

RIP and routing dynamically



Administrative Distance

If multiple paths to a destination: the path installed in the routing table is the one with the lowest Administrative Distance (AD)

Route Source	Administrative Distance
Directly connected	0
Static route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

Routing Table Sources

The **show ip route**: content of the routing table:

- **Local route interfaces** - Added to the routing table when an interface is configured. (displayed in IOS 15 or newer)
- **Directly connected interfaces** - Added to the routing table when an interface is configured and active.
- **Static routes** - Added when a route is manually configured and the exit interface is active.
- **Dynamic routing protocol** - Added when dynamic routing protocol learns networks.

The Routing Table

Remote Network Routing Entries

Interpreting the entries in the routing table.

D 10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0

Legend

- Identifies how the network was learned by the router.
- Identifies the destination network.
- Identifies the administrative distance (trustworthiness) of the route source.
- Identifies the metric to reach the remote network.
- Identifies the next-hop IP address to reach the remote network.
- Identifies the amount of elapsed time since the network was discovered.
- Identifies the outgoing interface on the router to reach the destination network.

Why Use Dynamic Routing?

- Initial configuration and maintenance is time-consuming.
- Configuration is error-prone, especially in large networks.
- Administrator intervention is required to maintain changing route information.
- Does not scale well with growing networks; maintenance becomes cumbersome.
- Requires complete knowledge of the whole network for proper implementation.

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

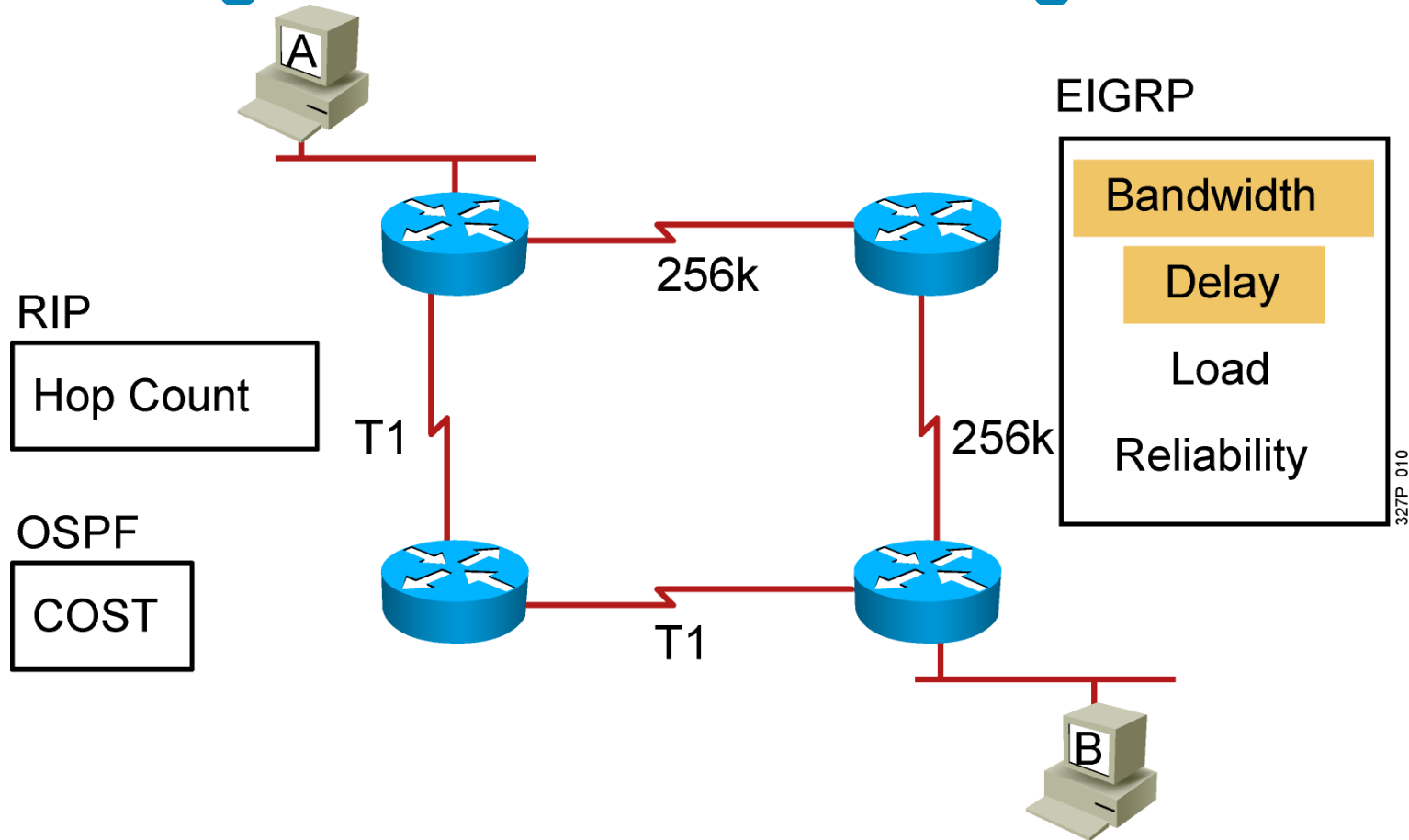
Main components of dynamic routing protocols

- **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.

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.

Selecting the Best Route Using Metrics

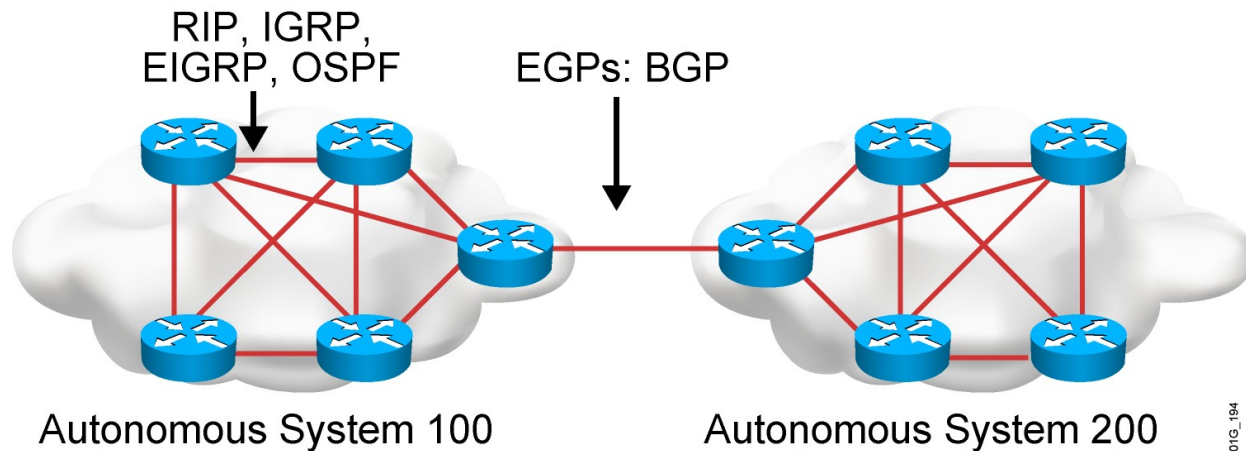


Achieving Convergence

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**.

Autonomous Systems: Interior or Exterior Routing Protocols

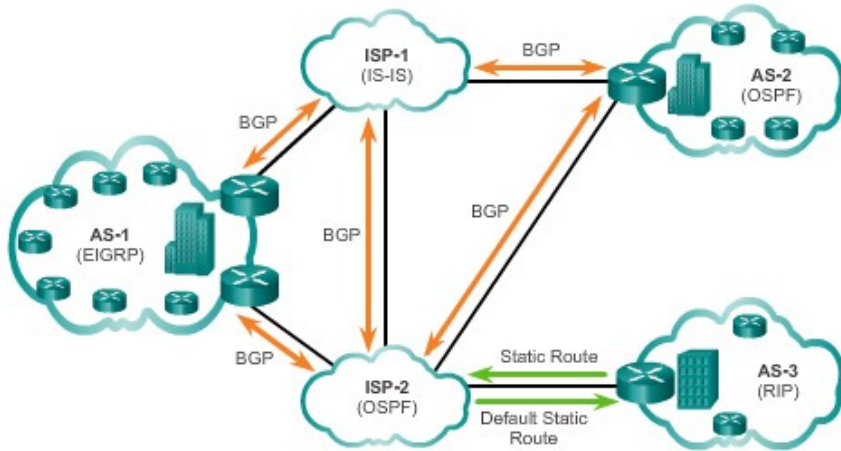


- An autonomous system is a collection of networks under a common administrative domain.
- IGPs operate within an autonomous system.
- EGPs connect different autonomous systems.

Types of Routing Protocols

IGP and EGP Routing Protocols

IGP versus EGP Routing Protocols



Interior Gateway Protocols (IGP) -

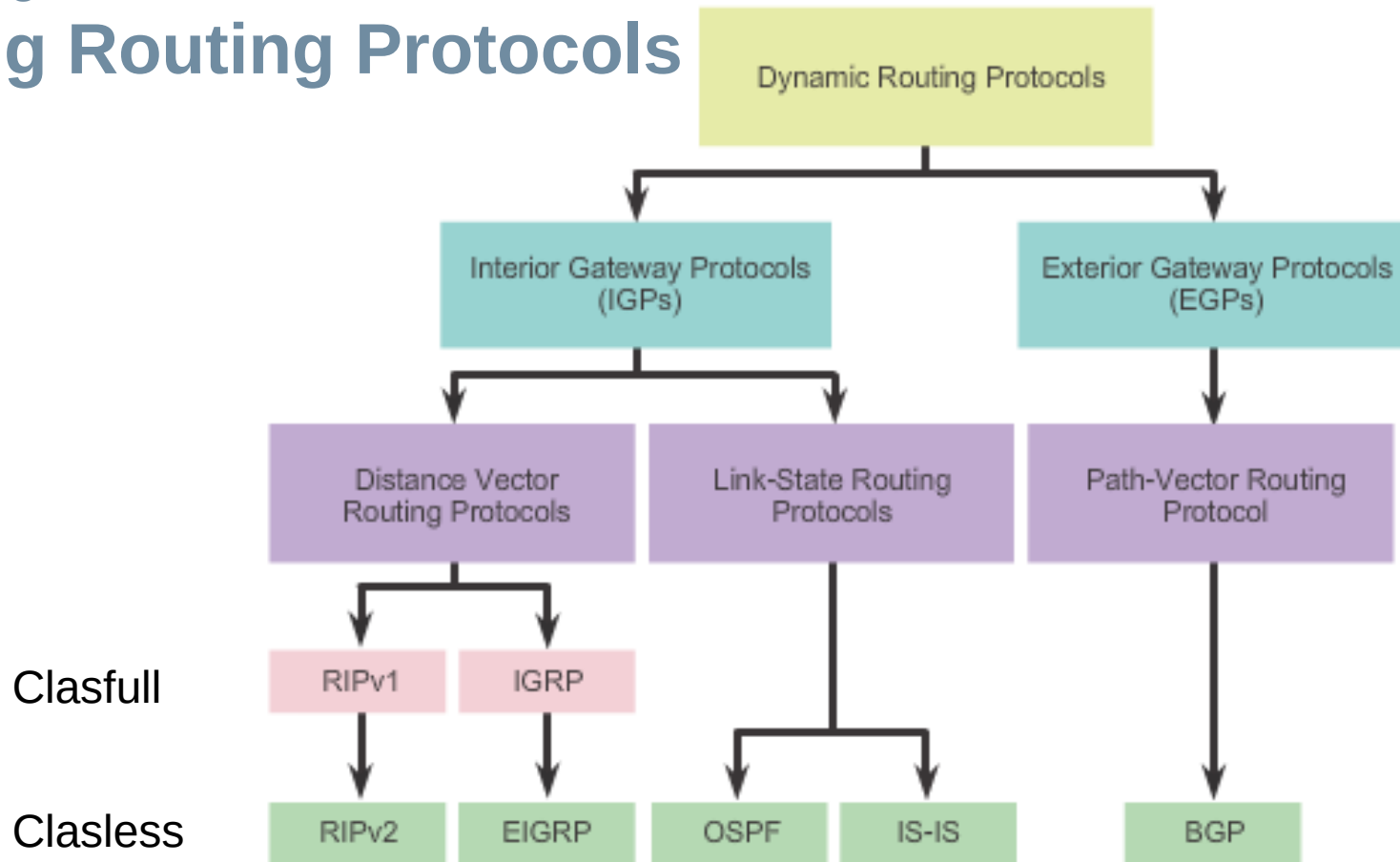
- Used for routing within an AS
- RIP, EIGRP, OSPF, IS-IS

Exterior Gateway Protocols (EGP) -

- Used for routing between AS
- BGP

Types of Routing Protocols

Classifying Routing Protocols



Distance Vector Routing Protocols

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

RIP uses the Bellman-Ford algorithm as its routing algorithm.

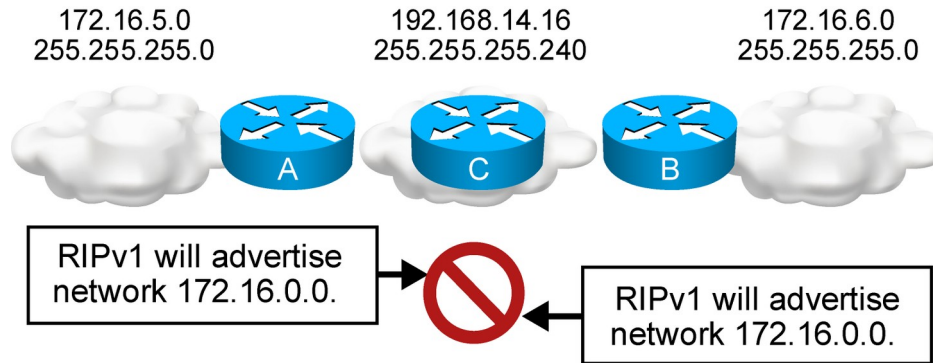
IGRP and EIGRP use the Diffusing Update Algorithm (DUAL) routing algorithm developed by Cisco.

Types of Routing Protocols

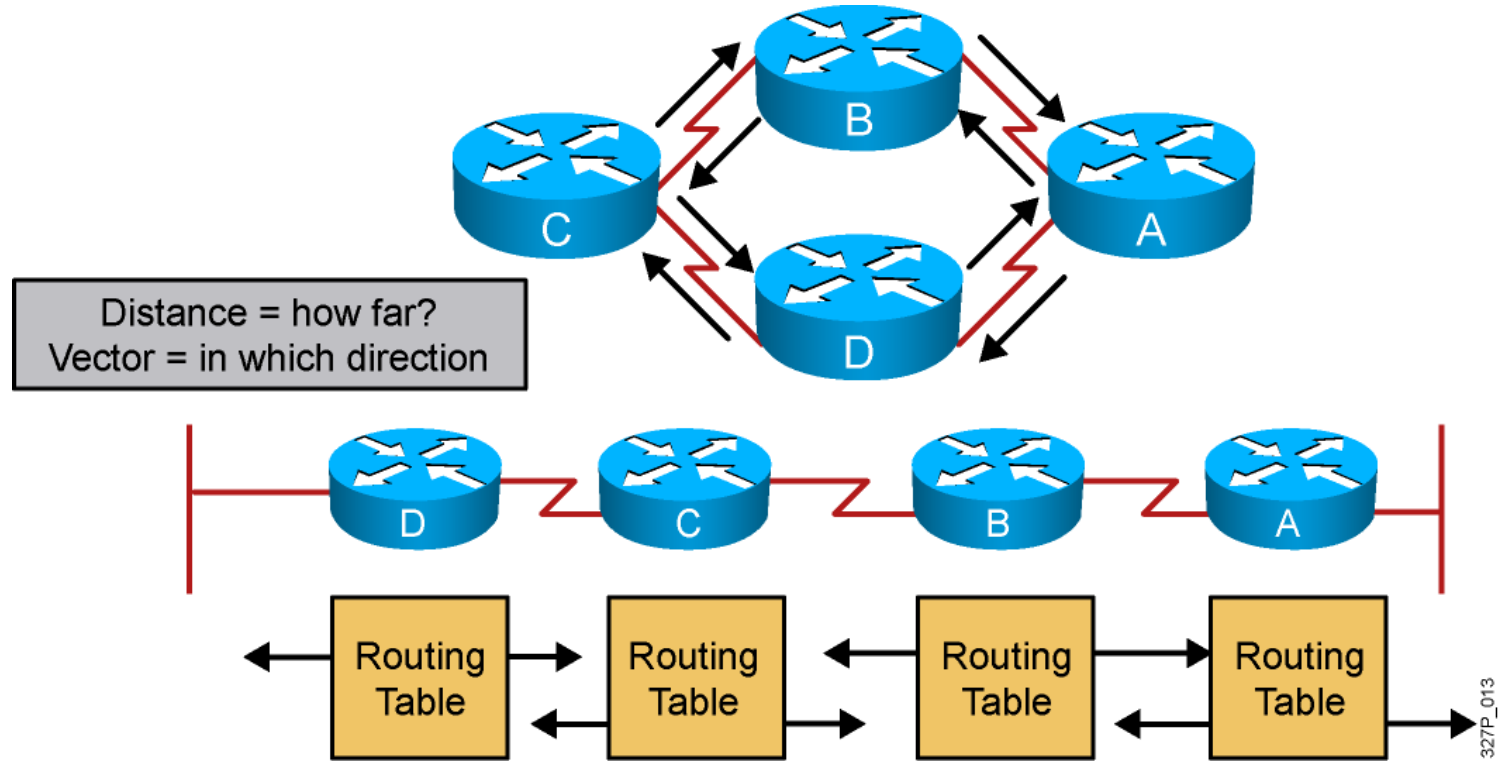
Classful Routing Protocols

Classful routing protocols **do not send** subnet mask information in their routing updates:

- Only old protocols: **RIPv1 and IGRP are classful.**
- Within the same network, consistency of the subnet masks is assumed. **(they do not support VLSM)**
- Create **problems in discontinuous networks.**

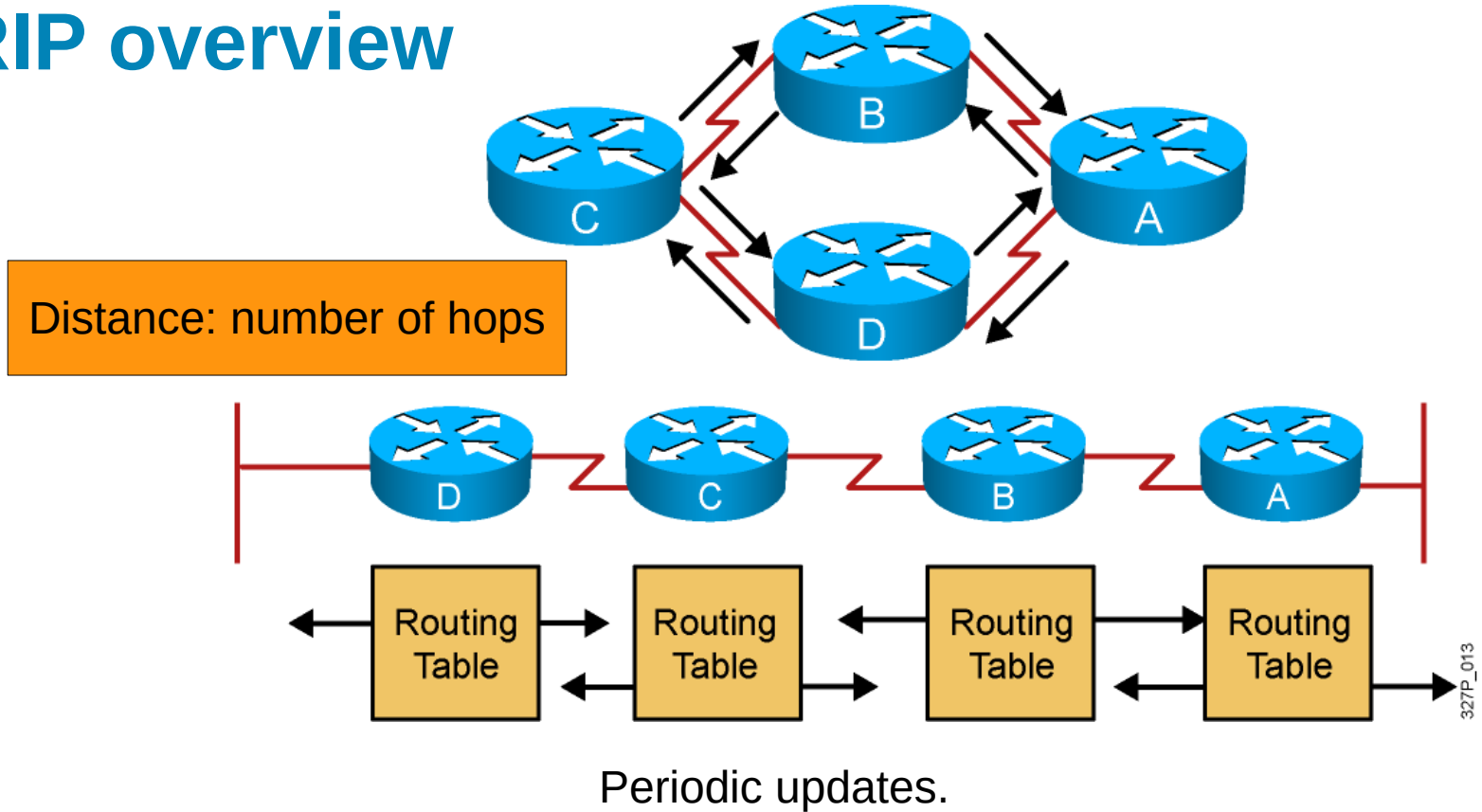


Distance Vector Routing Protocols

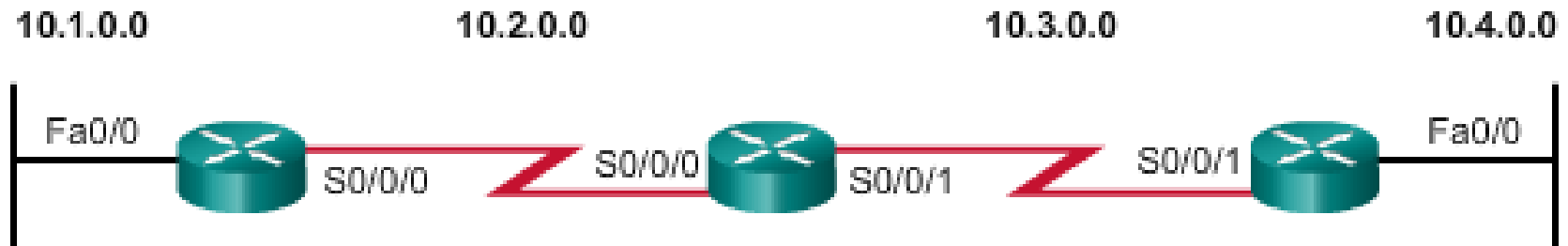


Routers pass periodic copies of their routing table to neighboring routers and accumulate distance vectors.

RIP overview



Cold Start



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

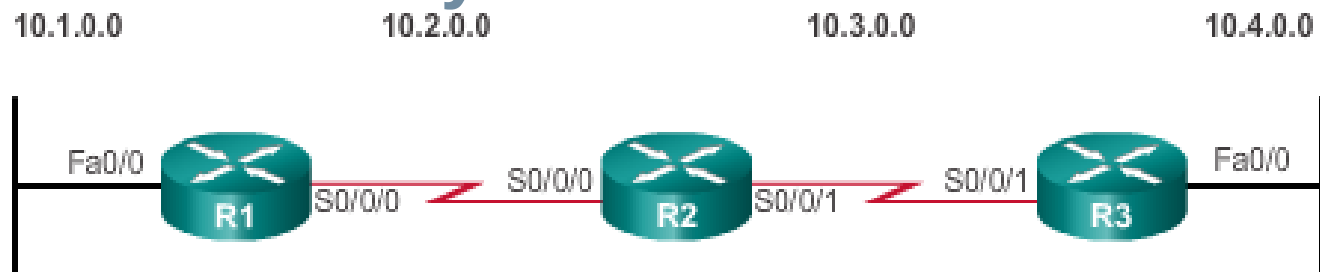
Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0

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

RIPv2

Network Discovery

Initial Exchange



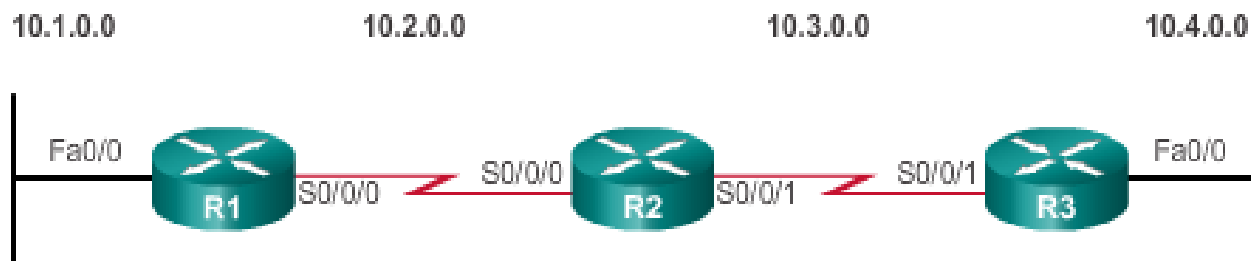
Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1

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

Network Discovery

Next Update

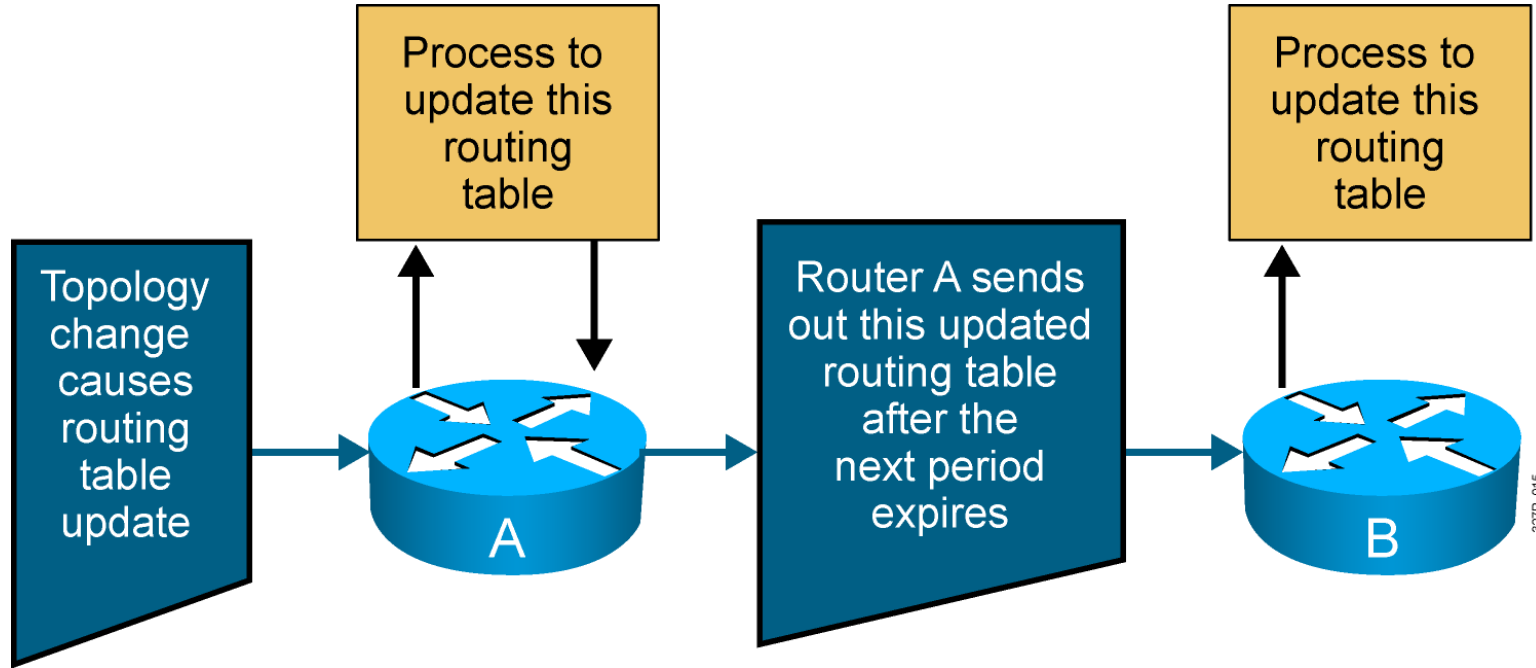


Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

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

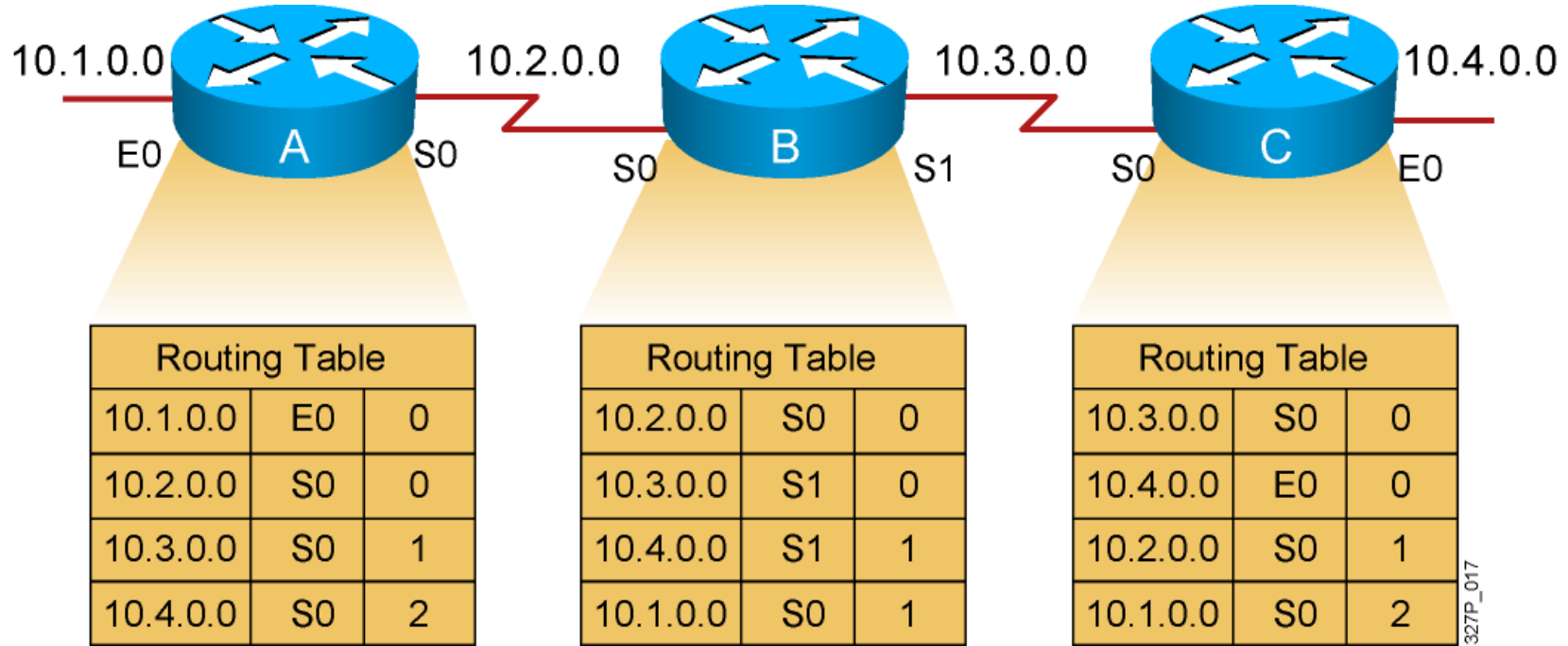
Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

Maintaining Routing Information

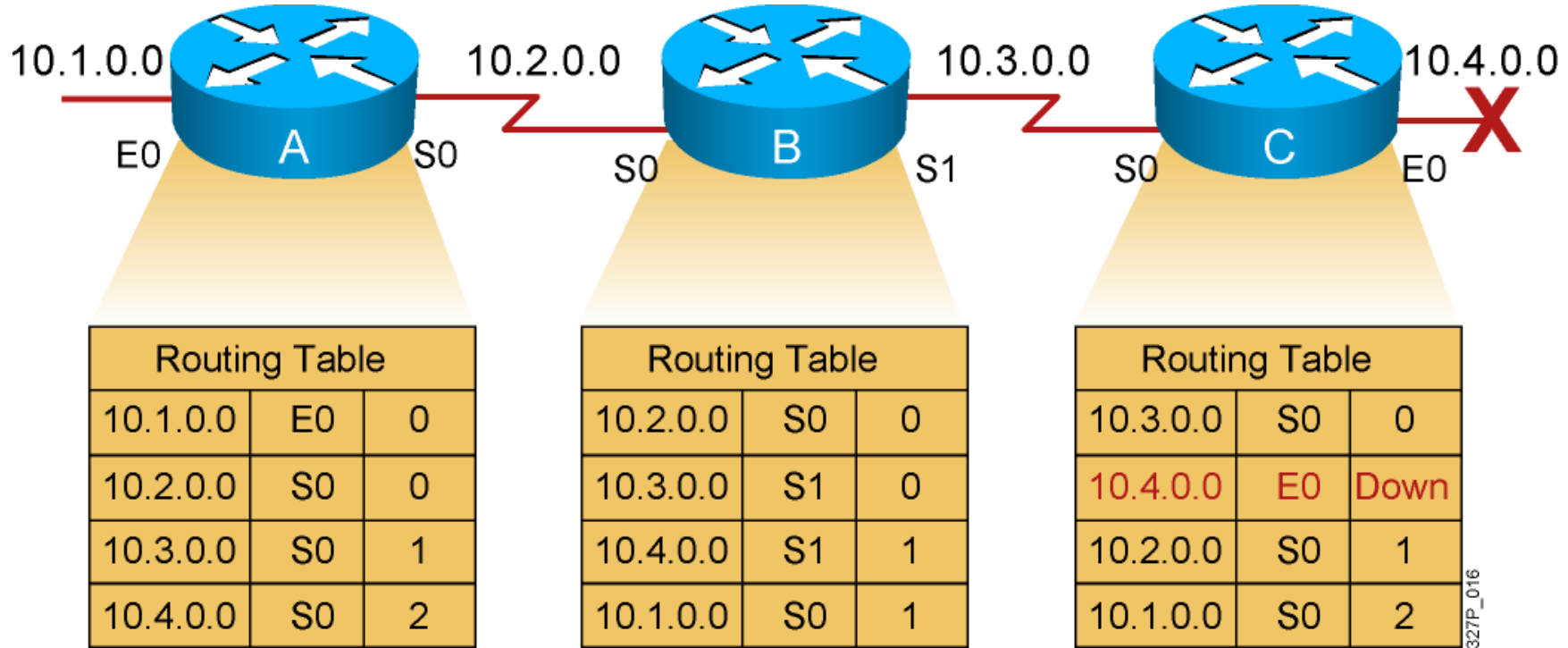


Updates propagate hop by hop from router to router.

Inconsistent Routing Entries: Counting to Infinity and Routing Loops

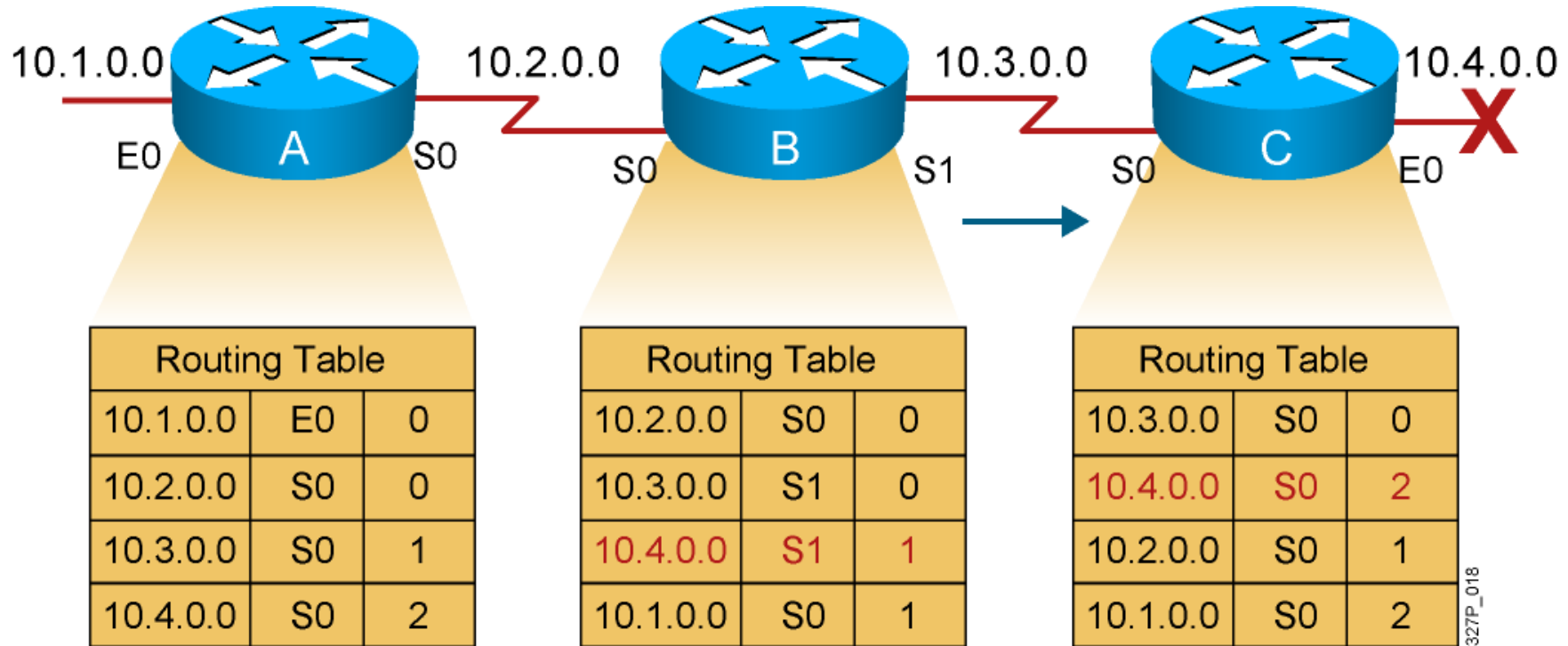


Counting to Infinity



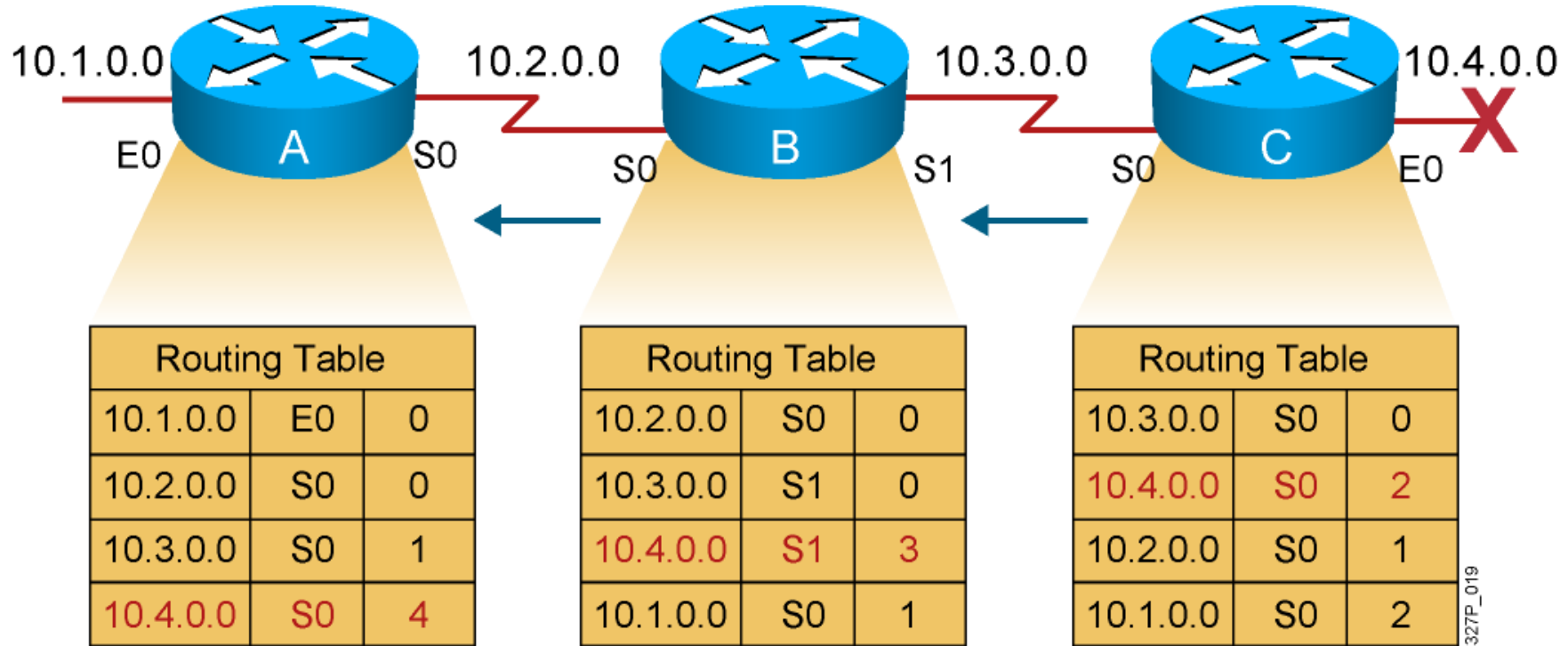
Slow convergence produces inconsistent routing.

Counting to Infinity (Cont.)



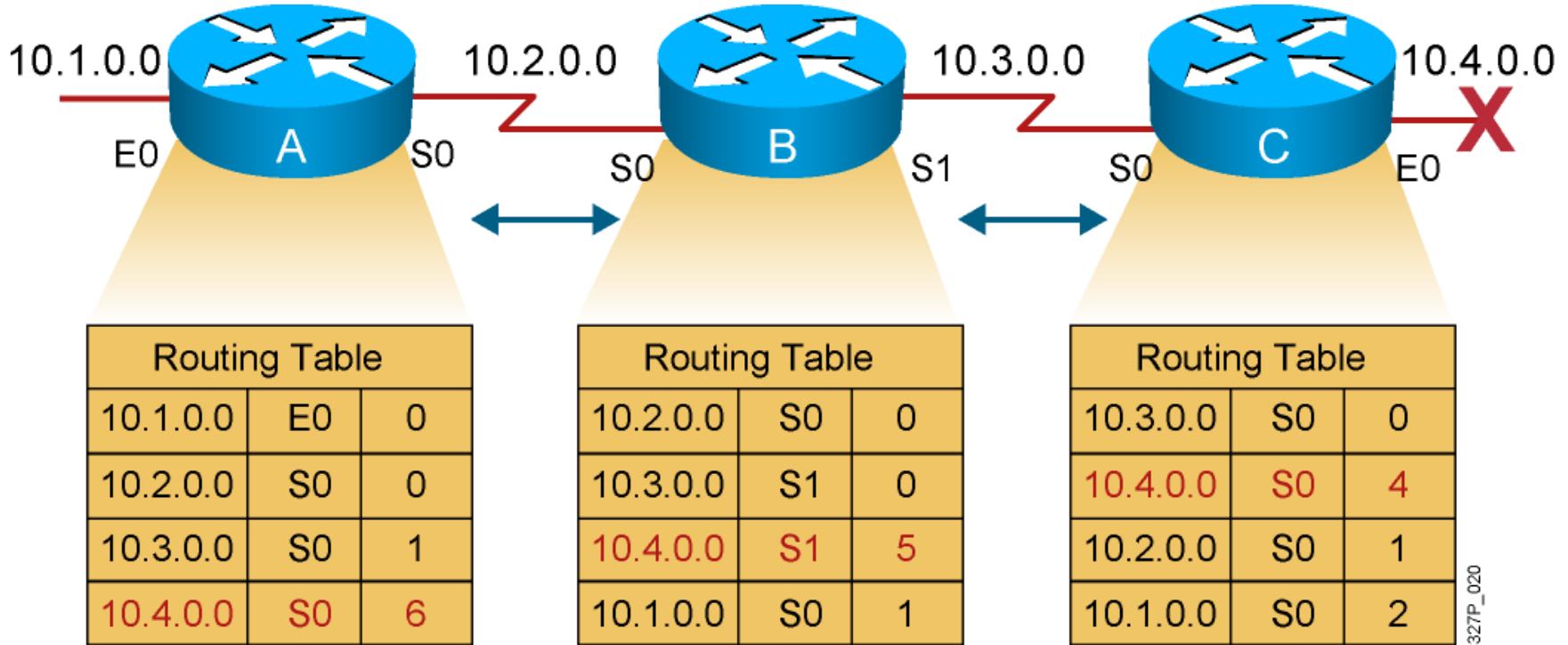
Router C concludes that the best path to network 10.4.0.0 is through router B.

Counting to Infinity (Cont.)



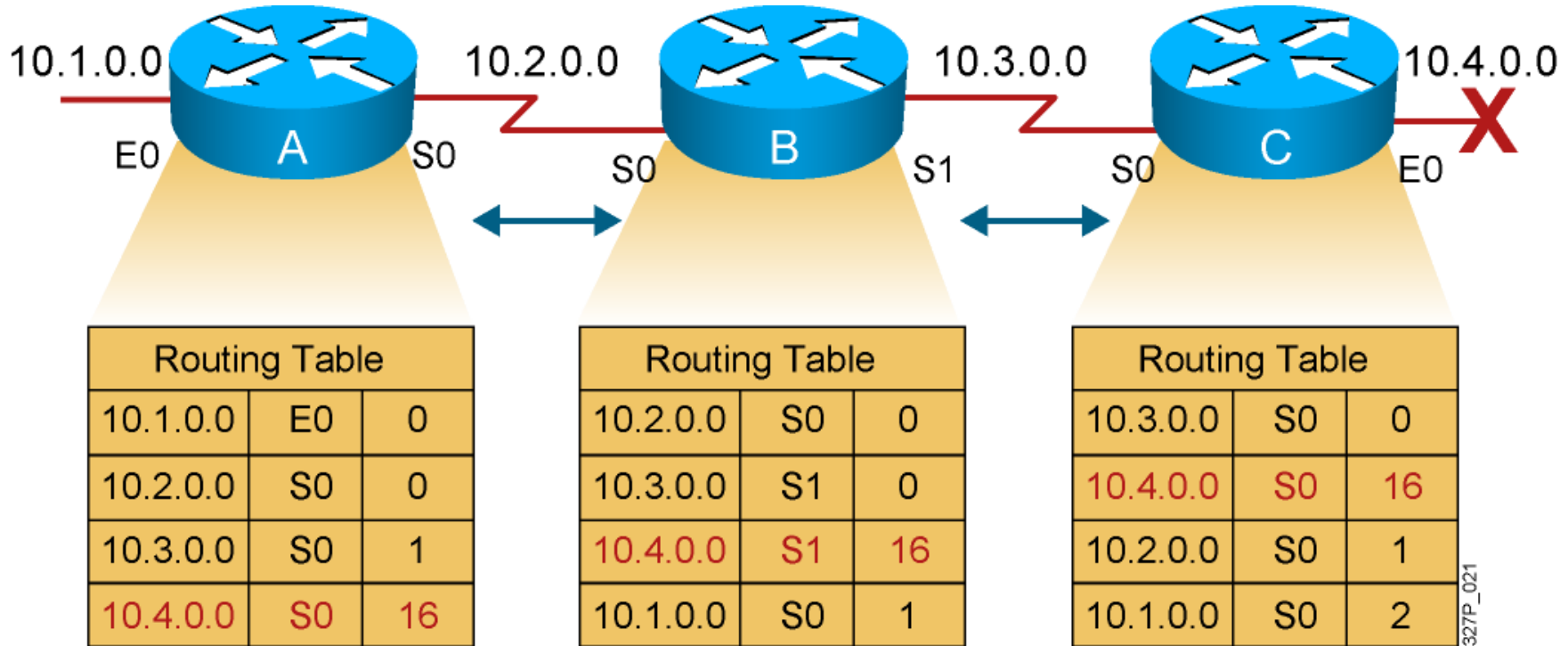
Router A updates its table to reflect the new but erroneous hop count.

Counting to Infinity (Cont.)



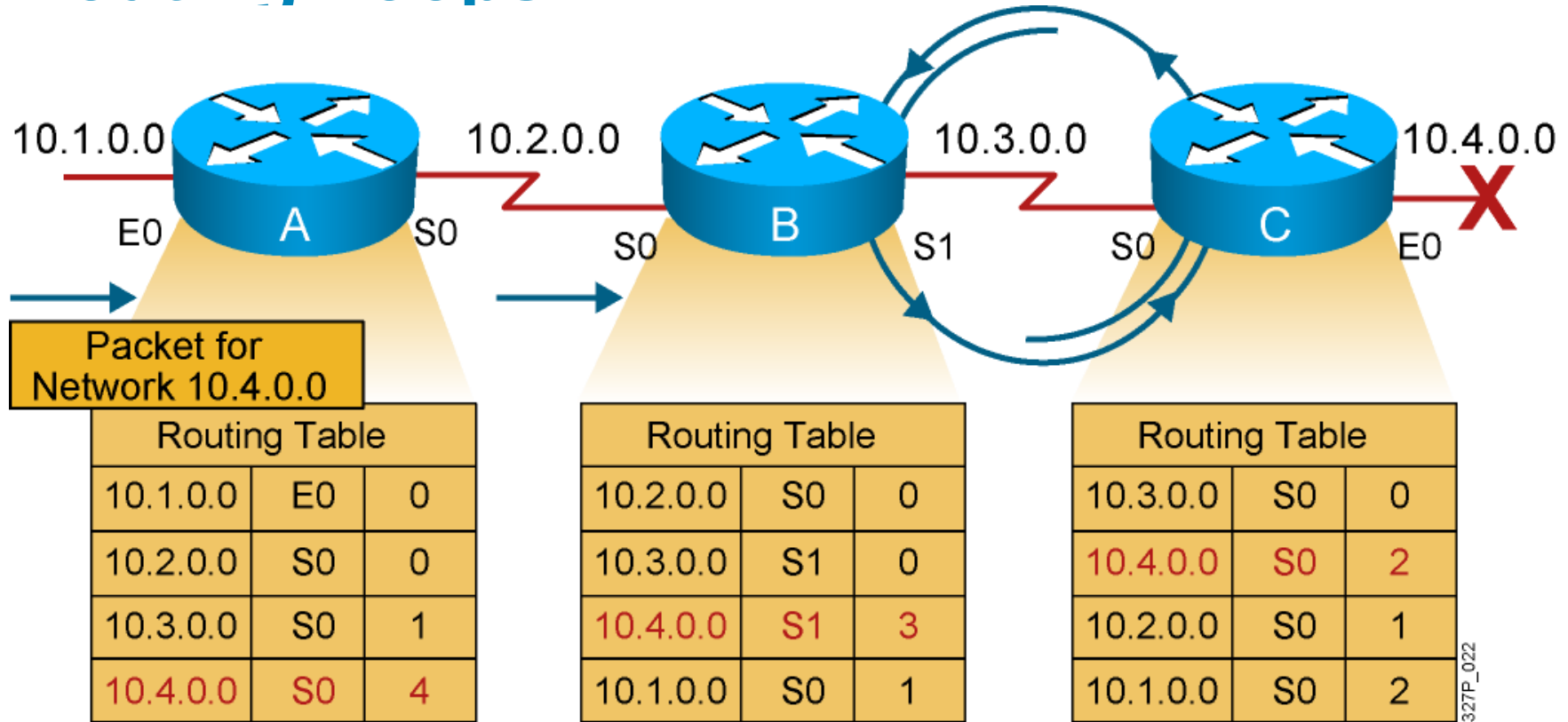
The hop count for network 10.4.0.0 counts to infinity.

Solution to Counting to Infinity: Defining a Maximum



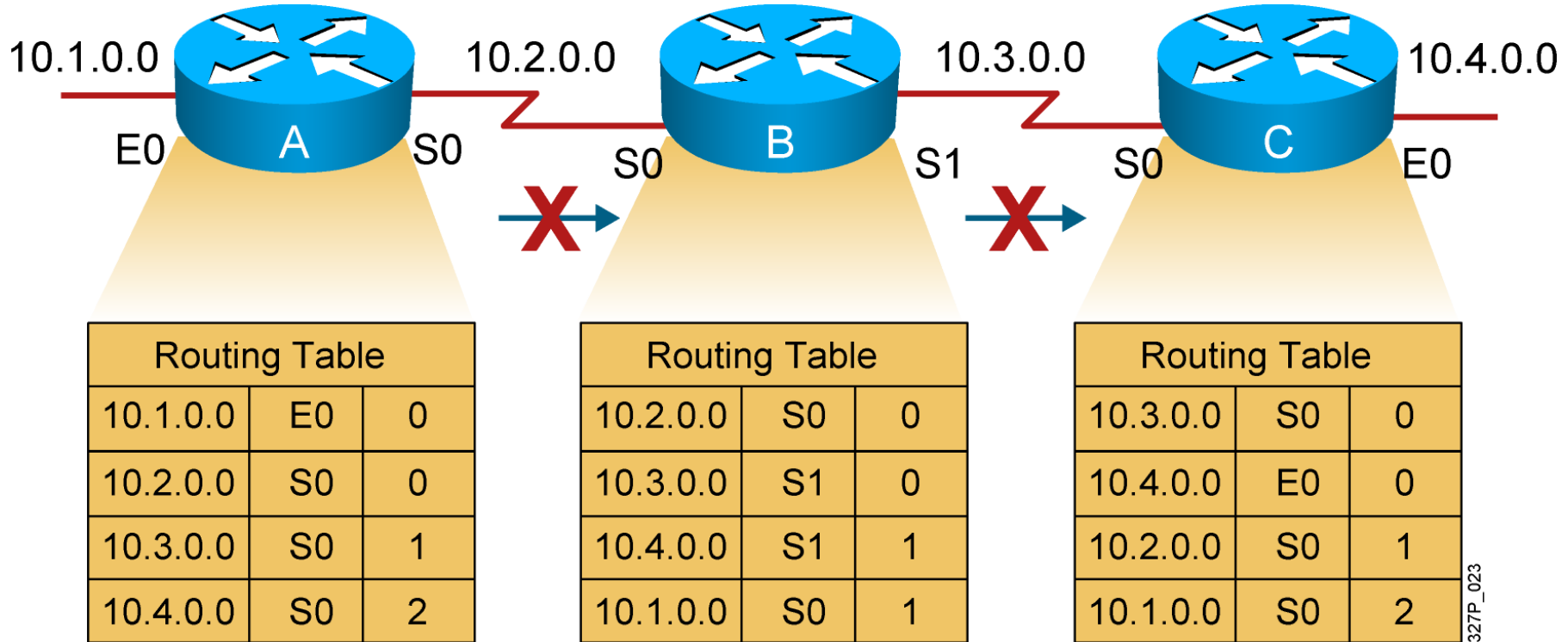
A limit is set on the number of hops to prevent infinite loops.

Routing Loops



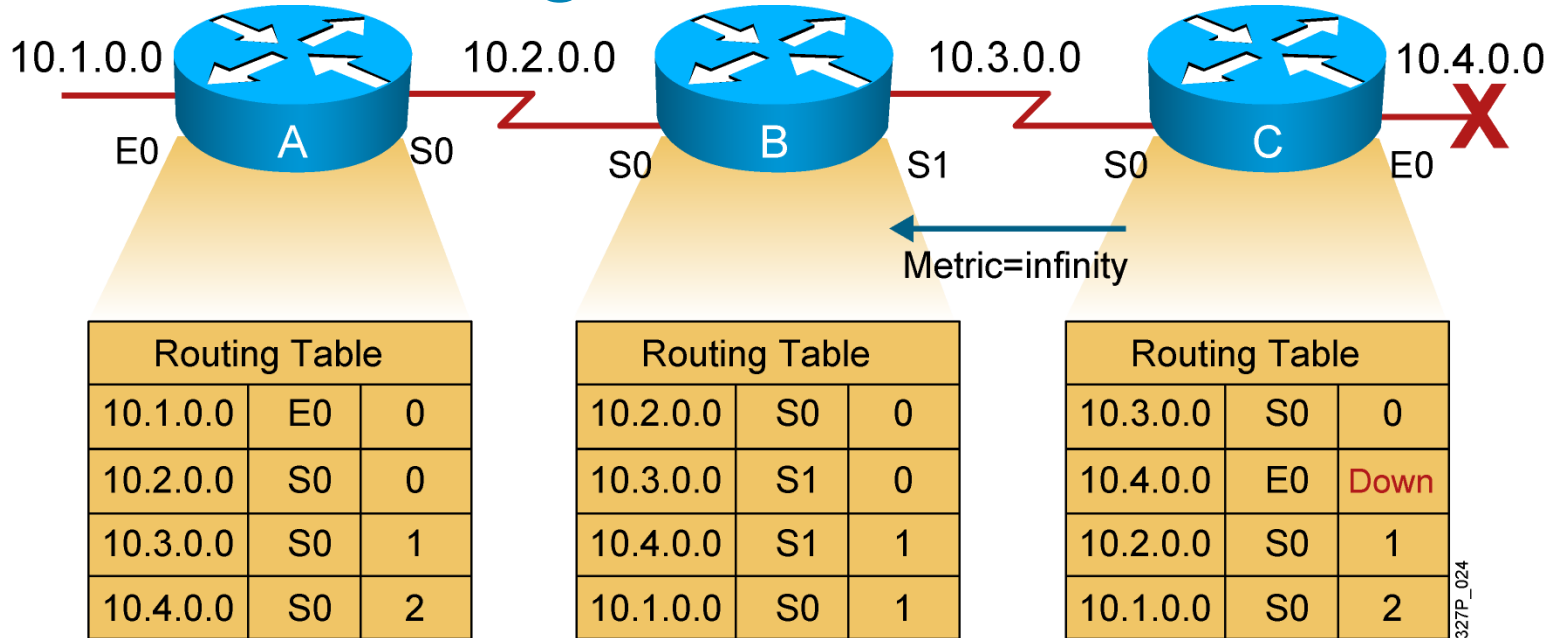
Packets for network 10.4.0.0 bounce (loop) between routers B and C.

Solution to Routing Loops: Split Horizon



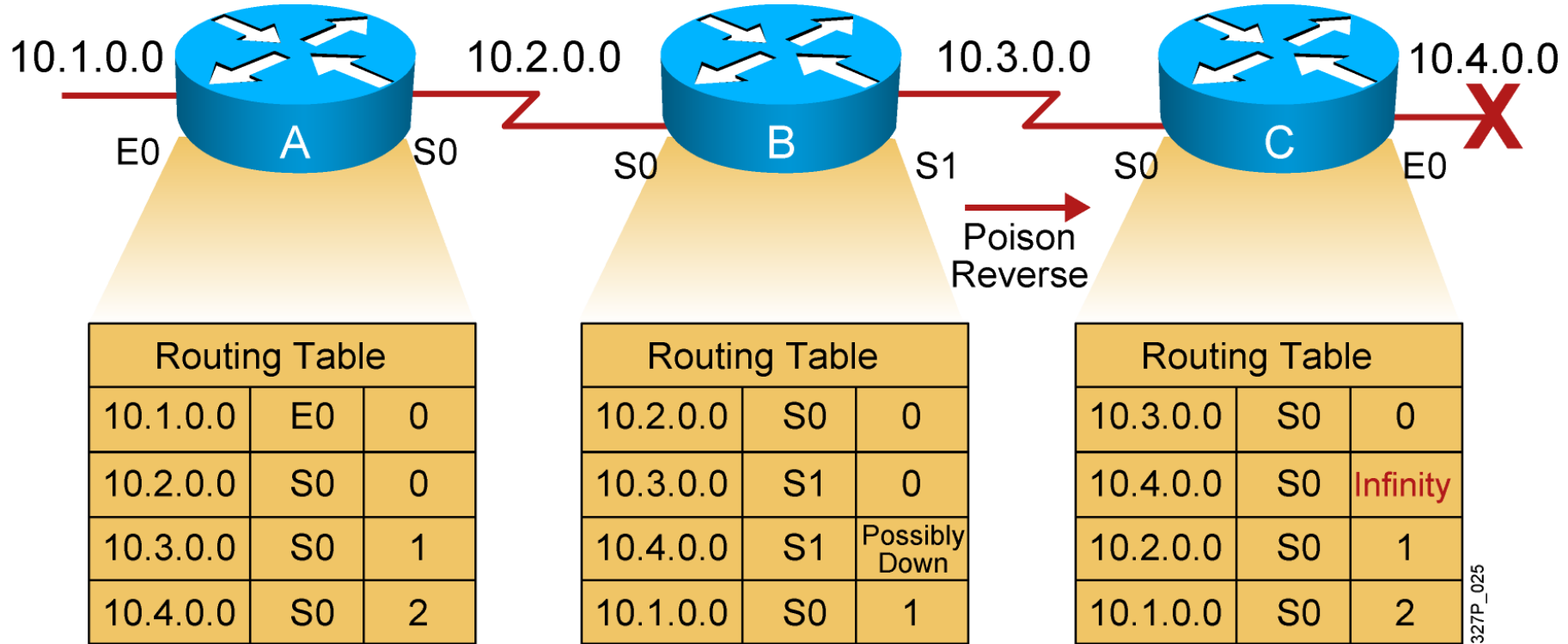
It is never useful to send information about a route back in the direction from which the original information came.

Solution to Routing Loops: Route Poisoning



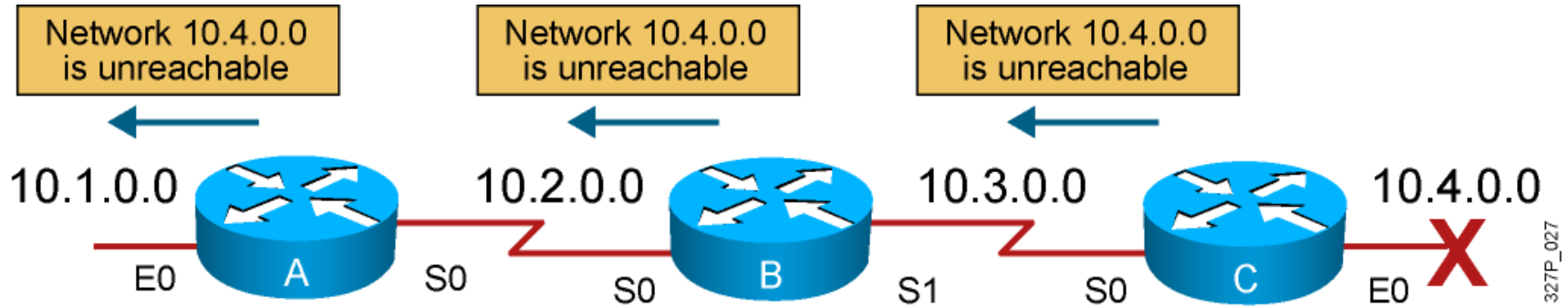
Routers advertise the distance of routes
that have gone down to infinity.

Solution to Routing Loops: Poison Reverse



Poison reverse is sent despite the split horizon.

Triggered Updates



The router sends updates when a change in its routing table occurs.

RIP Configuration

```
RouterX(config)# router rip
```

- Starts the RIP routing process

```
RouterX(config-router)# version 2
```

- Enables RIP version 2

```
RouterX(config-router)# network network-number
```

- Selects participating attached networks
- Requires a **major classful network number**
 - Otherwise changes the input to the classful number
 - 10.10.10.0 → 10.0.0.0

network command

- Selects all interfaces that have an IP address that falls within the range of the **classful** network command parameter
 - 1) All networks configured on these interfaces are **advertised**
 - 2) RIP updates are **sent** on these interfaces.
 - 3) RIP updates are **received** on these interfaces.

Configuring the RIP Protocol

Examining RIP Settings

```
R2#show ip route rip
```

```
R      192.168.10.0/24 [120/1] via 192.168.12.1, 00:00:07, FastEthernet0/0
```

```
R1#debug ip rip
```

```
RIP: sending v2 update to 224.0.0.9 via FastEthernet0/0 (192.168.12.1)
```

```
RIP: build update entries
```

```
      192.168.10.0/24 via 0.0.0.0, metric 1, tag 0
```

```
RIP: sending v2 update to 224.0.0.9 via FastEthernet0/1 (192.168.10.254)
```

```
RIP: build update entries
```

```
      192.168.12.0/24 via 0.0.0.0, metric 1, tag 0
```

Configuring the RIP Protocol

Examining RIP Settings

R1#show ip protocols

...

Routing Protocol is "rip"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Sending updates every 30 seconds, next due in 20 seconds

Invalid after 180 seconds, hold down 180, flushed after 240

Redistributing: rip

Default version control: send version 2, receive version 2

Interface	Send	Recv	Triggered RIP	Key-chain
-----------	------	------	---------------	-----------

FastEthernet0/0	2	2		
-----------------	---	---	--	--

Automatic network summarization is not in effect

Maximum path: 4

Routing for Networks:

192.168.10.0

192.168.12.0

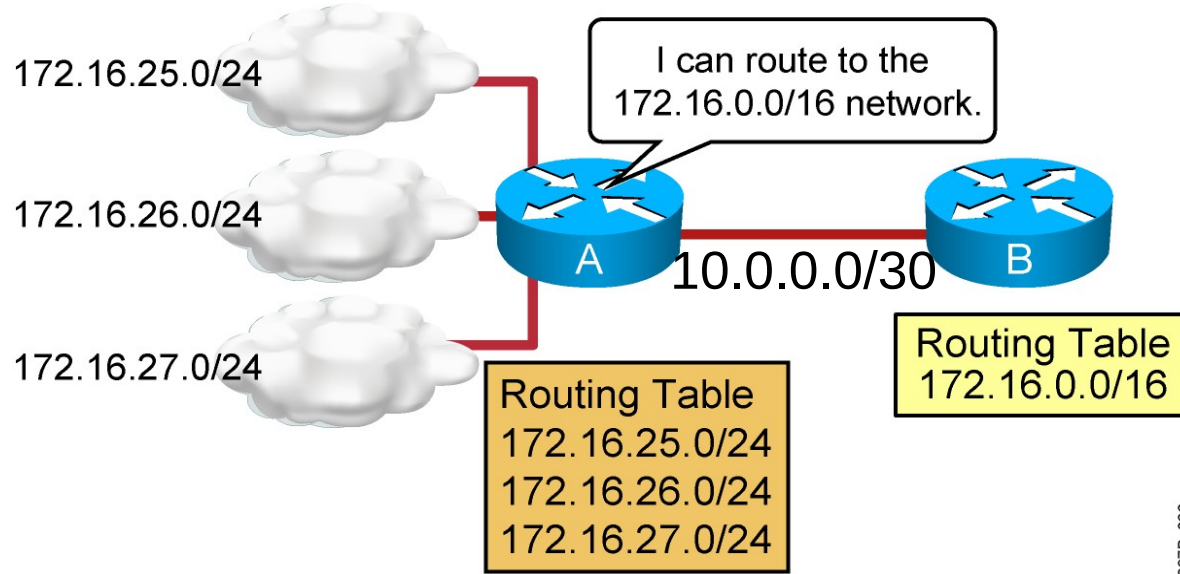
Passive Interface(s):

Routing Information Sources:

Gateway	Distance	Last Update
---------	----------	-------------

Distance: (default is 120)

Autosummarization



327P_036

- Autosummarization: RIPv1, RIPv2 automatically summarizes networks at major network boundaries by default.

Disabling Auto Summarization

- To cancel automatic summarization, use the **no auto-summary** router configuration mode command.
- This command has no effect when using RIPv1.
- When automatic summarization has been disabled, RIPv2 no longer summarizes networks to their classful address at boundary routers. RIPv2 now includes all subnets and their appropriate masks in its routing updates.

```
R1#show ip protocols
```

```
...
```

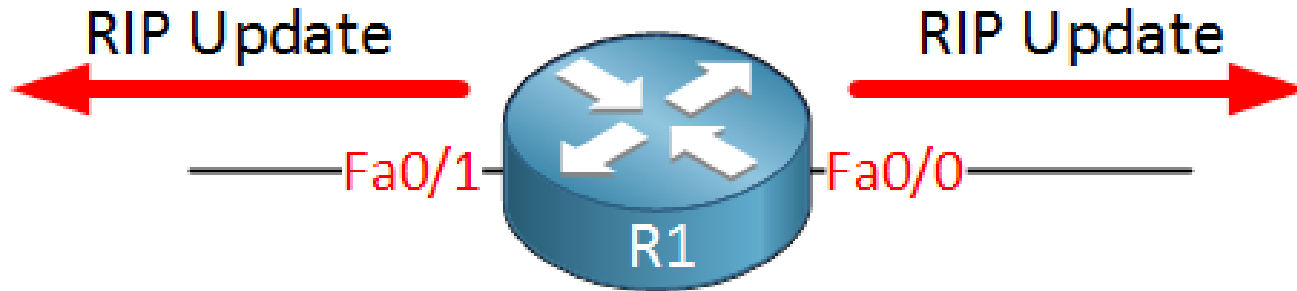
```
Routing Protocol is "rip"
```

```
...
```

```
Automatic network summarization is not in effect
```

```
...
```

Configuring Passive Interfaces



```
R1(config)#router rip
```

```
R1(config-router)#passive-interface Fa0/1
```

```
R1#show ip protocols
```

...

```
Routing Protocol is "rip"
```

...

```
Passive Interface(s):  
FastEthernet0/1
```

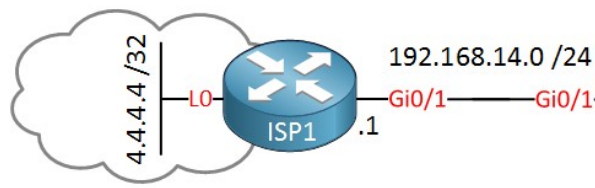
...

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

- Wasted Bandwidth
- Wasted Resources
- **Security Risk**

Configuring the RIP Protocol

Propagating a Default Route



```
R1(config)#router rip
```

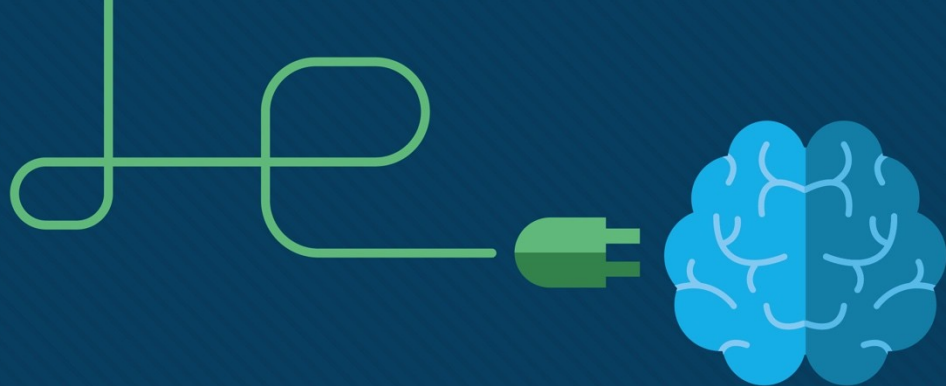
```
R1(config-router)#default-information originate
```

```
R2#show ip route rip
```

Gateway of last resort is 192.168.12.1 to network 0.0.0.0

```
R* 0.0.0.0/0 [120/1] via 192.168.12.1, 00:00:26, GigabitEthernet0/1
```

```
R 192.168.13.0/24 [120/1] via 192.168.12.1, 00:00:26, GigabitEthernet0/1
```

Module 12: IPv6 Addressing

Introduction to Networks v7.0
(ITN)



Module Objectives

Module Title: IPv6 Addressing

Module Objective: Implement an IPv6 Addressing scheme.

Topic Title	Topic Objective
IPv4 Issues ✓	Explain the need for IPv6 addressing.
IPv6 Address Representation ✓	Explain how IPv6 addresses are represented.
IPv6 Address Types	Compare types of IPv6 network addresses.
GUA and LLA Static Configuration » Lab	Explain how to Configure static global unicast and link-local IPv6 network addresses.
Dynamic Addressing for IPv6 GUAs » CCNA2	Explain how to configure global unicast addresses dynamically.

12.3 IPv6 Address Types

IPv6 Address Types

Unicast, Multicast, Anycast

There are three broad categories of IPv6 addresses:

- **Unicast** – Unicast uniquely identifies an interface on an IPv6-enabled device.
- **Multicast** – Multicast is used to send a single IPv6 packet to multiple destinations.
- **Anycast** – This is any IPv6 unicast address that can be assigned to multiple devices. A packet sent to an anycast address is routed to the nearest device having that address.

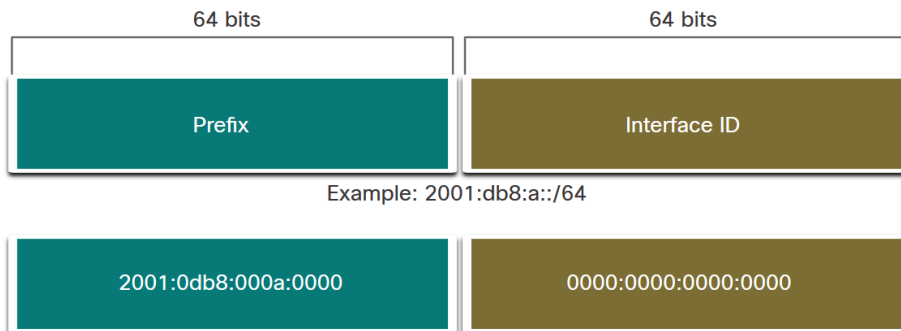
Note: Unlike IPv4, **IPv6 does not have a broadcast address**. However, there is an IPv6 all-nodes multicast address that essentially gives the same result.

IPv6 Address Types

IPv6 Prefix Length

Prefix length is represented in slash notation and is used to indicate the network portion of an IPv6 address.

The IPv6 prefix length can range from 0 to 128. The recommended IPv6 prefix length for LANs and most other types of networks is /64.

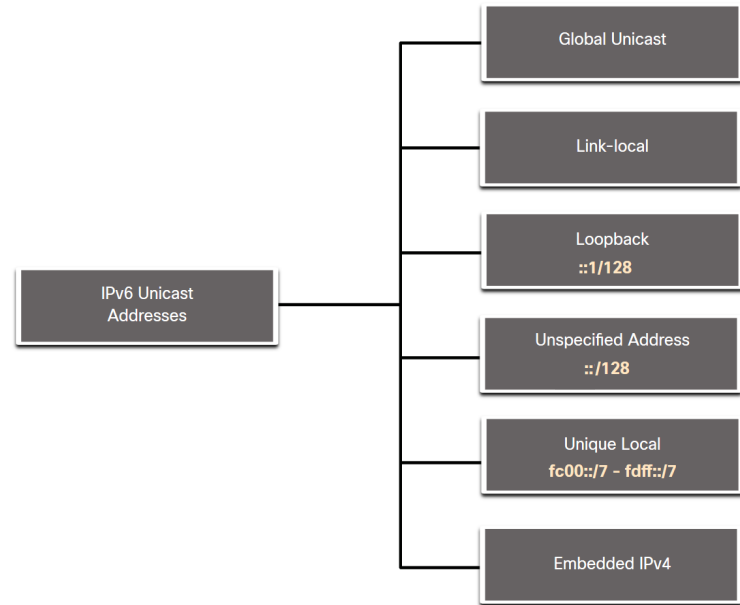


Note: It is strongly recommended to use a 64-bit Interface ID for most networks. This is because stateless address autoconfiguration (SLAAC) uses 64 bits for the Interface ID. It also makes subnetting easier to create and manage.

Types of IPv6 Unicast Addresses

Unlike IPv4 devices that have only a single address, IPv6 addresses typically have two unicast addresses:

- **Global Unicast Address (GUA)** – This is similar to a public IPv4 address. These are globally unique, internet-routable addresses.
- **Link-local Address (LLA)** - Required for every IPv6-enabled device and used to communicate with other devices on the same local link. LLAs are not routable and are confined to a single link.

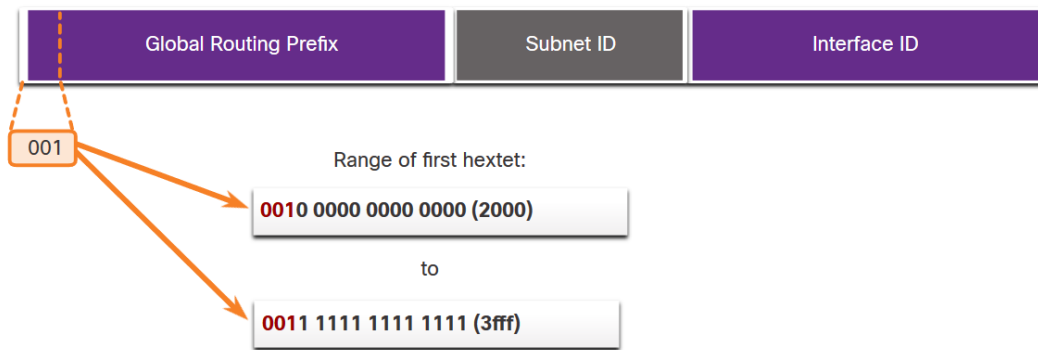


IPv6 Address Types

IPv6 GUA

IPv6 global unicast addresses (GUAs) are globally unique and routable on the IPv6 internet.

- Currently, only GUAs with the first three bits of 001 or 2000::/3 are being assigned.
- Currently available GUAs begins with a decimal 2 or a 3 (This is only 1/8th of the total available IPv6 address space).

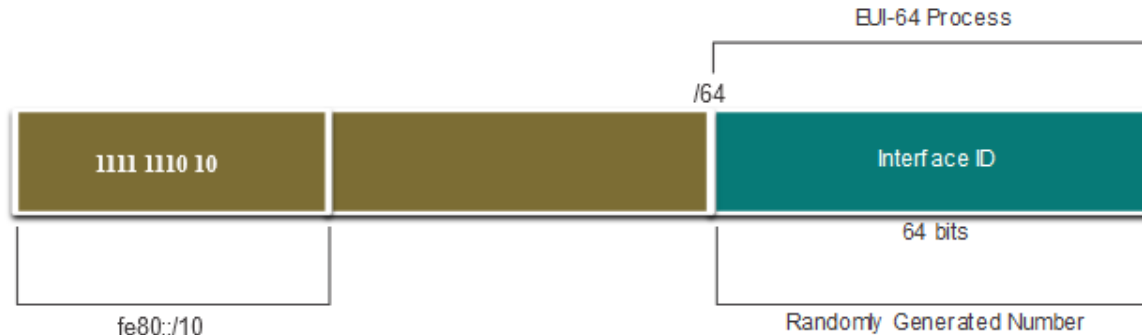


IPv6 Address Types

IPv6 LLA

An IPv6 link-local address (LLA) enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet).

- Packets with a source or destination LLA cannot be routed.
- Every IPv6-enabled network interface must have an LLA.
- If an LLA is not configured manually on an interface, the device will automatically create one.
- IPv6 LLAs are in the **fe80::/10** range.



12.7 IPv6 Multicast Addresses

IPv6 Multicast Addresses

Assigned IPv6 Multicast Addresses

IPv6 multicast addresses have the **prefix ff00::/8**, e.g.:

- **Well-Known multicast addresses**
- **Solicited node multicast addresses**
- **User-defined multicast addresses**

Note: Multicast addresses can only be destination addresses and not source addresses.

Well-Known IPv6 Multicast Addresses

Well-known IPv6 multicast addresses are assigned and are reserved for predefined groups of devices.

There are two common IPv6 Assigned multicast groups:

- **ff02::1 All-nodes multicast group** - This is a multicast group that all IPv6-enabled devices join. A packet sent to this group is received and processed by all IPv6 interfaces on the link or network.
- **ff02::2 All-routers multicast group** - This is a multicast group that all IPv6 routers join. A router becomes a member of this group when it is enabled as an IPv6 router with the **ipv6 unicast-routing** global configuration command.

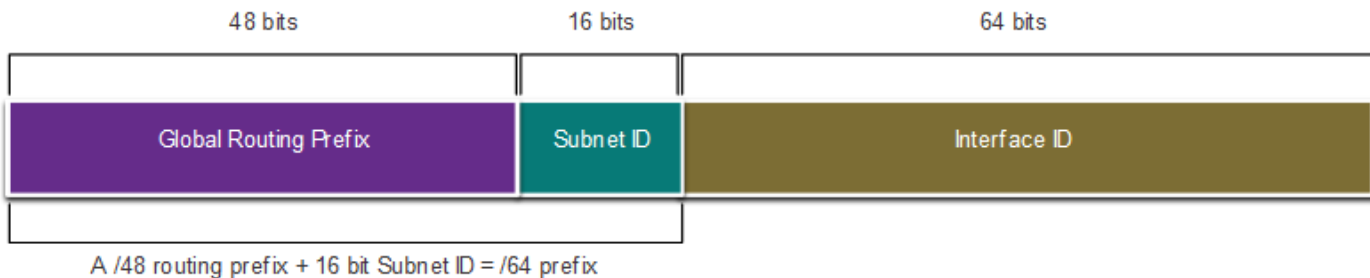
12.8 Subnet an IPv6 Network

Subnet an IPv6 Network

Subnet Using the Subnet ID

IPv6 was designed with subnetting in mind.

- A separate subnet ID field in the IPv6 GUA is used to create subnets.
- The subnet ID field is the area between the Global Routing Prefix and the interface ID.



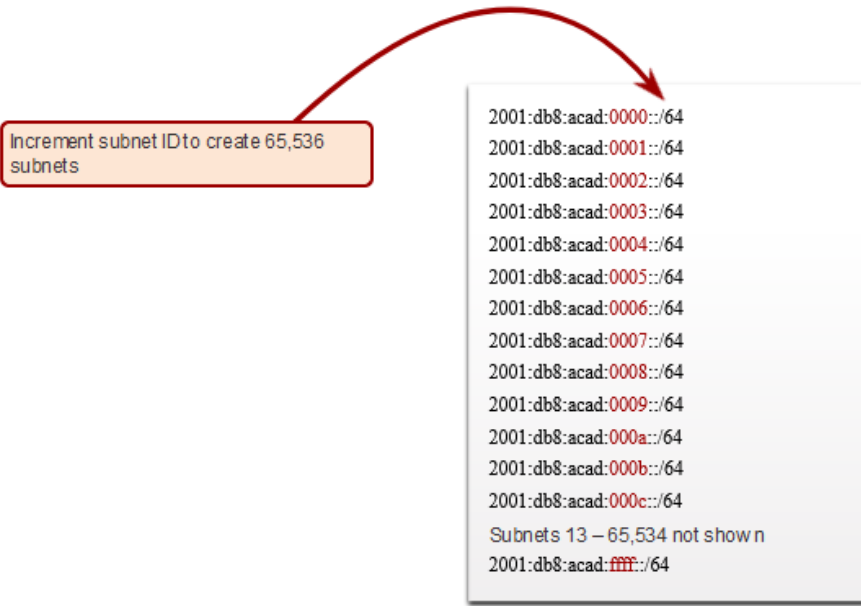
Subnet an IPv6 Network

IPv6 Subnetting Example

Given the 2001:db8:acad::/48 global routing prefix with a 16 bit subnet ID.

- Allows 65,536 /64 subnets
- The global routing prefix is the same for all subnets.
- Only the subnet ID hextet is incremented in hexadecimal for each subnet.

Increment subnet ID to create 65,536 subnets



```
2001:db8:acad:0000::/64
2001:db8:acad:0001::/64
2001:db8:acad:0002::/64
2001:db8:acad:0003::/64
2001:db8:acad:0004::/64
2001:db8:acad:0005::/64
2001:db8:acad:0006::/64
2001:db8:acad:0007::/64
2001:db8:acad:0008::/64
2001:db8:acad:0009::/64
2001:db8:acad:000a::/64
2001:db8:acad:000b::/64
2001:db8:acad:000c::/64
Subnets 13 – 65,534 not shown
2001:db8:acad:ffff::/64
```

IPv6

- VUT má přidělený adresní prostor 2001:67c:1220::/46. Určete první a poslední adresu pro adresování koncové stanice. Kolik koncových sítí /64 je možné vytvořit?

IPv6

- VUT má přidělený adresní prostor 2001:67c:1220::/46. Určete první a poslední adresu pro adresování koncové stanice. Kolik koncových sítí /64 je možné vytvořit?

První adresa: 2001:67c:1220::

IPv6

- VUT má přidělený adresní prostor 2001:67c:1220::/46. Určete první a poslední adresu pro adresování koncové stanice. Kolik koncových sítí /64 je možné vytvořit?

První adresa: 2001:67c:1220::

Poslední adresa: 2001:67c:1223:ffff:ffff:ffff:ffff

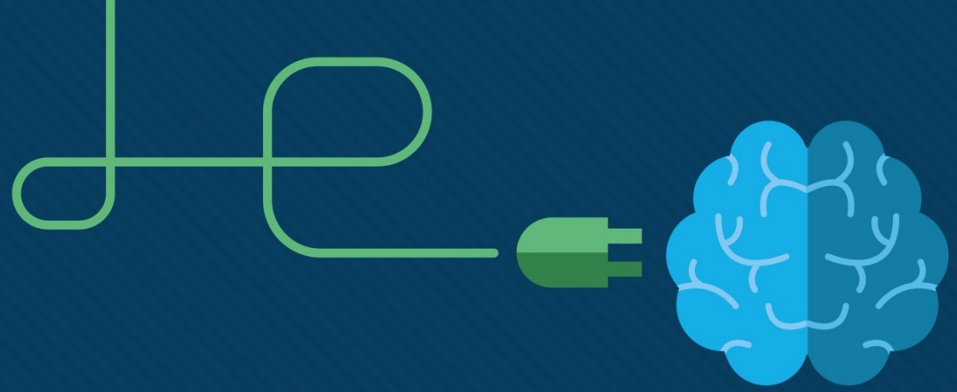
IPv6

- VUT má přidělený adresní prostor 2001:67c:1220::/46. Určete první a poslední adresu pro adresování koncové stanice. Kolik koncových sítí /64 je možné vytvořit?

První adresa: 2001:67c:1220::

Poslední adresa: 2001:67c:1223:ffff:ffff:ffff:ffff

Počet koncových sítí: $2^{64-46}=2^{18}=262144$



RIPng



Advertising IPv6 Networks

```
R1(config)# ipv6 unicast-routing
R1(config)#
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ipv6 rip RIP-AS enable
R1(config-if)# exit
R1(config)#
R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 rip RIP-AS enable
R1(config-if)# no shutdown
R1(config-if)#
```

Configuring the RIPng Protocol

Examining the RIPng Configuration

Verifying RIP Settings on R1

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip RIP-AS"
  Interfaces:
    Serial0/0/0
    GigabitEthernet0/0
  Redistribution:
    None
R1#
```

Verifying Routes on R1

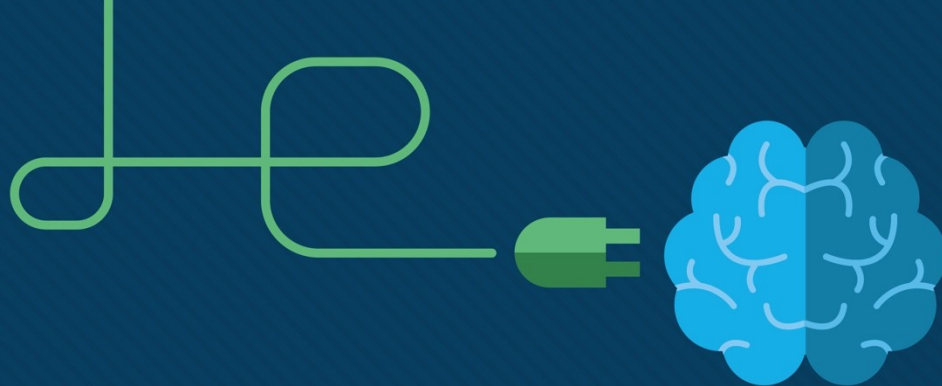
```
R1# show ipv6 route
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user
Static route
  B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
  IA - ISIS interarea, IS - ISIS summary, D - EIGRP,
  EX - EIGRP external, ND - ND Default,
  NDp - ND Prefix, DCE - Destination, NDr - Redirect,
  O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1,
  OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1,
  ON2 - OSPF NSSA ext 2
C 2001:DB8:CAFE:1::/64 [0/0]
  via GigabitEthernet0/0, directly connected
L 2001:DB8:CAFE:1::1/128 [0/0]
  via GigabitEthernet0/0, receive
R 2001:DB8:CAFE:2::/64 [120/2]
  via FE80::FE99:47FF:FE71:78A0, Serial0/0/0
R 2001:DB8:CAFE:3::/64 [120/3]
  via FE80::FE99:47FF:FE71:78A0, Serial0/0/0
C 2001:DB8:CAFE:A001::/64 [0/0]
  via Serial0/0/0, directly connected
L 2001:DB8:CAFE:A001::1/128 [0/0]
  via Serial0/0/0, receive
R 2001:DB8:CAFE:A002::/64 [120/2]
```

Configuring the RIPng Protocol

Examining the RIPng Configuration (cont.)

Verifying RIPng Routes on R1

```
R1# show ipv6 route rip
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user
Static route
    B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
    IA - ISIS interarea, IS - ISIS summary, D - EIGRP,
    EX - EIGRP external, ND - ND Default,
    NDp - ND Prefix, DCE - Destination, NDr - Redirect,
    O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1,
    OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1,
    ON2 - OSPF NSSA ext 2
R   2001:DB8:CAFE:2::/64 [120/2]
    via FE80::FE99:47FF:FE71:78A0, Serial0/0/0
R   2001:DB8:CAFE:3::/64 [120/3]
    via FE80::FE99:47FF:FE71:78A0, Serial0/0/0
R   2001:DB8:CAFE:A002::/64 [120/2]
    via FE80::FE99:47FF:FE71:78A0, Serial0/0/0
R1#
```



Module 9: Address Resolution

Introduction to Networks v7.0
(ITN)



Module Objectives

Module Title: Address Resolution

Module Objective: Explain how ARP and ND enable communication on a network.

Topic Title	Topic Objective
MAC and IP ✓	Compare the roles of the MAC address and the IP address.
ARP ✓	Describe the purpose of ARP.
Neighbor Discovery	Describe the operation of IPv6 neighbor discovery.

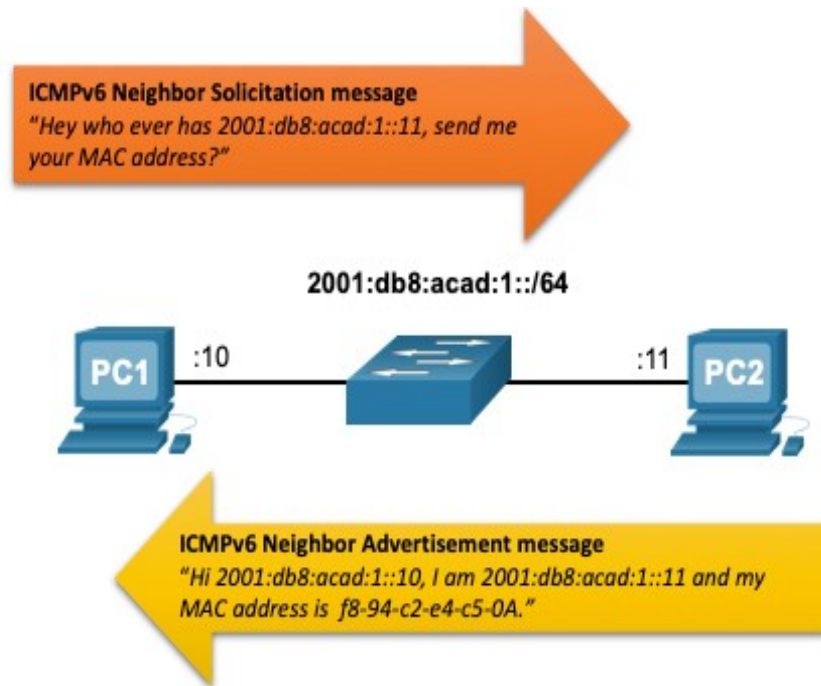
9.3 Neighbor Discovery (IPv6)

IPv6 Neighbor Discovery Messages

IPv6 Neighbor Discovery (ND) protocol provides:

- Address resolution
- Router discovery
- Redirection services
- ICMPv6 Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages are used for device-to-device messaging such as address resolution.
- ICMPv6 Router Solicitation (RS) and Router Advertisement (RA) messages are used for messaging between devices and routers for router discovery.
- ICMPv6 redirect messages are used by routers for better next-hop selection.

IPv6 Neighbor Discovery – Address Resolution



- IPv6 devices use ND to resolve the MAC address of a known IPv6 address.
- ICMPv6 Neighbor Solicitation messages are sent using special Ethernet and IPv6 multicast addresses.

