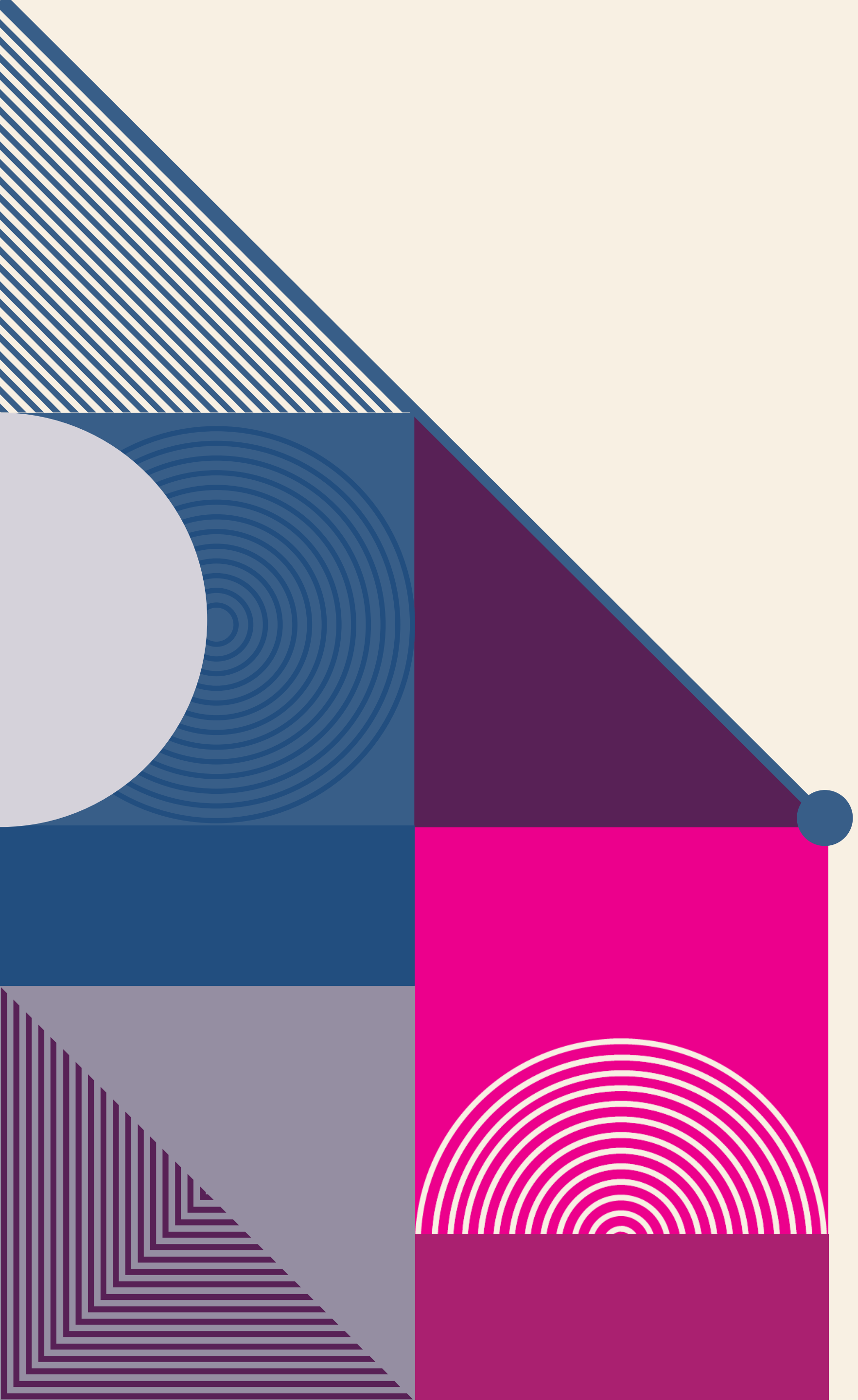
Lecture 7: Routing

Dr. Mai Zaki

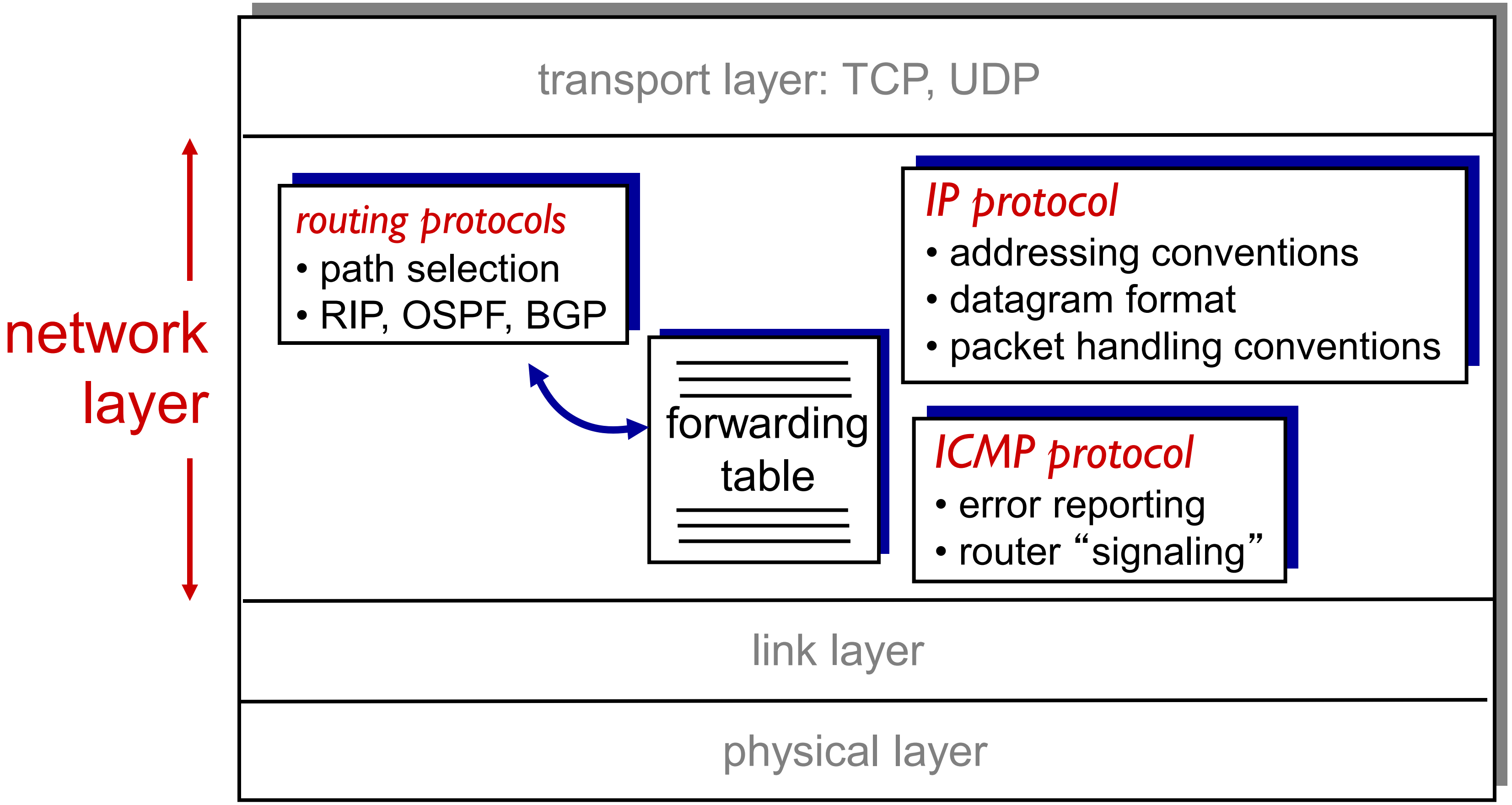


OBJECTIVES

- Understanding IP routing
- Static routing
- Dynamic routing
  - RIP
  - RIPv2
  - Verifying routing

The Internet network layer

host, router network layer functions:



IP datagram format

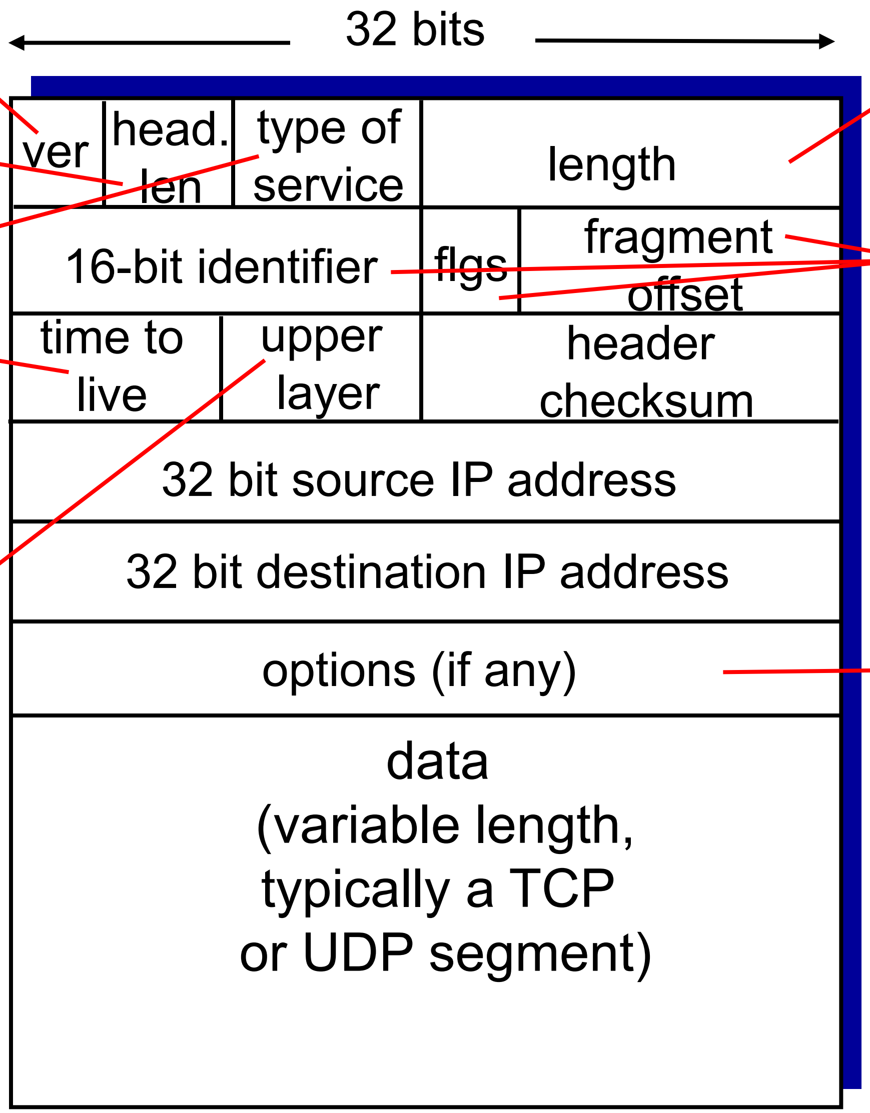
IP protocol version "4" number

header length (bytes)

"type" of data

max number remaining hops (decremented at each router)

upper layer protocol to deliver payload to



32 bits

ver | head. len | type of service | length

16-bit identifier | flgs | fragment offset

time to live | upper layer | header checksum

32 bit source IP address

32 bit destination IP address

options (if any)

data (variable length, typically a TCP or UDP segment)

total datagram length (bytes)

for fragmentation/ reassembly

e.g. timestamp, record route taken, specify list of routers to visit.

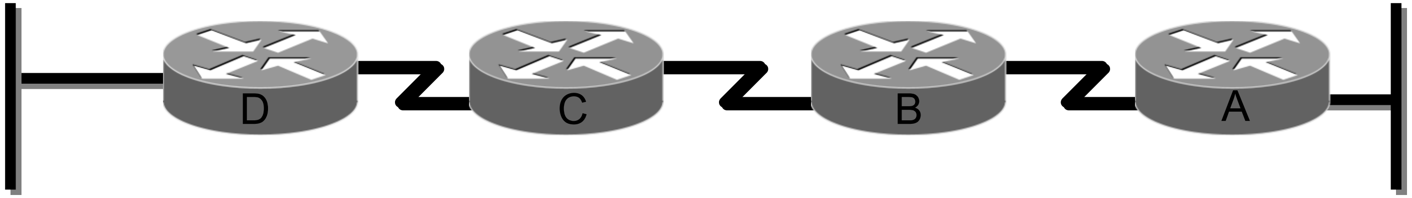
how much overhead?

- 20 bytes of TCP
- 20 bytes of IP
- = 40 bytes + app layer overhead

What is Routing?

To route a router need to know:

- Remote Networks
- Neighbor Routers
- All Possible routes to remote network
- The absolute best route to all remote networks
- Maintain and verify the routing information



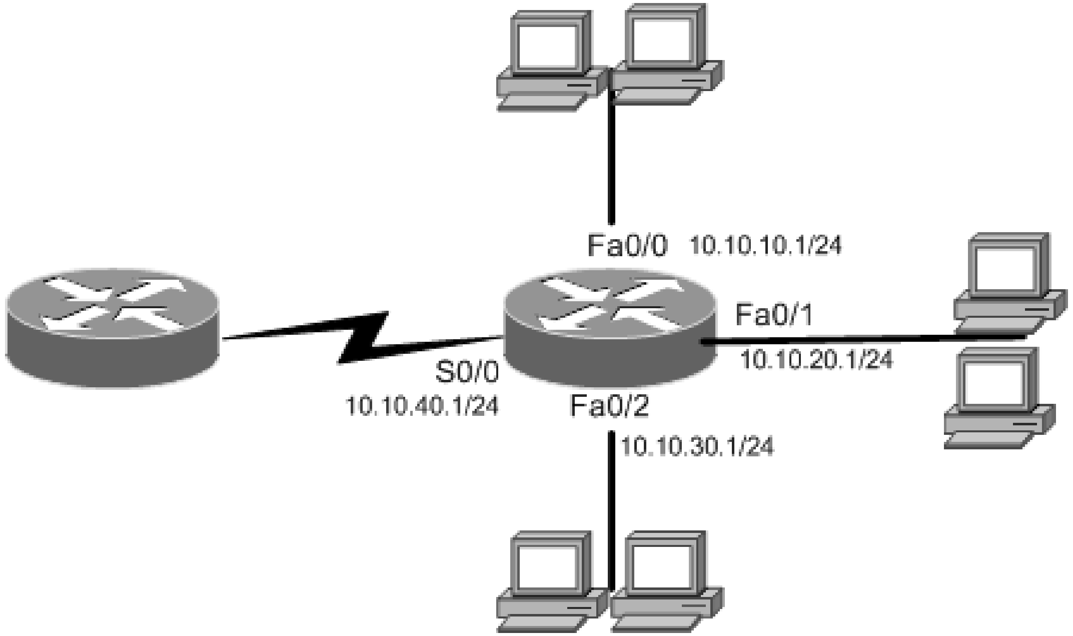
• Routing Basics

- The term *routing* is used for taking a packet from one device and sending it through the network to another device on a different network.

- Routers don't really care about hosts they only care about networks and the best path to each network.

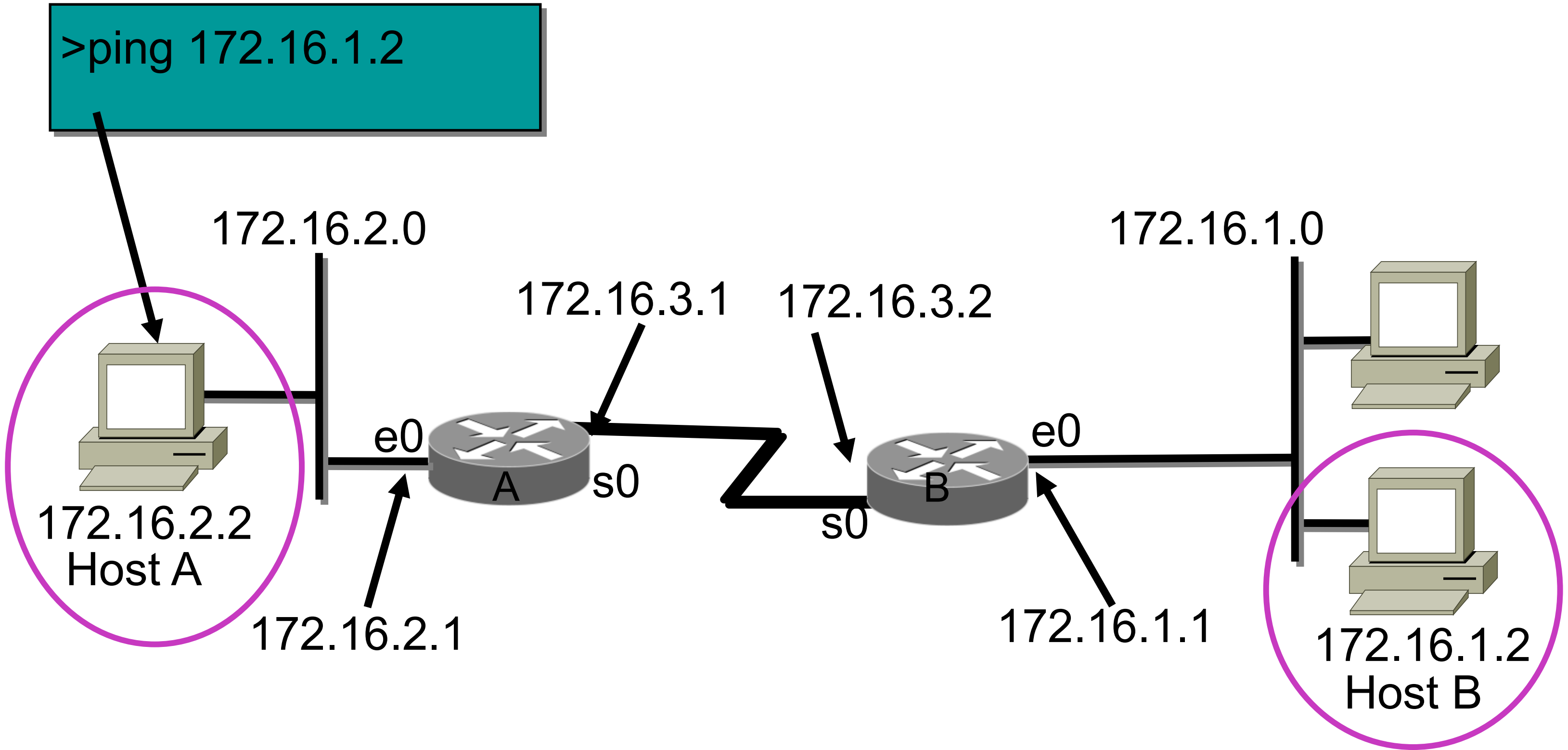
- The logical network address of the destination host is used to get packets to a network through a routed net work, and then the hardware address of the host is used to deliver the packet from a router to the correct destination host.

What interface will the router send out a packet if it has destination address of 10.10.10.18?

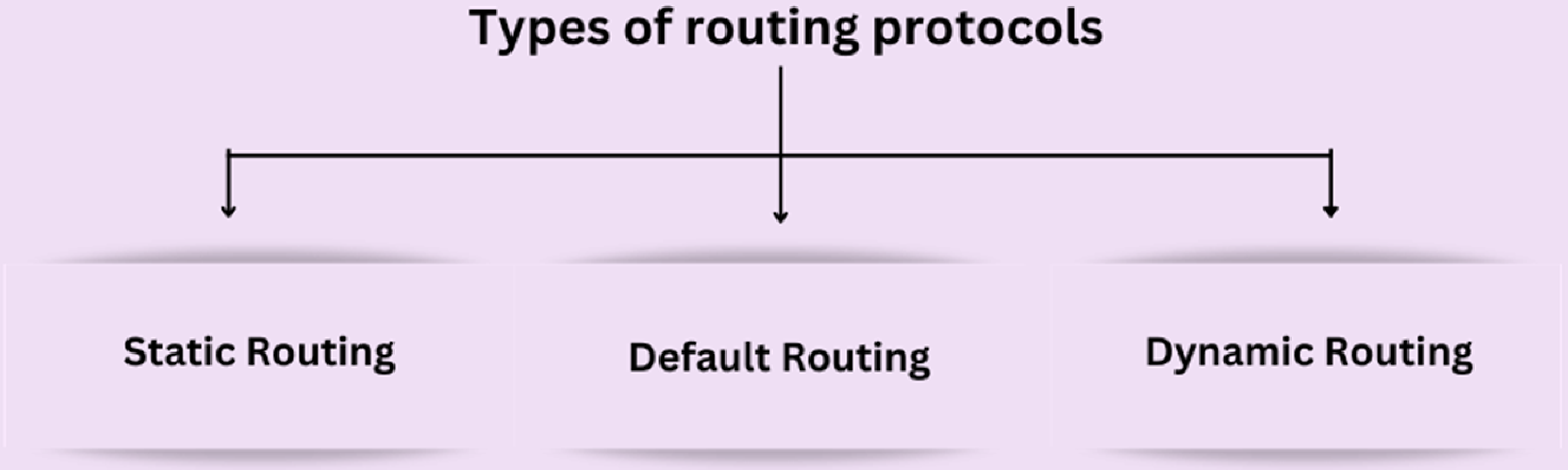


Simple IP Routing

- The IP routing process is fairly simple and doesn’t change, regardless of the size of network you have.
- For an example, we’ll describe step by step what happens when Host A wants to communicate with Host B on a different network.
- In this example, a user on Host A pings Host B’s IP address.



```
>ping 172.16.1.2
```



Types of routing protocols

Static Routing

Default Routing

Dynamic Routing

• Static Routing & Dynamic Routing

- The router learns about remote networks from neighbor routers or from an administrator. The router then builds a routing table (a map of the internetwork) that describes how to find the remote networks. If a network is directly connected, then the router already knows how to get to it.

- If a network isn't directly connected to the router, the router must use one of two ways to learn how to get to the remote network:
  - *static routing*
  - *dynamic routing*

- If *static routing* is used, the administrator is responsible for updating all changes by hand into all routers.

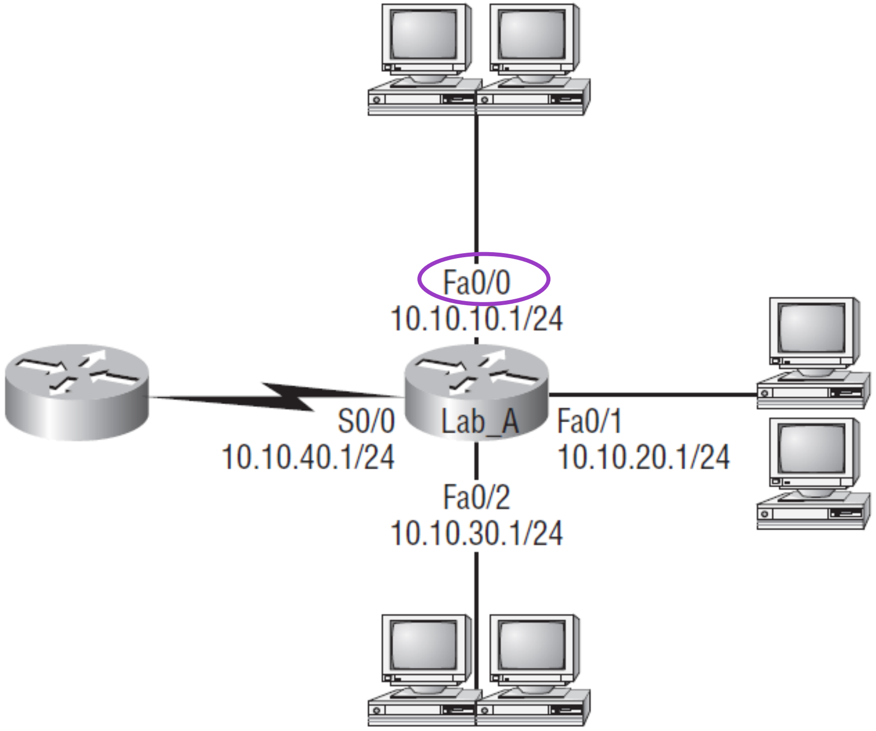
- In *dynamic routing*, a protocol on one router communicates with the same protocol running on neighbor routers. The routers then update each other about all the networks they know about and place this information into the routing table. If a change occurs in the network, the dynamic routing protocols automatically inform all routers about the event.

• Routing Basics

which interface Lab_A will use to forward an IP datagram to a host with an IP address of 10.10.10.10?

```
Lab_A#sh ip route
[output cut]
Gateway of last resort is not set
C       10.10.10.0/24 is directly connected, FastEthernet0/0
C       10.10.20.0/24 is directly connected, FastEthernet0/1
C       10.10.30.0/24 is directly connected, FastEthernet0/2
C       10.10.40.0/24 is directly connected, Serial 0/0
```

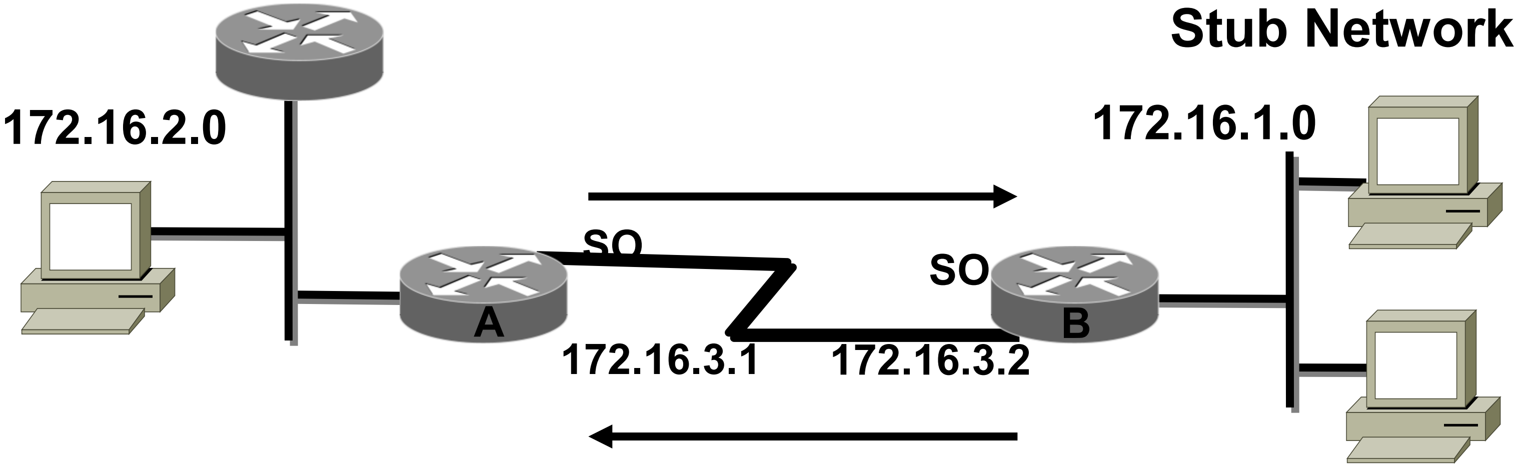
Directly connected



Use the show ip route command to display the current state of the routing table.

Static Routes

Static routing occurs when you manually add routes in each router's routing table.



Routes must be unidirectional

Static Routes

- Things that are good about static routing:
  - ✓ No overhead on the router CPU
  - ✓ No bandwidth usage between routers
  - ✓ Security (because the administrator can only allow routing to certain networks)

- Things that aren’t so good about static routing:
  - ✓ The administrator must **really understand the internetwork** and how each router is connected super well in order to configure routes correctly.
  - ✓ If a network is added to the internetwork, the administrator has to **add a route** to it on all routers—**by hand**.
  - ✓ It just won’t work for you in **large networks** because maintaining it would be a full-time job in itself.

Static Route Configuration

- Here's the command you use to add a static route to a routing table:

ip route [*destination_network*] [*mask*] [*next-hop_address or exit interface*] [*administrative_distance*] [permanent]

- **Ip route**: The command used to create the static route.
- **Destination network**: The network you're placing in the routing table.
- **Mask**: The subnet mask being used on the network.
- **Next-hop address**: The address of the next-hop router that will receive the packet and forward it to the remote network. This is a router interface that's on a directly connected network. You must be able to ping the router interface before you add the route.

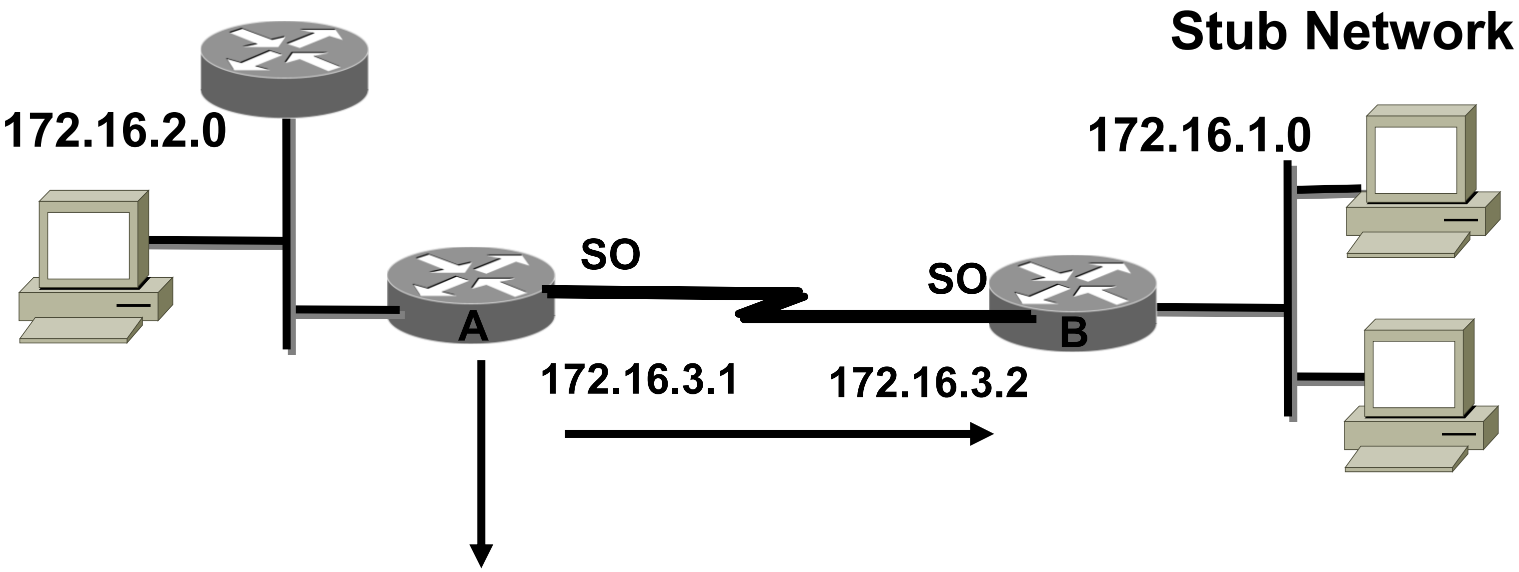
Static Route Configuration

ip route [*destination_network*] [*mask*] [*next-hop_address or exit interface*] [*administrative_distance*] [permanent]

- **Exit interface:** You can use it in place of the next-hop address if you want, but it's got to be on a **point-to-point link**, like a **WAN**. This command won't work on a **LAN like Ethernet**.
- **Administrative distance:** By default, static routes have an administrative distance of 1. You can change the default value by adding an administrative weight at the end of the command.
- **Permanent:** If the interface is **shut down**, or the router **can't communicate to the next-hop** router, the route will automatically be discarded from the routing table. Choosing the permanent option **keeps the entry** in the routing table no matter what happens.

```
Router(config)#ip route remote_network mask next_hop
```

Static Route Example



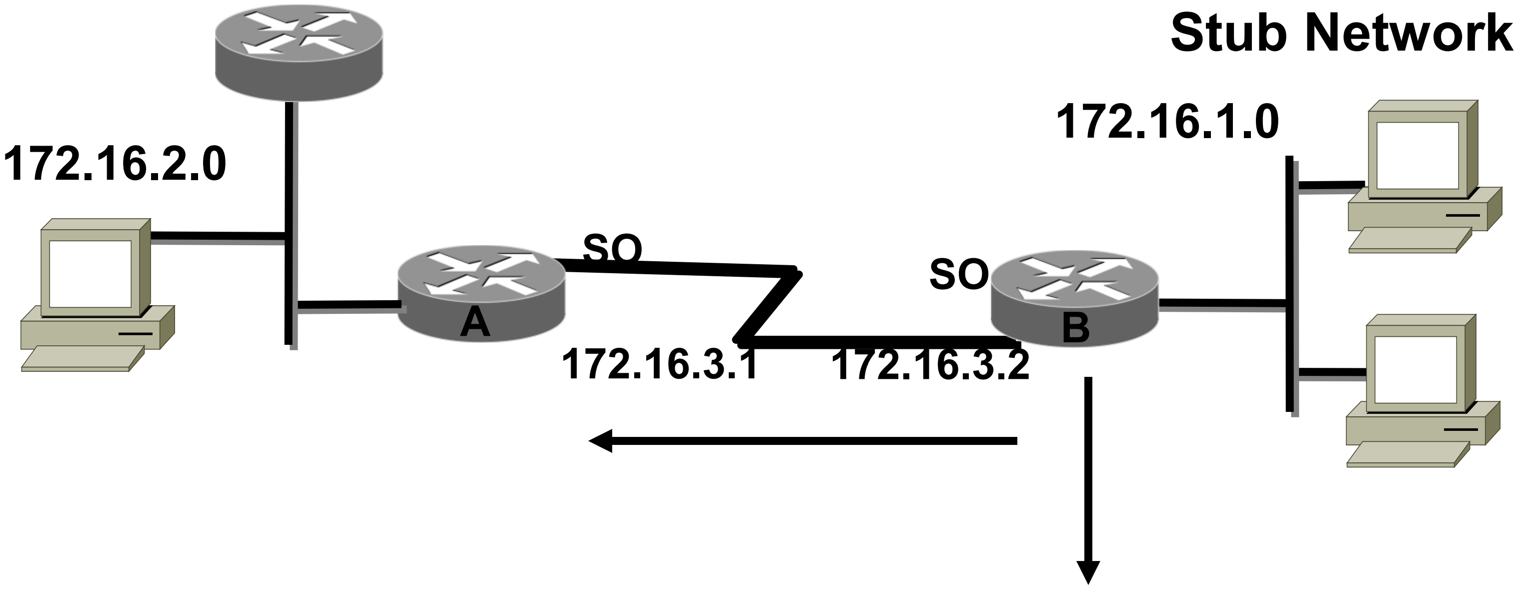
```
ip route 172.16.1.0 255.255.255.0 172.16.3.2
```

or

```
ip route 172.16.1.0 255.255.255.0 s0
```

Default Routes

- We use *default routing* to send packets with a remote destination network not in the routing table to the next-hop router.
- You can only use default routing on **stub networks**—**those with only one exit port** out of the network.



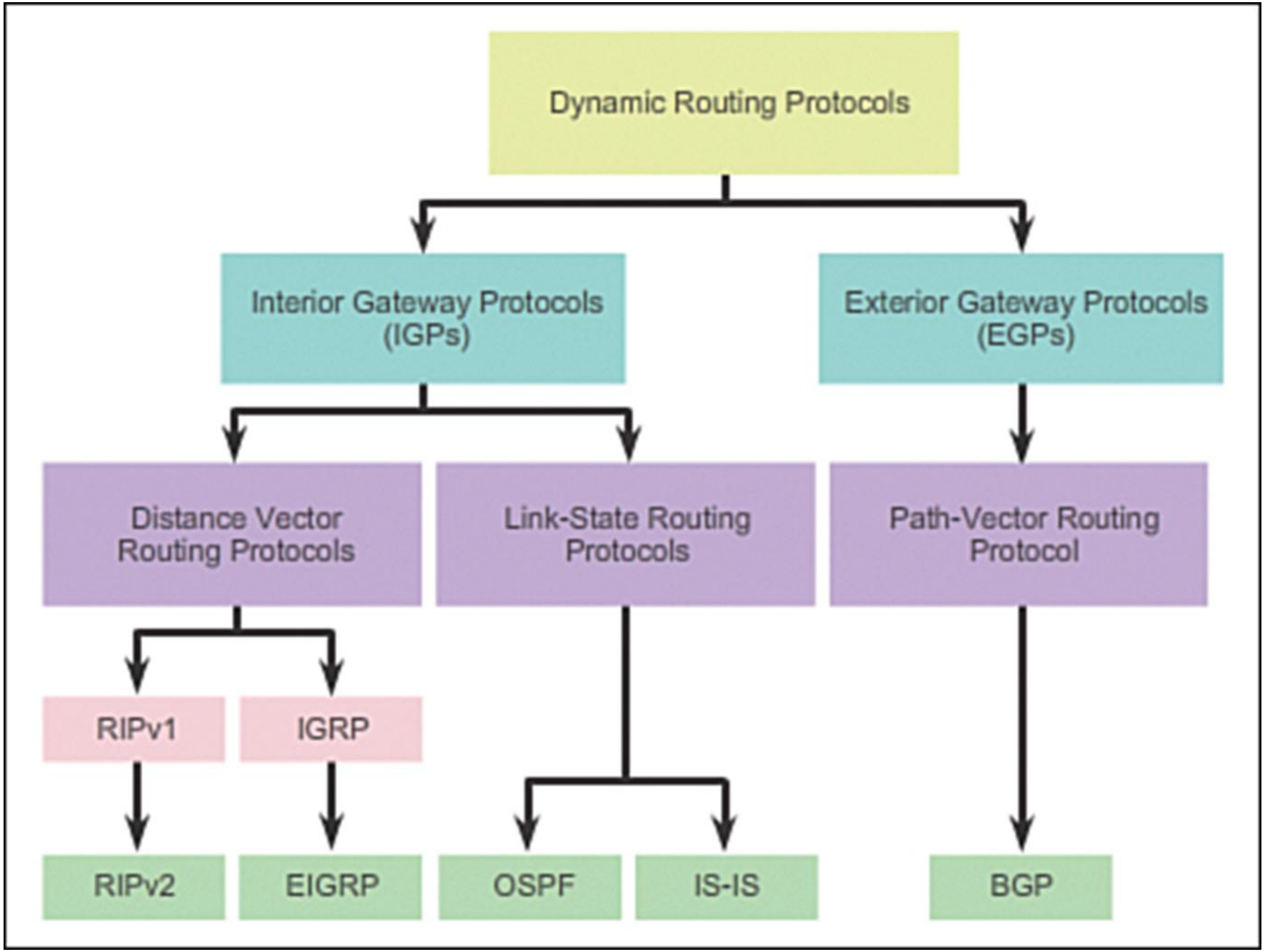
To send packets with a remote destination network not in the routing table to the next-hop router, only used for stub networks.

ip route 0.0.0.0 0.0.0.0 172.16.3.1

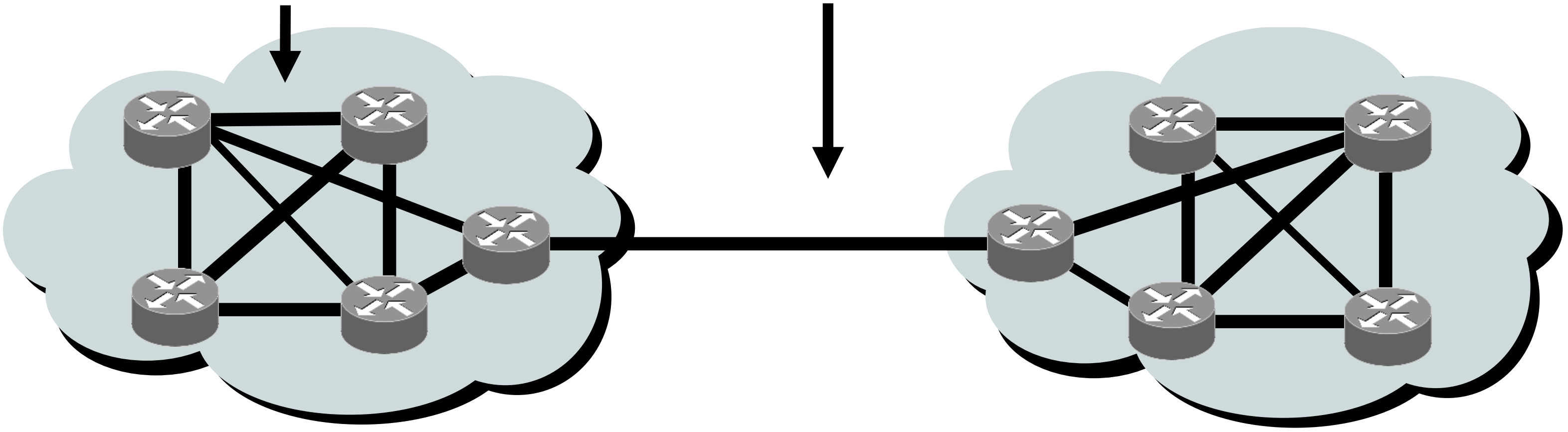
ip classless

Routing Protocols

- Routing protocols are used between routers to:
  - Determine the **path** of a packet through a network
  - **Maintain routing tables**
- Two types: interior/exterior gateway protocols (I/EGPs)
  - Examples:
    - IGP: RIP, IGRP;
    - EGP: Border Gateway Protocol (BGP)


Dynamic Routing Protocols
Interior Gateway Protocols (IGPs)
Exterior Gateway Protocols (EGPs)
Distance Vector Routing Protocols
Link-State Routing Protocols
Path-Vector Routing Protocol
RIPv1
IGRP
RIPv2
EIGRP
OSPF
IS-IS
BGP

Routing Protocols



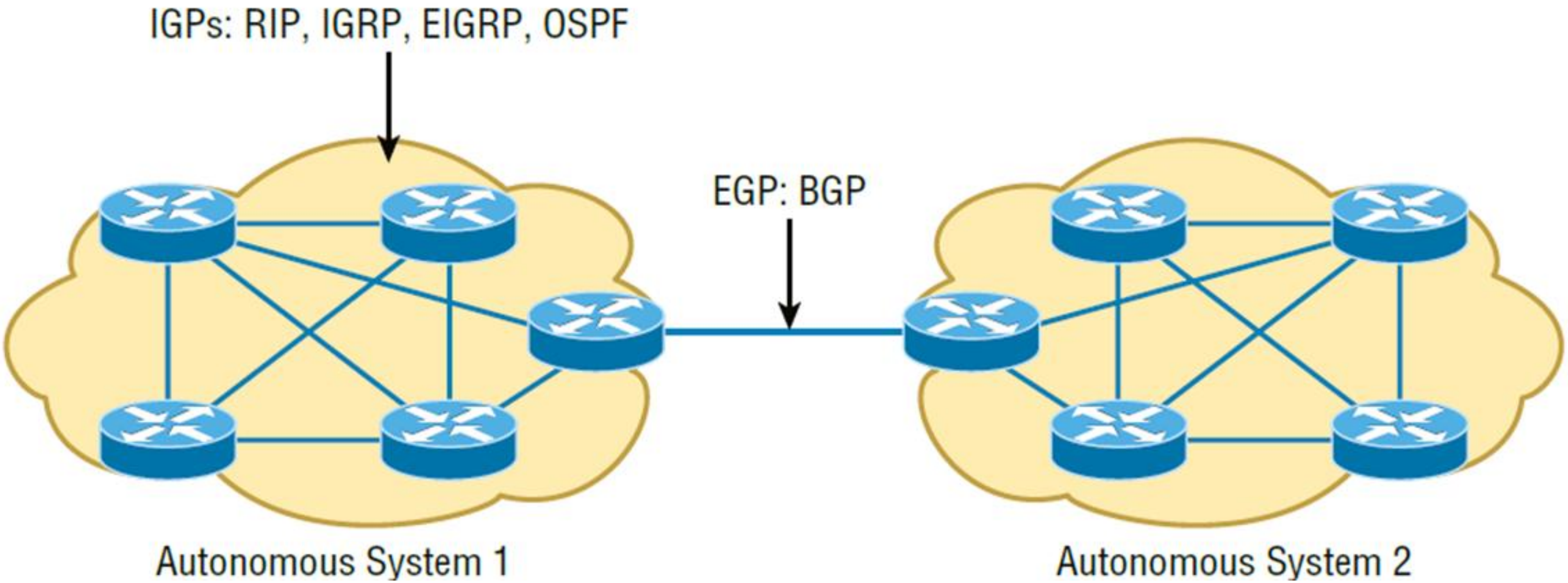
IGPs: RIP, IGRP

EGPs: BGP

Autonomous System 1

Autonomous System 2

- An autonomous system is a collection of networks under a common administrative domain, i.e., all routers sharing the same routing table are in the same AS.
- IGPs operate within an autonomous system. IGPs are used to exchange routing information with routers in the same autonomous system (AS).
- EGPs connect different autonomous systems.
- An example of an EGP is Border Gateway Protocol (BGP)


IGPs: RIP, IGRP, EIGRP, OSPF
EGP: BGP
Autonomous System 1
Autonomous System 2

Classful Routing Overview

Classful routing means that all devices in the network must use the same subnet mask.

Classful routing protocols do not include the subnet mask with the route advertisement.

– Within the same network, consistency of the subnet masks is assumed.

– Summary routes are exchanged between foreign networks.

– Examples of classful routing protocols:

- RIP Version 1 (RIPv1)
- IGRP

Classless Routing Overview

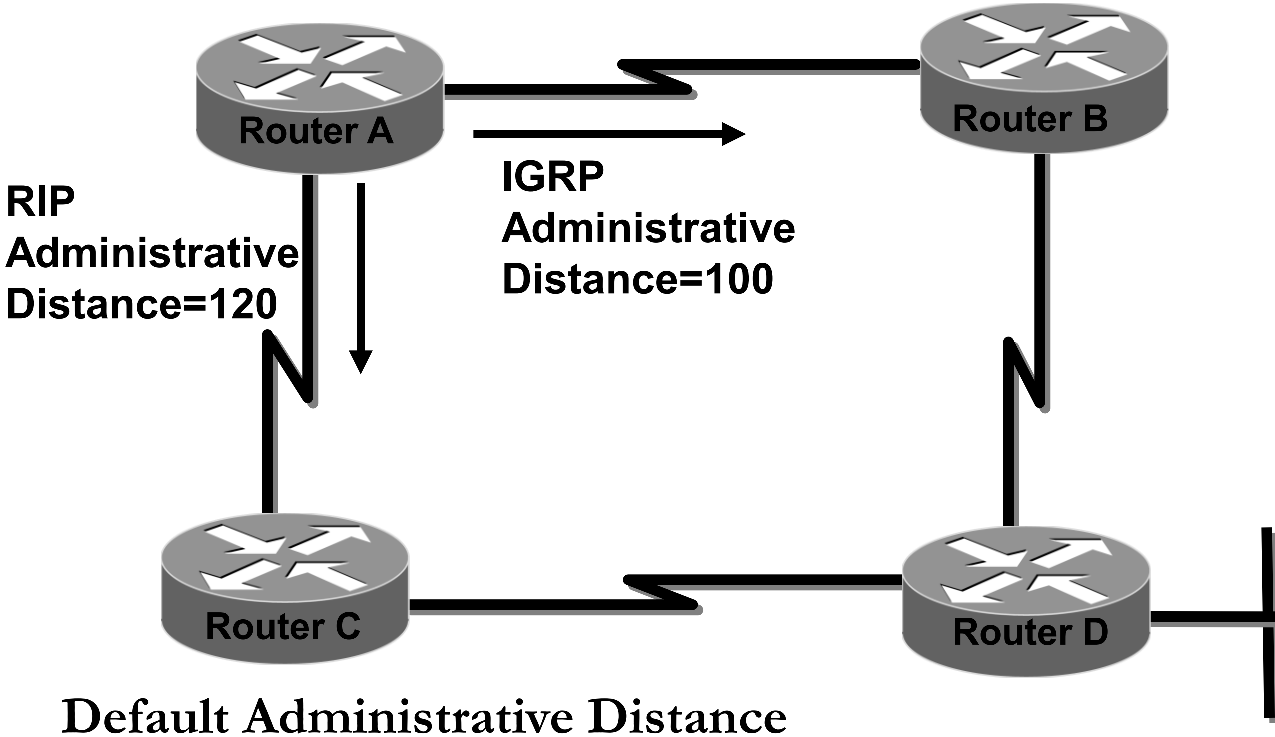
- **Classless routing protocols include the subnet mask with the route advertisement.**
  - Classless routing protocols support variable-length subnet masking (VLSM).
  - Summary routes can be manually controlled within the network.
  - Examples of classless routing protocols:
    - RIP Version 2 (RIPv2)
    - EIGRP
    - OSPF
    - IS-IS

Administrative Distance

- **The administrative distance (AD)** is used to rate the trustworthiness of routing information received on a router from a neighbor router.
- An administrative distance is an integer from 0 to 255, where 0 is the most trusted and 255 means no traffic will be passed via this route.
- If a router receives two updates listing the same remote network, the first thing the router checks is the AD. If one of the advertised routes has a lower AD than the other, then the route with the lowest AD will be placed in the routing table.
- If both advertised routes to the same network have the **same AD**, then routing protocol metrics (such as **hop count** or **bandwidth** of the lines) will be used to find the best path to the remote network.
- The advertised route with the lowest metric will be placed in the routing table. But if both advertised routes have the same AD as well as the same metrics, then the routing protocol will load-balance to the remote network.
- **RIP uses only hop count as the distance**.

Administrative Distance

Route Source	Default AD
Connected interface	0
Static route	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
External EIGRP	170
Unknown	255 (this route will never be used)



RIP
Administrative
Distance=120

IGRP
Administrative
Distance=100

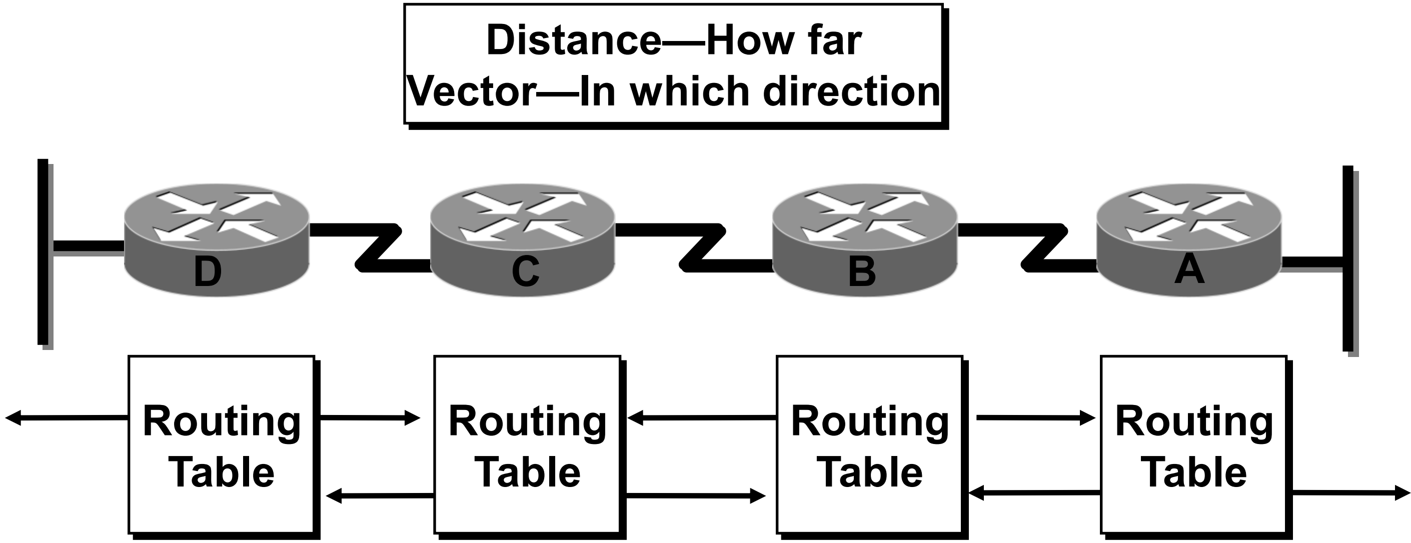
Default Administrative Distance
Directly Connected: 0
Static Route: 1
RIP: 120
IGRP: 100
EIGRP: 90
OSPF: 110

Administrative Distance

- If a network is directly connected, the router will always use the interface connected to the network.
- If you configure a static route, the router will then believe that route over any other learned routes. You can change the administrative distance of static routes, **but by default**, they have an **AD of 1**.
- **In our static route configuration, the AD of each route is set at 150 or 151. This lets us configure routing protocols without having to remove the static routes.**
- They'll be used as **backup routes** in case the routing protocol experiences a failure of some type.

Distance Vector

- The distance-vector protocols find the best path to a remote network by judging distance.
- Each time a packet goes through a router, that's called a hop. The route with the **least number of hops to the network is determined to be the best route.**
- The vector indicates the direction to the remote network. Both **RIP** and **IGRP** are distance-vector routing protocols.



- All routers just **broadcast** their **entire routing table** out **all active interfaces** on **periodic time intervals**
- Distance vector algorithms do not allow a router to know the exact topology of an internetwork.

Distance Vector

- It’s possible to have a network that has multiple links to the same remote network, and if that’s the case, the administrative distance of each received update is checked first.

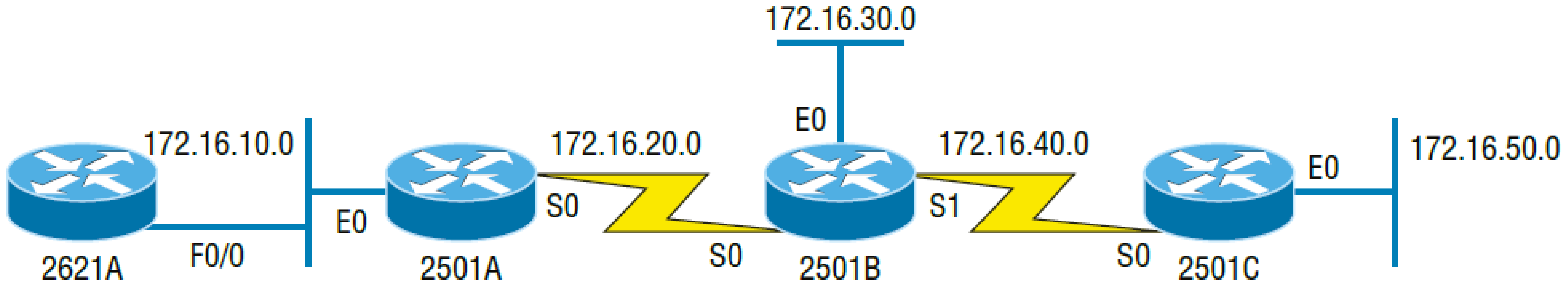
- If the AD is the same, the protocol will have to use other metrics to determine the best path to use to that remote network.

- **RIP uses only hop count** to determine the best path to a network.

- If RIP finds more than one link with the same hop count to the same remote network, it will automatically perform a **round-robin load balancing.**

- RIP can perform load balancing for up to **six equal-cost links**

Discovering Routes



Routing Table		
172.16.10.0	F0/0	0

Routing Table		
172.16.10.0	E0	0
172.16.20.0	S0	0

Routing Table		
172.16.20.0	S0	0
172.16.30.0	E0	0
172.16.40.0	S1	0

Routing Table		
172.16.40.0	S0	0
172.16.50.0	E0	0

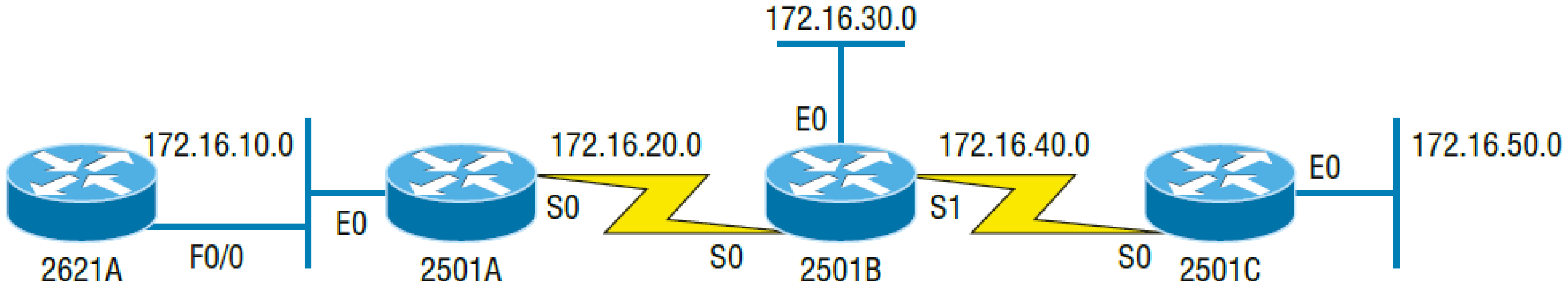
Routers, when powered up and the interfaces are enabled, have only their directly connected networks in the routing table

Discovering Routes: Converged Routing Tables

- The routing tables are complete because they include information about all the networks in the internetwork.
- They are considered converged.

That’s why fast convergence time is a serious plus.

- In fact, that’s one of the problems with **RIP**—its slow convergence time.



Routing Table		
172.16.10.0	F0/0	0
172.16.20.0	F0/0	1
172.16.30.0	F0/0	2
172.16.40.0	F0/0	2
172.16.50.0	F0/0	3

Routing Table		
172.16.10.0	E0	0
172.16.20.0	S0	0
172.16.30.0	S0	1
172.16.40.0	S0	1
172.16.50.0	S0	2

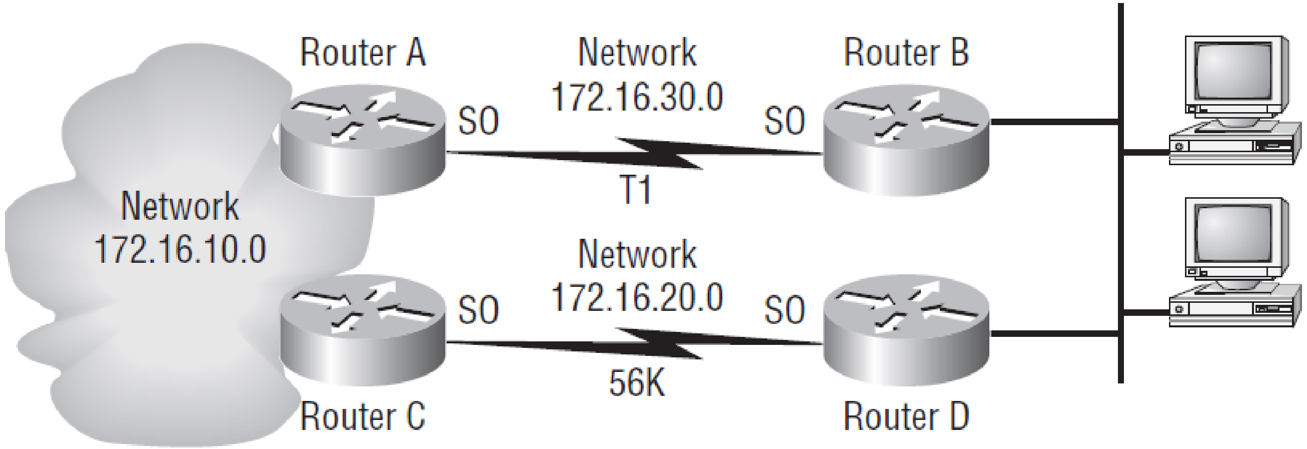
Routing Table		
172.16.20.0	S0	0
172.16.30.0	E0	0
172.16.40.0	S1	0
172.16.10.0	S0	1
172.16.50.0	S1	1

Routing Table		
172.16.40.0	S0	0
172.16.50.0	E0	0
172.16.10.0	S0	2
172.16.20.0	S0	1
172.16.30.0	S0	1

Pinhole Congestion

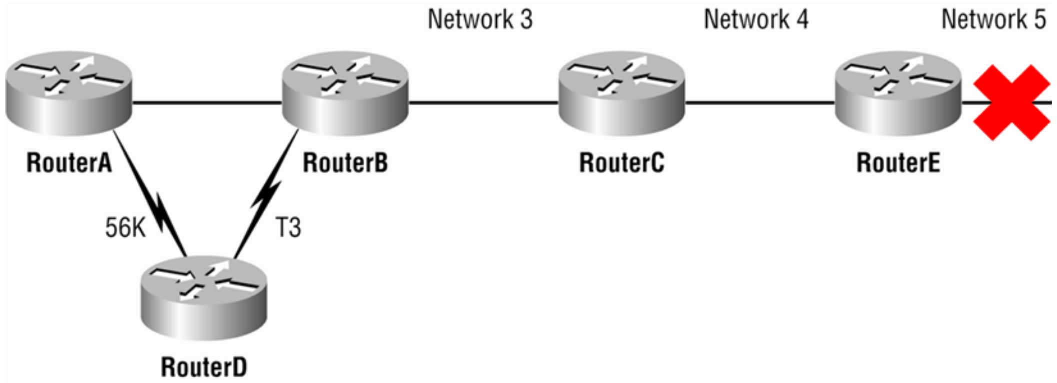
- A problem with this type of routing metric arises when the two links to a remote network are different bandwidths but the same hop count. Figure 6.12, for example, shows two links to remote network 172.16.10.0.

- Since network 172.16.30.0 is a T1 link with a bandwidth of 1.544Mbps and network 172.16.20.0 is a 56K link, you'd want the router to choose the T1 over the 56K link, right? But because hop count is the only metric used with **RIP** routing, the two links would be seen as being of equal cost. This little snag is called pinhole congestion.



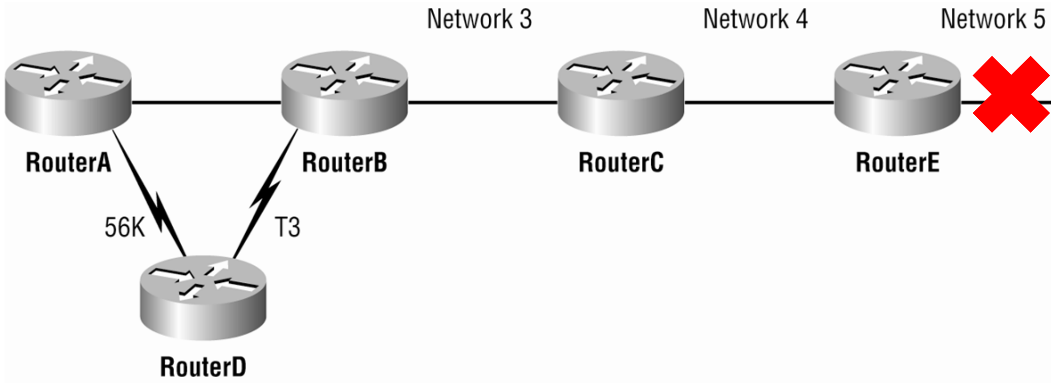
• Routing Loops

- Distance-vector routing protocols keep track of any changes to the internetwork by broadcasting periodic routing updates out all active interfaces.
- This broadcast includes the complete routing table.
- This works just fine, but it’s expensive in terms of CPU process and link bandwidth.
- And if a network outage happens, real problems can occur. Plus, the slow convergence of distance-vector routing protocols can result in inconsistent routing tables and routing loops.
- Routing loops can occur because every router isn’t updated simultaneously.



• Routing Loops

- Here’s an example—let’s say that the interface to Network 5 fails. All routers know about Network 5 from RouterE. RouterA, in its tables, has a path to Network 5 through RouterB.
- When Network 5 fails, RouterE tells RouterC. This causes RouterC to stop routing to Network 5 through RouterE. But routers A, B, and D don’t know about Network 5 yet, so they keep sending out update information. RouterC will eventually send out its update and cause B to stop routing to Network 5, but routers A and D are still not updated.
- To them, it appears that Network 5 is still available through RouterB with a metric of 3.
- The problem occurs when RouterA sends out its regular 30-second “Hello, I’m still here— these are the links I know about” message, which includes the ability to reach Network 5, and now routers B and D receive the wonderful news that Network 5 can be reached from RouterA
- so, routers B and D then send out the information that Network 5 is available. Any packet destined for Network 5 will go to RouterA, to RouterB, and then back to RouterA



• Maximum Hop Count

- The routing loop problem just described is called *counting to infinity*, and it's caused by gossip (broadcasts) and wrong information being communicated and propagated throughout the internetwork.
- One way of solving this problem is to define a *maximum hop count*.
- RIP permits a hop count of up to 15, so anything that requires 16 hops is deemed unreachable.
- Thus, the maximum hop count will control how long it takes for a routing table entry to become invalid or questionable.

Split Horizon

- Another solution to the routing loop problem is called *split horizon*. This reduces incorrect routing information and routing overhead in a distance-vector network by enforcing the rule that routing information cannot be sent back in the direction from which it was received.
- In other words, the routing protocol differentiates which interface a network route was learned on, and once this is determined, it won't advertise the route back out that same interface. This would have prevented RouterA from sending the updated information it received from RouterB back to RouterB.

Route Poisoning

For example, when Network 5 goes down, RouterE initiates route poisoning by advertising Network 5 as 16, or unreachable (sometimes referred to as *infinite*).

When RouterC receives a route poisoning from RouterE, it sends an update, called a *poison reverse*, back to RouterE.

Holddowns

A *holddown* prevents regular update messages from reinstating a route that is going up and down (called *flapping*). Typically, this happens on a serial link that's losing connectivity and then coming back up. If there wasn't a way to stabilize this, the network would never converge and that one flapping interface could bring the entire network down!

Holddowns prevent routes from changing too rapidly by allowing time for either the downed route to come back up or the network to stabilize somewhat before changing to the next best route. These also tell routers to restrict, for a specific time period, changes that might affect recently removed routes.