Routing

Anatomy of an IP Packet

IP packets consist of the data from upper layers plus an IP header. The IP header consists of the following:

0	4	8	16	19	24	31
VERS	HLEN	Service Type	Total Lenth			
Identification			Flags	Fragment Offset		
Time to Live		Protocol	Header Checksum			
Source IP Address						
Destination IP Address						
IP Options (if any)					Padding	
Data						
. . .						

These are the header fields in an IP packet header. All field lengths are fixed except for IP options and the padding fields

Introducing Routing

Routing is the process that a router uses to forward packets toward the destination network. A router makes decisions based upon the destination IP address of a packet. All devices along the way use the destination IP address to point the packet in the correct direction so that the packet eventually arrives at its destination. In order to make the correct decisions, routers must learn the direction to remote networks.

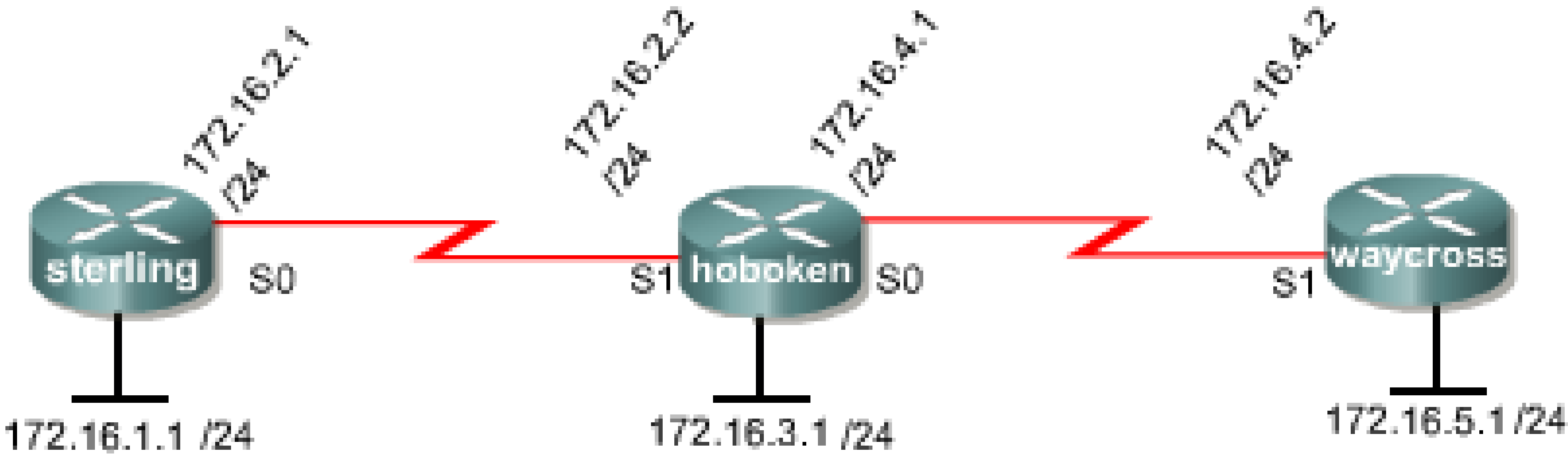
Static

Uses a programmed route that a network administrator enters into the router

Dynamic

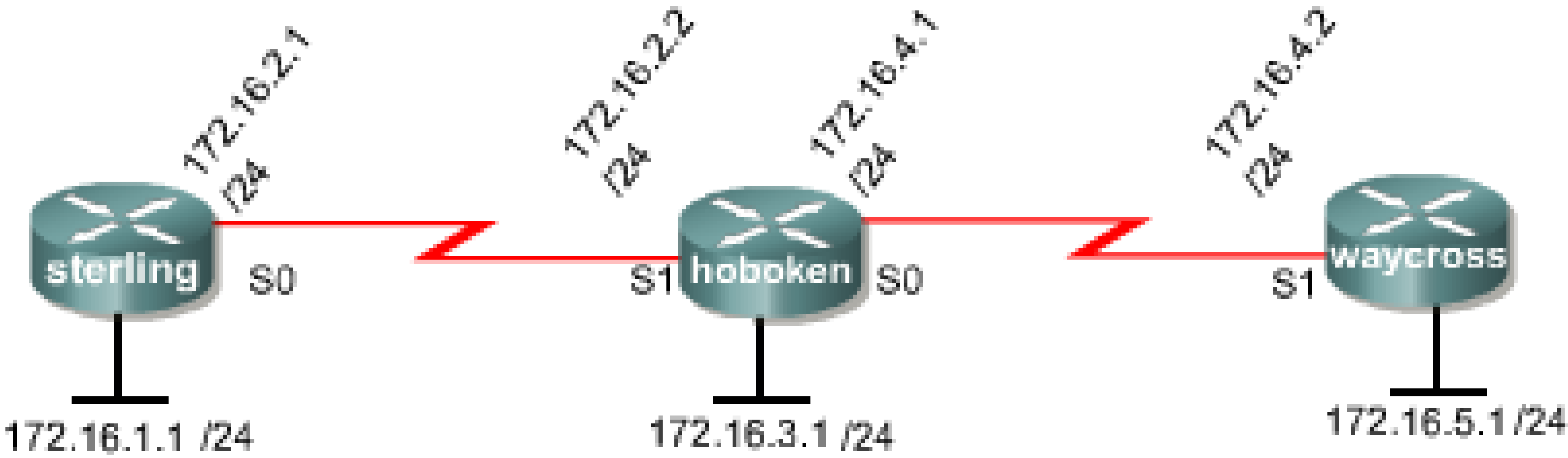
Uses a route that a routing protocol adjusts automatically for topology or traffic changes

Configuring Static Routes by Specifying Outgoing Interfaces




```
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 s1
               command  destination  sub mask      gateway
                          network
Hoboken(config)#ip route 172.16.5.0 255.255.255.0 s0
               command  destination  sub mask      gateway
                          network
```

Configuring Static Routes by Specifying Next-Hop Addresses




```
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1
```
command — destination network — sub mask — gateway

```
Hoboken(config)#ip route 172.16.5.0 255.255.255.0 172.16.4.2
```
command — destination network — sub mask — gateway

Administrative Distance

The administrative distance is an optional parameter that gives a measure of the reliability of the route. The range of an AD is 0-255 where smaller numbers are more desireable.

The default administrative distance when using next-hop address is 1, while the default administrative distance when using the outgoing interface is 0. You can statically assign an AD as follows:

Router(config)#**ip route 172.16.3.0 255.255.255.0 172.16.4.1 130**

Sometimes static routes are used for backup purposes. A static route can be configured on a router that will only be used when the dynamically learned route has failed. To use a static route in this manner, simply set the administrative distance higher than that of the dynamic routing protocol being used.

Configuring Default Routes

Default routes are used to route packets with destinations that do not match any of the other routes in the routing table.

A default route is actually a special static route that uses this format:

ip route 0.0.0.0 0.0.0.0 [*next-hop-address* | *outgoing interface*]

This is sometimes referred to as a "Quad-Zero" route.

Example using next hop address:

Router(config)#**ip route 0.0.0.0 0.0.0.0 172.16.4.1**

Example using the exit interface:

Router(config)#**ip route 0.0.0.0 0.0.0.0 s0/0**

Verifying Static Route Configuration

After static routes are configured it is important to verify that they are present in the routing table and that routing is working as expected.

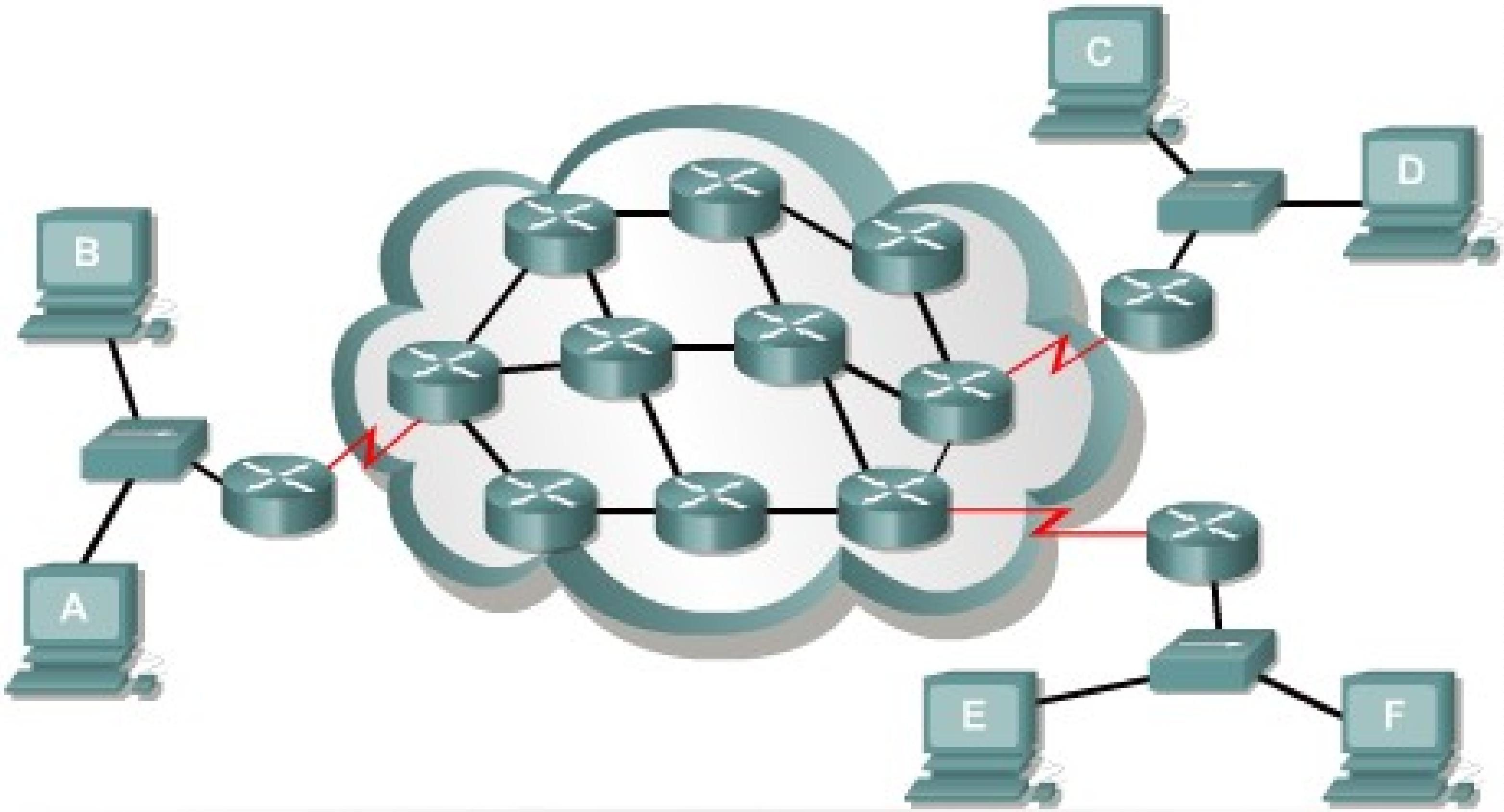
The command **show running-config** is used to view the active configuration in RAM to verify that the static route was entered correctly.

The **show ip route** command is used to make sure that the static route is present in the routing table.

Trouble Shooting Static Route Configuration

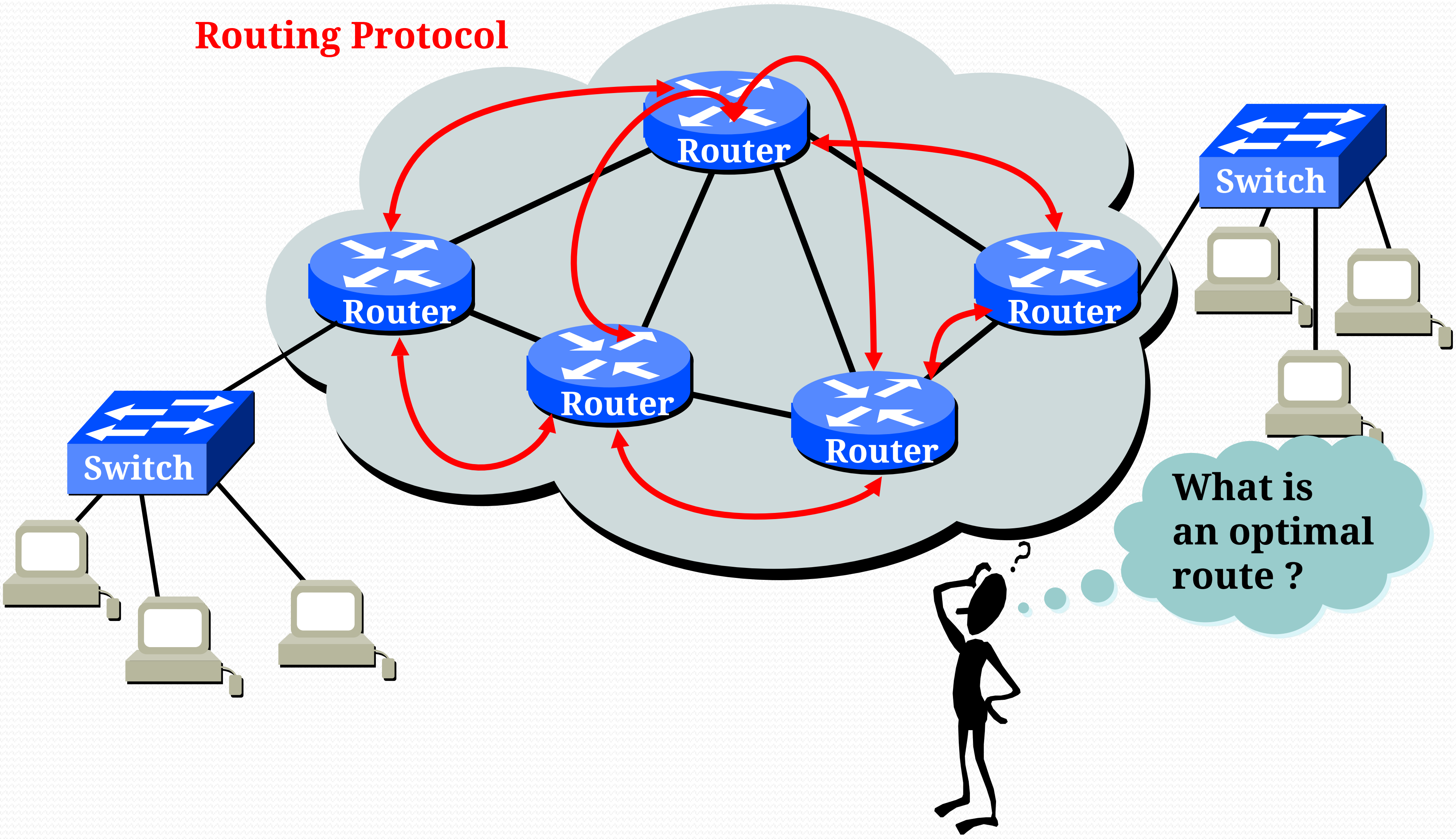
```
Sterling#ping 172.16.5.1
Type escape sequence to abort.
Sending 5,100-byte ICMP Echos to 172.16.5.1,timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
Sterling#traceroute 172.16.5.1
Type escape sequence to abort.
Tracing the route to 172.16.5.1
  1 172.16.2.2 16 msec 16 msec 16 msec
  2 172.16.4.2 32 msec 28 msec *
  3  *   *   *
  4  *   *   *
```

Path Determination Graphic



If computer A was sending data to computer F, what path would the data take? That is determined by the information in the routing table.

Routing Protocol



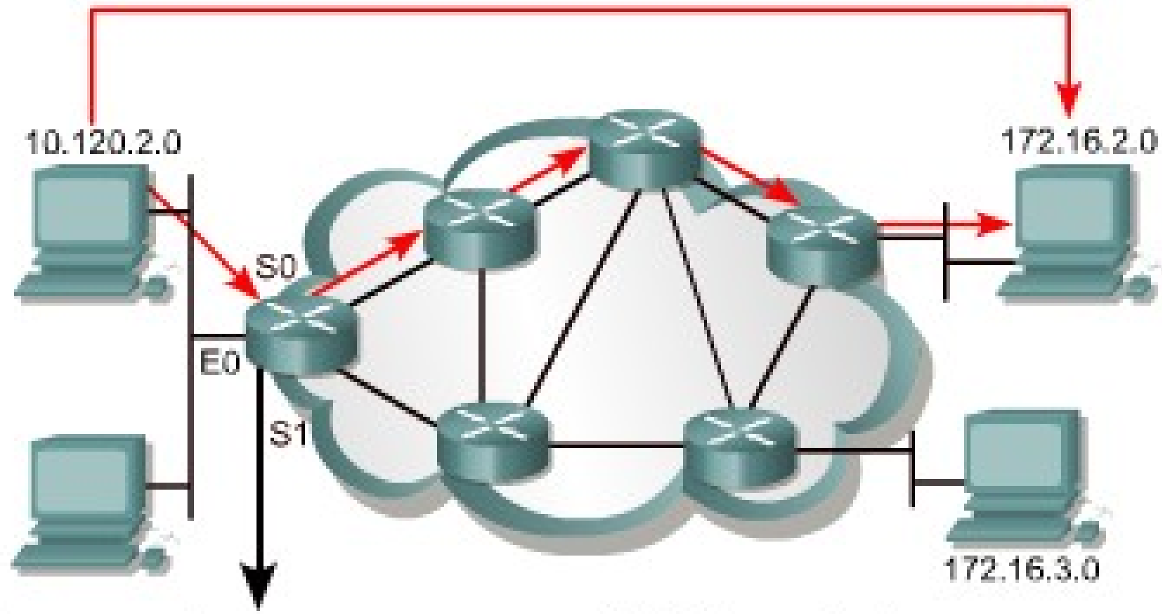
Routing Protocols

Routing protocols includes the following:

processes for sharing route information allows routers to communicate with other routers to update and maintain the routing tables

Examples of routing protocols that support the IP routed protocol are:

RIP, IGRP,
OSPF, BGP,
and EIGRP.

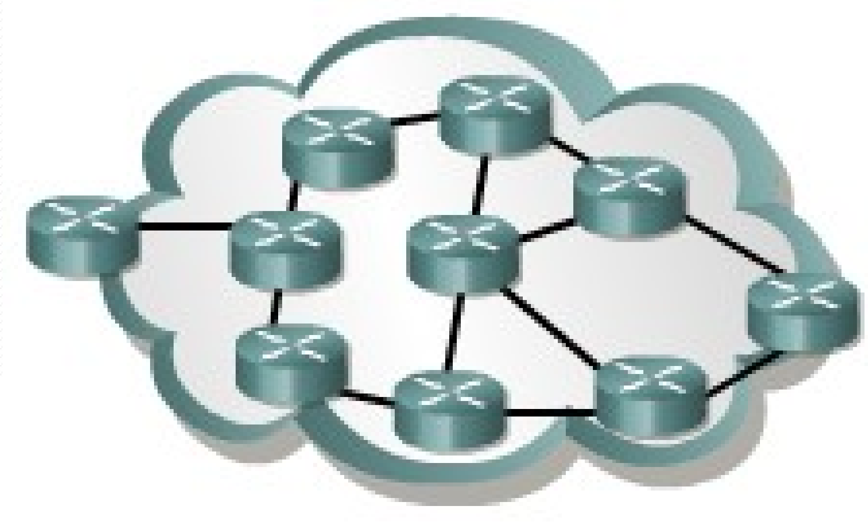


Network Protocol	Destination Network	Exit Interface
Connected	10.120.2.0	E0
RIP	172.16.2.0	S0
IGRP	172.16.3.0	S1

Routing protocols are used between routers to determine paths and maintaining routing tables

After the path is determined a router can route a routed protocol

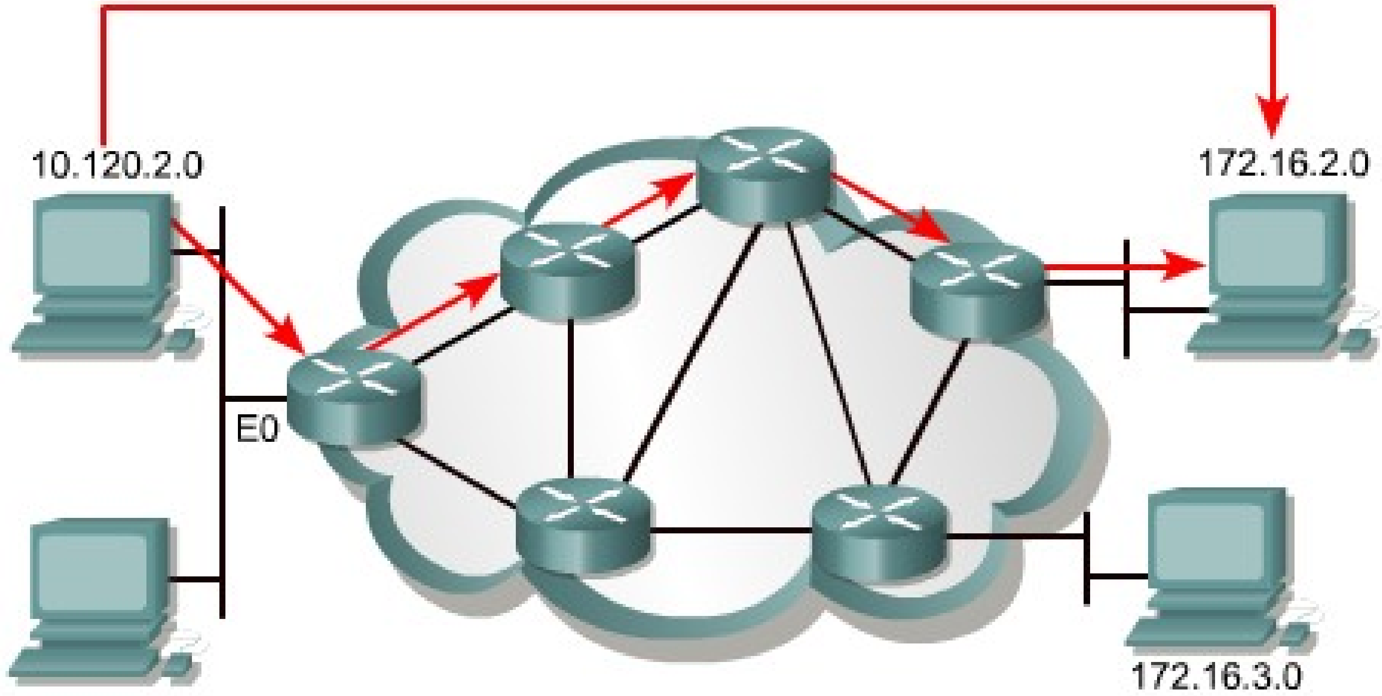
Routing Protocols



Routing protocol used between routers to maintain tables
Examples: RIP, IGRP, OSPF

Routed Protocols

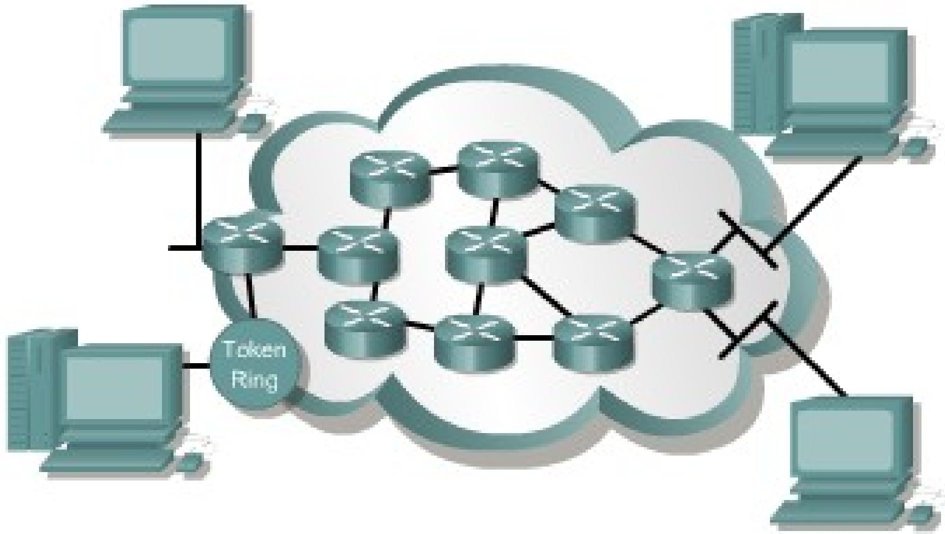
Protocols used at the network layer that transfer data from one host to another across a router are called routed or routable protocols. The Internet Protocol (IP) and Novell's Internetwork Packet Exchange (IPX) are examples of routed protocols. Routers use routing protocols to exchange routing tables and share routing information. In other words, routing protocols enable routers to route routed protocols.



Routed protocol transport data from one end-station to another.

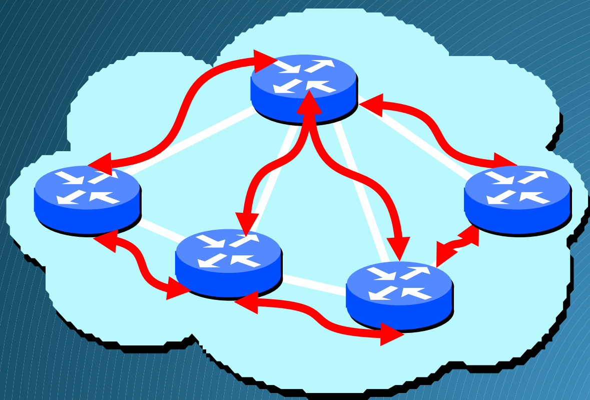
Routed Protocols

Routed protocol used between routers to direct user traffic
Examples: IP and IPX



Autonomous System

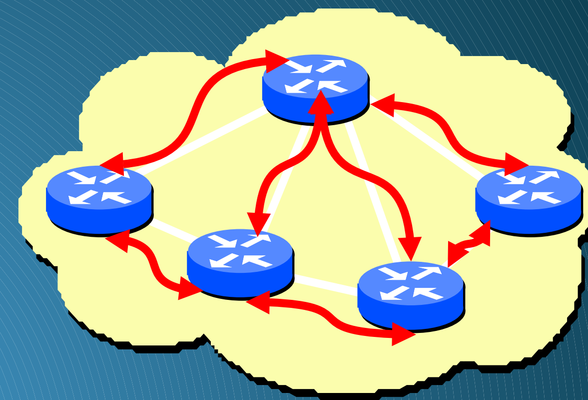
An Autonomous System (AS) is a group of IP networks, which has a single and clearly defined external routing policy.



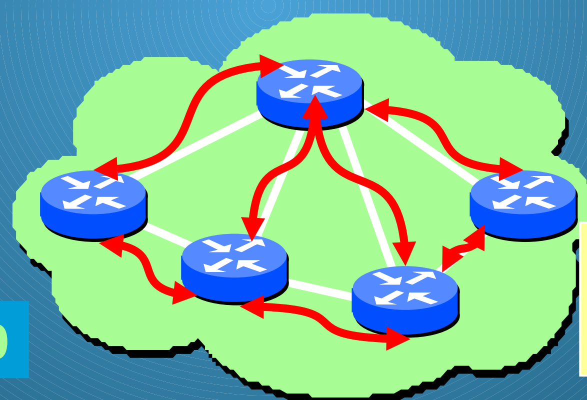
AS 1000

EGP

Exterior Gateway Protocols are used for routing between Autonomous Systems



AS 3000



AS 2000

IGP

Interior Gateway Protocols are used for routing decisions within an Autonomous System.

Fig. 48 IGP and EGP (TI1332EU02TI_0004 The Network Layer, 67)

Interior Gateway Protocol (IGP)

Exterior Gateway Protocol (EGP)

Interior Gateway Protocol (IGP)

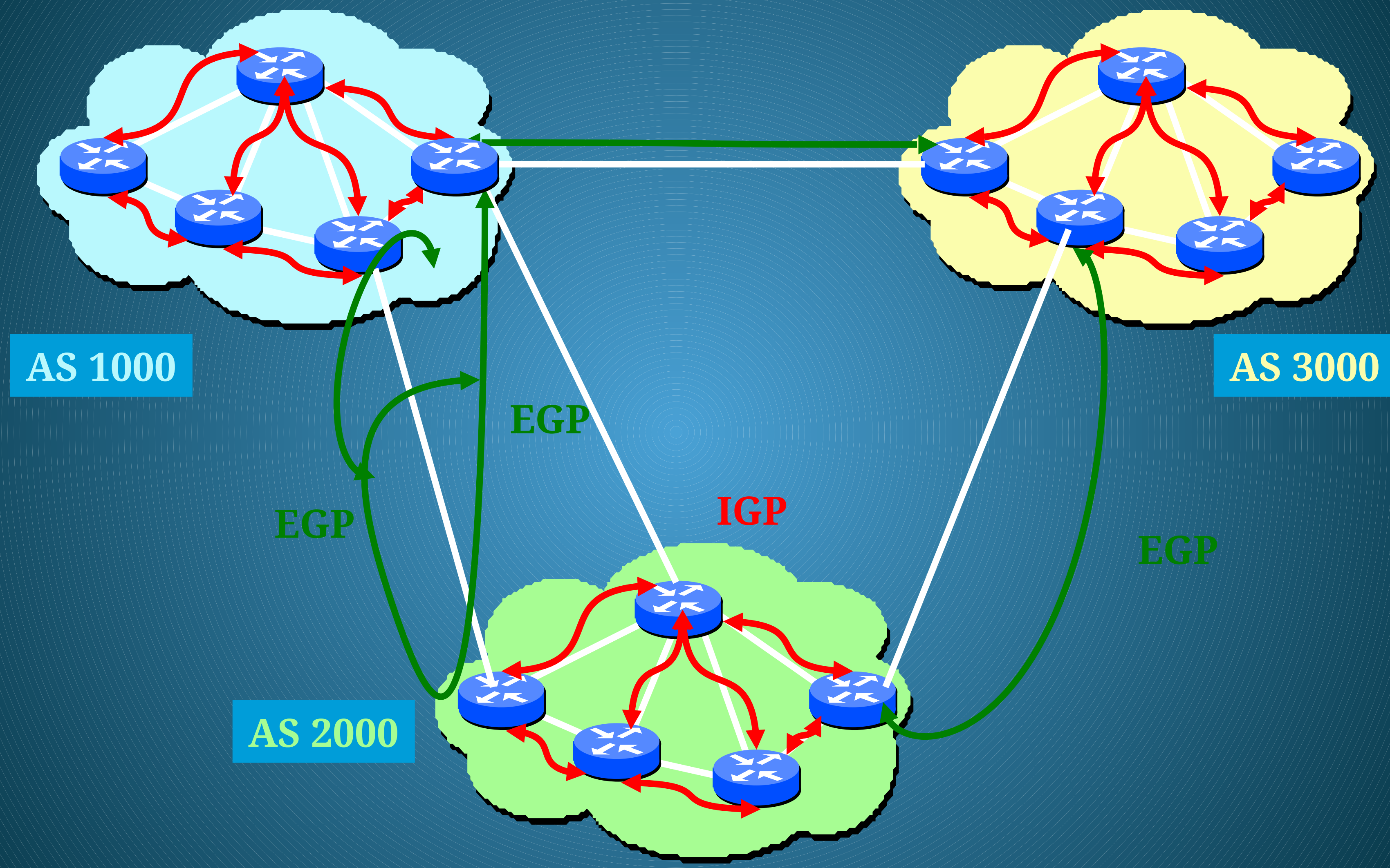
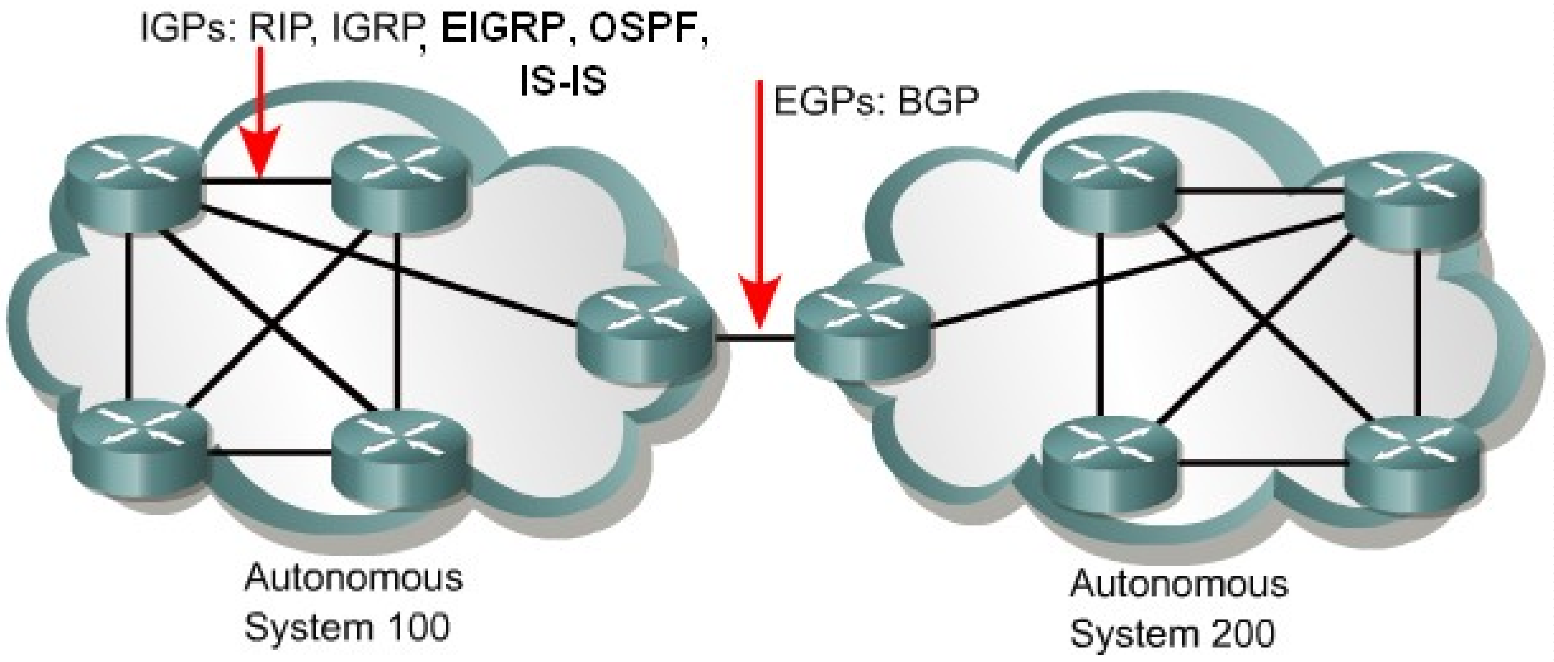


Fig. 49 The use of IGP and EGP protocols (TI1332EU02TI_0004 The Network Layer, 67)

IGP and EGP

An autonomous system is a network or set of networks under common administrative control, such as the cisco.com domain.



An autonomous system is a collection of networks under a common administrative domain. IGPs operate within an autonomous system. EGPs connect different autonomous system.

Categories of Routing Protocols

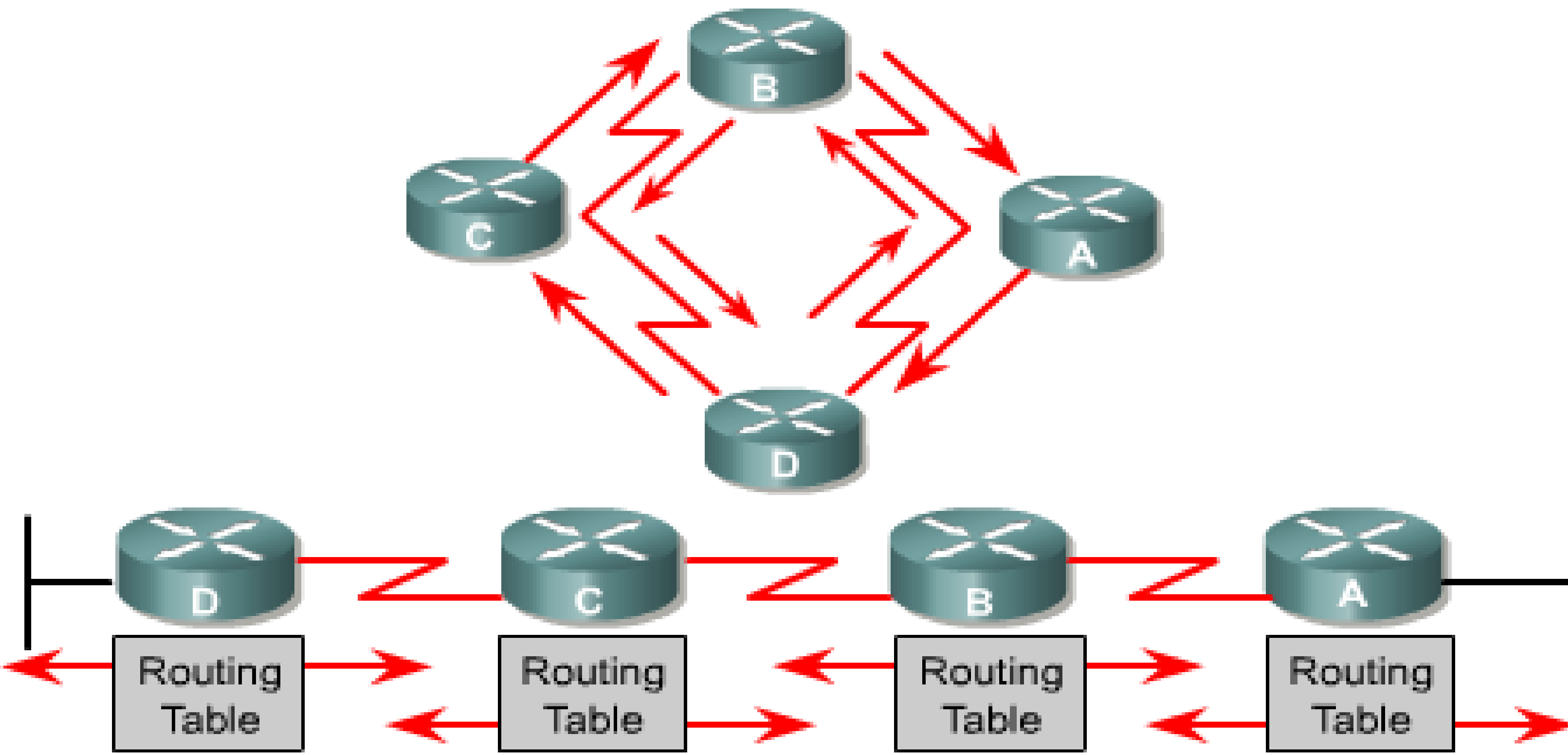
Most routing algorithms can be classified into one of two categories:

- distance vector
- link-state

The distance vector routing approach determines the direction (vector) and distance to any link in the internetwork.

The link-state approach, also called shortest path first, recreates the exact topology of the entire internetwork.

Distance Vector Routing Concepts

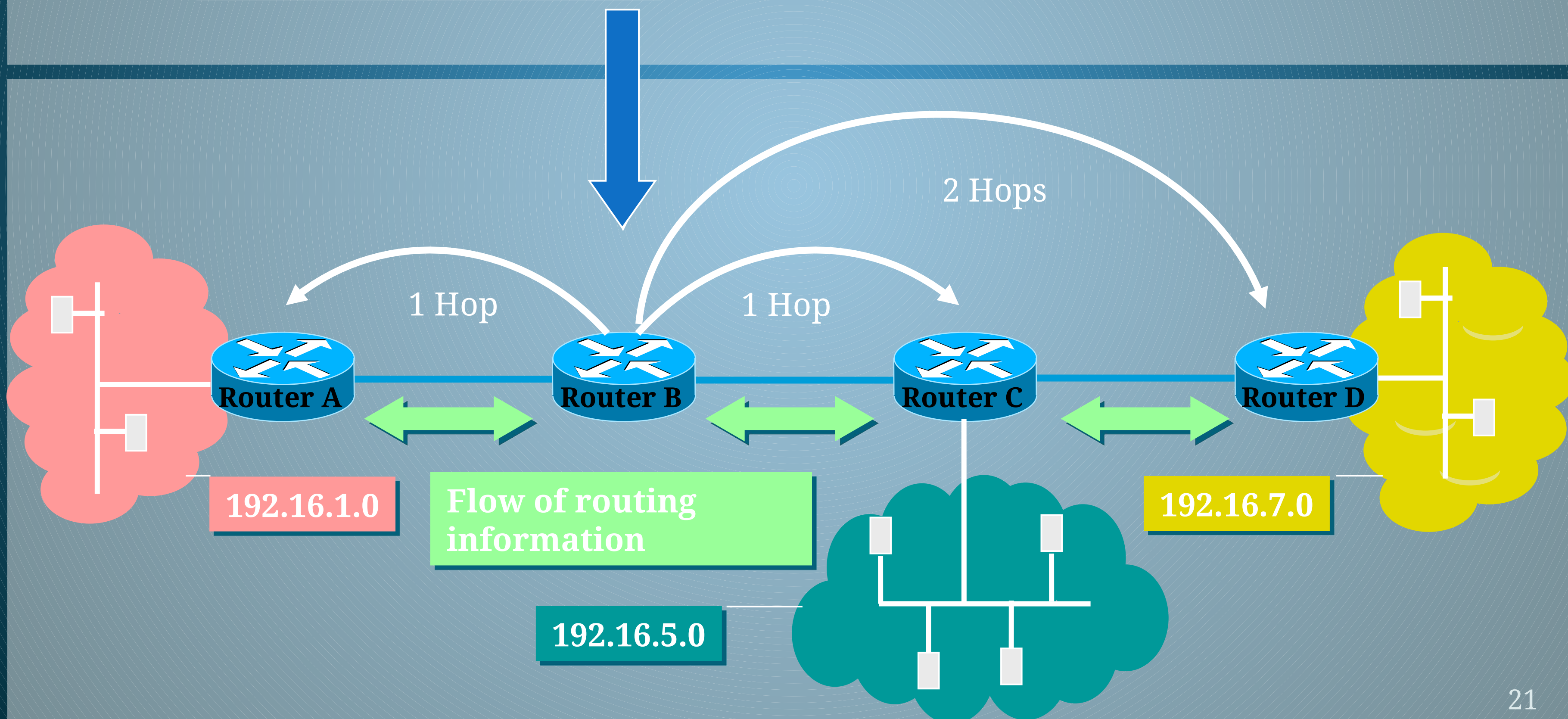


Pass periodic copies of a routing table to neighbor routers and accumulate distance vectors.

Distance Vector Routing (DVR)

Destination	Distance
192.16.1.0	1
192.16.5.0	1
192.16.7.0	2

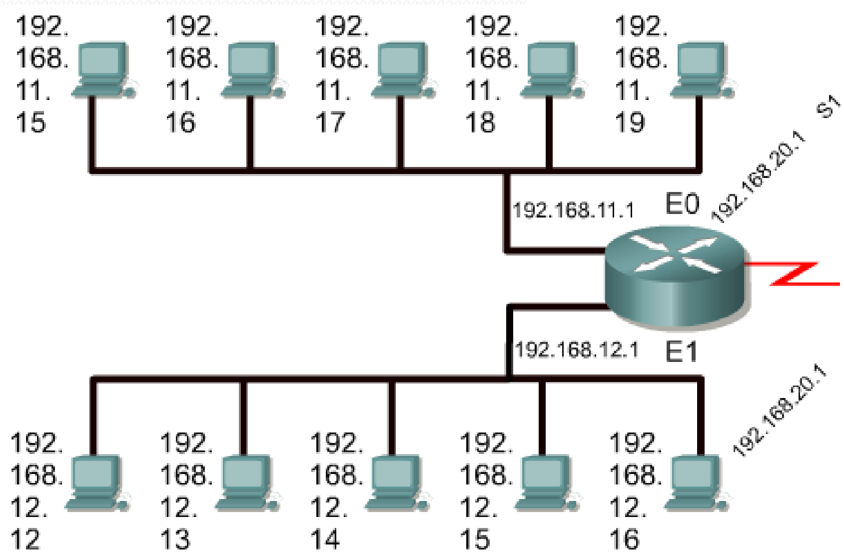
Routing table contains the addresses of destinations and the distance of the way to this destination.



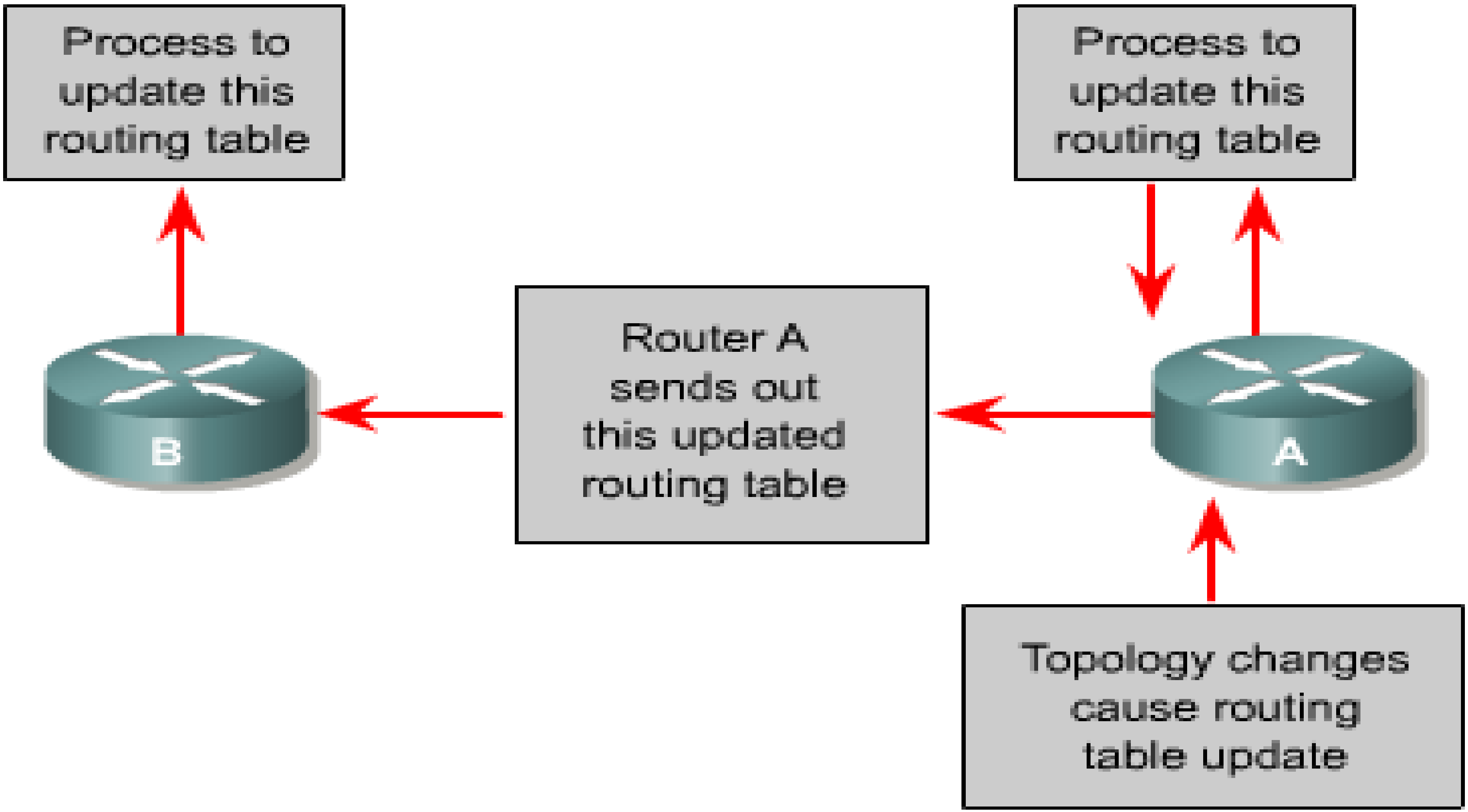
Routing Tables Graphic

Routing Table

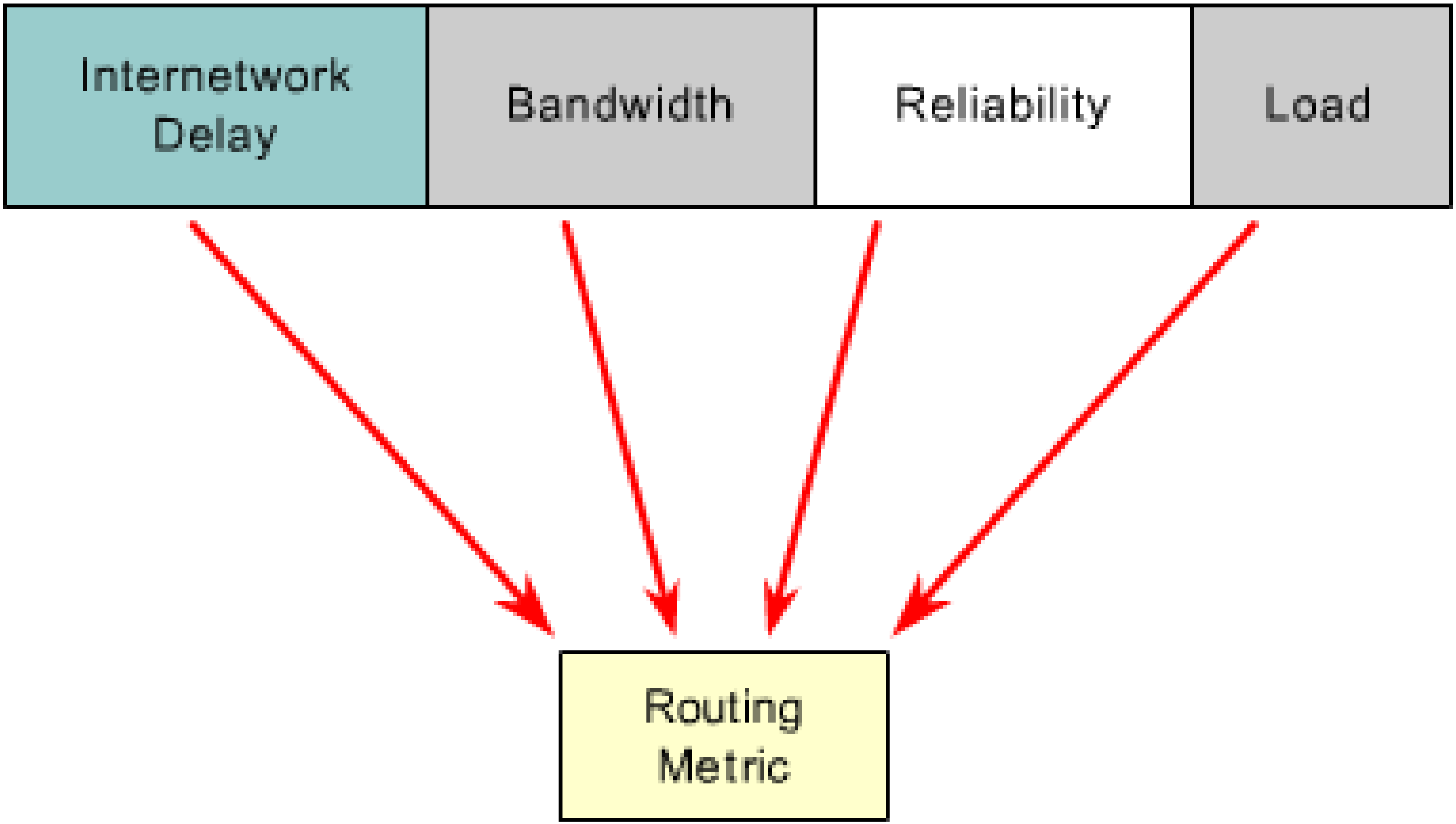
Learned		Network Address	Hop	Interface
C	-	192.168.11.0	0	E0
C	-	192.168.12.0	0	E1
C	-	192.168.20.0	0	S0
R	-	192.168.21.0	1	S0
R	-	192.168.22.0	1	S0



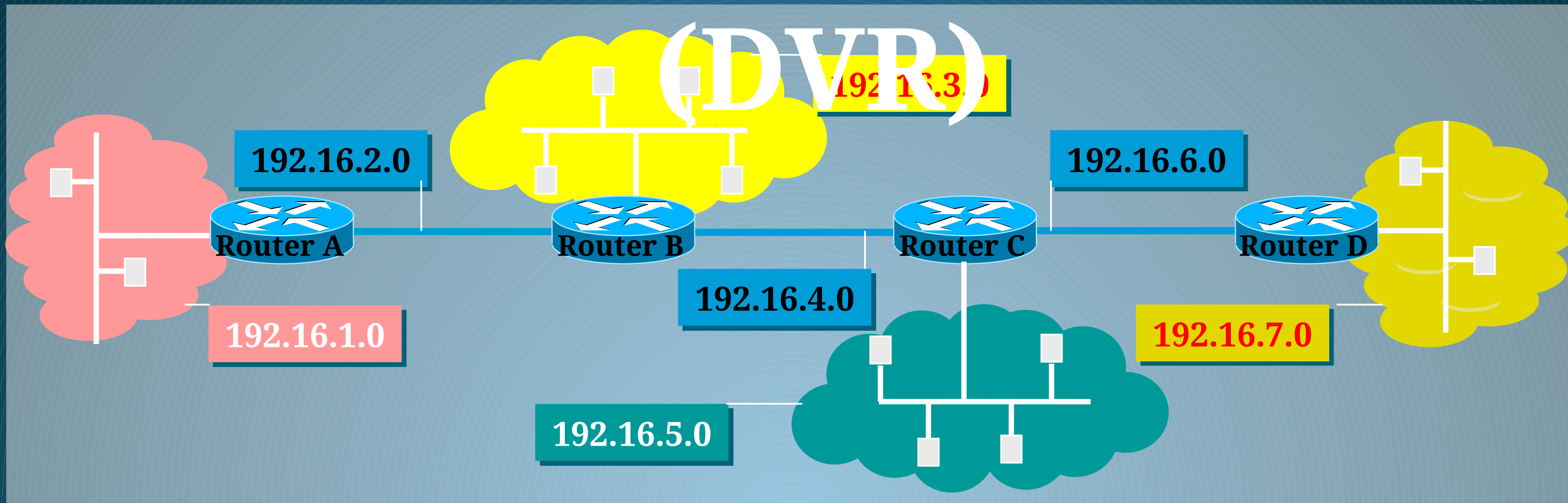
Distance Vector Topology Changes

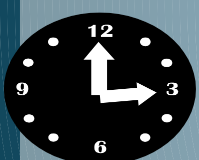


Router Metric Components

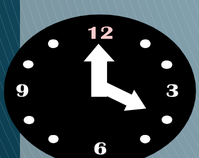


Distance Vector Routing (DVR)





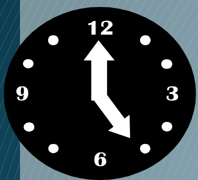
Router A			Router B			Router C			Router D		
192.16.1.0	0	L	192.16.2.0	0	L	192.16.4.0	0	L	192.16.6.0	0	L
192.16.2.0	0	L	192.16.3.0	0	L	192.16.5.0	0	L	192.16.7.0	0	L
			192.16.4.0	0	L	192.16.6.0	0	L			



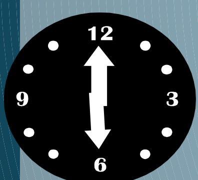
Router A			Router B			Router C			Router D		
192.16.1.0	0	L	192.16.2.0	0	L	192.16.4.0	0	L	192.16.6.0	0	L
192.16.2.0	0	L	192.16.3.0	0	L	192.16.5.0	0	L	192.16.7.0	0	L
192.16.3.0	1	B	192.16.4.0	0	L	192.16.6.0	0	L	192.16.5.0	1	C
192.16.4.0	1	B	192.16.1.0	1	A	192.16.3.0	1	B	192.16.4.0	1	C
			192.16.5.0	1	C	192.16.2.0	1	B			
			192.16.6.0	1	C	192.16.7.0	1	D			

L Locally connected

Distance Vector Routing (DVR)



192.16.1.0	0	L	192.16.2.0	0	L	192.16.4.0	0	L	192.16.6.0	0	L
192.16.2.0	0	L	192.16.3.0	0	L	192.16.5.0	0	L	192.16.7.0	0	L
192.16.3.0	1	B	192.16.4.0	0	L	192.16.6.0	0	L	192.16.5.0	1	C
192.16.4.0	1	B	192.16.1.0	1	A	192.16.3.0	1	B	192.16.4.0	1	C
192.16.5.0	2	B	192.16.5.0	1	C	192.16.2.0	1	B	192.16.3.0	2	C
192.16.6.0	2	B	192.16.6.0	1	C	192.16.7.0	1	D	192.16.2.0	2	C
			192.16.7.0	2	C	192.16.1.0	2	B			



192.16.1.0	0	L	192.16.2.0	0	L	192.16.4.0	0	L	192.16.6.0	0	L
192.16.2.0	0	L	192.16.3.0	0	L	192.16.5.0	0	L	192.16.7.0	0	L
192.16.3.0	1	B	192.16.4.0	0	L	192.16.6.0	0	L	192.16.5.0	1	C
192.16.4.0	1	B	192.16.1.0	1	A	192.16.3.0	1	B	192.16.4.0	1	C
192.16.5.0	2	B	192.16.5.0	1	C	192.16.2.0	1	B	192.16.3.0	2	C
192.16.6.0	2	B	192.16.6.0	1	C	192.16.7.0	1	D	192.16.2.0	2	C
192.16.7.0	3	B	192.16.7.0	2	C	192.16.1.0	2	B	192.16.1.0	3	C

Fig. 53 Distribution of routing information with distance vector routing protocol (cont.) (TI1332EU02TI_0004 The Network Layer, 71)

RIPv1

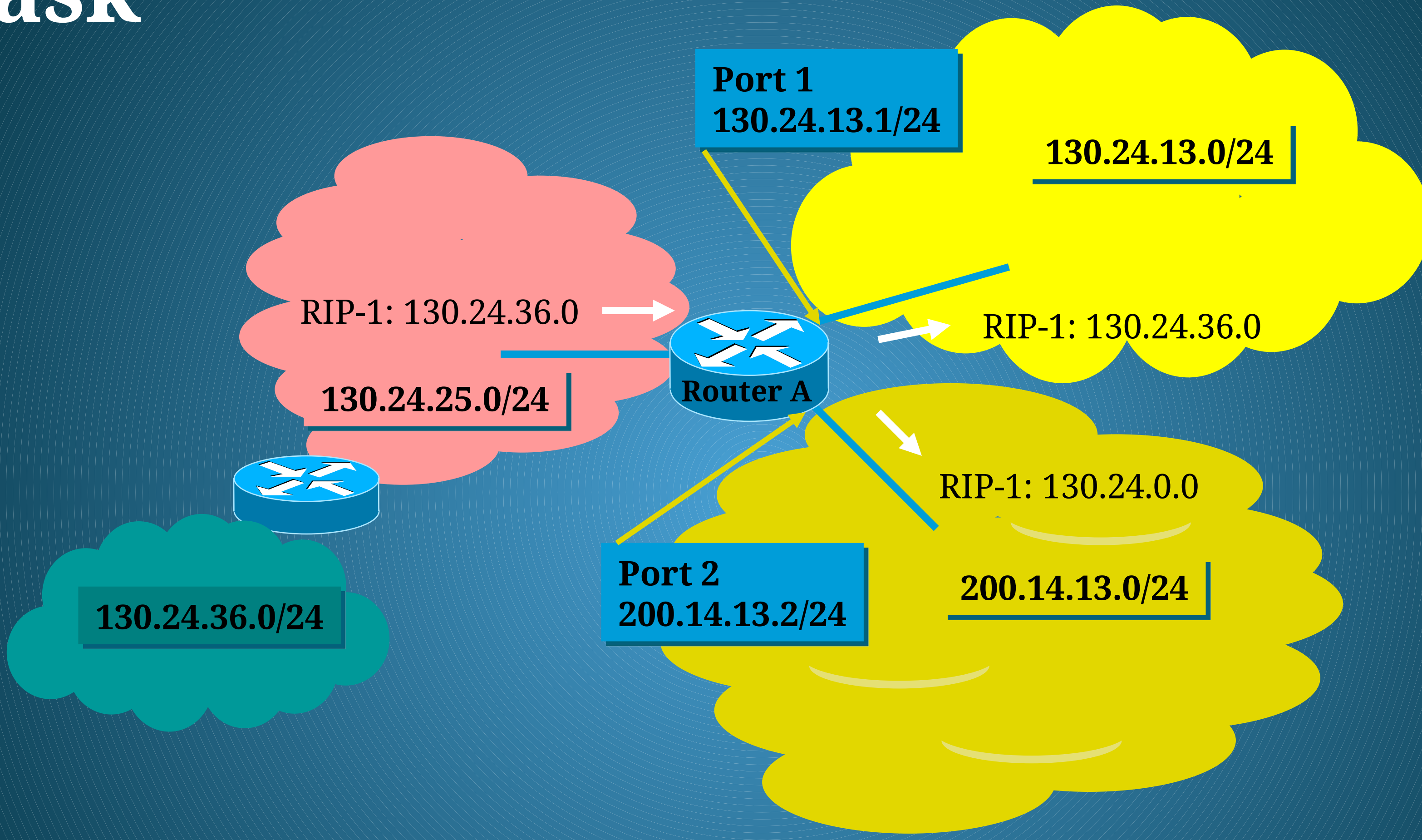
- Distance Vector Routing Protocol,
  classful
- Distribution of Routing Tables via broadcast
  to adjacent routers
- Only one kind of metric:
  Number of Hops
- Connections with different
  bandwidth can not be weighted
- Routing loops can occur
  -> bad convergence in case of a failure
- Count to infinity problem
  (infinity = 16)
- Maximum network size is limited
  by the number of hops

RIP Characteristics

The key characteristics of RIP include the following:

- It is a distance vector routing protocol.
- Hop count is used as the metric for path selection.
- If the hop count is greater than 15, the packet will be discarded.
- By default, routing updates are broadcast every 30 seconds.

RIP-1 permits only a Single Subnet Mask



Router Configuration

The **router** command starts a routing process.

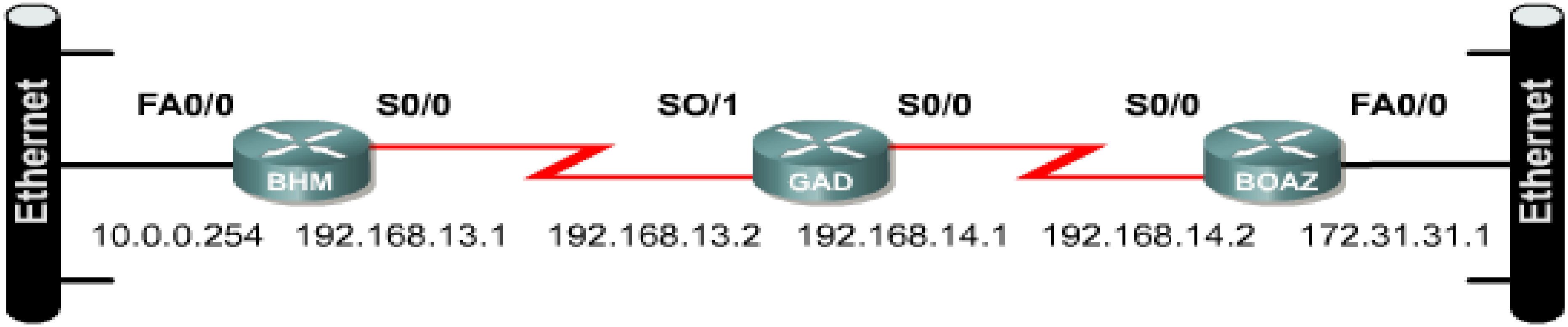
The **network** command is required because it enables the routing process to determine which interfaces participate in the sending and receiving of routing updates.

An example of a routing configuration is:

```
GAD(config)#router rip
GAD(config-router)#network 172.16.0.0
```

The network numbers are based on the network class addresses, not subnet addresses or individual host addresses.

Configuring RIP Example




```
BHM(config)#router rip
BHM(config-router)#network 10.0.0.0
BHM(config-router)#network 192.168.13.0
```

```
GAD(config)#router rip
GAD(config-router)#network 192.168.14.0
GAD(config-router)#network 192.168.13.0
```

```
BOAZ(config)#router rip
BOAZ(config-router)#network 192.168.14.0
BOAZ(config-router)#network 172.31.0.0
```

Verifying RIP Configuration

```
GAD#show ip protocols
Routing Protocol is "rip"
    Sending updates every 30 seconds, next due in 5
seconds
    Invalid after 180 seconds, hold down 180, flushed
after 240
    Outgoing update filter list for all interfaces is
    Incoming update filter list for all interfaces is
    Redistributing: Rip
    Default version control: send version 1, receive any
version
    Interface             Send     Recv      Triggered RIP    Key-chain
    FastEthernet0/0        1       1 2
    Serial0/0              1       1 2
  Routing for Networks:
    192.168.1.0
    192.168.2.0
  Routing Information Sources:
    Gateway                Distance                   Last Update
    192.168.2.2              120                        00:00:11
   Distance:  (default is 120)
```

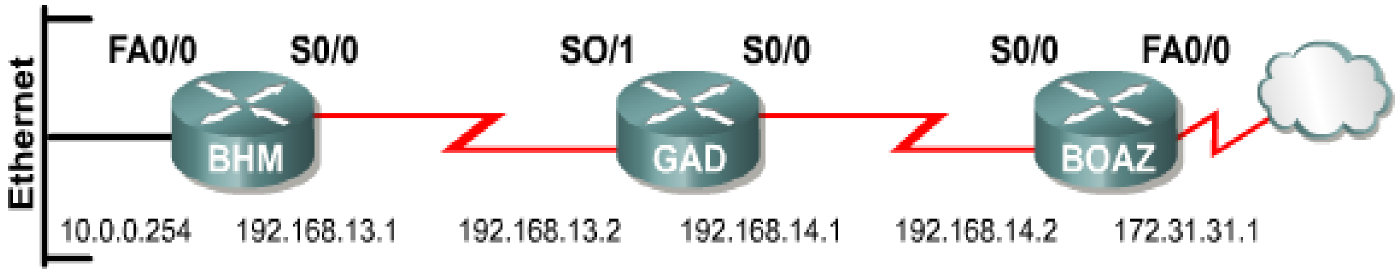
Verify RIP is Configured

Verify networks being advertised

Verify RIP interface

The debug ip rip Command

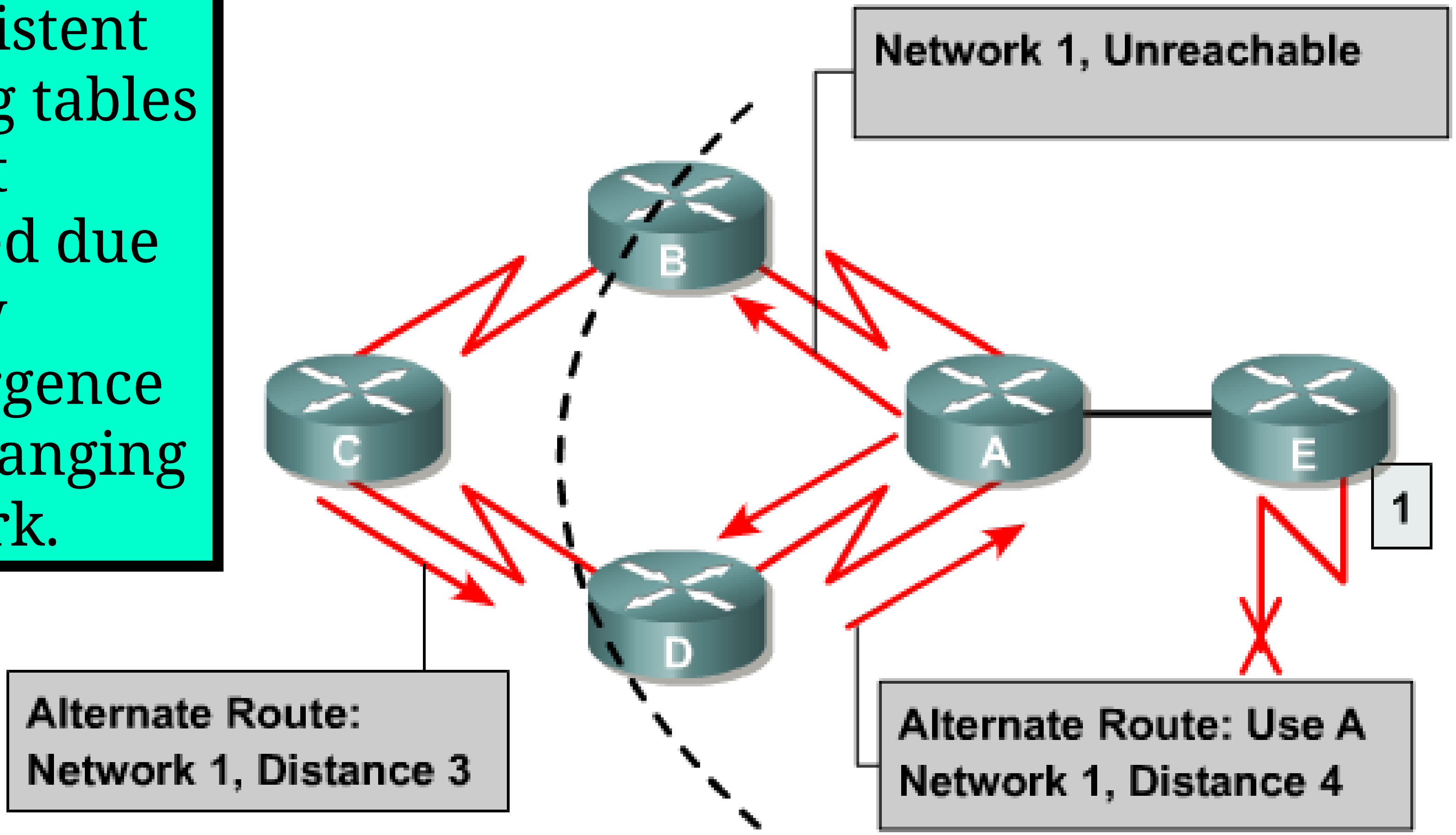
Most of the RIP configuration errors involve an incorrect network statement, discontiguous subnets, or split horizons. One highly effective command for finding RIP update issues is the **debug ip rip** command. The **debug ip rip** command displays RIP routing updates as they are sent and received.




```
BHM#debug ip rip
RIP event debugging is on
BHM#
00:45:33: RIP: received v1 update from 192.168.13.2
on Serial0/0
00:45:33:        192.168.14.0 in 1 hop
00:45:33:        172.31.0.0 in 2 hop
00:45:33:        172.29.0.0 15 hops
00:45:36: RIP: sending v1 update to 255.255.255.255
via Serial0/0 (192.168.13.1)
00:45:36:         network 10.0.0.0. metric 1
00:45:36: RIP: sending v1 update to 255.255.255.255
via FastEthernet0/0 (10.0.0.254)
00:45:36:          network 192.168.13.0. metric 1
00:45:36:          network 192.168.14.0. metric 2
00:45:36:          network 172.31.0.0. metric 3
00:45:36:          network 172.29.0.0. metric 16
```

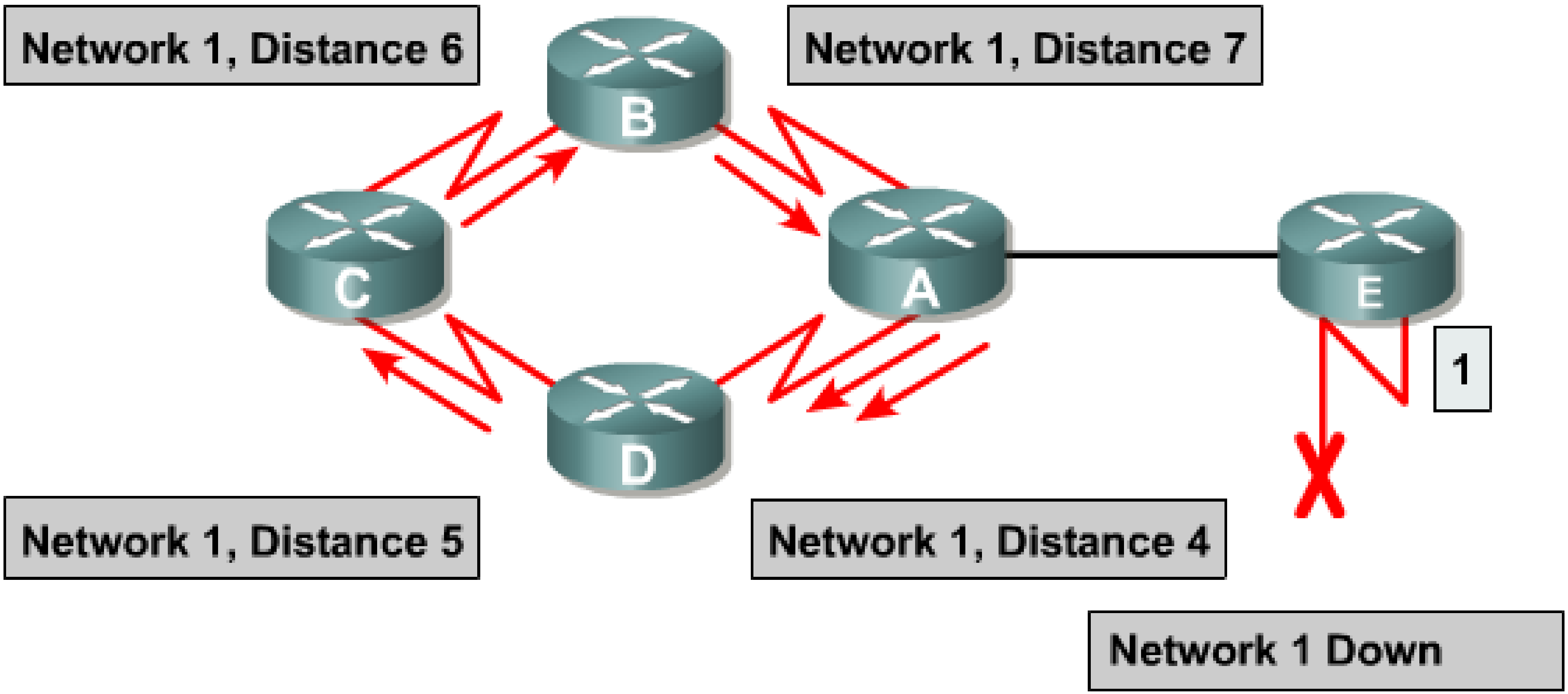
Routing loops can occur when inconsistent routing tables are not updated due to slow convergence in a changing network.

Problem: Routing Loops



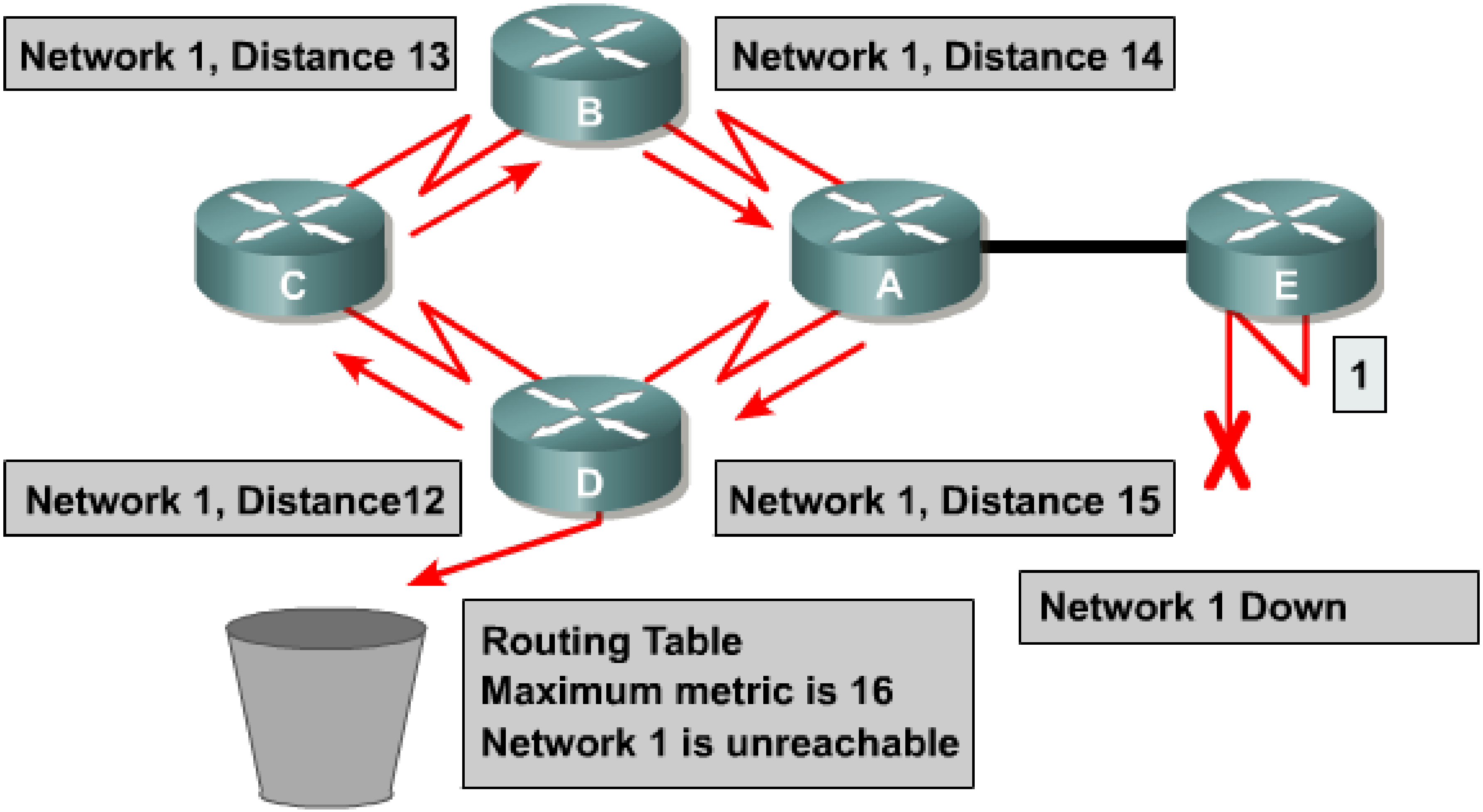
Alternate routes, slow convergence, inconsistent routing

Problem: Counting to Infinity



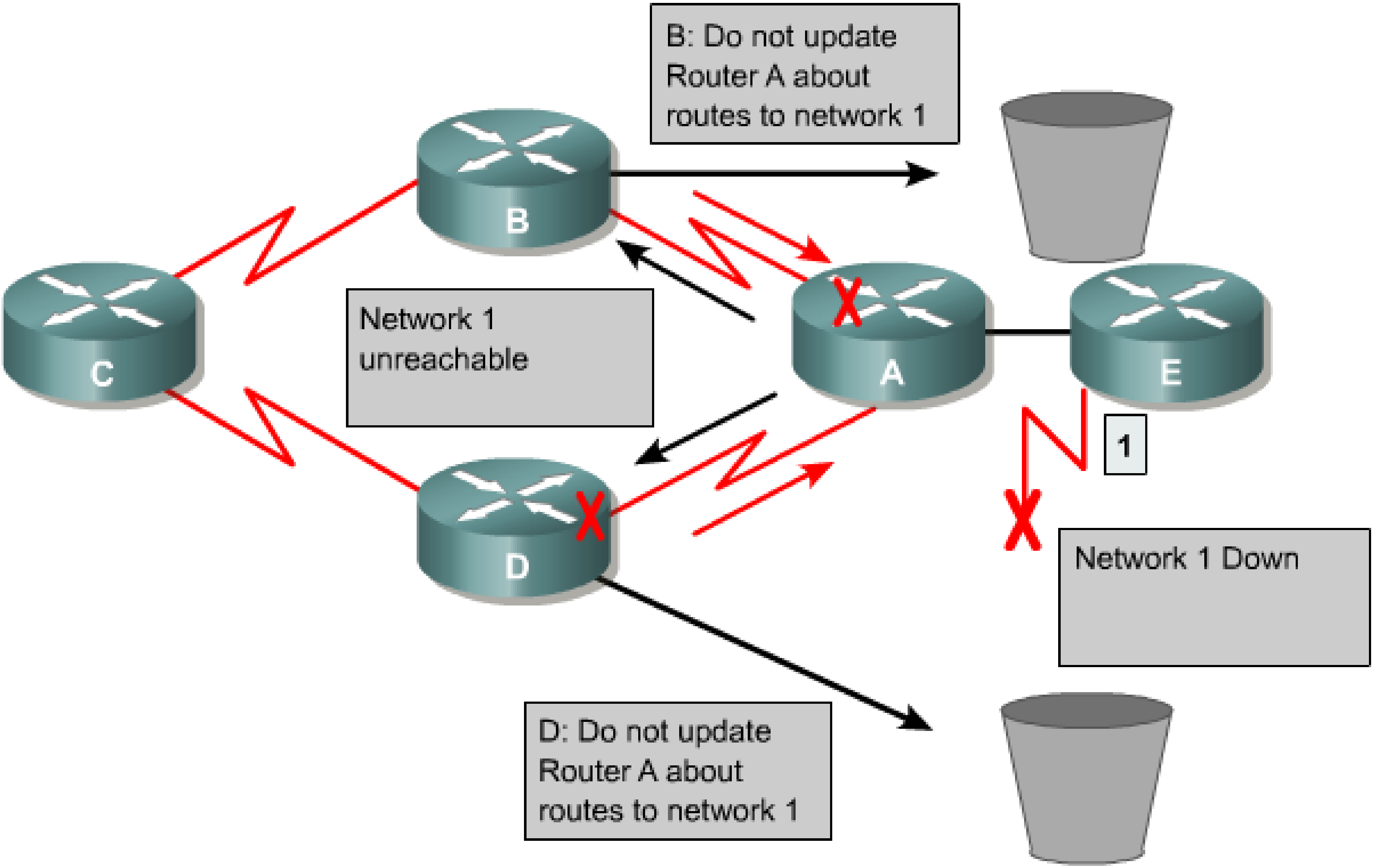
Routing loops increment the distance vector

Solution: Define a Maximum



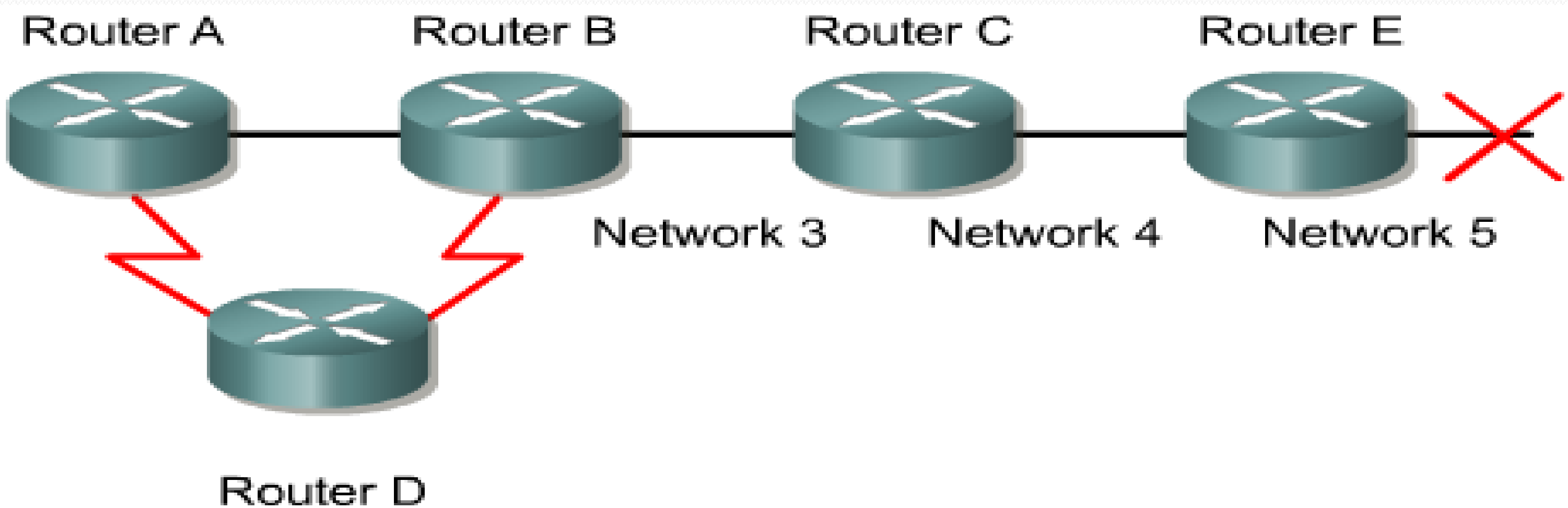
Specify a maximum distance vector metric as infinity

Solution: Split Horizon



Route Poisoning

Route poisoning is used by various distance vector protocols in order to overcome large routing loops and offer explicit information when a subnet or network is not accessible. This is usually accomplished by setting the hop count to one more than the maximum.



When Network 5 goes down, Router E initiates route poisoning by entering a table entry metric of 16 (unreachable).

Triggered Updates

New routing tables are sent to neighboring routers on a regular basis.

For example, RIP updates occur every 30 seconds.

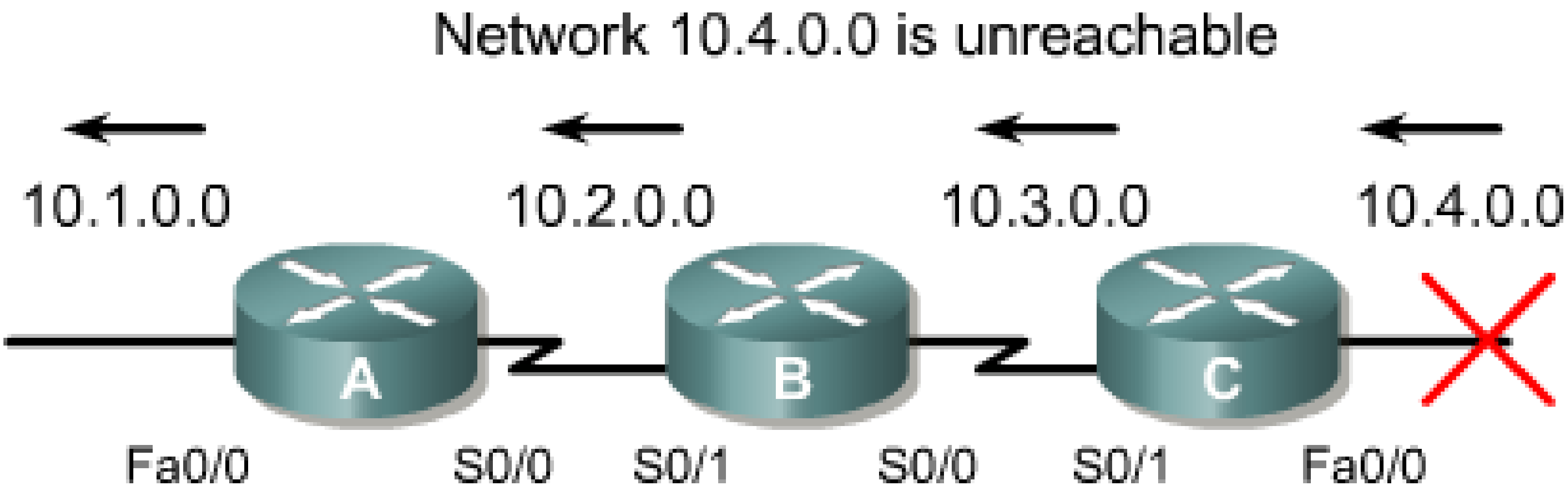
However a triggered update is sent immediately in response to some change in the routing table.

The router that detects a topology change immediately sends an update message to adjacent routers that, in turn, generate triggered updates notifying their adjacent neighbors of the change.

When a route fails, an update is sent immediately rather than waiting on the update timer to expire.

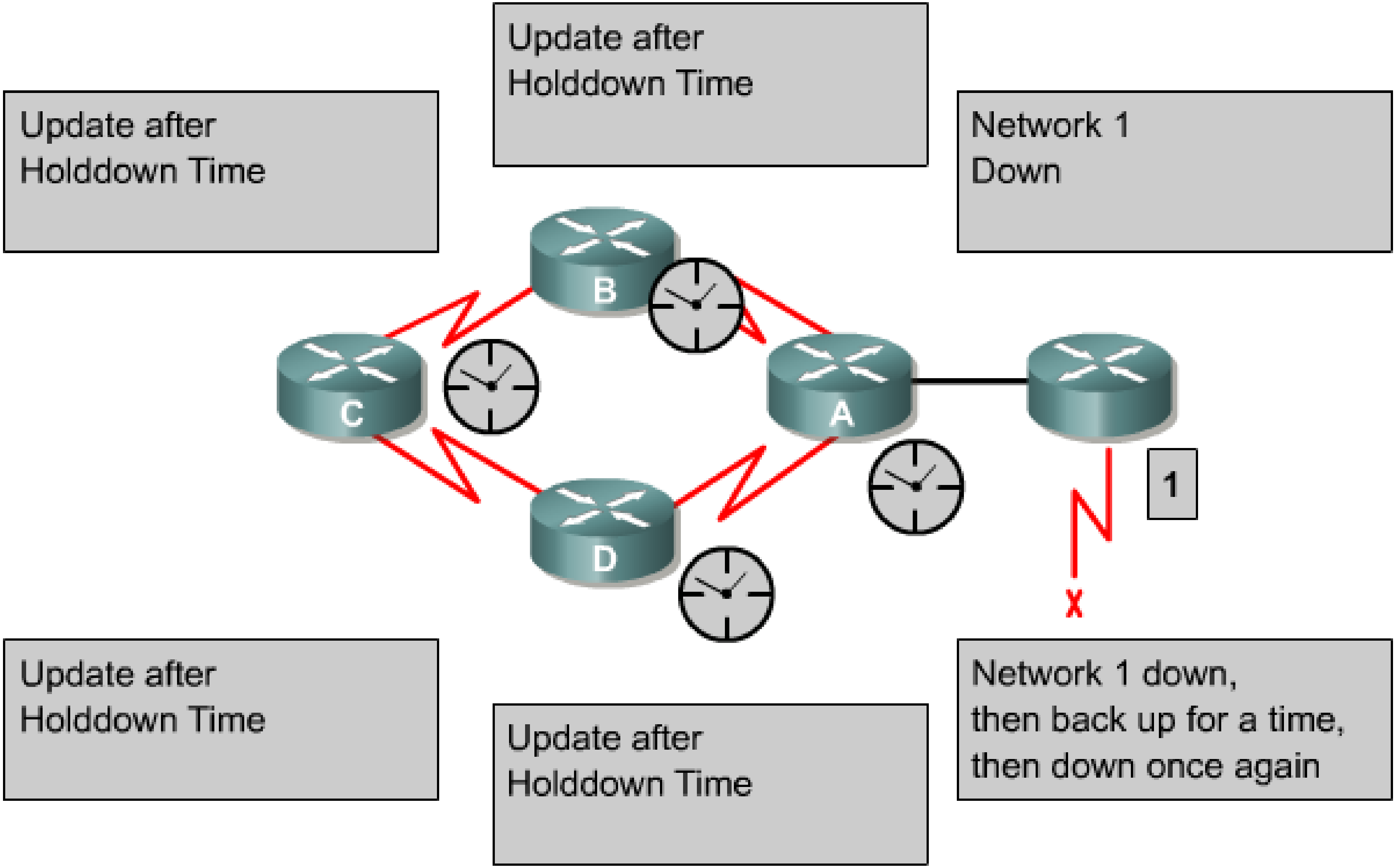
Triggered updates, used in conjunction with route poisoning, ensure that all routers know of failed routes before any holddown timers can expire.

Triggered Updates Graphic



With the triggered update approach, routers send messages as soon as they notice a change in their routing table.

Solution: Holddown Timers



IGRP

Interior Gateway Routing Protocol (IGRP) is a proprietary protocol developed by Cisco.

Some of the IGRP key design characteristics emphasize the following:

- It is a distance vector routing protocol.
- Routing updates are broadcast every 90 seconds.
- Bandwidth, load, delay and reliability are used to create a composite metric.

IGRP Stability Features

IGRP has a number of features that are designed to enhance its stability, such as:

- Holddowns
- Split horizons
- Poison reverse updates

Holddowns

Holddowns are used to prevent regular update messages from inappropriately reinstating a route that may not be up.

Split horizons

Split horizons are derived from the premise that it is usually not useful to send information about a route back in the direction from which it came.

Poison reverse updates

Split horizons prevent routing loops between adjacent routers, but poison reverse updates are necessary to defeat larger routing loops.

Today, IGRP is showing its age, it lacks support for variable length subnet masks (VLSM). Rather than develop an IGRP version 2 to correct this problem, Cisco has built upon IGRP's legacy of success with Enhanced IGRP.

Configuring IGRP

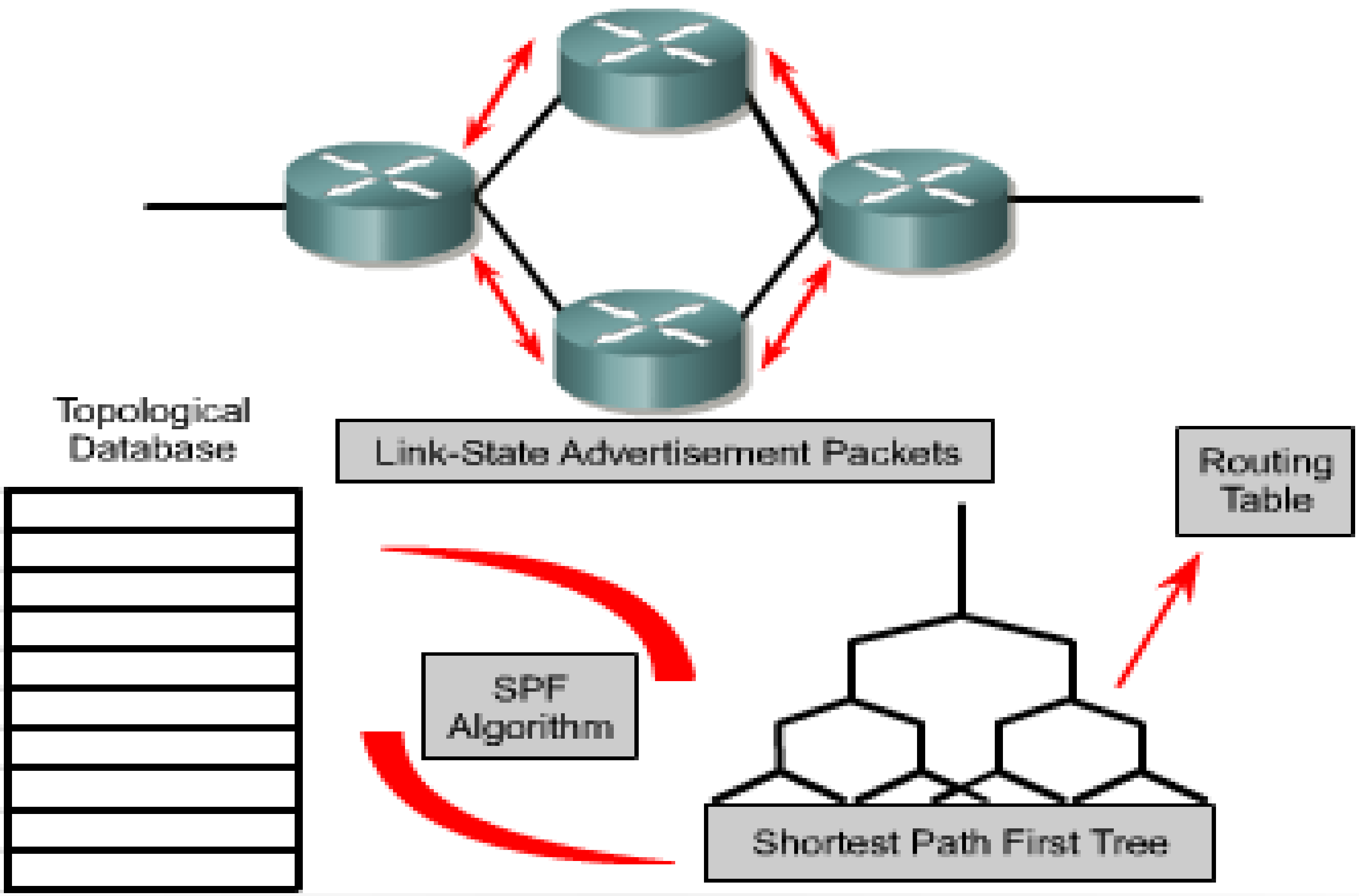
```
RouterA(config)#router igrp 101
RouterA(config-router)#network 192.168.1.0
RouterA(config-router)#network 192.168.2.0

RouterB(config)#router igrp 101
RouterB(config-router)#network 192.168.2.0
RouterB(config-router)#network 192.168.3.0
```

Routing Metrics Graphics

Protocol	Metric	Maximum number of routers	Origins
RIP	Hop count	15	Xerox
IGRP	• Bandwidth • Load • Delay • Reliability	255	Cisco

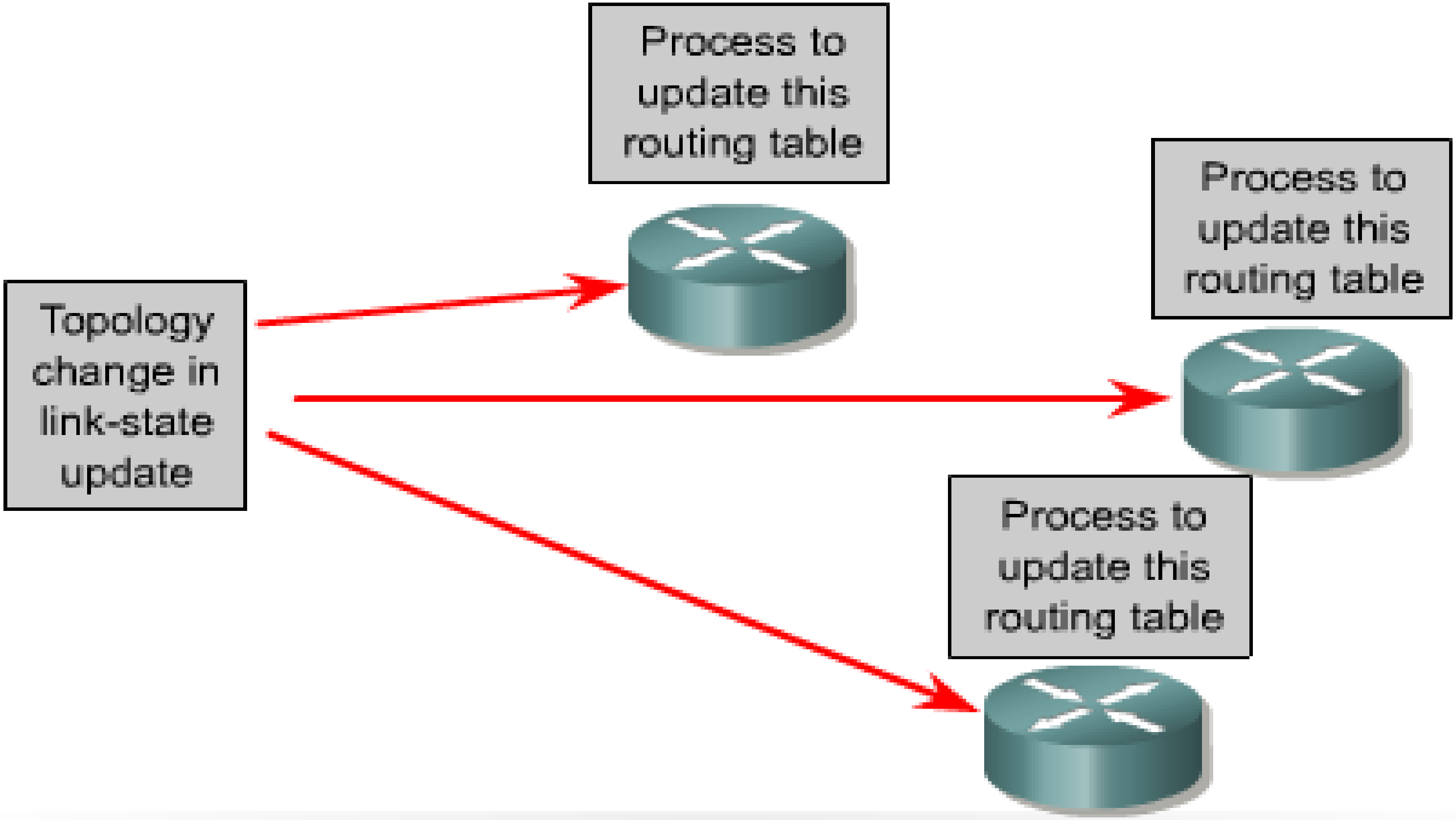
Routing metrics are the values used to determine the best path to the next hop.

Link State Concepts



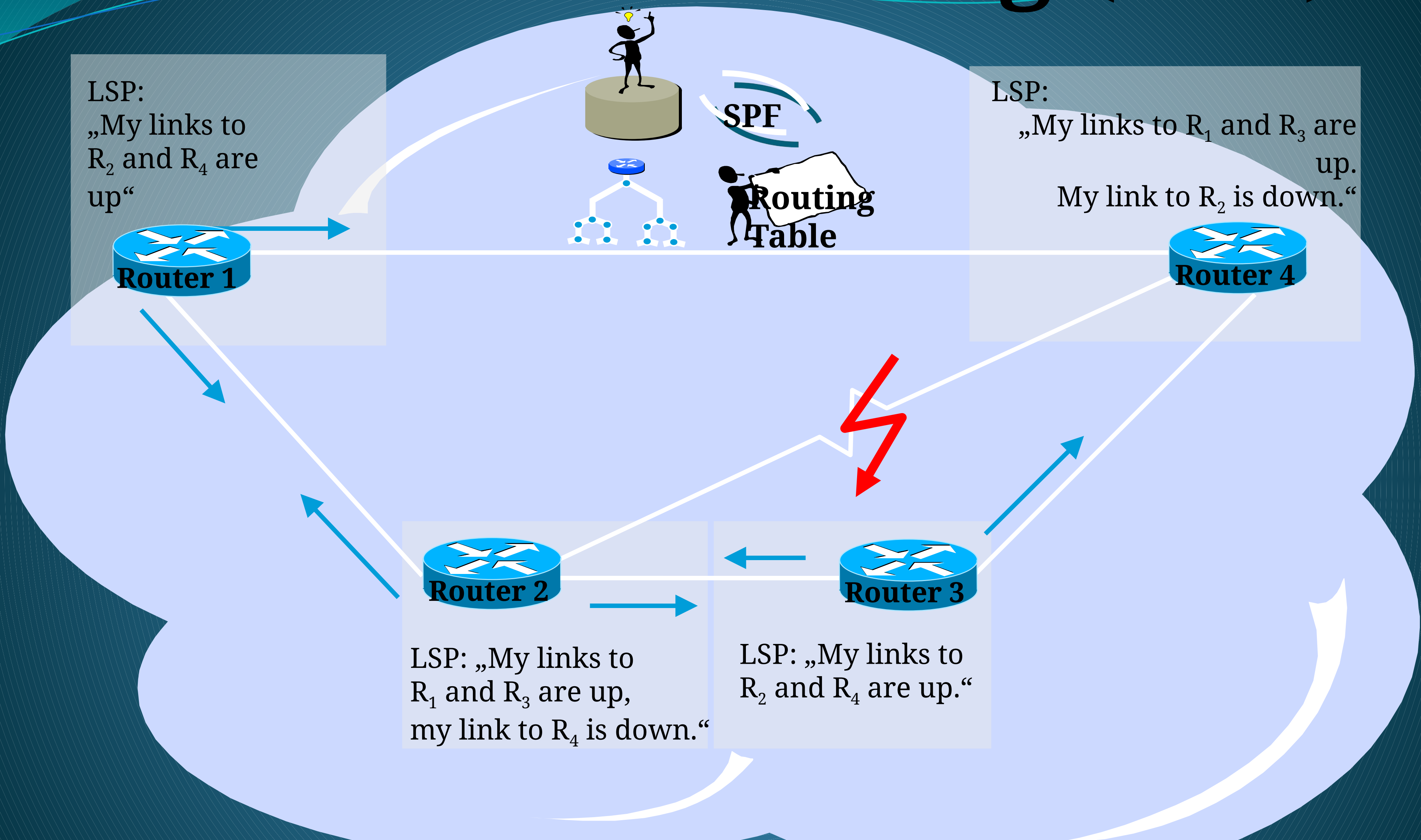
Routers send LSAs to their neighbors. The LSAs are used to build a topological database. The SPF algorithm is used to calculate the shortest path first tree in which the root is the individual router and then a routing table is created.

Link State Topology Changes



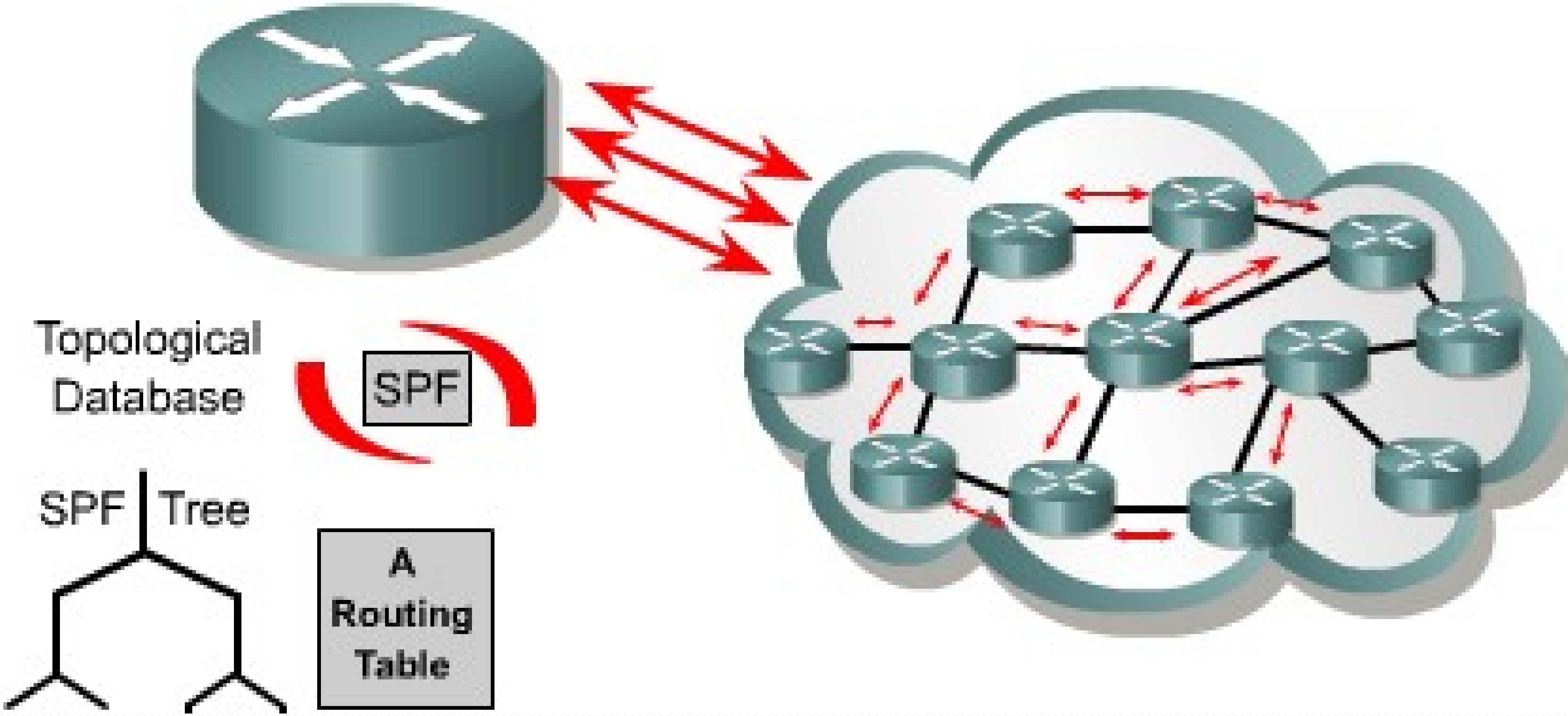
Each router has its own topological database on which the SPF algorithm is run.

Link State Routing (LSR)



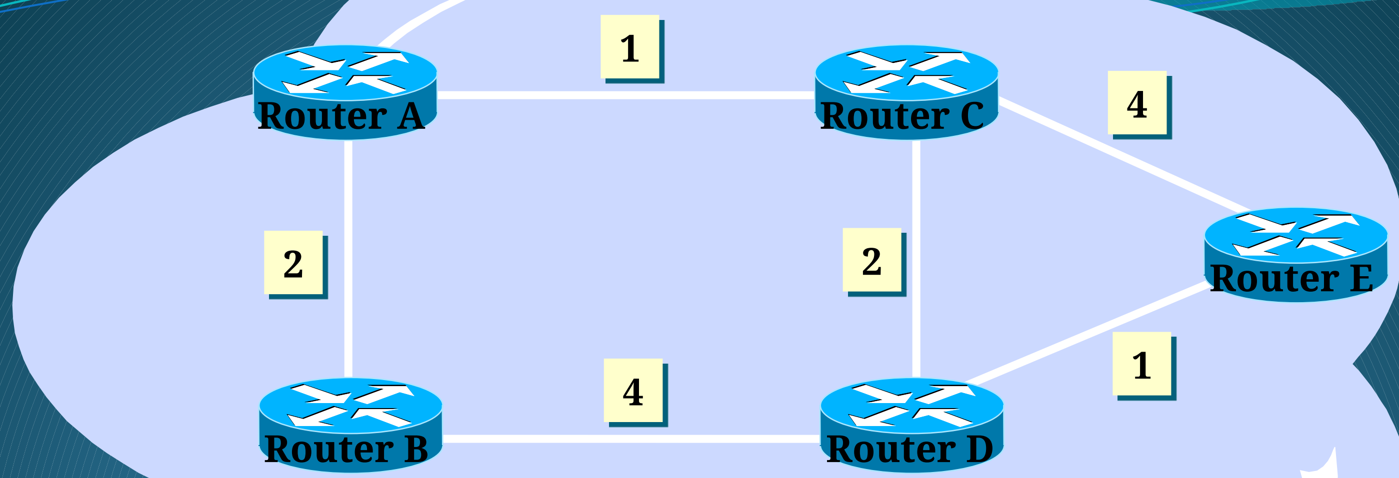
LSP....link state packet
SPF... shortest path first

Link State Concerns



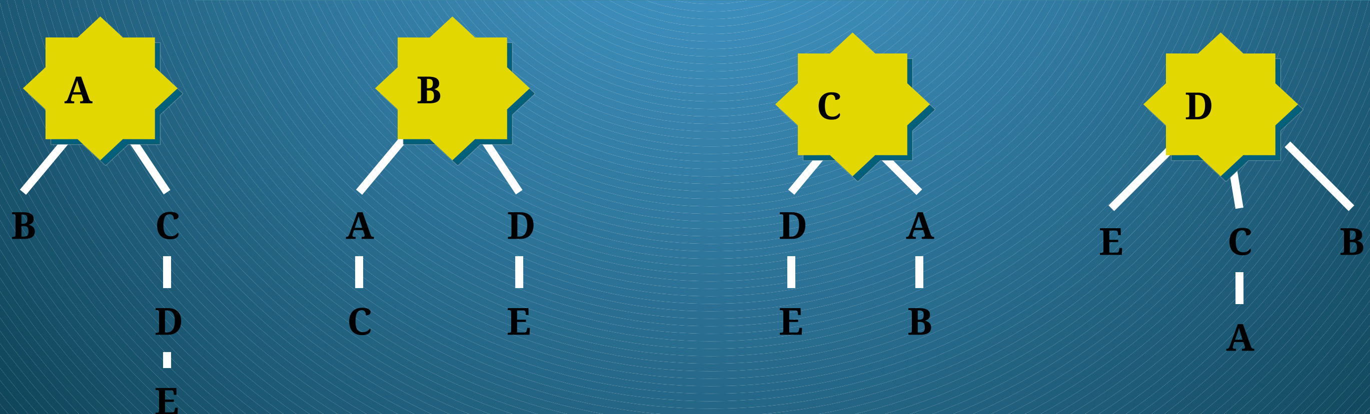
- Processing and memory requirements are increased for link-state routing.
- Bandwidth is consumed during the initial link-state flooding of LSAs.

Link State Routing (LSR)



Link State Database

Router A	Router B	Router C	Router D	Router E
B - 2 C - 1	A - 2 D - 4	A - 1 D - 2 E - 4	C - 2 B - 4 E - 1	C - 4 D - 1



Link State Routing Features

Link-state algorithms are also known as Dijkstras algorithm or as SPF (shortest path first) algorithms.

Link-state routing algorithms maintain a complex database of topology information.

The distance vector algorithm are also known as Bellman-Ford algorithms. They have nonspecific information about distant networks and no knowledge of distant routers.

A link-state routing algorithm maintains full knowledge of distant routers and how they interconnect. Link-state routing uses:

- **Link-state advertisements (LSAs)**
  A link-state advertisement (LSA) is a small packet of routing information that is sent between routers.
- **Topological database**
  A topological database is a collection of information gathered from LSAs.
- **SPF algorithm**
  The shortest path first (SPF) algorithm is a calculation performed on the database resulting in the SPF tree.
- **Routing tables** – A list of the known paths and interfaces.

Link State Routing

Advantages	Disadvantages
• Fast convergence: changes are reported immediately by the source affected • Robustness against routing loops • Routers know the topology • Link-state packets are sequenced and aged • The link-state database sizes can be minimized with careful network design	• Significant demands on memory and processing resources • Requires very strict network design • Requires a knowledgeable network administrator • Initial flooding can impede network performance

Comparing Routing Methods

Distance Vector	Link State
• View network topology from neighbor's perspective • Adds distance vectors from router to router • Frequent, periodic updates: Slow convergence • Passes copies of routing tables to neighbor routers	• Gets common view of entire network topology • Calculates the shortest path to other routers • Event-triggered updates: Faster convergence • Passes link-state routing updates to other routers

OSPF (Open Shortest Path First) Protocol

OSPF is a Link-State Routing Protocols

- Link-state (LS) routers recognize much more information about the network than their distance-vector counterparts,Consequently LS routers tend to make more accurate decisions.

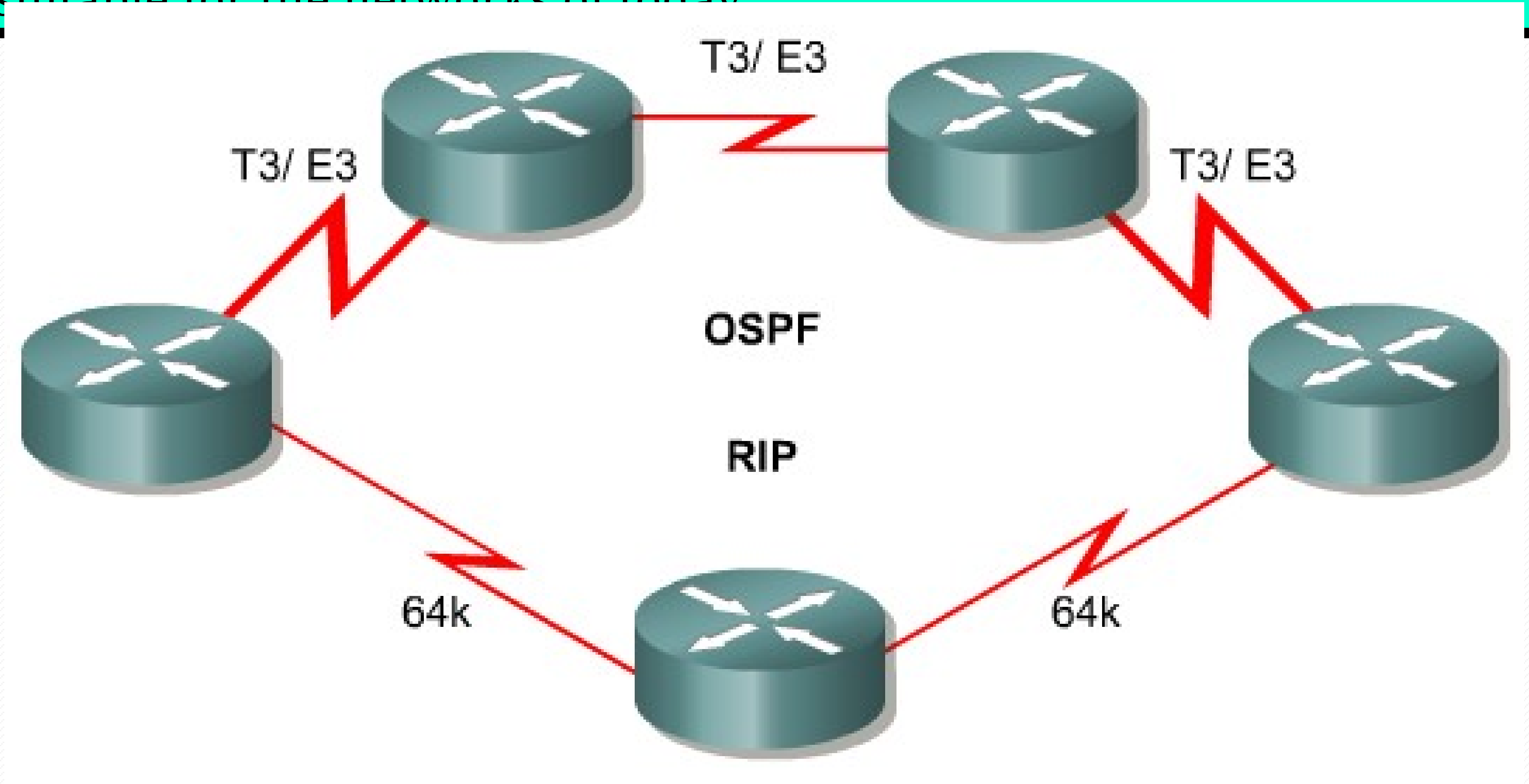
- Link-state routers keep track of the following:
  - Their neighbours
  - All routers within the same area
  - Best paths toward a destination

Link-State Data Structures

- Neighbor table:
  - Also known as the adjacency database (list of recognized neighbors)
- Topology table:
  - Typically referred to as LSDB (routers and links in the area or network)
  - All routers within an area have an identical LSDB
- Routing table:
  - Commonly named a forwarding database (list of best paths to destinations)

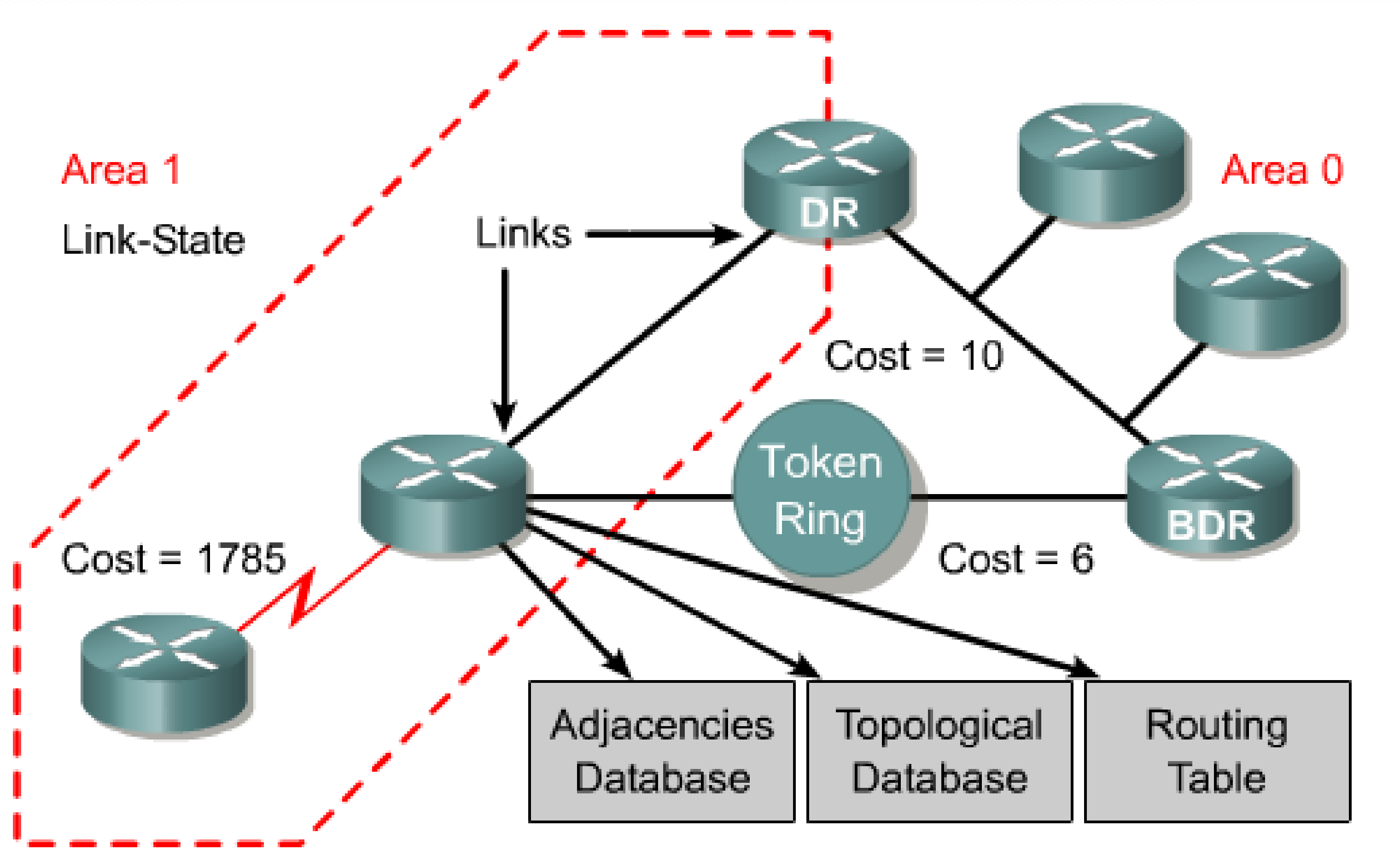
OSPF vs. RIP

RIP is limited to 15 hops, it converges slowly, and it sometimes chooses slow routes because it ignores critical factors such as bandwidth in route determination. OSPF overcomes these limitations and proves to be a robust and scalable routing protocol suitable for the networks of today.

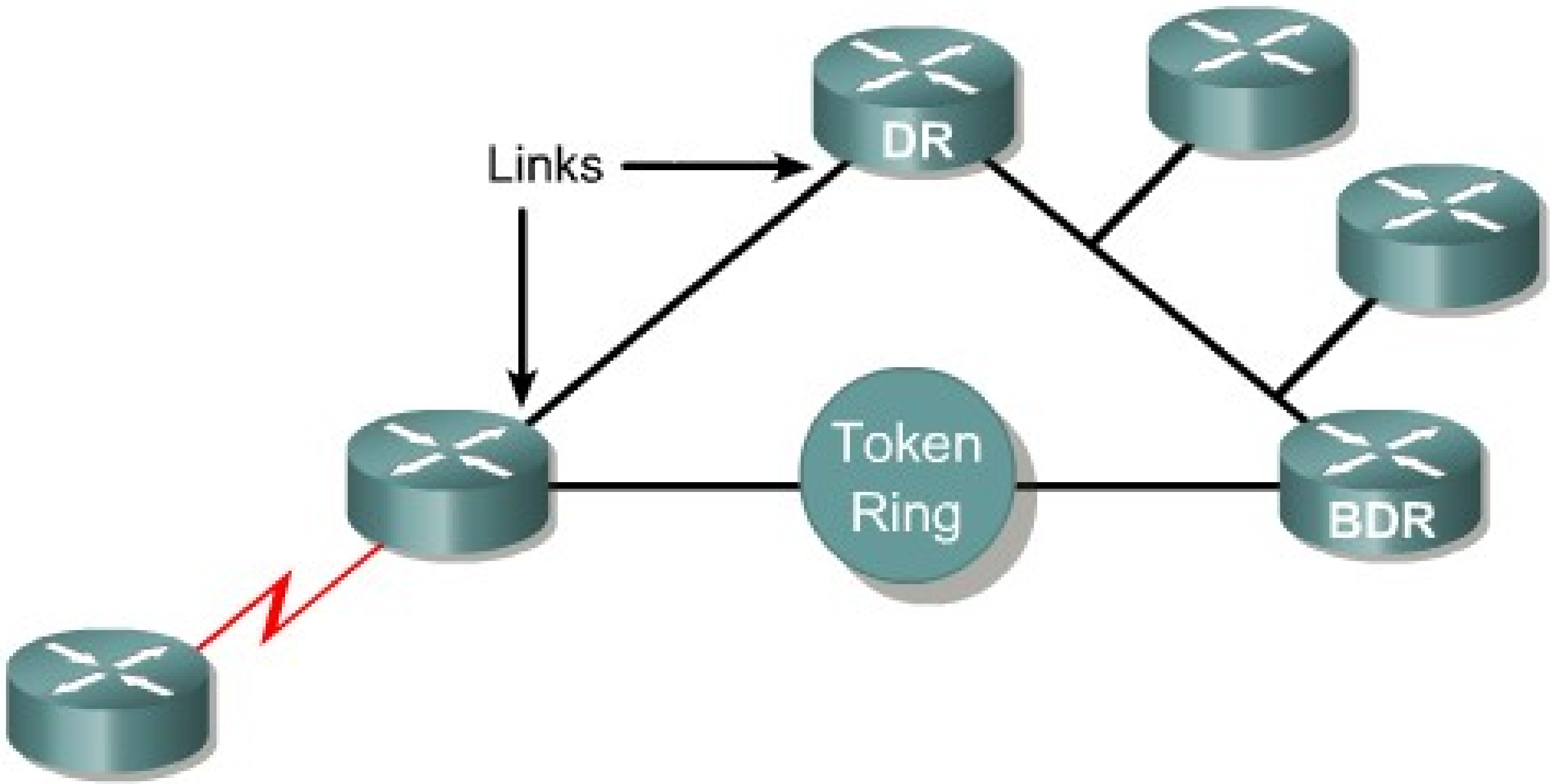


OSPF Terminology

The next several slides explain various OSPF terms -one per slide.

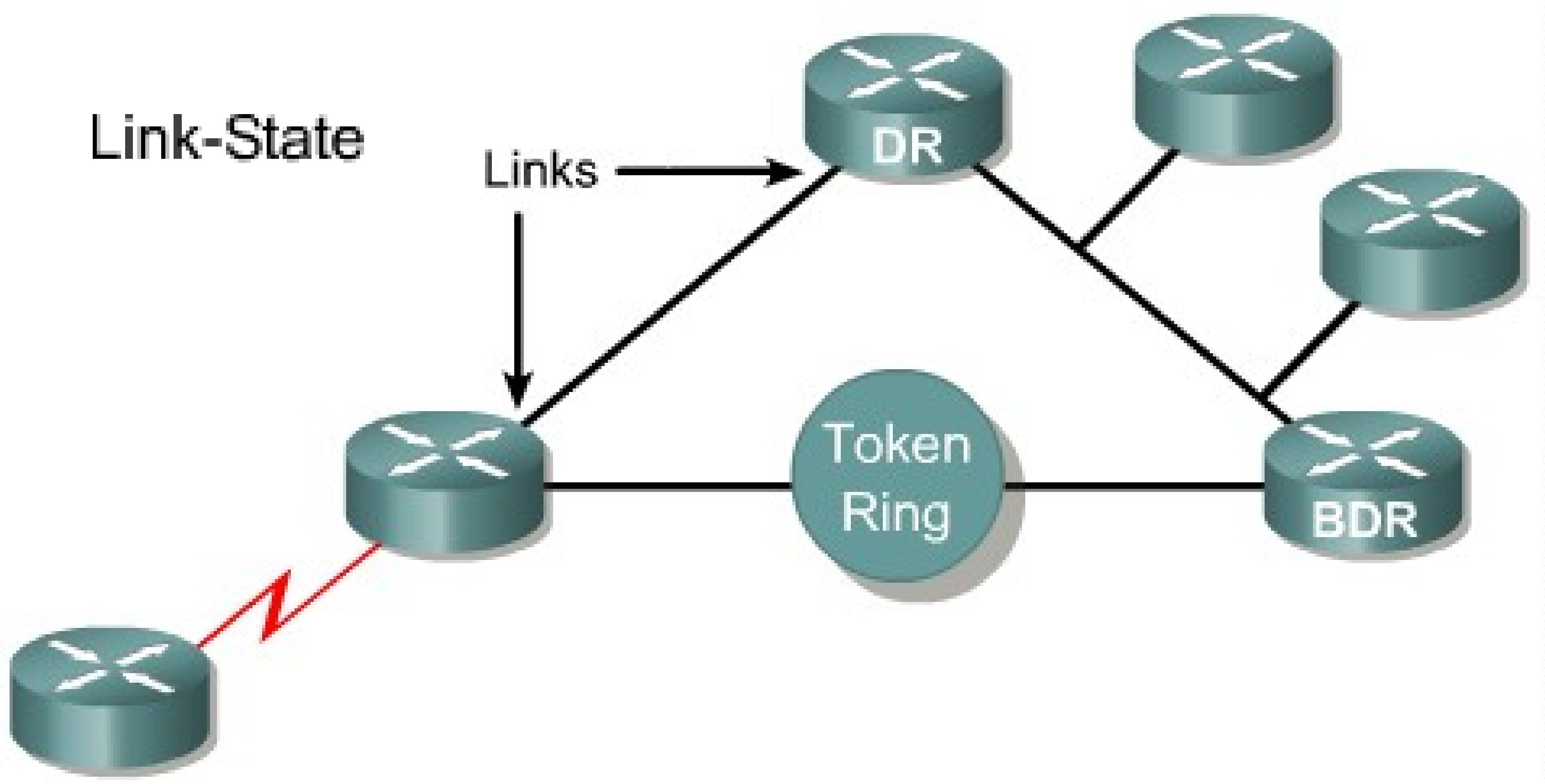


OSPF Term: Link



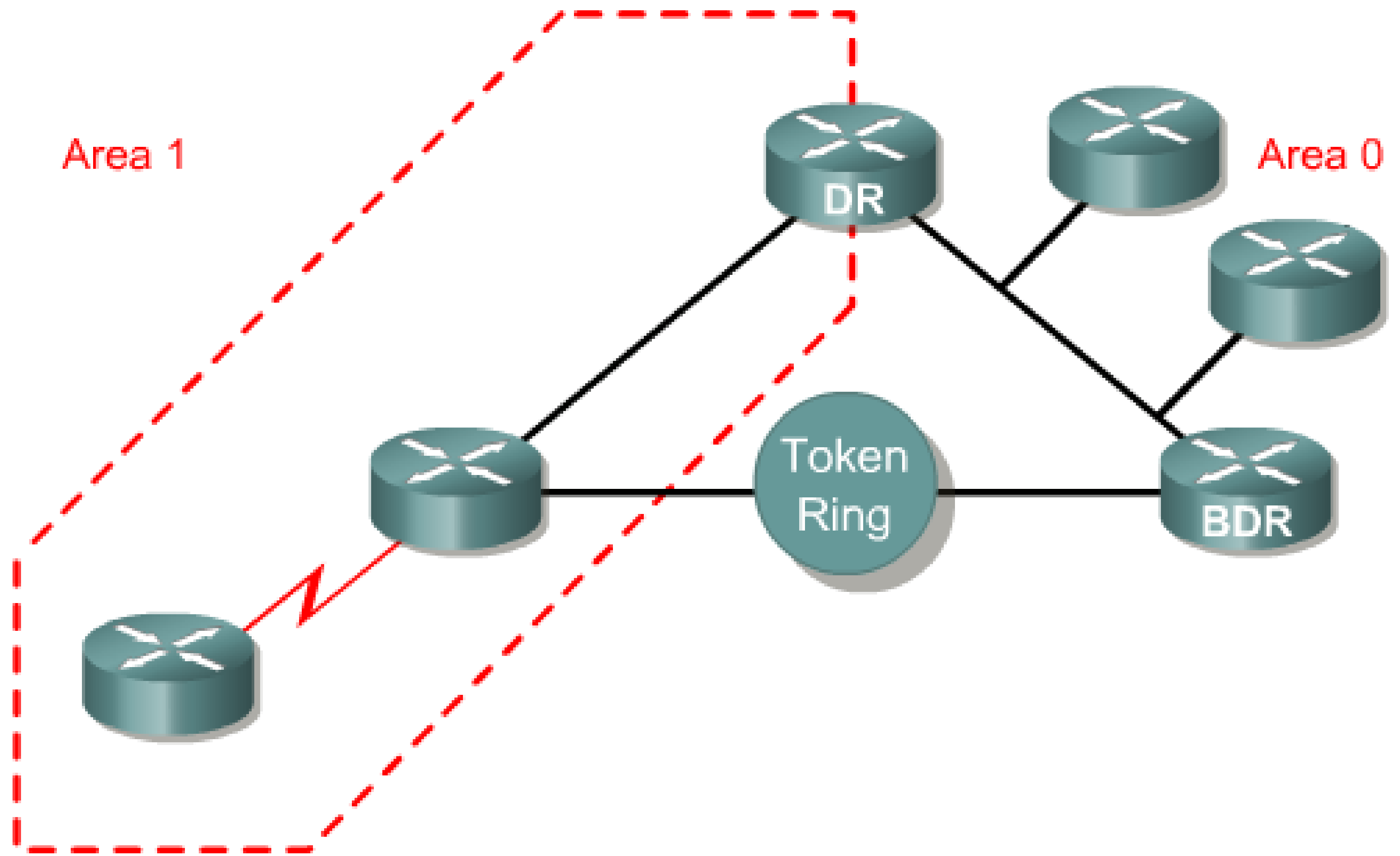
Link: An interface on a router.

OSPF Term: Link State



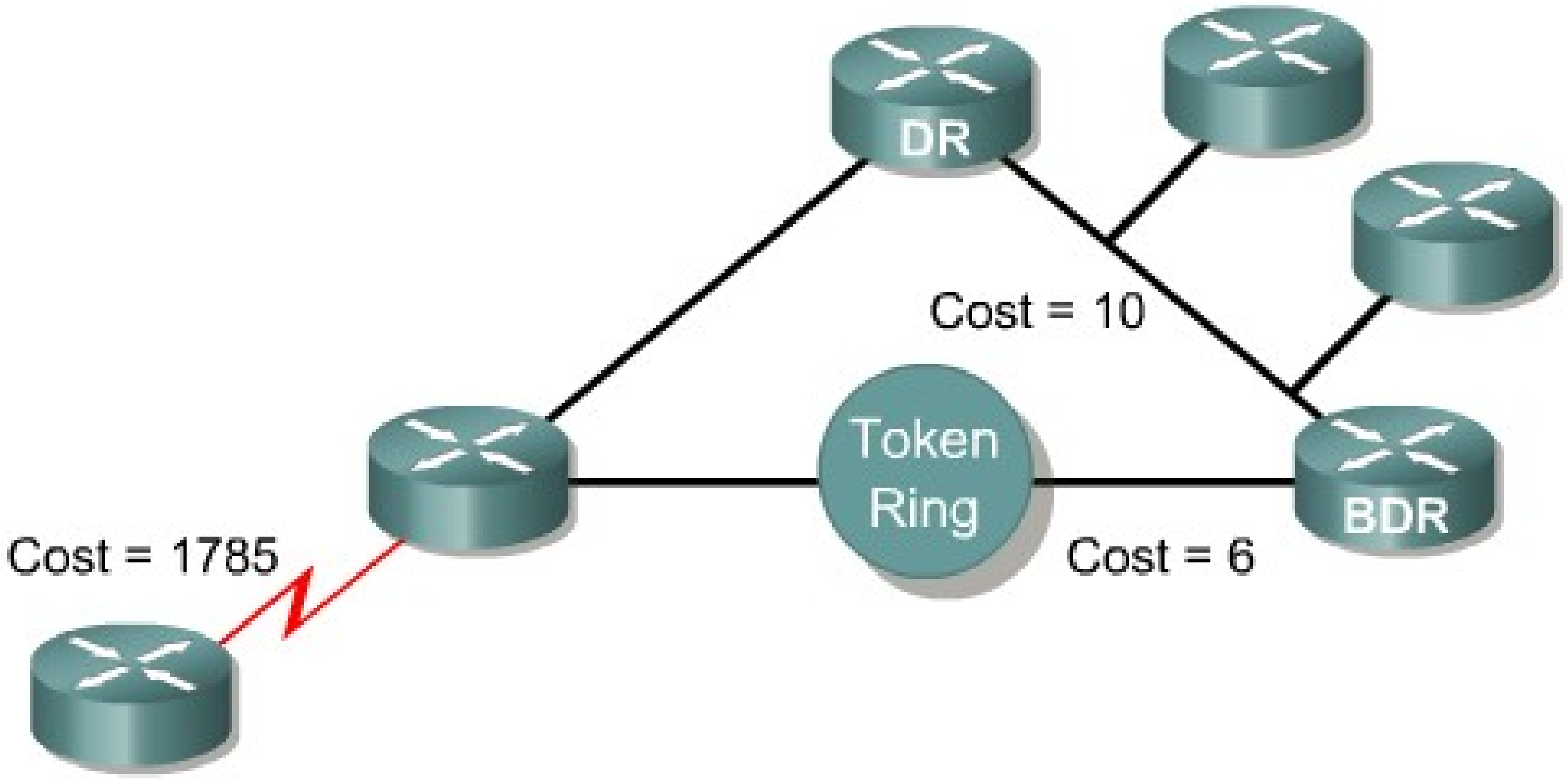
Link-State: The status of a link between two routers. Also a router interface and its relationship to its neighboring routers.

OSPF Term: Area



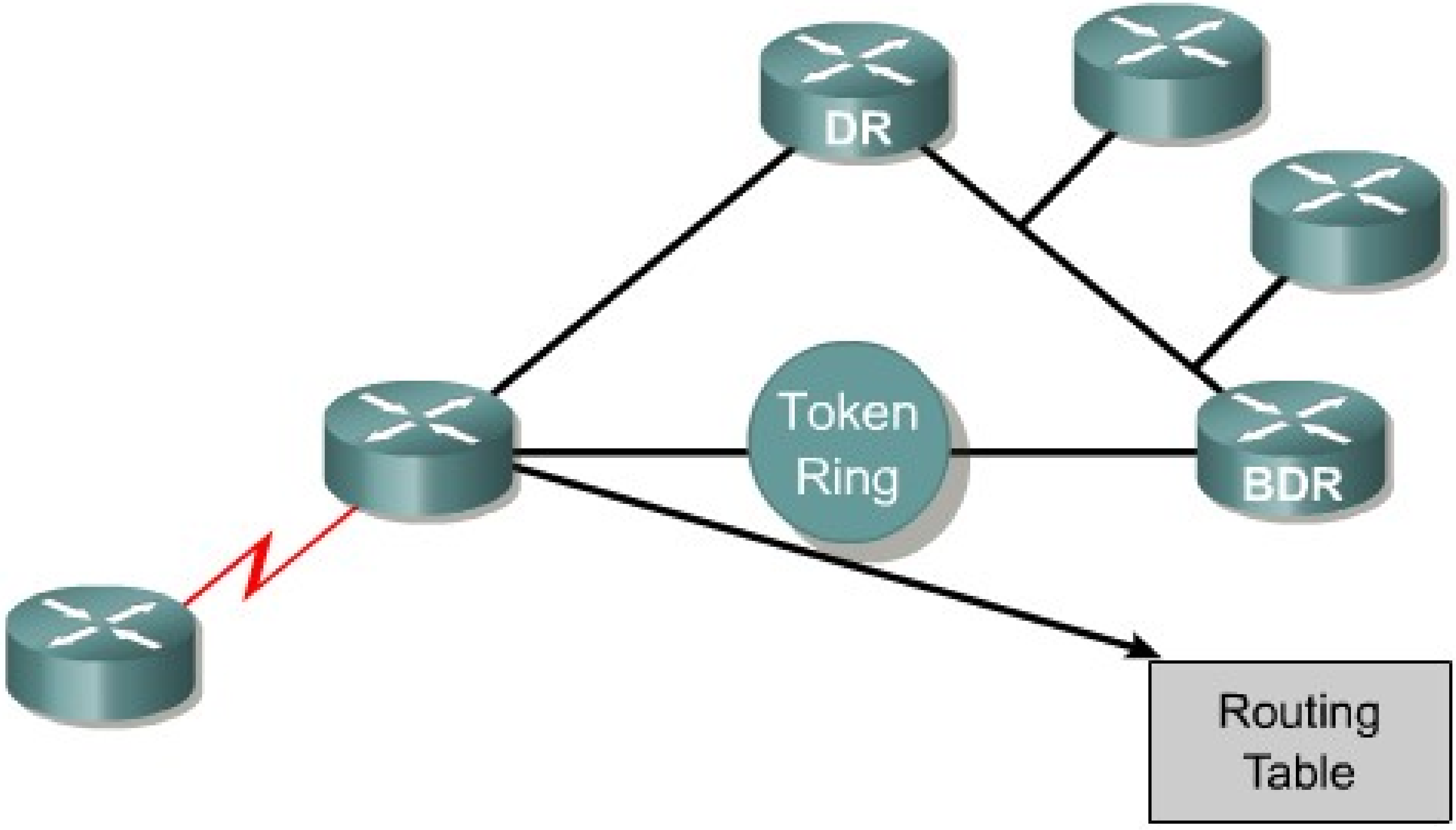
Area: A collection of networks and routers that has the same area identification. Each router within an area has the same link-state information. A router within an area is called an internal router.

OSPF Term: Link Cost



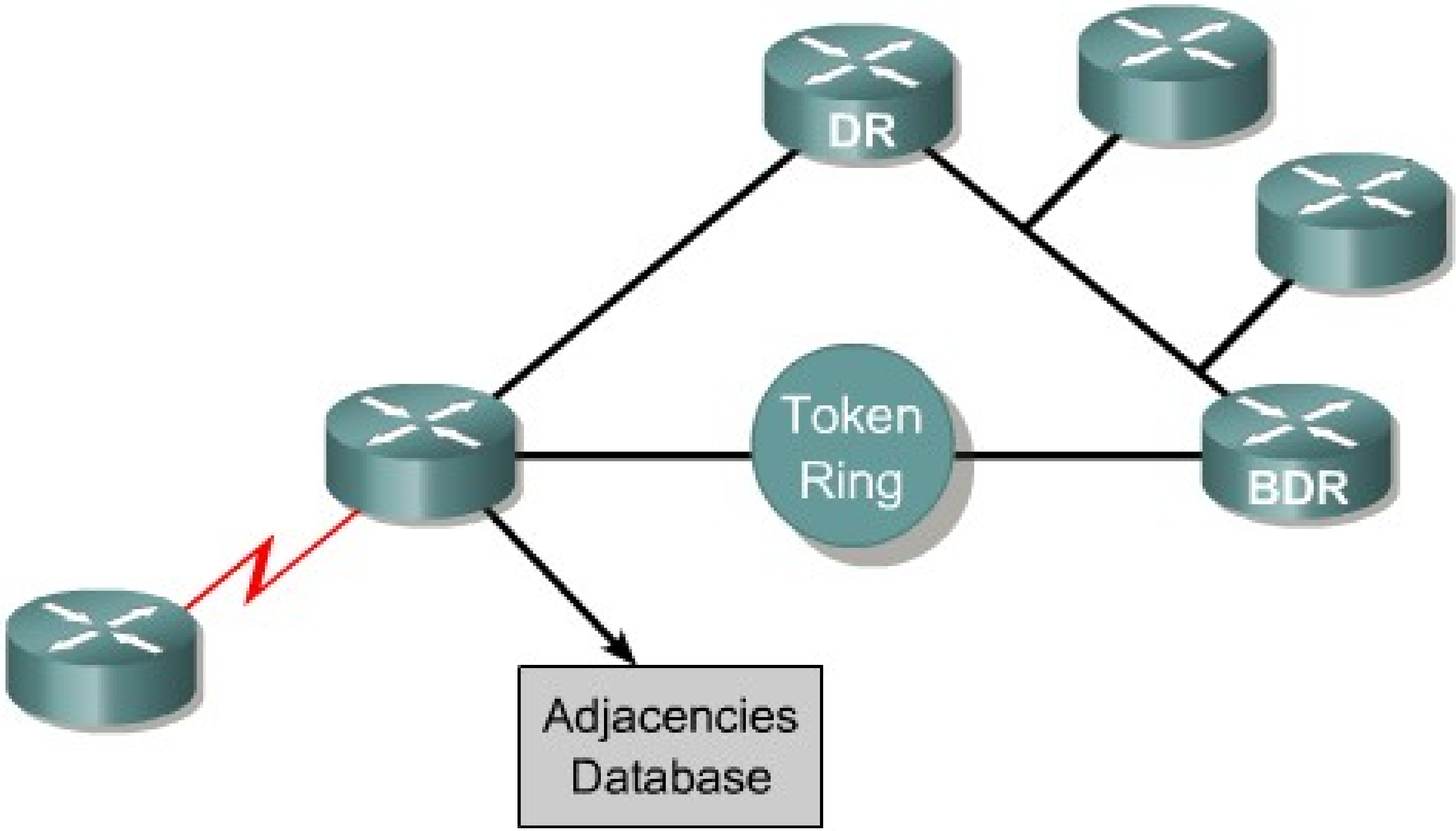
Cost: The value assigned to a link. Rather than hops, link-state protocols assign a cost to a link, which is based on the bandwidth of the link (transmission speed).

OSPF Term: Forwarding Database



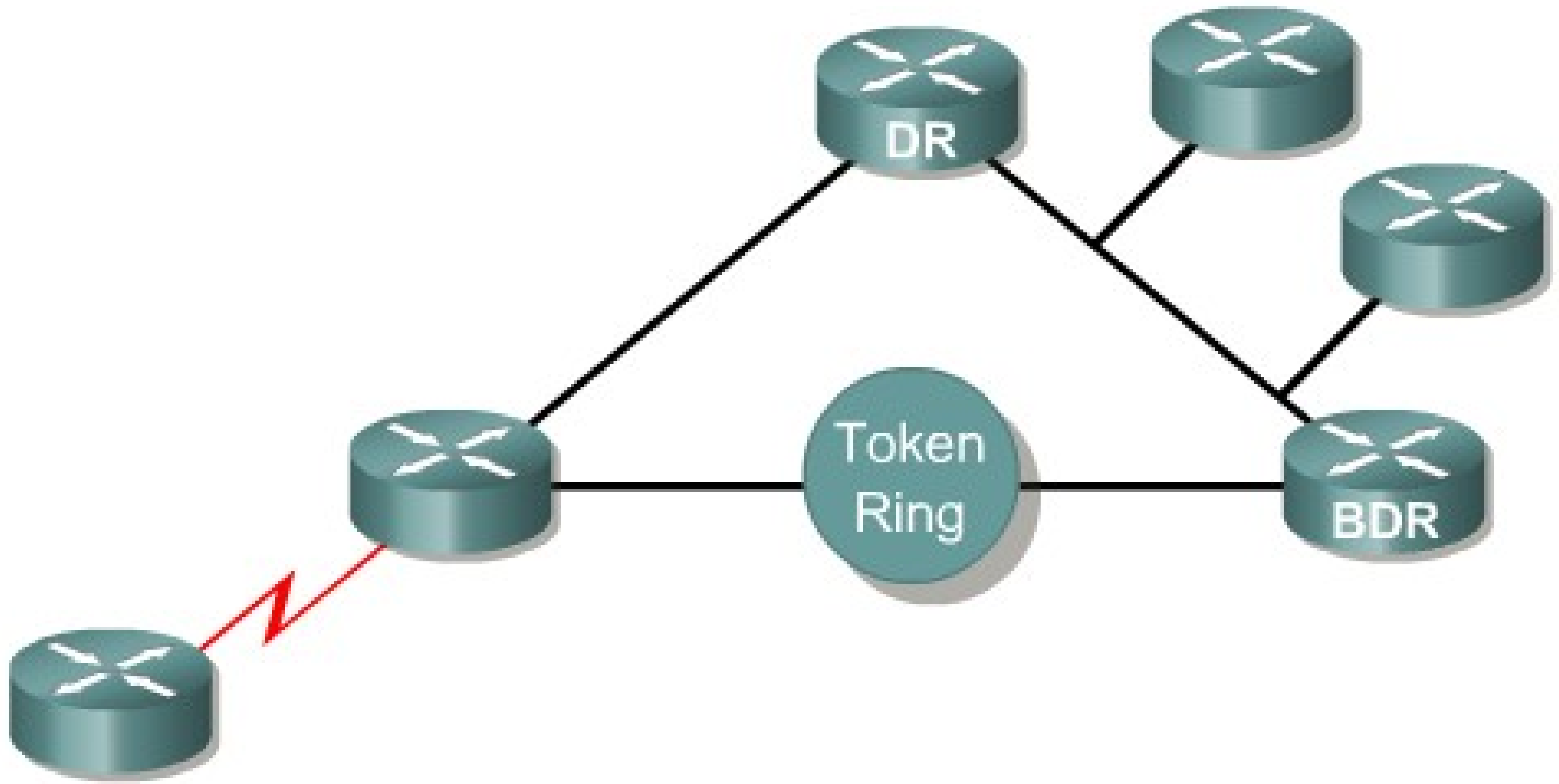
Routing table: The routing table, which is sometimes known as the forwarding database, is generated when an algorithm is run on the link-state database. The routing table for each router is unique.

OSPF Term: Adjacencies Database



Adjacencies database: A listing of all the neighbors to which a router has established a bi-directional communication.

OSPF Terms: DR & BDR



Designated router (DR) and backup designated router (BDR): A router that is elected by all other routers on the same LAN to represent all the routers. Each network has a DR and BDR.

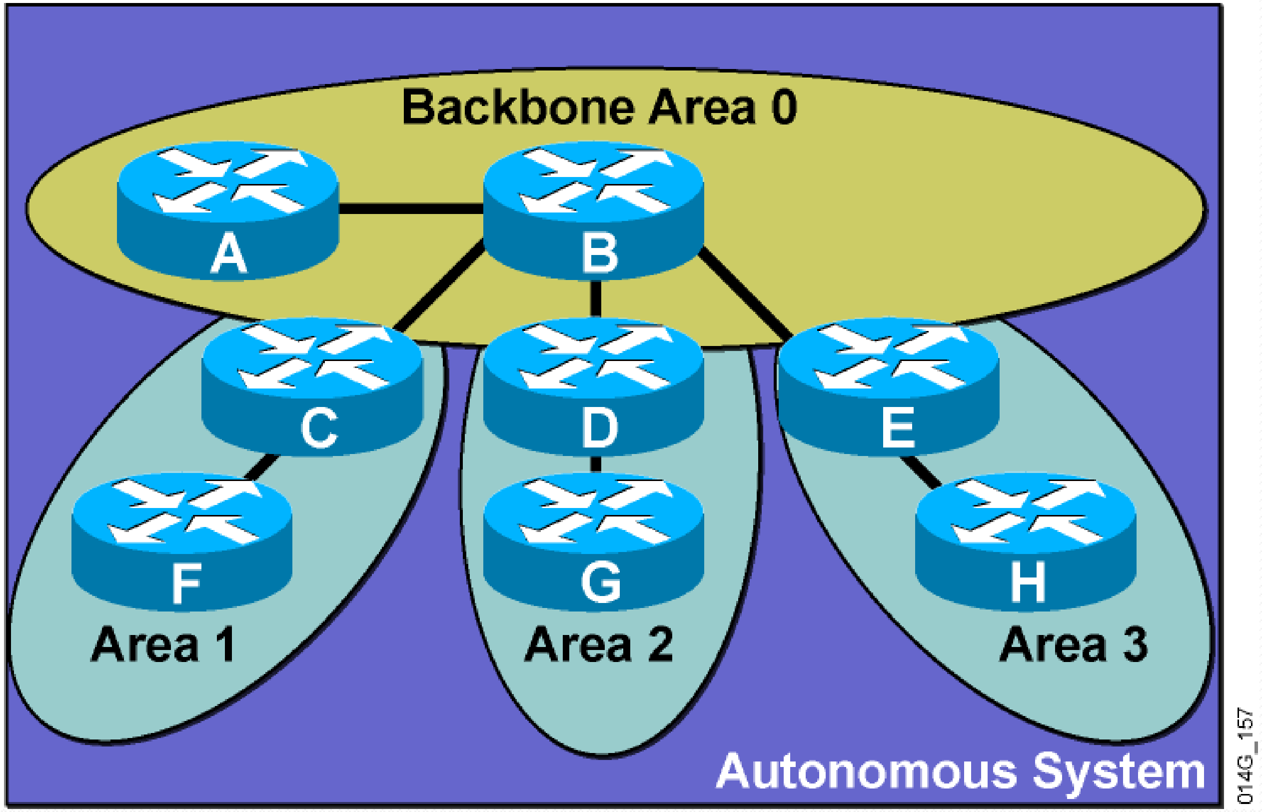
Link-State Data Structure: Network Hierarchy

- Link-state routing requires a hierachical network structure that is enforced by OSPF.
- This two-level hierarchy consists of the following:
- Transit area (backbone or area 0)
- Regular areas (nonbackbone areas)

OSPF Areas

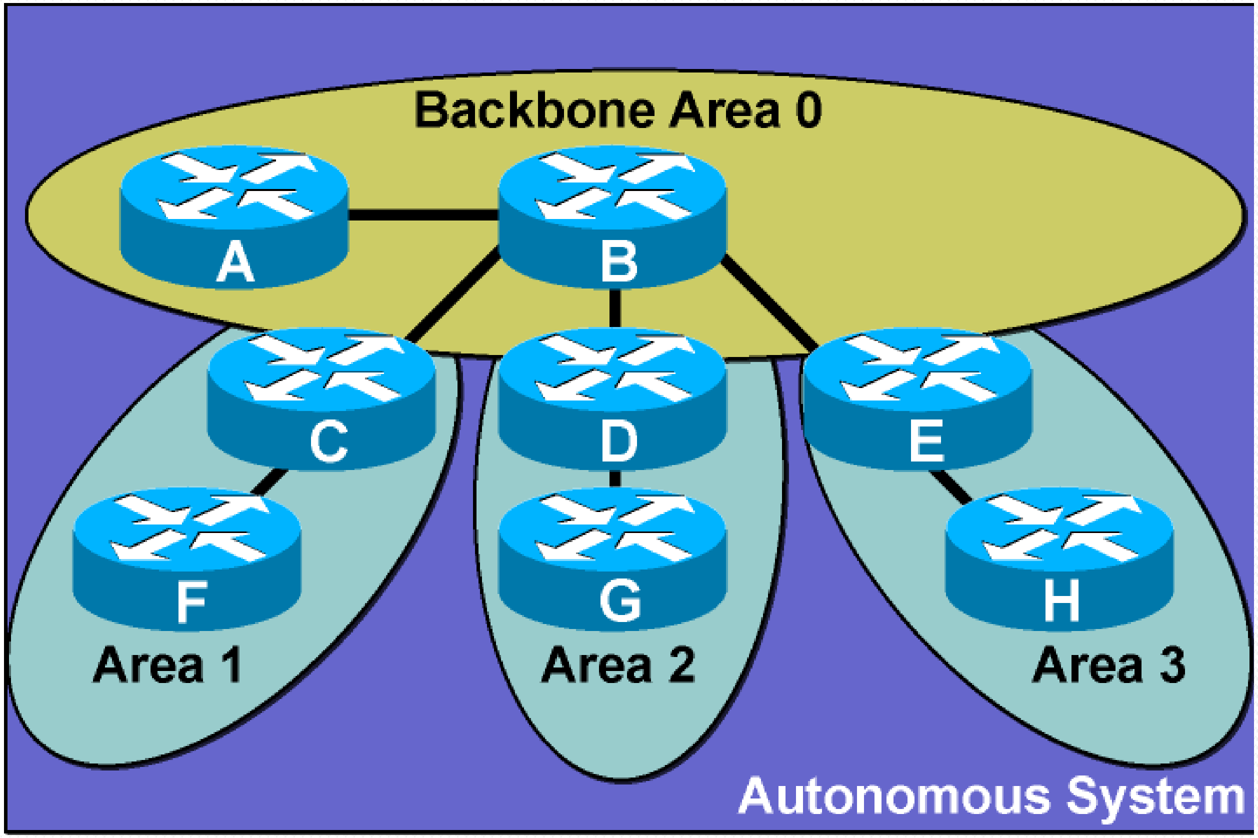
OSPF Area Characteristics:

- Minimizes routing table entries
- Localizes impact of a toplogy change within an area
- Detailed LSA flooding stops at the area boundary
- Requires a hierarchical network design



Area Terminology

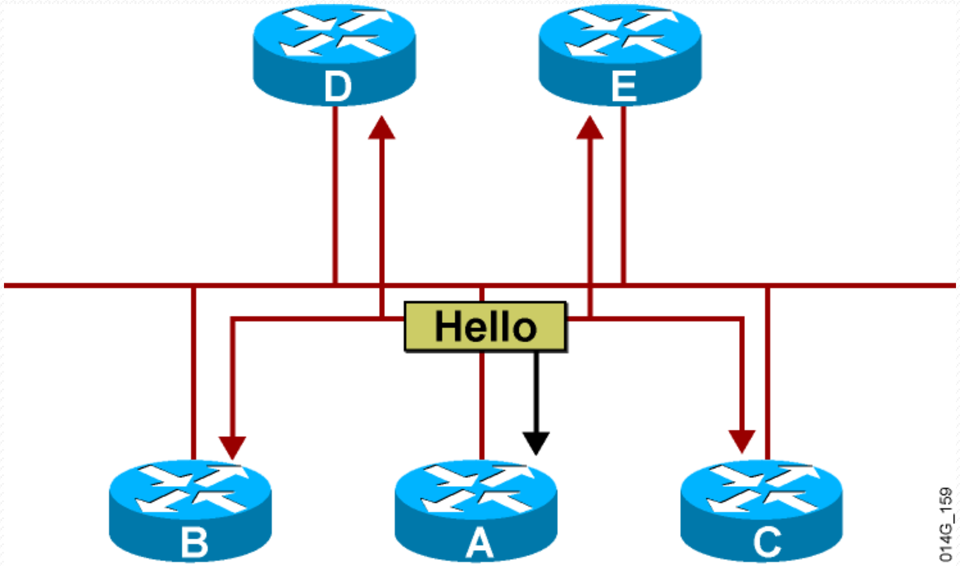
- Routers A and B are backbone routers.
- Backbone routers make up area 0.
- Routers C, D, and E are known as Area Border Routers (ABRs).
- ABRs attach all other areas to area 0.



LS Data Structures: Adjacency Database

- Routers discover neighbors by exchanging hello packets.
- Routers declare neighbors to be up after checking certain parameters or options in the hello packet.
- Point-to-point WAN links:
  - Both neighbors become fully adjacent.
- LAN links:
  - Neighbors form an adjacency with the DR and BDR.
  - Maintain two-way state with the other routers (DROTHERs).
- Routing updates and topology information are only passed between adjacent routers.

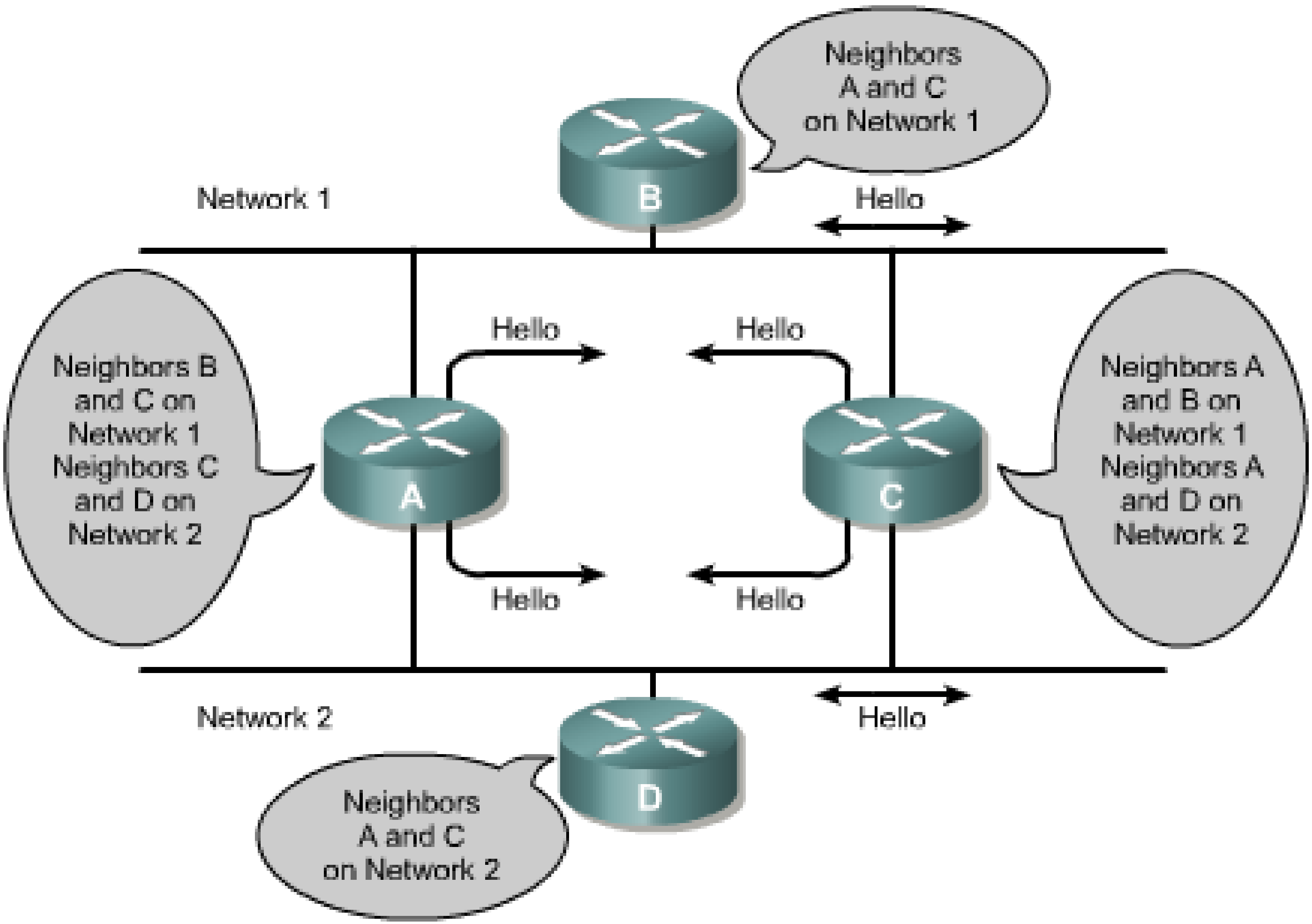
OSPF Adjacencies



Routers build logical adjacencies between each other using the Hello Protocol. Once an adjacency is formed:

- **LS database packets are exchanged to synchronize each other's LS databases.**
- **LSAs are flooded reliably throughout the area or network using these adjacencies.**

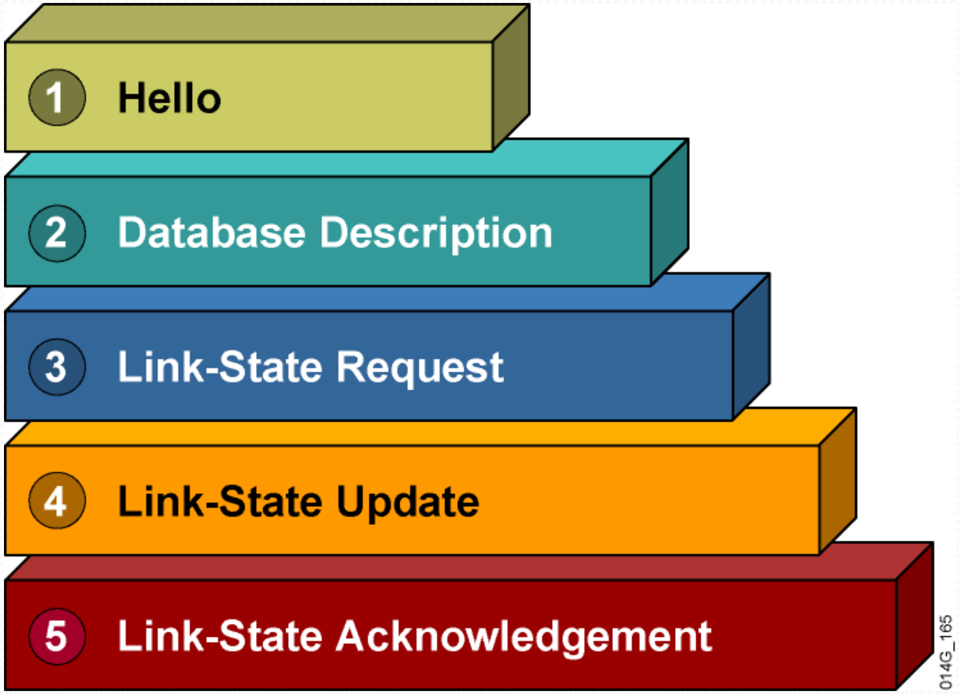
Link State Routing Graphic



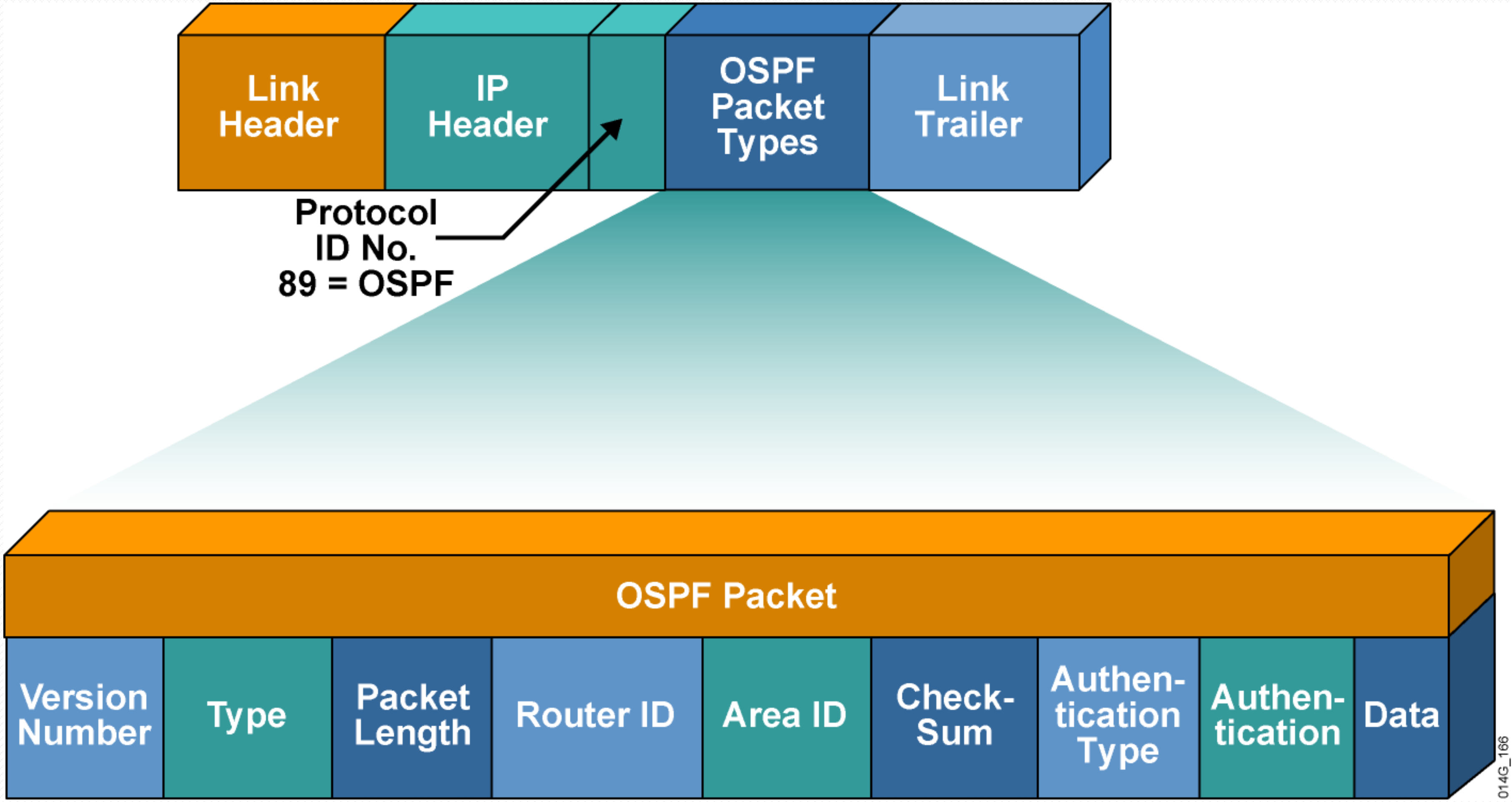
Open Shortest Path First Calculation

- Routers find the best paths to destinations by applying Dijkstra's SPF algorithm to the link-state database as follows:
  - Every router in an area has the identical link-state database.
  - Each router in the area places itself into the root of the tree that is built.
  - The best path is calculated with respect to the lowest total cost of links to a specific destination.
  - Best routes are put into the forwarding database.

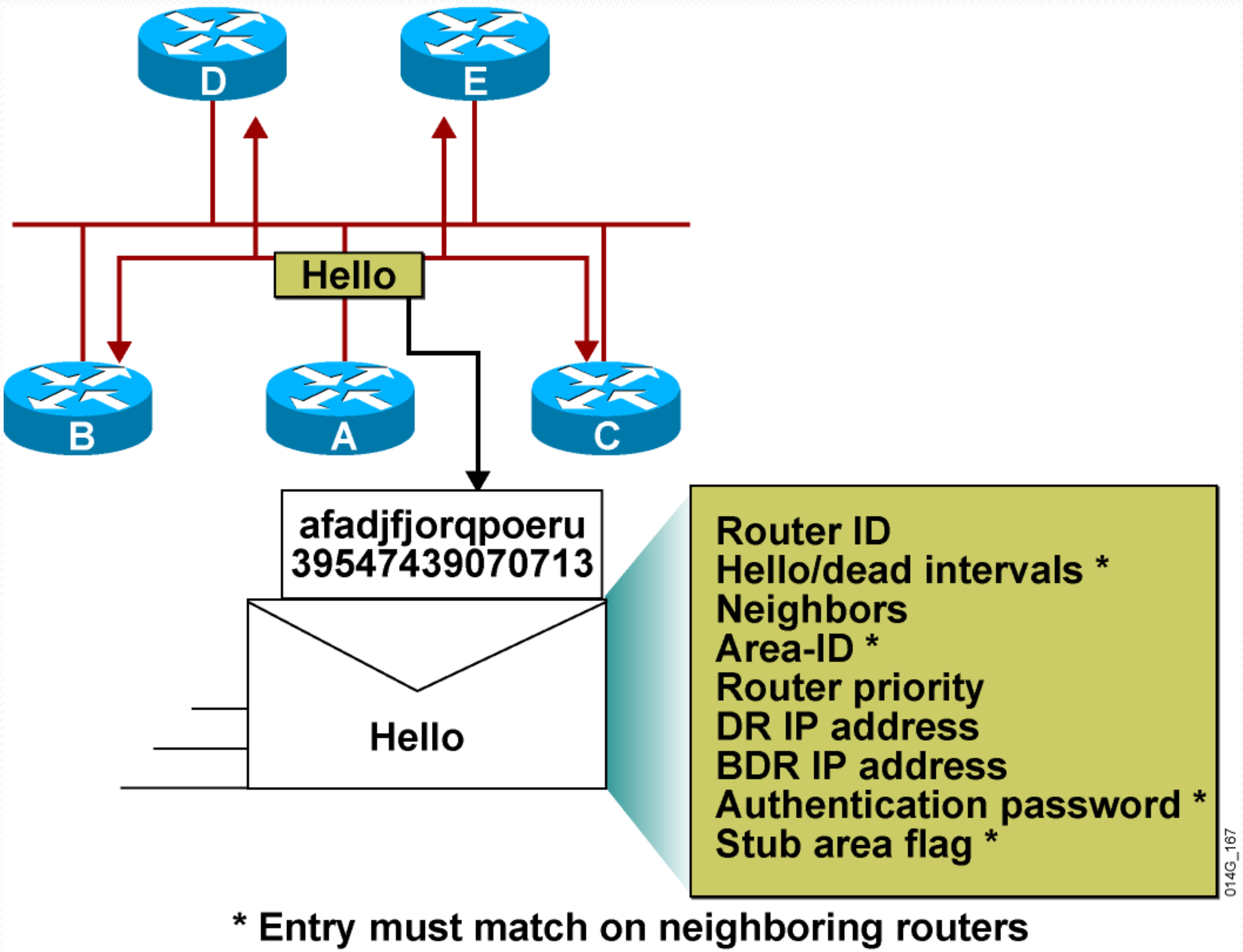
OSPF Packet Types



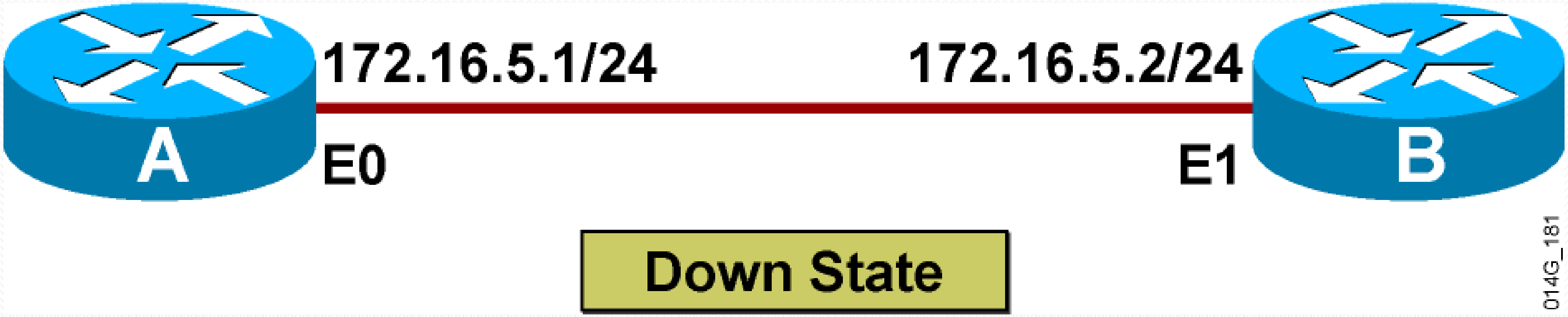
OSPF Packet Header Format



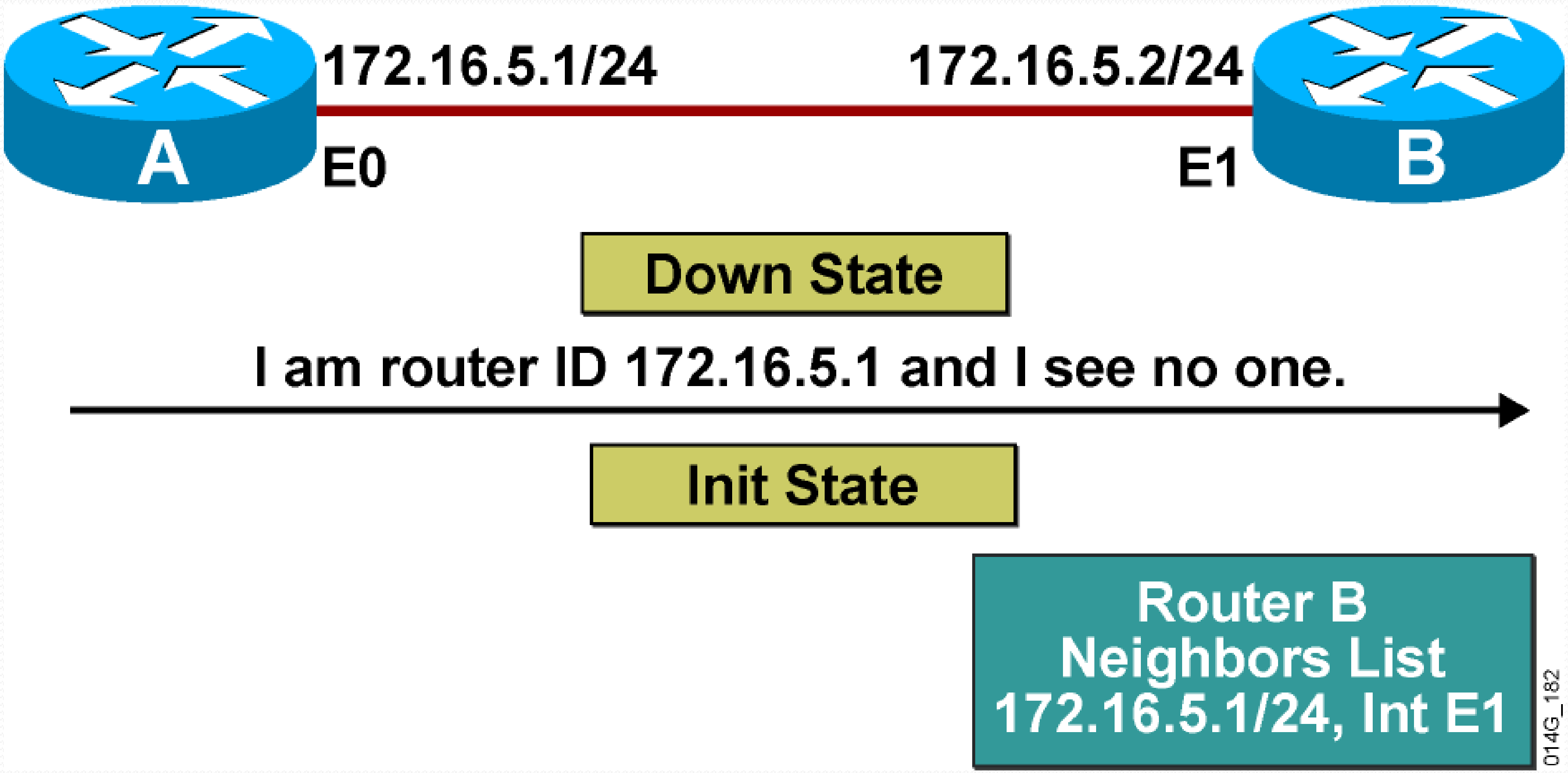
Neighborship



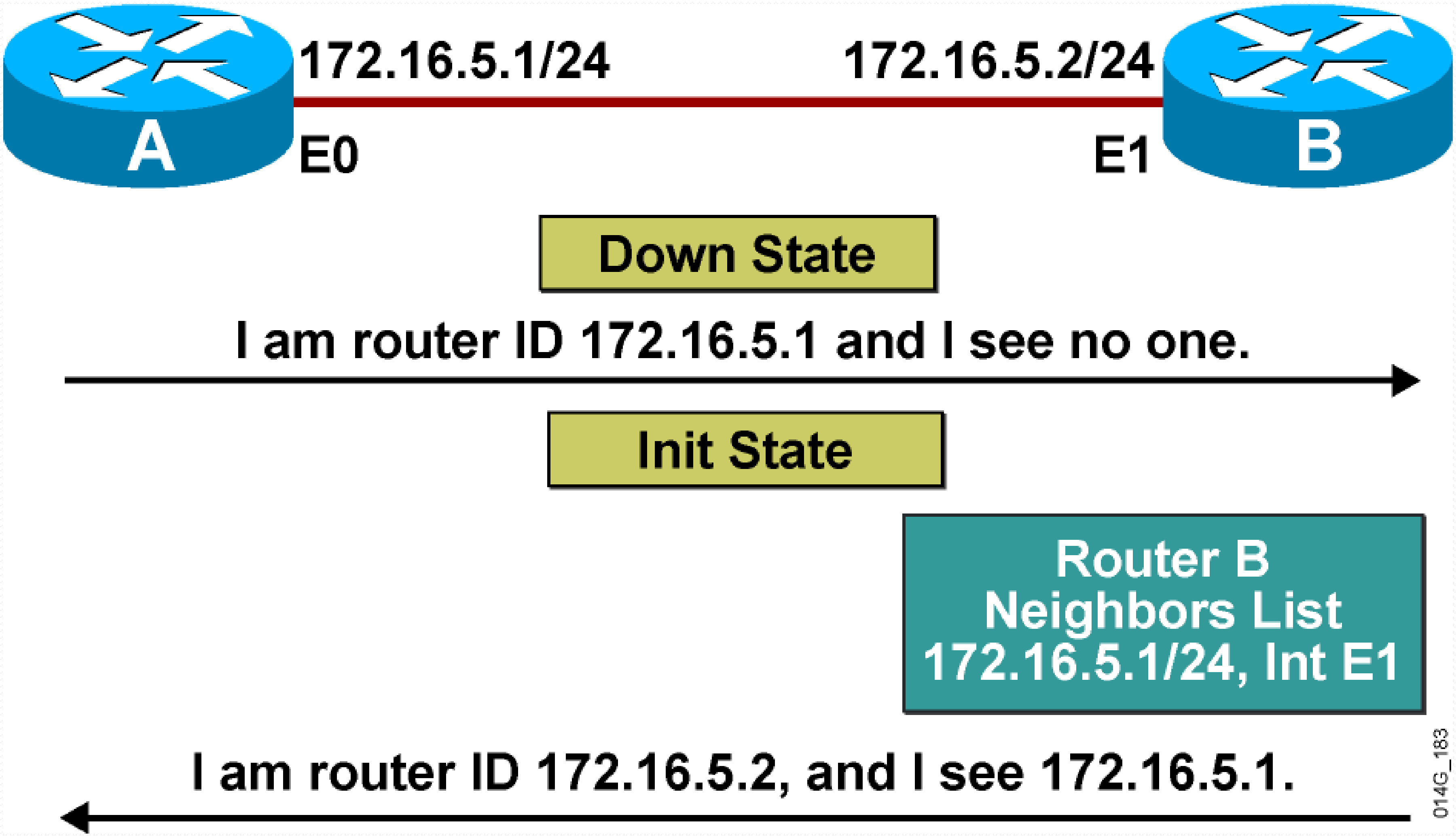
Establishing Bidirectional Communication



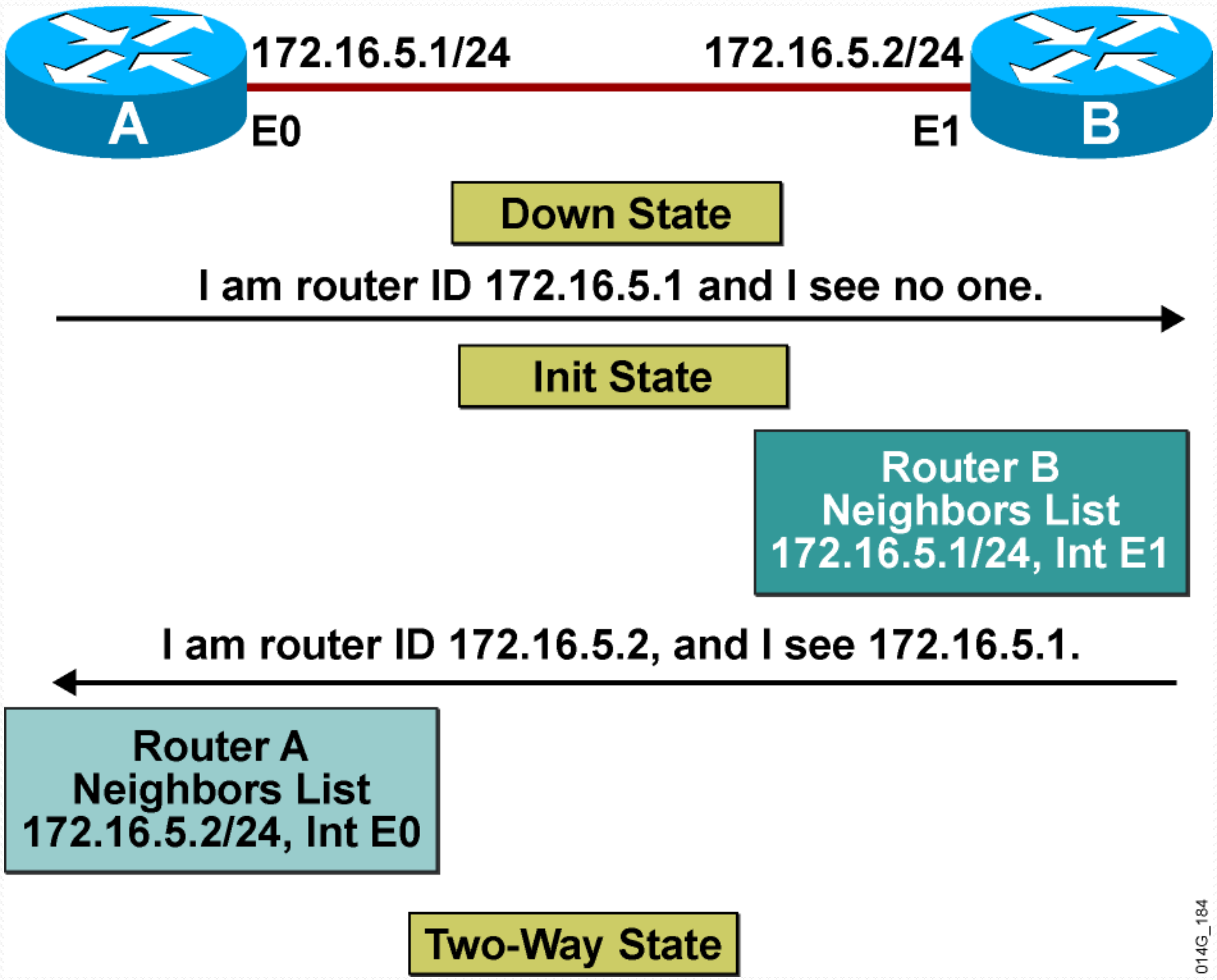
Establishing Bidirectional Communication (Cont.)



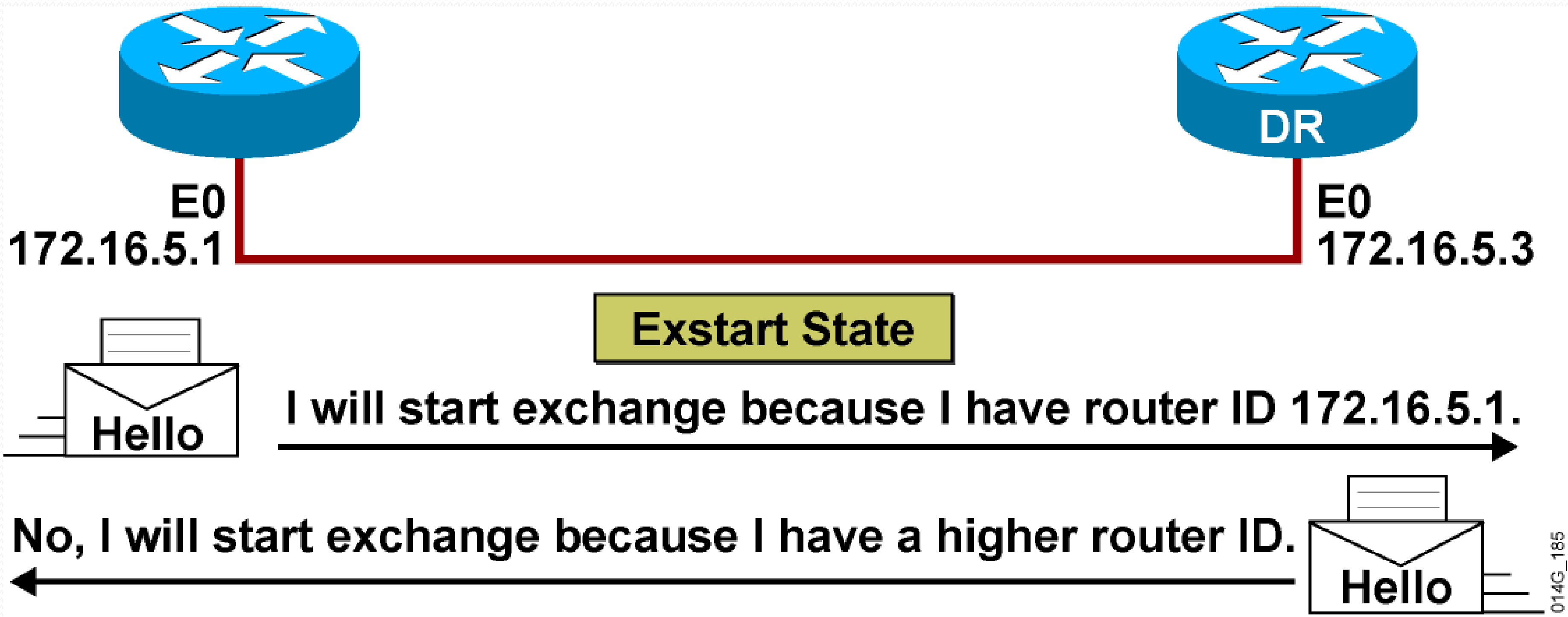
Establishing Bidirectional Communication (Cont.)



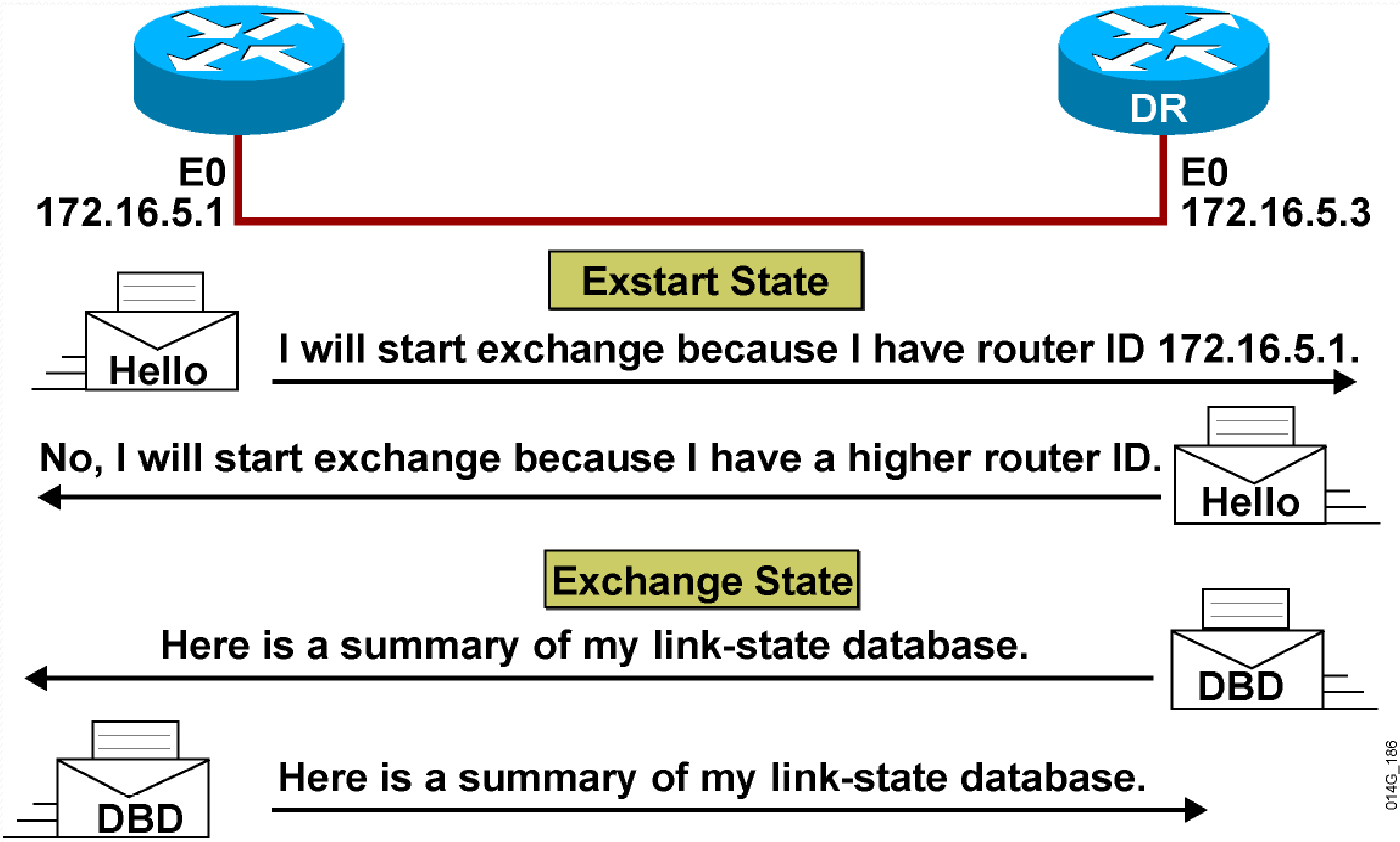
Establishing Bidirectional Communication



Discovering the Network Routes

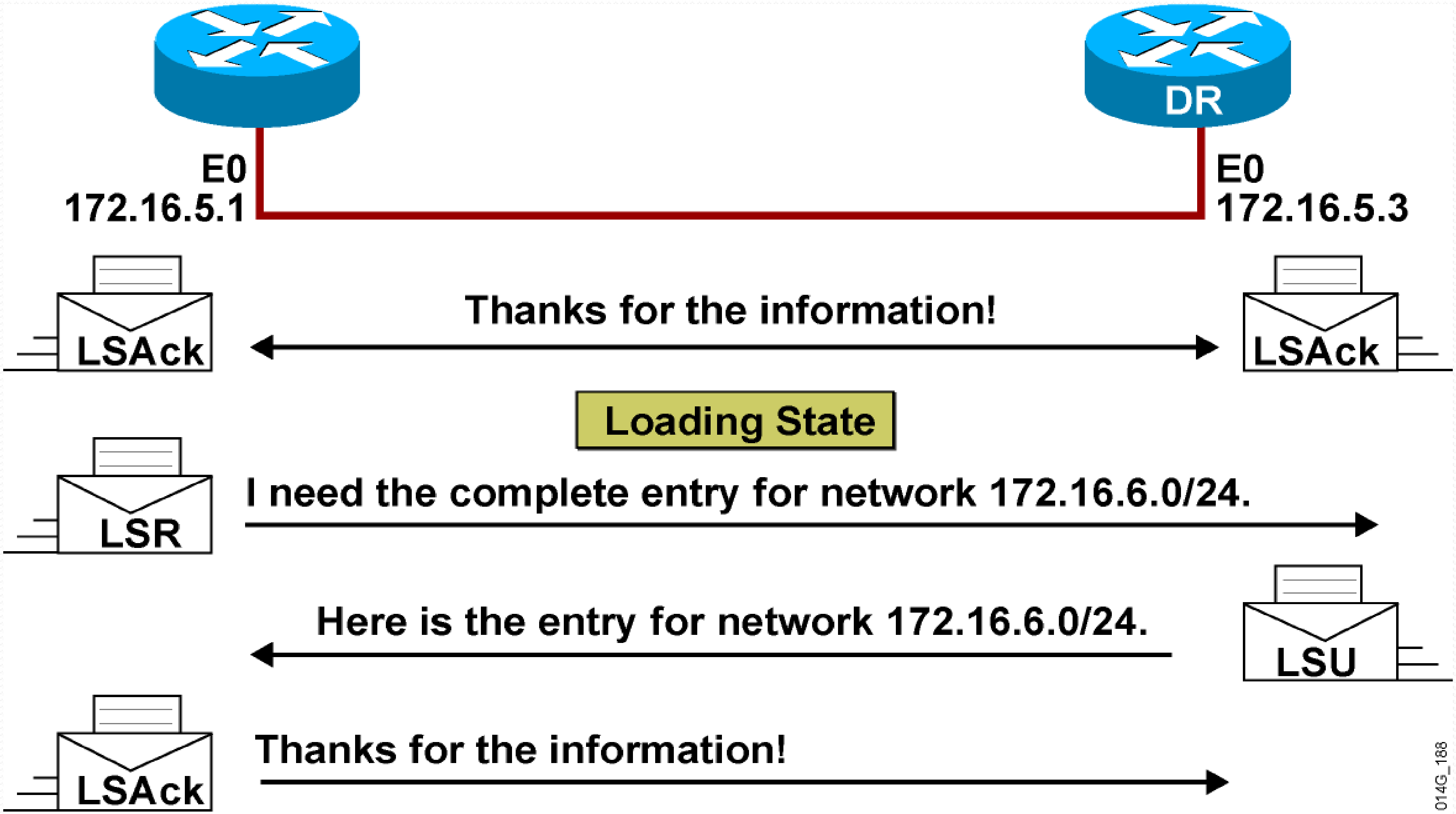


Discovering the Network Routes

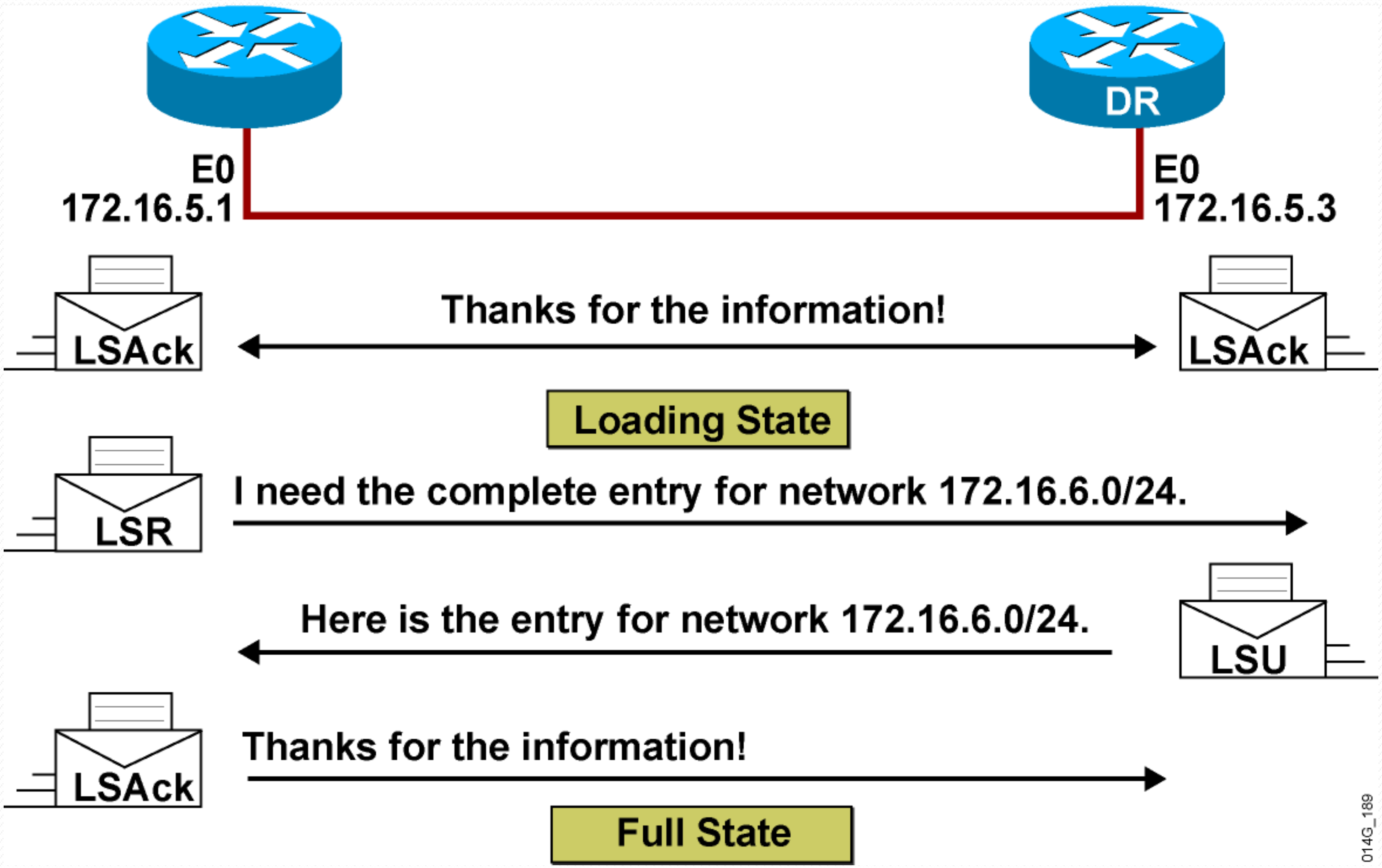


Adding the Link-State Entries

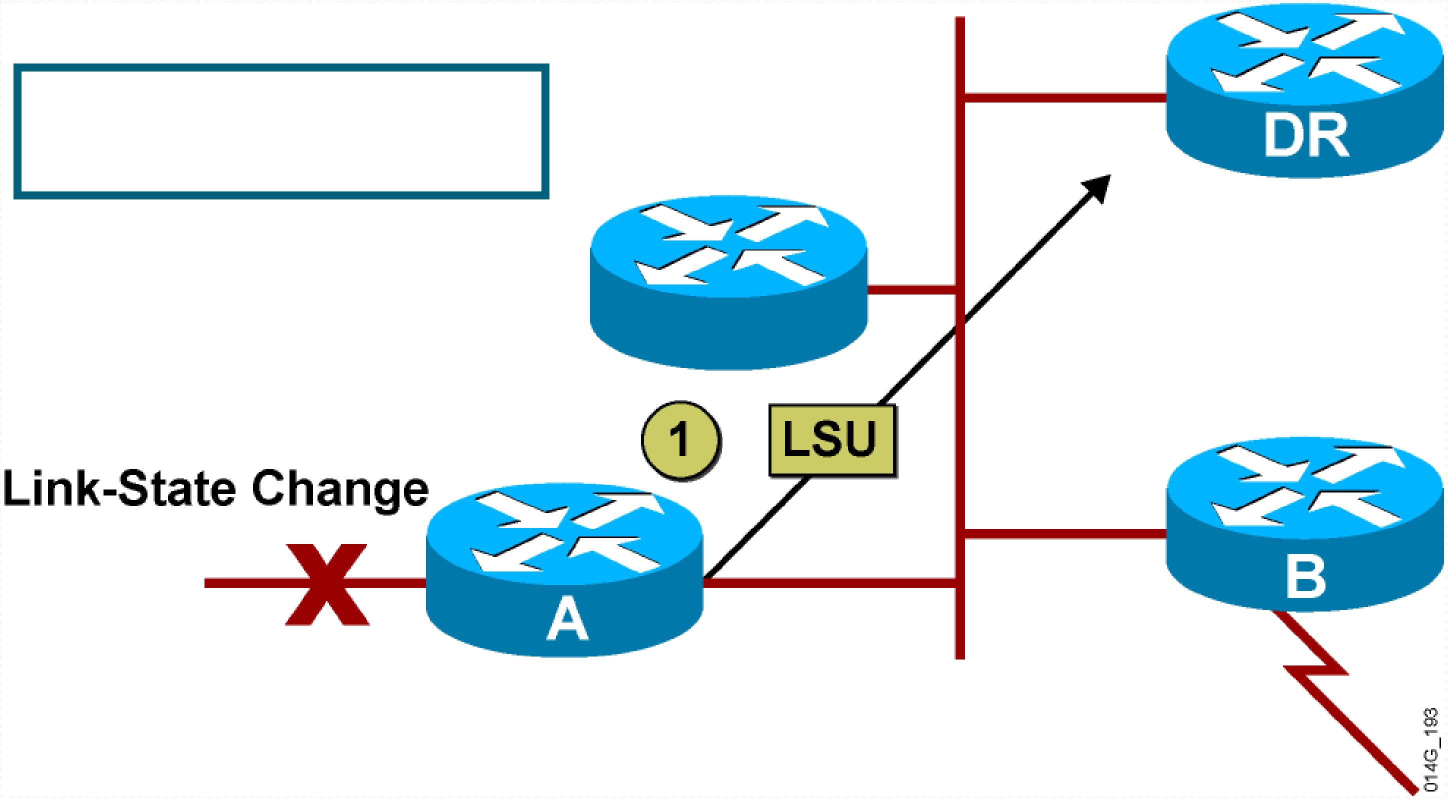
Adding the Link-State Entries (Cont.)



Adding the Link-State Entries

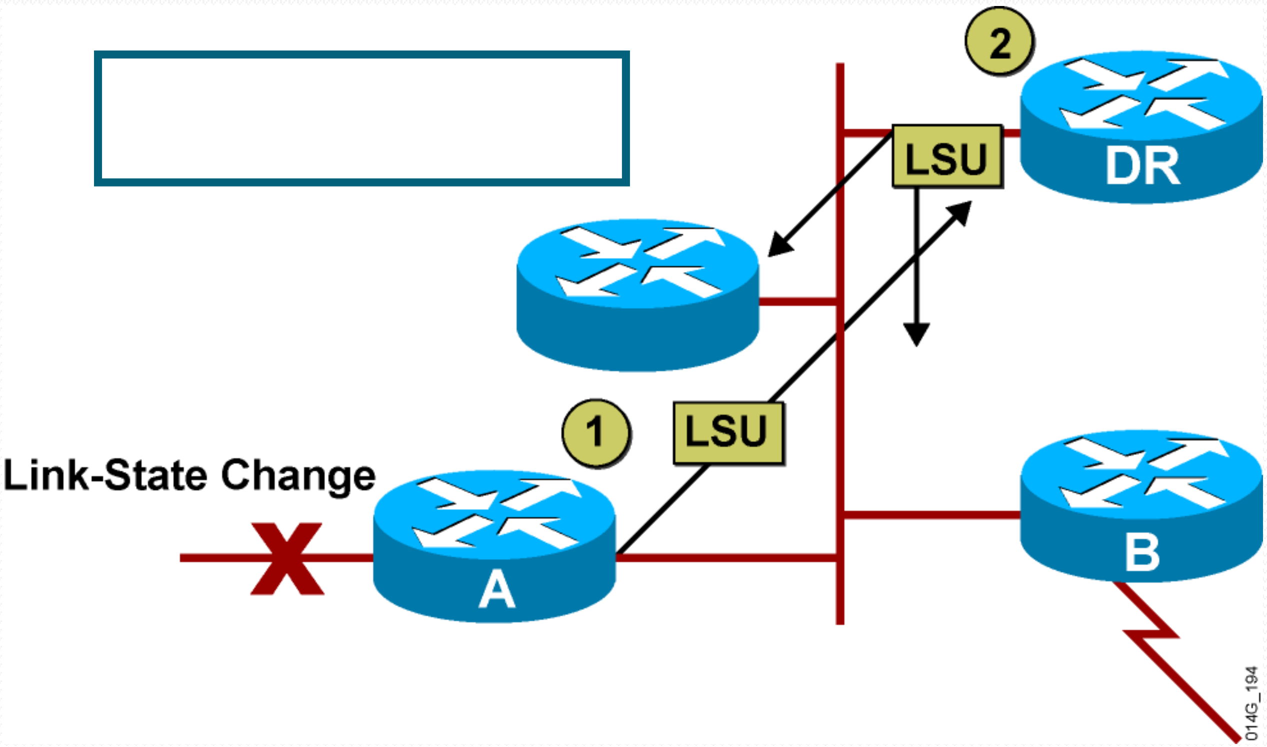


Maintaining Routing Information



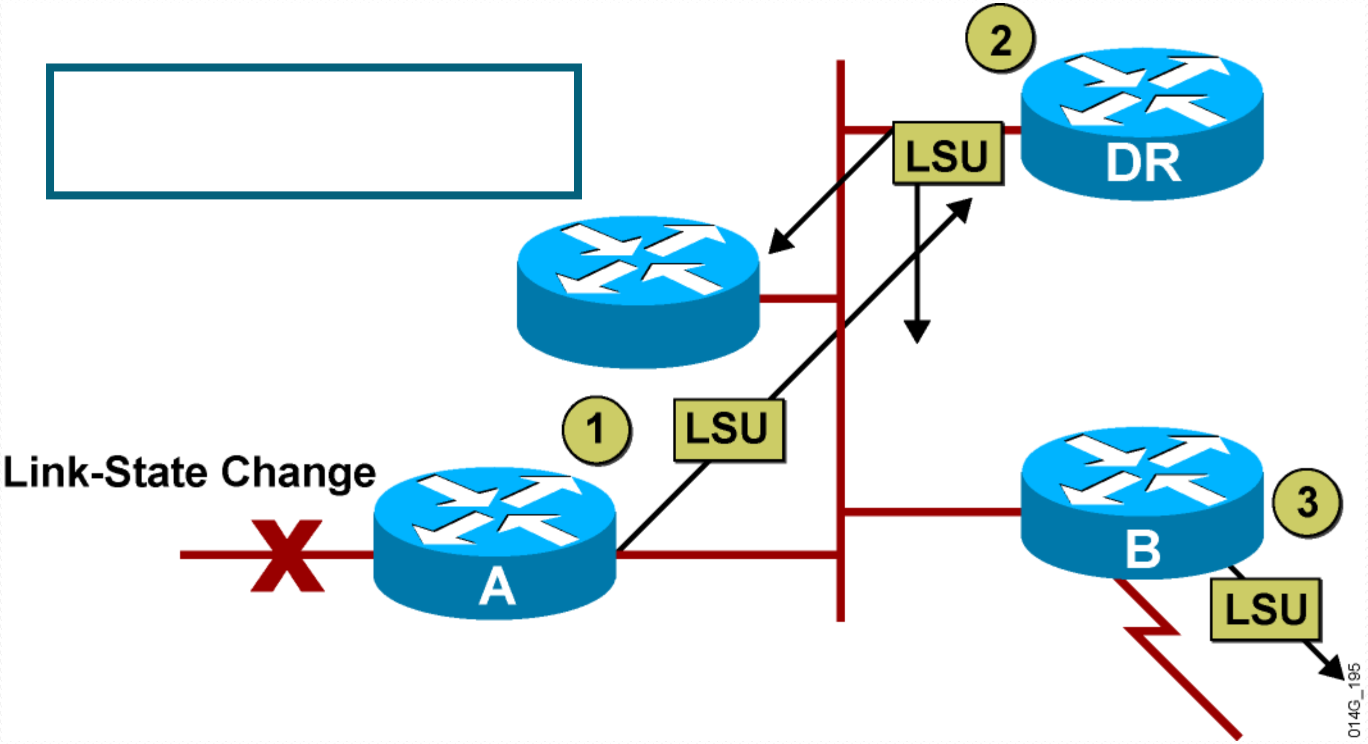
- **Router A notifies all OSPF DRs on 224.0.0.6**

Maintaining Routing Information (Cont.)



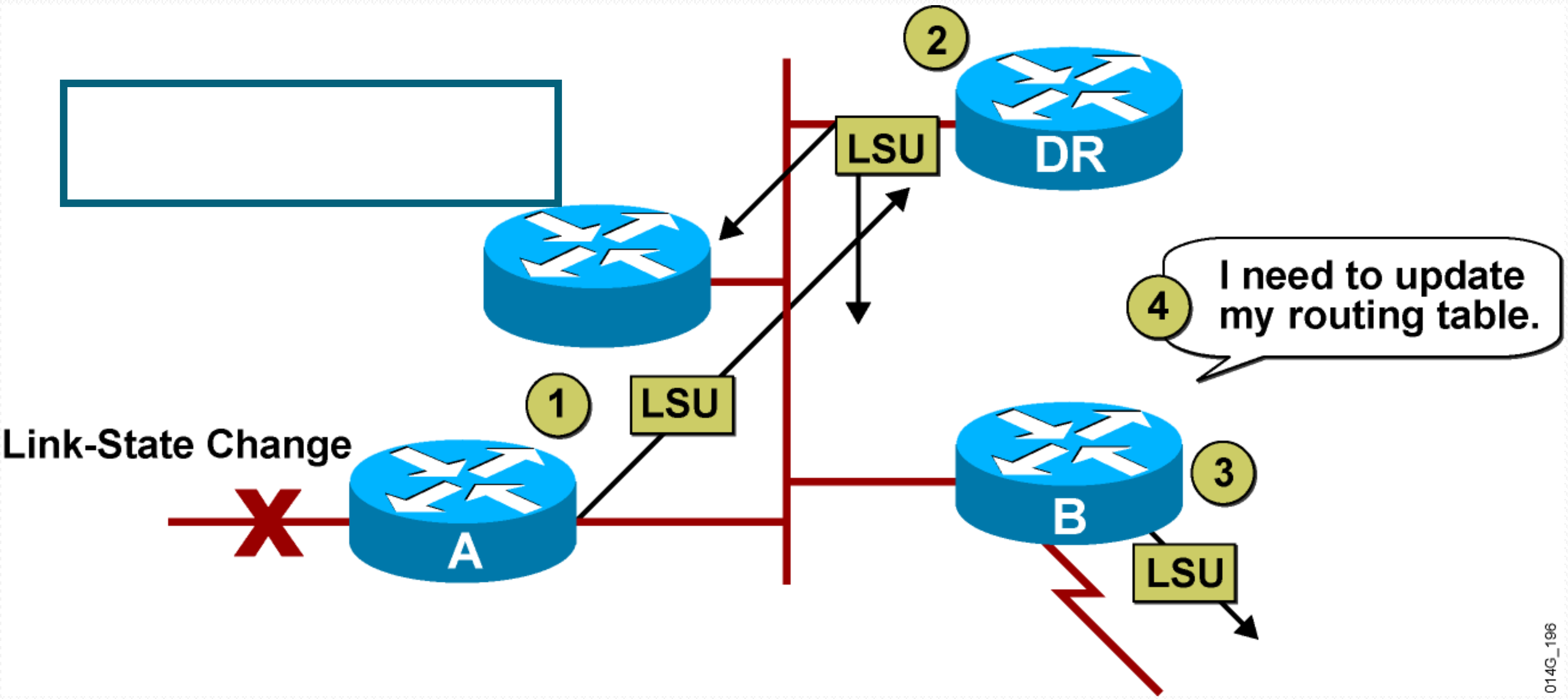
- **Router A notifies all OSPF DRs on 224.0.0.6**
- **DR notifies others on 224.0.0.5**

Maintaining Routing Information (Cont.)



- **Router A notifies all OSPF DRs on 224.0.0.6**
- **DR notifies others on 224.0.0.5**

Maintaining Routing Information



- **Router A notifies all OSPF DRs on 224.0.0.6**
- **DR notifies others on 224.0.0.5**

Configuring Basic OSPF: Single Area

Router(config)#

```
router ospf process-id
```

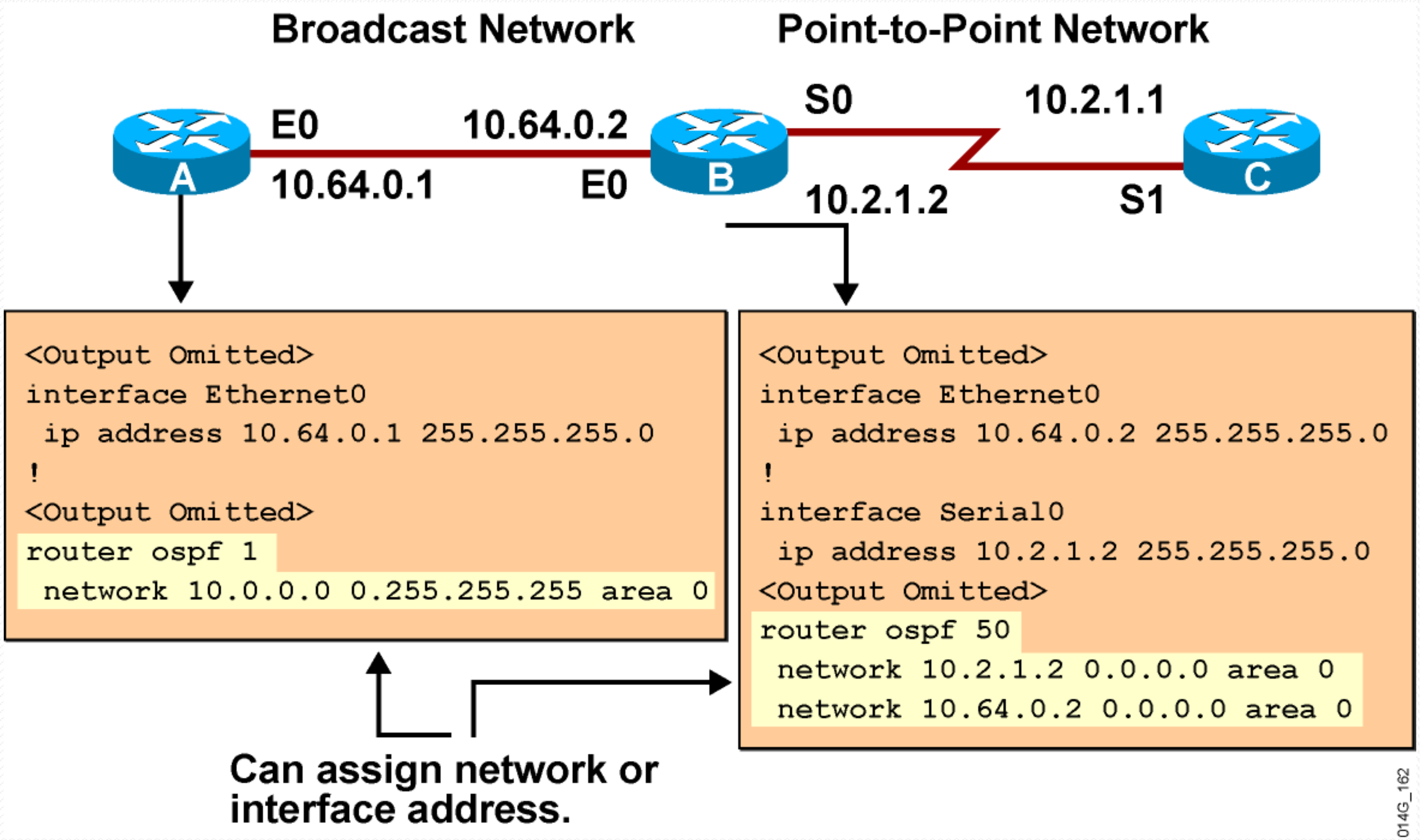
- **Turns on one or more OSPF routing processes in the IOS software.**

Router(config-router)#

```
network address inverse-mask area [area-id]
```

- **Router OSPF subordinate command that defines the interfaces (by network number) that OSPF will run on. Each network number must be defined to a specific area.**

Configuring OSPF on Internal Routers of a Single Area



Verifying OSPF Operation

Router#

```
show ip protocols
```

- **Verifies the configured IP routing protocol processes, parameters and statistics**

Router#

```
show ip route ospf
```

- **Displays all OSPF routes learned by the router**

Router#

```
show ip ospf interface
```

- **Displays the OSPF router ID, area ID and adjacency information**

Verifying OSPF Operation (Cont.)

```
Router#
show ip ospf
```

- **Displays the OSPF router ID, timers, and statistics**

```
Router#
show ip ospf neighbor [detail]
```

- **Displays information about the OSPF neighbors, including Designated Router (DR) and Backup Designated Router (BDR) information on broadcast networks**

The show ip route ospf Command

```
RouterA# show ip route ospf

 Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,

        B - BGP, D - EIGRP, EX - EIGRP external, O - OSPF,
        IA - OSPF inter area, E1 - OSPF external type 1,
        E2 - OSPF external type 2, E - EGP, i - IS-IS, L1 - IS-IS
        level-1, L2 - IS-IS level-2, * - candidate default

Gateway of last resort is not set
        10.0.0.0 255.255.255.0 is subnetted, 2 subnets
O       10.2.1.0 [110/10] via 10.64.0.2, 00:00:50, Ethernet0
```

The show ip ospf interface Command

```
RouterA# show ip ospf interface e0

Ethernet0 is up, line protocol is up
  Internet Address 10.64.0.1/24, Area 0
  Process ID 1, Router ID 10.64.0.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 10.64.0.2, Interface address 10.64.0.2
  Backup Designated router (ID) 10.64.0.1, Interface address 10.64.0.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.64.0.2  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

The show ip ospf neighbor Command

```
RouterB# show ip ospf neighbor

Neighbor ID     Pri    State         Dead Time      Address        Interface
10.64.1.1       1      FULL/BDR      00:00:31       10.64.1.1      Ethernet0
10.2.1.1        1      FULL/-        00:00:38       10.2.1.1       Serial0
```

show ip protocol

Displays parameters about timers, filters, metrics, networks, and other information for the entire router.

show ip route

Displays the routes known to the router and how they were learned. This is one of the best ways to determine connectivity between the local router and the rest of the internetwork.

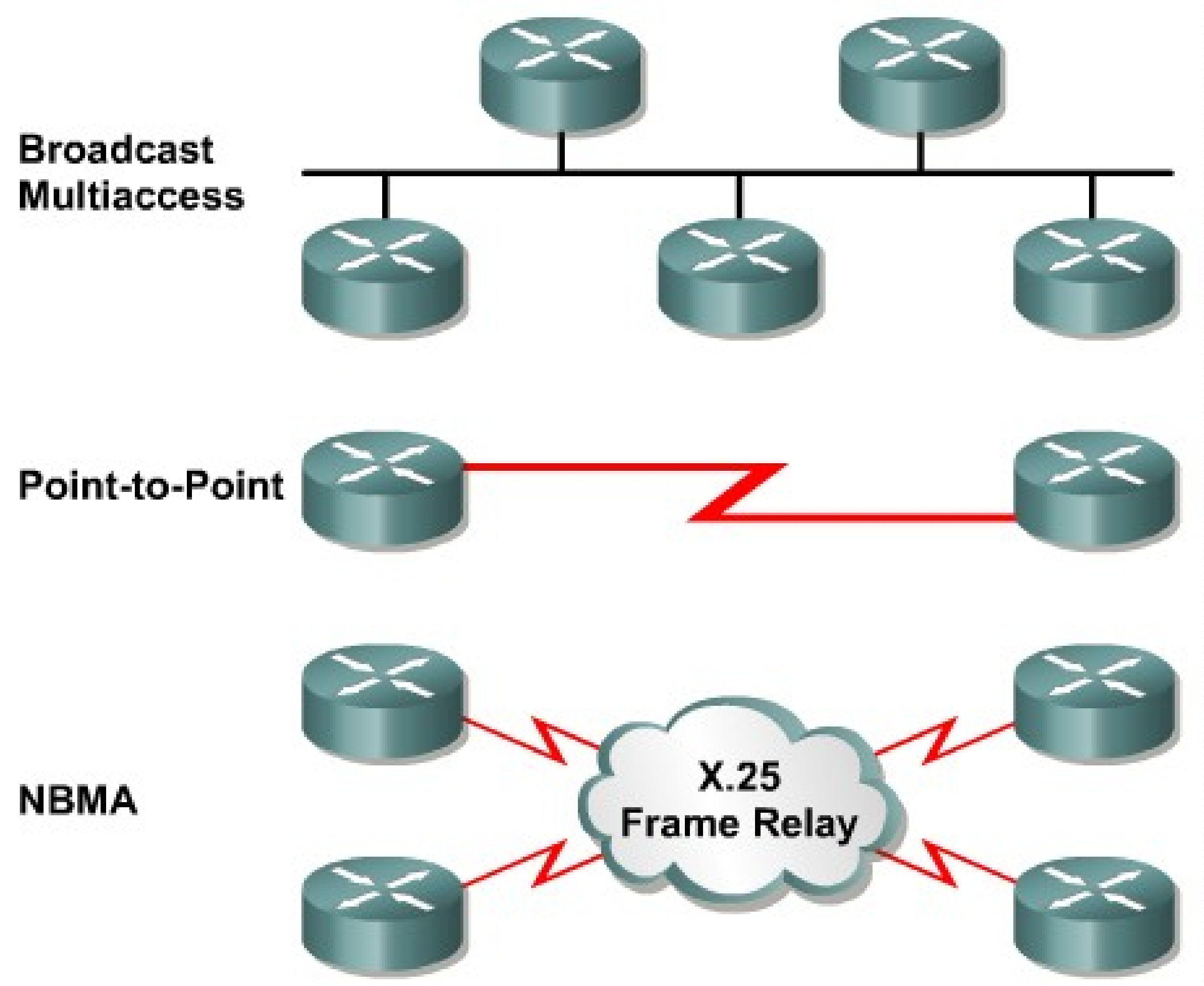
show ip ospf neighbor detail

Displays details list of neighbors, their priorities, and their state (for example: init, exstart, or full).

show ip ospf database

Displays the contents of the topological database maintained by the router. The command also shows the router ID and the OSPF process ID. A number of database types can be shown with this command using keywords. Refer to www.cisco.com for details about the keywords.

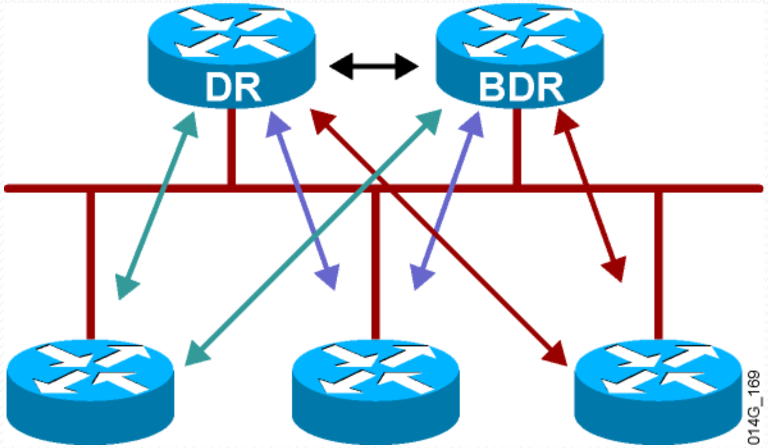
OSPF Network Types - 1



Point-to-Point Links

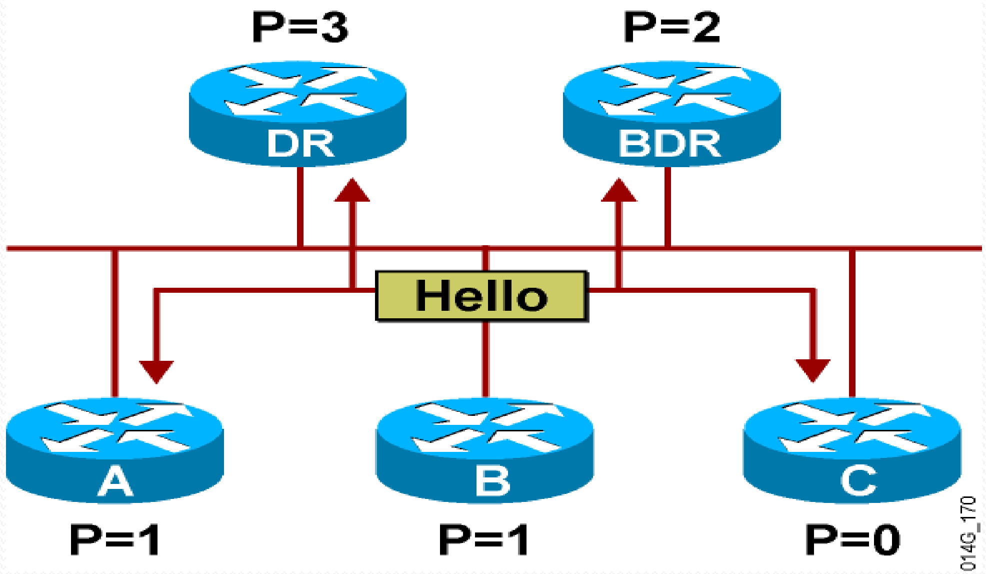
- Usually a serial interface running either PPP or HDLC
- May also be a point-to-point subinterface running Frame Relay or ATM
- No DR or BDR election required
- OSPF autodetects this interface type
- OSPF packets are sent using multicast 224.0.0.5

Multi-access Broadcast Network



- Generally LAN technologies like Ethernet and Token Ring
- DR and BDR selection required
- All neighbor routers form full adjacencies with the DR and BDR only
- Packets to the DR use 224.0.0.6
- Packets from DR to all other routers use 224.0.0.5

Electing the DR and BDR



- Hello packets are exchanged via IP multicast.
- The router with the highest OSPF priority is selected as the DR.
- Use the OSPF router ID as the tie breaker.
- The DR election is nonpreemptive.

Setting Priority for DR Election

```
Router(config-if)#
```

```
ip ospf priority number
```

- **This interface configuration command assigns the OSPF priority to an interface.**
- **Different interfaces on a router may be assigned different values.**
- **The default priority is 1. The range is from 0 to 255.**
- **0 means the router is a DROTHER; it can't be the DR or BDR.**

OSPF Network Types - 2

Network Type	Characteristics	DR Election?
Broadcast multiaccess	Ethernet, Token Ring, or FDDI	Yes
Nonbroadcast multiaccess	Frame Relay, X.25, SMDS	Yes
Point-to-point	PPP, HDLC	No
Point-to-multipoint	Configured by an administrator	No

Creation of Adjacencies

```
RouterA# debug ip ospf adj

Point-to-point interfaces coming up:  No election
%LINK-3-UPDOWN: Interface Serial1, changed state to up
OSPF: Interface Serial1 going Up
OSPF: Rcv hello from 192.168.0.11 area 0 from Serial1 10.1.1.2
OSPF: End of hello processing
OSPF: Build router LSA for area 0, router ID 192.168.0.10
OSPF: Rcv DBD from 192.168.0.11 on Serial1 seq 0x20C4 opt 0x2 flag 0x7 len 32
state INIT
OSPF: 2 Way Communication to 192.168.0.11 on Serial1, state 2WAY
OSPF: Send DBD to 192.168.0.11 on Serial1 seq 0x167F opt 0x2 flag 0x7 len 32
OSPF: NBR Negotiation Done. We are the SLAVE
OSPF: Send DBD to 192.168.0.11 on Serial1 seq 0x20C4 opt 0x2 flag 0x2 len 72
```

Creation of Adjacencies (Cont.)

```
RouterA# debug ip ospf adj

Ethernet interface coming up: Election
OSPF: 2 Way Communication to 192.168.0.10 on Ethernet0, state 2WAY
OSPF: end of Wait on interface Ethernet0
OSPF: DR/BDR election on Ethernet0
OSPF: Elect BDR 192.168.0.12
OSPF: Elect DR 192.168.0.12
       DR: 192.168.0.12 (Id)   BDR: 192.168.0.12 (Id)
OSPF: Send DBD to 192.168.0.12 on Ethernet0 seq 0x546 opt 0x2 flag 0x7 len 32
<…>
OSPF: DR/BDR election on Ethernet0
OSPF: Elect BDR 192.168.0.11
OSPF: Elect DR 192.168.0.12
       DR: 192.168.0.12 (Id)   BDR: 192.168.0.11 (Id)
```