International Journal of Innovation in Computer Science and Information Technology
Vol.5, NO.1 , P:1-19
Received: 21 October 2024
Accepted: 15 February 2025

# Investigating the basics and features of the EIGRP protocol along with the analysis of the operation, configuration and verification of this protocol in computer networks

**Mohammad Abasi Rad**
Bachelor's student, Computer Engineering,
Farabi College, University of Tehran, Iran
Mohamadabasirad4@gmail.com

**Abstract**

EIGRP or Enhanced gateway protocol is an efficient and advanced routing protocol offered by Cisco. Today, this protocol Is widely used In computer networks with high scal" because of its easy configuration, special features and high performance that are available to network engineers. This article studies the functionality, configuration and unique features of this protocol. At the beginning of the article, the features of this pr'tocol and comparison of these features with the characteristics of other routing protocols are presented. Moreover, the terms of the Dual algorithm, types of tables, types of packets and the method of metr'c calculation in this protocol are discussed. Then, the configuration of this protocol and Its features are discussed. At the end, Verification Is investigated in order to troubleshooting along with how to create authentication mechanism In this protocol. This article can be a useful guide to better understand and gain the optimal use of EIGRP protocol for network and students of this field.

Keywords: EIGRP, Routing Protocols, Configuration, Cisco, Computer Networks

## Introduction

For small networks, using static routing can be sufficient. However, when a network is large or continuously expanding, configuring static routes for packet routing is not recommended. For example, if a new network is added to a large network with many routers, each router within the network would need to be updated to add the route for the newly connected network. Repeating this process can lead to significant time and energy waste. In such situations, routing protocols should be used to automate this process. With routing protocols, routes are dynamically determined based on the information that routers share with each other, eliminating the need for manual route entry as with static routes. Essentially, routing protocols define how routers interact, how data is transferred between them, and how the best path is chosen. Routing protocols are generally divided into two categories: IGP (Interior Gateway Protocol) and EGP (Exterior Gateway Protocol). If a routing protocol operates within a single Autonomous System, it is considered an IGP; however, if it connects multiple Autonomous Systems and routes between them, it is classified as an EGP. An Autonomous System refers to a group of routers managed under a single authority.

## IGP Categories

IGP (Interior Gateway Protocol) is further divided into three categories: Distance Vector, Link State, and Hybrid. IGRP and RIP

International Journal of Innovation in Computer Science and Information Technology
Vol.5, NO.1 , P:1-19
Received: 21 October 2024
Accepted: 15 February 2025

are examples of Distance Vector protocols, while OSPF and IS-IS are examples of Link State protocols. EIGRP, on the other hand, is an example of a Hybrid protocol. Today, IS-IS and IGRP protocols are obsolete, and the most commonly used protocols are OSPF and EIGRP. In the EGP (Exterior Gateway Protocol) category, BGP is a notable example.

Distance Vector protocols select routes with the fewest hops for packet transmission, while Link State protocols choose routes with better bandwidth and lower delay. In Distance Vector protocols, each router's database contains information provided by its neighbors, making them less resource-intensive. However, they are prone to routing loops. In Link State protocols, each router maintains a database of the entire network topology, making these protocols resource-intensive. However, due to their awareness of the whole network, they are not prone to routing loops. Di'tance Vector protocols operate In a classful manner and are generally slower, while Link St'te protocols are faster and can also operate In a classless manner.

EIGRP is an optimized version of the IGP protocol. This Advanced Distance Vector or Hybrid protocol combines positive attributes of both Distance Vector and Link State protocols. EIGRP was introduced by Cisco in 1993, replacing IGRP, which had been introduced in the mid-1980s. Until 2013, EIGRP was proprietary to Cisco, but It was later standardized and is now available on some other devices as well.

**EIGRP Features**

EIGRP is an advanced Distance Vector protocol. Traditional Distance Vector protocols had certain disadvantages. For instance, in these protocols, routers would send their routing table to neighbors every 30 seconds without any reason, even if no changes had occurred in the network. This behavior was unnecessary and resulted in additional traffic. Another issue was the use of hop count in metric calculations. For example, the RIP protocol would send data through the path with the fewest hops to the destination, which is not always an optimal routing metric.

EIGRP has the shortest convergence time among all routing protocols, which, according to Cisco, is about 200 milliseconds. Convergence time refers to the time It takes for all routers In the network to recognize a change, such as the addition of a new network or the disconnection of an existing one. Compared to protocols like RIP, where convergence time in large networks could take up to 3 minutes, this 200 milliseconds is remarkably fast.

EIGRP supports VLSM (Variable Length Subnet Mask), allowing each network to be advertised with a subnet mask defined by the network administrator. For instance, 10.0.0.0 with a subnet mask of 255.0.0.0 is considered a Class A IP address. If the routing protocol In use does not support VLSM, the network would still be advertised with the 255.0.0.0 subnet mask. However, if the routing protocol supports VLSM, it allows for classless addressing. For example, networks such as 10.1.1.0 and 10.1.2.0 can be advertised with

International Journal of Innovation in Computer Science and Information Technology
Vol.5, NO.1 , P:1-19
Received: 21 October 2024
Accepted: 15 February 2025

a subnet mask of 255.255.255.0 within the network.

Another feature of EIGRP is Partial Update**.** For example, the RIP protocol sends its entire routing table to its neighbors every 30 seconds. However, EIGRP only sends updates when a network is attached or goes down, and it sends only the changes in the routing table instead of the entire routing table. EIGRP supports layer 3 OSI protocols such as IP, IPX, and AppleTalk. EIGRP has a flexible network design. For example, in OSPF, adding a new router requires careful planning based on areas and the design established beforehand. But with EIGRP's flexibility, adding a new network or router can be done at any time.

EIGRP uses Multicast Address 224.0.0.10 instead of Broadcast Address to send update packets. It also supports summarization throughout the network, unlike OSPF, which only supports summarization at routers that are ABR or ASBR. This mechanism can be implemented automatically or manually using specific commands in the protocol.

Due to the features built into EIGRP, it maintains loop-free operation. It also has a simple configuration for both LANs and WANs. EIGRP also supports authentication.

EIGRP can perform Load Balancing over paths with equal or unequal costs.

For example, Figure 1 provides a clearer understanding of Load Balancing. In Figure 1, the metric that Router 1 uses to reach Network Y through Router 2 is 5000. A metric is a value that the source router calculates to forward packets to the destination router. There is also a backup path through Router 4 to reach Network Y. The metric calculated by Router 1 for Network Y through Router 4 is 6000. Under this condition, Router 1 will choose the path with the lower metric to send packets, so all traffic to Network Y will be sent through Router 2. However, if EIGRP is configured in this network, traffic can be load-balanced across both paths to Network Y. In fact, backup paths with higher metrics can also be used for forwarding traffic. This is made possible by the "Variance" command, a feature not available in other routing protocols. For example, in OSPF, the costs within a path must be equal to perform load balancing.

International Journal of Innovation in Computer Science and Information Technology
Vol.5, NO.1 , P:1-19
Received: 21 October 2024
Accepted: 15 February 2025

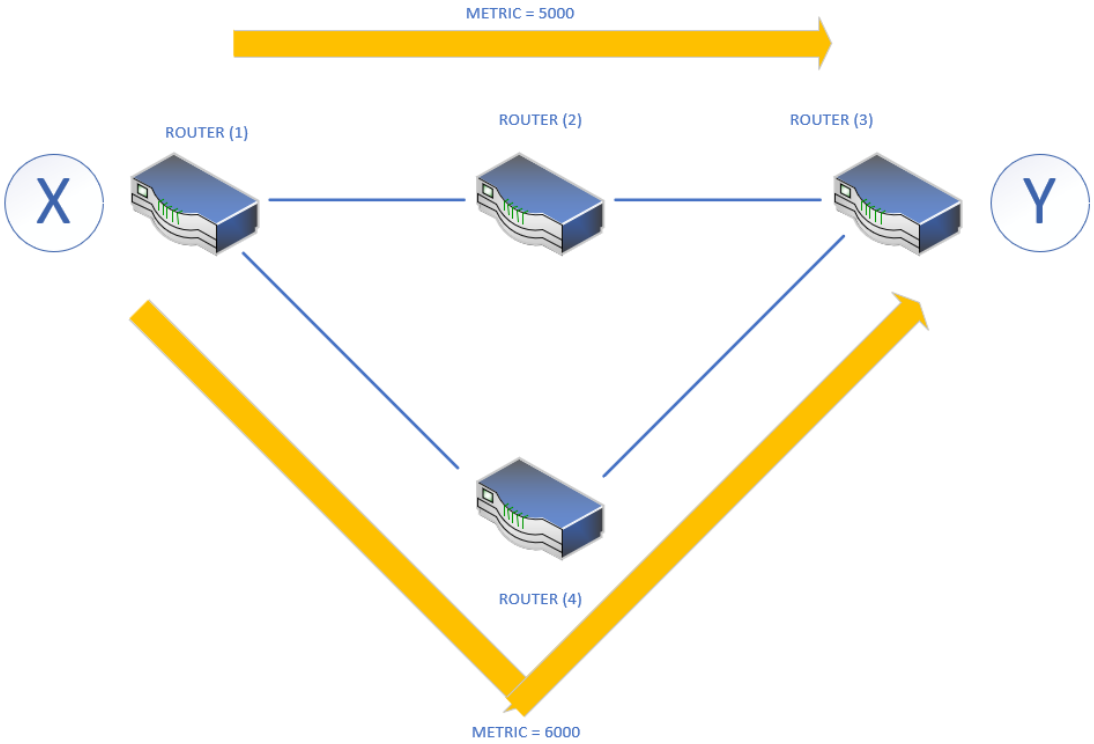


**Figure 1 – An example to explain Load-Balancing**

**Dual Terminology**

EIGRP uses the **DUAL (Diffusing Update Algorithm)**, which includes several terms crucial to understanding its operation. Some of these terms include **AD** (Advertised Distance), **FD** (Feasible Distance), **Current Successor**, and **Feasible Successor**. These terms are important in determining how EIGRP calculates and selects paths.

For example, in **Figure 2**, Router 1 calculates a **Metric** of 5000 to reach Network Y via Routers 2 and 3, and another **Metric** of 6000 via Router 5. In this case, the primary path to Network Y is through Routers 2 and 3 because it has the lower metric, while the backup path is through Router 5 with a metric of 6000.

- **AD (Advertised Distance)** or **Reported Distance** is the metric calculated by the neighbor router (Router 2) to the destination. According to this example, Router 2 has calculated an AD of 4000 to Network Y. AD represents the metric from the neighbor to the destination.
- **FD (Feasible Distance)** is the metric (5000 in this example) that Router 1 calculates to reach Network Y. This represents the total cost of the path from Router 1 to the destination and is essentially the **lowest cost**.
- **Current Successor** (or simply Successor) is the next-hop router on the path with the lowest cost, which in this case is Router 2.
- **Feasible Successor** is the next-hop router in the backup path. In this example, Router 5 is the **Feasible Successor**.

International Journal of Innovation in Computer Science and Information Technology
Vol.5, NO.1 , P:1-19
Received: 21 October 2024
Accepted: 15 February 2025

A critical point to note is that the **Advertised Distance** from the **Feasible Successor** must be lower than the **Feasible Distance** (FD) calculated by the **Current Successor** in order for it to be chosen as the backup path. If the AD of the Feasible Successor is greater than the FD of the Current Successor, it cannot be used as a backup.

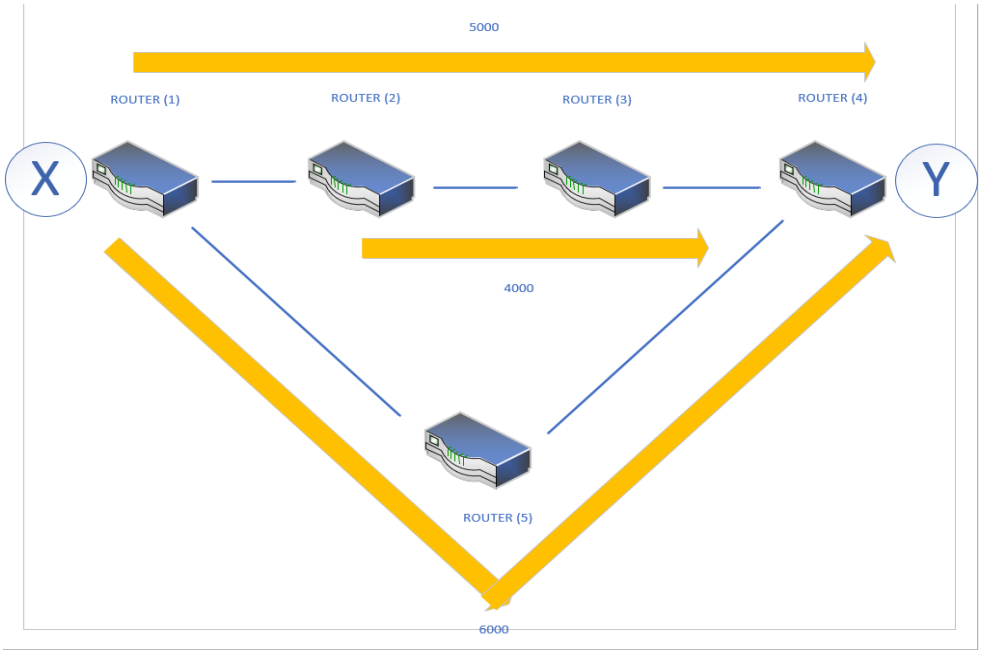


**Figure 2 – An example to explain the terms of the Dual algorithm**

The reason routing protocols store backup paths is to ensure high **convergence time**. For example, suppose the path between Router 1 and Router 2 is broken. In this case, Router 1 no longer has a path to reach Network Y, so it must quickly replace the path with a backup route, which in this case involves Router 5.

**EIGRP Tables**

EIGRP uses three tables:

1. **Neighbor Table**: This table stores information about all neighbors. It contains the IP address of the neighbor router and the port number through which the router is connected to that neighbor.
2. **Topology Table**: This table contains the primary and secondary paths to a destination. It includes **Advertised Distance (AD)**, **Feasible Distance (FD)**, and the IP address of the neighbor router. There may be multiple paths to the same destination in this table.
3. **Routing Table**: This table is derived from the **Topology Table** and contains the best routes with the lowest metric. It also stores data like the metric and the port number connected to the neighboring router. For example, Router C reaches Network 10.1.1.0 with a subnet mask of 255.255.255.0 through Routers A and B.

International Journal of Innovation in Computer Science and Information Technology
Vol.5, NO.1 , P:1-19
Received: 21 October 2024
Accepted: 15 February 2025

Tables 1, 2, and 3 provide examples of these EIGRP tables based on the previous example.

**Table 1 – An example of the Neighbor Table in EIGRP**

| NEXT-HOP ROUTER | INTERFACE |
|---|---|
| ROUTER A IP | **ETHERNET 0** |
| ROUTER B IP | **ETHERNET 1** |

**Table 2 – An Example of the Topology Table in EIGRP**

| NETWORK | FEASIBLE DISTANCE (METRIC) | ADVERTISED DISTANCE | EIGRP NEIGHBOR |
|---|---|---|---|
| ١٠.١.١.٠/٢٤ | ٢٠٠٠ | ١٠٠٠ | **ROUTER A IP** |
| ١٠.١.١.٠/٢٤ | ٢٥٠٠ | ١٥٠٠ | **ROUTER B IP** |

**Table 3 - An Example of the Routing Table in EIGRP**

| NETWORK | FEASIBLE DISTANCE (METRIC) | OUTBOUND INTERFACE | NEXT-HOP (EIGRP NEIGHBOR) |
|---|---|---|---|
| ١٠.١.١.٠/٢٤ | ٢٠٠٠ | ETHERNET 0 | **ROUTER A IP** |

**EIGRP Neighborship**

To establish communication and exchange routing tables between routers, the establishment of a neighbor relationship must first occur. For two routers to become neighbors, they must have the same AS number, identical K-Value values, identical authentication settings, and synchronized clock and date. Additionally, both routers must advertise the same network.

**EIGRP Packets**

EIGRP has 5 types of packets: Hello**,** Update**,** Query**,** Reply**,** and Acknowledge**.** For example, if EIGRP is configured on Router 1 and the desired networks are advertised using a command, Router 1 will send a Hello packet on the port connected to its neighbor. The Hello packet is used for neighbor discovery and to announce activity. Router 2, which is connected to Router 1, will then respond with an Acknowledgment of the Hello packet. After the neighbor relationship is established, Router 2 will send Update packets regarding its networks. In these Update packets, information from their respective Topology Tables is exchanged. Once received, Router 1 will send an Acknowledge packet, confirming the receipt of the information. Router 1 will then send its own Update packets, and Router 2 will send an Acknowledge packet upon receiving the

International Journal of Innovation in Computer Science and Information Technology
Vol.5, NO.1 , P:1-19
Received: 21 October 2024
Accepted: 15 February 2025

Update packets, confirming receipt. In this way, routers that have formed a neighbor relationship exchange information from their Topology Tables and then each router builds its own Routing Table from the Topology Table.

Once the neighbor relationship is established, any changes in the routing tables are communicated to neighbors. Additionally, Hello packets are sent periodically to ensure that routers are still active. If a router does not receive a Hello packet from its neighbor within a specific period, the router considers it Down and removes any routes learned from that neighbor from its routing table. The typical Hello packet interval is every 5 seconds, and if a router does not receive a Hello packet from the other router within 15 seconds, it considers the router Down. The Query packet is used to request a specific route. When a router sends a Query about a network, a Reply packet is sent back in response.

**EIGRP Metric**

The EIGRP metric consists of five components: Bandwidth, Delay, Reliability, Loading, and MTU. The two primary parameters in calculating the metric are Bandwidth and Delay, while the other three parameters are by default assigned a coefficient of zero in the formula. However, these values can be adjusted if needed to change how the metric is calculated. When only the two primary parameters are considered, the calculated metric is equal to the sum of Delay and Bandwidth.

- **Delay** is calculated by multiplying the sum of the delays along the path by 256.
- **Bandwidth** is calculated by dividing 10,000,000 by the smallest bandwidth on the path (in kilobits per second), and then multiplying the result by 256.

In EIGRP, the Delay and Bandwidth values can be modified using a command, which will affect the Routing Table. EIGRP uses 5 K-values. By default, K1 and K3 are set to 1, while K2, K4, and K5 are set to 0. These K-values represent the coefficients for the metric components. The main formula for calculating the metric in EIGRP is shown in Figure 3.

$$\text{Metric} = 256 * \left[ \left( K_1 * \frac{10^7}{\text{Min. Bandwidth}} + \frac{\frac{K_2 * \text{Min. Bandwidth}}{10^7}}{256 - \text{Load}} + \frac{K_3 * \text{Total Delay}}{10} \right) * \frac{K_5}{K_4 + \text{Reliability}} \right]$$

**Figure 3 – The Main Formula for Calculating Metric In EIGRP**

According to the above formula, K1 and K3 are the coefficients for the Bandwidth and Delay components, which both have a value of 1. This is why these two parameters are essential for calculating the Metric, as they have non-zero coefficients in the formula. The values of these coefficients can be changed using a command, but it is not recommended to do so, as it will completely alter how the Metric is calculated for this protocol. If these K-values need to be changed, they must be updated on all routers in the network because, in order to form a neighbor relationship between two routers, these values must be identical on both routers. Figure 4 provides an example to explain the Bandwidth and Delay parameters.

International Journal of Innovation in Computer Science and Information Technology
Vol.5, NO.1 , P:1-19
Received: 21 October 2024
Accepted: 15 February 2025

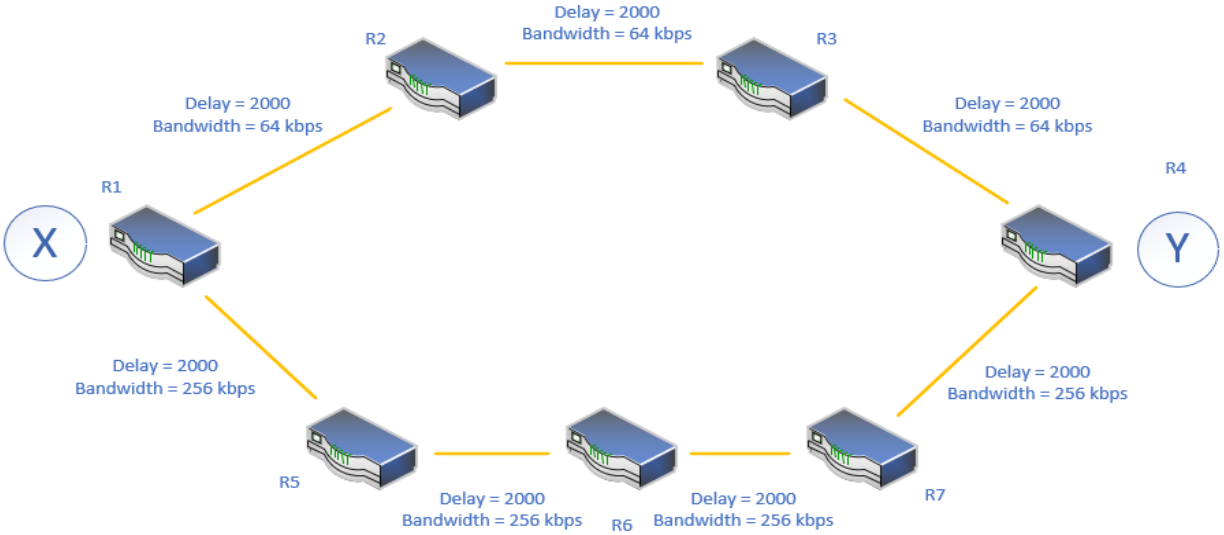


**Figure 4 – An Example to Explain the Bandwidth and Delay Parameters**

According to Figure 4, Router 1 has two paths for sending packets to the destination Network Y. In the path involving Routers 3 and 4, the lowest bandwidth is 64 kbps, and the total delays are 6000. In the other path, the lowest bandwidth is 256 kbps, and the total delays are 8000. According to the formula, the Metric for the upper path is 43,153,600, and the Metric for the lower path is 12,048,000. Because the Metric for the lower path is smaller, it is selected as the primary path for sending packets.

## Findings

### EIGRP Configuration

To activate this protocol, the command router eigrp autonomous-system-number must be entered in Global Configuration mode. The parameter autonomous-system-number is a number that should be the same on routers that need to form a neighbor relationship with each other. Then, in Specific Configuration mode, the command network network-number [wildcard-mask] must be entered. The network-number parameter refers to the networks that are directly connected to this router. Networks that are advertised must belong to the same AS (Autonomous System). It is not necessary to advertise all networks directly connected to the router; only the interfaces that should participate in the EIGRP process need to be advertised. With this command, the networks are advertised within the network and learned by neighboring routers. It also activates the Hello Packet on the interfaces that have their networks advertised, in order to establish a neighbor relationship. The wildcard-mask is an optional parameter that can be omitted. This parameter is the inverse of the Subnet Mask. To calculate this parameter from the Subnet Mask, subtract each octet of the Subnet Mask from 255. For example, if the Subnet Mask is 255.255.0.0, the Wildcard Mask would be 0.0.255.255.

International Journal of Innovation in Computer Science and Information Technology
Vol.5, NO.1 , P:1-19
Received: 21 October 2024
Accepted: 15 February 2025

Sometimes, networks connected to a router might belong to the same IP class. For example, if a router is connected to the networks 10.20.0.0, 10.30.0.0, 10.40.0.0, 172.16.10.0, and 172.16.20.0, there are two ways to configure this. In the first method, the network network-number [wildcard-mask] command can be entered for each of the networks. In this method, each network can be advertised with a wildcard mask specified by the network administrator. For example, the network 172.16.20.0 can be advertised with a wildcard mask of 0.0.0.255. In the second method, for simplicity and easier troubleshooting, the configuration can be done with just two commands: network 10.0.0.0 and network 172.16.0.0. However, if the second method is used, auto-summary must be disabled. If not disabled, IPs from each class will be advertised with the default subnet mask of that class. For example, the network 10.10.20.0/32 will be advertised with the default subnet mask of Class A, which is 255.0.0.0. Therefore, to avoid incorrect routing, this mechanism should be disabled. Essentially, by using this command, VLSM (Variable Length Subnet Mask) is activated, and each network is advertised with the subnet mask specified by the network administrator. The command to disable this mechanism is no auto-summary. In Cisco devices with software versions 15 and later, when EIGRP is configured, this command is automatically executed.

**EIGRP Bandwidth & Delay**

If there is a need to change the Bandwidth and Delay of links in order to modify how the EIGRP Metric is calculated, you must first enter the desired port in Global Configuration mode using the command interface gigabitEthernet number, and then, in Specific Configuration mode, use the commands bandwidth number and delay number to change the bandwidth and delay of the link. The bandwidth value should be entered in kilobits, and the delay value should be entered in tens of microseconds.

These changes can have a significant impact. For example, if two routers are using two paths with the same metric for Load-Balancing, and one of the links fails, causing some packets to not reach the destination, you can adjust the delay or bandwidth of the faulty link to reroute all traffic to the other link until the failed link is restored. By increasing the delay or reducing the bandwidth of the failing link, the metric of that link will increase, and it will be removed from the routing table, but it will remain in the Topology Table as a backup path. This backup path can then be used if the primary route goes down.

An example of executing the delay and bandwidth commands is shown in Figure 5.

```
R3(config)#interface fast 0/0
R3(config-if)#bandwidth 1000
R3(config-if)#delay 3000
```

**Figure 5 – Example of commands to change Bandwidth and Delay**

International Journal of Innovation in Computer Science and Information Technology
Vol.5, NO.1 , P:1-19
Received: 21 October 2024
Accepted: 15 February 2025

**EIGRP Load-Balancing**

EIGRP can implement the Load-Balancing mechanism in two ways. In the first method, the metrics towards the destination are the same, and by default, this protocol can perform Load-Balancing across up to 32 paths In newer IOS versions. By default, It performs Load-Balancing across 4 paths, and the number of links can be changed using the command `maximum-paths number`. The other method occurs when there are multiple paths with unequal metrics. In this case, Unequal Load-Balancing is performed. Load-Balancing in the second method is done using the `variance multiplier` command in a Specific Configuration environment. With this command, a Feasible Successor can be converted into a Successor. The `Variance` command works as follows: If the calculated metric for a Network in the Primary Route is 1000 and the calculated metric for the Backup path is 1500, If the Variance value Is set to 2, the Backup path will also be chosen for Packet forwarding because 1500 is less than twice 1000. Essentially, the Variance value is multiplied by the metric of the primary route, and Unequal Load-Balancing is performed on paths whose metrics are smaller than this calculated value. An example of executing this command is provided In Figure 6.

```
R4(config)#router eigrp 1
R4(config-router)#variance 2
R4(config-router)#maximum-paths 8
```

**Figure 6 – An example of executing the “variance” and “maximum-paths” commands**

**EIGRP Summarization**

If Auto Summarization is not disabled, networks are advertised with their class default Subnet Mask and in a classful manner. For example, the network 172.16.10.0/24 would be advertised with a Subnet Mask of 255.255.0.0 because 172 belongs to the Class B IP range. This could lead to incorrect routing. To prevent this, Auto Summarization should be disabled using the command no auto-summary.

## EIGRP Passive-Interface

An important point is that neighbor relationships are formed only between routers. A router's interface might be connected to a switch, which in turn is connected to several PCs. In this case, the network associated with that interface is advertised, but no neighbor relationship is formed because this interface is not connected to another router. Using a command, this behavior can be prevented, so that the Hello Packet is only sent on interfaces that are connected to routers and need to form a neighbor relationship. When this command is used, only the network related to the interface is advertised, and no Hello Packet is sent on that interface. The command used for this purpose is passive-interface fast port-number, which should be executed in Specific Configuration mode. Figure 7 provides an example of how this command is used.

International Journal of Innovation in Computer Science and Information Technology
Vol.5, NO.1 , P:1-19
Received: 21 October 2024
Accepted: 15 February 2025

```
R2(config)#router eigrp 1
R2(config-router)#passive-interface fast 0/0
```

**Figure 7 – An example of executing the "passive-interface" command**

If needed, the "metric weight" command can be used to change the K-Value coefficients. After this command, the values for the coefficients from K1 to K5 must be entered In order. These coefficients can only have values of 0 or 1. It is important to note that one of the conditions for establishing a neighbor relationship between routers is that the K-Values must be the same. Therefore, if the values of these coefficients are changed on one router, they must also be updated on the neighboring routers. Figure 8 provides an example of how to execute the command to change the coefficient values.

```
R2(config)#router eigrp 1
R2(config-router)#metric weight 1 0 1 1 0 0
```

**Figure 8 – Example of executing the K-Value coefficient adjustment command**

In Figure 9, an example of a network with six routers Is shown. To prevent IP wastage, a /30 subnet Is used between the routers, which includes only 4 IP addresses. One of these Is the network IP, and anotherr is the broadcast IP. The remaining two IP addresses are assigned to the two router interfaces on either side of the link. Additionally, each router has a Loopback Interface representing the LAN behind it, configured with a subnet mask of 255.255.255.255. All routers are within the same Autonomous System, identified by the number 1. To further clarify the previous explanations and commands, the EIGRP configuration commands for the routers In this network are provided below.

International Journal of Innovation in Computer Science and Information Technology
Vol.5, NO.1 , P:1-19
Received: 21 October 2024
Accepted: 15 February 2025

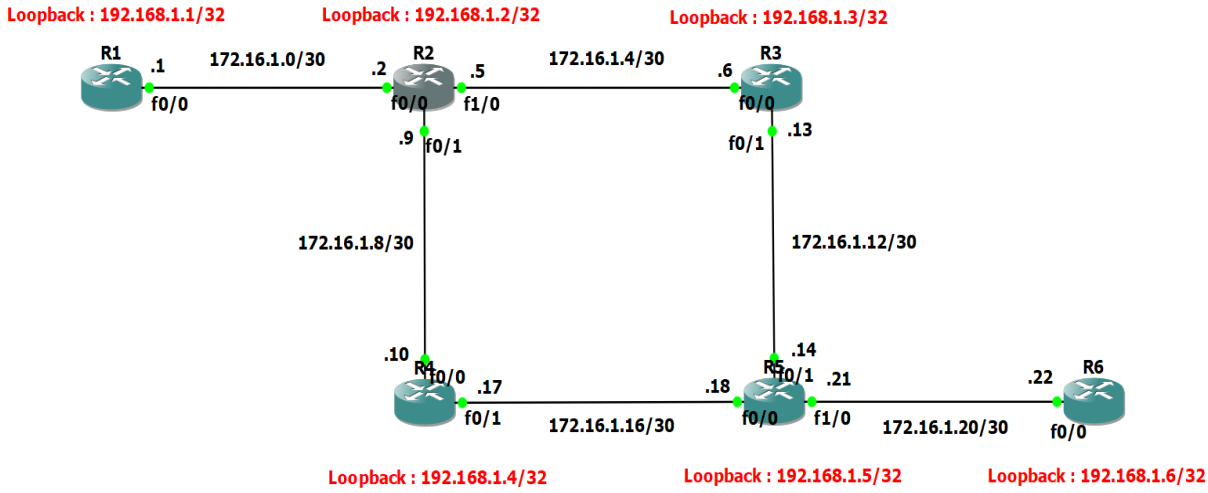


**Figure 9 – A sample network for configuring EIGRP**

The configuration commands for Router number 5 are provided as an example in Figure 10. This configuration includes assigning IP addresses to physical ports and the Loopback interface, along with configuring the EIGRP protocol.

```
R5#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R5(config)#int fast 0/0
R5(config-if)#no shutdown
R5(config-if)#ip address 172.16.1.18 255.255.255.252
R5(config-if)#exit
R5(config)#int fast 0/1
R5(config-if)#no shutdown
R5(config-if)#ip address 172.16.1.14 255.255.255.252
R5(config-if)#exit
R5(config)#int fast 1/0
R5(config-if)#no shutdown
R5(config-if)#ip address 172.16.1.21 255.255.255.252
R5(config-if)#exit
R5(config)#int loopback 1
R5(config-if)#ip address 192.168.1.5 255.255.255.255
R5(config-if)#exit
R5(config)#router eigrp 1
R5(config-router)#network 172.16.0.0
R5(config-router)#network 192.168.0.0
R5(config-router)#no auto-summary
R5(config-router)#exit
R5(config)#exit
R5#wr
```

**Figure 10 – An Example of Router Configuration Commands**

International Journal of Innovation in Computer Science and Information Technology
Vol.5, NO.1 , P:1-19
Received: 21 October 2024
Accepted: 15 February 2025

**EIGRP Verifying**

To verify and check the proper functioning of the protocol, various commands can be used. The first command is show ip eigrp neighbors**,** which is used to verify the Neighbor Table. These show commands should be executed in the Privileged EXEC mode. Depending on the network design, a router may have multiple AS numbers configured for EIGRP. This command displays information for all AS numbers configured on the router.

The output of this command includes parameters such as Address, Interface, Hold, Uptime, and Q Count, among others. In the Address field, the IP address of the Next-Hop Router with which this router has formed a neighbor relationship is shown. The Interface field displays the port number through which the router is connected to the next-hop router. The Hold parameter indicates the duration the router waits for a Hello Packet, and if it does not receive it within this period, it will tear down the neighbor relationship. The Uptime parameter shows how long the neighbor relationship has been active between the two routers. The Q Count field shows the number of packets that are queued for update between the two routers. If the Q Count value is high in a real network, it indicates a problem between the routers, such as a congested link or high CPU load on the routers, preventing them from processing packets efficiently.

An example of using the command to verify neighbors is shown in Figure 11.

```
R5#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q
Seq
                                                   (sec)         (ms)       Cnt
Num
2   172.16.1.17             Fa0/0                    11 00:00:38   40   240  0
5
1   172.16.1.13             Fa0/1                    11 00:00:38 1259  5000  0
5
0   172.16.1.22             Fa1/0                    11 00:00:38   32   192  0
4
```

**Figure 11 – An example of executing the command to verify neighbors**

The next command is show ip route eigrp**,** which is used to verify the Routing Table. If the command show ip route is executed by itself, the entire Router's Routing Table will be displayed, including routes for Directly Connected networks, OSPF routes, and so on. However, when the command is executed along with EIGRP, it limits the output to only show routes that have been learned through EIGRP.

The code for EIGRP routes in the Dual algorithm is the character D, and the code for Directly Connected routes is C. The output of this command will display the networks learned by the EIGRP protocol. The information includes the Administrative Distance for the protocol in the Internal state, which is 90, and also the calculated Metric for this router to reach the destination network.

International Journal of Innovation in Computer Science and Information Technology
Vol.5, NO.1 , P:1-19
Received: 21 October 2024
Accepted: 15 February 2025

The output is displayed in the form [AD, Metric].

In the next section, the IP address of the Next-Hop Router through which the route was learned is shown after the word "via". Following that, the time elapsed since this update reached the router and when it learned this route from the update will be displayed. Lastly, the port number through which the router reaches the destination network will be shown.

If there are many configuration lines in the router, making it difficult to find the desired destination, you can use the command show ip route ip-add**,** where you replace ip-add with the destination IP address. In the output of this command, you will see details such as the AS Number**,** Administrative Distance**,** Metric Type**,** Next-Hop Router's IP address, the port number through which the last update was received, the time elapsed since the update was received, and the metric calculation parameters such as Minimum Bandwidth and Total Delay**.**

Examples of executing the command to verify the Routing Table are shown in Figures 12, 13, and 14.

```
R5#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 9 subnets, 2 masks
D        172.16.1.0/30 [90/33280] via 172.16.1.17, 00:00:41, FastEthernet0/0
                       [90/33280] via 172.16.1.13, 00:00:41, FastEthernet0/1
D        172.16.1.4/30 [90/30720] via 172.16.1.13, 00:00:41, FastEthernet0/1
D        172.16.1.8/30 [90/30720] via 172.16.1.17, 00:00:46, FastEthernet0/0
C        172.16.1.12/30 is directly connected, FastEthernet0/1
L        172.16.1.14/32 is directly connected, FastEthernet0/1
C        172.16.1.16/30 is directly connected, FastEthernet0/0
L        172.16.1.18/32 is directly connected, FastEthernet0/0
C        172.16.1.20/30 is directly connected, FastEthernet1/0
L        172.16.1.21/32 is directly connected, FastEthernet1/0
      192.168.1.0/32 is subnetted, 3 subnets
D        192.168.1.1 [90/161280] via 172.16.1.17, 00:00:41, FastEthernet0/0
                     [90/161280] via 172.16.1.13, 00:00:41, FastEthernet0/1
D        192.168.1.2 [90/158720] via 172.16.1.17, 00:00:41, FastEthernet0/0
                     [90/158720] via 172.16.1.13, 00:00:41, FastEthernet0/1
C        192.168.1.5 is directly connected, Loopback1
```

**Figure 12 – An example of executing the command "show ip route"**

International Journal of Innovation in Computer Science and Information Technology
Vol.5, NO.1 , P:1-19
Received: 21 October 2024
Accepted: 15 February 2025

```
R5#show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 9 subnets, 2 masks
D        172.16.1.0/30 [90/33280] via 172.16.1.17, 00:00:55, FastEthernet0/0
                       [90/33280] via 172.16.1.13, 00:00:55, FastEthernet0/1
D        172.16.1.4/30 [90/30720] via 172.16.1.13, 00:00:55, FastEthernet0/1
D        172.16.1.8/30 [90/30720] via 172.16.1.17, 00:01:00, FastEthernet0/0
      192.168.1.0/32 is subnetted, 3 subnets
D        192.168.1.1 [90/161280] via 172.16.1.17, 00:00:55, FastEthernet0/0
                     [90/161280] via 172.16.1.13, 00:00:55, FastEthernet0/1
D        192.168.1.2 [90/158720] via 172.16.1.17, 00:00:55, FastEthernet0/0
                     [90/158720] via 172.16.1.13, 00:00:55, FastEthernet0/1
```

**Figure 13 - An example of executing the command show ip route eigrp.**

```
R2#sho ip route 192.168.1.1
Routing entry for 192.168.1.1/32
  Known via "eigrp 1", distance 90, metric 156160, type internal
  Redistributing via eigrp 1
  Last update from 172.16.1.1 on FastEthernet0/0, 00:00:30 ago
  Routing Descriptor Blocks:
  * 172.16.1.1, from 172.16.1.1, 00:00:30 ago, via FastEthernet0/0
      Route metric is 156160, traffic share count is 1
      Total delay is 5100 microseconds, minimum bandwidth is 100000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

**Figure 14 – An example of executing the command "show ip route ip-add"**

The next command is "show ip protocols", which displays information about all routing protocols configured on the router. If EIGRP is configured on the router, it will display details such as the AS Number, K-Value coefficients, Variance, Administrative Distance for both external and internal routes, Maximum Path, and the networks that the router Is advertising through the EIGRP protocol.

An example of the output from this command is provided in Figure 15

International Journal of Innovation in Computer Science and Information Technology
Vol.5, NO.1 , P:1-19
Received: 21 October 2024
Accepted: 15 February 2025

```
R5#show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "application"
  Sending updates every 0 seconds
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Maximum path: 32
  Routing for Networks:
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 4)

Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 192.168.1.5
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
    192.168.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.1.22           90      00:00:16
    172.16.1.17           90      00:00:15
    172.16.1.13           90      00:00:15
  Distance: internal 90 external 170
```

**Figure 15 – An example of executing the command “show ip protocols”**

To verify the Topology Table, the command “show ip eigrp topology” can be used. This table stores both primary and backup routes to a network. At the beginning of the table, there are codes indicating the status of each route:

- A: Active
- P: Passive
- U: Update

If the code P is displayed next to a network, it means the router is in a normal state for that network and has fully learned it. However, if the code A appears, it indicates an issue with that network that requires troubleshooting.

In the output of this command, additional details are provided, including the number of successors, the Feasible Distance (FD), and the port number through which the router reaches the target network.

For networks that are not directly attached, two additional numbers are displayed in the format (X/Y):

International Journal of Innovation in Computer Science and Information Technology
Vol.5, NO.1 , P:1-19
Received: 21 October 2024
Accepted: 15 February 2025

- X: The calculated metric or Feasible Distance.
- Y: The Reported Distance or Advertised Distance (AD), which is the metric calculated by the neighbor router toward the destination network.

An example of the output from this command is provided in Figure 16.

```
R5#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(1)/ID(192.168.1.5)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 172.16.1.16/30, 1 successors, FD is 28160
        via Connected, FastEthernet0/0
P 172.16.1.8/30, 1 successors, FD is 30720
        via 172.16.1.17 (30720/28160), FastEthernet0/0
P 192.168.1.1/32, 2 successors, FD is 161280
        via 172.16.1.13 (161280/158720), FastEthernet0/1
        via 172.16.1.17 (161280/158720), FastEthernet0/0
P 172.16.1.12/30, 1 successors, FD is 28160
        via Connected, FastEthernet0/1
P 172.16.1.4/30, 1 successors, FD is 30720
        via 172.16.1.13 (30720/28160), FastEthernet0/1
P 172.16.1.20/30, 1 successors, FD is 28160
        via Connected, FastEthernet1/0
P 192.168.1.2/32, 2 successors, FD is 158720
        via 172.16.1.13 (158720/156160), FastEthernet0/1
        via 172.16.1.17 (158720/156160), FastEthernet0/0
P 172.16.1.0/30, 2 successors, FD is 33280
        via 172.16.1.13 (33280/30720), FastEthernet0/1
        via 172.16.1.17 (33280/30720), FastEthernet0/0
```

**Figure 16 – An example of executing the command "show ip eigrp topology"**

**EIGRP Authentication**

Each authentication requires a key or password. For authentication in EIGRP, a Key-Chain (a chain of keys) must first be created and assigned a Key-ID. To configure multiple passwords in this Key-Chain, a Key-String is created within it, and the password is entered along with the Key-String. Within this Key-Chain, the parameters Accept-LifeTime and Send-LifeTime can be configured for the password. These parameters define the time during which the password is valid for acceptance and the time during which it should be sent to neighbors. The configuration of these times is entirely optional, but if used, they must be identical on both neighbors.

If these two parameters are used, it is crucial to ensure that the NTP protocol is correctly configured in the network to synchronize the devices' clocks.

After setting up these configurations, you need to enter the configuration mode of the interface that will establish a neighbor

International Journal of Innovation in Computer Science and Information Technology
Vol.5, NO.1 , P:1-19
Received: 21 October 2024
Accepted: 15 February 2025

relationship with another router. Authentication is activated on this interface, and its mode is defined using the command:

ip authentication mode eigrp autonomous-system md5

Next, the command

ip authentication key-chain eigrp autonomous-system name-of-chain

is used to specify which Key-Chain will be used for authentication. The name of the Key-Chain does not need to be the same on both routers forming a neighbor relationship, but the Key-IDs within the Key-Chains on both sides must match. Additionally, the Key-Strings in the configuration of both routers must also match.
If the Accept-LifeTime and Send-LifeTime parameters for the first key expire, the configuration automatically switches to the next key with a new password. This eliminates the need for manually changing passwords.

**Figure 17 provides an example of how to configure authentication in the EIGRP protocol.**

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#key chain ch1
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string st1
R2(config-keychain-key)#accept-lifetime 01:00:00 Jan 1 2024 infinite
R2(config-keychain-key)#send-lifetime 01:00:00 Jan 1 2024 infinite
R2(config-keychain-key)#exit
R2(config-keychain)#key 2
R2(config-keychain-key)#key-string st2
R2(config-keychain-key)#accept-lifetime 01:00:00 Jan 5 2024 infinite
R2(config-keychain-key)#send-lifetime 01:00:00 Jan 5 2024 infinite
R2(config-keychain-key)#do wr
```

**Figure 17 - An example of Authentication configuration in EIGRP**

To verify the correctness of this mechanism's configuration, the command debug eigrp packets can be used. The output of this command shows the processes currently running on the router, which can be used for troubleshooting.

**Discussion and Conclusion**

Analysis of EIGRP reveals that this dynamic routing protocol, with its unique features such as very low convergence time, support for VLSM, partial updates, unequal load-balancing, easy configuration, MD5 authentication mechanism, and more, can serve as a flexible, reliable, and efficient tool for configuring routing in large-scale, complex computer networks. Given the increasing complexity of modern computer networks and the need for secure and error-free routing, EIGRP can be an ideal choice for network administrators. It effectively addresses the fundamental needs of computer networks, enhancing efficiency and improving overall network performance. Considering the advantages and unique features of this protocol, EIGRP is a suitable

option for optimizing the infrastructure of organizational networks.

## References

1- حسینقلی پور، مسعود، ۱۴۰۱، آموزش عملی و تصویری کاربردیCCNA 200-125 ، چاپ سوم، تهران، انتشارات دانشگاهی کیان
2- حسینقلی پور، مسعود، ۱۳۹۳، آموزش عملی و کاربردیCCNP Route 642-902 ، چاپ سوم، تهران، انتشارات دانشگاهی کیان
3- حسینقلی پور، مسعود، ۱۳۹۱، آموزش عملی و کاربردیCCNA Security 640-553 امنیت Cisco ، چاپ دوم، تهران، انتشارات دانشگاهی کیان
4- نوبری، سابینا، آب نیکی، روح اله، آقازاده، سکینه، ۱۳۹۳، شبکه‌های کامپیوتری، چاپ اول، تهران، انتشارات فراهوش
5- Wendell, Odom. (2013). CCNA Routing and Switching 200-120 Official Cert Guide Library. Pearson education
6- Hucaby, David. (2014). CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. Pearson education
7- Pepelnjak, Ivan. (2000). EIGRP Network Design Solutions. Cisco Press
8- D. Black, Uyless. (2000). IP Routing Protocols RIP, OSPF, BGP, PNNI, and Cisco Routing Protocols. Prentice Hall
9- Aweya, James. (2021). IP Routing Protocols Fundamentals and Distance-Vector Routing Protocols. CRC Press