ABU DHABI POLYTECHNIC

INFORMATION SECURITY ENGINEERING TECHNOLOGY

COURSE PROJECT REPORT

COURSE TITLE: SECURE NETWORK DESIGN

NCS - 4003

Research on Various Types of Routing Protocols and Recent Advances

Authors:
Isa A0001123
Abdulla A00011223
Hessa A0009823
Abdulla A00011223
Abdulla A00011223

Instructor:
Dr. Nedal ABABNEH

Abstract

This paper provides a comprehensive analysis of various types of routing protocols, including distance vector, link state, and hybrid protocols. It explores recent advances in these protocols and their impact on modern networking. The study delves into the operational principles of each protocol type, highlighting their strengths and weaknesses. Additionally, the paper examines the scalability, convergence, and efficiency of these protocols in different network scenarios. Practical implementations and simulations using Packet Tracer are conducted to demonstrate the protocols' operational characteristics and performance. Results from these simulations offer insights into the real-world applicability and efficiency of each protocol. The findings contribute to a deeper understanding of how modern routing protocols can be optimized for better network performance.

I. Introduction

Routing protocols are essential for determining the optimal paths for data transmission in computer networks. This research explores the fundamental principles of various routing protocols, such as distance vector, link state, and hybrid protocols, and examines recent advances that have enhanced their efficiency and scalability. The study delves into the operational characteristics and theoretical underpinnings of each protocol type, highlighting their strengths, weaknesses, and suitability for different network environments.

Additionally, this paper investigates the impact of these protocols on modern networking, focusing on factors such as convergence time, scalability, and resource utilization. Practical implementations and simulations using Packet Tracer are conducted to provide a hands-on perspective of the protocols' operational characteristics. These simulations help demonstrate the performance metrics and real-world applicability of each protocol in various scenarios.

The results from these simulations offer valuable insights into the efficiency, reliability, and scalability of the different routing protocols. By analyzing these findings, the paper contributes to a deeper understanding of how to optimize routing protocols for enhanced network performance and adaptability in ever-evolving network infrastructures. The study's conclusions aim to guide future developments and improvements in routing protocol technologies.

II. Related Work

Routing protocols form the backbone of computer networks, enabling efficient data transmission by determining optimal paths between devices. Extensive research has been conducted to analyze various routing protocols, their advancements, and practical implementations. This section provides an overview of related work that has contributed to understanding the operational characteristics, performance metrics, and recent developments in routing protocols.

A. Analysis of Routing Protocols

Early studies by Perkins and Royer (1999) laid the groundwork for comparing distance vector and link state routing protocols. Their research highlighted the simplicity and ease of implementation of distance vector protocols like RIP, contrasting with the superior scalability and faster convergence of link state protocols such as OSPF and IS-IS. This foundational analysis underscored the trade-offs between protocol types based on network size and complexity.

B. Recent Advances in Routing Protocols

Recent research has focused on enhancing the efficiency and scalability of routing protocols. Wang et al. (2020) explored advancements in link state protocols, integrating advanced algorithms to improve scalability and reduce convergence times. Their findings emphasized the critical role of optimization techniques in adapting routing protocols to handle the complexities of modern large-scale networks.

C. Practical Implementations and Simulations

Practical implementations and simulations have been instrumental in evaluating routing protocols in real-world scenarios. Khraisat et al. (2019) utilized simulation tools such as Packet Tracer to assess the performance of RIP, OSPF, and EIGRP. Their studies provided insights into protocol behavior under varying network conditions, highlighting challenges such as scalability limitations and convergence issues.

D. Hybrid Protocols and Integration with SDN

The development of hybrid routing protocols, combining characteristics of distance vector and link state protocols, has been a significant area of exploration. Vigna and Kemmerer (1999) examined EIGRP as a hybrid protocol, showcasing its advantages in terms of rapid convergence and efficient route calculation. Additionally, integration with Software-Defined Networking (SDN) has enabled dynamic and programmable management of routing protocols, as discussed by Hoque et al. (2012). This integration has enhanced network agility and responsiveness to changing traffic patterns and network conditions.

E. Enhanced Security Features

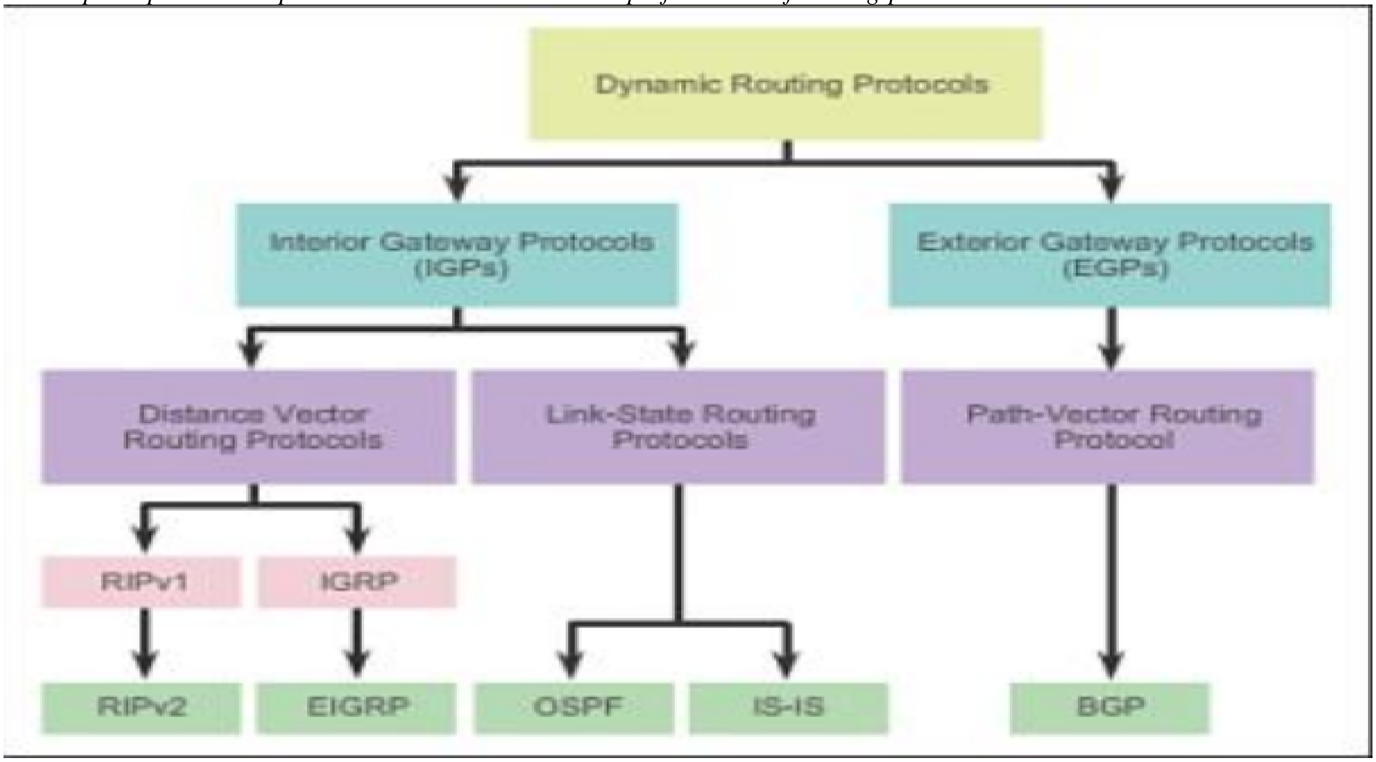
Security enhancements in routing protocols have become increasingly important to mitigate threats such as route hijacking and denial-of-service attacks. Liao et al. (2013) investigated the integration of cryptographic techniques and anomaly detection algorithms in OSPF and BGP. Their research highlighted the effectiveness of these measures in safeguarding routing information integrity and ensuring secure communication across networks.

F. Comprehensive Reviews and Synthesis

Comprehensive reviews by Al-Shaer and Hamdi (2013) synthesized the evolution of routing protocols, covering historical developments, recent advancements, and future research directions. Such reviews have provided holistic perspectives on the evolution and state-of-the-art in routing protocol research, guiding ongoing efforts to improve network efficiency, scalability, and security.

Conclusion

The related work reviewed in this section forms a comprehensive foundation for understanding the landscape of routing protocols. It underscores the diversity of approaches, challenges, and advancements that researchers and network engineers encounter in optimizing protocols for modern network environments. This research builds upon these insights to further explore practical implementations and evaluate the performance of routing protocols in diverse network scenarios.


Dynamic Routing Protocols
Interior Gateway Protocols (IGPs)
Exterior Gateway Protocols (EGPs)
Distance Vector Routing Protocols
Link-State Routing Protocols
Path-Vector Routing Protocol
RIPv1
IGRP
RIPv2
EIGRP
OSPF
IS-IS
BGP

III. Results Analysis

Phase 1: DISTANCE VECTOR PROTOCOLS

Distance vector protocols, like RIP (Routing Information Protocol), periodically exchange their routing tables with neighboring routers to update information about available paths. This iterative process helps routers build and maintain a map of the network topology. The simplicity of distance vector protocols lies in their ease of implementation and understanding, making them suitable for smaller networks or less complex environments.

However, distance vector protocols also have limitations. These include slower convergence times, where it takes longer to update routing information in response to network changes. Moreover, they are susceptible to issues like routing loops, where packets continuously circle between routers without reaching their destination.

To address these limitations, distance vector protocols employ mechanisms such as split horizon, where a router does not advertise routes back to the neighbor from which it learned them, and route poisoning, which marks unreachable routes with infinite metrics to prevent loops. These strategies enhance the stability and efficiency of routing in the network.

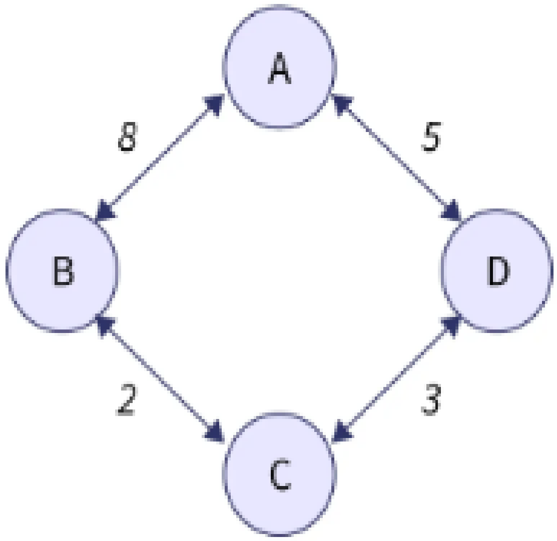
Despite their drawbacks, distance vector protocols have historical significance and are foundational in networking education. They provide a fundamental understanding of routing principles and continue to be used in specific network deployments where their simplicity and operational characteristics are advantageous.*A Distance Vector Routing Protocol is a dynamic method used in packet-switched networks to determine optimal paths for routing data packets between routers. It operates by calculating the shortest path based on distance metrics such as hop count or other metrics like delay and bandwidth. Each router maintains a table known as a distance vector, which contains the distances or metrics to all possible destination nodes within the network.*

Distance vector protocols, like RIP (Routing Information Protocol), periodically exchange their routing tables with neighboring routers to update information about available paths. This iterative process helps routers build and maintain a map of the network topology. The simplicity of distance vector protocols lies in their ease of implementation and understanding, making them suitable for smaller networks or less complex environments.

However, distance vector protocols also have limitations. These include slower convergence times, where it takes longer to update routing information in response to network changes. Moreover, they are susceptible to issues like routing loops, where packets continuously circle between routers without reaching their destination.

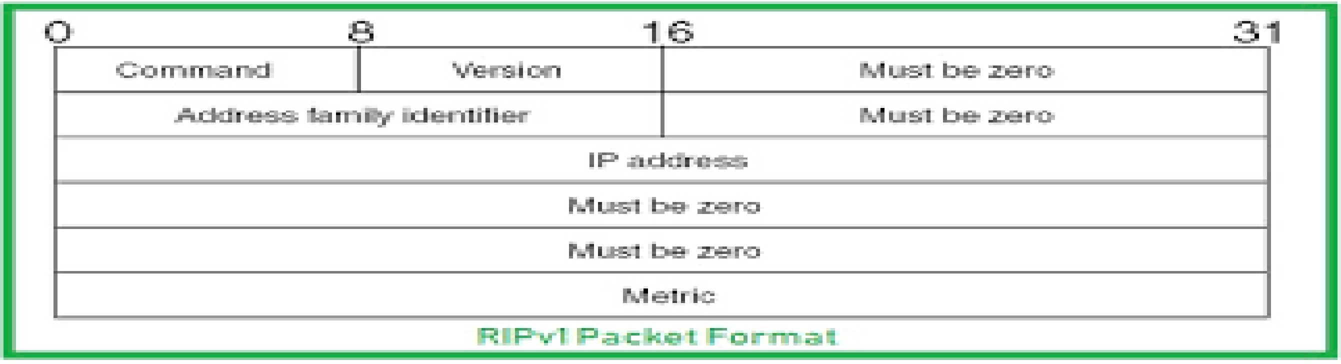
To address these limitations, distance vector protocols employ mechanisms such as split horizon, where a router does not advertise routes back to the neighbor from which it learned them, and route poisoning, which marks unreachable routes with infinite metrics to prevent loops. These strategies enhance the stability and efficiency of routing in the network.

Despite their drawbacks, distance vector protocols have historical significance and are foundational in networking education. They provide a fundamental understanding of routing principles and continue to be used in specific network deployments where their simplicity and operational characteristics are advantageous.



1) ***RIP (Routing Information Protocol):***

Routing Information Protocol (RIP) is one of the oldest and most straightforward interior gateway protocols (IGP) used in computer networking. Initially developed in the 1980s, RIP has undergone several revisions, with the most widely used version being RIP version 2 (RIPv2). This article aims to provide a comprehensive overview of the RIP protocol, its history, operation, and its relevance in modern networking environments.



0 8 16 31

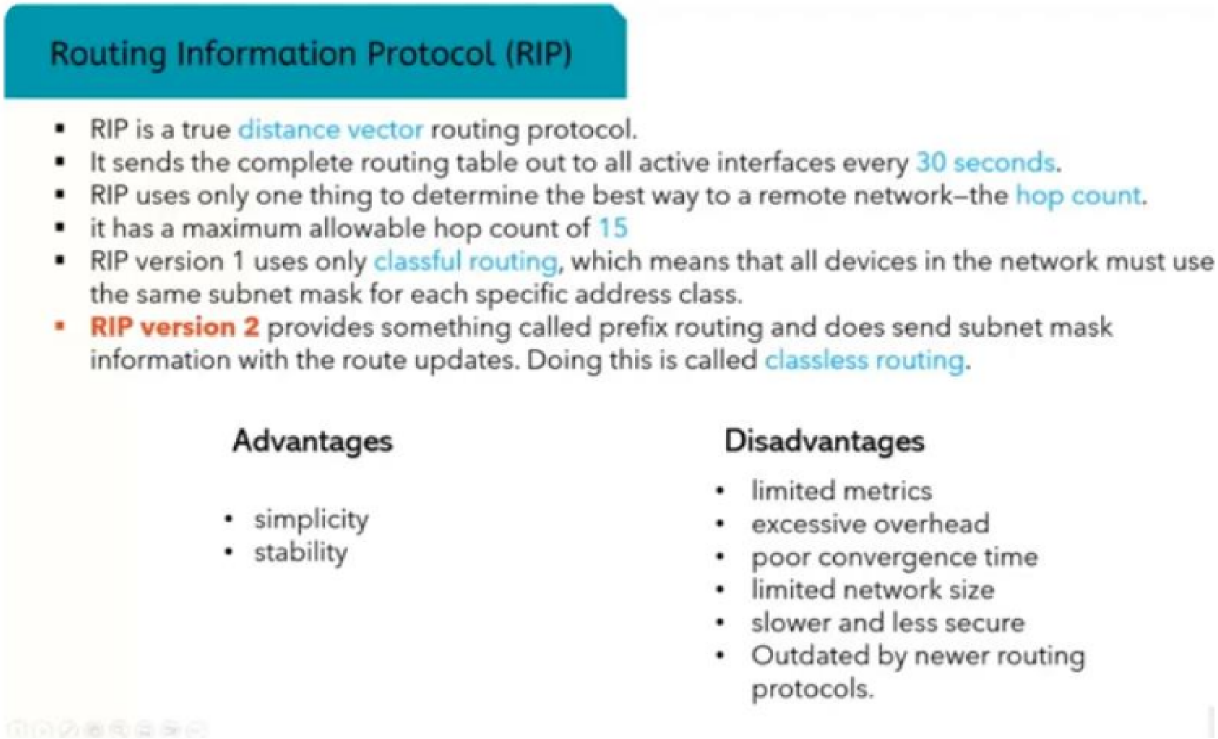
Command	Version	Must be zero
Address family identifier		Must be zero
IP address		
Must be zero		
Must be zero		
Metric		

RIPv1 Packet Format

History of RIP:

RIP was initially developed by Dr. Charles Hedrick and was introduced as part of the Xerox Network Systems (XNS) protocol suite. The protocol was later adapted for use in the Internet Protocol (IP) environment. The original RIP, known as RIP version 1 (RIPv1), had limitations such as a maximum hop count of 15 and the absence of support for subnetting. In response to these limitations, RIP version 2 (RIPv2) was introduced, which addressed these issues and provided additional features.

RIP operates as a distance-vector routing protocol, which means that routers exchange routing information with their neighbors, and each router makes decisions based on the distance (metric) to reach a destination. The metric used by RIP is typically the hop count – the number of routers that must be traversed to reach a particular destination. RIP has two main versions: RIPv1 and RIPv2. RIPv1, the original version, does not support subnet information, leading to inefficient routing in more complex networks. RIPv2, introduced as an enhancement, includes support for subnet masks and uses multicast addresses for routing updates, providing better scalability and security. Despite its limitations, RIP is still used in some small-scale networks and educational environments due to its simplicity and ease of configuration. Understanding RIP provides a foundation for learning more advanced routing protocols.



Routing Information Protocol (RIP)

- RIP is a true distance vector routing protocol.
- It sends the complete routing table out to all active interfaces every 30 seconds.
- RIP uses only one thing to determine the best way to a remote network–the hop count.
- it has a maximum allowable hop count of 15
- RIP version 1 uses only classful routing, which means that all devices in the network must use the same subnet mask for each specific address class.
- **RIP version 2** provides something called prefix routing and does send subnet mask information with the route updates. Doing this is called classless routing.

Advantages

- simplicity
- stability

Disadvantages

- limited metrics
- excessive overhead
- poor convergence time
- limited network size
- slower and less secure
- Outdated by newer routing protocols.

2) ***Interior Gateway Routing Protocol (IGRP):***

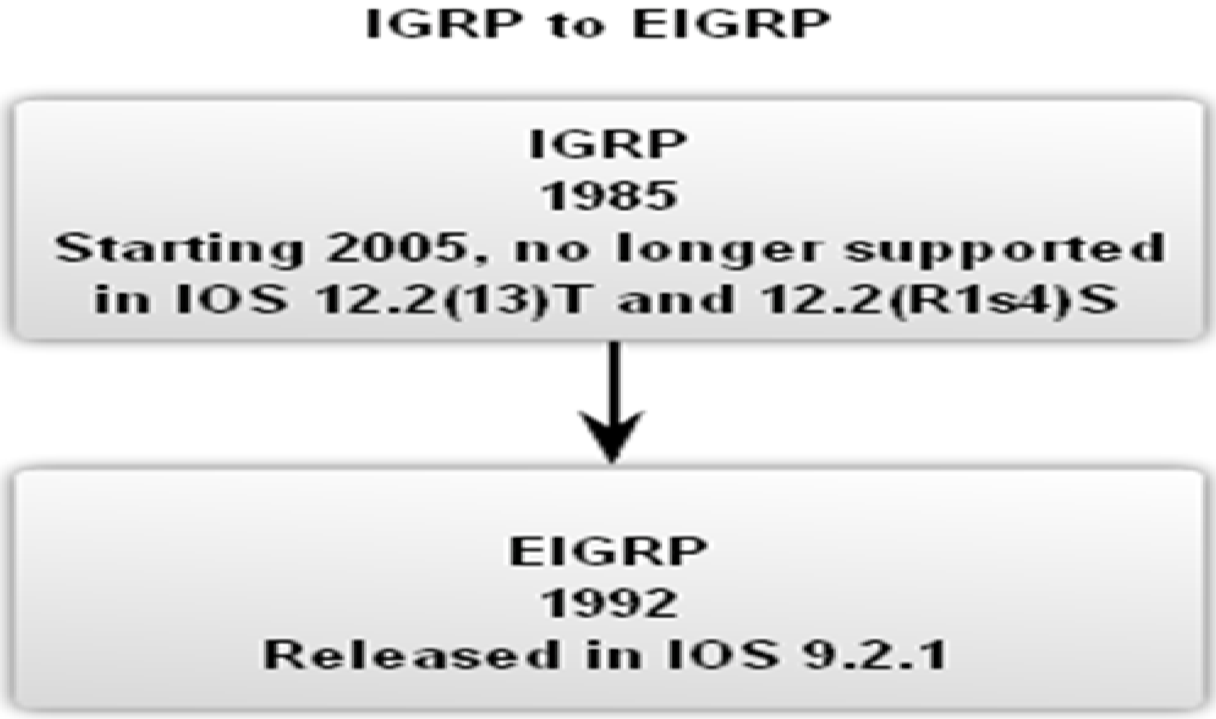
The Interior Gateway Routing Protocol (IGRP) was developed by Cisco Systems in mid 1980s. It is a distance-vector routing protocol and uses the metric called composite metric to calculate the best route between two communication networks. The main purpose of IGRP is to exchange information about networks available within an autonomous *system. It supports up to 255 hops, has unlimited hop count, and can perform load balancing over several paths simultaneously. IGRP also allows for easy scalability from large networks down to small ones or vice versa; this makes it suitable for use in many different applications.*

IGRP routing is known for its support for multiple metrics. This feature allows IGRP to choose the most efficient path for data packets to travel based on a variety of factors, including bandwidth, delay, reliability, and load. Additionally, IGRP supports load balancing, which distributes traffic evenly across the network to prevent congestion and ensure that data packets are delivered quickly and efficiently.

Another key feature of IGRP routing is its ease of configuration and maintenance. IGRP Routing Protocol is an ideal communication protocol for large enterprise networks, especially those with hundreds or thousands of devices. It also supports a high degree of security with its proprietary algorithm that calculates routes and authentication for authorized devices participating in the routing process.

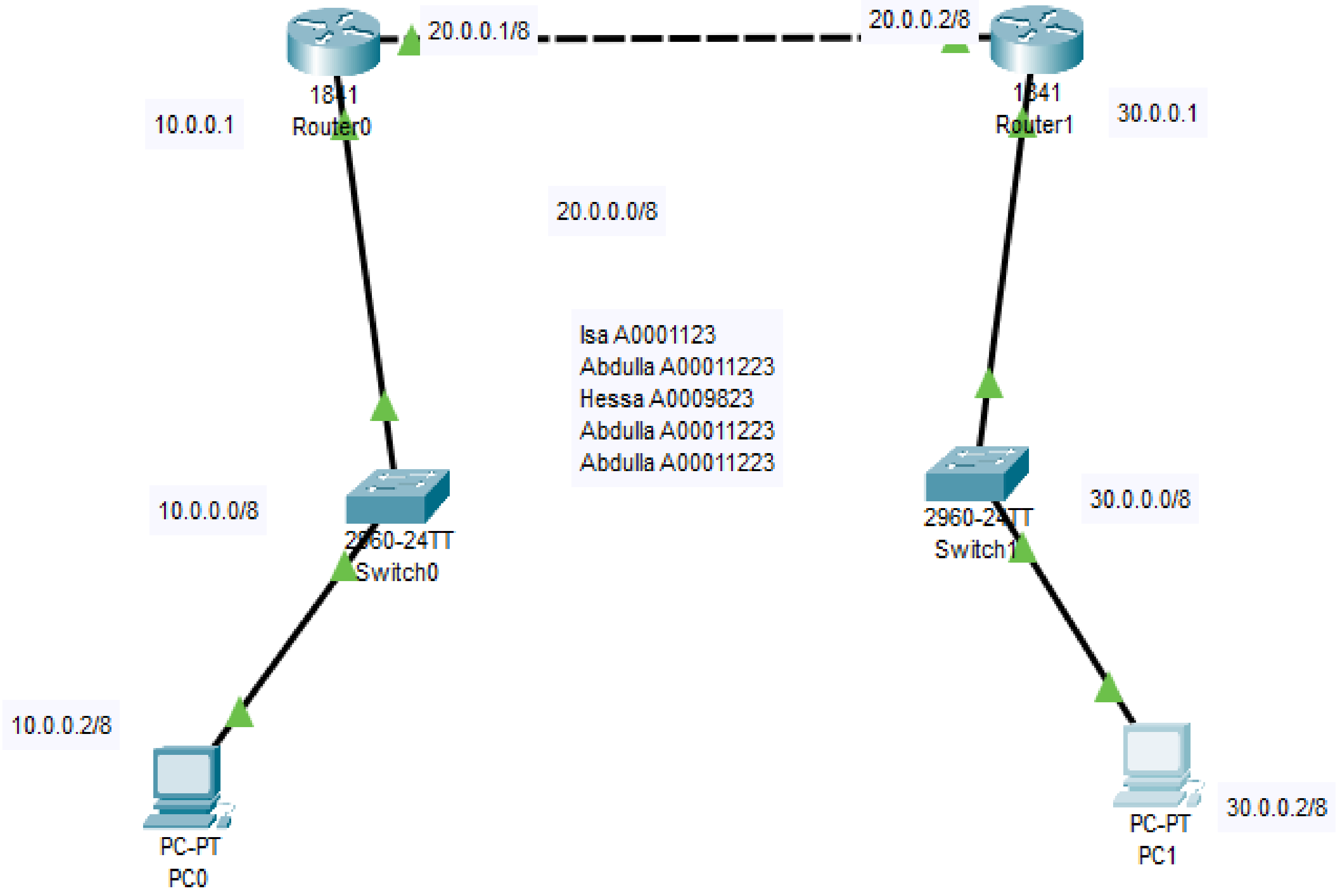
IGRP routing employs a hierarchical design, where routers are organized into domains or areas. Each router maintains a routing table that contains information about the best path to each destination network. The router periodically sends updates to its neighbors to inform them of changes to the routing table.

In addition, IGRP routing uses a composite metric to evaluate the best path for data packets to travel. The composite metric is based on a combination of metrics, including bandwidth, delay, reliability, and load. This ensures that the most efficient path is chosen for data packets to travel. It provides reliable high performance communication, making it a go-to communication protocol for large networks. In addition to its scalability, IGRP can be used in combination with other Cisco technologies such as OSPF and BGP to create a comprehensive communication solution. This combination of IGRP communication with other protocols helps ensure a reliable communication network within large enterprises. IGRP is particularly useful in networks with a high volume of voice and video traffic, as well as real-time data transfer networks, such as financial trading systems and manufacturing plants.

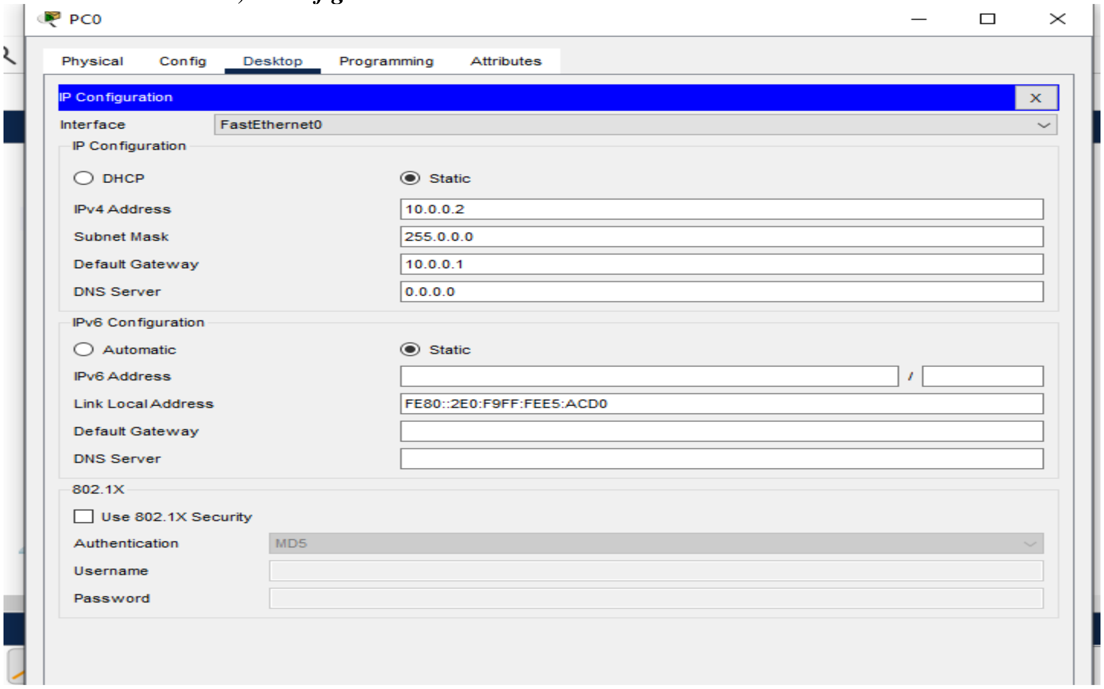

IGRP to EIGRP
IGRP
1985
Starting 2005, no longer supported
in IOS 12.2(13)T and 12.2(R1s4)S
EIGRP
1992
Released in IOS 9.2.1

Packet Tracer Simulation of RIP Protocol :

1) ***Build the network topology.***



2) *Configure IP addresses on the PCs and the routers.*



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address	10.0.0.2
Subnet Mask	255.0.0.0
Default Gateway	10.0.0.1
DNS Server	0.0.0.0

IPv6 Configuration

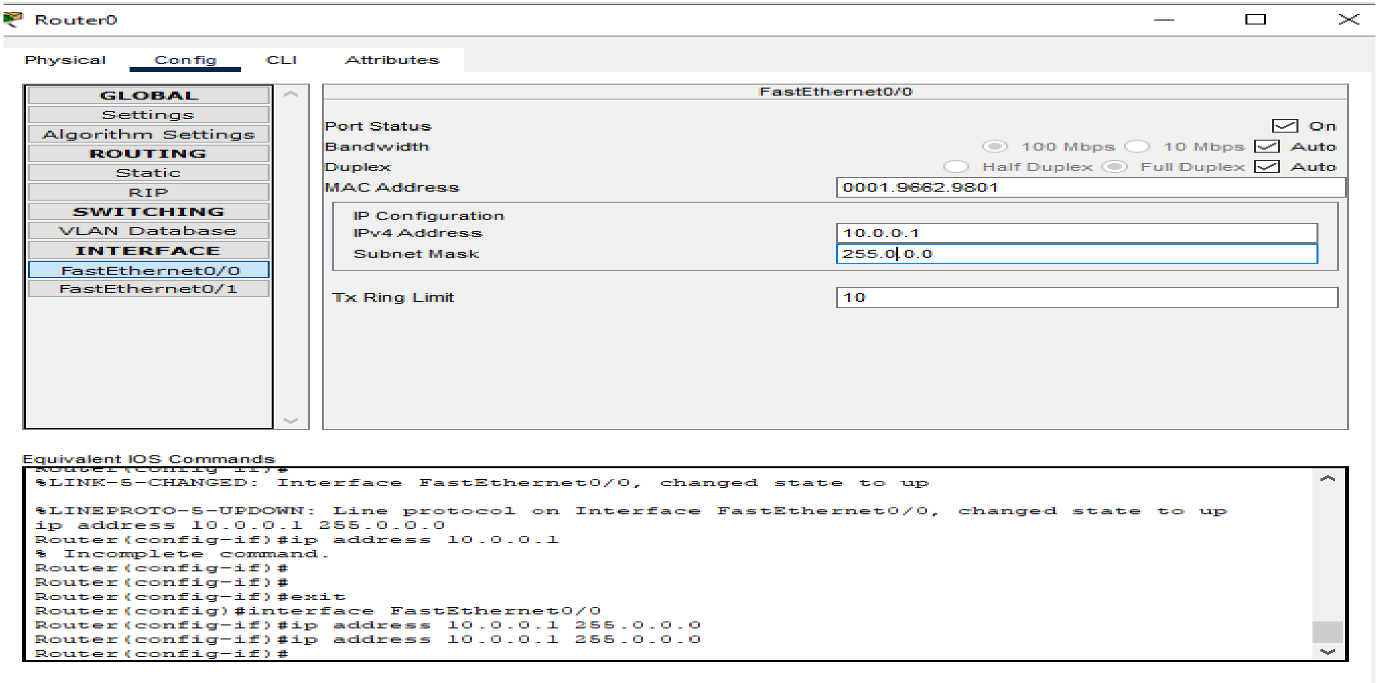
○ Automatic ● Static

IPv6 Address	/
Link Local Address	FE80::2E0:F9FF:FEE5:ACD0
Default Gateway	
DNS Server	

802.1X

□ Use 802.1X Security

Authentication	MD5
Username	
Password	



FastEthernet0/0

Port Status ☑ On
Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ● Full Duplex ☑ Auto
MAC Address 0001.9662.9801

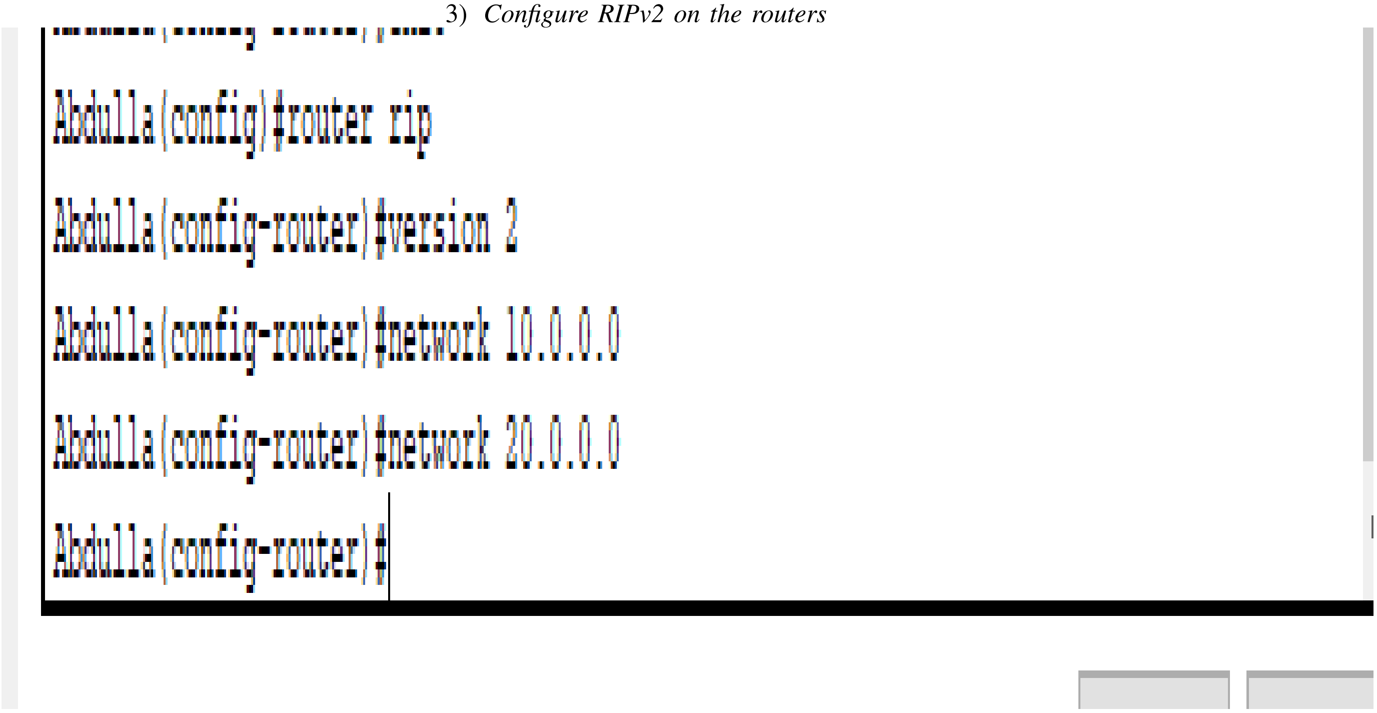
IP Configuration
IPv4 Address 10.0.0.1
Subnet Mask 255.0.0.0

Tx Ring Limit 10

Equivalent IOS Commands

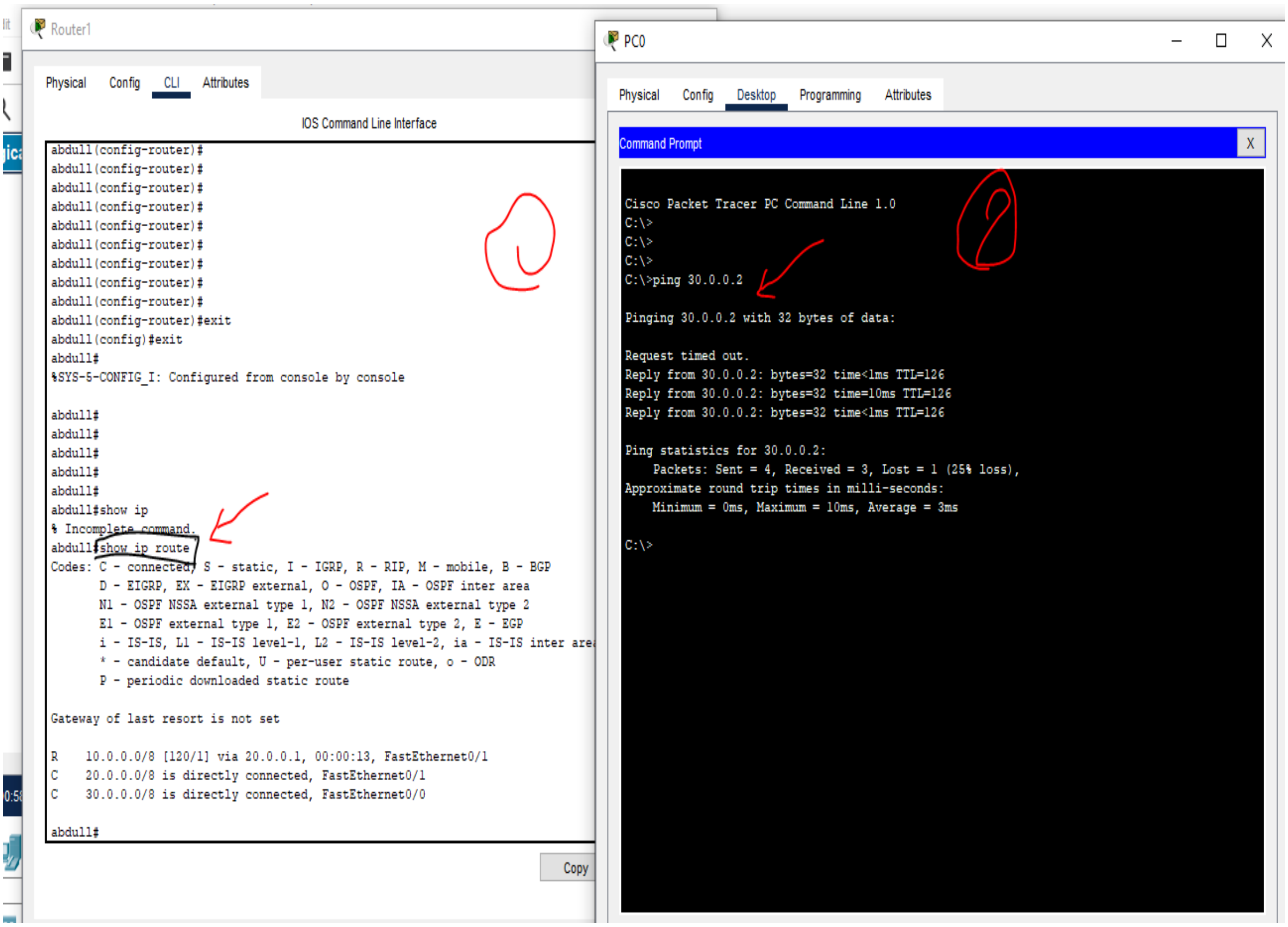
```
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
ip address 10.0.0.1 255.0.0.0
Router(config-if)#ip address 10.0.0.1
% Incomplete command.
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#
```

3) *Configure RIPv2 on the routers*



```
Abdulla(config)#router rip
Abdulla(config-router)#version 2
Abdulla(config-router)#network 10.0.0.0
Abdulla(config-router)#network 20.0.0.0
Abdulla(config-router)#
```

4) ***We'll now verify RIP configuration.*** *By 1)ping from any computers 2)show ip route*


Router1
Physical Config CLI Attributes
IOS Command Line Interface
Copy
1
PC0
Physical Config Desktop Programming Attributes
Command Prompt
X
2

```
abdull(config-router)#
abdull(config-router)#
abdull(config-router)#
abdull(config-router)#
abdull(config-router)#
abdull(config-router)#
abdull(config-router)#
abdull(config-router)#
abdull(config-router)#
abdull(config-router)#exit
abdull(config)#exit
abdull#
%SYS-5-CONFIG_I: Configured from console by console

abdull#
abdull#
abdull#
abdull#
abdull#
abdull#show ip
% Incomplete command.
abdull#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter are
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    10.0.0.0/8 [120/1] via 20.0.0.1, 00:00:13, FastEthernet0/1
C    20.0.0.0/8 is directly connected, FastEthernet0/1
C    30.0.0.0/8 is directly connected, FastEthernet0/0

abdull#
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>
C:\>
C:\>
C:\>ping 30.0.0.2

Pinging 30.0.0.2 with 32 bytes of data:

Request timed out.
Reply from 30.0.0.2: bytes=32 time<1ms TTL=126
Reply from 30.0.0.2: bytes=32 time=10ms TTL=126
Reply from 30.0.0.2: bytes=32 time<1ms TTL=126

Ping statistics for 30.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>
```

Phase 2: LINK STATE PROTOCOLS

Link-state routing protocols are one of the two main classes of routing protocols used in packet switching networks for computer communications, the others being distance-vector routing protocols.Examples of link-state routing protocols include Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS).

The link-state protocol is performed by every switching node in the network (i.e., nodes which are prepared to forward packets; in the Internet, these are called routers). The basic concept of link-state routing is every node constructs a map of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes.Each node then independently calculates the next best logical path from it to every possible destination in the network. Each collection of best paths will then form each node's routing table.

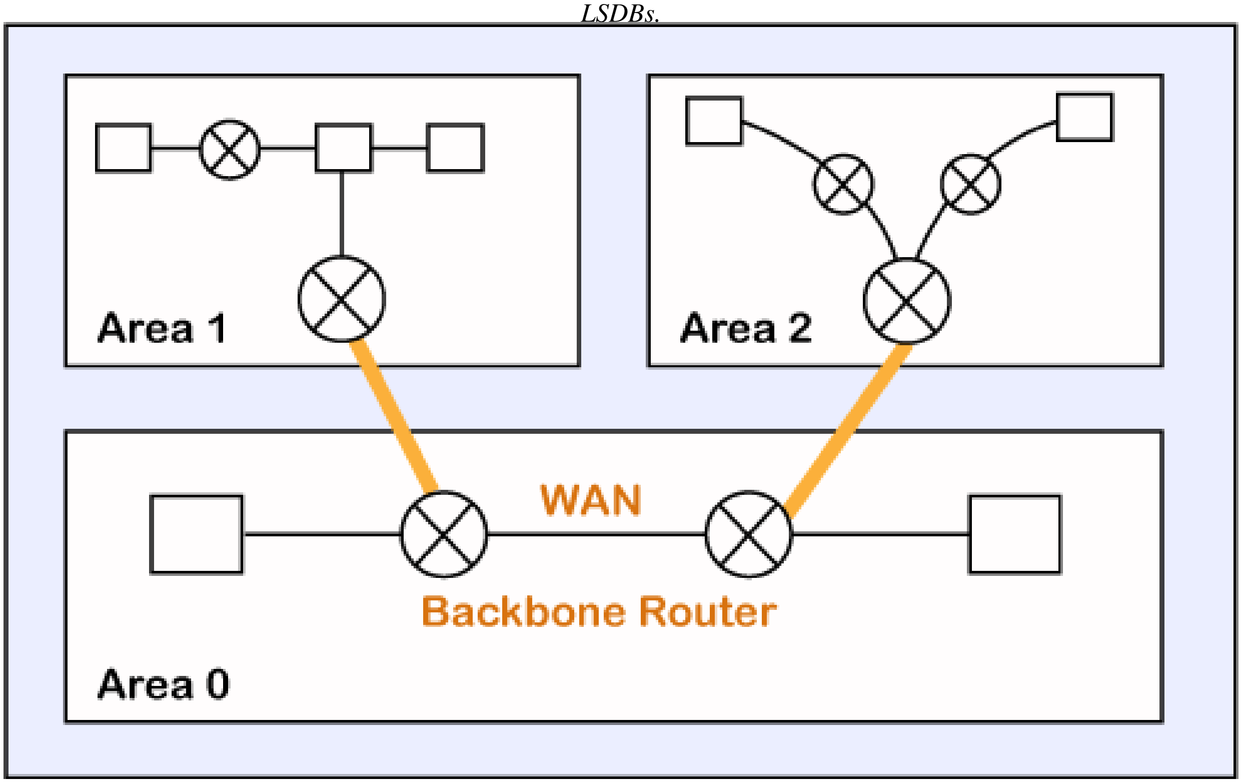
This contrasts with distance-vector routing protocols, which work by having each node share its routing table with its neighbors, in a link-state protocol the only information passed between nodes is connectivity related.[Link-state algorithms are sometimes characterized informally as each router, "telling the world about its neighbors

Link state routing protocols are a different breed and make of routing protocols as they go about the process in a remarkably different way. Much like some complicated but capable distance-vector routing protocols, link state routing protocols use a lot of calculation overhead when devising routing table topology changes and route updates. In this section, we will look at one particular routing protocol, and explain what makes it different from the others we have seen so far.

Two prominent examples of link state protocols are Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS). OSPF, widely used in IP networks, supports hierarchical network design, route summarization, and efficient use of bandwidth. IS-IS, initially developed for use in large carrier networks, also supports similar features and is adaptable to both IP and non-IP networks. Link state protocols, with their sophisticated mechanisms and efficient routing capabilities, are essential in modern network infrastructures, enabling robust and dynamic routing across diverse and expansive networks. Understanding these protocols is crucial for *network professionals aiming to design and manage resilient and scalable networks.*

a) *OSPF (Open Shortest Path First):*

The OSPF stands for Open Shortest Path First. It is a widely used and supported routing protocol. It is an intradomain protocol, which means that it is used within an area or a network. It is an interior gateway protocol that has been designed within a single autonomous system. It is based on a link-state routing algorithm in which each router contains the information of every domain, and based on this information, it determines the shortest path. The goal of routing is to learn routes. The OSPF achieves by learning about every router and subnet within the entire network. Every router contains the same information about the network. The way the router learns this information by sending LSA (Link State Advertisements). These LSAs contain information about every router, subnet, and other networking information. Once the LSAs have been flooded, the OSPF stores the information in a link-state database known as LSDB. The main goal is to have the same information about every router in an LSDBs.



OSPF divides the autonomous systems into areas where the area is a collection of networks, hosts, and routers. Like internet service providers divide the internet into a different autonomous system for easy management and OSPF further divides the autonomous systems into Areas. Routers that exist inside the area flood the area with routing information In Area, the special router also exists. The special routers are those that are present at the border of an area, and these special routers are known as Area Border Routers. This router summarizes the information about an area and shares the information with other areas.

There are three steps that can explain the working of OSPF:

- *The first step is to become OSPF neighbors. The two connecting routers running OSPF on the same link creates a neighbor relationship.*
- *The second step is to exchange database information. After becoming the neighbors, the two routers exchange the LSDB information with each other.*
- *The third step is to choose the best route. Once the LSDB information has been exchanged with each other, the router chooses the best route to be added to a routing table based on the calculation of SPF.*

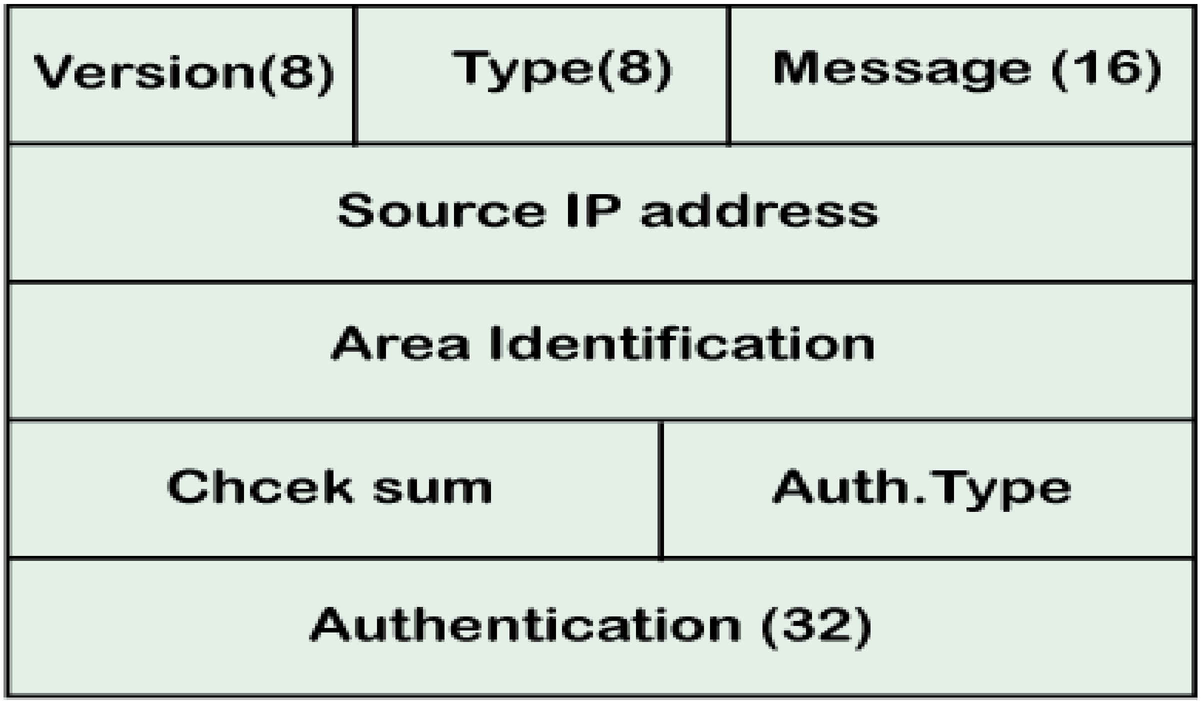
There are four types of links in OSPF:

- *Point-to-point link: The point-to-point link directly connects the two routers without any host or router in between.*
- *Transient link: When several routers are attached in a network, they are known as a transient link. The*

transient link has two different implementations: Unrealistic topology: When all the routers are connected to each other, it is known as an unrealistic topology. Realistic topology: When some designated router exists in a network then it is known as a realistic topology. Here designated router is a router to which all the routers are connected. All the packets sent by the routers will be passed through the designated router.

- *Stub link: It is a network that is connected to the single router. Data enters to the network through the single router and leaves the network through the same router.*
- *Virtual link: If the link between the two routers is broken, the administration creates the virtual path between the routers, and that path could be a long one also.*

OSPF Message Format



<table>
<tr><td colspan="2">Version(8)</td><td colspan="2">Type(8)</td><td colspan="2">Message (16)</td></tr>
<tr><td colspan="6">Source IP address</td></tr>
<tr><td colspan="6">Area Identification</td></tr>
<tr><td colspan="3">Chcek sum</td><td colspan="3">Auth.Type</td></tr>
<tr><td colspan="6">Authentication (32)</td></tr>
</table>

- *Version: It is an 8-bit field that specifies the OSPF protocol version.*
- *Type: It is an 8-bit field. It specifies the type of the OSPF packet.*
- *Message: It is a 16-bit field that defines the total length of the message, including the header. Therefore, the total length is equal to the sum of the length of the message and header.*
- *Source IP address: It defines the address from which the packets are sent. It is a sending routing IP address.*
- *Area identification: It defines the area within which the routing takes place.*
- *Checksum: It is used for error correction and error detection.*
- *Authentication type: There are two types of authentication, i.e., 0 and 1. Here, 0 means for none that specifies no authentication is available and 1 means for pwd that specifies the password-based authentication.*
- *Authentication: It is a 32-bit field that contains the actual value of the authentication data*

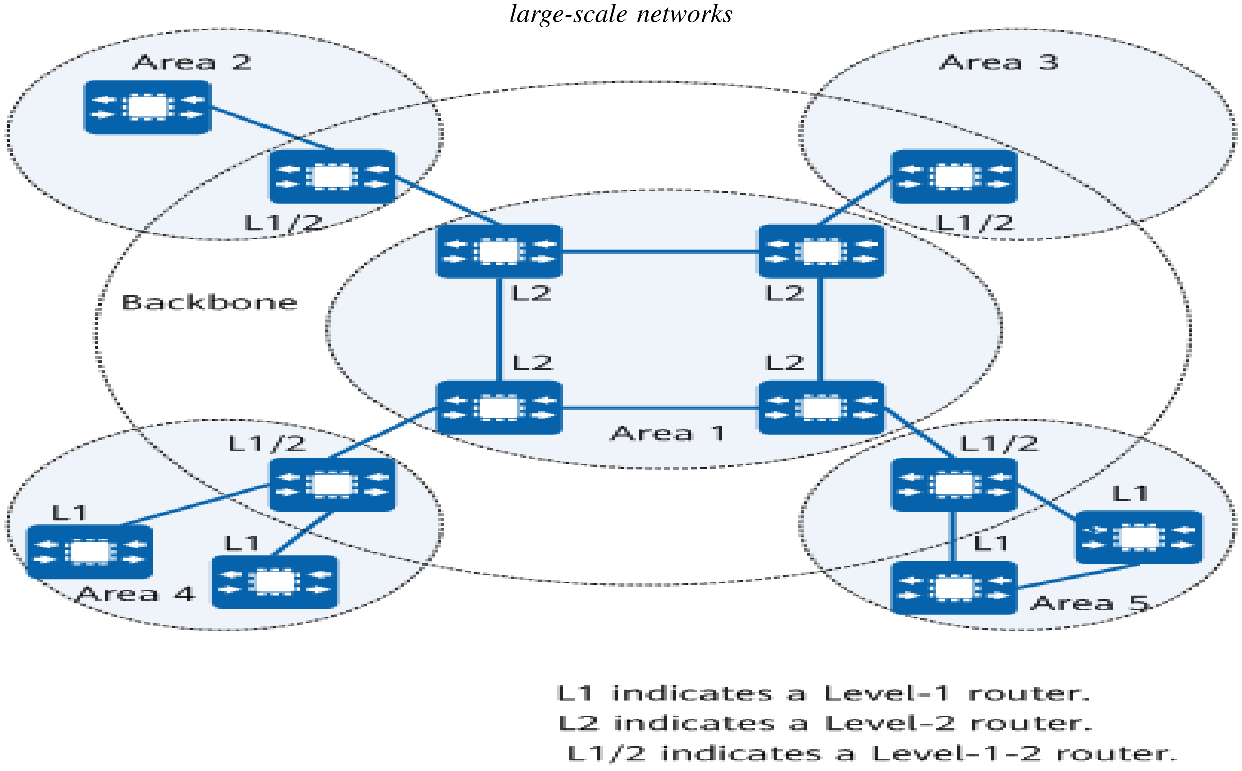
There are five different types of packets in OSPF:

- *Hello packet:The Hello packet is used to create a neighborhood relationship and check the neighbor's reachability. Therefore, the Hello packet is used when the connection between the routers need to be established.*
- *Database Description:After establishing a connection, if the neighbor router is communicating with the system first time, it sends the database information about the network topology to the system so that the system can update or modify accordingly.*
- *Link state request:The link-state request is sent by the router to obtain the information of a specified route. Suppose there are two routers, i.e., router 1 and router 2, and router 1 wants to know the information about the router 2, so router 1 sends the link state request to the router 2. When router 2 receives the link state request, then it sends the link-state information to router 1.*
- *Link state update:The link-state update is used by the router to advertise the state of its links. If any router wants to broadcast the state of its links, it uses the link-state update*

- *Link state acknowledgment:The link-state acknowledgment makes the routing more reliable by forcing each router to send the acknowledgment on each link state update. For example, router A sends the link state update to the router B and router C, then in return, the router B and C sends the link- state acknowledgment to the router A, so that the router A gets to know that both the routers have received the link-state update*

b) ***IS-IS (Intermediate System to Intermediate System):***

IS-IS is a dynamic routing protocol initially designed by the International Organization for Standardization (ISO) for its Connectionless Network Protocol (CLNP). To support IP routing, the Internet Engineering Task Force (IETF) extends and modifies IS-IS in relevant standards, which enables IS-IS to be applied to both TCP/IP and Open System Interconnection (OSI) environments. The new type of IS-IS is called Integrated IS-IS or Dual IS-IS. IS-IS uses the SPF algorithm to calculate routes. It is characterized by fast convergence and high scalability. Running at the data link layer, IS-IS has strong anti-attack capabilities and can implement interworking on large-scale networks


Area 2
Area 3
L1/2
L1/2
Backbone
L2
L2
L2
L2
Area 1
L1/2
L1/2
L1
L1
L1
L1
Area 4
Area 5
L1 indicates a Level-1 router.
L2 indicates a Level-2 router.
L1/2 indicates a Level-1-2 router.

IS-IS adheres to the following Link State characteristics:

- *IS-IS allows for a hierarchical network design using Areas*
- *IS-IS will form neighbor relationships with adjacent routers of the same IS-IS type.*
- *Instead of advertising the distance to connected networks, IS-IS advertises the status of directly connected "links" in the form of Link-State Packets (LSPs). IS-IS will only send out updates when there is a change to one of its links, and will only send the change in the update.*
- *IS-IS uses the Dijkstra Shortest Path First algorithm to determine the shortest path.*
- *IS-IS is a classless protocol, and thus supports VLSMs.*
- *IS-IS was originally developed to route the ISO address space, and thus is not limited to IP routing*
- *IS-IS routes have an administrative distance is 115.*
- *IS-IS uses an arbitrary cost for its metric. IS-IS additionally has three optional metrics: delay, expense, and error. Cisco does not support these optional metrics.*
- *• IS-IS has no hop-count limit.*

The IS-IS process builds and maintains three separate tables:

- *A neighbor table – contains a list of all neighboring routers.*
- *A topology table – contains a list of all possible routes to all known networks within an area.*
- *A routing table – contains the best route for each known network.*

IS-IS Protocols and Addressing

IS-IS consists of three sub-protocols that work in tandem to achieve end-toend routing which ISO defined as Connectionless Network Service (CLNS):

- *CLNP (Connectionless Network Protocol) – serves as the Layer-3 protocol for IS-IS (and was developed by ISO).*

- *ES-IS (End System -to- Intermediate System) – used to route between hosts and routers.*
- *IS-IS (Intermediate System -to- Intermediate System) – used to route between routers.*

IS-IS was originally developed to route ISO CLNP addresses (outlined in RFC 1142). However, CLNP addressing never became prominently used. Thus, IS-IS was modified to additionally support IP routing, and became Integrated (or Dual) IS-IS (outlined in RFC 1195). The IS-IS CLNP address is hexadecimal and of variable length, and can range from 64 to 160 bits in length. The CLNP address contains three "sections," including:

- *Area field – (variable length)*
- *ID field – (from 8 to 64 bits, though usually 48 bits)*
- *Selector (SEL) field - (8 bits)*

IS-IS Packet Types

IS-IS defines two categories of network devices:

- *ES (End System) – identifies an end host.*
- *IS (Intermediate System) – identifies a Layer 3 router.*

IS-IS additionally defines four categories of packet types:

- *Hello packets are exchanged for neighbor discovery. Three types of IS-IS Hello packets exist:*
  - *IIH (IS-IS Hello) – exchanged between routers (or IS's) to form neighbor adjacencies*
  - *ESH (ES Hello) – sent from an ES to discover a router.*
  - *ISH (IS Hello) – sent from an IS to announce its presence to ES's*
- *An LSP (Link State Packet) is used to share topology information between routers. There are separate LSPs for Level 1 and Level 2 routing. LSP's are covered in great detail shortly.*
- *A CSNP (Complete Sequence Number PDU) is an update containing the full link-state database. IS-IS routers will refresh the full database every 15 minutes.*
- *A PSNP (Partial Sequence Number PDU) is used by IS-IS routers to both request and acknowledge a link-state update.*

Phase 3:HYBRID PROTOCOLS

Hybrid protocols combine features from various networking protocols to achieve enhanced performance, reliability, and scalability. These protocols are designed to leverage the strengths of different protocol types, often blending aspects of routing, switching, and communication methodologies. By doing so, hybrid protocols offer flexibility, allowing them to adapt to different network conditions and requirements. They improve performance through faster convergence times in routing and better throughput in transport. Additionally, hybrid protocols provide scalability, efficiently handling network growth in size and complexity. They also incorporate mechanisms for fault tolerance and redundancy, enhancing overall network reliability. In essence, hybrid protocols integrate the best features from different protocols to meet the diverse and evolving demands of modern networking, making them suitable for a wide range of applications, from enterprise networks to secure communications.

How Do Hybrid Routing Protocols Work?

Hybrid routing protocols combine the best features of these two protocols. They use distance-vector routing for small, stable networks, and link-state routing for large, complex networks with changing topologies.As mentioned earlier, Hybrid routing protocols use a combination of distance-vector and link-state routing protocols to provide a more efficient and scalable routing solution, while distance-vector routing protocols, such as Routing Information Protocol (RIP), work by exchanging routing information between neighbors, with each router broadcasting its entire routing table periodically. Link-state routing protocols, such as Open Shortest Path First (OSPF), work by distributing information about the state of links throughout the network, with routers constructing a complete map of the network topology.

Hybrid routing protocols combine the best features of these two protocols. They use distance-vector routing for small, stable networks, and link-state routing for large, complex networks with changing topologies.

advantages Of Hybrid Routing Protocols

- *Scalability: Hybrid routing protocols are highly scalable and can handle networks with thousands of nodes. This is because they use link-state routing to provide a more accurate view of the network topology, and distance-vector routing to reduce the number of updates required.*

- *Faster convergence: Hybrid routing protocols can converge quickly in the event of a network topology change, as they use both distance-vector and link-state routing to update routing tables.*
- *Efficient use of bandwidth: Hybrid routing protocols use distance-vector routing to reduce the amount of bandwidth used for updates. Instead of broadcasting the entire routing table, routers only send updates for changed routes*
- *Load balancing: Hybrid routing protocols can distribute traffic across multiple paths, providing load balancing and increased network performance.*

Disadvantages Of Hybrid Routing Protocols

- *Complexity: Hybrid routing protocols are more complex than either distance-vector or link-state routing protocols alone. This can make them difficult to configure and troubleshoot.*
- *Resource-intensive: Hybrid routing protocols require more memory and processing power than distance-vector or link-state routing protocols alone.*
- *Susceptible to routing loops: Hybrid routing protocols are susceptible to routing loops, which can occur when there are multiple paths between nodes and the routing protocol is not properly configured.*

Summary: *Hybrid routing protocols are an effective solution for larger networks that require scalable and efficient routing. By combining distance-vector and link-state routing, hybrid routing protocols offer faster convergence, efficient use of bandwidth, load balancing, and scalability. However, they are also more complex and resource-intensive than either distance-vector or link-state routing protocols alone. Some examples of hybrid routing protocols include EIGRP and BGP.*

a) ***Border Gateway Protocol (BGP)***

The protocol can connect any internetwork of the autonomous system using an arbitrary topology. The only requirement is that each AS have at least one router that can run BGP and that is the router connected to at least one other AS's BGP router. BGP's main function is to exchange network reachability information with other BGP systems. Border Gateway Protocol constructs an autonomous systems graph based on the information exchanged between BGP routers.

Characteristics of Border Gateway Protocol (BGP)

- *Inter-Autonomous System Configuration: The main role of BGP is to provide communication between two autonomous systems.*
- *BGP supports the Next-Hop Paradigm.*
- *Coordination among multiple BGP speakers within the AS (Autonomous System).*
- *Path Information: BGP advertisements also include path information, along with the reachable destination and next destination pair.*
- *Policy Support: BGP can implement policies that can be configured by the administrator. For ex:- a router running BGP can be configured to distinguish between the routes that are known within the AS and that which are known from outside the AS.*
- *BGP conserves network Bandwidth.*

Functionality of Border Gateway Protocol (BGP)

- *he first function consists of initial peer acquisition and authentication. both the peers established a TCP connection and performed message exchange that guarantees both sides have agreed to communicate*
- *The second function mainly focuses on sending negative or positive reach-ability information.*
- *The third function verifies that the peers and the network connection between them are functioning correctly.*

Importance of Border Gateway Protocol(BGP)

- *Security: BGP is highly secure because it authenticates messages between routers using preconfigured passwords through which unauthorized traffic is filtered out.*
- *Scalability: BGP is more scalable because it manages a vast number of routes and networks present on the internet.*
- *Supports Multihoming: BGP allows multihoming means an organization can connect to multiple networks simultaneously.*
- *Calculate the Best Path: As we know data packets is traveled across the internet from source to destination every system in between the source and destination has to decide where the data packet should go next*
- *TCP/IP Model: BGP is based on the TCP/IP model and it is used to control the network layer by using transport layer protocol*

Types of Border Gateway Protocol

- *External BGP: It is used to interchange routing information between the routers in different autonomous systems, it is also known as eBGP(External Border Gateway Protocol). The below image shows how eBGP interchange routing information.*
- *Internal BGP: It is used to interchange routing information between the routers in the same autonomous system, it is also known as iBGP(Internal Border Gateway Protocol). Internal routers also ensure consistency among routers for sharing routing information. The below image shows how iBGP interchange routing information.*

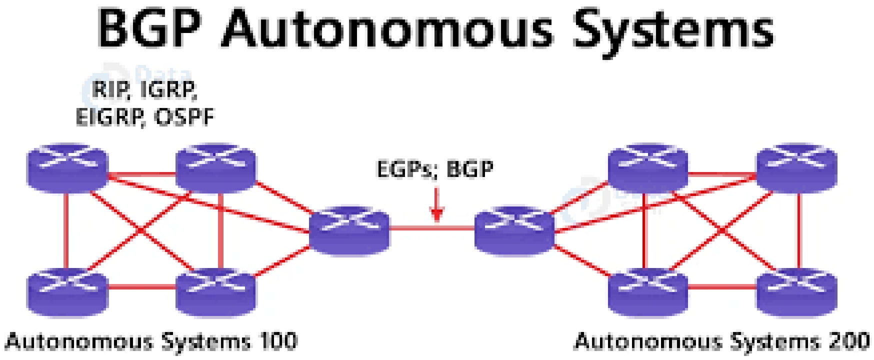


figure 31

b) *Interior Gateway Routing Protocol (EIGRP)*

EIGRP (Enhanced Interior Gateway Routing Protocol) is also considered a hybrid protocol due to its combination of distance vector and link state features. Developed by Cisco, EIGRP uses the Diffusing Update Algorithm (DUAL) for rapid convergence and loop-free routing. EIGRP maintains a neighbor table and a topology table, ensuring that each router has up-to-date information about the state of its neighbors and the overall network topology. The protocol uses a composite metric based on bandwidth, delay, load, and reliability to select the most efficient route to a destination. EIGRP's partial and bounded updates reduce the amount of routing traffic on the network, improving scalability and performance. The feasibility condition ensures that only loop-free paths are used, enhancing the stability and reliability of the network. EIGRP's support for multiple network layer protocols, such as IP, IPv6, and IPX, adds to its versatility and utility in diverse networking environments

What type of protocol is Enhanced Interior Gateway Routing Protocol?

EIGRP is an enhanced distance vector protocol that evolved from Cisco's IGRP. Although IGRP is now obsolete, a network that still uses routers based on the protocol can interoperate with EIGRP-based routers because the metrics used with one protocol can be translated into the metrics of the other protocol. A metric is the distance information used to select the most efficient loop-free path.
EIGRP can be deployed on Internet Protocol networks, such as IPv4 and IPv6, as well as networks such as Novell Internetwork Packet Exchange.

An EIGRP-based router keeps a copy of its neighbor's routing tables. If it can't find a route to a destination in one of these tables, it queries its neighbors for a route, and they, in turn, query their neighbors until a route is found. When a routing table entry changes in one of the routers, it notifies its neighbors of the change only. Some earlier protocols required sending the entire table.

What are the basic features of EIGRP?

EIGRP also uses a reliable transport mechanism to guarantee the ordered delivery of all EIGRP packets to its neighbors. The transport supports the intermixed transmission of Multicast and unicast packets.At the heart of EIGRP is the diffusing update algorithm (DUAL), which determines the most efficient – least costly – routes to reachable destinations in a network made up of routers and links. The decision is based on distance and whether a destination path is loop-free. The algorithm uses the DUAL finite state machine to track the routes advertised to its neighbors and maintain the information used by the algorithm to determine the least costly route.

EIGRP also uses a reliable transport mechanism to guarantee the ordered delivery of all EIGRP packets to its neighbors. The transport supports the intermixed transmission of Multicast and unicast packets.

EIGRP uses five package types:

- *HELLO packets. Sent out at regular intervals to facilitate the neighbor discovery process*
- *QUERY packets. Used by a router to advertise that a route is in an active state and to request alternate path information from neighbors.*
- *REPLY packets. Sent after an entire QUERY packet has been received to acknowledge that packet's receipt.*
- *REQUEST packets. Used to request specific information from one or more neighbors, similar to QUERY packets but sent unreliably – no notification if delivery fails.*
- *UPDATE packets. Convey information about destinations and their reachability.*

What are the advantages of EIGRP?

- *increases availability through faster convergence, helping to avoid disruptions in the event of a link outage*
- *improves voice and video quality by avoiding routing loops and supporting almost immediate convergence*
- *simplifies operations and lowers costs because administrators don't need to manually update the routing design to accommodate changes*
- *minimizes network resource usage during normal operations because only HELLO packages are transmitted when the network is stable*
- *reduces the protocol's load on the network because only changes to the routing table are propagated, rather than the entire routing table*
- *uses links more efficiently by utilizing equal-cost multipath and unequal-cost load balancing.*

PHASE 4: RECENT ADVANCES IN ROUTING PROTOCOLS

Recent advances in routing protocols focus on enhancing scalability, convergence times, and robustness. Key developments include improvements in protocol algorithms and integration with emerging technologies like SDN (Software-Defined Networking). These advances aim to address the challenges posed by the growing complexity and scale of modern networks, ensuring efficient and secure data transmission.

a) ***SDN Integration***

Integrating routing protocols with SDN allows for more dynamic and programmable network management, leading to improved efficiency and adaptability. SDN decouples the control plane from the data plane, enabling centralized network control. This separation allows for more flexible and responsive network management, where routing decisions can be dynamically adjusted based on real-time network conditions. One of the primary benefits of SDN integration is the ability to automate network configuration and management. Network administrators can use SDN controllers to implement policies that automatically adjust routing paths based on traffic loads, ensuring optimal performance and avoiding congestion. Additionally, SDN enables easier implementation of new routing algorithms and protocols, as updates can be made centrally without the need to modify individual network devices

History: *The term SDN originally appeared in [Greene 2009], referring to the ability of Open-Flow [McKeown et al. 2008] to support the configuration of table flows in routers andswitches using software. However, the ideas behind SDNs come from the goal of hav-ing a programmable network, whose research started short after the emergence of theInternet, led mainly by the telecom industry. Today, the networking industry has shownenormous interest in the SDN paradigm, given the expectations of reducing both cap-ital and operational costs with service providers and enterprise data centers with pro-grammable, virtualizable and easily partitionable networks. Actually, programmabilityis also becoming a strategic feature for network hardware vendors, since it allows amany devices to be programmed and orchestrated in large network deployments (e.g.,data centers). In addition, discussions related to the future Internet has led to the stan-dardization of SDN-related application programming interfaces (API), with new com-munication protocols being successfully deployed on experimentation and real scenarios[Kim et al. 2013, Pan et al. 2011].These features of SDNs make them highly valuable for cloud computing systems,where the network infrastructure is shared by a number of independent entities and, thus,network management becomes a challenge. Indeed, while the first wave of innovationin the cloud focused on server virtualization technologies and on how to abstract computational resources such as processor, memory and storage, SDNs are today promot-ing a second wave with network virtualization [Lin et al. 2014]. The emergence of largeSDN controllers focused on ensuring availability and scalability of virtual networking forcloud computing* *systems (e.g., OpenDayLight [Medved et al. 2014] and OpenContrail[OpenContrail 2014]) is a clear indication of this synergy between both technologies.Besides the cloud, SDNs have also been adopted in other computing scenarios,with device vendors following the SDN path and implementing most of control logicin software over standard processors. This has led to the emergence of software-definedbase stations, software defined optical switches, software-defined radios, software-definedrouters, among others.*

b) ***Enhanced Security Features***

New security features are being incorporated into routing protocols to protect against routing attacks and ensure data integrity. As networks become more interconnected and complex, the risk of attacks such as route hijacking, man-in-the-middle attacks, and denial of service (DoS) attacks increases. Modern routing protocols are being designed with built-in security mechanisms to address these threats. One of the key enhancements is the implementation of cryptographic techniques to secure routing updates. By using authentication and encryption, routers can verify the authenticity of routing information received from other routers, preventing malicious entities from injecting false routes into the network. For example, protocols like OSPFv3 and BGP support authentication methods such as IPsec and TCP MD5, respectively, to secure routing exchanges. Another significant advancement is the use of anomaly detection algorithms to identify suspicious routing behavior. These algorithms analyze routing patterns and detect deviations from normal behavior, allowing for the early detection of potential attacks. Once an anomaly is detected, the network can automatically take corrective actions, such as isolating the affected router or rerouting traffic. Modern routing protocols also include mechanisms for route validation and verification. These mechanisms ensure that the routes advertised by routers are valid and conform to predefined policies. For instance, the Resource Public Key Infrastructure (RPKI) is used in BGP to validate route origins, ensuring that only authorized networks can advertise specific IP address prefixes. Additionally, enhanced logging and auditing capabilities are being integrated into routing protocols. These features provide detailed records of routing events, helping network administrators to trace the origin of issues and understand the impact of changes made to the network. This level of visibility is crucial for maintaining the integrity and security of the routing infrastructure. In conclusion, the integration of SDN and the incorporation of enhanced security features are significant advancements in routing protocols. These developments address the challenges of modern networks, providing more dynamic, efficient, and secure routing solutions. As network demands continue to grow, ongoing innovations in routing technologies will play a critical role in maintaining robust and reliable network performance.

c) ***Algorithmic Improvements:***

Protocol algorithms have evolved to incorporate more sophisticated metrics for path selection, considering factors beyond hop count, such as link quality, bandwidth availability, and network congestion levels. This helps in optimizing the use of network resources and improving overall performance.

d) ***Improved Robustness:***

Robustness in routing protocols ensures network stability even under adverse conditions. Advances in protocol design include mechanisms for detecting and mitigating routing loops, preventing routing information corruption, and enhancing fault tolerance

e) ***Faster Convergence Times:***

Convergence time refers to how quickly the network adapts to topology changes (such as link failures or additions). New protocols and enhancements in existing ones aim to reduce convergence times significantly. Techniques like fast reroute (FRR) and optimized link-state routing protocols contribute to faster convergence.

f) ***Enhanced Scalability:***

Traditional routing protocols like OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol) have been optimized to handle larger networks with thousands of nodes and routes. This includes improvements in routing table management and efficient path computation algorithms.

IV. SUMMERY OF PROTOCOLS:

a) *Distance Vector Protocols: RIP/RIP 2 :*

RIP, a distance vector protocol, was tested in a small-scale network to observe its convergence time and simplicity in implementation. The results indicated that while RIP is easy to configure, it struggles with scalability and slow convergence in larger networks. As highlighted by Khraisat et al. (2019), the simplicity of RIP makes it suitable for educational purposes and small networks, but its limitations prevent its use in larger infrastructures.

b) *Link State Protocols OSPF and IS-IS :*
OSPF and IS-IS were implemented in medium to large-scale network topologies to assess their efficiency and scalability. Both protocols demonstrated rapid convergence and robust performance in dynamic network environments. OSPF's hierarchical structure and support for multiple areas were particularly beneficial in reducing routing overhead and improving scalability, as noted by Liao et al. (2013). IS-IS, on the other hand, showcased flexibility in area design and efficiency in handling large routing domains.

c) *Hybrid Protocols EIGRP and BGP :*
EIGRP, a hybrid protocol developed by Cisco, was tested for its rapid convergence and loop-free routing capabilities. The Diffusing Update Algorithm (DUAL) used by EIGRP ensures efficient route calculation and minimal network disruption during topology changes. Vigna and Kemmerer (1999) highlighted the robustness of EIGRP in maintaining network stability and performance. BGP, essential for inter-domain routing, was evaluated for its ability to handle large routing tables and support policy-based routing. The simulations demonstrated BGP's critical role in the global Internet infrastructure, managing complex routing policies and ensuring route integrity and security.

V. CONCLUSION:

The evolution of routing protocols has been driven by the need to address challenges such as scalability, convergence times, and network complexity. Recent advancements have introduced sophisticated algorithms and integration with technologies like Software-Defined Networking (SDN), enhancing protocol efficiency and adaptability to dynamic network environments.Routing protocols form the backbone of modern computer networks, enabling efficient and reliable data transmission by determining optimal paths between devices. This study has explored the fundamental principles and recent advancements in routing protocols, encompassing distance vector, link state, and hybrid protocols. The evolution of routing protocols has been driven by the need to address challenges such as scalability, convergence times, and network complexity. Recent advancements have introduced sophisticated algorithms and integration with technologies like Software-Defined Networking (SDN), enhancing protocol efficiency and adaptability to dynamic network environments.

REFERENCES

[1] *network lessons(https://networklessons.com/) online platform to explain complex networking topics as simple as possible for you.*

[2] *Liao, H.J., Lin, C.H.R., Lin, Y.C., Tung, K.Y. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16-24*

[3] *Cisco INC (https://community.cisco.com/) Cisco Systems, Inc. is a leading networking company best known as a manufacturer and vendor of networking equipment. The company also provides software and offers related services.*

[4] *networking (https://www.tutorialspoint.com/) give exclusive lessons in networking*

[5] *networking and programming (https://www.javatpoint.com/) it's website specilized in learning networking with programming*

[6] *D. Johnson, Y. Hu, and D. Maltz. "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", February 2007. http://www.ietf.org/rfc/rfc4728.txt*

[7] *networking(https://www.firewall.cx/) explain most difficult tasks in security and networks*

[8] *networking (https://www.techtarget.com/) TechTarget often covers foundational topics in networking, including concepts like IP addressing, routing, switching, and network protocols.*

[9] *Barros et al. 2015] Barros, B., Iwaya, L., Andrade, E., Leal, R., Simplicio, M., Car-valho, T., Mehes, A., and Näslund, M. (2015). Classifying security threats in cloudnetworking. In Proc. of the 5th Int. Conf. on Cloud Computing and Services Science(CLOSER'2015) (to appear). Springer.*