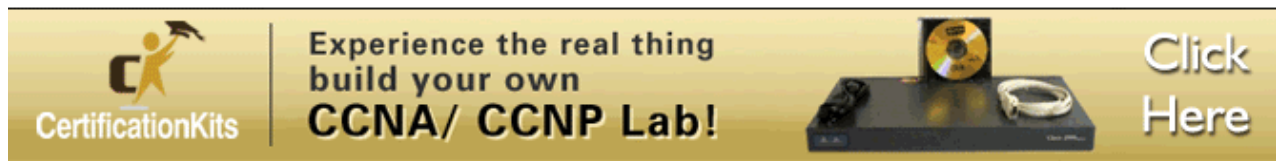


EIGRP part 1

 ccnablog.com/eigrp-part-1



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 (Diffusion 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

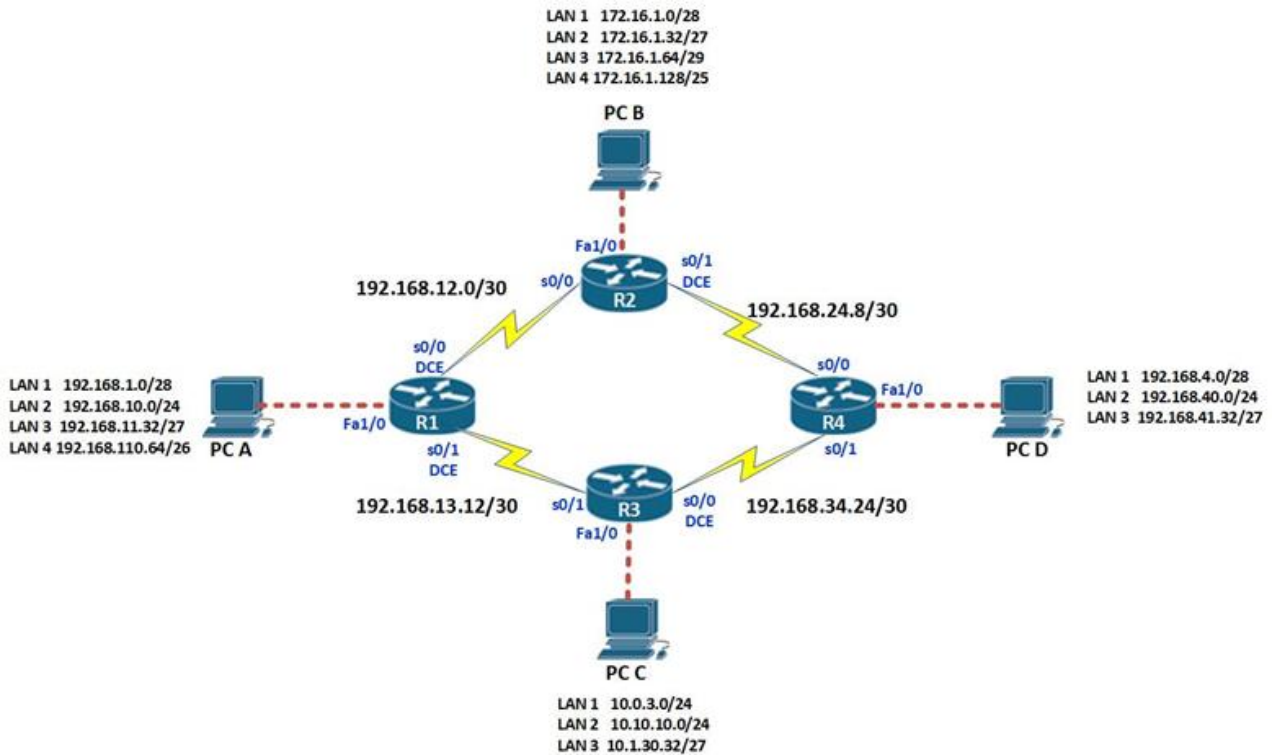
The routing table shows the best route as calculated by DUAL and is used to forward packets in EIGRP.

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 step will be the initial configuration on all the routers. We will not repeat these steps but you as a student and for practice you are expected to configure the following parameters on all the routers:

- Host name
- Enable a plain password "cisco"
- Disable ip domain lookup
- Configure the line console with the password "cisco" and require login to access console
- change the executive timeout to 45 minutes in the line console
- Configure synchronous logging in the console line
- Configure 4 telnet lines with the password "cisco" and require login to access console
- change the executive timeout to 25 minutes in the vty
- Configure synchronous logging in the vty
- Configure all the ip addresses and clock rates according to the scheme shown above and enable all interfaces
- Save the configuration to the NVRAM.

After these configurations we can now start configuration for EIGRP.

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>

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.

In our scenario, the commands needed to configure EIGRP on all the routers successfully are shown in the table below. You should enter these commands carefully so as to avoid misconfiguration.

Router name	Configuration commands
R1	R1(config)#router eigrp 100 R1(config-router)#network 192.168.12.0 R1(config-router)#network 192.168.13.12 R1(config-router)#network 192.168.1.0 R1(config-router)#network 192.168.10.0 R1(config-router)#network 192.168.11.33 R1(config-router)#network 192.168.110.64 R1(config-router)#no auto-summary
R2	R2(config)#router eigrp 100 R2(config-router)#no auto-summary R2(config-router)#net 192.168.12.0 R2(config-router)#net 192.168.24.8 R2(config-router)#net 172.16.1.0 R2(config-router)#net 172.16.1.32 R2(config-router)#net 172.16.1.64 R2(config-router)#net 172.16.1.128
R3	R3(config)#router eigrp 100 R3(config-router)#no auto-summary R3(config-router)#network 192.168.34.24 R3(config-router)#network 192.168.13.12 R3(config-router)#network 10.0.3.0 R3(config-router)#network 10.10.10.0 R3(config-router)#network 10.1.30.32
R4	R4(config)#router eigrp 100 R4(config-router)#net 192.168.34.24 R4(config-router)#net 192.168.24.8 R4(config-router)#network 192.168.4.0 R4(config-router)#network 192.168.40.0 R4(config-router)#network 192.168.41.32

After this configuration, you should be able to see the following output on each of the routers. The figure below shows the output on router R1.

```
*Mar 1 01:17:32.879: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.12.2 (Serial0/0) is up: new adjacency
```

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.

The diagrams below show the output of each of the above commands on router R1.

Show ip eigrp interfaces:

```
R1#show ip eigrp interfaces
IP-EIGRP interfaces for process 100

      Xmit Queue Mean Pacing Time Multicast Pending
Interface Peers Un/Reliable SRTT Un/Reliable Flow Timer Routes
Se0/0      1      0/0      0      0/15      50      0
Se0/1      1      0/0     22      0/15     103      0
Fa1/0      0      0/0      0      0/1       0       0
Lo0        0      0/0      0      0/1       0       0
Lo1        0      0/0      0      0/1       0       0
Lo2        0      0/0      0      0/1       0       0
R1#
```

As you can see from the output above, highlighted in RED the process ID is shown as 100 and all the interfaces participating in EIGRP are also shown.

This command will be useful in verifying passive interfaces.

Show ip route

The table below shows the output of the show ip route on R1.

```

R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.12.0/30 is directly connected, Serial0/0
D    192.168.12.0/24 [90/3705856] via 192.168.13.14, 00:18:42, Serial0/1
     192.168.13.0/30 is subnetted, 1 subnets
C    192.168.13.12 is directly connected, Serial0/1
     192.168.110.0/26 is subnetted, 1 subnets
C    192.168.110.64 is directly connected, Loopback2
     192.168.24.0/30 is subnetted, 1 subnets
D    192.168.24.8 [90/3193856] via 192.168.13.14, 00:18:42, Serial0/1
C    192.168.10.0/24 is directly connected, Loopback0
D    192.168.40.0/24 [90/2809856] via 192.168.13.14, 00:18:43, Serial0/1
     172.16.0.0/16 is variably subnetted, 4 subnets, 4 masks
D    172.16.1.128/25 [90/3321856] via 192.168.13.14, 00:18:43, Serial0/1
D    172.16.1.32/27 [90/3321856] via 192.168.13.14, 00:18:44, Serial0/1
D    172.16.1.0/28 [90/3196416] via 192.168.13.14, 00:18:44, Serial0/1
D    172.16.1.64/29 [90/3321856] via 192.168.13.14, 00:18:45, Serial0/1
     192.168.11.0/27 is subnetted, 1 subnets
C    192.168.11.32 is directly connected, Loopback1
     192.168.41.0/27 is subnetted, 1 subnets
D    192.168.41.32 [90/2809856] via 192.168.13.14, 00:18:45, Serial0/1
     192.168.4.0/28 is subnetted, 1 subnets
D    192.168.4.0 [90/2684416] via 192.168.13.14, 00:18:46, Serial0/1
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D    10.0.3.0/24 [90/2172416] via 192.168.13.14, 00:18:46, Serial0/1
D    10.10.10.0/24 [90/2297856] via 192.168.13.14, 00:18:46, Serial0/1
D    10.1.30.32/27 [90/2297856] via 192.168.13.14, 00:18:46, Serial0/1
     192.168.34.0/30 is subnetted, 1 subnets
D    192.168.34.24 [90/2681856] via 192.168.13.14, 00:18:47, Serial0/1
     192.168.1.0/28 is subnetted, 1 subnets
C    192.168.1.0 is directly connected, FastEthernet1/0

```

As you can see from the output above, R1 has all the routes to all networks in the network diagram.

The line highlighted in RED shows the routing protocol indicator as “D” which means EIGRP. 192.168.24.8 is the network that has been learnt and it has an EIGRP administrative distance of 90 and a metric of 3193856, this router learnt of this route from 192.168.13.14, which is R3 and this information was learnt via interface s0/1 which is the connection to R3.

Show ip eigrp topology

This command will show all the routes that this router has learnt via EIGRP. This includes the main routes as well as the backup routes.

```
R1#show ip eigrp topology
IP- EIGRP Topology Table for AS(100)/ID(192.168.110.65)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.0.3.0/24, 1 successors, FD is 2172416
   via 192.168.13.14 (2172416/28160), Serial0/1
P 10.10.10.0/24, 1 successors, FD is 2297856
   via 192.168.13.14 (2297856/128256), Serial0/1
P 10.1.30.32/27, 1 successors, FD is 2297856
   via 192.168.13.14 (2297856/128256), Serial0/1
P 172.16.1.128/25, 1 successors, FD is 3321856
   via 192.168.13.14 (3321856/2809856), Serial0/1
P 192.168.40.0/24, 1 successors, FD is 2809856
   via 192.168.13.14 (2809856/2297856), Serial0/1
P 192.168.11.32/27, 1 successors, FD is 128256
   via Connected, Loopback1
P 192.168.110.64/26, 1 successors, FD is 128256
   via Connected, Loopback2
P 192.168.34.24/30, 1 successors, FD is 2681856
   via 192.168.13.14 (2681856/2169856), Serial0/1
P 192.168.41.32/27, 1 successors, FD is 2809856
   via 192.168.13.14 (2809856/2297856), Serial0/1
P 192.168.10.0/24, 1 successors, FD is 128256
   via Connected, Loopback0
P 192.168.12.0/24, 1 successors, FD is 3705856
   via 192.168.13.14 (3705856/3193856), Serial0/1
P 192.168.12.0/30, 1 successors, FD is 2169856
   via Connected, Serial0/0
P 192.168.1.0/28, 1 successors, FD is 28160
   via Connected, FastEthernet1/0
P 192.168.13.12/30, 1 successors, FD is 2169856
   via Connected, Serial0/1
P 192.168.4.0/28, 1 successors, FD is 2684416
   via 192.168.13.14 (2684416/2172416), Serial0/1
P 192.168.24.8/30, 1 successors, FD is 3193856
   via 192.168.13.14 (3193856/2681856), Serial0/1
P 172.16.1.32/27, 1 successors, FD is 3321856
   via 192.168.13.14 (3321856/2809856), Serial0/1
P 172.16.1.0/28, 1 successors, FD is 3196416
   via 192.168.13.14 (3196416/2684416), Serial0/1
P 172.16.1.64/29, 1 successors, FD is 3321856
   via 192.168.13.14 (3321856/2809856), Serial0/1
```

These are all the routes R1 knows about. The line highlighted in RED shows that this router has a route to 172.16.1.64/29, which was learnt via 192.168.13.14.

The successor and the FD will be discussed in the next part.

Show ip eigrp neighbors

This command will show the directly connected routers that are participating in EIGRP.

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H Address          Interface      Hold Uptime  SRTT  RTO  Q  Seq
  (sec)          (ms)  Cnt Num
0 192.168.12.2     Se0/0         14 00:01:04  1 5000 2 75
1 192.168.13.14   Se0/1         10 00:27:51  22 200 0 34
```

As shown in the output above, R1 has 2 neighbors which it learnt of via interface se0/0 and se0/1. This command will be useful in discovery of routers that are not participating in EIGRP.

After this configuration, all the host PCs should be able to ping.

This marks the end of the EIGRP basic configuration, YES, it is as easy as that.

Summary

In this chapter, we have learnt about EIGRP, we have looked at the various key terminology used in EIGRP as well as some concepts. We have also done basic configuration of EIGRP. In the next part, we will continue looking at EIGRP, we will explore more concepts and do more EIGRP configurations.