Lecture 9

EIGRP and OSPF

Dr. Mai Zaki

OBJECTIVES

- Enhanced IGRP
    - EIGRP tables
    - Configuring EIGRP
    - Verifying EIGRP
- Open Shortest Path First
    - Configuring OSPF
    - Verifying OSPF
    - Configuring OSPF with wildcards

What Is Enhanced IGRP (EIGRP)?

- Enhanced Interior Gateway Routing Protocol (**EIGRP**) is a proprietary Cisco protocol that runs on Cisco routers.

- There are a number of powerful features that make EIGRP a real stand out from IGRP and other protocols. The main ones are listed here:

  - ✓ Efficient neighbor discovery
  - ✓ Rapid convergence
  - ✓ Support for VLSM/CIDR
  - ✓ Support for summaries and discontiguous networks
  - ✓ Reduced bandwidth usage
  - ✓ Uses Diffused Update Algorithm (DUAL) to select the best routes
  - ✓ Up to six unequal paths to a remote network (4 by default)

Comparing EIGRP and IGRP

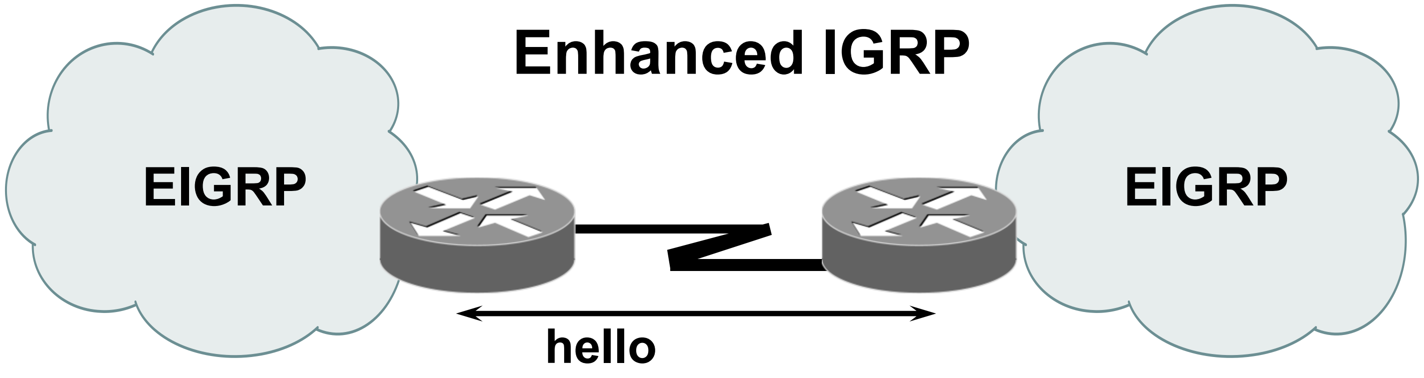
- Enhanced IGRP (EIGRP) is a classless, enhanced distance-vector protocol.

- Like IGRP, EIGRP uses the concept of an autonomous system to describe the set of contiguous routers that run the same routing protocol and share routing information.

- But unlike IGRP, EIGRP includes the subnet mask in its route updates, the advertisement of subnet information allows us to use VLSM and summarization when designing our networks!
  - Similar metric
  - Same load balancing
  - Improved convergence time
  - Reduced network overhead
  - Maximum hop count of 255 (100 default)
  - EIGRP can differentiate between internal and external routes

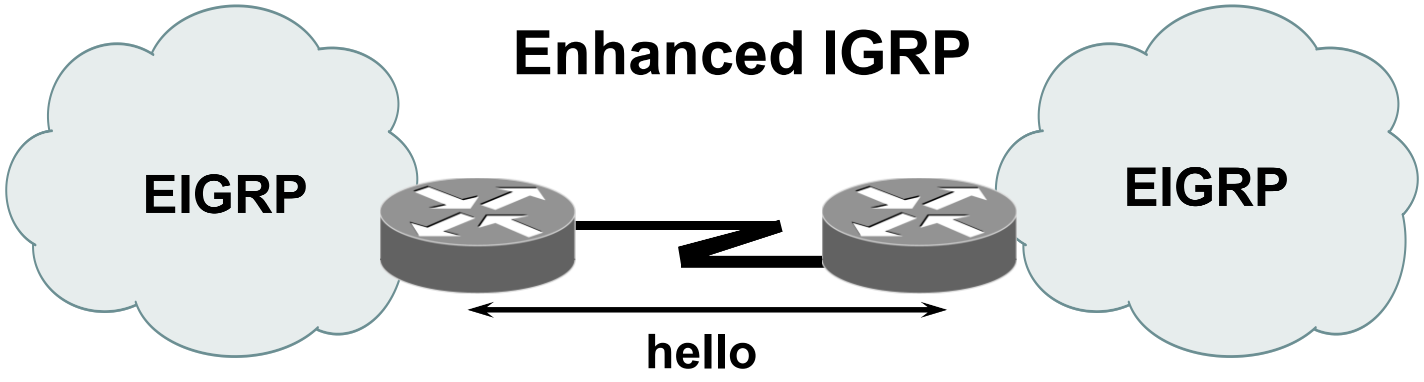
EIGRP for IP

- EIGRP is sometimes referred to as a hybrid routing protocol because it has characteristics of both distance-vector and link-state protocols.
- And EIGRP has link-state characteristics as well—it synchronizes routing tables between neighbors at startup, and then sends specific updates only when topology changes occur.
- No periodic updates. Route updates sent only when a change occurs – multicast on 224.0.0.10
- Hello messages sent to neighbors every 5 seconds (60 seconds in most WANs)



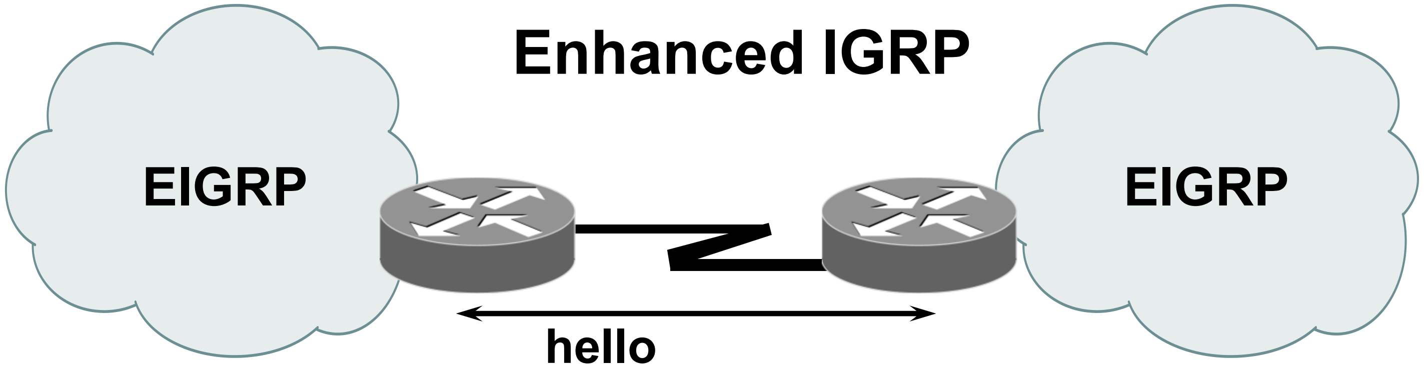
Neighbor Discovery

- Before EIGRP routers are willing to exchange routes with each other, they must become neighbors.
- There are three conditions that must be met for neighborship establishment:
  - ✓ **Hello or ACK received**
  - ✓ **AS numbers match**
  - ✓ **Identical metrics (K values)**
- Link-state protocols tend to use Hello messages to establish neighborship (also called adjacencies) because
  - They normally do not send out periodic route updates and
  - There has to be some mechanism to help neighbors realize when a new peer has moved in or an old one has left or gone down.



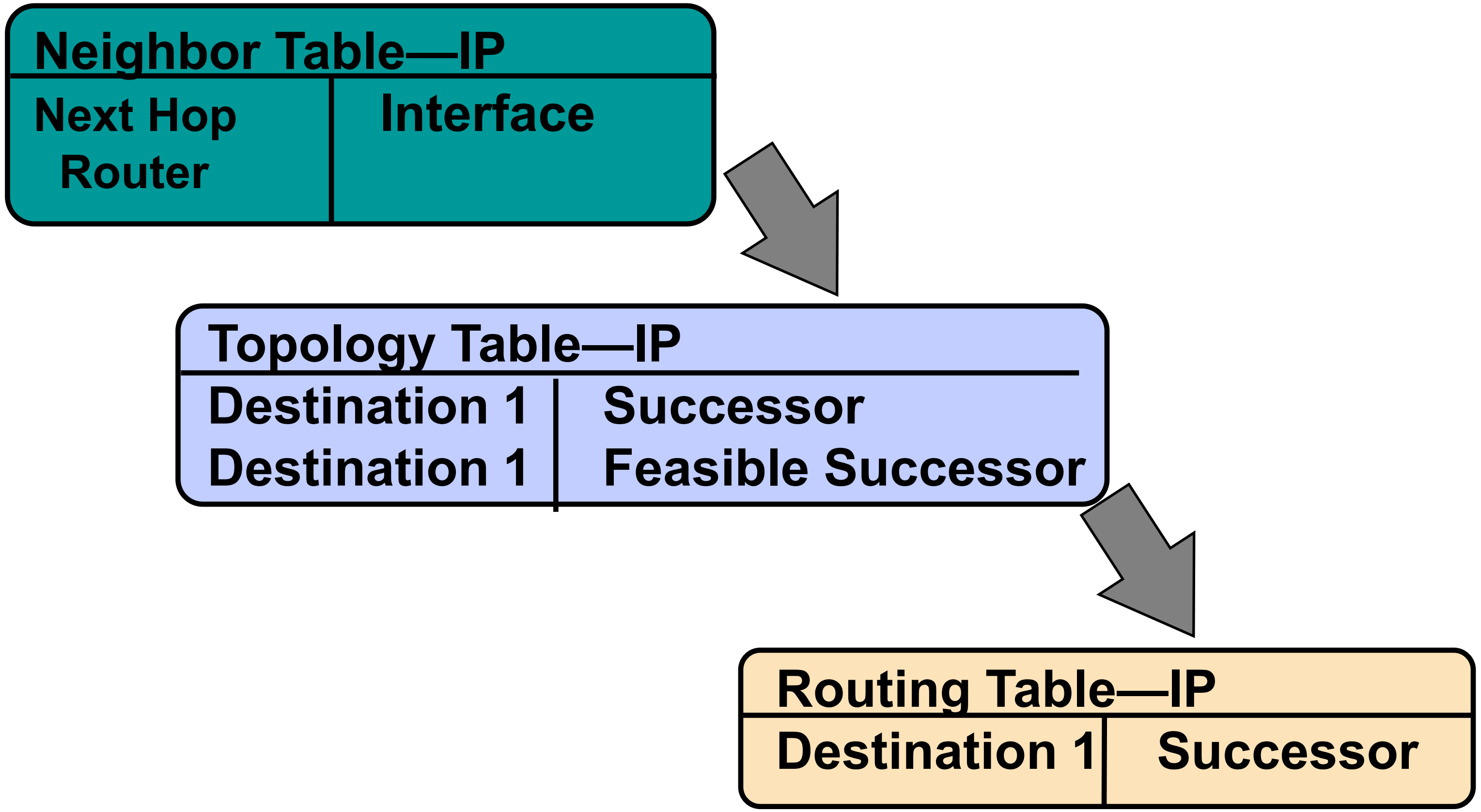
Neighbor Discovery

- To maintain the neighborship relationship, EIGRP routers must also continue receiving Hellos from their neighbors.
- The only time EIGRP advertises its entire routing table is when it discovers a new neighbor and forms an adjacency with it through the exchange of Hello packets. .
- When this happens, both neighbors advertise their entire routing tables to one another. After each has learned its neighbor's routes, only changes to the routing table are propagated from then on.



EIGRP Terminology

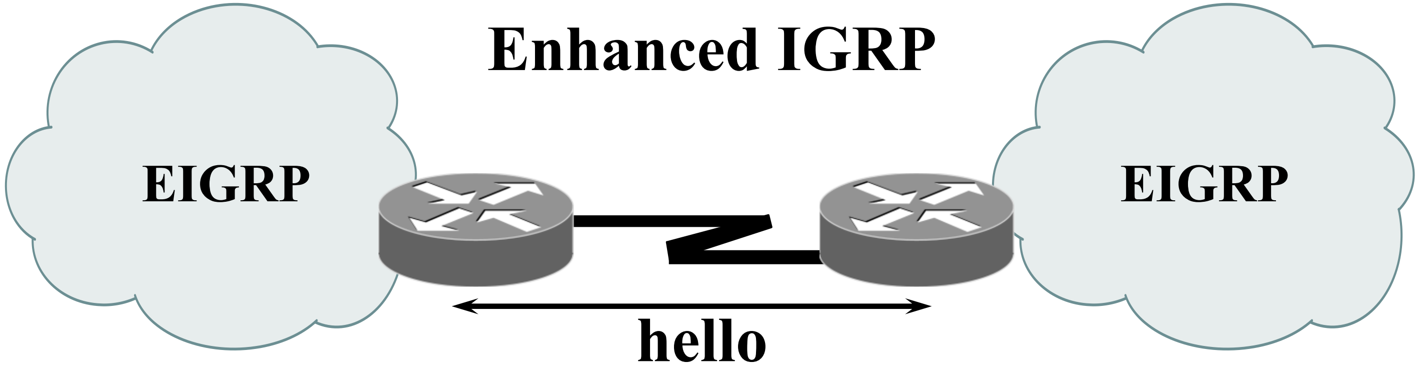
- The neighbor table records information about routers with whom neighborship relationships have been formed.
- The topology table stores the route advertisements about every route in the internetwork received from each neighbor.
- The routing table stores the routes that are currently used to make routing decision.



Note: A feasible successor is a backup route and stored in the Topology table

EIGRP Tables

- The neighbor table and topology table are maintained through the use of hello and update packets.



- To see all feasible successor routes known to a router, use the **show ip eigrp topology** command

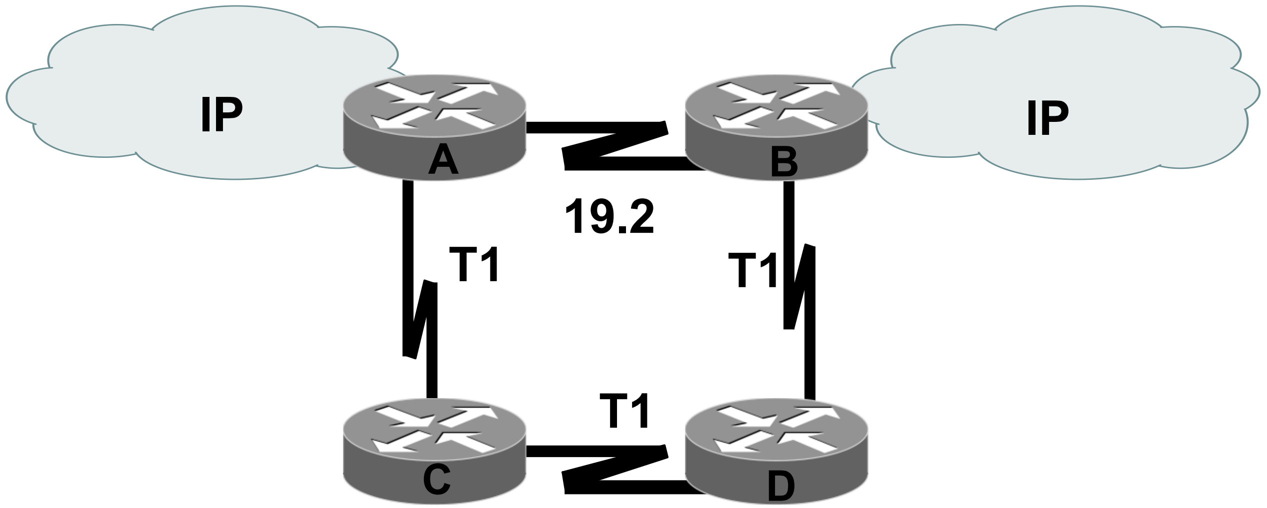
Successor routes

- **Successor route** is used by EIGRP to forward traffic to a destination
- A successor route may be backed up by a feasible successor route
- Successor routes are stored in both the topology table and the routing table

Topology Table—IP	
Destination 1	Successor
Destination 1	Feasible Successor

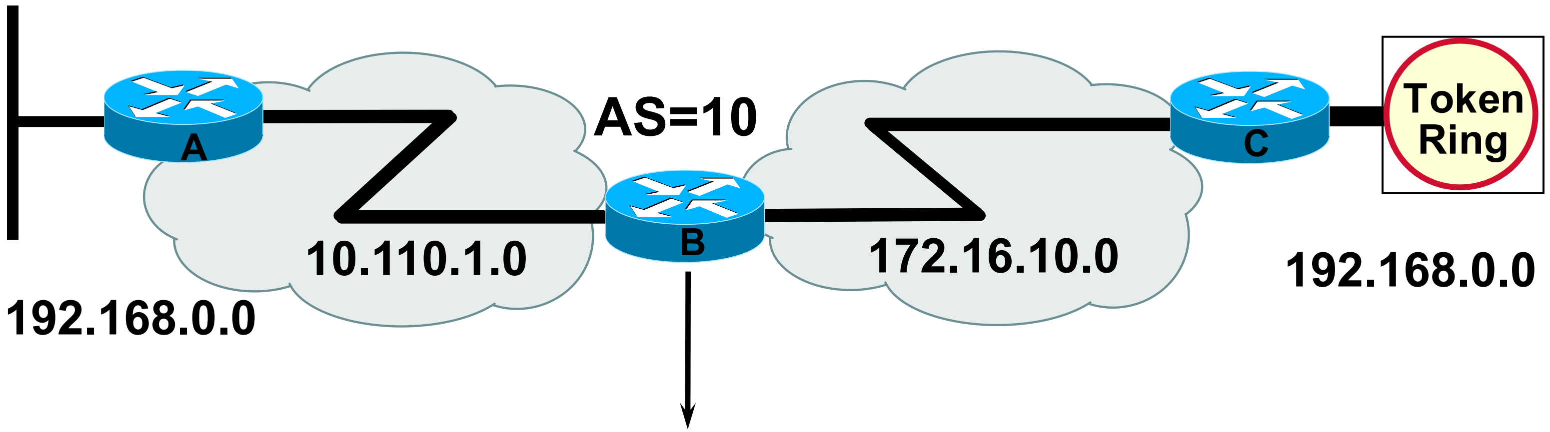
Routing Table—IP	
Destination 1	Successor

Choosing Routes



- EIGRP uses a composite metric to pick the best path: bandwidth and delay of the line
- EIGRP will keep up to six feasible successors in the topology table.

Configuring EIGRP for IP



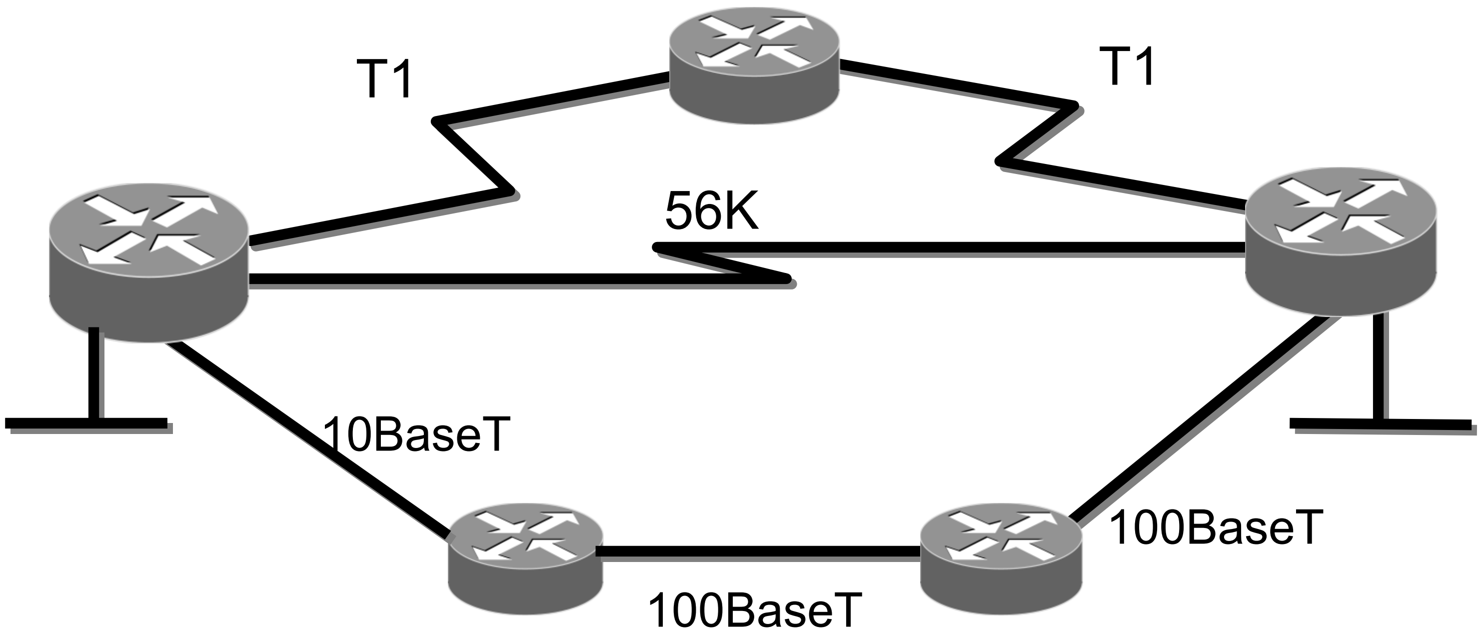
Enable EIGRP → Router(config)#**router eigrp 10**

Assign networks → Router(config-router)#**network 10.0.0.0**

→ Router(config-router)#**network 172.16.0.0**

Route Path

Assuming all default parameters, which route will RIP (v1 and v2) take, and which route will EIGRP take?



- RIPv1 and RIPv2 use the same metric (hop count) and would find the 56K link the best path to the remote network.
- EIGRP and IGRP use the same metric as well (bandwidth and delay of the line) and would use the path through the LAN interfaces, not the serial T1's.

Verifying Enhanced IGRP Operation

Router# **show ip eigrp neighbors**	• Displays the neighbors discovered by IP Enhanced IGRP
Router# **show ip eigrp topology**	• Displays the IP Enhanced IGRP topology table
Router# **show ip route eigrp**	• Displays current Enhanced IGRP entries in the routing table
Router# **show ip protocols**	• Displays the parameters and current state of the active routing protocol process
Router# **show ip eigrp traffic**	• Displays the number of IP Enhanced IGRP packets sent and received

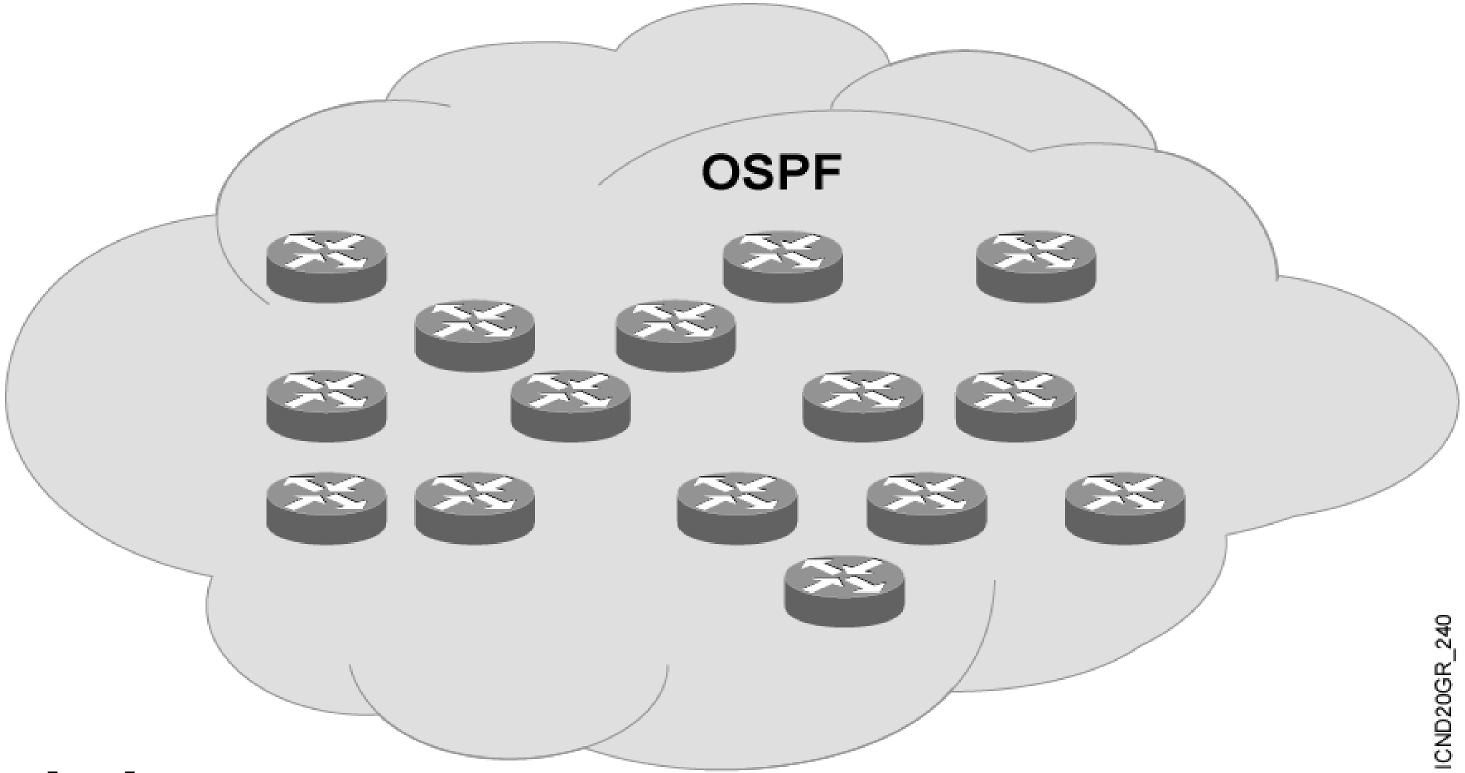
Show IP Route

```
P1R1#sh ip route
[output cut]
Gateway of last resort is not set
D    192.168.30.0/24 [90/2172] via 192.168.20.2,00:04:36, Serial0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/0
D    192.168.40.0/24 [90/2681] via 192.168.20.2,00:04:36, Serial0/0
C    192.168.20.0/24 is directly connected, Serial0/0
D    192.168.50.0/24 [90/2707] via 192.168.20.2,00:04:35, Serial0/0
P1R1#
```

-D is for “Dual”

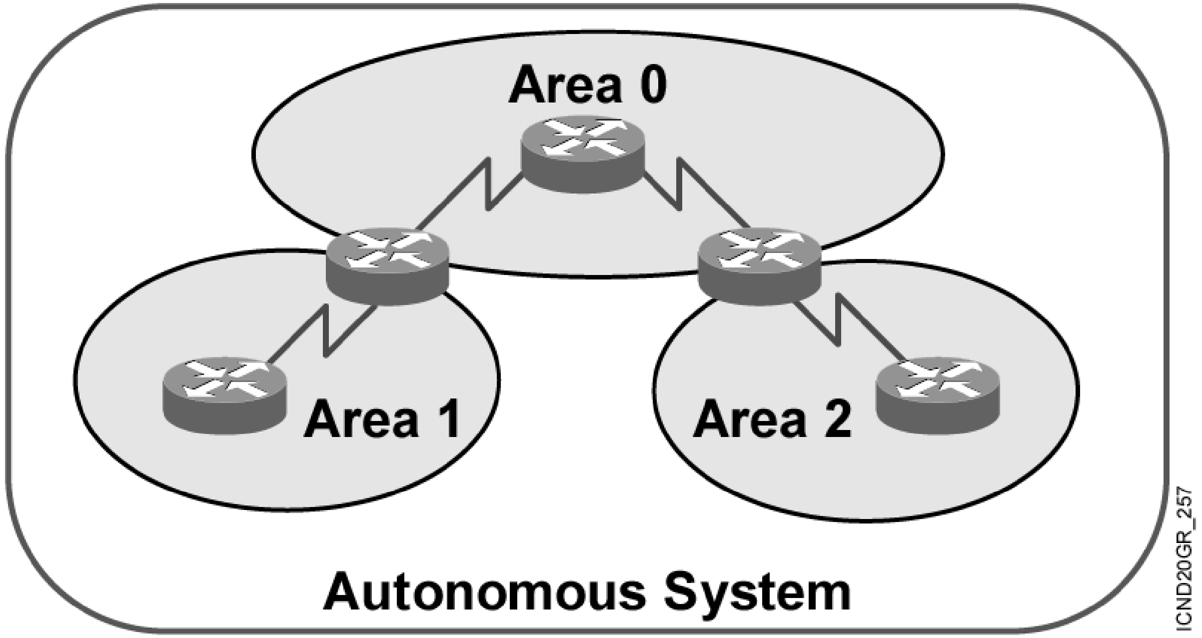
-[90/2172] is the administrative distance and cost of the route. The cost of the route is a composite metric comprised from the bandwidth and delay of the line

Open Shortest Path First (OSPF)



- Open standard
- Shortest path first (SPF) algorithm
- Link-state routing protocol
- Can be used to route between AS's
- OSPF converges quickly, although perhaps not as quickly as EIGRP, and it supports multiple, equal-cost routes to the same destination.

OSPF Hierarchical Routing



- Consists of areas and autonomous systems (OSPF is supposed to be designed in a hierarchical fashion, which basically means that you can separate the larger internetwork into smaller Internetworks called areas.)
- Minimizes routing update traffic
- Supports VLSM
- Unlimited hop count

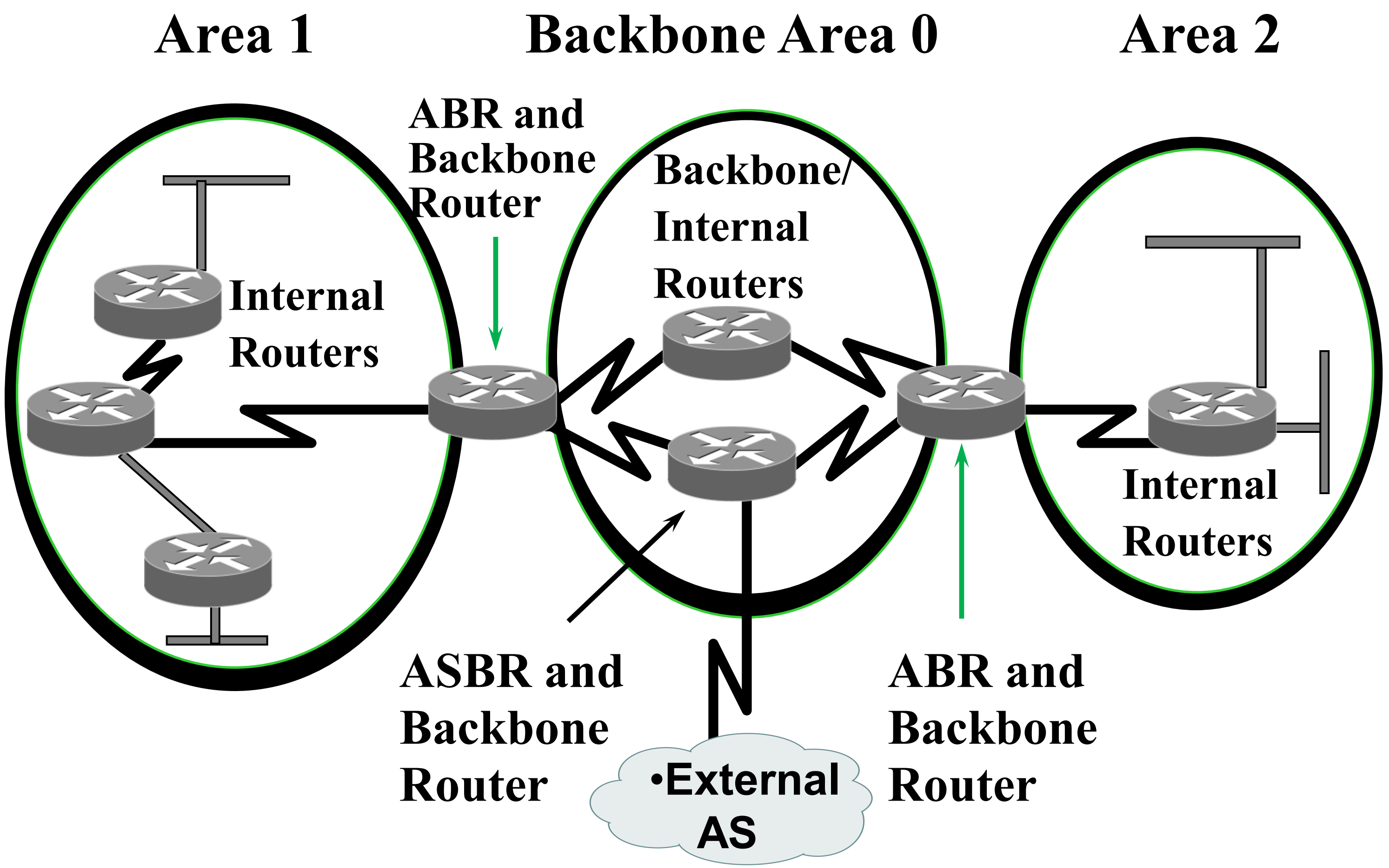
Types of OSPF Routers

- OSPF must have an area 0 (called the backbone area), and all OSPF areas must connect to area 0

- Routers that connect other areas within an AS together are called Area Boundary Routers (**ABRs**).
- Still, at least one interface must be in area 0.

- OSPF runs inside AS, but can also connect multiple autonomous systems together.

- The router that connects these AS's together is called an Autonomous System Boundary Router (**ASBR**).



Link State Vs. Distance Vector

Link State:

- Provides common view of entire topology
- Calculates shortest path
- Utilizes event-triggered updates
- Can be used to route between AS's

Distance Vector:

- Exchanges routing tables with neighbors
- Utilizes frequent periodic updates

Configuring OSPF

- Configuring basic OSPF isn't as simple as RIP, IGRP and EIGRP, and it can get really complex once the many options that are allowed within OSPF are factored in.
- These two elements are the basic elements of OSPF configuration:
  - Enabling OSPF
  - Configuring OSPF areas

```
Router(config)#router ospf process-id
```

- OSPF process ID is locally significant meaning that it is local to the router. Cisco IOS are able to run multiple OSPF processes on the same device.
- Its role is mainly use to distinguish between multiple OSPF processes running on the same physical interface.
- The easiest, and also least scalable way to configure OSPF is to just use a single area.

Configuring Single Area OSPF

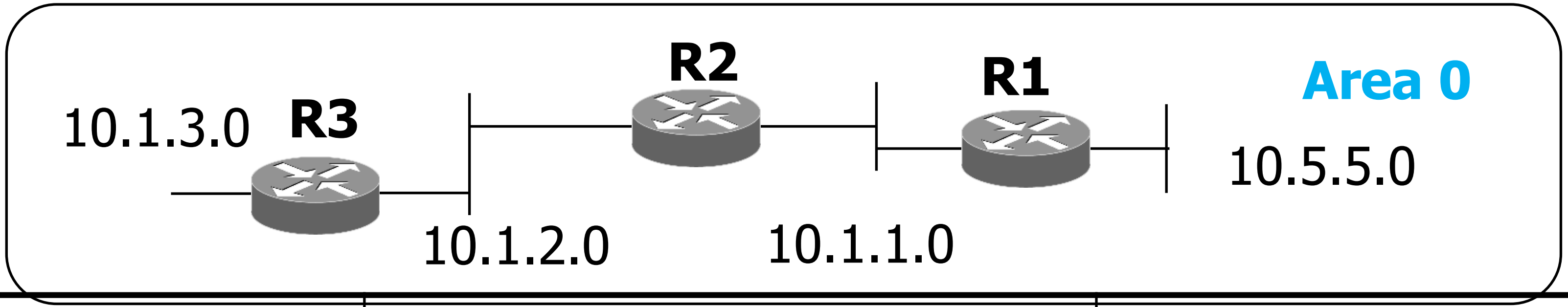
```
Router(config-router)#network address wildcard-mask area area-id
```

- A 0 octet in the **wildcard mask** indicates that the corresponding octet in the network must match exactly. On the other hand, a 255 indicates that you don't care what the corresponding octet is in the network number.

- A network and wildcard mask combination of 1.1.1.1 0.0.0.0 would match 1.1.1.1 only, and nothing else. This is really useful if you want to activate OSPF on a specific interface.

- If you insist on matching a range of networks, the network and wildcard mask combination of 1.1.0.0 0.0.255.255 would match anything in the range 1.1.0.0–1.1.255.255. Because of this, it's simpler and safer to stick to using wildcard masks of 0.0.0.0 and identify each OSPF interface individually.

OSPF Example



hostname R3	hostname R2	hostname R1
router ospf 10 network 10.1.2.3 0.0.0.0 area 0 network 10.1.3.1 0.0.0.0 area 0	router ospf 20 network 10.0.0.0 0.255.255.255 area 0	router ospf 30 network 10.1.0.0 0.0.255.255 area 0 network 10.5.5.1 0.0.0.0 area 0

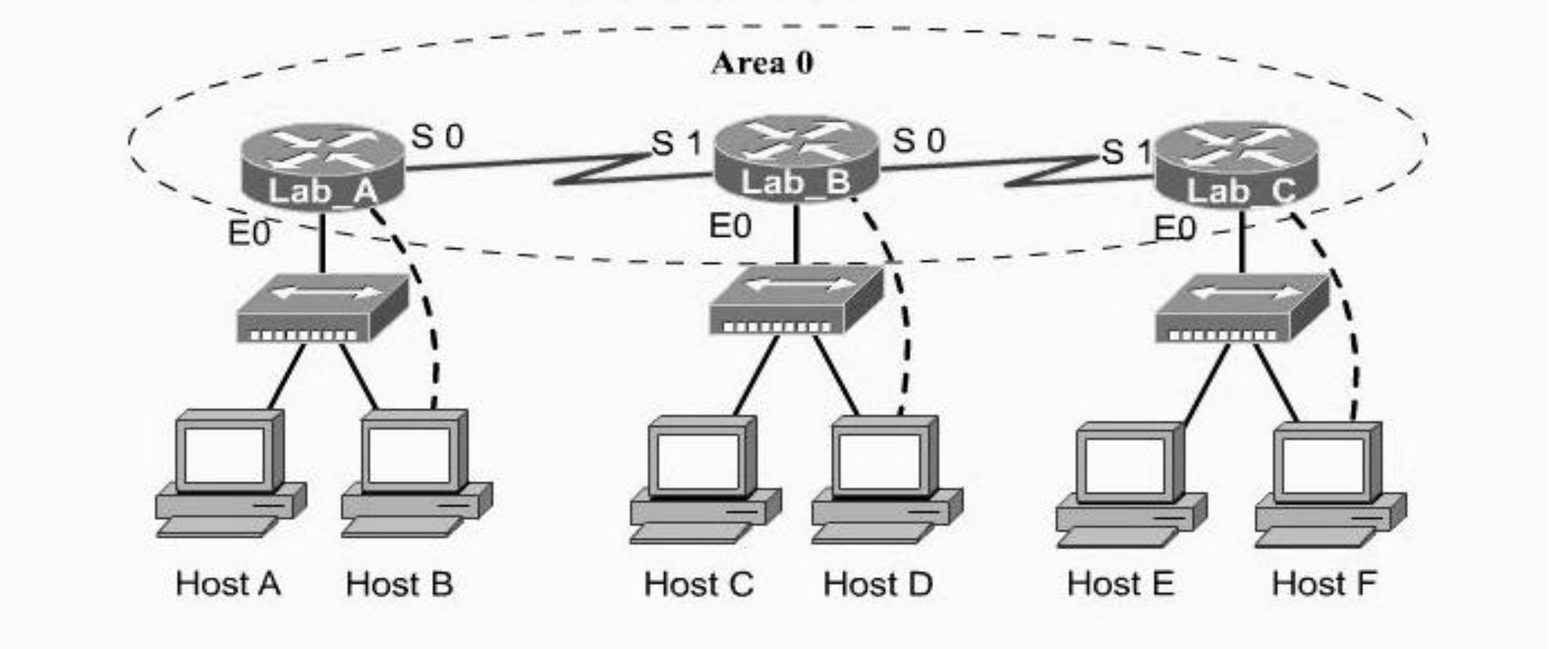
- The configuration of R3 shows how the 0.0.0.0 wildcard is used to place each interface individually into area 0
- R2 show how two interface can be configured into area 0 with one wildcard network statement of 0.255.255.255
- R1 shows the wildcards of 0.0.255.255 and 0.0.0.0
- It doesn't matter how you configure the network statements, the results are the same.
- Remember, the process ID is irrelevant and can be the same on each router, or different on each router, as they are in this example.

Wildcard

The wildcard address is always one less than the block size….

- 192.168.10.8/30 = 0.0.0.3
- 192.168.10.48/28 = 0.0.0.15
- 192.168.10.96/27 = 0.0.0.31
- 192.168.10.128/26 = 0.0.0.63

Wildcard Configuration of the Lab_B Router



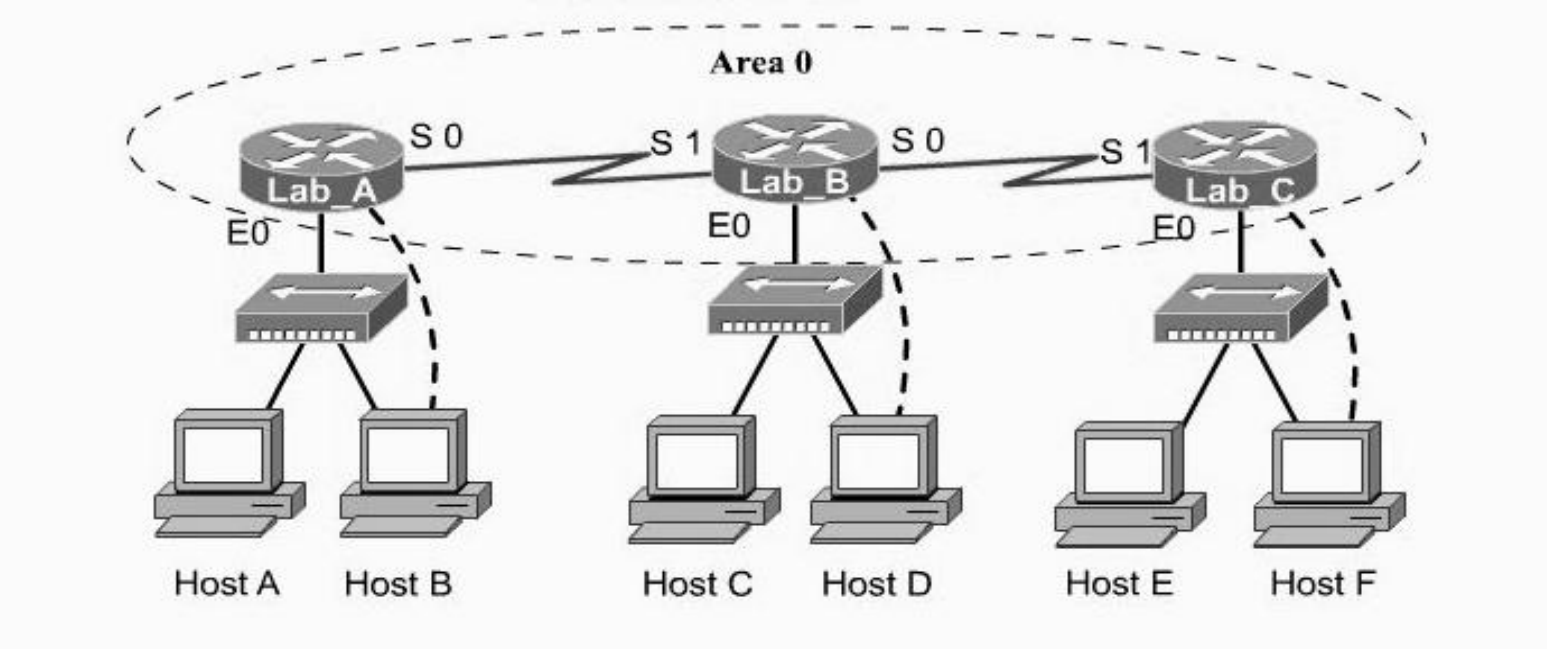
- Lab_A
- E0: 192.168.30.1/24
- S0: 172.16.10.5/30

- **Lab_B**
- **E0: 192.168.40.1/24**
- **S0: 172.16.10.10/30**
- **S1: 172.16.10.6/30**

- **Lab_C**
- **E0: 192.168.50.1/24**
- **S1: 172.16.10.9/30**

```
router ospf 1
Network  192.168.40.1 0.0.0.0 area 0
Network  172.16.10.8  0.0.0.3 area 0
Network  172.16.10.4  0.0.0.3 area 0
```

Wildcard Configuration of the Lab_B Router



- Lab_A
- E0: 192.168.30.1/24
- S0: 172.16.10.5/30

- **Lab_B**
- **E0: 192.168.40.1/24**
- **S0: 172.16.10.10/30**
- **S1: 172.16.10.6/30**

- **Lab_C**
- **E0: 192.168.50.1/24**
- **S1: 172.16.10.9/30**

NOTE: to remove a bad entry, use the following example:
Router(config)#router ospf 1
Router(config-router)#no network 192.168.10.4 0.0.0.4 area 0
Router(config-router)#network 192.168.10.4 0.0.0.3 area 0

OSFP Neighbors

- OSPF uses hello packets to create adjacencies and maintain connectivity with neighbor routers
- OSPF uses the multicast address 224.0.0.5

•**Hello packets** provides dynamic neighbor discovery
•**Hello Packets** maintains neighbor relationships
•**Hello packets** and (Link State Advertisement) LSA's from other routers help build and maintain the topological database
•Link State Advertisement (LSA) is an OSPF data packet containing link-state and routing information that's shared among OSPF routers.

Loopback interfaces

- **Loopback interfaces** are logical interfaces, which are virtual, software-only interfaces; they are **not real router interfaces**.
- You use the loopback interface to identify the device. While you can use any interface address to determine if the device is online, the loopback address is the preferred method. Whereas interfaces might be removed or addresses changed based on network topology changes, the loopback address never changes.
- If a loopback interface is configured with an IP address, the Cisco IOS software will use this IP address as its **router ID**, even if other interfaces have larger IP addresses. Because loopback interfaces never go down, greater stability in the routing table is achieved
- Using loopback interfaces with your **OSPF configuration** ensures that an interface is always active for OSPF processes.

Router ID (RID)

- Each router that is participating in OSPF needs to be uniquely identified. The method of identification that OSPF uses is **Router IDs (RID) - 32 bits .**

- Highest IP address in router is **RouterID** Overridden by Loopback interface if present Even if Loopback address has lower value

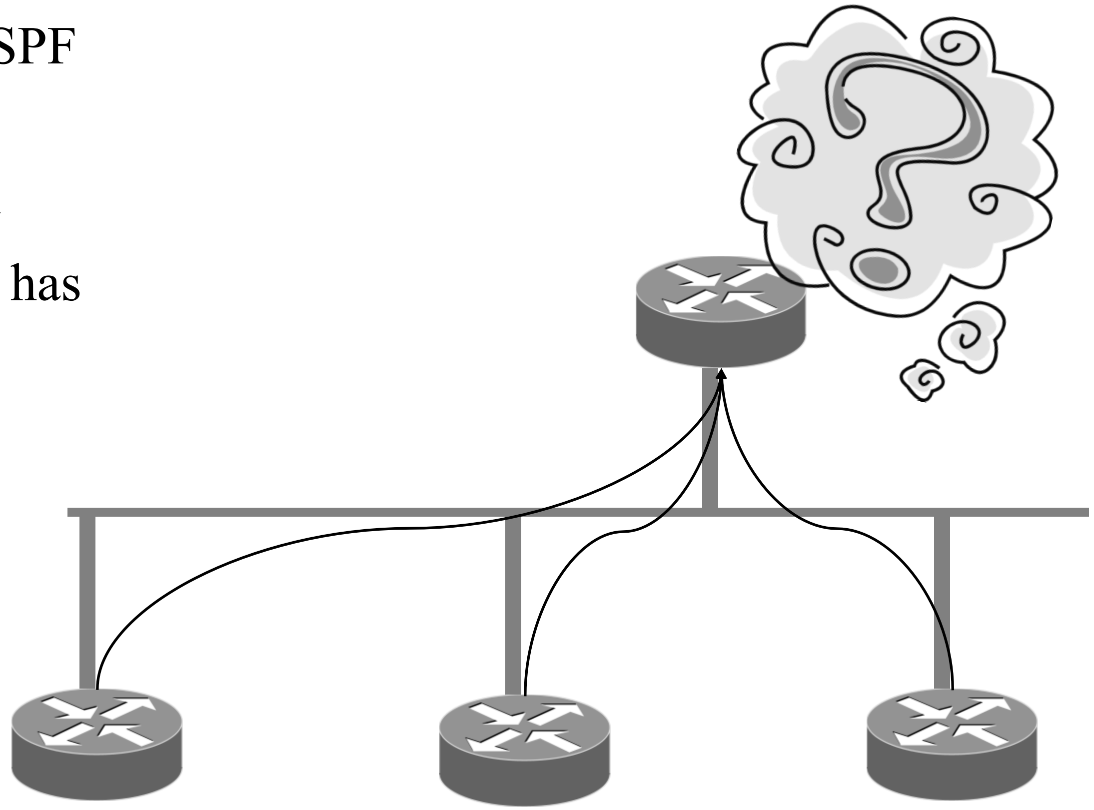
- Recommended to use loopback interface
  - ✓ Easier to manipulate this number
  - ✓ Always up

Interface loopback 0
Ip address 10.1.1.1 255.255.255.0

- You can also Statically assign the Router ID in the OSPF router configuration mode:

(config)# router ospf 1
(config)#router router-id

- **Do NOT use same loopback address on different routers**



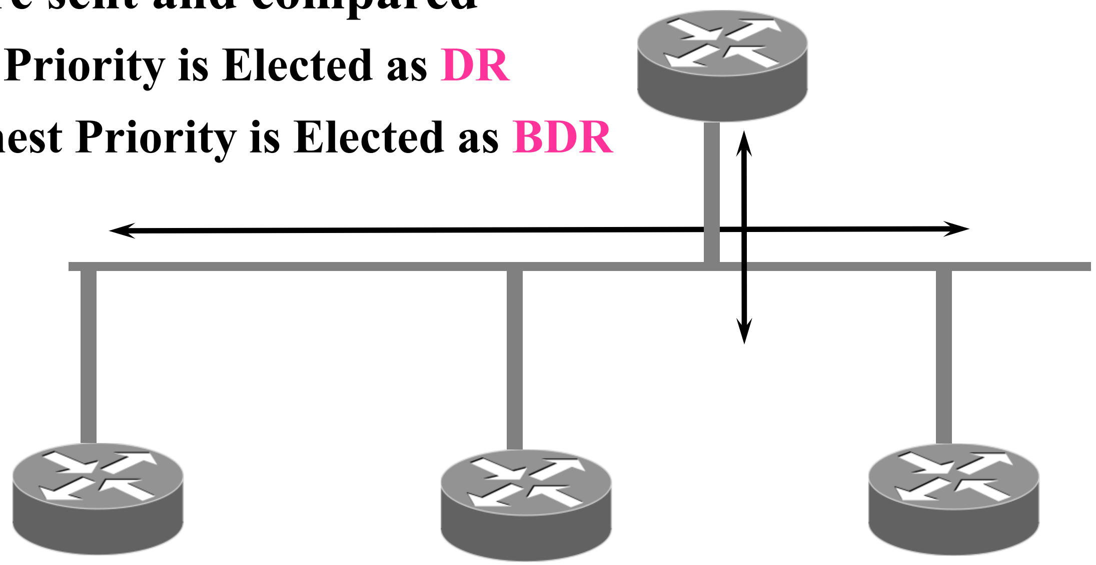
Each router in OSPF needs to be uniquely identified to properly arrange them in the Neighbor tables.

Electing the DR and BDR

Multicast Hellos are sent and compared

Router with Highest Priority is Elected as DR

Router with 2nd Highest Priority is Elected as BDR



- **DR**: the primary router responsible for exchanging routing information with all other routers on the segment. It acts as a central point for routing updates.

- **BDR**: The BDR is a backup for the DR. If the DR fails, the BDR takes over its role.

- OSPF sends Hellos which elect DRs and BDRs (to act as the main point of contact for the network segment)
- Router form adjacencies with DRs and BDRs in a multi-access environment

Electing the DR and BDR

- The following outlines the process OSPF takes and rules that are followed when electing a **Designated Router** based on:
    1. Priority
    2. Router ID
- Routers elect a DR and BDR per network
- All routers set by default to priority 1 (0-255)
- Router with highest priority wins DR (1 – 255).
- If DR fails, BDR promoted to DR and a new BDR is elected
- Existing DR will not be overthrown if “better” router is turned on after initial election
- DRs and BDRs listen to multicast traffic on both multicast address 224.0.0.5 and 224.0.0.6

Interface Priorities

What is the default OSPF interface priority?

- Sometimes it is desirable for a router to be configured so that it is not eligible to become the DR or BDR.
- You can do this by setting the OSPF priority to zero with the ip ospf priority priority# interface subcommand.

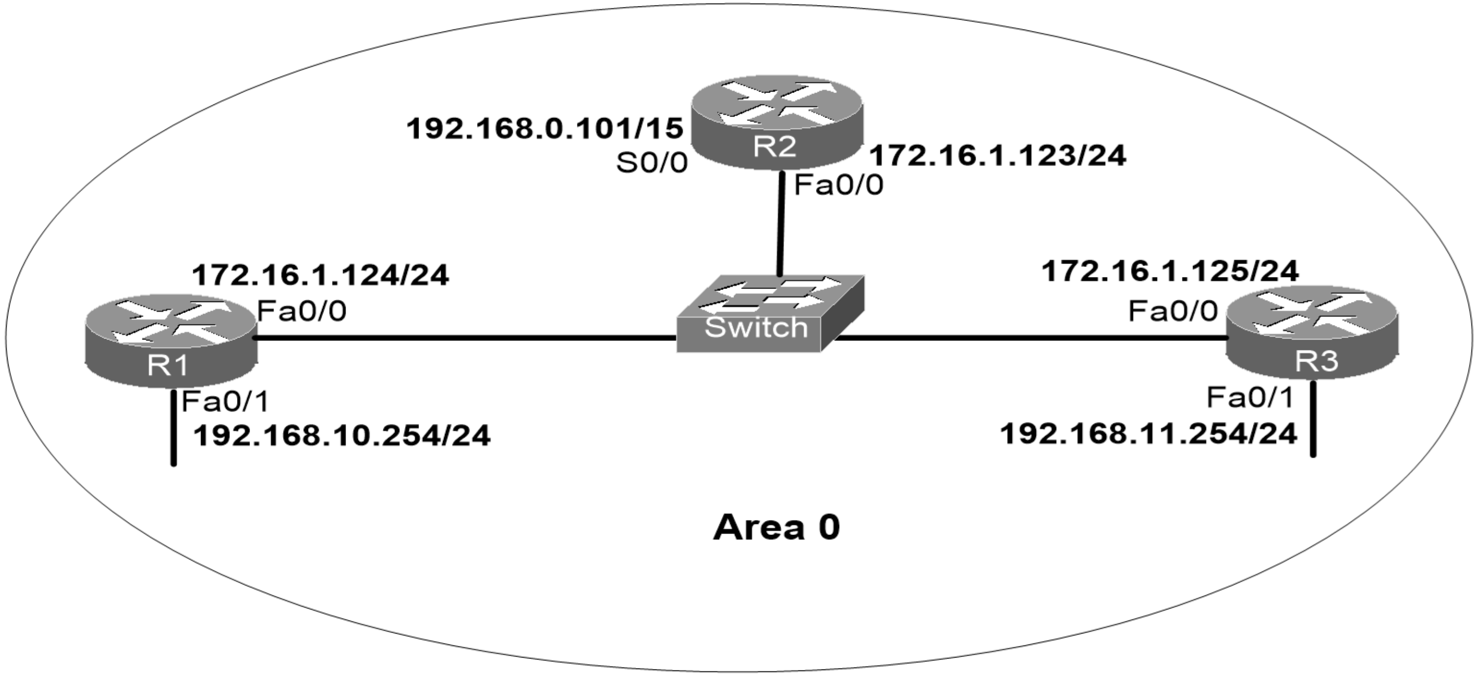
- Router(config-if)# ip ospf priority {0 – 255}
  - Change the priority of a router on an interface
  - 0 means to not participate in election
  - 1 is default, 255 is highest priority

Ensuring your DR

What options can you configure that will ensure that R2 will be the DR of the LAN segment?

There are three options that will ensure that R2 will be the DR for the LAN segment 172.16.1.0/24:

1. Configure the priority value of the Fa0/0 interface of the R2 router to a higher value than any other interface on the Ethernet network
2. Configure a loopback interface on the R2 with an IP address higher than any IP address on the other routers
3. Change the priority value of the Fa0/0 interface of R1 and R3 to zero



Verifying the OSPF Configuration

Router#**show ip protocols**	Verifies that OSPF is configured
Router#**show ip route**	Displays all the routes learned by the router
Router#**show ip ospf interface**	Displays area-ID and adjacency information
Router#**show ip ospf neighbor**	Displays OSPF-neighbor information on a per-interface basis