Comparison of IP Routing Protocols

By Vladimir Rachev

# Introduction

In modern large-scale internetworks that there are many autonomous systems, dynamic routing protocol used more often than static routing protocol. The most effective and efficient routing protocol is needed to support modern network on a large scale. [1] Routing protocols determine the optimal paths for data packets to travel from source to destination, ensuring seamless communication across networks. These protocols fall into two primary categories: distance-vector protocols and link-state protocols.

This coursework aims to provide a practical understanding of routing protocols, focusing on Routing Information Protocol Version 2 (RIPv2) and Open Shortest Path First (OSPF). Through hands-on implementation in Cisco Packet Tracer (see figure 1), this investigation will explore the configuration, behaviour, and efficiency of these protocols in an internetwork environment.

Figure – Network Topology

A diagram of a computer network

AI-generated content may be incorrect.

Additionally, the coursework will extend the investigation to Enhanced Interior Gateway Routing Protocol (EIGRP), a Cisco-proprietary protocol that, while classified as an advanced distance-vector protocol, incorporates many features typically found in link-state protocols. By analysing routing tables, convergence speeds, and protocol responses to topology changes, this report will evaluate the strengths and weaknesses of each protocol. The findings will provide insights into which routing protocol is best suited for different network scenarios.

# Theory and Background

## 2.1 Understanding Routing Protocols

Routing protocols are essential components of internetwork infrastructure, responsible for determining the most efficient paths for data transmission between devices across a network. These protocols enable routers to communicate with one another, share information about network topology, and dynamically adjust routes in response to changes in network conditions. The ability of a routing protocol to effectively determine the best path between networked devices is crucial in ensuring optimal network performance, reducing latency, and avoiding congestion.

There are two primary categories of routing protocols: distance-vector routing protocols and link-state routing protocols. Distance-vector protocols determine routes based on the number of hops (routers) between the source and destination, whereas link-state protocols rely on a complete view of the network topology to calculate the most efficient path. This section explores the fundamental differences between these protocols and examines the key characteristics of Routing Information Protocol Version 2 (RIPv2), Open Shortest Path First (OSPF), and Enhanced Interior Gateway Routing Protocol (EIGRP).

## 2.2 Distance-Vector vs. Link-State Routing

There are two approaches to adaptive routing protocols for wide-area store-and-forward networks: distance vector and link-state. Distance-vector algorithms use O(N x e) storage at each node, whereas link-state algorithms use O(N^2), where N is the number of nodes in the network and e is the average degree of a node. [2]

### 2.2.1 Distance-Vector Routing

Distance-vector routing protocols determine the best path to a destination based on hop count, which represents the number of routers a packet must traverse before reaching its target. Each router periodically exchanges its entire routing table with directly connected neighbours. These neighbours then pass the information along to their own neighbours, eventually spreading routing updates throughout the network. Since the advertising through a routing domain occurs in an iterative fashion, and the new route eventually snowballs through the domain, it may take a while for the best routes to be made known to all. [3]

The primary advantage of distance-vector routing is its simplicity—it requires minimal configuration and computational power. However, because routers blindly trust the information they receive from neighbours, distance-vector protocols are susceptible to routing loops, which occur when incorrect routing information circulates indefinitely within the network. To prevent this, protocols like RIPv2 implement loop-prevention mechanisms, including:

* Split Horizon – Prevents a router from advertising a route back in the direction it was learned from.
* Route Poisoning – Assigns an unreachable hop count (16 in RIP) to a failed route to ensure it is quickly removed from routing tables.
* Hold-Down Timers – Delays accepting new routes for a certain period to avoid flapping (rapid route changes).

Despite these improvements, distance-vector routing protocols face scalability issues because of slow convergence times—it can take several update cycles for an network to recognize and adapt to topology changes. Additionally, periodic updates consume significant bandwidth, making distance-vector protocols inefficient for large internetworks.

### 2.2.2 Link-State Routing

Link-state routing protocols offer a more sophisticated and efficient approach to path selection. From a more technical side, the link-state approach is a straight-forward brute-force approach where each node maintains a view of the network topology with a cost for each link, and uses this view to obtain minimum cost routes for each destination [2].Unlike distance-vector protocols, which depend on neighbouring routers to gradually share updates, link-state protocols require each router to independently maintain a complete, synchronized map of the network topology. This is achieved through link-state advertisements (LSAs), which contain detailed information about a router’s directly connected links, including:

* Link bandwidth and speed
* Network connectivity status
* Neighbouring routers and their costs

When a router starts up, it floods LSAs to all other routers in the network, ensuring that every router has a consistent and up-to-date database of the entire network. Using this information, routers individually calculate the shortest path to each destination using Dijkstra’s Shortest Path First (SPF) algorithm. Because every router performs calculations based on the same set of link-state information, all routers eventually reach a loop-free and stable routing topology.

**Key Characteristics of Link-State Routing**

1. Topological Awareness – Every router builds a network-wide view, not just a local neighbour-based table.
2. Event-Driven Updates – Unlike distance-vector protocols that send periodic updates, link-state protocols only send updates when network changes occur, reducing bandwidth consumption.
3. Faster Convergence – When a link fails, LSAs are immediately propagated across the network, allowing routers to quickly recalculate routes without waiting for periodic updates.
4. Hierarchical Scalability – Some link-state protocols support area-based segmentation, which divides the network into manageable sections, improving efficiency in large-scale networks.

Link-state protocols offer several advantages over distance-vector protocols, particularly in terms of scalability and convergence speed. Since routers store and process a full topology map, they can make more informed routing decisions based on actual link bandwidth and cost, rather than just hop count. However, this comes at the cost of higher CPU and memory usage, as routers must store and process detailed internetwork information.

## 2.3 Types of Routing Protocols

### 2.3.1 Routing Information Protocol Version 2 (RIPv2)

Routing Information Protocol version 2 (RIPv2) is an improved version of RIP, designed to support classless routing, subnetting, and multicast updates. Like its predecessor, RIPv2 is a distance-vector protocol that determines the best path based on hop count, with a maximum hop limit of 15. This limitation restricts the protocol’s scalability, as any destination beyond 15 hops is considered unreachable.

RIPv2 operates using the Bellman-Ford algorithm, in which routers periodically exchange their entire routing table with directly connected neighbours. These updates occur every 30 seconds, which, while simple, leads to high bandwidth consumption and slow convergence. This periodic approach means that network failures may take up to three update cycles (90 seconds) to be recognized and resolved, making RIPv2 unsuitable for networks with frequent topology changes.

Loop prevention in RIPv2 relies on mechanisms such as split horizon and route poisoning, which help reduce routing loops but do not eliminate them entirely. Additionally, because RIPv2 broadcasts full routing tables rather than sending only updates, it is inefficient in larger internetworks.

Despite its limitations, RIPv2 remains useful for small networks that require a simple and automatic routing configuration. Its low processing requirements make it ideal for environments with limited hardware resources. [4]

### 2.3.2 Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is a link-state routing protocol that overcomes the limitations of distance-vector protocols by building a complete topology map and calculating the shortest paths using Dijkstra’s SPF algorithm. Unlike RIPv2, OSPF does not rely on hop count but instead assigns a cost to each link, where higher-bandwidth links are preferred over slower ones. This allows OSPF to optimize traffic flow and reduce congestion. Fast convergence to topology changes has emerged as a critical requirement for today's routing infrastructures, however limiting the processing/bandwidth overhead of the routing protocol continues to be as important as before. OSPF, being a distributed protocol, requires timely execution of certain operations, e.g., generation and processing of hello packets, by the participating routers. [5]

OSPF routers exchange Link-State Advertisements (LSAs), which describe network links and their status. These LSAs are only propagated when a change occurs, reducing unnecessary bandwidth usage. Routers use this information to construct a Link-State Database (LSDB), ensuring that all OSPF routers maintain an identical view of the internetwork.

One of OSPF’s distinguishing features is its hierarchical area-based design. Large internetworks can be divided into multiple areas, with Area 0 (backbone area) serving as the central link between other areas. This segmentation reduces processing overhead and improves scalability.

The complexity of OSPF configuration requires detailed planning, particularly in assigning area numbers, link costs, and router IDs. Despite its complexity, OSPF’s fast convergence, loop-free routing, and efficient use of bandwidth make it the preferred choice for large enterprise and ISP internetworks.

# Routing Protocol Configuration and Verification

## 3.1 Configuring RIPv2 on the Network

The implementation of Routing Information Protocol Version 2 (RIPv2) was performed on all routers in the network except for the ISP router, as it is outside the scope of internal routing. The configuration involved enabling RIPv2, specifying the directly connected networks for each router, and propagating a default route from the Boundary Router to ensure connectivity with external networks.

To avoid redundancy, screenshot for every router configuration will not be provided, as many routers follow a repetitive and nearly identical setup to those already shown. Instead, representative examples that illustrate the general RIPv2 configuration process across different router types have been included. The remaining routers were configured using the same methodology, ensuring consistency in network advertisement and route propagation. Since RIPv2 supports classless routing, the **no auto-summary command** was used to allow the advertisement of subnetted networks (the command is not included in the screenshots because it was configured in a later instance).

### ABR 2

Router-PT ABR 2 is connected to routers A2BB, WG3 and WG4, as well as A0SW1 and A0SW2 directly. (see Figures 2 and 3)

Figure – ABR 2 Configuration

A screen shot of a computer

AI-generated content may be incorrect.

Figure – Area 0 Topology

A diagram of a diagram

AI-generated content may be incorrect.

### ABR 1

Router-PT ABR 1 is connected to router GFE and switches A0SW1, FESW1 directly. (see Figure 4)

Figure – Router ABR 1 configuration

A screenshot of a computer error

AI-generated content may be incorrect.

### GFE

Router-PT GFE is connected to router ABR 1 directly and router WG1 and WG2 through GFESW. (see Figures 5 and 6)

Figure – Router GFE configuration

A screenshot of a computer program

AI-generated content may be incorrect.

Figure – Area 1 Topology

A diagram of a router

AI-generated content may be incorrect.

### WG1

Router-PT WG1 is connected to ABR 1, WG1 PC and router GFE through switches FESW1, WG1SW and GFESW, respectively. (see Figure 7)

Figure – Router WG1 Configuration

A screenshot of a computer

AI-generated content may be incorrect.

### A2BB

A diagram of a graph

AI-generated content may be incorrect.Router-PT A2BB is directly connected to router ABR 2 and connected to router WG3 and WG4 through switch A2BBSW. (see Figure 8)

Figure – Area 1 topology

A black text on a white background

AI-generated content may be incorrect.

Figure 8 – Router A2BB Configuration

### Boundary Router

The Boundary Router is directly connected to the ISP router and to router ABR 2 through switch A0SW2. (see Figures 9 and 10). Router of last resort is propagated to all other routers.

Figure – Boundary Router configuration

A screenshot of a computer code

AI-generated content may be incorrect.

Figure – External network topology

A diagram of a router

AI-generated content may be incorrect.

### 3.1.1 Ping and Traceroute tests

PC WG1 being able to ping every other PC and any exterior router on the Internet. (see Figures 11 and 12 below)

Figure - Traceroute to WG2, WG3, WG4 and Exterior Router

Figure - Pinging PC WG2, WG3, WG4 and Exterior Router

A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A black screen with white text

AI-generated content may be incorrect.

## 3.2 Configuring OSPF on the Network

The implementation of Open Shortest Path First (OSPF) was carried out across all internal routers in the network, ensuring efficient routing and fast convergence. Unlike RIPv2, which relies on hop count, OSPF determines the best path using cost, calculated based on link bandwidth. The network was divided into hierarchical areas, with Area 0 (Backbone) serving as the central hub for inter-area communication. Each router was assigned to its respective area and configured to advertise its directly connected networks.

To avoid redundancy, a screenshot for every router configuration will not be provided, as many routers follow a repetitive and nearly identical setup to those already shown. Instead, representative examples that illustrate the general OSPF configuration process have been included, covering different router types and area assignments. The remaining routers were configured using the same methodology, ensuring consistent area segmentation and route advertisement. Since OSPF requires manual area assignment, each router was carefully placed in the correct area using the **network <ip> <wildcard> area <id> command.**

### ABR 2

Router-PT ABR 2 is connected to routers A2BB, WG3 and WG4, as well as A0SW1 and A0SW2 directly.

(see Figure 13)

Figure – ABR 2 Configuration

A number on a white background

AI-generated content may be incorrect.

### ABR 1

Router-PT ABR 1 is connected to router GFE and switches A0SW1, FESW1 directly. (see Figure 14)

Figure – ABR 1 Configuration

A number of numbers on a white background

AI-generated content may be incorrect.

### GFE

Router-PT GFE is connected to router ABR 1 directly and router WG1 and WG2 through GFESW. (see Figure 15)

Figure – GFE Configuration

A black text on a white background

AI-generated content may be incorrect.

### WG1

Router-PT WG1 is connected to ABR 1, WG1 PC and router GFE through switches FESW1, WG1SW and GFESW, respectively. (see Figure 16)

Figure – WG1 Configuration

A black text on a white background

AI-generated content may be incorrect.

### A2BB

Router-PT A2BB is directly connected to router ABR 2 and connected to router WG3 and WG4 through switch A2BBSW. (see Figure 17)

Figure – A2BB Configuration

A white background with black text

AI-generated content may be incorrect.

### Boundary Router

The Boundary Router is directly connected to the ISP router and to router ABR 2 through switch A0SW2 (see Figure 18). Router of last resort is propagated to all other routers.

Figure – Boundary Router Configuration



### 3.2.1 Ping and Traceroute tests

PC WG1 being able to ping every other PC and any exterior router on the Internet. (see Figures 19 and 20 below)

A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.

Figure – Traceroute tests from WG1

A screenshot of a computer

AI-generated content may be incorrect.Figure – Ping tests from WG1

A screenshot of a computer screen

AI-generated content may be incorrect.

# Analysis and Investigation

## 4.1 Routing Tables Analysis

The routing table of routers ABR 1 and the Boundary Router was analysed under three different routing protocols: RIPv2, OSPF and EIGRP. The objective of this comparison is to identify differences in the number of routes, metric values, and default route propagation between the three protocols.

We can observe that both ABR 1 and the Boundary Router display the same number of routes under RIPv2, OSPF, and EIGRP. This confirms that all three protocols are learning the full routing table correctly. However, the way each protocol determines the best path, calculates metrics, and selects the optimal routes still varies significantly.   
This section will provide an analysis of the metric systems used by each protocol and how they influence routing Decisions.

Each routing protocol evaluates paths differently, leading to variations in the metric values assigned to the same destinations. Consulting with figures 21,22 and 23 we can observe that RIPv2’s metric type is hop count, namely [120/X]. The best route selection criteria for RIP are the fewest number of hops. For OSPF, the metric type is Cost, namely [110/X]. The best route selection criteria for OSPF are the best bandwidth path (lower cost is better). EIGRP uses a composite metric [90/X] and is a bit more complicated than the other two routing protocols. I will use the default route (0.0.0.0/0) metric to perform comparisons between the ABR 1 Routers to support my analysis.

Figure - ABR 1 Routing Table

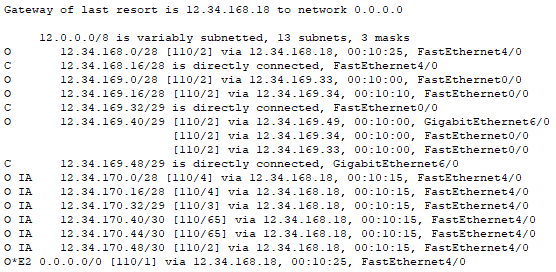


Figure - Boundary Router OSPF Routing Table

A screenshot of a computer program

AI-generated content may be incorrect.

Figure - ABR 1 RIPv2 Routing Table

A screenshot of a computer

AI-generated content may be incorrect.

Figure - Boundary Router RIPv2 Table

A screenshot of a computer screen

AI-generated content may be incorrect.

Figure - ABR 1 EIGRP Routing Table

A screenshot of a computer program

AI-generated content may be incorrect.

Figure - Boundary Router EIGRP Routing Table

A computer screen shot of a computer code

AI-generated content may be incorrect.

In EIGRP, the numbers displayed are the two key components of the route metric, in this case “90” is the administrative distance (AD), and “56320 “is the EIGRP composite metric. Lower AD values, which is a measure of the trustworthiness of the source of a route, indicate more preferred routes. For example, we can observe from the figures below that EIGRP internal (D) has an AD value of 90, whereas EIGRP External (D EX) has an AD value of 170, making the internal routes of EIGRP more preferred than OSPF (110) or RIP (120).   
The second number (56320) determines the best path to a destination. This metric is calculated using a formula based on: Bandwidth – Lower bandwidth links increase the metric and Delay – higher delay increases the metric.

## 4.1.1 EIGRP calculates its metric using the following default formula [6]:

A black background with white text

AI-generated content may be incorrect.

* The next-hop interface is FastEthernet4/0, which has a bandwidth of 100,000 kbps (100 Mbps).
* Using the bandwidth formula: 10^7 / Bandwidth (kbps), we get 10^7 / 100,000 = 100
* The total delay is the sum of interface delays in tens of microseconds (μs).
* Assuming the total delay from the router to the next-hop is 2000 μs (this is estimated based on standard Cisco FastEthernet delay values).
* Convert it into tens of microseconds: Total Delay=2000×10=20,000
* Using the EIGRP metric formula:

((10^7 / bandwidth) + delay) x 256 = **53760**

* Compare with our Routing Table
* Our routing table shows **56320**, which is slightly higher than the calculated **53760**.
* The difference is likely due to additional propagation delays in the network or rounding in Cisco’s internal calculations. [6]

## 4.1.2 Routing Tables Metrics Comparison

Now that we know how each one of the routing protocols performs their calculations, we can analyse their default route metrics **for ABR 1**. From our findings, OSPF has the lowest metric (1), meaning it sees the default route as the most optimal path based on bandwidth efficiency. EIGRP assigns a metric of 56320, which we previously calculated. This metric is much higher than OSPF because it involves a more complex calculation. RIPv2, on the other hand, has the simplest metric (2), since it only counts the number of hops. This means it completely ignores bandwidth, delay, and link quality.

Additionally, by comparing the metrics for the **Boundary router** to network 12.34.169.16/28, we can see that all three protocols successfully converged with the same number of routes. However, the metrics this time are different than our previous discovery. In this analysis, OSPF has a metric of 4, whereas RIPv2 has a metric of 3. After performing OSPF’s metric calculation which is Cost = 100/ Interface Bandwidth we can see that OSPF is indeed faster than RIPv2. A lower hop-count does not necessarily mean a better route, as the network may have slow links. In our case, RIPv2 chooses the FastEthernet connection which has a lower bandwidth than the Gigabit connection that OSPF chooses. This means that even though RIPv2 passes through less routers, it is not faster than OSPF’s route.

OSPF has a more accurate path selection, which is based on actual link speed, ensuring that higher bandwidth links are preferred. EIGRP also accounts for bandwidth the same way OSPF does, but is influenced by delay, which can lead to suboptimal path choices. In addition, EIGRP is Cisco-proprietary, limiting its use in multi-vendor environments. Furthermore, RIP, even though having the simplest metric, is suboptimal in large networks due to its 15-hop limit and its potential to choose a slow link just because it has fewer routers.

By analysing the default route metrics, we can see that OSPF consistently selects the best possible route based on link bandwidth, whereas EIGRP uses a more complex calculation and RIP simply counts hops, often resulting in inefficient routing.

## 4.2 OSPF Reference Bandwidth increase

After increasing the reference bandwidth of all the routers to 1000Mbit/s, the cost of the routes increased. A higher metric means OSPF now considers these routes as more expensive and will likely avoid them if there is a lower-cost alternative. In the original OSPF table the cost for most networks was 110/3-4, meaning that OSPF saw them as efficient routes. Some links that previously had low costs now have higher costs because their relative bandwidth is much lower (see Figure 27). For example, we can see that at 12.34.170.40 and .44 the cost is 7822. This is due to the fact that they’re connected by Serial links. In Packet Tracer, the default bandwidth (and thus, speed) for a serial interface is typically 1.544 Mbps (T1). But if we perform the calculation Cost = 1000/1.544 = 647 we see that the cost is much higher than the expected cost for 1.544Mbps. This means that the router’s serial connection is 128 kbps which would equal exactly to 7822 (1000/0.128). We can confirm this by entering the command **show interface serial2/0** on Router ABR 2 which then tells us that the bandwidth is indeed 128Kbit/sec. (see Figure 28).

The other costs have increased as well due to their low FastEthernet bandwidth being capped at 100,000 Kbit/sec or 100 Mbps.

A screen shot of a computer

AI-generated content may be incorrect.

Figure – costs have increased significantly

Figure – low bandwidth of interface on router ABR 2

A screenshot of a computer program

AI-generated content may be incorrect.

## 4.3 Responses to changes in Topology

### 4.3.1 How RIP responds to changes in the topology

To evaluate how RIPv2 responds to changes in network topology, the Serial 3/0 interface on Router ABR2 was disconnected, and a traceroute test was performed to observe how the network adapted to the failure. The goal of this test was to analyse RIPv2’s convergence speed and how effectively it recalculates new paths when a link becomes unavailable. Traceroute was first performed while the Se3/0 interface is still up. We can see that we were able to establish a connection between WG1 and the network 12.34.170.16 almost instantly without any issues. (see Figure 29)

Figure – traceroute working seamlessly

A screenshot of a computer program

AI-generated content may be incorrect.

Upon disconnecting the link (see Figure 31), a **tracert** command was initiated from WG1 PC to the destination 12.34.170.16(see Figure 30). The results indicated that RIPv2 took a noticeable amount of time to update its routing tables (25 seconds to be exact), during which packets experienced looping behaviour as routers continued to forward traffic along the failed path until the failure was fully recognized by RIP’s periodic updates.

Since RIPv2 uses a periodic update mechanism (every 30 seconds by default), the convergence time was significantly slower compared to OSPF or EIGRP, which react more dynamically to network changes. The way RIP update timers work is like a clock, they keep running all the time, so if an interface is shut down right before the next scheduled update, the change may be sent out almost immediately, however if the interface shuts down right after an update, you may have to wait up to 30 seconds for the next periodic update. This delay can cause temporary packet loss, increased latency, or routing loops, as seen in the traceroute output where packets kept cycling between certain routers before stabilizing.

This experiment highlights one of the major weaknesses of RIPv2, as its reliance on timers rather than immediate topology change detection results in slower adaptability to network failures.

Figure – Disconnecting the link

Figure – Packets looping after disconnect

A screenshot of a computer program

AI-generated content may be incorrect.A diagram of a graph

AI-generated content may be incorrect.

Here the **debug ip routing command** was ran (Figure 32) which allows us to see how routers that are directly affected by the topology change perform their new routing. We can see that routes via serial 3/0 disappear and RIPv2 finds an alternate path. However, there was a delay before the new route was found.

Figure – debug ip routing

A screenshot of a computer

AI-generated content may be incorrect.

After the update was received, the PC was then able to find its way to the network but on a new path via router WG3. (see Figure 33)

Figure – tracert succesful through WG3

A screenshot of a computer

AI-generated content may be incorrect.

### 4.3.2 How OSPF responds to changes in the topology

Now, we will conduct the same topology change test using OSPF instead of RIPv2. The goal is to observe how OSPF reacts to a serial interface failure and compare it with RIP. First, a traceroute was performed while the Se3/0 interface is still up. We can see that we were able to establish a connection in a similar manner as RIP between WG1 and the network 12.34.170.16 almost instantly without any issues. However, there is one significant difference. The last connection, namely 12.34.170.16 appears on the traceroute that was performed on the OSPF configuration (see Figure 34), whereas when it was performed on the RIP configuration, we could only see the last hop (see Figure 28,32). This behaviour occurs due to fundamental differences that were previously discussed in the report in how RIPv2 and OSPF handle routing updates. To reiterate, RIP uses hop count as its only metric, meaning it only cares about how many routers are in the path rather than link cost, whereas OSPF considers the cost of each link rather than just hop count. Consulting with Figure 35, we can use a **command show ip ospf neighbour** which helps us see which neighbours are active, down, or re-establishing. As we can observe, all neighbours are up, including Se3/0.

Figure – OSPF tracert successful

A screenshot of a computer screen

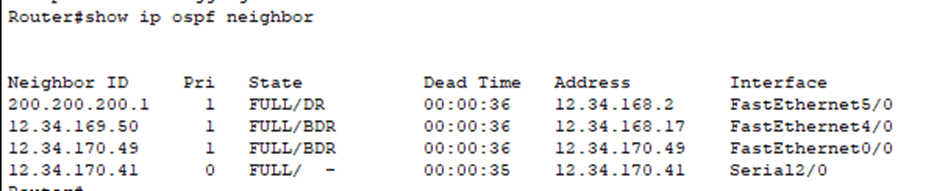
AI-generated content may be incorrect.

Figure – show ip ospf neighbor showing active neighboursA number of numbers and a number of objects

AI-generated content may be incorrect.

Once we shutdown the Se3/0 interface and perform the same command again, we can now see that the neighbour that was previously on Se3/0 is now absent (Figure 36).

Figure - .45 is now absent



In addition, we can perform the command **debug ip ospf adj**, which will show when OSPF detects the change and recalculates routes (see Figure 37). The provided debug output demonstrates how OSPF reacts instantly when a link failure occurs. In this case, the Serial3/0 interface was shut down, causing an immediate OSPF neighbour state change. At 00:47:55, the following sequence of events took place:

The interface was administratively shut down, leading to a LINK-5-CHANGED and LINEPROTO-5-UPDOWN message.

OSPF immediately detected the loss of the neighbour (Router ID 12.34.170.45) and changed its state from FULL to DOWN.

Within the same second (00:47:55), OSPF began recalculating routes by generating and flooding new LSAs (Link-State Advertisements) for Areas 1 and 2.

The LSA sequence numbers (0xFFFFFFFF8000000F and 0xFFFFFFFF80000009) indicate the immediate update and propagation of new topology information to all OSPF routers.

This instantaneous response is a key advantage of OSPF over RIP, as it ensures that alternate routes are calculated and deployed in real time, minimizing packet loss and downtime. In contrast, RIP would take up to 30 seconds to detect the failure due to its periodic update mechanism as we previously discussed. This proves OSPF’s superior convergence speed, which is critical in maintaining efficient and reliable network operations. Consulting Figure 38, we can observe that after the Serial3/0 interface was shut down, the traceroute continued to function seamlessly, demonstrating OSPF’s rapid convergence and dynamic rerouting capabilities

Figure – recalculation of routes

A computer code on a white background

AI-generated content may be incorrect.

Figure – traceroute functioning after se3/0 is shut down

A screenshot of a computer screen

AI-generated content may be incorrect.

# Conclusion

This investigation provided valuable hands-on experience in configuring and analysing RIPv2, OSPF, and EIGRP. By comparing their routing tables, metric calculations, and convergence times, I gained insight into how different protocols determine optimal paths in a network.

One key takeaway was the clear advantage of OSPF over RIPv2 and EIGRP. While RIPv2's hop count metric limits scalability, and EIGRP’s composite metric considers bandwidth and delay, OSPF’s link-state approach offers superior convergence speed and dynamic adaptability. Testing topology changes confirmed that OSPF reacts almost instantly, while RIPv2 relies on periodic updates, leading to slower reconvergence.

Additionally, exploring Cisco’s OSPF commands—such as show ip ospf database—provided deeper insights than RIPv2’s database commands, reinforcing OSPF’s robustness. Adjusting the OSPF reference bandwidth also demonstrated how metric calculations can be optimized for real-world scenarios.

**Future Investigations**

A logical next step would be testing multi-protocol routing, examining route redistribution between OSPF, EIGRP, and RIPv2. Additionally, studying the impact of network congestion on routing decisions could provide further insights into protocol efficiency under heavy traffic.

This study has strengthened my understanding of routing protocols, troubleshooting, and network optimization, preparing me for more advanced networking challenges.

# References

|  |  |
| --- | --- |
| [1] | A. F. M. F. I. a. A. S. U. Masruroh, “Performance evaluation of routing protocol RIPv2, OSPF, EIGRP with BGP,” IEEE, Salatiga, Indonesia, 017 International Conference on Innovative and Creative Information Technology (ICITech). |
| [2] | A. U. a. A. Shankar, “Performance comparison of routing protocols using MaRS: distance-vector versus link-state,” Association for Computing Machinery, New York, NY, USA, 1992. |
| [3] | U. Black, “Route Discovery Principles,” in *IP Routing Protocols*, Pearson, 2000. |
| [4] | M. M. A. a. K. T. A. G. K. Dey, “Performance analysis and redistribution among RIPv2, EIGRP & OSPF Routing Protocol,” IEEE, Rajshahi, Bangladesh, 2015 International Conference on Computer and Information Engineering (ICCIE). |
| [5] | M. Goyal, “Improving Convergence Speed and Scalability in OSPF: A Survey,” 2012. |
| [6] | M. M. M. a. M. Bhuiyan, “An Exploration of the Ambiguities of EIGRP Cost Matrix,” Saudi Arabia, 2012. |
| [7] | M. Goyal, “Improving Convergence Speed and Scalability in OSPF: A Survey,” IEEE, 2012. |