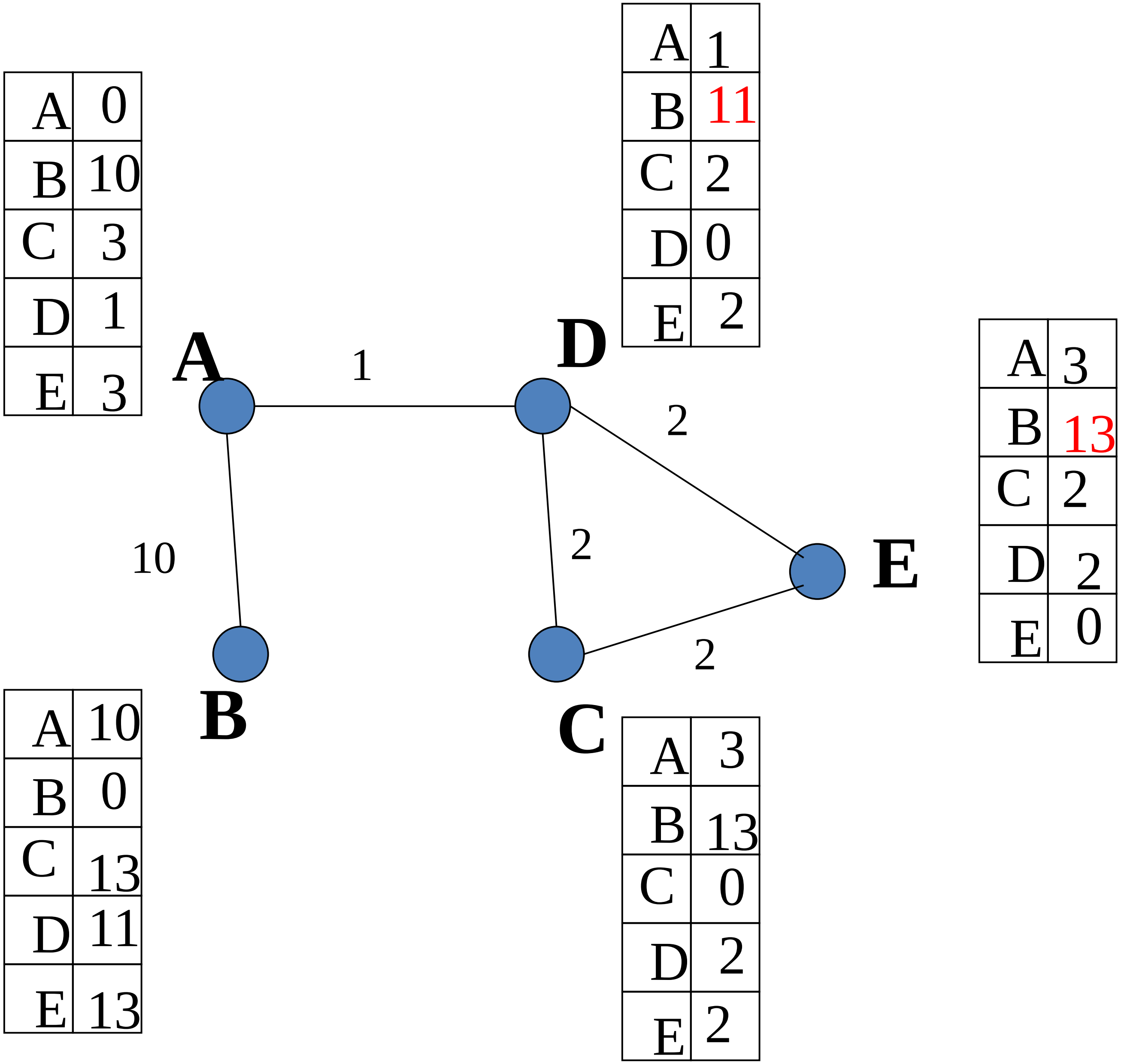
A	0
B	10
C	3
D	1
E	3

A	1
B	11
C	2
D	0
E	2

A	3
B	11
C	2
D	2
E	0

A	10
B	0
C	13
D	11
E	13

A	3
B	13
C	0
D	2
E	2



A	0
B	10
C	3
D	1
E	3

A	1
B	11
C	2
D	0
E	2

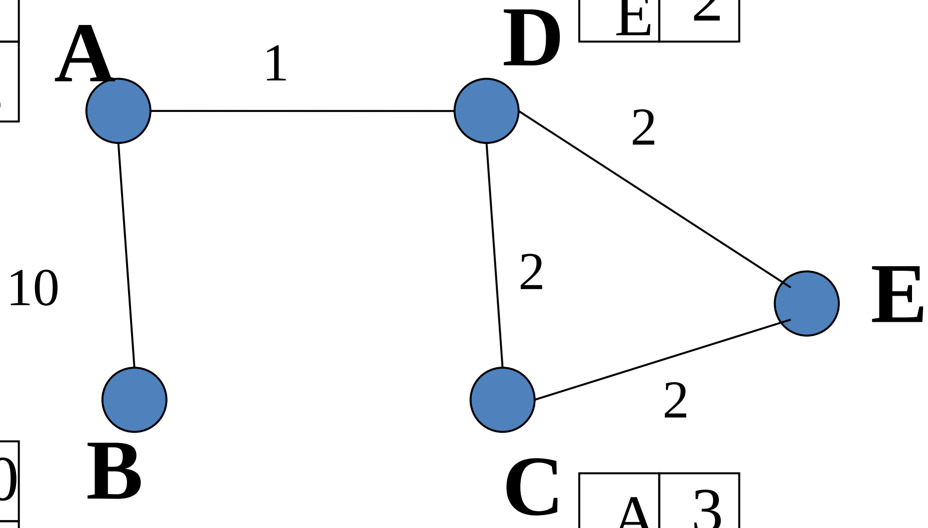
A	3
B	13
C	2
D	2
E	0

A	10
B	0
C	13
D	11
E	13

A	3
B	13
C	0
D	2
E	2

A	0
B	10
C	3
D	1
E	3

A	1
B	11
C	2
D	0
E	2



A	3
B	13
C	2
D	2
E	0

A	10
B	0
C	13
D	11
E	13

A	3
B	13
C	0
D	2
E	2

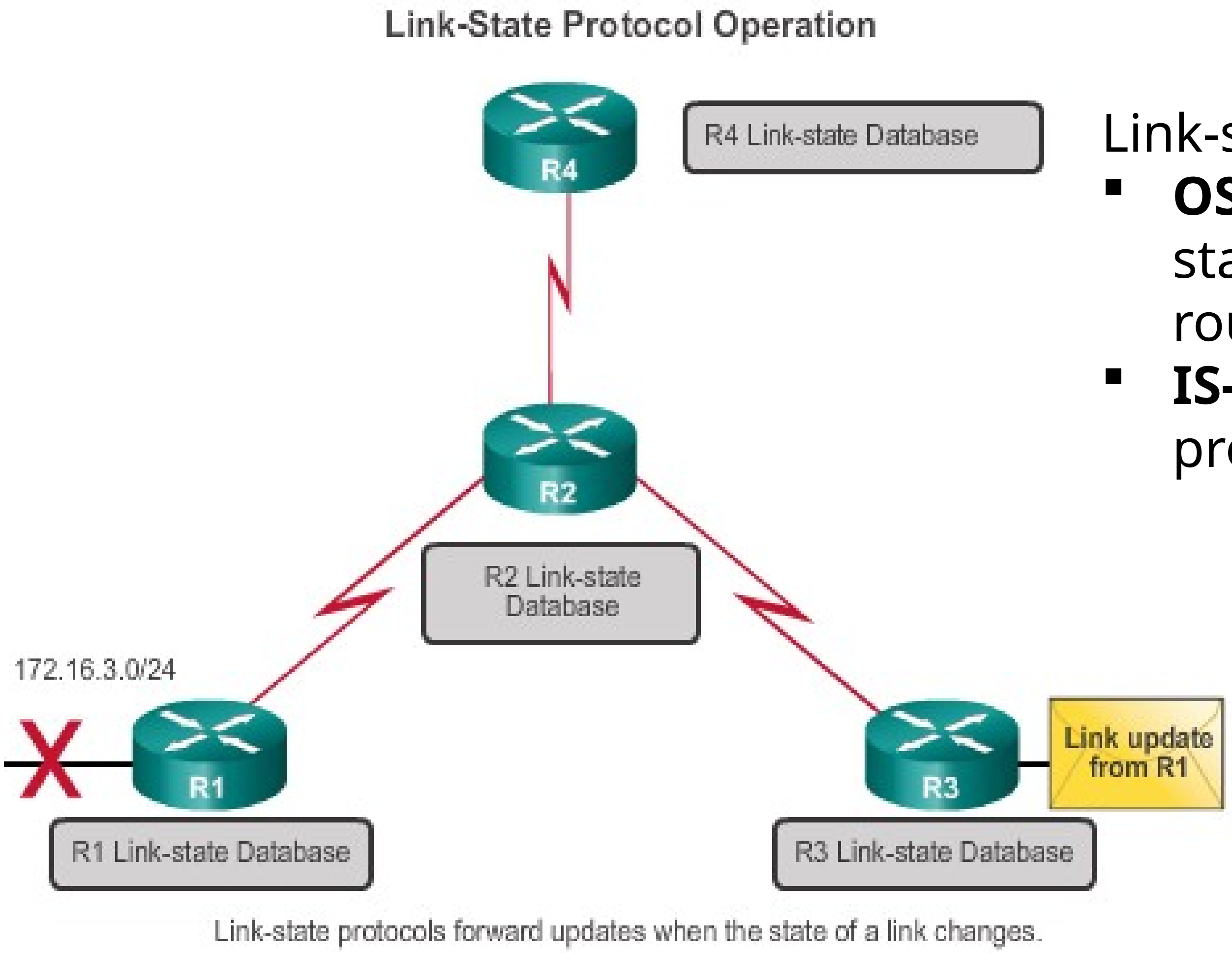
Stability again

Loop Breaking Heuristics

- Set infinity to a limited number, e.g. 16.
- Split horizon
- Split horizon with poison reverse

Link State Routing Protocols

Link-State Routing Protocols

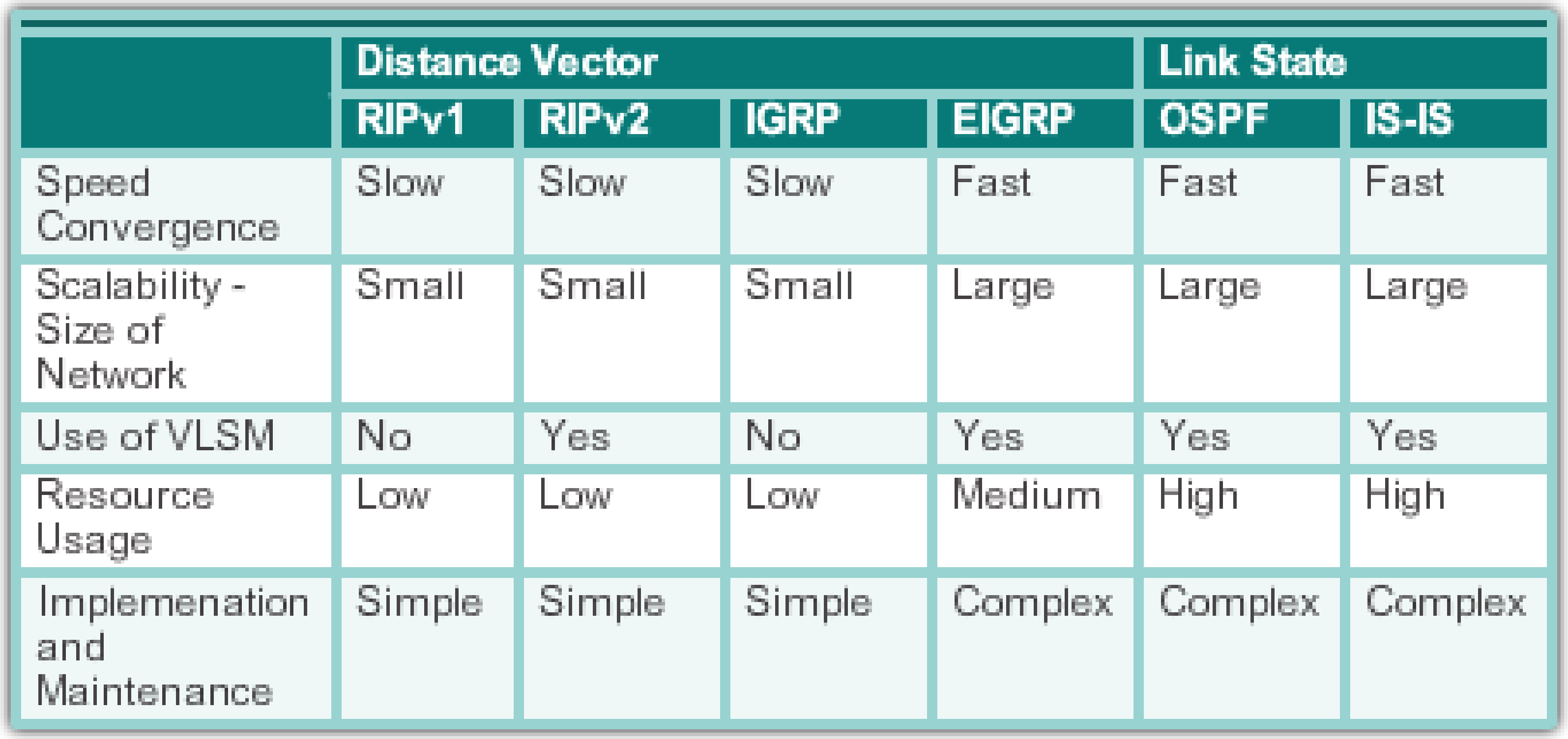


Link-state protocols forward updates when the state of a link changes.

Link-state IPv4 IGPs:

- **OSPF** - Popular standards based routing protocol
- **IS-IS** - Popular in provider networks.

Routing Protocol Characteristics

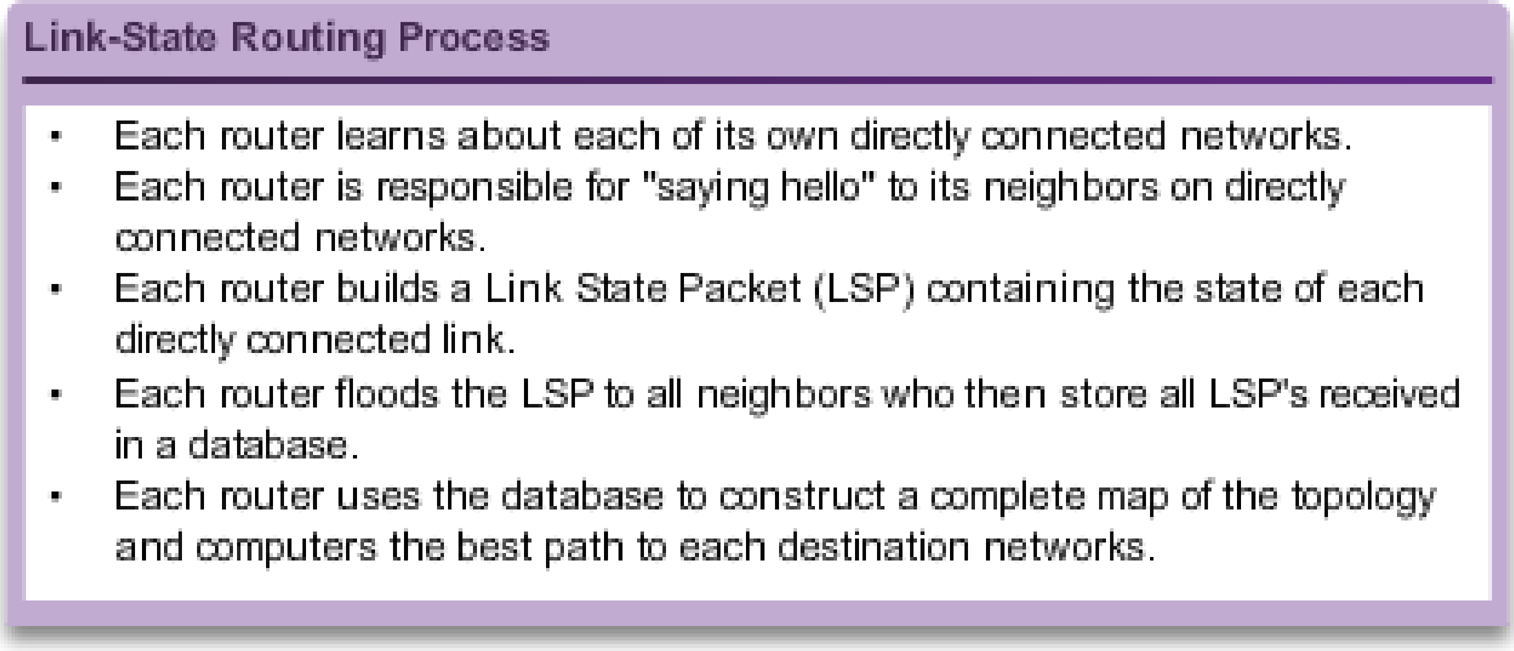


	Distance Vector				Link State	
	RIPv1	**RIPv2**	**IGRP**	**EIGRP**	**OSPF**	**IS-IS**
Speed Convergence	Slow	Slow	Slow	Fast	Fast	Fast
Scalability - Size of Network	Small	Small	Small	Large	Large	Large
Use of VLSM	No	Yes	No	Yes	Yes	Yes
Resource Usage	Low	Low	Low	Medium	High	High
Implemenation and Maintenance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

Open Shortest Path First

Features of OSPF

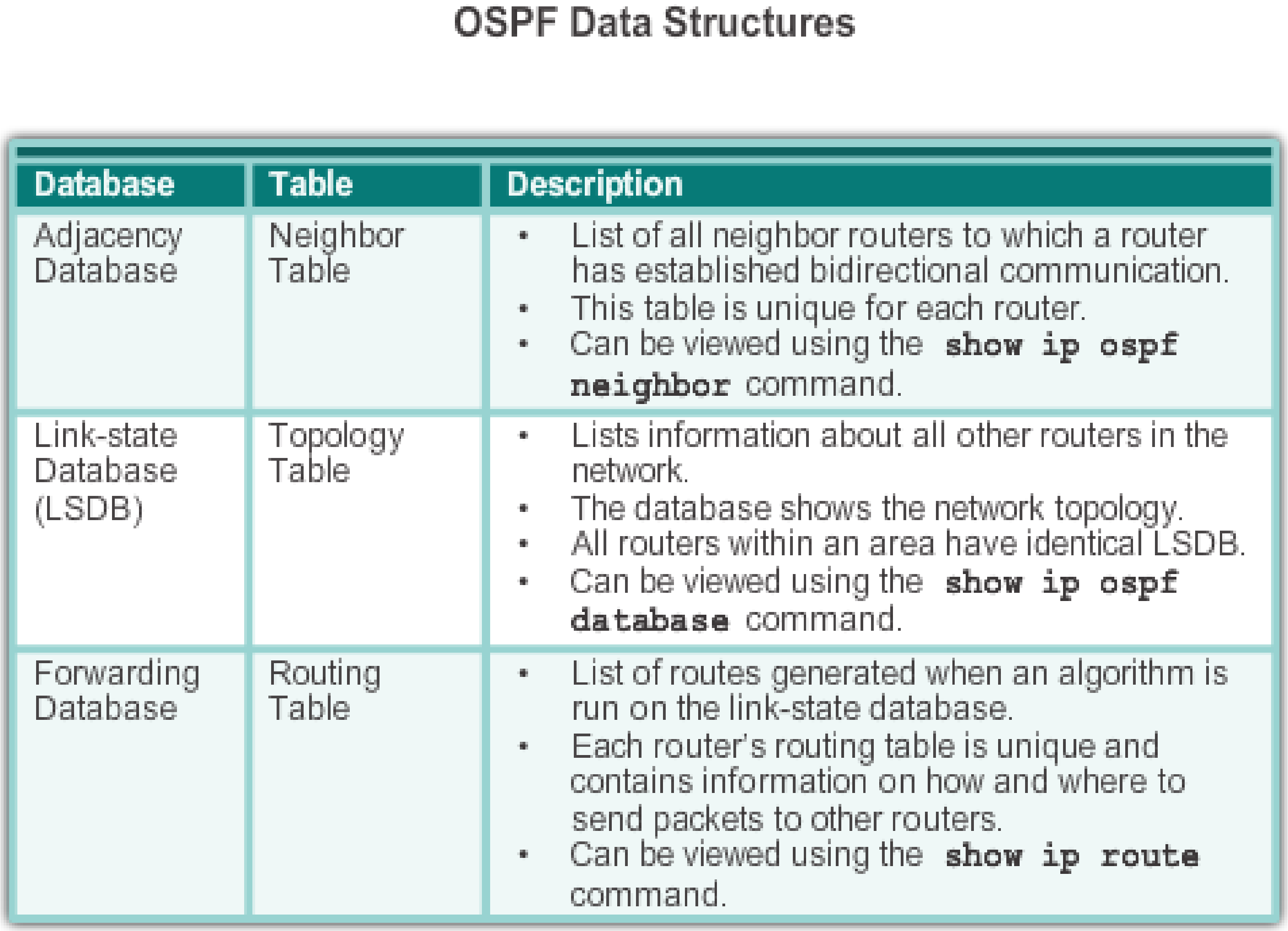
Link-State Routing Process



Link-State Routing Process

- Each router learns about each of its own directly connected networks.
- Each router is responsible for "saying hello" to its neighbors on directly connected networks.
- Each router builds a Link State Packet (LSP) containing the state of each directly connected link.
- Each router floods the LSP to all neighbors who then store all LSP's received in a database.
- Each router uses the database to construct a complete map of the topology and computers the best path to each destination networks.

Components of OSPF



OSPF Data Structures

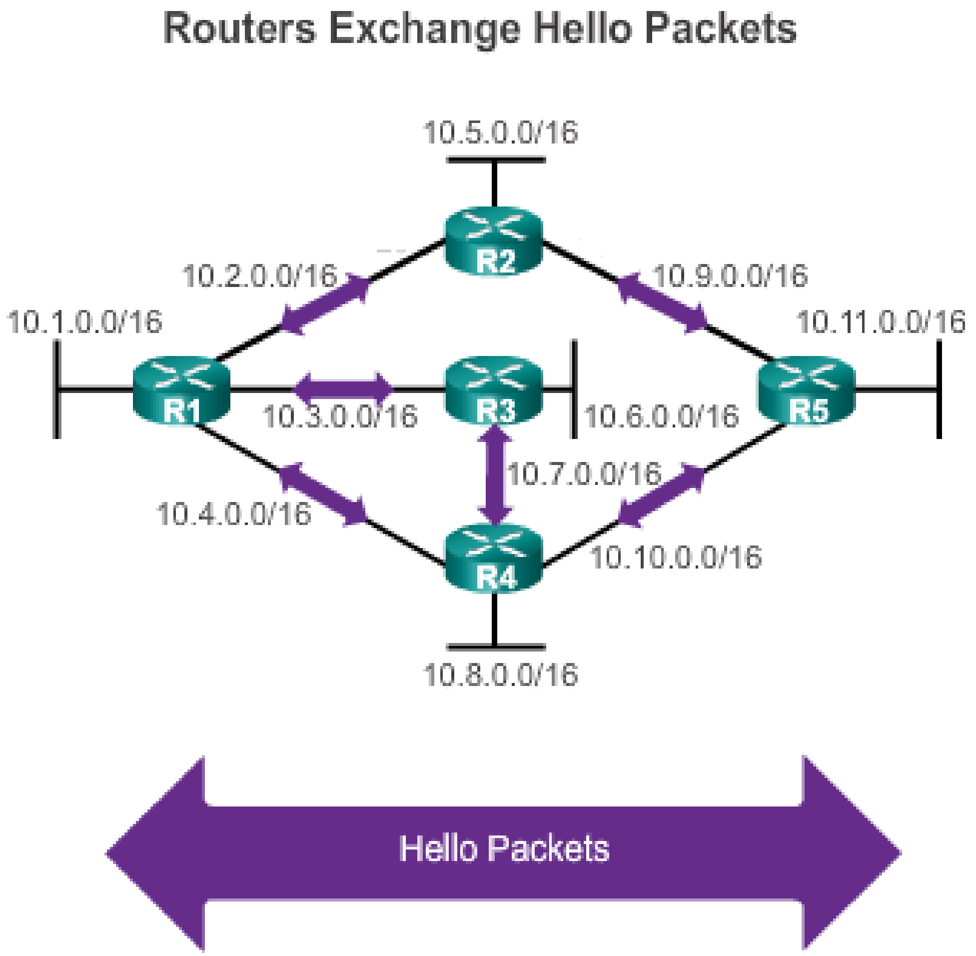
Database	Table	Description
Adjacency Database	Neighbor Table	- List of all neighbor routers to which a router has established bidirectional communication. - This table is unique for each router. - Can be viewed using the **`show ip ospf neighbor`** command.
Link-state Database (LSDB)	Topology Table	- Lists information about all other routers in the network. - The database shows the network topology. - All routers within an area have identical LSDB. - Can be viewed using the **`show ip ospf database`** command.
Forwarding Database	Routing Table	- List of routes generated when an algorithm is run on the link-state database. - Each router's routing table is unique and contains information on how and where to send packets to other routers. - Can be viewed using the **`show ip route`** command.

Components of OSPF

OSPF Routers Exchange Packets - These packets are used to discover neighboring routers and also to exchange routing information to maintain accurate information about the network.

Hello packets
Database Description packets
Link-state Request packets
Link-state Update packets
Link-state Acknowledgment packets

Hello Exchange

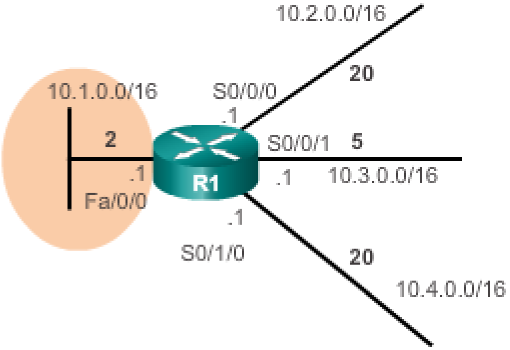


If a neighbor is present, the OSPF-enabled router attempts to establish a neighbor adjacency with that neighbor

Link and Link-State

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

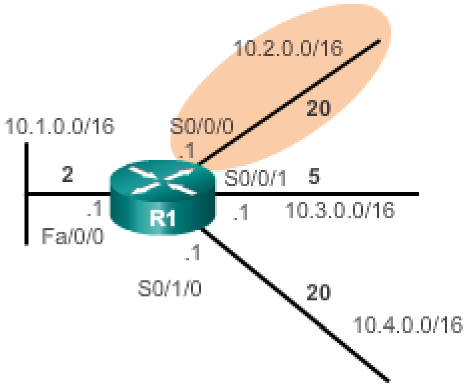
Link-State of Interface Fa0/0



Link 1

- Network: **10.1.0.0/16**
- IP address: **10.1.0.1**
- Type of network: **Ethernet**
- Cost of that link: **2**
- Neighbors: **None**

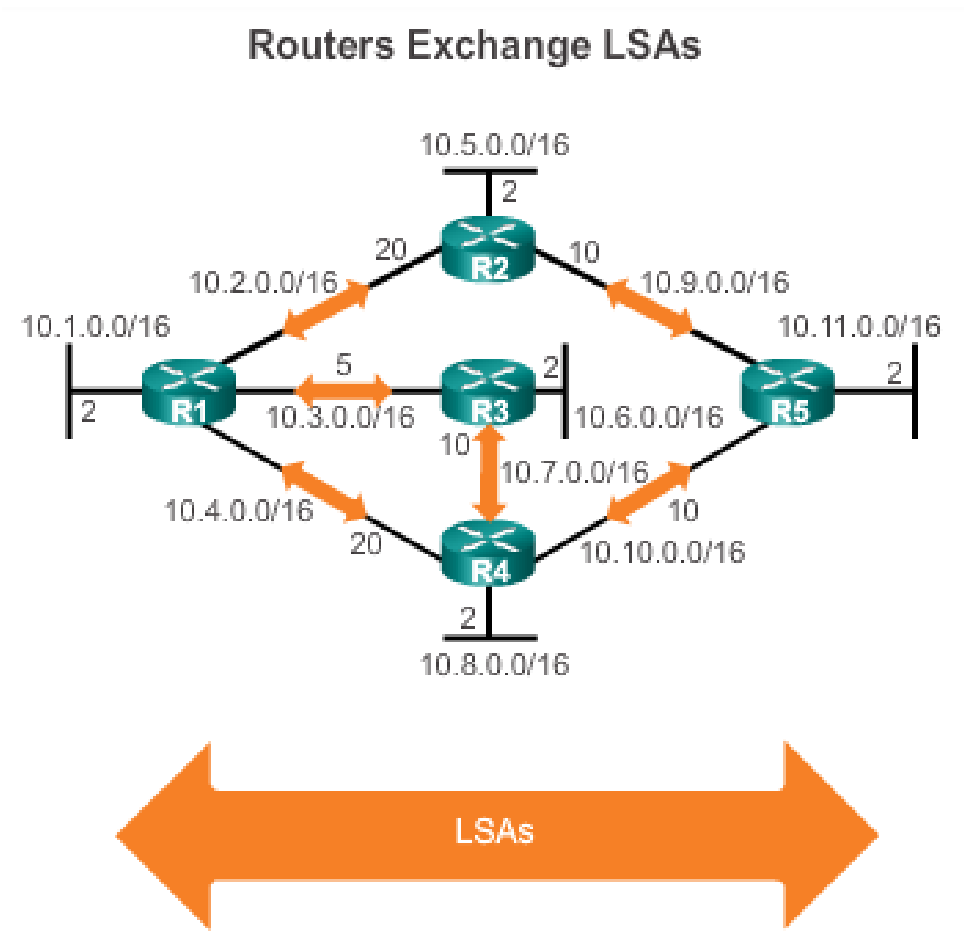
Link-State of Interface S0/0/0



Link 2

- Network: **10.2.0.0/16**
- IP address: **10.2.0.1**
- Type of network: **Serial**
- Cost of that link: **20**
- Neighbors: **R2**

Exchange of LSA

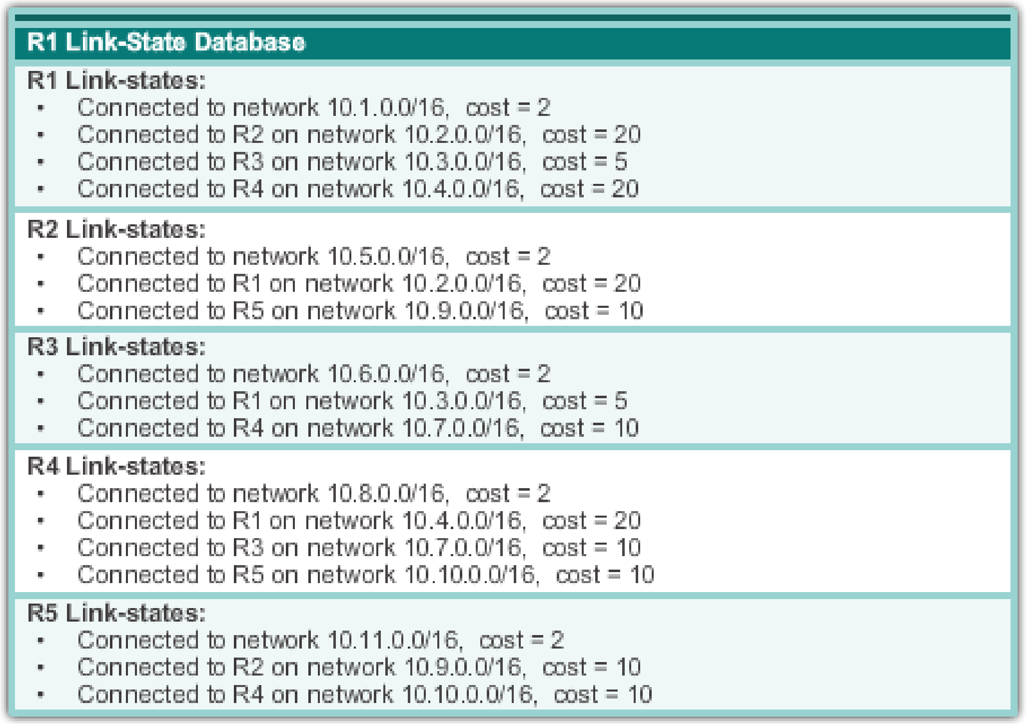


- LSAs contain the state and cost of each directly connected link.
- Routers flood their LSAs to adjacent neighbors.
- Adjacent neighbors receiving the LSA immediately flood the LSA to other directly connected neighbors, until all routers in the area have all LSAs.

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.

Contents of the Link-State Database



R1 Link-State Database

R1 Link-states:
- Connected to network 10.1.0.0/16, cost = 2
- Connected to R2 on network 10.2.0.0/16, cost = 20
- Connected to R3 on network 10.3.0.0/16, cost = 5
- Connected to R4 on network 10.4.0.0/16, cost = 20

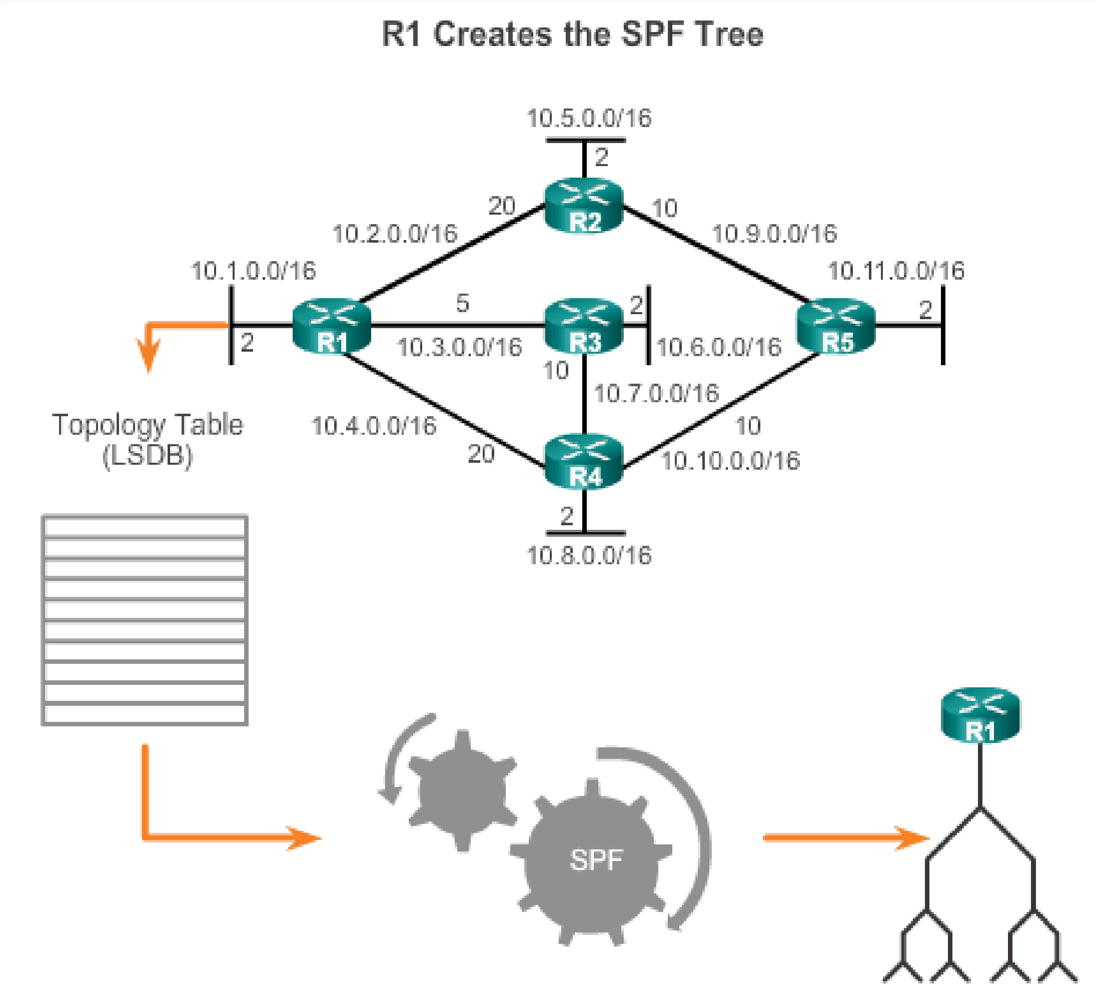
R2 Link-states:
- Connected to network 10.5.0.0/16, cost = 2
- Connected to R1 on network 10.2.0.0/16, cost = 20
- Connected to R5 on network 10.9.0.0/16, cost = 10

R3 Link-states:
- Connected to network 10.6.0.0/16, cost = 2
- Connected to R1 on network 10.3.0.0/16, cost = 5
- Connected to R4 on network 10.7.0.0/16, cost = 10

R4 Link-states:
- Connected to network 10.8.0.0/16, cost = 2
- Connected to R1 on network 10.4.0.0/16, cost = 20
- Connected to R3 on network 10.7.0.0/16, cost = 10
- Connected to R5 on network 10.10.0.0/16, cost = 10

R5 Link-states:
- Connected to network 10.11.0.0/16, cost = 2
- Connected to R2 on network 10.9.0.0/16, cost = 10
- Connected to R4 on network 10.10.0.0/16, cost = 10

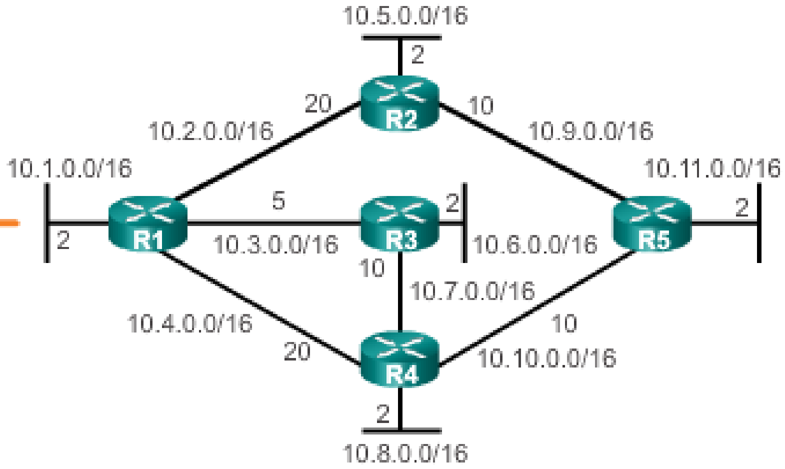
Creating SPF Tree



- Build the topology table based on the received LSAs.
- This database eventually holds all the information about the topology of the network.
- Execute the SPF Algorithm.

SPF Tree to best path Calculation

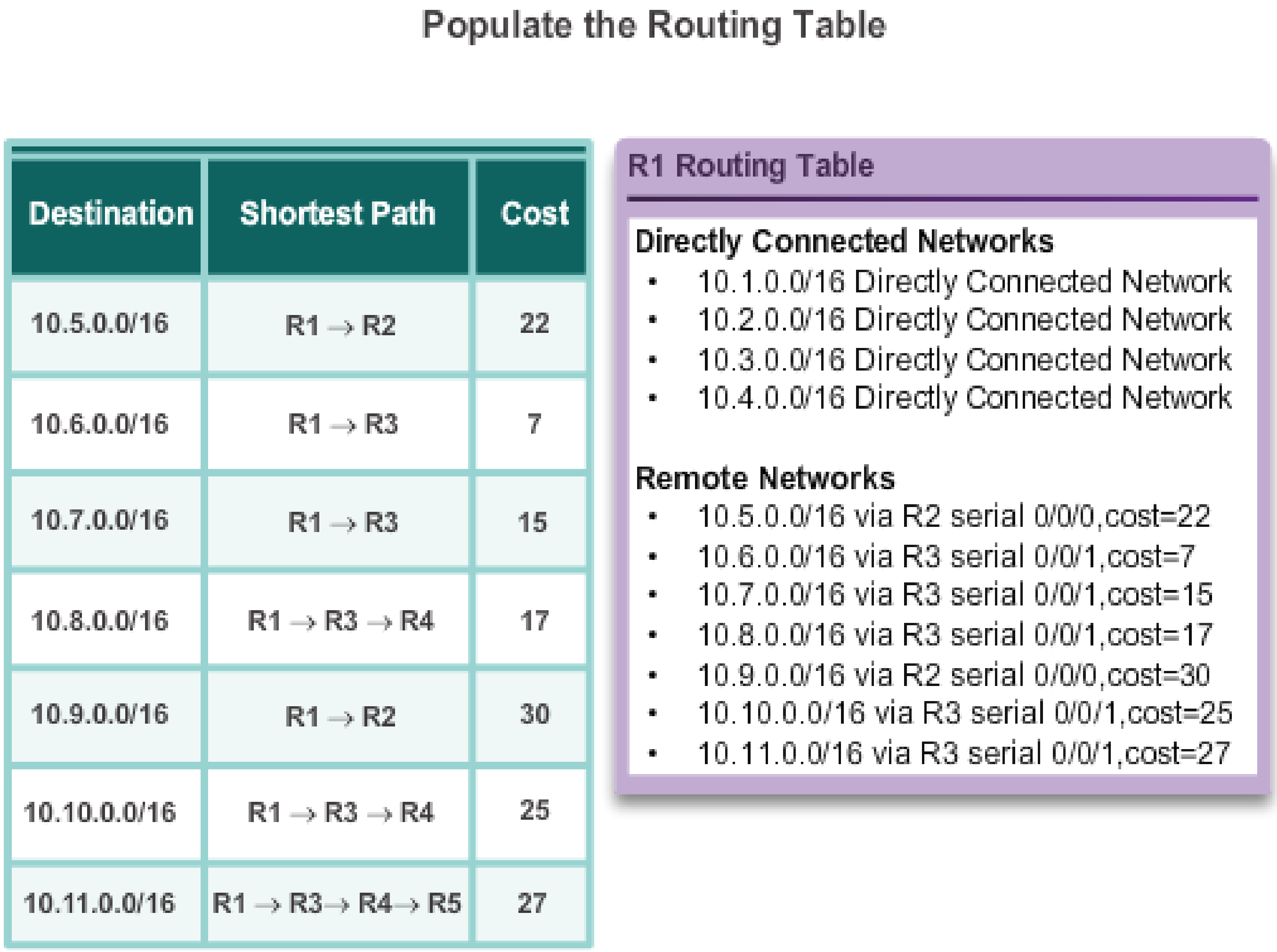
Content of the R1 SPF Tree



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

From the SPF tree, the best paths are inserted into the routing table.

Adding OSPF Routes to the Routing Table



Populate the Routing Table

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

R1 Routing Table

Directly Connected Networks

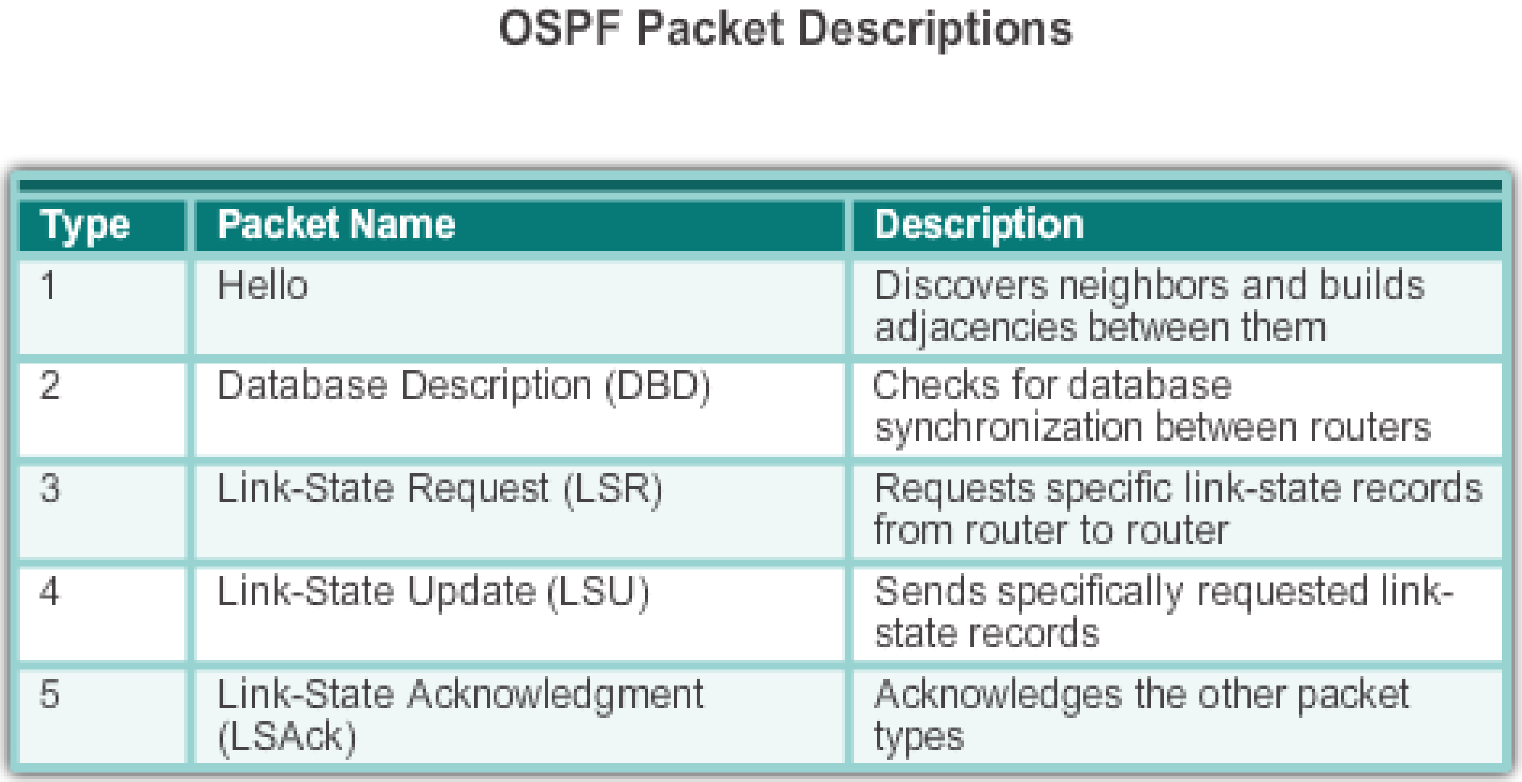
- 10.1.0.0/16 Directly Connected Network
- 10.2.0.0/16 Directly Connected Network
- 10.3.0.0/16 Directly Connected Network
- 10.4.0.0/16 Directly Connected Network

Remote Networks

- 10.5.0.0/16 via R2 serial 0/0/0,cost=22
- 10.6.0.0/16 via R3 serial 0/0/1,cost=7
- 10.7.0.0/16 via R3 serial 0/0/1,cost=15
- 10.8.0.0/16 via R3 serial 0/0/1,cost=17
- 10.9.0.0/16 via R2 serial 0/0/0,cost=30
- 10.10.0.0/16 via R3 serial 0/0/1,cost=25
- 10.11.0.0/16 via R3 serial 0/0/1,cost=27

OSPF Messages

Types of OSPF Packets



OSPF Packet Descriptions

Type	Packet Name	Description
1	Hello	Discovers neighbors and builds adjacencies between them
2	Database Description (DBD)	Checks for database synchronization between routers
3	Link-State Request (LSR)	Requests specific link-state records from router to router
4	Link-State Update (LSU)	Sends specifically requested link-state records
5	Link-State Acknowledgment (LSAck)	Acknowledges the other packet types

Hello Packet

OSPF Type 1 packet = Hello packet:

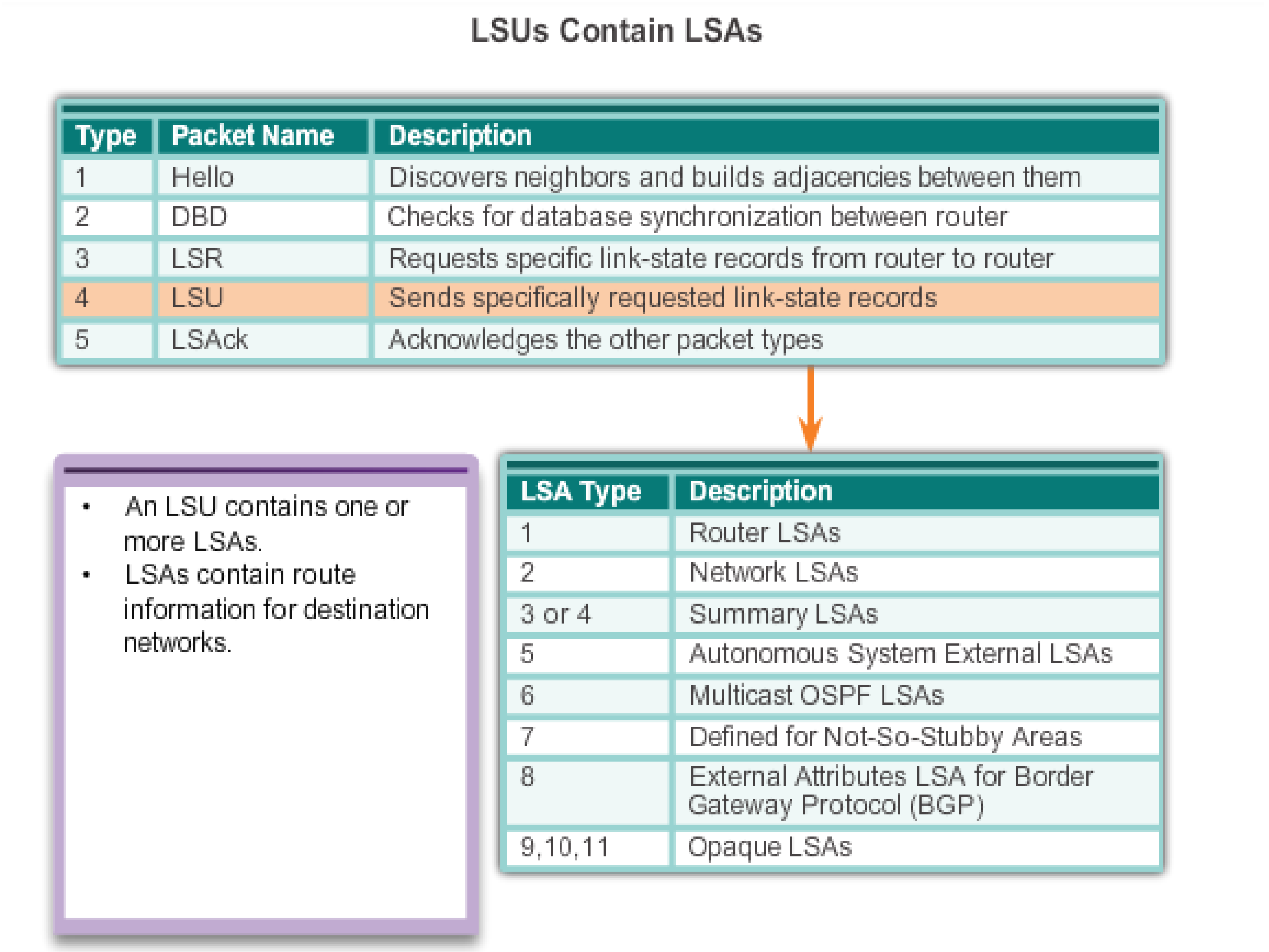
- Discover OSPF neighbors and establish neighbor adjacencies.
- Advertise parameters on which two routers must agree to become neighbors.
- Elect the Designated Router (DR) and Backup Designated Router (BDR) on multiaccess networks like Ethernet and Frame Relay.

Hello Packet Intervals

OSPF Hello packets are transmitted:

- To 224.0.0.5 in IPv4 and FF02::5 in IPv6 (all OSPF routers)
- Every 10 seconds (default on multiaccess and point-to-point networks)
- Every 30 seconds
- Dead interval is the period that the router waits to receive a Hello packet before declaring the neighbor down
- Router floods the LSDB with information about down neighbors out all OSPF enabled interfaces

Link-State Updates



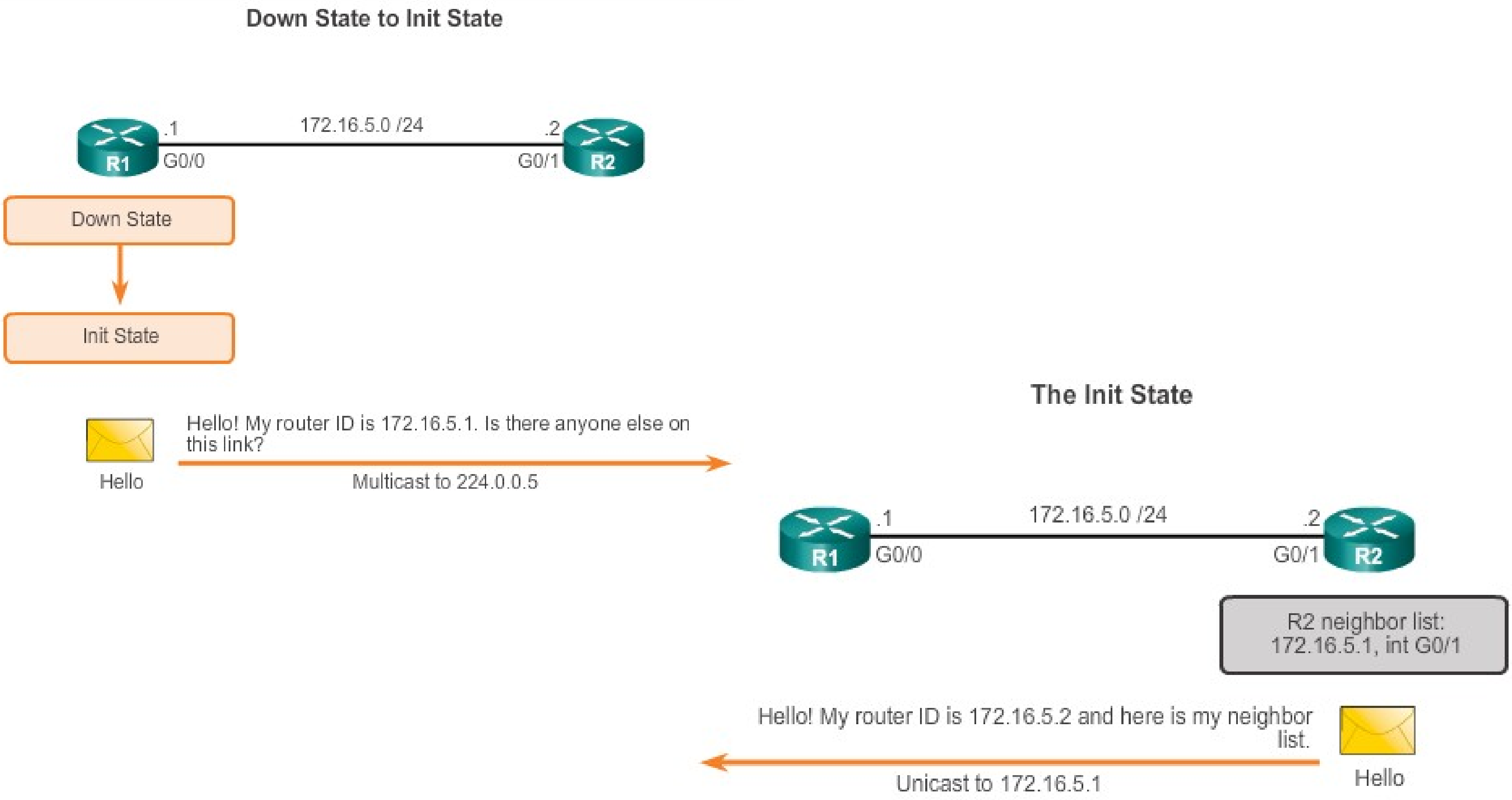
LSUs Contain LSAs

Type	Packet Name	Description
1	Hello	Discovers neighbors and builds adjacencies between them
2	DBD	Checks for database synchronization between router
3	LSR	Requests specific link-state records from router to router
4	LSU	Sends specifically requested link-state records
5	LSAck	Acknowledges the other packet types

- An LSU contains one or more LSAs.
- LSAs contain route information for destination networks.

LSA Type	Description
1	Router LSAs
2	Network LSAs
3 or 4	Summary LSAs
5	Autonomous System External LSAs
6	Multicast OSPF LSAs
7	Defined for Not-So-Stubby Areas
8	External Attributes LSA for Border Gateway Protocol (BGP)
9,10,11	Opaque LSAs

Establish Neighbor Adjacencies



Down State to Init State

Hello! My router ID is 172.16.5.1. Is there anyone else on this link?

Multicast to 224.0.0.5

The Init State

R2 neighbor list:
172.16.5.1, int G0/1

Hello! My router ID is 172.16.5.2 and here is my neighbor list.

Unicast to 172.16.5.1

OSPF Operation

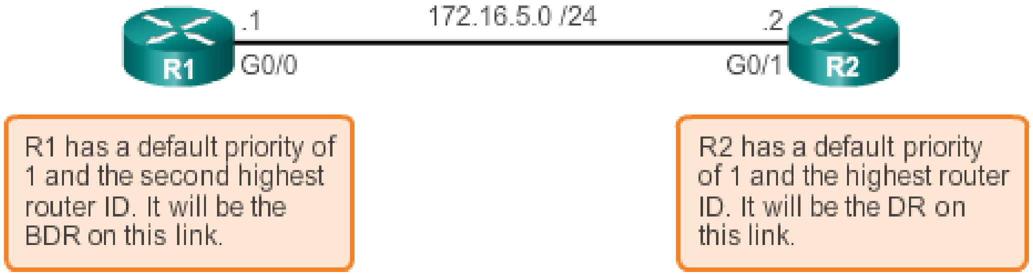
Establish Neighbor Adjacencies (cont.)

Two-Way State

R1 neighbor list:
172.16.5.2, int Fa0/0

Two-Way State

Elect the DR and BDR

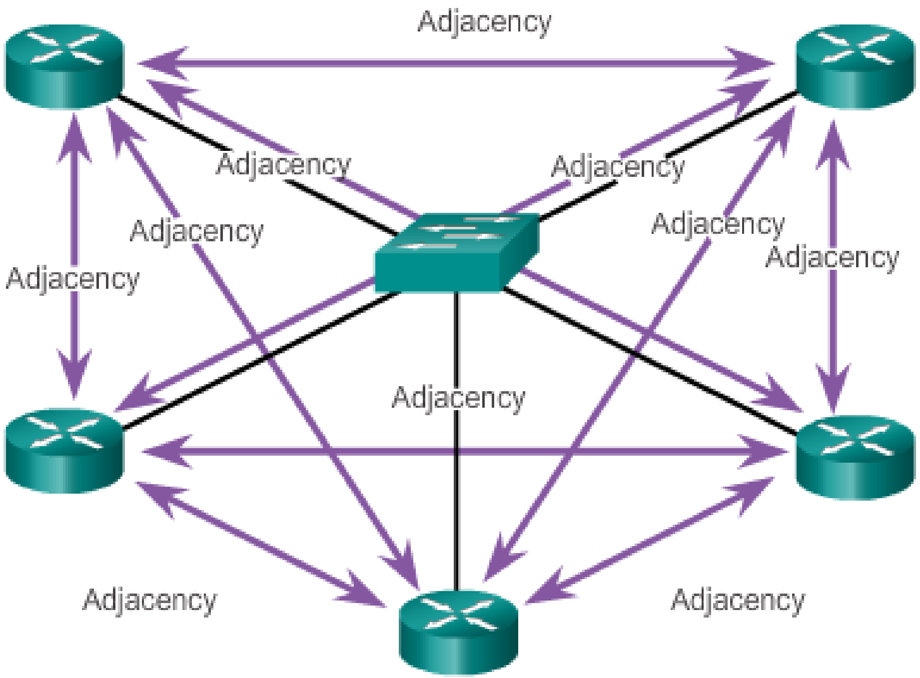


R1 has a default priority of 1 and the second highest router ID. It will be the BDR on this link.

R2 has a default priority of 1 and the highest router ID. It will be the DR on this link.

DR and BDR election only occurs on multi-access networks such as Ethernet LANs.

OSPF DR and BDR

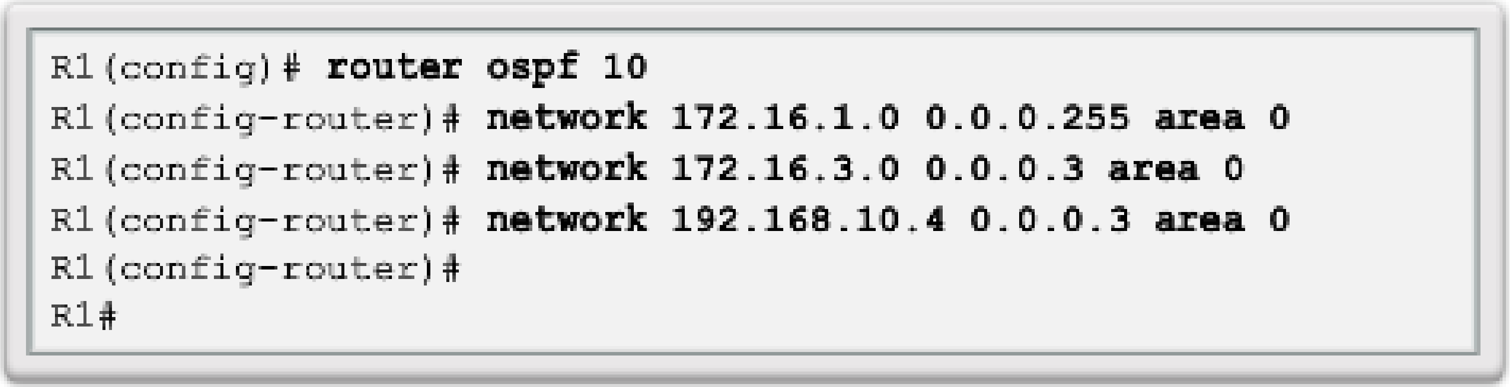


Creating Adjacencies With Every Neighbor

Number of Adjacencies=n(n-1)/2
n=number of routers
Example:5 routers (5-1)/2=10 adjacencies

Configure Single-area OSPFv2

Assigning Interfaces to an OSPF Area



```
R1(config)# router ospf 10
R1(config-router)# network 172.16.1.0 0.0.0.255 area 0
R1(config-router)# network 172.16.3.0 0.0.0.3 area 0
R1(config-router)# network 192.168.10.4 0.0.0.3 area 0
R1(config-router)#
R1#
```

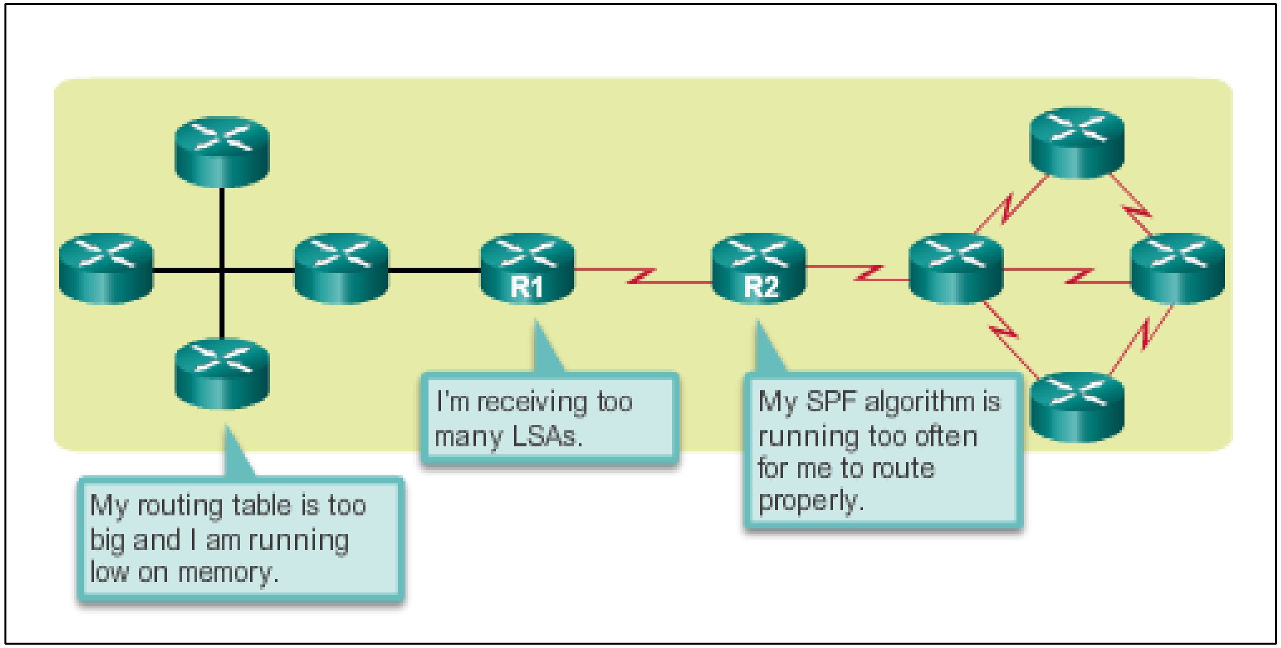
Single vs. Multi-Area OSPF

Why Multiarea OSPF?

Single-Area OSPF

Single-area OSPF is useful in smaller networks. If an area becomes too big, the following issues must be addressed:

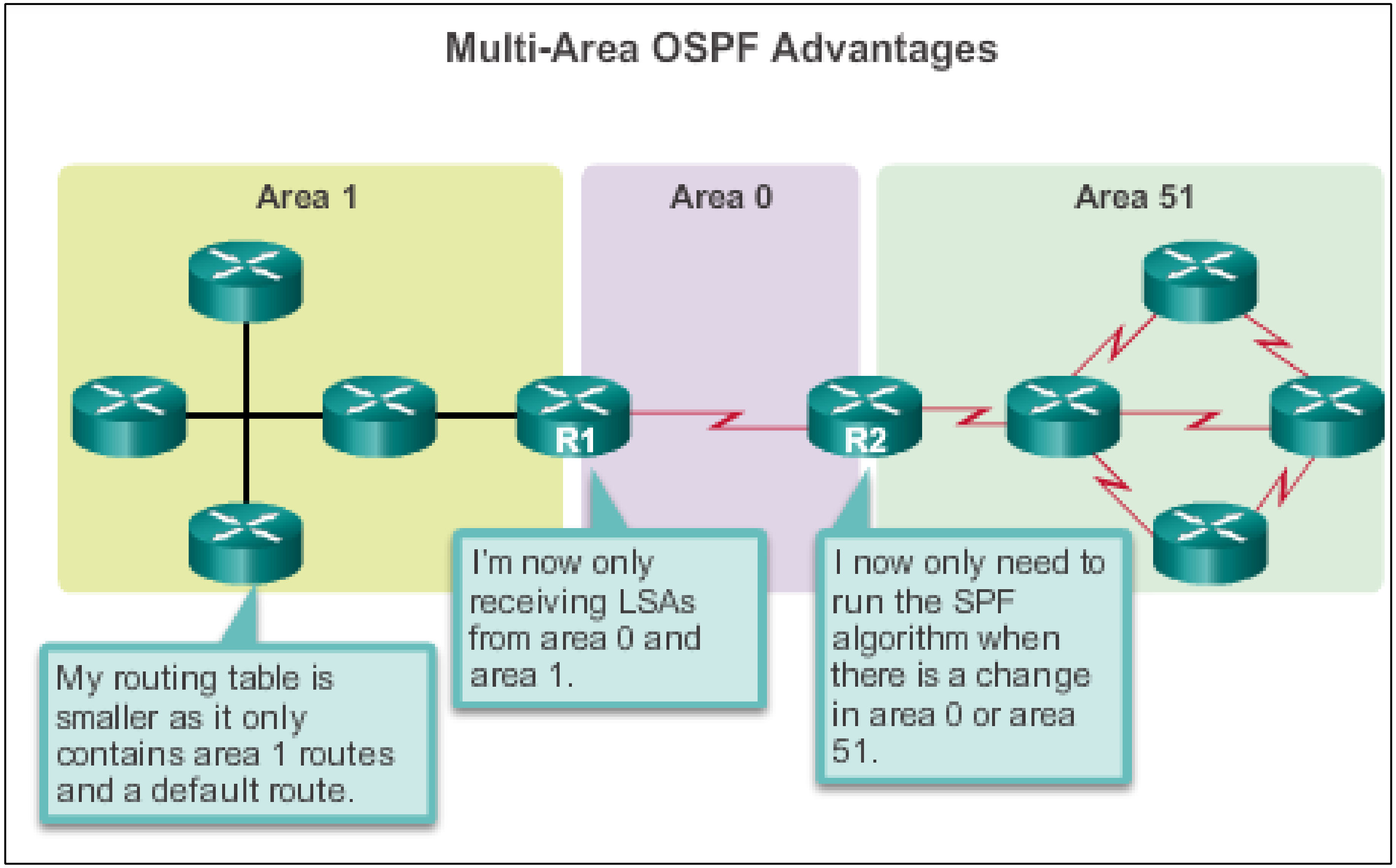
- Large routing table (no summarization by default)
- Large link-state database (LSDB)
- Frequent SPF algorithm calculations



Why Multiarea OSPF?

Multiarea OSPF

Multiarea OSPF requires a hierarchical network design and the main area is called the backbone area, or area 0, and all other areas must connect to the backbone area.



My routing table is smaller as it only contains area 1 routes and a default route.

I'm now only receiving LSAs from area 0 and area 1.

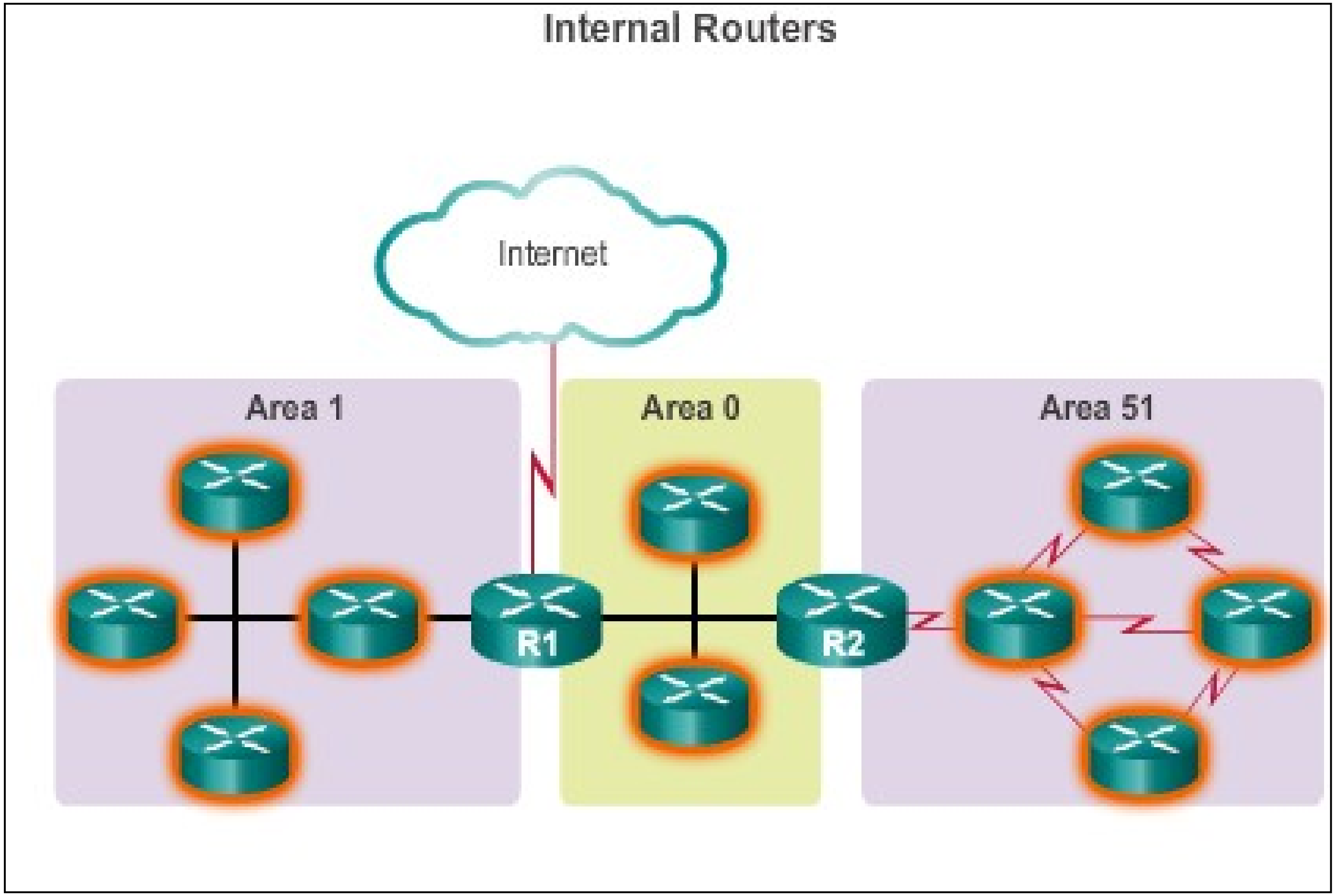
I now only need to run the SPF algorithm when there is a change in area 0 or area 51.

OSPF Two-Layer Area Hierarchy

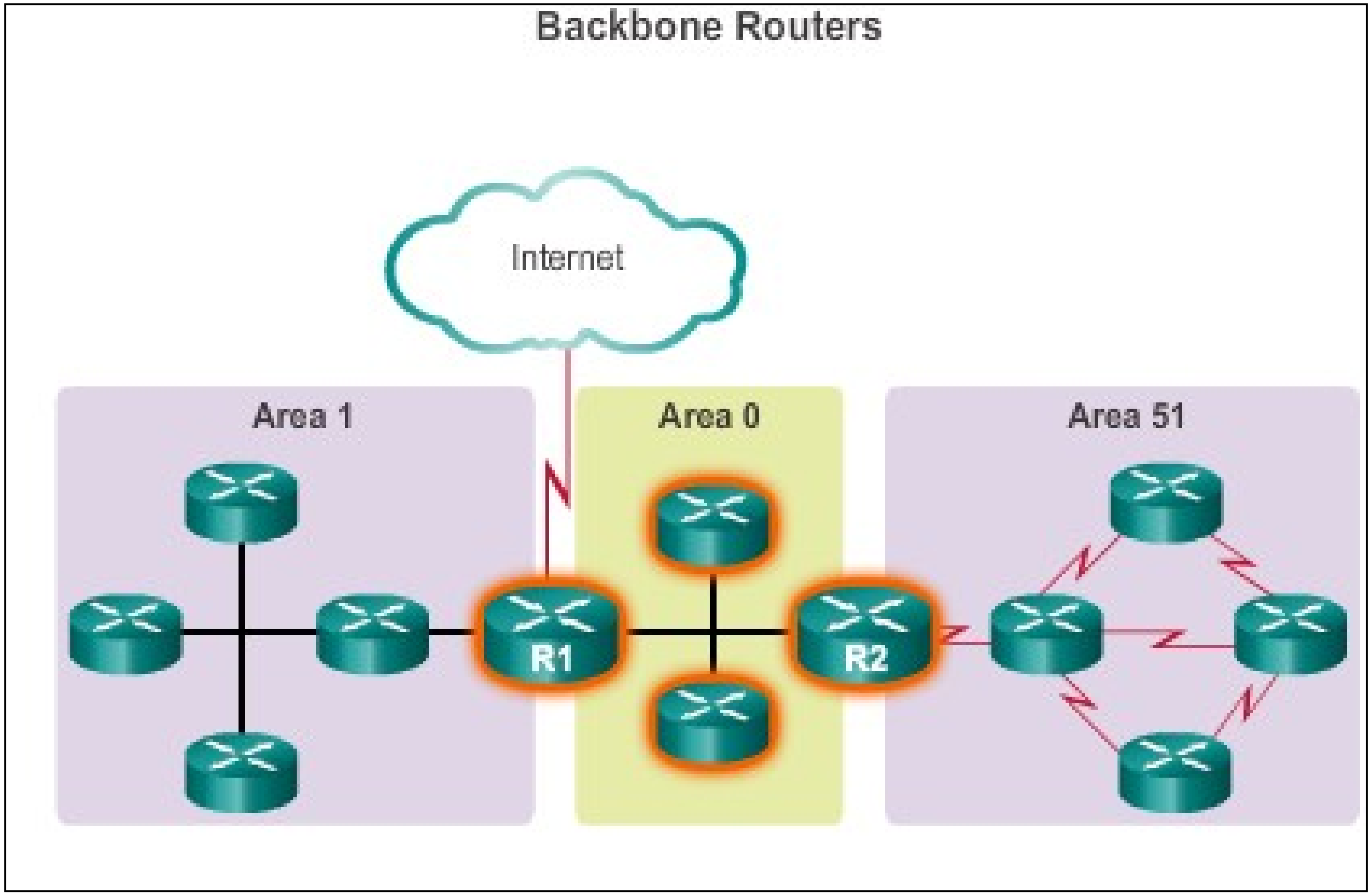
Multiarea OSPF is implemented in a two-layer area hierarchy:

- **Backbone (transit) area**
  - Area whose primary function is the fast and efficient movement of IP packets.
  - Interconnects with other OSPF area types.
  - Called OSPF area 0, to which all other areas directly connect.
- **Regular (nonbackbone) area**
  - Connects users and resources.
  - A regular area does not allow traffic from another area to use its links to reach other areas.

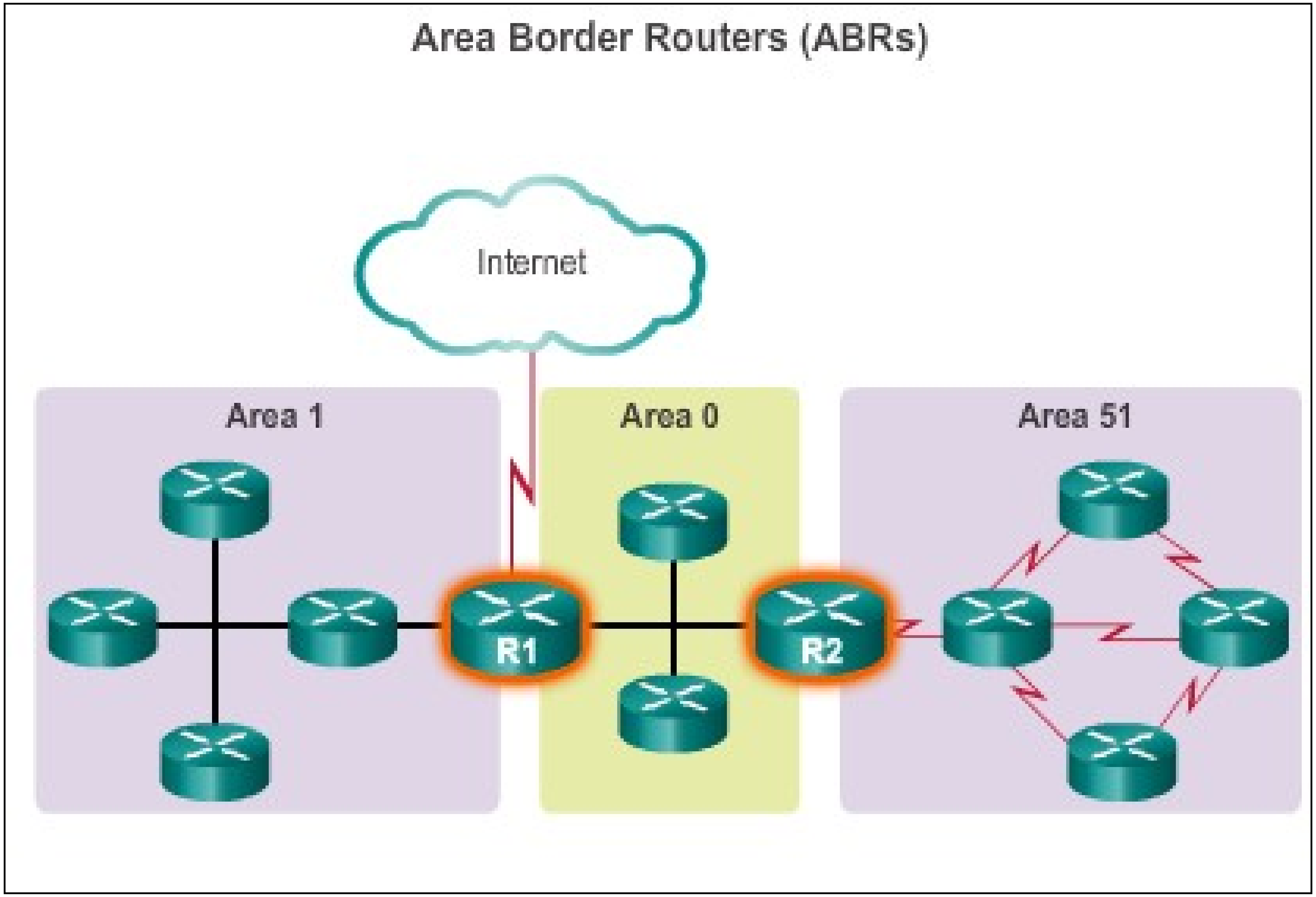
Types of OSPF Routers



Types of OSPF Routers (cont.)

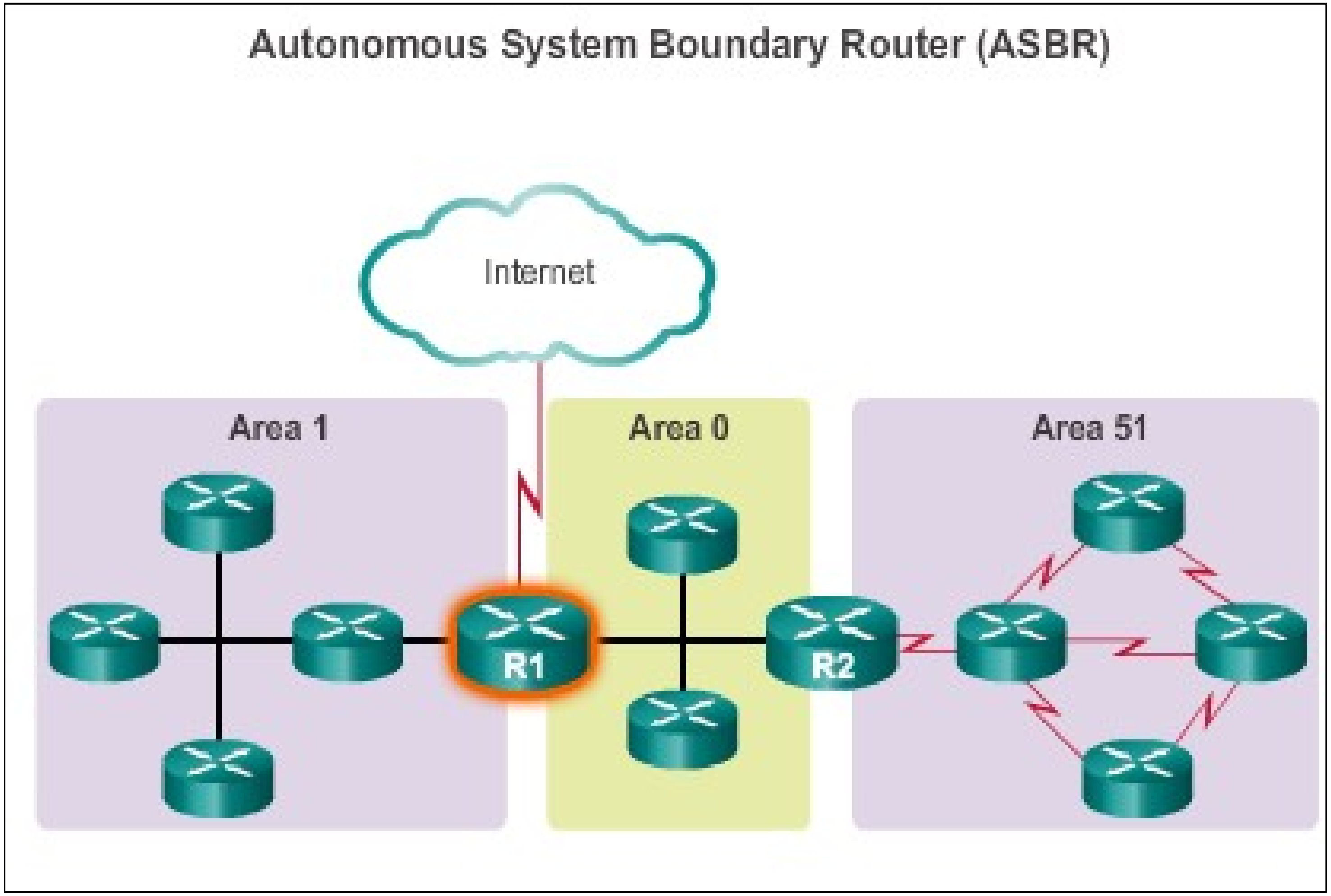


Types of OSPF Routers (cont.)



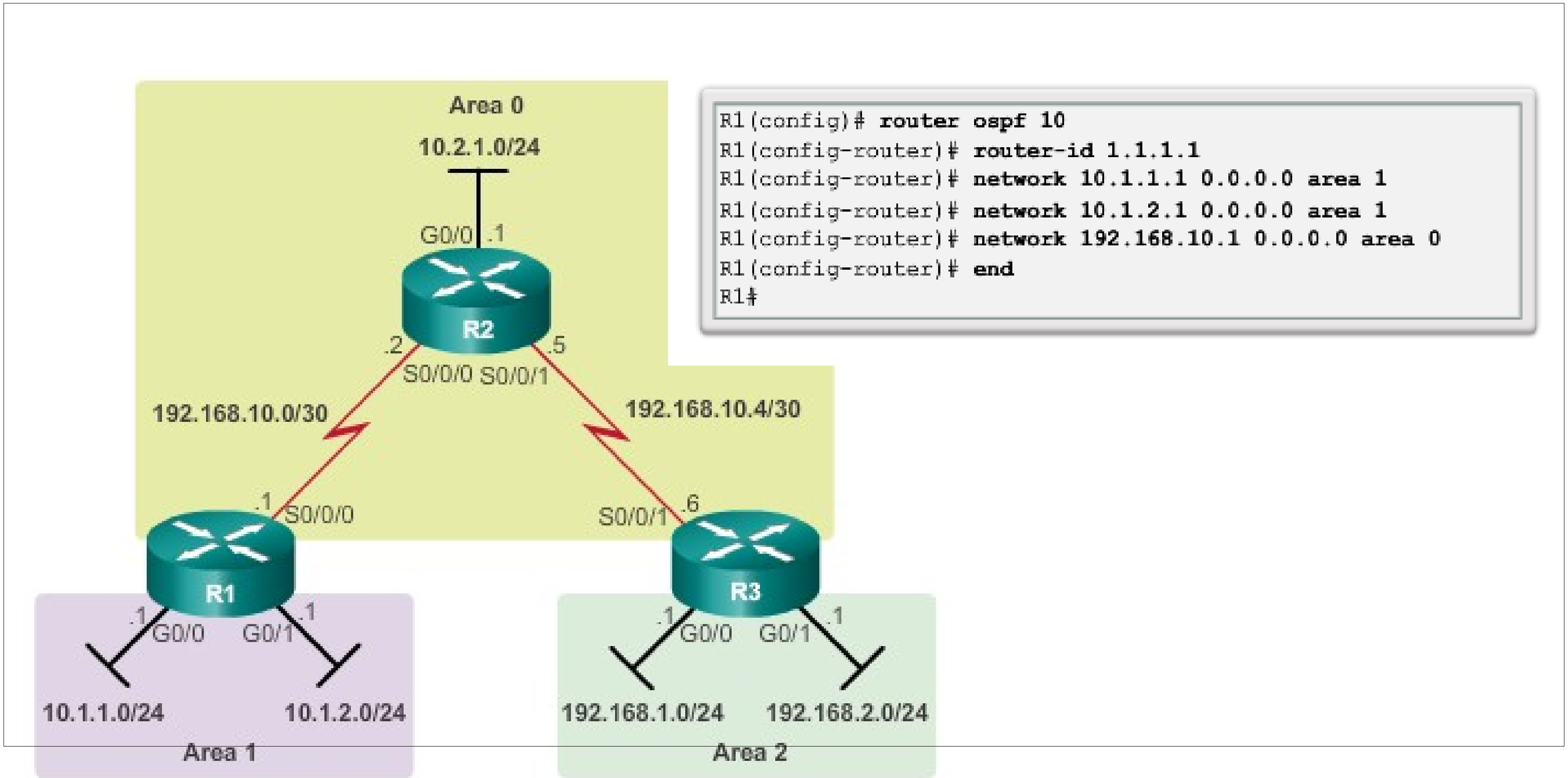
Why Multiarea OSPF?

Types of OSPF Routers (cont.)



Configuring Multi Area OSPF

Configuring Multiarea OSPF



```
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 10.1.1.1 0.0.0.0 area 1
R1(config-router)# network 10.1.2.1 0.0.0.0 area 1
R1(config-router)# network 192.168.10.1 0.0.0.0 area 0
R1(config-router)# end
R1#
```

Verifying Multiarea OSPF

The same verification commands are used to verify single-area OSPF and can be used to verify multiarea OSPF:

- **`show ip ospf neighbor`**
- **`show ip ospf`**
- **`show ip ospf interface`**

Commands specific to multiarea information include:

- **`show ip protocols`**
- **`show ip ospf interface brief`**
- **`show ip route ospf`**
- **`show ip ospf database`**