EIGRP Routing Protocol

Overview

Welcome to the world of EIGRP. In this chapter, we will look at CISCO's proprietary routing protocol which is EIGRP. In part 1, we will look at the foundation concepts into distance vector routing protocols operation. We will then look at the EIGRP concepts and get to know how it works as well as basic configuration of EIGRP, we will also look at verification of EIGRP. In the second part we will look at other EIGRP concepts such as load balancing, and passive interfaces. So let's get into it.

Distance vector routing protocols

As we discovered from the previous chapter, Interior Gateway Protocols, can be classified into two; distance vector routing protocols and link-state routing protocols. In this section, we will explore distance vector routing protocols, these concepts will be crucial in understanding EIGRP.

The name Distance Vector means that the routes that are advertised by these routing protocols are usually sent as vectors of direction and distance.

If we were to use an analogy of a tourist in a foreign land, distance vector protocols would be described as road signs that only state the direction and the distance to get to a particular destination. They do not give any inclination as to the whole country. The tourist only knows of another point once they get to the point they were directed to by another road sign.

In this same way, distance vector routing protocols only say the next hop or the direction to a destination and the metric or the distance to get there.

A router using a distance vector routing protocol does not have the knowledge of the entire path to a destination network. Instead the router knows only:

- The direction or outbound interface
- Distance or metric towards the destination

There are several characteristics inherent with distance vector routing protocols.

- Periodic updates sent at regular intervals or bounded updates.
- Neighbors are directly connected routers.
- Entire routing table updates with the exception of EIGRP

Like all other routing protocols, the use of an algorithm is usually to determine the best path. The routing update usually defines mechanisms for:

- Exchange of Routing information by sending and receiving messages.
- A means to calculate the best path
- A method to determine topology changes and updating accordingly.

When the routers configured with the same routing protocol boot up, the following happens before communication can happen between hosts.

- Exchange of initial information. This may include routing protocol security, discovery packets among others.
- Exchange of routes. The routers exchange routes by examining updates they receive via broadcast from other routers. They examine the routes they have learnt from their neighbors and based on the algorithm calculations, the best path is added to the routing table.

- Convergence. This is the state where all routers in the routing domain have exchanged routing information. All the routers can communicate. The speed by which this happens depends on;
    - How many routers are in the routing domain.
    - The speed by which the routers learn of new routes when there is a topology change.
    - The speed of the algorithm to calculate the costs to each network in the topology.

The concepts behind the distance vector routing protocols are crucial to understanding routing using EIGRP. In the next section we will begin our discussion on EIGRP.

Introduction to EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol), is CISCO's second proprietary routing protocol that was first released in 1992. It was a classless advancement to CISCO's first proprietary routing protocol IGRP. Since this is a CISCO proprietary protocol, it only runs on CISCO routers.

In previous chapters, we looked at the difference between classful and classless routing protocols. We said that the classless routing protocols include the subnet mask in advertising networks and thus VLSM and CIDR can be used.

Some of the most notable features of EIGRP include the following.

- RTP – Reliable Transport Protocol
- Bounded updates – updates are only sent if and when there is a topology change and to affected routers.
- It uses the DUAL algorithm (Difussion Update Algorithm) to find the best paths
- It establishes adjacencies with neighboring routers

- It maintains the neighbor table, the topology table as well as the routing table

The operation of EIGRP has some similarities with link-state routing protocols such as OSPF, however, it is still a distance vector routing protocol.

The Algorithm

The DUAL algorithm is the engine that is used by EIGRP in path determination and maintaining updated routes. This is unlike other distance vector routing protocols which use the Bellman-Ford algorithm. When a change is detected in an EIGRP routing domain, the routers exchange several messages to establish redundant links or to update accordingly. The updates in EIGRP are usually partial and bounded, this means that if a route goes down, the router will only notify affected routers of the missing route and it will only notify them of the missing route.

The routing updates that are sent using EIGRP are vectors of distance and are only transmitted to the directly connected and affected neighboring routers in the routing domain.

Protocol-dependent modules (PDM)

The operation of EIGRP is not limited to the IP protocol, EIGRP can route for different network layer protocols such as IP, IPX and apple talk. This support is made possible through the use of (PDMs) Protocol-Dependent Modules.

Reliable Transport Protocol (RTP)

The messages that are transmitted in an EIGRP routing domain are supported by RTP (Reliable Transport Protocol). This protocol requires that acknowledgement packets be sent for the various messages by the recipient of a particular message. The address used by this protocol to run is the EIGRP multicast address of 224.0.0.10.

EIGRP Packet Types

The packet types in EIGRP are crucial in understanding how it exchanges routing information. It is important to note that there are 5 packet types that EIGRP uses to maintain adjacencies. Some of them are used in pairs as discussed below.

Hello packets

The Hello packet is the first packet that is sent when EIGRP is configured, this packet is sent to discover neighbors and form adjacencies with those neighbors. The hello packet is usually sent in intervals of 60 seconds on slow links and at intervals of 5 seconds on links with bandwidth exceeding 1.544mbps such as T1 links.

The EIGRP hello packet also has a hold timer, which is three times the length of the hello packet. if a router in an EIGRP routing domain does not respond to three hellos, it is usually considered as down. The reply to hellos means that the routes are still active.

NOTE: the hello packet is one of the best ways to diagnose EIGRP issues. The use of debugging commands can help establish where the problems occur in EIGRP.

Update

In EIGRP, the update packets are used to send routing information to its neighbors. As we mentioned earlier, the routing updates that are sent by EIGRP are usually partial and bounded. This means that unless there is a topology change, the updates are not usually sent. When a topology change has been detected, the EIGRP update packets are either sent as a unicast to a single affected router or multicast to several affected routers in the routing domain.

Acknowledgement (ACK)

The ACK packets are used to verify that updates or other types of messages were received. RTP ensures that ACK messages are delivered using Reliable delivery.

Query and reply packets

When a router is missing a route, it is the work of the query and reply packets to probe neighbors for the missing routes. The queries are usually sent as multicast messages, while the replies are usually unicast messages.

EIGRP and routes propagation

When routers configured with EIGRP boot up, the hello messages are usually sent to all the routers in the domain to form adjacencies, when the neighbors reply, they form neighbor relationships. The routers then send updates containing their information to the neighbors. When this is done, the routers draw up a topology table with all the best routes as well as alternative or backup paths. From this the best path is determined and used for packet forwarding.

NOTE: we will learn more on this when we discuss DUAL in more detail at a subsequent chapter.

Advantages and disadvantages of EIGRP

Some of the advantages of EIGRP are listed below.

- As compared to other routing protocols, EIGRP is very fast to converge and re-converge in the event of failure.
- Simplified configuration compared to link-state routing protocols and static routing
- The range of features is more than any other IGP
- Route summarization at any point in the network

- Supports load balancing

The main disadvantage of EIGRP in the networking world is the fact that it is CISCO proprietary. This means that a network that may have router brands other than CISCO would not be able to run EIGRP.

EIGRP tables

In EIGRP, there are three tables we need to know about.

Neighbor table

This contains all the directly connected routers in the same autonomous system that are running EIGRP. The formation of neighbor relationships is started by the hello packets.

Topology table

The topology table shows all the routes that are known by the router in the EIGRP domain. The topology table shows the main routes, and the backup paths.

Routing table

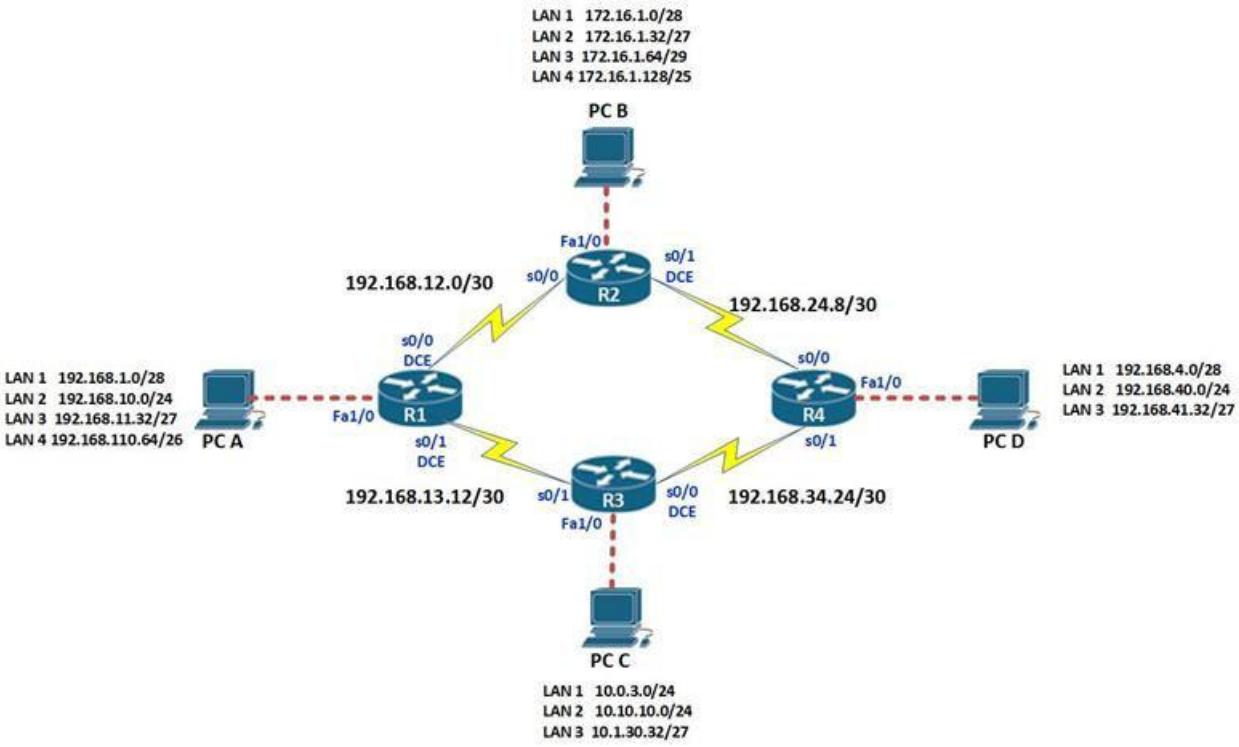
The routing table shows the best route as calculated by DUAL and is used to forward packets in EIGRP.

We will explore more on these concepts further in the coming chapters.

Basic configuration and verification of EIGRP

Now that we have understood some of the concepts that make EIGRP work, it is time to do the basic configuration.

The diagram shown below will be the main topology that will be used in EIGRP. We will switch things up a bit but it will be the main reference diagram.



The topology that is shown consists of four routers and four host PCs. Each router has several routers connected to it. LAN 1 on each of the routers is the network segment for the PCs. The other LANs have been configured using loopback interfaces.

Please note that this will be the main topology used in EIGRP although some segments may change, this should be kept in mind.

The table below shows the ip addressing scheme used on this network.

Device name	Interface n	Ip address	Subnet mask	Default gateway
PC A	NIC	192.168.1.2	255.255.255.240	192.168.1.1
R1	Fa1/0	192.168.1.1	255.255.255.240	
	S0/0	192.168.12.1	255.255.255.252	
	S0/1	192.168.13.13	255.255.255.252	
	Lo0	192.168.10.1	255.255.255.0	
	Lo1	192.168.11.33	255.255.255.224	
	Lo2	192.168.110.65	255.255.255.192	
PC B	NIC	172.16.1.2	255.255.255.240	172.16.1.1
R2	Fa1/0	172.16.1.1	255.255.255.240	
	S0/0	192.168.12.2	255.255.255.252	
	S0/1	192.168.24.9	255.255.255.252	
	Lo0	172.16.1.33	255.255.255.224	
	Lo1	172.16.1.65	255.255.255.248	
	Lo2	172.16.1.129	255.255.255.128	
PC C	NIC	10.0.3.2	255.255.255.0	10.0.3.1
	Fa1/0	10.0.3.1	255.255.255.0	
	S0/1	192.168.13.14	255.255.255.252	
	S0/0	192.168.34.25	255.255.255.252	
	Lo0	10.10.10.1	255.255.255.0	
	Lo1	10.1.30.33	255.255.255.224	
PC D	NIC	192.168.4.2	255.255.255.240	192.168.4.1
	Fa1/0	192.168.4.1	255.255.255.240	
	S0/0	192.168.24.10	255.255.255.252	
	S0/1	192.168.34.26	255.255.255.252	
	Lo0	192.168.40.1	255.255.255.0	
	Lo1	192.168.41.33	255.255.255.224	

The first thing we need to understand is the autonomous system.

The autonomous system, is a way to identify all networks which are controlled or owned by a single entity and which may have the same policies. In EIGRP, the AS is always the same. A different name is the routing domain.

The process ID, is needed to identify the EIGRP process on the routing domain. If we needed several instances of EIGRP to run on 1 router, we would need different process IDs to identify each of them.

NOTE: the process id must match on all routers in the routing domain for EIGRP to work.

On all the routers, we need to go into the global configuration mode, and start the EIGRP routing protocol by entering the command:

"**router eigrp <process_ID>**"

This command is used to initiate EIGRP on a router. The process-ID, in EIGRP is a numeric value between 1 and 65536. And it identifies the EIGRP process as 1. This means that we can have several instances of EIGRP running on a router, however, communication will only work when the process_ID is the same in the routing domain. Therefore and EIGRP process 1 cannot communicate with and EIGRP process 2.

In our scenario, the process-ID we will use will be 100. And the command needed on R1 is as shown below.

```
R1(Config)#router eigrp 100
```

This command should be entered on all the routers in this routing domain. When this command is executed, we will enter the specific configuration mode for EIGRP which is denoted by the prompt shown below.

```
Router(config-router)#
```

Dynamic routing protocols work by advertising their directly connected networks. Therefore, on the routers, we need to advertise these networks using the command shown below.

Router(config-router)# network <network-ID> <subnet mask>

The network should be the specific subnet that is being advertised. On R1 for example, we will advertise all the subnets that are directly connected to it.

Even though EIGRP is a classless routing protocol, it behaves as a classful routing protocol. This means that the routes will be automatically summarized to their default classes. This means that we can miss some routes even though our configuration is correct. This means that we need to disable default route summarization to the classful boundaries using the command:

Router(config-router)# network no auto-summary

NOTE: for this command to work effectively, it is usually best practice to execute it immediately after the router eigrp command.

Verification of EIGRP

After the configuration on all the routers, we need to verify that EIGRP is indeed configured and working on all the routers. The commands needed to do this are:

- Show ip eigrp interfaces – this will show the interfaces participating in EIGRP as well as the process ID
- Show ip route – this will show the main routes used for traffic forwarding that have been learnt via EIGRP
- Show ip eigrp topology – this will show all the primary and backup routes that EIGRP has learnt as well as the process ID
- Show ip eigrp neighbors – this will show the neighbors that each router has as well as the process ID
- Debug ip eigrp – this will show the eigrp statistics for each router actively.

OSPF Routing Protocol

Overview

Welcome to the world of OSPF (Open Shortest Path First) routing. This protocol was developed to replace RIP and it is a classless Link State routing protocol that uses areas so as to scale better. This chapter is divided into four parts since it is too broad. The concepts we will learn will be useful in not only the ICND 1, ICND 2 and CCNA composite exam but also in the real world.

In part 1 of this chapter, we will review concepts on link-state routing protocols and learn how they work. We will then look at the OSPF packets and discuss the algorithm that OSPF uses to find the best part. We will then configure OSPF in a single area and finally we will learn some of the commands that can be used to verify OSPF.

The concepts you will learn in this part, will be important in understanding OSPF in the routing world and will be useful as you progress in your studies in CCNP and CCIE.

Link-state routing protocols

As we learnt in a previous chapter, internal routing protocols fall into two categories, distance vector routing protocols and link state routing protocols. OSPF falls in the link-state routing protocol category. We also used an analogy of a tourist trying to find his destination using a map and said that this is how link state routing protocols work.

Link-state protocols work by calculating the cost along the path from a source network to the destination network and use the SPF algorithm which was developed by Edsger Dijkstra. the steps shown below describe how Link-state routing protocols such as OSPF work.

1. All the routers that have been configured with the link-state routing protocol in a domain will learn about the directly connected networks.

2. The routers that share a link will recognize the neighboring routers and form relationships.
3. When this relationship has been formed, they will share their directly connected routes with each other. This is done when the router in a link-state routing protocol sends a packet that contains the routes.
4. The neighbors that receive this information will then propagate it to other neighbors.
5. When all the neighbors know oof all the routes, each router will use the information to create a “MAP” to all the destinations in the networks.
6. When this map has been created, the SPF (Shortest Path First) algorithm, is run to determine which the best route to a particular remote network is.

This is the basic operation of Link state routing protocols such as OSPF and IS-IS, we will continue learning these steps in more detail as we continue in the world of OSPF.

OSPF operation

In OSPF, the process above is followed, however, the terms differ and are discussed in this section. There are key concepts that we need to know, so as to understand the operation of OSPF.

OSPF packets types

There are 5 different types of packets in OSPF that we need to understand. These are:

1. **Hello** – this are the first messages that are sent by routers that have been configured with OSPF. they use the multicast IP address specially reserved for

OSPF which is 224.0.0.5. the hello packets are used sent so as to discover neighbors and maintain relationships – adjacency with them.

NOTE: hello packets are multicast at 10 second intervals in multicast and point to point networks and 30 seconds on NBMA networks. We will explore more of this at a later stage.

in OSPF, the hello packets have three main tasks as listed below.

1. Discovery and establishment of neighbor adjacencies
2. Advertisesment on OSPF parameters needed to form neighbor relationship
3. Election of the DR (Designated Router) and the BDR (Backup Designated Router) in multi-access networks.

1. **DBD (Database Description)**– this packet is a list which contains a summary of routes that have been learnt by a particular router in the routing domain. The router that receives this packet, checks the list against its own link-state database, to discover any missing routes.
2. **LSR – Link-state request –** when a router discovers that it is missing some routes as a result of the information contained in a DBD packet it has received, it sends this packet to the router that informed it of the missing routes, requesting more detailed information on the missing routes. This is done so that it can update its link-state database with these missing routes.
3. **LSU – Link-State Update –** this packet is sent by a router that has information on any missing routes. It contains detailed information about a particular route, including the next-hop information and the cost to reach the particular route that was requested using an LSR.
4. **LSAck – Link-State Acknowledgment –** this is a packet that is sent to confirm that a router has received an LSU.

NOTE: at this stage, you are not expected to fully understand these concepts, we will explore them in more detail as we continue in this chapter.

Dijkstra's algorithm, administrative distance and metric

As mentioned above, OSPF uses the SPF algorithm. The information contained in a router's OSPF link state database is the "MAP" that is used to calculate the best path to a remote network. However, unlike EIGRP, OSPF does not keep backup paths to routes, rather, when a route to a network goes down, the SPF algorithm is run again to determine a backup or alternate path.

OSPF uses an administrative distance of 110. This means that it is preferred over other routing protocols such as RIP, however it is not as trusted as much as EIGRP, static routes and directly connected routes.

The metric used in OSPF is the cost. This is the bandwidth on each link or the cost as configured by the administrator using the ip ospf cost command. More on this will be discussed later.

Advantages of link state routing protocols

There are several advantages of using link state routing protocols. As listed below.

1. **Topology map –** as we have seen earlier, this is a map that is stored in the link-state database and it contains information on all the routes in the domain. This is a major advantage since finding a redundant path is simple. The router simply looks in the MAP for an alternative route and calculates the cost to get there using the SPF algorithm.
2. **Fast convergence –**unlike distance vector routing protocols that have to calculate information on a route they have received before passing it along to other routers, link-state routing protocols usually flood this information to the other routers on

interfaces other than the one they received the packet on. Each router in the domain can then decide whether the information is relevant or not.

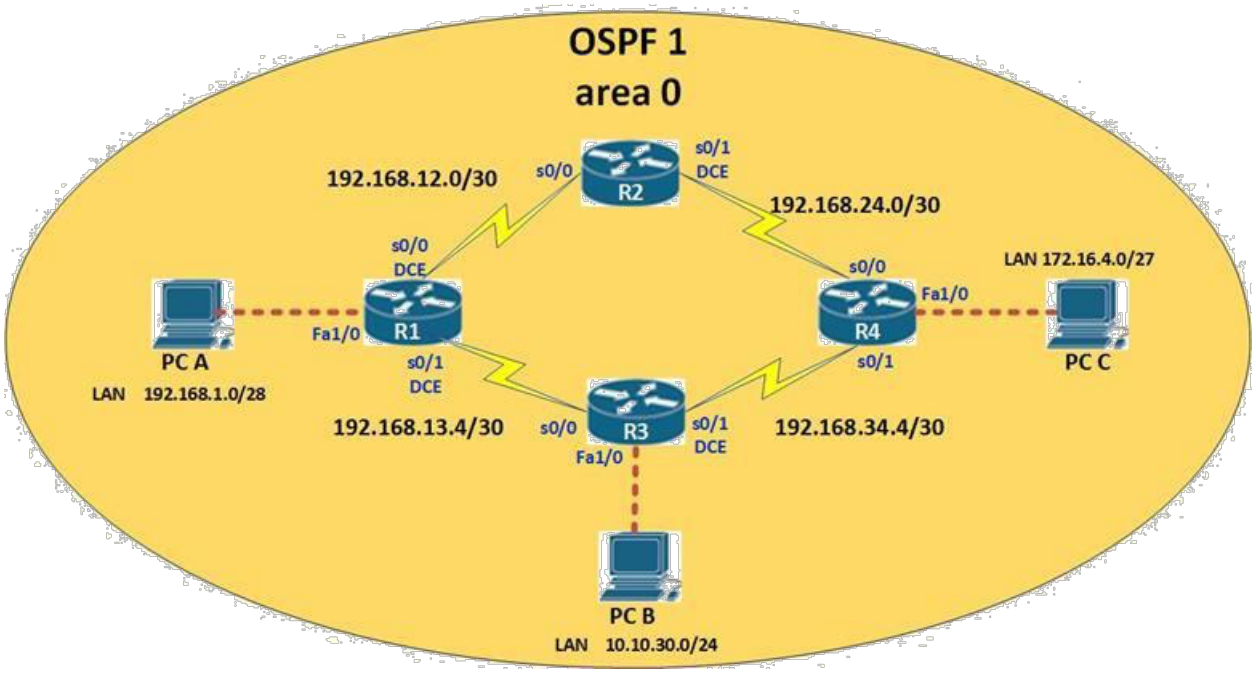
3. **Event-driven updates –** just like in EIGRP, routers in OSPF do not update other routers at regular intervals, rather this is done when a change has occurred and the information that is sent is only pertaining the change.
4. **Hierarchical design –**

   the use of areas is a huge advantage to link-state routing protocols. The use of these areas enables the creation of routes in a hierarchical ip addressing format. However, this means that summarization can only be done at the boundaries between areas.

Now that we have some of the concepts of OSPF, we can get into it and start configuration. More concepts will be introduced in the next part as we continue in this chapter.

The topology

The topology shown below is our lab in this section of OSPF configuration.



The network consists of 4 routers labeled R1 to R4, there are also 3 LAN segments connected to R1, R3 and R4. The ip subnets in use are shown in the diagram and the ip addressing scheme in use is shown below. The clock rate in use on the DCE interfaces is 64000

Device	Interface	Ip address	Subnet mask	Default gateway
PC A	NIC	192.168.1.2	255.255.255.240	192.168.1.1
PC B	NIC	10.10.30.2	255.255.255.0	10.10.30.1
PC C	NIC	172.16.4.2	255.255.255.224	172.16.4.1
R1	Fa1/0	192.168.1.1	255.255.255.240	
	s0/0	192.168.12.1	255.255.255.252	
	s0/1	192.168.13.5	255.255.255.252	
R2	s0/0	192.168.12.2	255.255.255.252	
	s0/1	192.168.24.1	255.255.255.252	
R3	Fa1/0	10.10.30.1	255.255.255.0	
	s0/0	192.168.13.6	255.255.255.252	
	s0/1	192.168.34.5	255.255.255.252	
R4	Fa1/0	172.16.4.1	255.255.255.224	
	s0/0	192.168.24.2	255.255.255.252	
	s0/1	192.168.34.6	255.255.255.252	

Before we begin the OSPFv2 configuration, design the network above and configure the following

- Appropriate host names on all devices
- Appropriate passwords to the console lines and the telnet lines
- Banners
- Disable ip domain lookup
- Ip addresses, subnet masks, default gateways and clock rates appropriately
- Enable the devices and ensure connectivity on directly connected networks

Basic ospf configuration

By now you should be able to do the basic configuration on your own so we will not dwell on it, rather, we will start with the basic OSPF configuration.

Router ospf command.

To enable OSPF on our routers, we need to configure the "**router ospf <process-ID>"**command in the global configuration mode of our routers.

The process-ID is a logically significant number between 1 and 65535, this number is locally signifcicant which means that it only identifies the OSPF process running on a router. You should note that the OSPF process-ID is not the same as the EIGRP processs ID, thus, neighboring routers do not need this number to match so as to form adjacency.

However, in this course, we recommend that you use the same process ID for consistency.

In our topology, we will use 10 as our process ID on all the routers.

So on R1, we need to execute the command shown below.

R1(config)#router ospf 10

This command allows us to enter the OSPF specific configuration mode. From here, we will be able to configure most of the OSPF options that we need.

The network command

Just like in EIGRP, the network command is used to advertise routes in OSPF, however, the format differs a bit: the network command in OSPF is shown below:

router(config-router)#network <network_address> <wildcard_mask> area <area_ID>

Notice that we have two more parameters, which are the wildcard mask and the area ID.

Area– As we discussed earlier, OSPF uses areas, all the routers in an area usually have the same map. In this chapter, we will only deal with the backbone area which is **area 0** this means that all the routers will be in this area.

As the networks grow, the use of multiple-areas is introduced so as to reduce the size of the map. This will be discussed in an upcoming chapter.

NOTE: you must configure the area as "area 0" on all network statements and all routers.

The wildcard mask– or inverse mask is a special type of IP address that is used by OSPF to determine the specific subnet that is being advertised.

Wildcard mask

The wildcard mask is usually the inverse of the subnet mask. To calculate the inverse mask of a network address follow the steps below.

1. Write down the subnet mask of 255.255.255.255 which is the broadcast address for any host or the broadcast address of the zero network (global broadcast address)
2. Write down the subnet mask of the network or the ip address in question
3. Subtract the values of the network's subnet mask from the subnet mask of 255.255.255.255

This is shown in the table below for the network of 192.168.1.0/27

Octet	First	Second	Third	Fourth
Network address	192	168	1	0
Broadcast address	255	255	255	255
Subnet mask	255	255	255	224
Inverse mask	0	0	0	31

Therefore the inverse mask or wildcard mask for the network 192.168.1.0/27 is 0.0.0.31.

When the router is determining the network it should advertise, a value of **"0"** will be considered while any value higher than that will be ignored, therefore in the above example, when advertising network 192.168.1.0/27 in OSPF, the first three octets will be considered, while the fourth octet will only be partially considered.

This means that, when the route 192.168.1.0/27 is advertised,

The router will advertise only routes matching the first three octets and ignore the fourth octet.

NOTE: the most specific wildcard mask that can be used to advertise networks in OSPF is 0.0.0.0, which means that the router will advertise only a specific ip address and not a network address.

Just like in EIGRP, we advertise the directly connected networks that we want to participate in OSPF

To advertise the network 192.168.1.0/28 in OSPF, the command we need on R1 is shown below:

R1(config-router)#network 192.168.1.0 0.0.0.15 area 0

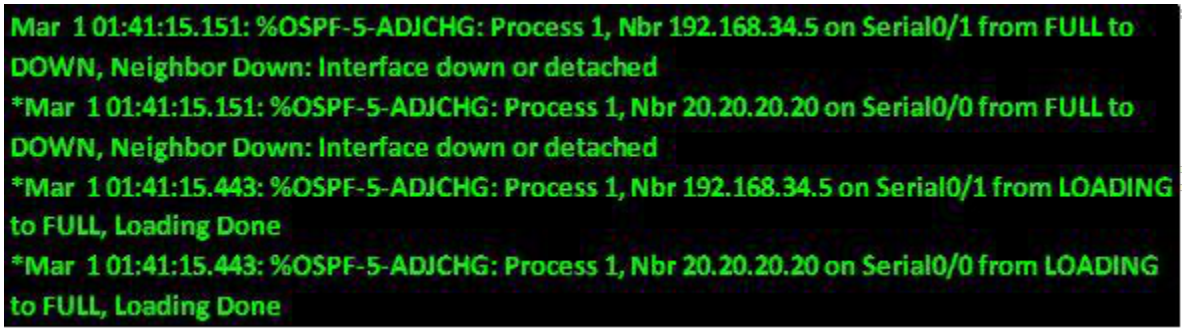
Back to the configuration

In our topology therefore, we will advertise all the directly connected networks on each of the routers using the commands shown in the table below.

Router name	Command
R1	R1(config)#router ospf 1 R1(config-router)#network 192.168.1.0 0.0.0.15 area 0 R1(config-router)#network 192.168.12.0 0.0.0.3 area 0 R1(config-router)#network 192.168.13.4 0.0.0.3 area 0
R2	R2(config)#router ospf 1 R2(config-router)#network 192.168.12.0 0.0.0.3 area 0 R2(config-router)#network 192.168.24.0 0.0.0.3 area 0
R3	R3(config)#router ospf 1 R3(config-router)#network 10.10.30.0 0.0.0.255 area 0 R3(config-router)#network 192.168.13.4 0.0.0.3 area 0 R3(config-router)#network 192.168.34.4 0.0.0.3 area 0
R4	R4(config)#router ospf 1 R4(config-router)#network 172.16.40.0 0.0.0.31 area 0 R4(config-router)#network 192.168.24.0 0.0.0.3 area 0 R4(config-router)#network 192.168.34.4 0.0.0.3 area 0

NOTE: When making these configurations make sure that you calculate all the wildcard-masks so that you understand the concept clearly.

After making these configurations you on all the routers you should be able to see the output shown below:



This shows that OSPF is working and all the routes have been learnt. Notice the speed by which this happens, this is how fast OSPF takes to converge.

OSPF Router-ID

In OSPF, the router-ID is a way to name each router in the routing domain. It is simply an ip address that is specially selected to name a router in OSPF. with CISCO routers, the router-ID is selected based on the criteria shown below.

1. The IP address configured using the command "***router-ID <IP_ADDRESS>"*** in the OSPF configuration mode.
2. If it is not configured, use the highest IP address of any of the configured loopback interfaces.
3. If there is no loopback interface, the router uses the highest IP address of any of the ACTIVE physical interfaces.

NOTE: the highest ACTIVE physical interface is an interface that is able to forward packets.

The use and importance of the router ID will be discussed later.

Configuring the router-ID

The router-ID is configured in the OSPF configuration mode which is denoted by the prompt shown below:

Router(config-router)#

The command used to configure the router-ID is:

router(config-router)#router-id <unique_ip_address>

on R1, we will use the ip address 1.1.1.1 as the router-id and this is configured as shown below.

R1(config-router)#router-id 1.1.1.1

When the command above is executed, the router will be set with the manual router-id of 1.1.1.1

On the four routers, we will use the ip addresses shown in the table below as the router-IDs

Router name	OSPF Router-id
R1	1.1.1.1
R2	20.20.20.20
R3	3.3.3.30
R4	4.40.40.40

Configuring Loopback interfaces

As we mentioned earlier, a loopback interface can be used as the router ID.

A loopback interface is a virtual interface – this means, that it only exists in the router and is not connected to any other physical device in the network. A loopback interface, once configured automatically transitions to UP. The command needed to configure a loopback interface is:

Router(config)#interface <loopback> <Loopback_interface_number>

After executing this command, you will be taken to the interface configuration mode where you can configure other options such as the ip address.

To configure the loopback interface, with an ip address of 172.16.1.1/24 on R1, enter the following command:

```
R1(config)interface loopback 0
R1(config-if)ip address 172.16.1.1 255.255.255.0
```

Note: when these commands are executed, a new interface will be shown in the "show ip interface brief". The loopback interface is always up and operates as a physical interface.

After configuring ospf and saving, the router-ID in use will still be the highest active physical interface that we used, and the router-ID configured using the ***router-id***command will still not be active as shown in the output below.

```
R2(config-router)#router-id 20.20.20.20
Reload or use "clear ip ospf process" command, for this to take effect
```

We need to make the router-ID active by restarting the OSPF process on all the routers: to do this, we have to enter the command "**clear ip ospf process**" in the privileged exec mode as shown below.

Executing this command will prompt us to confirm this command and we should answer with "**YES**"

```
R2#clear ip ospf process
Reset ALL OSPF processes? [no]: yes
```

After executing this command on all the routers, the new router-ids will be in effect.

Verifying OSPF operation

After configuring OSPF we need to verify that everything is working fine on all the routers. To verify OSPF we will use these commands:

1. Show ip ospf neighbor
2. Show ip ospf database
3. Show ip route
4. Show ip ospf interface
5. Show ip protocols
6. Show ip ospf
7. Debug ip ospf adj
8. Debug ip ospf hello