A Study on Routing Protocols based on their Implementations using GNS3

A. Gheisari, A. Shorafa, and M. Ghazvini
Department of Computer Engineering, Faculty of Engineering,
Shahid Bahonar University of Kerman, Iran
alirezashorafa@eng.uk.ac.ir, mghazvini@uk.ac.ir, amirreza.gheisari@eng.uk.ac.ir
Corresponding author: mghazvini@uk.ac.ir

***Abstract*- Dynamic routing protocols play a crucial role in computer networks by providing high throughput, flexibility, low overhead, scalability, easy configuration, and optimal bandwidth and CPU utilization. Organizations select routing protocols based on criteria such as their size, number of users, data volume, policies, needs, and network infrastructure. In this study, we utilize GNS3 software to simulate real-world scenarios to offer a detailed review and comparison of key routing protocols, including RIP, OSPF, BGP, IGRP, EIGRP, and ISIS. Our comparison encompasses protocol type, scalability, convergence time, load balancing capabilities, support for Variable Length Subnet Masks (VLSM), and metrics. The goal is to assist organizations in making informed decisions when selecting a routing protocol for their network infrastructure by identifying the most suitable and practical protocols for different environments. We present a comprehensive analysis of the strengths and weaknesses of these protocols, enabling organizations to choose the most appropriate one based on their specific requirements.**

***Index Terms*-** Routing protocols, Topologies, GNS3, Implementation.

I. INTRODUCTION

In today's interconnected world, computer networks play a crucial role in facilitating communication and data exchange. One of the fundamental aspects of computer networking is routing, which involves finding the best path for data to travel between different network devices. Routing protocols are responsible for selecting a specific path to route packets along. This process, known as routing, involves choosing the best path among routers in the network. Routing is necessary for different networks to communicate with each other, and it is accomplished through routing protocols. A routing protocol is a set of rules that govern how routers communicate with one another to exchange information and determine the best routes between nodes in a computer network. Routers

Manuscript received 13-Jan.-2022 and revised 19-May-2022,
Accepted on 22- June-2022

P- ISSN: 2322-4088
E- ISSN: 2322-3936

play a crucial role in directing traffic on the Internet. Routing protocols are software programs that implement specific routing algorithms, which are mathematical procedures used to calculate the cost of different paths or routes through the network. By determining the optimal routes, routing protocols help to ensure that network traffic is efficiently and reliably routed to its destination.

To achieve efficient and reliable routing, various routing protocols have been developed. Each of these dynamic routing protocols has its strengths and weaknesses. For example, one protocol may have fast convergence, while another may be very reliable. In this context, the present article aims to explore the different routing protocols, including OSPF, EIGRP, RIP, and BGP, IGRP, ISIS, and investigate their implementation using GNS3, a popular network simulation software. The study examines the advantages and disadvantages of each protocol in different network topologies and provides practical guidance on how to configure and implement them in a simulated environment.

The article highlights the importance of selecting the appropriate routing protocol based on the specific requirements of the network and its topology. It shows how GNS3 can be a valuable tool for testing and validating different routing protocols. The insights provided in this study are aimed at network engineers and researchers who are interested in studying routing protocols and their implementation using GNS3. Besides, this project aims to examine routing protocols in a specialized way and compare them based on their types, scales, convergence time, load balancing, VLSM support, metrics, and other features, and ultimately determine which protocols are more suitable for what locations.

The remainder of this paper is organized as follows. Section II explains a brief introduction to routing protocols and their importance in computer networks. Section III provides an overview of various routing protocols, including OSPF, RIP, BGP, EIGRP, IGRP, and ISIS, while the comparisons of these routing protocols based on various criteria and their examinations are given in Section IV. Section V concludes the paper as well as some future research directions.

II. ROUTING PROTOCOLS

A routing protocol is a method of communication between routers in a computer network that enables them to select routes between nodes or hops. Routers perform the function of directing traffic on the Internet. Routing protocols are software implementations of specific routing algorithms, which use mathematical procedures to optimize the cost of different routes or paths through the Internet to route traffic. Data packets are transmitted through Internet networks from router to router until they reach their destination computer. Routing algorithms determine the specific path to take. Each router only has information about networks that are directly connected to it. A routing protocol initially shares this information with its direct neighbors and then across the network as a whole. In this way, routers acquire knowledge about the topology of the network. The ability of routing protocols to dynamically adjust to changing conditions such as connections, inactive components, and routing around obstacles is what makes the Internet resilient and highly available.

Special features of routing protocols include a method for avoiding routing loops, how preferred are selected, the use of hop counts information, the time required to achieve routing convergence, their scalability, and cloud access framework parameters. The goal of routing protocols is to select the best route for routing and to update the routing table. The tasks of routing protocols include:

- Sharing their routing table with other routers in the network,
- Sending and receiving update messages from other routers and processing them,
- Automatically updating the routing table of routers in the network,
- Calculating the best route to reach the destination and placing it in the routing table.

The purpose of Dynamic Routing Protocols are:

- Discovery of remote networks,
- Maintaining up-to-date routing information,
- Choosing the best path to destination networks,
- Ability to find a new best path if the current path is no longer available [1].

In summary, a routing protocol is responsible for selecting the best path by which data packets can be transmitted between networks. Without the capability of routing, it is impossible to find the best communication path between two networks.

A. Characteristics of Routing protocols

1) Algorithm

Each routing protocol uses a specific algorithm to determine the best path for data to travel. This algorithm takes into account factors such as link cost, network topology, and traffic load.

2) Convergence

Convergence refers to the speed at which the network adapts to changes in the topology or traffic patterns. Some routing protocols have faster convergence times than others.

3) Scalability

Routing protocols should be able to handle networks of different sizes and complexities. Some protocols are better suited for small networks, while others are designed for large and complex networks.

4) Administrative distance

The administrative distance (AD) is a Cisco-specific parameter that assigns a numerical value between 0 and 255 to each routing protocol. When a router has multiple paths the

Table I. Routing protocols administrative distance

Route Source	Default AD	Route Source	Default AD
RIP	120	External EIGRP	170
Internal EIGRP	90	OSPF	110

destination in its routing table, the administrative distance parameter is used to select which protocol to use for routing such as OSPF, EIGRP, or Static Route. Any routing protocol with a lower AD is preferred. Table I. shows the AD values of various routing protocols.

5) *Metrics*

Routing protocols use metrics to determine the best path for data to travel. Metrics can include factors such as hop count, bandwidth, delay, and reliability [2].

6) *Type*

There are two main types of routing protocols: static and dynamic. Static routing protocols require manual configuration, while dynamic routing protocols enable routers to automatically exchange information about network topology and select the best path for data to travel.

7) *Convergence time*

Convergence time is the time it takes for the network to adapt to changes in network topology or traffic patterns. Some routing protocols have faster convergence times than others [1].

Understanding the characteristics of different routing protocols is essential for selecting the appropriate protocol for a particular network and ensuring optimal network performance and reliability.

III. CLASSIFICATION OF ROUTING PROTOCOLS

This section describes multiple routing protocols (especially particularly dynamic routing protocols) as shown in *Fig. 1*. and explains their relative strengths and weaknesses.

A. ROUTING INFORMATION PROTOCOL

Routing Information Protocol (RIP) is a distance-vector routing protocol used in computer networks to distribute routing information between routers. It is one of the oldest routing protocols

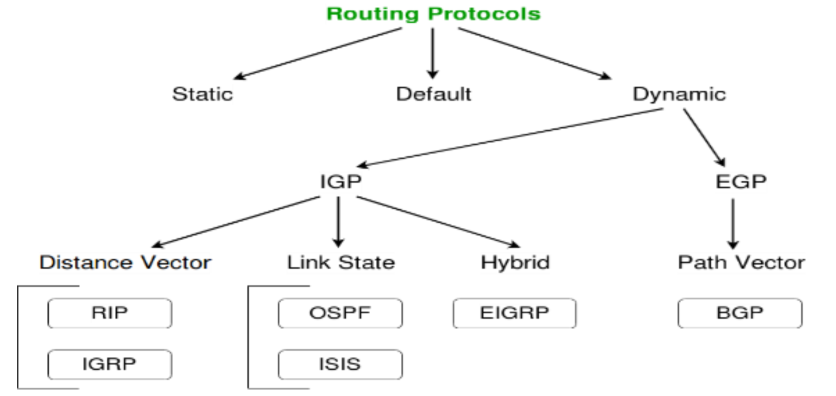


Fig. 1. Classification of routing protocols

and was originally designed for small networks with a maximum of 15 hops. There are three standardized versions of the Routing Information Protocol: RIPv1 and RIPv2 for IPv4, and RIPng for IPv6. RIP uses the Uses Datagram Protocol (UDP) as its transport protocol and is assigned the reserved 520 [2]-[3].

1) RIPv1

The RIP version 1 uses hop count as the only metric to determine the best path for data to travel. The maximum number of hops allowed is 15, which limits the size of the network. RIP version 1 does not support classless routing, which means that all subnets within a network must be of the same size. When updating the routing table between network routers, RIP uses broadcast messages (255.255.255.255). Every 30 seconds, it publishes the entire routing table through the active interfaces, which creates overhead in the network and consumes significant bandwidth.

2) RIPv2

RIP version 2 was introduced to overcome the limitations of RIP version 1. It supports classless routing and uses several metrics, including hop count, bandwidth, and delay, to determine the best path for data to travel. The maximum number of hops allowed is still 15. RIP v2 uses multicast (224.0.0.9) to send routing updates, which reduces network traffic and improves overall network performance. Support for Variable-Length Subnet Mask (VLSM) is a critical feature that reduces IP address waste in the network by allowing for more efficient use of available IP addresses.

In addition to broadcast, support for multicast is another important feature that reduces network bandwidth consumption. By allowing messages to be sent to multiple recipients simultaneously, multicast can significantly reduce network traffic and improve overall network performance. RIP v2 also offers authentication support, which allows routers to authenticate before sending their routing table to another router. This helps to prevent unauthorized access and ensures that only authorized routers can exchange routing information.

3) *RIPng*

RIPng is the IPv6 version of RIP. It is similar to RIP version 2 but uses IPv6 addresses instead of IPv4 addresses [3]-[4]. The advantages of version 2 of the RIP protocol are:

- Support for Variable-Length Subnet Mask (VLSM) is a critical feature that reduces IP address waste in the network by allowing for more efficient use of available IP addresses.
- In addition to broadcast, support for multicast is another important feature that reduces network bandwidth consumption. By allowing messages to be sent to multiple recipients simultaneously, multicast can significantly reduce network traffic and improve overall network performance.
- In RIP v2, the multicast address used for broadcasting routing updates is 224.0.0.9. This address is reserved for the Routing Information Protocol and is used by routers to exchange routing information with each other. By using multicast, RIP v2 reduces network traffic compared to RIP v1, which uses broadcast to send updates [2].
- Authentication support, is an important feature that allows routers to authenticate before sending their routing table to another router. This helps to prevent unauthorized access and ensures that only authorized routers can exchange routing information.
- In RIP v2, authentication can be configured using a simple password-based authentication scheme or a stronger message digest-based authentication scheme [4].
- RIP uses a round-robin system of load-balancing between equal metric routes. When a router has multiple routes with the same metric value to a destination, it will distribute traffic across the routes in a round-robin fashion. This helps to evenly balance traffic across the available routes and prevent congestion on any one route.
- The main advantage of RIP is its simplicity. It is easy to configure and requires minimal network resources. However, RIP has several limitations, including slow convergence times and limited scalability. In addition, RIP is vulnerable to routing loops and other network problems [5].

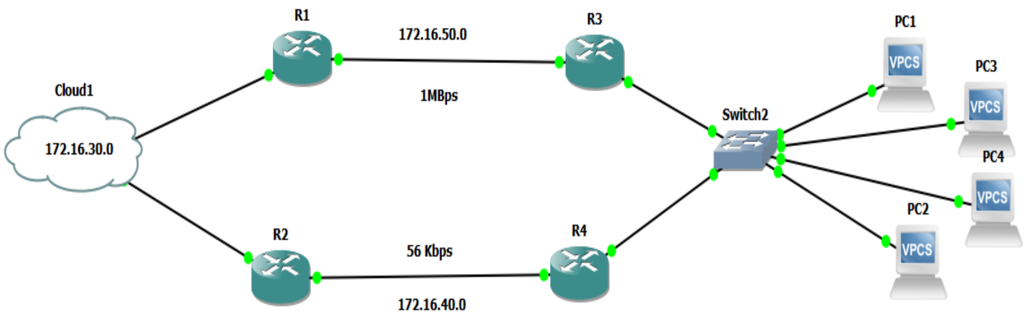


Fig. 2. Ripv2 load balancing

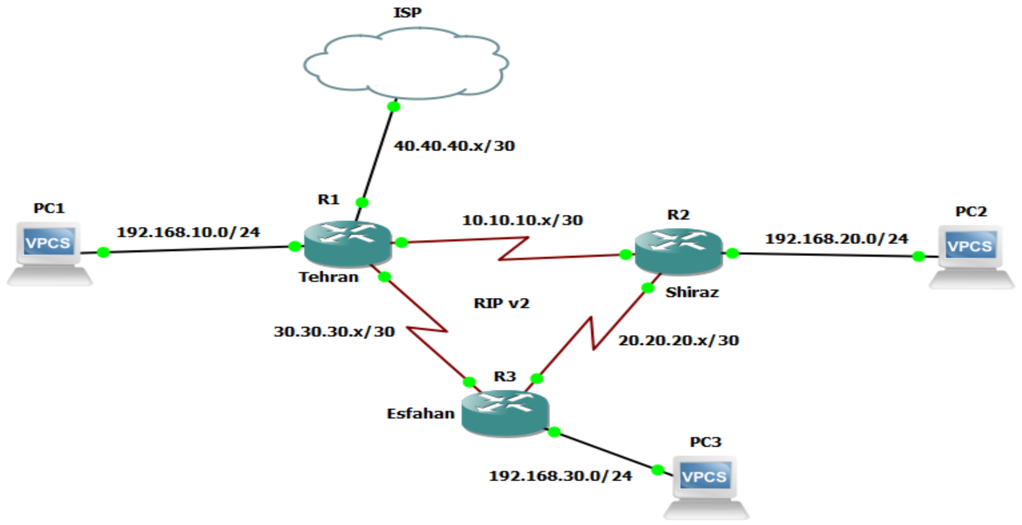


Fig. 3. Ripv2 application scenario

Disadvantages of version 2 of the RIP protocol are:

- The maximum number of hops it supports is 15 and counting to infinity is one of the vulnerabilities.
- It has no understanding of the concept of neighborhood. RIP has slow convergence and counts to infinity problems.

4) *Metric Calculation in RIPv2*

The RIP protocol always chooses the best route in such a way that there are fewer routers or hops in that route [3]. In Fig. 2 and 3. one of the problems of the RIP protocol is that if we have several paths whose communication links have different speeds and there are the same number of routers in both paths, then the RIP protocol performs load balancing on all paths. It causes the network speed to decrease and efficiency to decrease [1].

```
R1(config) # router rip
R1(config-router) # version 2
R1(config-router) # network 10.10.10.1 255.255.255.252
R1(config-router) # network 30.30.30.1 255.255.255.252
R1(config-router) # network 40.40.40.1 255.255.255.252
R1(config-router) # network 192.168.10.1 255.255.255.0
R1(config-router) # no auto summary
R1(config-router) # ip route 0.0.0.0 0.0.0.0 40.40.40.2
R1(config-router) # ip split-horizon
R1(config-router) # maximum-path 6
R1(config-router) # passive-interface fast Ethernet 0/1
R1(config-router) # default-information originate
R1(config-router) # timers basic 30 90 180 270
```

Comprehending the traits and distinctions among various RIP versions is vital for choosing the right protocol, and ensuring optimal network performance and reliability. RIP suits small, straightforward networks like homes or small offices, while larger and intricate networks benefit from protocols like OSPF and BGP, offering improved scalability, faster convergence, and advanced capabilities [6].

B. OPEN SHORTEST PATH FIRST

Open Shortest Path First (OSPF) is a link-state routing protocol vital for distributing routing insights within computer networks. It shines in larger, intricate networks such as enterprises and service providers. OSPF comes in different versions: OSPFv1, OSPFv2, and OSPFv3. OSPFv1 is outdated, while OSPFv2, tailored for IPv4 networks, is widely used. OSPFv3 is crafted for IPv6 networks. The hierarchical structure of OSPF maximizes network resources and supports scalable expansion. The notion of areas is central, grouping routers and networks logically. In each area, a designated router (DR) and backup designated router (BDR) manage routing information distribution. OSPF employs a "cost" metric based on link bandwidth. Higher bandwidth translates to lower costs inversely. Load balancing is facilitated, distributing traffic across various paths. This protocol offers several benefits compared to alternatives, particularly rapid convergence times. By utilizing a link-state database, OSPF enables routers to swiftly adapt to shifts in the network topology. In essence, OSPF is an essential link-state routing protocol catering to substantial and intricate networks. Its versions cater to IPv4 and IPv6 networks, offering hierarchical structures, efficient resource usage, rapid convergence, and dynamic traffic distribution capabilities [7]-[8].

1) Types of areas in terms of number in OSPF

In the Single-area mode of OSPF, there exists a sole area called the Backbone. Here, any alteration in the network triggers changes across the entire area. In contrast, the multi-area mode features a Backbone area linked to other areas. Changes, such as link or router adjustments, or updates, impact only the specific areas involved, leaving the rest of the network unaffected [2].

2) *Types* of areas by type in OSPF

a) Backbone Area

In Fig. 4. The OSPF protocol establishes a central point known as the Backbone Area (Area 0), serving as the hub to which all other OSPF areas must connect. This pivotal role ensures network cohesion and effective routing organization.

b) Standard Area

Beyond the Backbone Area, Standard Areas encompass a mix of internal and external routes within their databases. These areas contribute to the overall network structure by systematically distributing routing information.

c) Stub Area

In Fig. 5. Designed to streamline routing table efficiency, Stub Areas houses only internal routes alongside a default route. This minimalist approach reduces clutter and enhances network performance.

d) Totally Stubby Area

In Fig. 5. An exclusive feature found on Cisco routers, the Stubby Area is characterized by its database containing solely its internal area routes and a default route. This specialization contributes to optimized routing strategies.

e) Not-So-Stubby Area

In Fig. 5. NSSAs accommodate internal routes, redistributed routes, and a default route. Their unique purpose is to import external routes into OSPF, thereby managing routing table size while enhancing network capabilities.

f) Totally NSSA *Area*

Another Cisco-specific addition, the Totally NSSA Area mirrors the NSSA's role but extends to include both internal and redistributed routes, as well as a default route. This fine-tuned approach is designed to meet specific networking needs.

g) *Backbone Router*

A Backbone Router boasts at least one interface directly connected to the Backbone Area (Area 0), ensuring its crucial role in maintaining the core network structure.

h) *Internal Router*

Defined by its interfaces all belonging to a single OSPF area, an Internal Router contributes to the organization and management of routing within that specific area.

i) *Area Border Router*

Operating at the nexus of different OSPF areas, an ABR facilitates efficient routing by connecting and coordinating information between distinct OSPF domains.

j) *Autonomous System Boundary Router*

The ASBR bridges OSPF networks and external routing protocols like EIGRP or BGP, enabling the exchange of route information and expanding network connectivity [8]-[9].

3) *Metric Calculation in OSPF*

In OSPF, the term "cost" signifies the metric for route evaluation, determined by the outgoing interface's bandwidth. A route's optimal path is defined by the lowest cost, leading OSPF to consistently favor the path with the minimal cost for reaching the destination network.

The calculation of the metric in OSPF is as follows:

$$\text{Cost} = (100\ \text{Mbps}) / \text{Bandwidth} \tag{1}$$

As bandwidth influences the interface's cost, lower values represent superior interface performance and reliability. Hence, smaller numerical values indicate higher-quality interfaces within OSPF routing [10].

```
R2(config)# router ospf 110
R2(config-router) # router-id 2.2.2.2
R2(config-router) # network 10.1.1.5 0.0.0.3 area 0
R2(config-router) # network 10.1.1.1 0.0.0.3 area 0
R2(config-router) # network 10.1.1.18 0.0.0.3 area 1
R2(config-router) # network 12.12.12.1 0.0.0.3 area 4
R2(config-router) # network 2.2.2.2 0.0.0.0 area 0
R2(config-router) # area 4 NSSA default-information
Originate
```

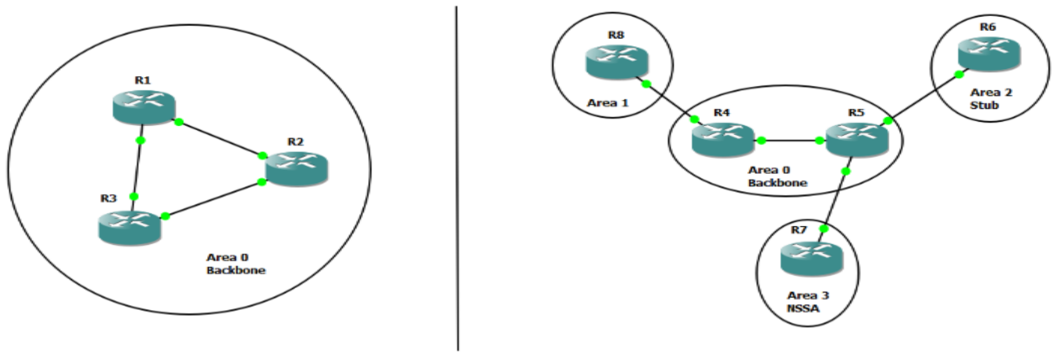


Fig. 4. Types of areas in the type of number

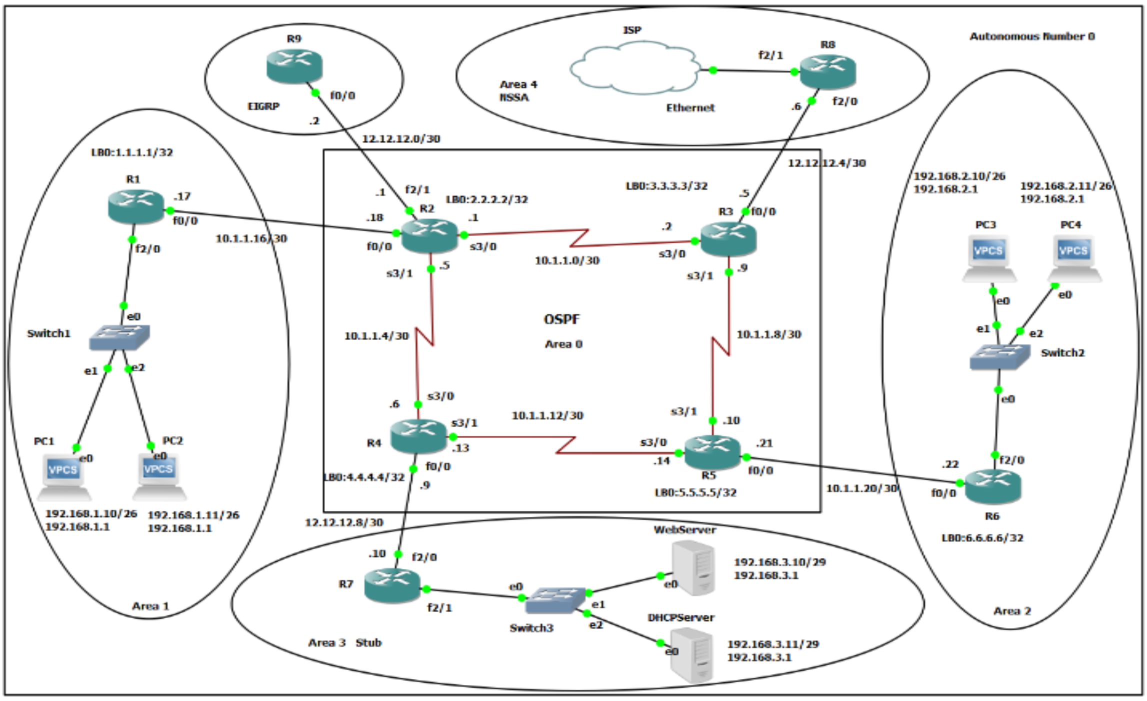


Fig. 5. OSPF scenario in GNS3

OSPF stands as a robust and adaptable routing protocol, notably beneficial for extensive and intricate networks. Familiarity with OSPF's various versions and their attributes is crucial for protocol selection, guaranteeing peak network performance and dependability [6].

C. BORDER GATEWAY PROTOCOL

Border Gateway Protocol (BGP) is a crucial path-vector routing protocol used for routing information exchange across distinct autonomous systems (AS). It takes center stage as the primary routing protocol on the internet, aptly designed to handle the vast multitude of networks and routes inherent to the online realm. BGP spans four versions: BGP-1, BGP-2, BGP-3, and the widely embraced BGP-4, currently the standard bearer. BGP employs intricate regulations to determine optimal paths for data between various ASs. This selection process factors in elements like AS hops, path length, and AS policies, culminating in the identification of the most suitable route for efficient and reliable data transmission. Fig. 6 shows an example of the BGP scenario in GNS3.

1) BGP-1

The inaugural version of BGP emerged in 1989, aiming to facilitate routing information exchange across autonomous systems (AS). However, BGP-1 exhibited limitations such as the absence of support for Classless Inter-Domain Routing (CIDR) and route aggregation, hindering its effectiveness.

2) BGP-2

Introduced in 1991, BGP-2 tackled BGP-1's shortcomings. It embraced CIDR, enabling more efficient IP address space utilization, and introduced route aggregation to streamline routing table sizes.

3)BGP-3

Arriving in 1992, BGP-3 brought the Border Gateway Protocol Identifier (BGP ID) into the fold, serving as a distinctive identifier for BGP speakers. BGP-3 also welcomed support for Multiprotocol Label Switching (MPLS), optimizing traffic routing across expansive networks.

4) BGP-4

As the contemporary standard was introduced in 1994, BGP-4 ushered in significant advancements. It embraced CIDR and route aggregation, bolstering route selection. Notably, BGP-4 introduced Multi-Protocol BGP (MP-BGP), enabling the conveyance of routing information for various protocols, including IPv4, IPv6, and MPLS [11]-[12].

BGP stands as a robust and versatile routing protocol, proving advantageous for expansive networks and service providers. Grasping the nuances of its diverse versions and their attributes holds key significance in protocol selection, ensuring peak network performance and unwavering reliability [13].

D. INTERIOR GATEWAY PROTOCOL

IGRP (Interior Gateway Routing Protocol) is a proprietary routing protocol created by Cisco Systems. Functioning as a distance-vector protocol, it employs a modified Bellman-Ford algorithm to identify optimal routes to destination networks. IGRP is tailored for sizable networks containing multiple routers and is compatible with classful routing.

IGRP, the Interior Gateway Routing Protocol, has three versions: IGRP version 1, IGRP version 2, and IGRP+ (Enhanced IGRP or EIGRP).

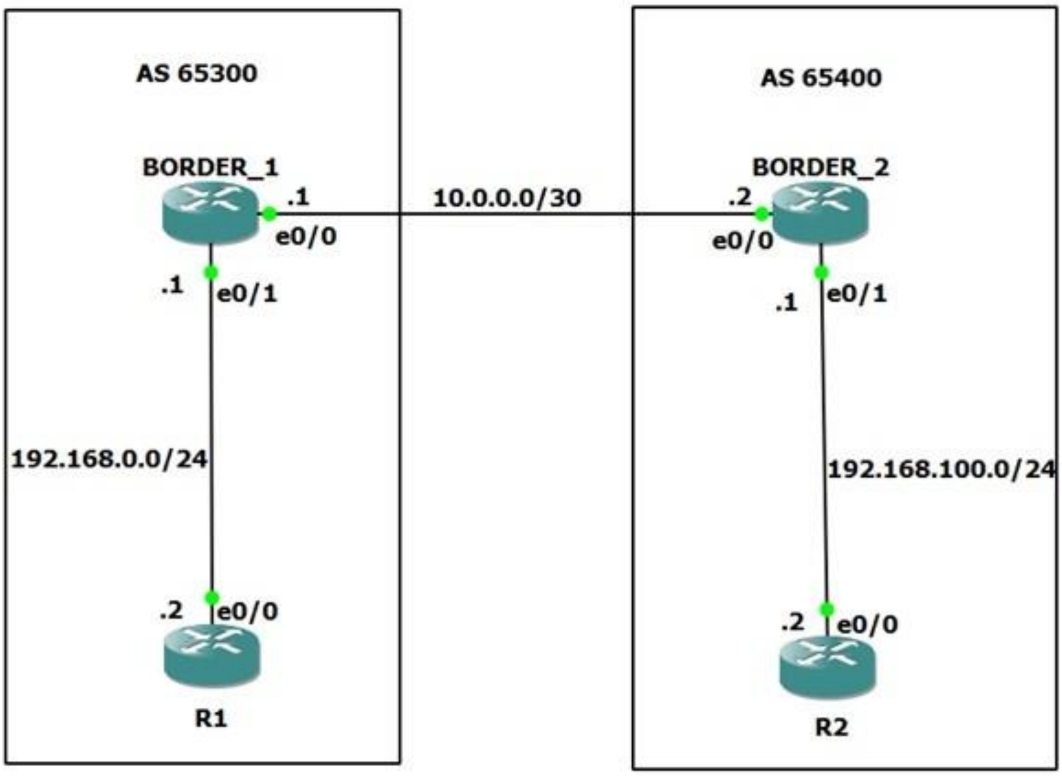


Fig. 6. BGP Scenario in GNS3

1) *IGRP version 1*

It was introduced in the early 1990s. Supports only classful routing, lacking VLSM and CIDR support. Modern networks' needs for IP address conservation are not accommodated.

2) *IGRP version 2*

They were introduced in the mid-1990s to enhance version 1. Embraces VLSMs and CIDR for better IP address utilization. Adds authentication, route summarization, and multicast routing.

3) *IGRP+ (EIGRP)*

Cisco's mid-1990s innovation. Combines distance-vector and link-state routing qualities. Supports VLSMs, CIDR, unequal-cost load balancing, route tagging, and automatic summarization. Efficiency is improved through bandwidth and delay metrics for optimal path determination. IGRP and its versions play a vital role in efficiently directing traffic within expansive networks. They prioritize scalability, durability, and ease of setup. These protocols are extensively utilized in both enterprise and service provider networks. However, the proprietary nature of IGRP restricts its use to Cisco routers, unlike vendor-neutral options like OSPF and BGP. IGRP's initial classful routing constraint diminished its relevance in modern setups. Yet, IGRP version 2 and EIGRP (IGRP+) remain prevalent, particularly EIGRP in enterprise networks for their advanced capabilities and resource optimization. Nevertheless, EIGRP's exclusivity to Cisco routers limits its application. In essence, IGRP and its iterations are crucial for sizeable networks, particularly those employing Cisco routers. IGRP version 1's limitations stem from its sole support for classful routing, while IGRP version 2 and EIGRP (IGRP+) provide more efficiency and scalability through VLSMs, CIDR, and enhanced features [12]-[14].

E. ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL

EIGRP (Enhanced Interior Gateway Routing Protocol) is a proprietary routing protocol from Cisco Systems, merging distance-vector and link-state traits to form a hybrid routing approach. It employs the Diffusing Update Algorithm (DUAL) to determine optimal paths to destination networks. Suited for extensive networks with multiple routers, EIGRP accommodates classless routing.

EIGRP has two versions: EIGRP version 1 and EIGRP version 2. The latter, being the current iteration, offers more advanced capabilities.

1) EIGRP version 1

Introduced in the mid-1990s, it supported solely classful routing, lacking VLSM and CIDR support. It also had a hop count limit of 100, constraining network size.

2) EIGRP version 2

Introduced in the early 2000s, rectified these issues. It embraces VLSMs and CIDR for efficient IP address utilization. Authentication, route summarization, and multicast routing were added. With a hop count limit of 255, it accommodates larger networks. EIGRP is significant for efficiently directing traffic within vast and intricate networks. It is tailored for scalability, speed, and reliability, finding extensive use in enterprise and service provider networks. EIGRP's prominence in enterprises stems from advanced features and resource efficiency. Key to EIGRP is its ability to support unequal-cost load balancing, distributing traffic across paths of varying costs. It also excels in route redundancy and rapid convergence, enhancing reliability compared to other protocols. Automatic summarization is another boon, summarizing multiple subnets into one route advertisement, reducing routing table size, and boosting network efficiency. Key features of EIGRP include simplified configuration, support for various protocols (IP, IPv6, IPX, AppleTalk), scalability across network sizes, compatibility with VLSM and CIDR, swift convergence for quick routing table formation, and the capacity for routing and load balancing on equal and unequal paths. EIGRP employs multicast and unicast messages to

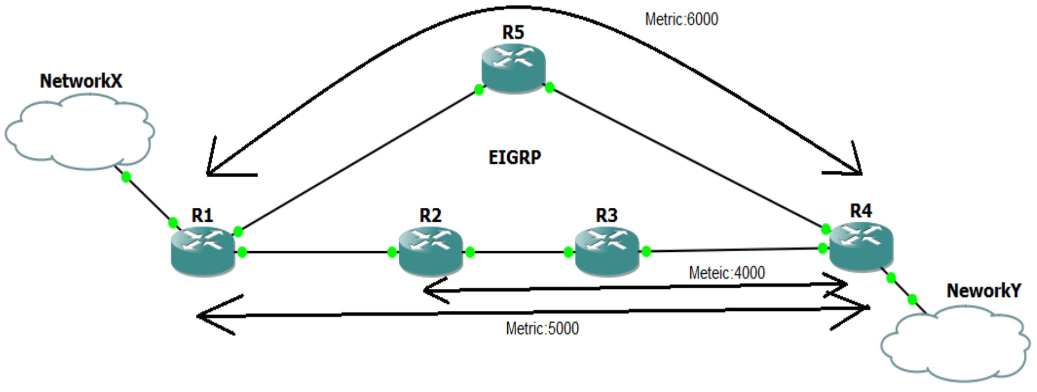


Fig. 7. EIGRP terminology

Table II. EIGRP Metric Parameters

Bandwidth	The bandwidth of the path in kilobits per second (kbps)
Delay	The delay of the path in tens of microseconds (10^-6 seconds)
Reliability	The reliability of the path is expressed as a number from 0 to 255 (255 is 100 percent reliability)
Load	Effective load on the link is expressed as a number from 0 to 255 (255 is 100 percent loading)
MTU	The minimum MTU of the path; usually equals that for the Ethernet interface, which is 1500 bytes

economize bandwidth and forestall network inefficiencies.

3) EIGRP Terminology

a) Successor Route

The path with the lowest metric to a destination. In an illustration (Fig. 7.), the "R1R2R3R4" route is the successor.

b) Successor

The first next-hop router for the successor route. In a scenario (Fig. 7.), "R2" serves as the successor for the "R1R2R3R4" route.

c) Feasible Distance (FD)

Metric for the shortest path to reach a destination. For example, in Fig. 7., the feasible distance is 5000.

d) Reported Distance (RD)

Distance is stated by a router to access a prefix, which equals the feasible distance for that advertising router. For instance, in Fig. 7., "R2" has a calculated metric of 4000.

e) Feasibility Condition

A rule where a backup route must have a reported distance lower than the locally calculated feasible distance to be considered. This condition ensures loop-free paths.

f) Feasible Successor

A backup route that meets the feasibility condition and maintains loop-free status. For example, in Fig. 7., the "R1R5R4" route is a feasible successor [15].

2)Metric Calculation in EIGRP

EIGRP's metric calculation involves several parameters like bandwidth, delay, reliability, load, and MTU of network links. Through a complex formula, EIGRP computes this metric, considering all these factors, to determine the optimal path to a destination. In summary, EIGRP is vital for large networks, especially those using Cisco routers. EIGRP version 2, the current version, boasts advanced attributes including VLSM, CIDR, and unequal-cost load balancing. Its scalability, speed, and reliability make it a favored choice for enterprise and service provider networks[14].

$$\text{metric} = 256*[(10^7/ \text{Min B.W. in (Kbps)}) + (\text{Total sum of delay } (\mu sec/10)] \qquad (2)$$

EIGRP's default metric calculation employs bandwidth and delay factors, each assigned specific weights. Illustrated by Fig. 8. paths between routers A and D, EIGRP determines the primary and secondary routes via its metric formula.

For "ABCD" route

- Lowest bandwidth: 64 kbps
- Sum of delays: 6000 milliseconds

For "AGFED" route

- Lowest bandwidth: 256 kbps
- Sum of delays: 4000 milliseconds

Using these metrics, EIGRP favors the "AGFED" route as primary, considering its lower metric value of 10,204,800 compared to the "ABCD" route's 40,153,600. This decision stems from the lower metric, highlighting the "AGFED" route as the preferred choice[8].

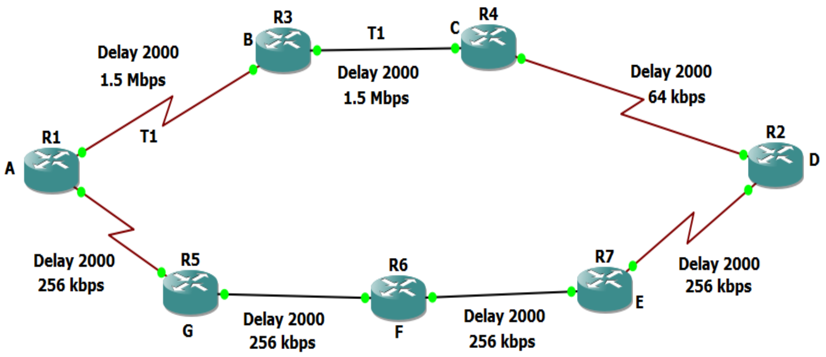


Fig. 8. Selection of primary and secondary path in EIGRP

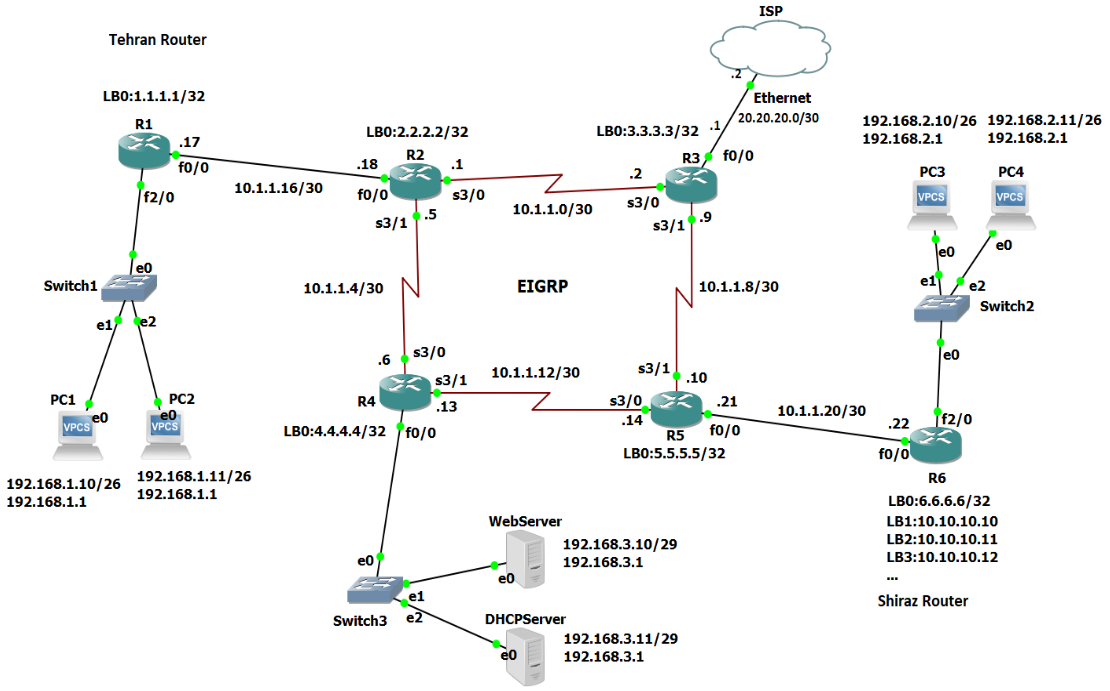


Fig. 9. EIGRP Scenario in GNS3

```
R3(config) # router eigrp 90
R3(config-config) # network 3.3.3.3 0.0.0.0
R3(config-config) # network 10.1.1.2 0.0.0.252
R3(config-config) # network 10.1.1.9 0.0.0.252
R3(config-config) # no auto-summary
R3(config) # ip route 0.0.0.0 0.0.0.0 20.20.20.2
```

For an enhanced scalability of EIGRP, the utilization of a structured hierarchical topology incorporating route summarization is recommended. Fig. 9. shows the EIGRP scenario in GNS3

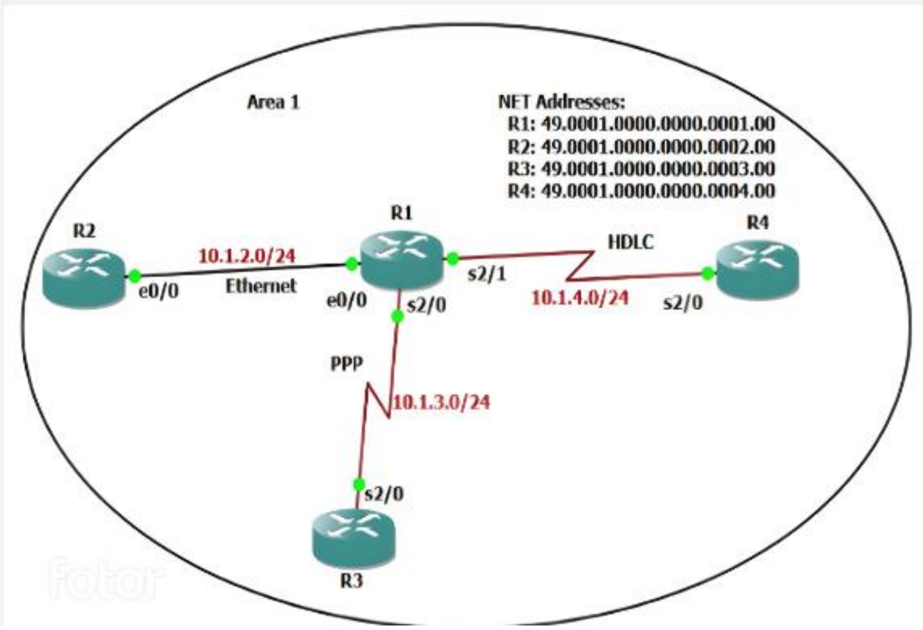

Area 1
NET Addresses:
R1: 49.0001.0000.0000.0001.00
R2: 49.0001.0000.0000.0002.00
R3: 49.0001.0000.0000.0003.00
R4: 49.0001.0000.0000.0004.00
R1
R2
R4
HDLC
10.1.2.0/24
Ethernet
e0/0
e0/0
s2/0
s2/1
10.1.4.0/24
s2/0
PPP
10.1.3.0/24
s2/0
R3
Fotor

Fig. 10. ISIS Scenario in GNS3

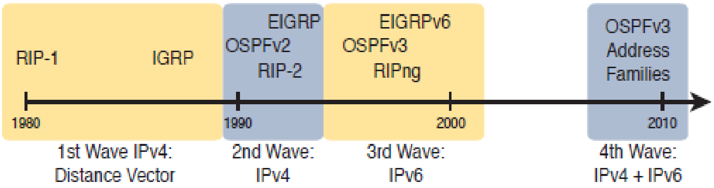


Fig. 11. Evolution of Internet Routing Protocols from 1980 to 2010

F. INTERMEDIATE SYSTEM to INTERMEDIATE SYSTEM

ISIS (Intermediate System to Intermediate System) is a prominent link-state routing protocol extensively employed in sizable networks. It encompasses a multitude of attributes encompassing scalability, security, traffic engineering, QoS, control, and adaptability. Fig. 10 shows the EIGRP scenario in GNS3.

ISIS comes in three versions: ISIS Version 1, ISIS Version 2, and ISIS for IPv6. Each version possesses distinct features and capabilities. Fig. 11. shows the evolution of internet routing protocols.

1) ISIS Version 1

This older iteration solely supports classful routing, lacking route summarization and authentication features. Presently, it sees minimal usage.

2) ISIS Version 2

Widely adopted, Version 2 supports both classful and classless routing, incorporating built-in route summarization and authentication. It also features traffic engineering extensions (TE extensions),

Table III. Comparison of Routing Protocols

Routing Protocol	Scalability	Security	Traffic Engineering	Quality of Service	Control	Flexibility
RIP	Limited	Weak	No	No	Limited	Limited
OSPF	High	Strong	Yes	Yes	High	High
BGP	High	Strong	Yes	Limited	High	Moderate
IGRP	Medium	Moderate	No	No	Moderate	Limited
EIGRP	High	Moderate	Yes	Yes	High	Moderate
ISIS	High	Strong	Yes	Yes	High	High

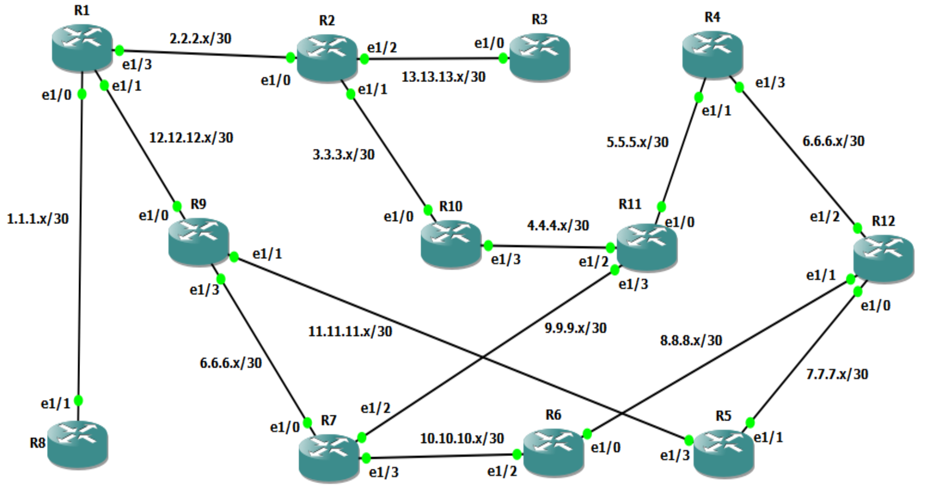


Fig. 12. A large scenario for comparison convergence time in routing protocols

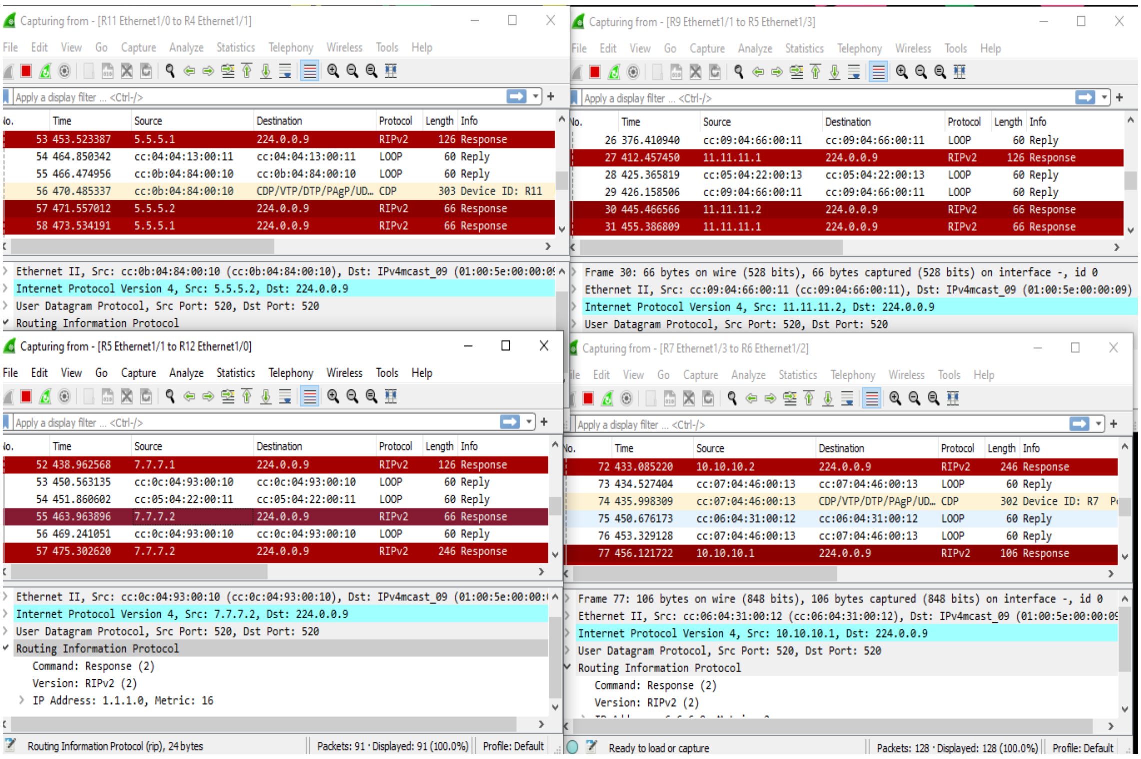
enabling optimized traffic flow through the ability to establish multiple paths between routers, specifying bandwidth and delay for each path.

2) ISIS for IPv6

An extension of Version 2, tailored for IPv6 networks, it offers the same capabilities while accommodating IPv6 addresses. ISIS holds significance due to its array of attributes encompassing scalability, security, traffic engineering, QoS, control, and adaptability. It excels in accommodating extensive networks with multiple routers, utilizing a hierarchical design that simplifies scalability as the network expands. Notably, ISIS grants elevated control over routing updates among routers, leveraging route filters for precise routing table management.

Table IV. Calculation of convergence time by traffic analysis between two routers in the RIPV2 protocol

Router Pair	Convergence Time (seconds)
R4 and R11	18.033625
R5 and R9	33.009116
R5 and R12	25.001338
R6 and R7	26.406418
Average for all pairs	25.61262425


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

Capturing from - [R11 Ethernet1/0 to R4 Ethernet1/1]

```
No.   Time        Source             Destination          Protocol Length Info
   53 453.523387  5.5.5.1            224.0.0.9            RIPv2      126 Response
   54 464.850342  cc:04:04:13:00:11  cc:04:04:13:00:11    LOOP        60 Reply
   55 466.474956  cc:0b:04:84:00:10  cc:0b:04:84:00:10    LOOP        60 Reply
   56 470.485337  cc:0b:04:84:00:10  CDP/VTP/DTP/PAgP/UD… CDP        303 Device ID: R11
   57 471.557012  5.5.5.2            224.0.0.9            RIPv2       66 Response
   58 473.534191  5.5.5.1            224.0.0.9            RIPv2       66 Response

> Ethernet II, Src: cc:0b:04:84:00:10 (cc:0b:04:84:00:10), Dst: IPv4mcast_09 (01:00:5e:00:00:0
> Internet Protocol Version 4, Src: 5.5.5.2, Dst: 224.0.0.9
> User Datagram Protocol, Src Port: 520, Dst Port: 520
v Routing Information Protocol
```

Capturing from - [R9 Ethernet1/1 to R5 Ethernet1/3]

```
No.   Time        Source             Destination          Protocol Length Info
   26 376.410940  cc:09:04:66:00:11  cc:09:04:66:00:11    LOOP        60 Reply
   27 412.457450  11.11.11.1         224.0.0.9            RIPv2      126 Response
   28 425.365819  cc:05:04:22:00:13  cc:05:04:22:00:13    LOOP        60 Reply
   29 426.158506  cc:09:04:66:00:11  cc:09:04:66:00:11    LOOP        60 Reply
   30 445.466566  11.11.11.2         224.0.0.9            RIPv2       66 Response
   31 455.386809  11.11.11.1         224.0.0.9            RIPv2       66 Response

> Frame 30: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface -, id 0
> Ethernet II, Src: cc:09:04:66:00:11 (cc:09:04:66:00:11), Dst: IPv4mcast_09 (01:00:5e:00:00:09)
> Internet Protocol Version 4, Src: 11.11.11.2, Dst: 224.0.0.9
> User Datagram Protocol, Src Port: 520, Dst Port: 520
```

Capturing from - [R5 Ethernet1/1 to R12 Ethernet1/0]

```
No.   Time        Source             Destination          Protocol Length Info
   52 438.962568  7.7.7.1            224.0.0.9            RIPv2      126 Response
   53 450.563135  cc:0c:04:93:00:10  cc:0c:04:93:00:10    LOOP        60 Reply
   54 451.860602  cc:05:04:22:00:11  cc:05:04:22:00:11    LOOP        60 Reply
   55 463.963896  7.7.7.2            224.0.0.9            RIPv2       66 Response
   56 469.241051  cc:0c:04:93:00:10  cc:0c:04:93:00:10    LOOP        60 Reply
   57 475.302620  7.7.7.2            224.0.0.9            RIPv2      246 Response

> Ethernet II, Src: cc:0c:04:93:00:10 (cc:0c:04:93:00:10), Dst: IPv4mcast_09 (01:00:5e:00:00:
> Internet Protocol Version 4, Src: 7.7.7.2, Dst: 224.0.0.9
> User Datagram Protocol, Src Port: 520, Dst Port: 520
v Routing Information Protocol
    Command: Response (2)
    Version: RIPv2 (2)
  > IP Address: 1.1.1.0, Metric: 16

Routing Information Protocol (rip), 24 bytes    Packets: 91 · Displayed: 91 (100.0%)    Profile: Default
```

Capturing from - [R7 Ethernet1/3 to R6 Ethernet1/2]

```
No.   Time        Source             Destination          Protocol Length Info
   72 433.085220  10.10.10.2         224.0.0.9            RIPv2      246 Response
   73 434.527404  cc:07:04:46:00:13  cc:07:04:46:00:13    LOOP        60 Reply
   74 435.998309  cc:07:04:46:00:13  CDP/VTP/DTP/PAgP/UD… CDP        302 Device ID: R7   P
   75 450.676173  cc:06:04:31:00:12  cc:06:04:31:00:12    LOOP        60 Reply
   76 453.329128  cc:07:04:46:00:13  cc:07:04:46:00:13    LOOP        60 Reply
   77 456.121722  10.10.10.1         224.0.0.9            RIPv2      106 Response

> Frame 77: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface -, id 0
> Ethernet II, Src: cc:06:04:31:00:12 (cc:06:04:31:00:12), Dst: IPv4mcast_09 (01:00:5e:00:00:0
> Internet Protocol Version 4, Src: 10.10.10.1, Dst: 224.0.0.9
> User Datagram Protocol, Src Port: 520, Dst Port: 520
v Routing Information Protocol
    Command: Response (2)
    Version: RIPv2 (2)

Ready to load or capture    Packets: 128 · Displayed: 128 (100.0%)    Profile: Default
```

Fig. 13. Analyze RIP Traffic

Security is upheld through authentication via MD5, safeguarding routing updates and thwarting unauthorized access, thus bolstering network security. Furthermore, ISIS exhibits dedicated support for traffic engineering and QoS, enabling effective traffic flow optimization and the prioritization of specific traffic types [3]-[16].

IV. COMPARISON OF ROUTING PROTOCOLS

The goal is to assess the convergence time of RIP v2, EIGRP, and OSPF routing protocols in a specific scenario based on Fig. 12. Initially, RIP v2 is set up on all routers with established connectivity via successful pinging. Subsequently, the Ethernet interface 1/0 on Router R1 is deactivated, and packet exchanges are observed through Wireshark. The convergence time is quantified for Routers R4, R5, R6, R7, R9, R11, and R12, specifically to eliminate the 1.1.1.0 network from their routing tables [16]-[17].

Referring to Fig.13, the RIP routing protocol demonstrated a convergence time of 25.61 seconds, indicating a relatively sluggish pace. This characteristic renders it suitable primarily for compact networks featuring a constrained router count. For larger networks, the elongated convergence time of RIP can present a notable challenge, motivating the adoption of alternative routing protocols such as EIGRP and OSPF [17]-[18].

Based on Fig.14., we can see that the EIGRP routing protocol took only 0.34259025 seconds to converge in the network. This is considered very fast and is suitable for large and scalable advanced networks. EIGRP's fast convergence time is due to its efficient use of bandwidth and its ability to perform incremental updates, which helps to minimize the amount of traffic on the network [19].

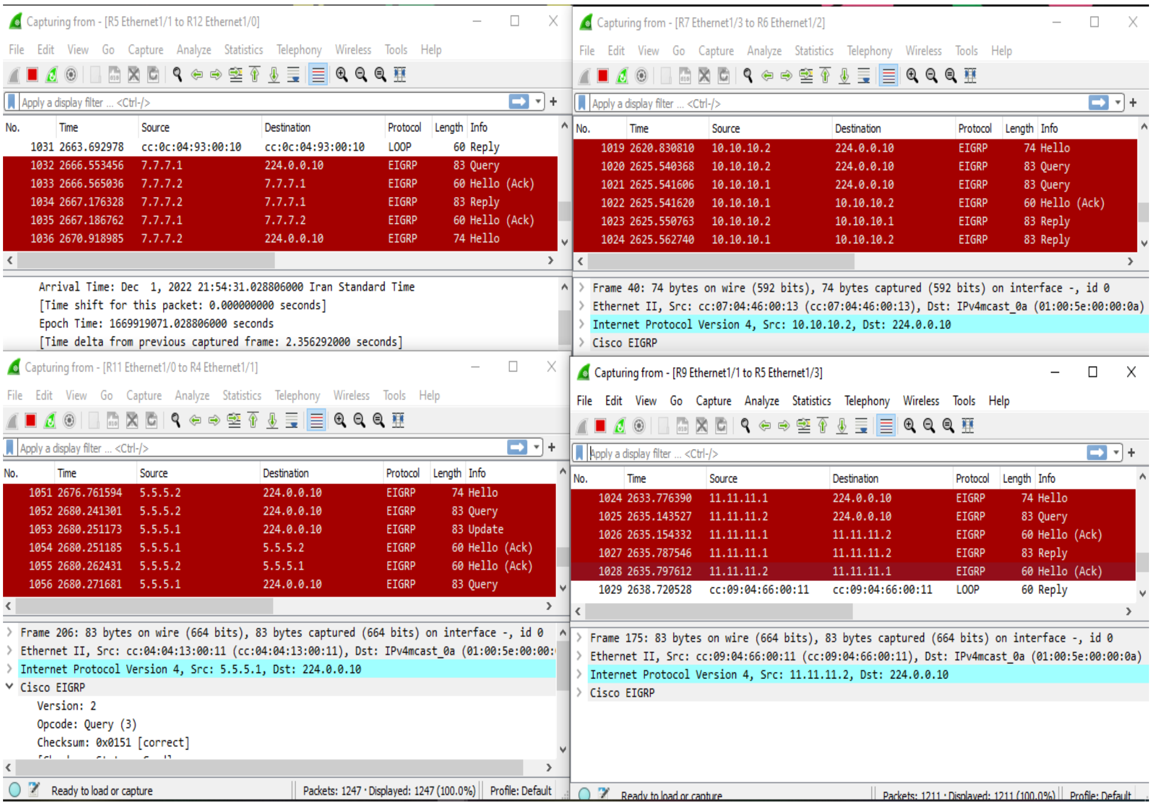
Referring to Fig. 15., OSPF demonstrated a convergence time of 2.39 seconds, showcasing its rapid adaptation to network changes. Unlike RIP, OSPF's efficient link-state routing minimizes convergence time, making it suitable for large, dynamic networks with numerous routers. OSPF's distributed approach enhances scalability and fault tolerance, making it a preferred choice for complex environments.

V. CONCLUSION

The analysis of various routing protocols, including RIP, OSPF, BGP, EIGRP, and ISIS, has revealed distinct strengths and weaknesses for each protocol. OSPF and BGP are highlighted as robust choices for complex networks, while RIP is more suitable for smaller networks with simpler requirements. EIGRP and ISIS, being hybrid protocols, combine the advantages of both distance vector and link-state protocols. This examination emphasizes the significance of carefully evaluating network needs such as size, bandwidth, and security considerations to determine the most appropriate protocol. It also stresses the crucial role of thorough training and familiarity with routing protocols for effective configuration management and support provision by network teams. In certain situations, a combination of routing protocols can offer optimal solutions. For example, utilizing OSPF for internal networks in conjunction with BGP for internet connectivity can lead to efficient outcomes. It is important to note that routing protocols continually evolve to adapt to changing network environments, making it essential for network engineers and administrators to stay updated on advancements in routing technologies. The comparisons underscore that each protocol caters to specific requirements, with OSPF and BGP being suitable for large networks with advanced features

Table V. Calculation of convergence time by traffic analysis between two routers in the EIGRP Protocol

Router Pair	Convergence Time (seconds)
R4 and R11	0.052397
R5 and R9	0.654085
R5 and R12	0.633306
R6 and R7	0.030819
Average	0.34259025


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Ready to load or capture
Profile: Default

```
Capturing from - [R5 Ethernet1/1 to R12 Ethernet1/0]

No.     Time         Source             Destination        Protocol  Length Info
   1031 2663.692978  cc:0c:04:93:00:10  cc:0c:04:93:00:10  LOOP          60 Reply
   1032 2666.553456  7.7.7.1            224.0.0.10         EIGRP         83 Query
   1033 2666.565036  7.7.7.2            7.7.7.1            EIGRP         60 Hello (Ack)
   1034 2667.176328  7.7.7.2            7.7.7.1            EIGRP         83 Reply
   1035 2667.186762  7.7.7.1            7.7.7.2            EIGRP         60 Hello (Ack)
   1036 2670.918985  7.7.7.2            224.0.0.10         EIGRP         74 Hello

    Arrival Time: Dec  1, 2022 21:54:31.028806000 Iran Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1669919071.028806000 seconds
    [Time delta from previous captured frame: 2.356292000 seconds]
```

```
Capturing from - [R7 Ethernet1/3 to R6 Ethernet1/2]

No.     Time         Source             Destination        Protocol  Length Info
   1019 2620.830810  10.10.10.2         224.0.0.10         EIGRP         74 Hello
   1020 2625.540368  10.10.10.2         224.0.0.10         EIGRP         83 Query
   1021 2625.541606  10.10.10.1         224.0.0.10         EIGRP         83 Query
   1022 2625.541620  10.10.10.1         10.10.10.2         EIGRP         60 Hello (Ack)
   1023 2625.550763  10.10.10.2         10.10.10.1         EIGRP         83 Reply
   1024 2625.562740  10.10.10.1         10.10.10.2         EIGRP         83 Reply

> Frame 40: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface -, id 0
> Ethernet II, Src: cc:07:04:46:00:13 (cc:07:04:46:00:13), Dst: IPv4mcast_0a (01:00:5e:00:00:0a)
> Internet Protocol Version 4, Src: 10.10.10.2, Dst: 224.0.0.10
> Cisco EIGRP
```

```
Capturing from - [R11 Ethernet1/0 to R4 Ethernet1/1]

No.     Time         Source             Destination        Protocol  Length Info
   1051 2676.761594  5.5.5.2            224.0.0.10         EIGRP         74 Hello
   1052 2680.241301  5.5.5.2            224.0.0.10         EIGRP         83 Query
   1053 2680.251173  5.5.5.1            224.0.0.10         EIGRP         83 Update
   1054 2680.251185  5.5.5.1            5.5.5.2            EIGRP         60 Hello (Ack)
   1055 2680.262431  5.5.5.2            5.5.5.1            EIGRP         60 Hello (Ack)
   1056 2680.271681  5.5.5.1            224.0.0.10         EIGRP         83 Query

> Frame 206: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface -, id 0
> Ethernet II, Src: cc:04:04:13:00:11 (cc:04:04:13:00:11), Dst: IPv4mcast_0a (01:00:5e:00:00:
> Internet Protocol Version 4, Src: 5.5.5.1, Dst: 224.0.0.10
v Cisco EIGRP
    Version: 2
    Opcode: Query (3)
    Checksum: 0x0151 [correct]

Ready to load or capture    Packets: 1247 · Displayed: 1247 (100.0%)    Profile: Default
```

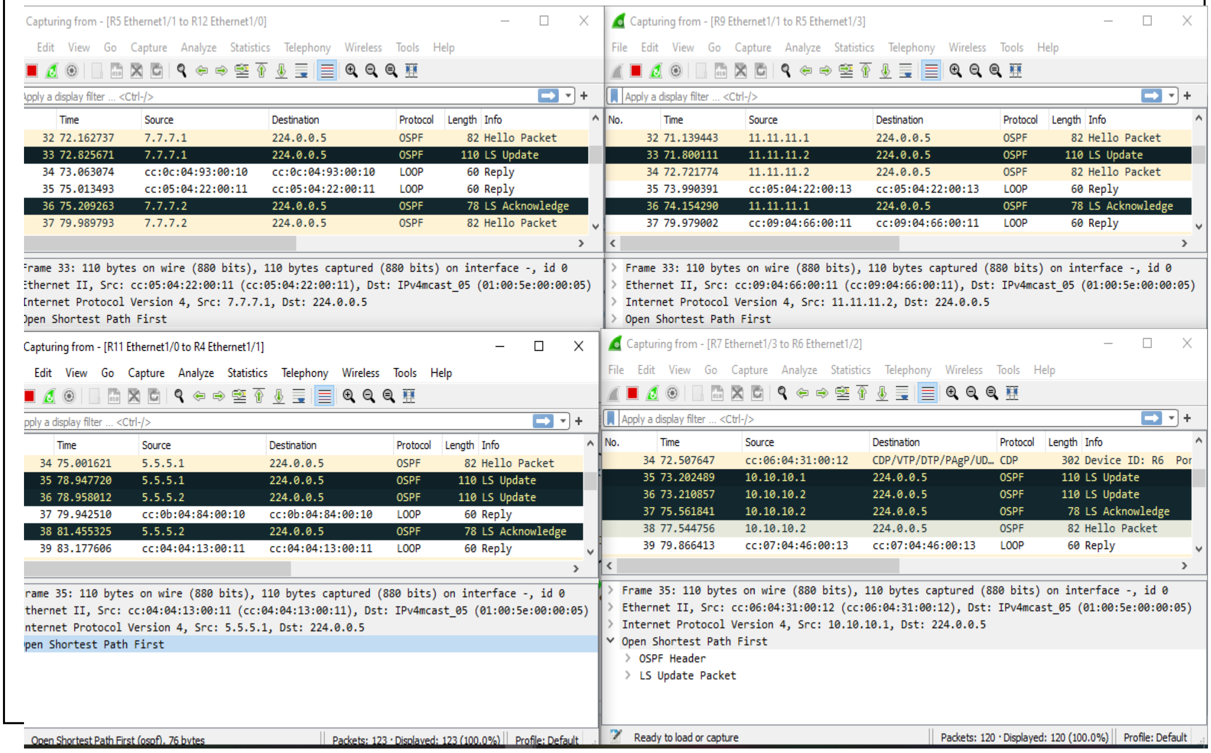
```
Capturing from - [R9 Ethernet1/1 to R5 Ethernet1/3]

No.     Time         Source             Destination        Protocol  Length Info
   1024 2633.776390  11.11.11.1         224.0.0.10         EIGRP         74 Hello
   1025 2635.143527  11.11.11.2         224.0.0.10         EIGRP         83 Query
   1026 2635.154332  11.11.11.1         11.11.11.2         EIGRP         60 Hello (Ack)
   1027 2635.787546  11.11.11.1         11.11.11.2         EIGRP         83 Reply
   1028 2635.797612  11.11.11.2         11.11.11.1         EIGRP         60 Hello (Ack)
   1029 2638.720528  cc:09:04:66:00:11  cc:09:04:66:00:11  LOOP          60 Reply

> Frame 175: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface -, id 0
> Ethernet II, Src: cc:09:04:66:00:11 (cc:09:04:66:00:11), Dst: IPv4mcast_0a (01:00:5e:00:00:0a)
> Internet Protocol Version 4, Src: 11.11.11.2, Dst: 224.0.0.10
> Cisco EIGRP

Ready to load or capture    Packets: 1211 · Displayed: 1211 (100.0%)    Profile: Default
```

Fig. 14. Analyze EIGRP Traffic

like load balancing and hierarchical topology, contrasting with RIP v2's effectiveness in smaller networks with basic needs.

Table VI. Calculation of convergence time by traffic analysis between two routers in the OSPF Protocol

Router Pair	Convergence Time (seconds)
R4 and R11	2.507605
R5 and R9	2.354179
R5 and R12	2.383592
R6 and R7	2.354179
Average	2.39988875



```
Capturing from - [R5 Ethernet1/1 to R12 Ethernet1/0]

    Time          Source              Destination         Protocol  Length Info
 32 72.162737     7.7.7.1             224.0.0.5           OSPF          82 Hello Packet
 33 72.825671     7.7.7.1             224.0.0.5           OSPF         110 LS Update
 34 73.063074     cc:0c:04:93:00:10   cc:0c:04:93:00:10   LOOP          60 Reply
 35 75.013493     cc:05:04:22:00:11   cc:05:04:22:00:11   LOOP          60 Reply
 36 75.209263     7.7.7.2             224.0.0.5           OSPF          78 LS Acknowledge
 37 79.989793     7.7.7.2             224.0.0.5           OSPF          82 Hello Packet

rame 33: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface -, id 0
thernet II, Src: cc:05:04:22:00:11 (cc:05:04:22:00:11), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
nternet Protocol Version 4, Src: 7.7.7.1, Dst: 224.0.0.5
pen Shortest Path First
```

```
Capturing from - [R9 Ethernet1/1 to R5 Ethernet1/3]

No.     Time          Source              Destination         Protocol  Length Info
     32 71.139443     11.11.11.1          224.0.0.5           OSPF          82 Hello Packet
     33 71.800111     11.11.11.2          224.0.0.5           OSPF         110 LS Update
     34 72.721774     11.11.11.2          224.0.0.5           OSPF          82 Hello Packet
     35 73.990391     cc:05:04:22:00:13   cc:05:04:22:00:13   LOOP          60 Reply
     36 74.154290     11.11.11.1          224.0.0.5           OSPF          78 LS Acknowledge
     37 79.979002     cc:09:04:66:00:11   cc:09:04:66:00:11   LOOP          60 Reply

> Frame 33: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface -, id 0
> Ethernet II, Src: cc:09:04:66:00:11 (cc:09:04:66:00:11), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
> Internet Protocol Version 4, Src: 11.11.11.2, Dst: 224.0.0.5
> Open Shortest Path First
```

```
Capturing from - [R11 Ethernet1/0 to R4 Ethernet1/1]

    Time          Source              Destination         Protocol  Length Info
 34 75.001621     5.5.5.1             224.0.0.5           OSPF          82 Hello Packet
 35 78.947720     5.5.5.1             224.0.0.5           OSPF         110 LS Update
 36 78.958012     5.5.5.2             224.0.0.5           OSPF         110 LS Update
 37 79.942510     cc:0b:04:84:00:10   cc:0b:04:84:00:10   LOOP          60 Reply
 38 81.455325     5.5.5.2             224.0.0.5           OSPF          78 LS Acknowledge
 39 83.177606     cc:04:04:13:00:11   cc:04:04:13:00:11   LOOP          60 Reply

rame 35: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface -, id 0
thernet II, Src: cc:04:04:13:00:11 (cc:04:04:13:00:11), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
nternet Protocol Version 4, Src: 5.5.5.1, Dst: 224.0.0.5
pen Shortest Path First

Open Shortest Path First (ospf), 76 bytes    Packets: 123 · Displayed: 123 (100.0%)    Profile: Default
```

```
Capturing from - [R7 Ethernet1/3 to R6 Ethernet1/2]

No.     Time          Source              Destination            Protocol  Length Info
     34 72.507647     cc:06:04:31:00:12   CDP/VTP/DTP/PAgP/UD…   CDP          302 Device ID: R6   Por
     35 73.202489     10.10.10.1          224.0.0.5              OSPF         110 LS Update
     36 73.210857     10.10.10.2          224.0.0.5              OSPF         110 LS Update
     37 75.561841     10.10.10.2          224.0.0.5              OSPF          78 LS Acknowledge
     38 77.544756     10.10.10.2          224.0.0.5              OSPF          82 Hello Packet
     39 79.866413     cc:07:04:46:00:13   cc:07:04:46:00:13      LOOP          60 Reply

> Frame 35: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface -, id 0
> Ethernet II, Src: cc:06:04:31:00:12 (cc:06:04:31:00:12), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
> Internet Protocol Version 4, Src: 10.10.10.1, Dst: 224.0.0.5
v Open Shortest Path First
    > OSPF Header
    > LS Update Packet

Ready to load or capture    Packets: 120 · Displayed: 120 (100.0%)    Profile: Default
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

Table VII. Comparison of all protocols

Criteria	RIP	OSPF	BGP	IGRP	EIGRP	ISIS
Type	Distance vector	Link state	Path vector	Distance vector	Hybrid	Link state
Default Metric	Number of hops	Cost	Multiple attributes	Bandwidth and delay	Bandwidth and delay	Cost
Administrative Distance	120	110	Internal: 200 External: 20	Internal: 90 External: 170	Internal: 90 External: 170	Internal: 115 External: 120
Hop Limit	15	Unlimited	Internal neighbor: 1 External neighbor: Unlimited	224	224	Unlimited
Convergence Speed	Slow	Fast	Slow	Medium	Fast	Fast
Update Timer	30 seconds	Varies based on changes	Varies based on changes	Only when changes occur	Only when changes occur	Only when changes occur
Update Type	Full table	Partial updates	Partial updates	Partial updates	Partial updates	Partial updates
Classless	Yes	Yes	Yes	Yes	Yes	Yes
VLSM	Yes	Yes	Yes	Yes	Yes	Yes
Algorithm	Bellman-Ford	Dijkstra	Best path	Distance vector	Dual	SPF
Update Address	224.0.0.9	224.0.0.5 224.0.0.6	TCP port 179	N/A	N/A	N/A
Protocol and Port Number	N/A	IP protocol 89	TCP port 179	IP protocol 88	IP protocol 88	N/A
Summary	Manual	Manual	Automatic and manual	Automatic and manual	Automatic and manual	Manual
Network Size	Small	Large	Large	Medium	Large	Large
Split Horizon	Yes	Yes	Yes	Yes	Yes	Yes
Load Balancing - Equal-Cost Paths	Yes	Yes	No	Yes	Yes	Yes
Load Balancing - Unequal-Cost Paths	No	No	No	Yes	No	No
Hierarchical Topology	No	Yes	No	No	No	No

References

[1] Academy, N. Routing Protocol Companion Guide. In Routing Protocol Companion Guide (p. 179). Indianapolis: Cisco Press, 2014.

[2] M.H. Pour, Video applied scientific education CCNA 200-125. *In M Hosseingholipour, Video applied scientific education* CCNA 200-125 (pp. 191-197,227-234,287-292). Tehran: Kian Publication, 2018.

D. R. Al-Ani and A. R. Al-Ani, "The Performance of IPv4 and IPv6 in Terms of Routing Protocols using GNS3 Simulator," *in Procedia Computer Science*, vol. 130, doi: 10.1016/j.procs.2018.04.147, 2018. Applications, 2021

[3] Md. H. Kabir, Md. A. Kabir, Md. S. Islam, M.G. Mortuza, and M. Mohiuddin, “Performance analysis of mesh-based enterprise network using RIP, EIGRP, and OSPF routing protocols,” *The 8th International Electronic Conference on Sensors and Applications*, 2021

[4] A. Balchunas, Routing Information Protocol. 1-2,8, 2012

[5] www.gns3.com

[6] C. Wijaya, “Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPv4 and IPv6 Network,” *First International Conference on Informatics and Computational Intelligence,* Bandung, Indonesia, 12-14 Dec. 2011.

[7] G. E. Norvor, M. Asante, F. Xavier, and K. Akotoye, “Routing Behavior of IS-IS and OSPFv3 with Database Query, Remote Login, and FTP in IPv6 Networks,” *Int. J. Inven. Eng. Sci*., no. 3, pp. 2319–9598, 2016.

[8] J. Ghanbari, What is OSPF and how to configure it? Retrieved from tosinso.com: https://cisco.tosinso.com/fa/ articles/30774/OSPF.

[9] I.J. Okonkwo and I.D. Emmanuel, “Comparative study of EIGRP and OSPF protocol based on network convergence,” *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 6, 2020.

[10] Cisco, Enhanced Interior Gateway Routing Protocol [Online]. Available: http:// docwiki.cisco.com/wiki/Enhanced_ Interior_Gateway_Routing_Protocol.

[11] S. U. Masruroh, A. Fiade, and M.F. Iman, “Performance evaluation of routing protocol RIPv2, OSPF, EIGRP with BGP,” *Intern. Conference on innovative and creative information Technology*, pp. 1–7, Nov. 2017.

[12] J. Tiso and E. C. Designing “Cisco Network Service Architectures (ARCH),” *In E. C. John Tiso, Designing Cisco Network Service Architectures (ARCH) (pp*. 204,206,213). Indianapolis: Cisco Press, 2012.

[13] Faradars.com

[14] B. Edgeworth, CCNP and CCIE Enterprise Core ENCOR350-401 Official Cert Guide, p. 194, Cisco Press, 2020.

[15] G. Kanti Dey, Md. M. Ahmed, and K. Ahmmed, “Performance analysis and redistribution among RIPv2, EIGRP & OSPF routing protocol,” *International Conference on Computer & Information Engineering*, ICCIE, Bangladesh, Nov. 2015.

[16] B. Vachon, D. Teare, and R. Graziani, Implementing Cisco IP Routing (ROUTE), 2015. Indianapolis: ciscopress.com.

[17] W. Odom, CCNA Routing and Switching 200-125 Official Cert Gui Library, p. 491. Indianapolis: Cisco Press, 2016.

[18] S. G. Thorenoor, “Dynamic Routing Protocol implementation decision,” *2nd International Conference on Computer and Network Technology,* June 2010, Bangkok, Thailand..