Routing in IP-based Networks

By

Mr. Murad Khan

CIIT/SP11-REE-047/ISB

MS Thesis

In

Electrical Engineering

COMSATS Institute of Information Technology
Islamabad – Pakistan
Spring, 2012

COMSATS Institute of Information Technology

Routing in IP-based Networks

A Thesis presented to

COMSATS Institute of Information Technology

In partial fulfillment

of the requirement for the degree of

MS (Electrical Engineering)

By

Mr. Murad Khan

CIIT/SP11-REE-047/ISB

Spring, 2012

Routing in IP-based Networks

A post Graduate Thesis submitted to Department of Electrical Engineering as partial fulfillment of the requirement for the award of Degree of M.S (Electrical Engineering).

Name	Registeration Number
Mr. Murad Khan	CIIT/SP11-REE-047/ISB

Supervisor:

Dr. Nadeem Javaid,

Assistant Professor,

Department of Electrical Engineering,

COMSATS Institute of Information Technology (CIIT)

Islamabad Campus

June, 2012

Final Approval

This thesis titled

Routing in IP-based Networks

By

Mr. Murad Khan

CIIT/SP11-REE-047/ISB

Has been approved

For the COMSATS Institute of Information Technology, Islamabad

External Examiner: _____

Supervisor: _____

Dr. Nadeem Javaid /Assistant professor
Department of Electrical Engineering
Islamabad Campus

HoD: _____

Dr. Shafayat Abrar / Associate professor
Department of Electrical Engineering
Islamabad Campus

Declaration

I Mr. Murad Khan, *CIIT/SP11-REE-047/ISB* hereby declare that I have produced the work presented in this thesis, during the scheduled period of study. I also declare that I have not taken any material from any source except referred to wherever due that amount of plagiarism is within acceptable range. If a violation of HEC rules on research has occurred in this thesis, I shall be liable to punishable action under the plagiarism rules of the HEC.

Date: _____

_____

Mr. Murad Khan

CIIT/SP11-REE-047/ISB

Certificate

It is certified that **Mr. Murad Khan**, CIIT/SP11-REE-047/ISB has carried out all the work related to this thesis under my supervision at the Department of Electrical Engineering COMSATS Institute of Information Technology, Islamabad and the work fulfills the requirements for award of MS degree.

Date: _____

Supervisor:_____

Dr. Nadeem Javaid /Assistant professor
Department of Electrical Engineering
CIIT Islamabad Campus

Head of Department:

_____

Dr. Shafayat Abrar/Associate professor
HoD Electrical Engineering

DEDICATION

Dedicated to my family and friends

ACKNOWLEDGMENT

I am heartily grateful to my supervisor, Dr. Nadeem Javed, whose patient encouragement, guidance and insightful criticism from the beginning to the final level enabled me have a deep understanding of the thesis.

Lastly, I offer my profound regard and blessing to everyone who supported me in any respect during the completion of my thesis.

Mr. Murad Khan
CIIT/SP11-REE-047/ISB

ABSTRACT

Routing Protocols are very important in the modern day's communications, as with the increasing number of network devices it has become very vital to understand and implement the correct routing protocol for the network and to process and communicate the huge routing information among all the network nodes. Dynamic Routing protocol selects the best optimal path from source node to destination node. There are three major types of dynamic routing protocols, each having their own criteria for the route selection and propagation. These are categorized as.

1) Distance Vector
2) Linked Stated
3) Hybrid

The major example of Distance Vector Routing (DVR) Protocol is Routing Information Protocol (RIP). RIP is normally used for smaller networks and its hop limit is 15. On the other hand, two other routing protocols, i.e., Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) are designed for the huge networks and are much more efficient routing protocols as compared to Distance Vector Routing Protocols. EIGRP falls under the category of Hybrid Routing Protocols or sometime it's called as advanced distance vector routing protocol. EIGRP is Cisco proprietary routing protocol. Open Shortest Path First (OSPF) is widely used routing protocol based on Dijkstra's Algorithm. OSPF is open standard routing protocol as it is not bound to any specific vendor equipment. All these routing protocols have different route selection mechanism, different architecture, route processing, convergence and delay. In this thesis we present a study of these routing protocols for the real time application using OPNET. In order to study the performance of RIP, EIGRP and OSPF, we present different scenarios to evaluate which routing protocols efficiency is better than the others. The performance evaluation of these routing protocols is based on different metrics like convergence time, end-to-end delay, throughput, jitter, and packet loss. Results show that EIGRP routing protocol provides better performance than OSPF and RIP routing protocols for real time applications.

Table of Contents

List of Figures

Chapter 1
Introduction

1

Introduction

1.1 Routing protocols

At present, communication networks are growing at a rapid speed. They facilitate users by providing different services like voice, video streaming and voice applications. Internet is a major example of communication networks. Communication networks provide the basic infrastructure whereas routing protocols provide the mechanism to exchange information among different nodes. Routing protocols reside at network layer of Open System Interconnection (OSI) model. There are two types of protocols working at network layer, i.e.,

- Routed Protocol
- Routing Protocol

Routed protocols carry the data like Internet Protocol (IP), Inter-network Packet eXchange (IPX) etc., whereas routing protocols are used for the path selections like RIP, EIGRP and OSPF etc. Routing protocols can be further classified into two major categories.

- Interior Gateway Routing Protocol (IGRP)
- Exterior Gateway Routing Protocol (EGRP)

IGRP is used for the route selection within the autonomous system. IGRP can be classified into three major categories.

1. Distance Vector Routing (DVR) Protocol

2. Linked state routing protocol

3. Hybrid routing protocol (Advanced distance vector)

Bellman-Ford algorithm is used for path computation by DVR protocol. DVR protocol periodically exchanges its complete routing table. DVR protocols broadcast its complete routing table to its neighboring nodes. Whereas link-state protocols use the triggered update instead of periodic updates. The DVR protocol doesn't use sophisticated process to compute the path. Linked state routing protocol uses the multicast to inform any change occurred in the topology. Linked state routing protocols have much better self healing and path computational mechanism.

Distance vector routers do not know about the complete network topology. These routers only have information which is passed by the connected neighboring devices: Distance vector routing protocol only uses the hop-count as its metric. Linked state and hybrid routing protocols also consider other parameters to compute the path.

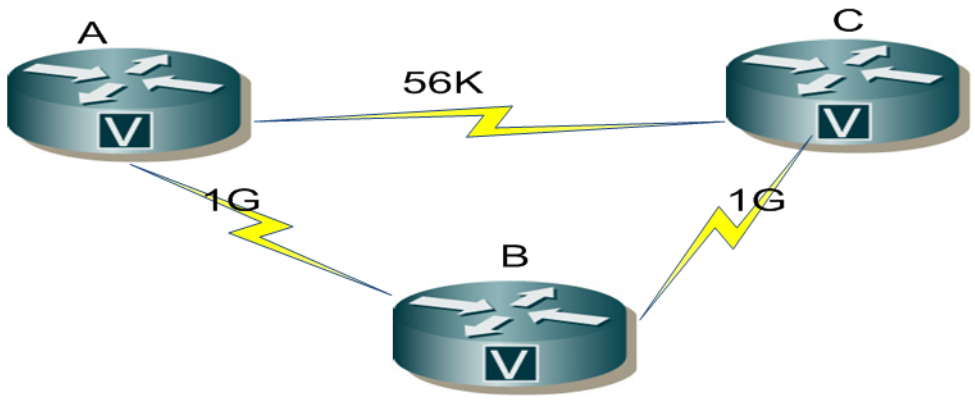

Figure 1.1: *Distance vector protocol*

In Figure 1.1, we have a topology in which three routers are connected with each others. We have two routes for reaching A-C, one is directly from A-C and the second route is A-B-C. If in this scenario RIP is used as a routing protocol it will select A-B as the best path as according to Bellman-Ford algorithms only considers the hop count, A-B has lesser hop-count as compared to path A-B-C. Although A-B is only 56K link whereas A-B-C is 1 Gigabit links. If we implement any linked state or hybrid routing protocol in this scenario it will always consider path A-B-C, as this path have greater bandwidth as compared to path A-B. As both the linked state and hybrid routing protocols mainly considers the bandwidth

for path computational and selection.

RIPv1 and RIPv2 and IGRP are the major example of distance vector routing protocol. EGP and BGP are not pure distance vector routing protocols. A DVR protocol calculates routes based solely on the link costs, whereas in BGP, the local route preference value takes priority over the link cost.

Enhanced IGRP (EIGRP) is one of the major examples of hybrid routing protocols. EIGRP is Cisco's proprietary protocol. EIGRP provides much efficient route computation as compared to DVR protocols.

1.2 Motivation

Packet Switched networks require much excellent, proactive and efficient routing protocol. To select the best routing protocol among RIP, EIGRP and OSPF for the real time applications like streaming videos, IP telephony, IP unicast and IP multicast traffic is the major motivation for this thesis. We have analyzed that which routing protocol will perform better in different scenarios and environment.

1.3 Problem Statement

Routing protocols operate at layer 3 of OSI model. The basic purpose of network layer is sorting and distribution of IP packets. There are several routing protocols for dynamically selecting the best path. The main drawback of the EIGRP routing protocol is that it only works when all devices are from Cisco. Convergence time of EIGRP is faster and easy to configure as compared to other routing protocols. In contrast, OSPF is a link-state interior gateway protocol. OSPF is based on Dijkstra algorithm. OSPF routing protocol is difficult to configure. OSPF requires high memory and high processor requirements.

Routing Information protocol (RIP) is not widely used routing protocol these days, it's only used in small network setup, and RIP uses a very simple routing algorithms Bellman Ford algorithms. There are many drawbacks of RIP which are discussed in chapter 3 and chapter 4. In this thesis, focus is on measurement, architecture, performance and verification of the IGRP.

1.4 Thesis organization

We provide technical details about routing protocols in chapter 2. Chapter 3 presents a review of analyzed routing protocols. Chapter 4 presents an analytical analysis of the selected protocols using OPNET simulator. We conclude the thesis in chapter 5.

Chapter 2
Routing Protocols - Background

2

Routing Protocols - Background

2.1 Overview

In traditional packet switched networks, routing protocols usually transmits packets routing information between interconnected nodes. In an IP network routing decision takes place in hop by hop fashion. All the Routing protocols must have these objectives:

1. To communicateobetween the different routers placed at different location.
2. To make correct and efficient routing decisions
3. To exchange information among neighbor's routers.
4. To build error free routing tables
5. To learn existing routes

Routers are used to communicate among the different subnets and exchange routing information among them. The main concept of "routing protocols" is to create the best possible path from one end to the other that is to find out the best route from source to destination. These are built on basis of various properties of the path. For IP based routing, Dynamic IGP protocols can be classified as;

- Linked State RoutingoProtocols
- Distance Vector Routing Protocols
- Hybrid.

2.2 Routing Protocols Attribute and Characteristics

The main characteristics of routing protocols are given below:

2.2.1 Best Possible Routes

One of the characteristics of routing protocols is to find the best route possible for communication. It might be one of the smallest or with least traffic depending on the situation.

2.2.2 Faster Convergence

The communication time should be small in the inter-router communication so information regarding routers can be easily acknowledged.

2.2.3 Security Options

The protocol makes sure that data is transmitted securely from source to given destination.

2.2.4 Avoiding Loops

Loop free is used to find out the effective bandwidth of the network by making sure that there are no loops in the network as loops would not only slow down but would also make it tough to calculate effective bandwidth.

2.3 Important Concepts About Routing and Metrics

Understandings of these concepts are very essential before we start our study about any IGP or EGP routing protocols.

2.3.1 Metrics

Metric can be simply define as decision making criteria of any routing protocol on the basis of which it makes the routing decision is called as metric. All protocols have different criteria for considering the best route. For example in case of RIP hop-count is metric, EIGRP uses composite metric which is the combination of different attributes like, load, reliability, MTU, bandwidth and delay, Whereas metric of OSPF is cost based on bandwidth.

2.3.2 Need of a Metric

Metrics normally determine the best possible path in case when more than one path is available for the same destination node. There are various ways to compute best path and metrics for each routing protocol.

2.3.3 Parameters of a Metric

Every routing protocol uses Metrics to measure and then rank routes on the basis of; Best to worst of most preferred to least preferred. Various routing protocols use various routing techniques and parameters to measure the different metrics. Following metrics are usually used to determine best paths by any routing protocol.

- Delay: determines the amount of time needed to travel from one point to other. It depends on various parameters, like; bandwidth utilization of link, physical distance travelled, and port queues.
- Cost: can be based on any single metric or combination of metrics as it can be determined by shortest distance or least traffic path. It is normally administered by network administrators.
- Load: It is calculated by the traffic on the specific nodes. The routing protocol normally uses loadoin the calculationoof a best route.
- Hop-count: It counts the number of routers for which a packet has to cross to reach destination.
- Bandwidth: also plays an important role in the path identification which normally results in choosing a high bandwidth link over a low bandwidth link.

- Reliability: can be calculated by referencing to the earlier failure happenings or previous error counts.

2.4 classification of Routing Protocols

Routing means best possible route. Routing protocols can be classified in to two major categories that is State route vs. Dynamic route. State route are the routes configured by network administrator. Static routes administrative distance is always 1, means if there is static route in a network and some other dynamic routing protocols are also used for the path selection that static route will always be considered as a best route because it has lesser administrative distance as compared with the any routing protocol. Dynamic routes are the routes selected using routing protocol. Dynamic routes can be classified in to two major categories that is interior gateway routing protocols and exterior gateway routing protocols. Interior gateway routing protocols are used for route selection within the autonomous system the most popular IGP protocols are RIP,OSPF ,IS-IS and EIGRP. Each of the routing protocol has their own metric and administrative distances. Exterior gateway routing protocols are used for routing among different autonomous system; the major example of exterior gateway routing protocol is Border gateway routing protocols. Routing protocols can be classified in the following fashion.

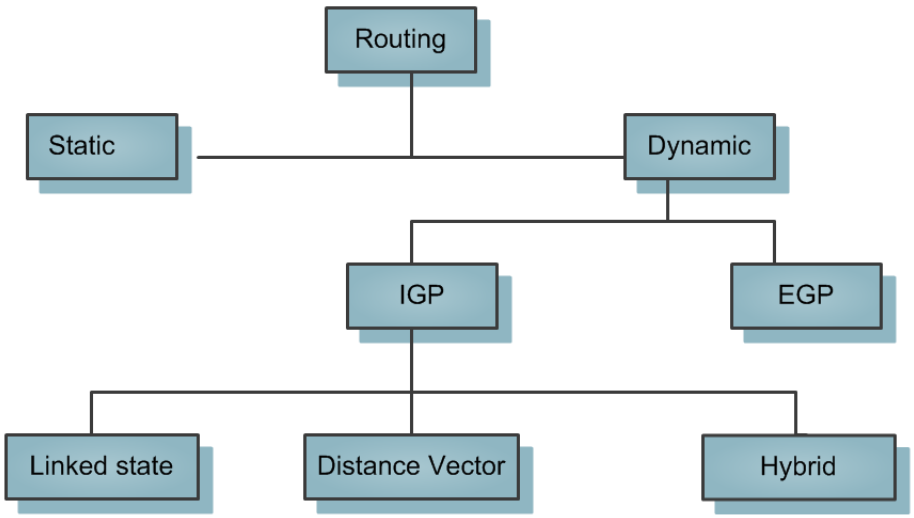

Figure 2.1: *Classification of Routing Protocols*

2.5 Static and Dynamic Routing

In static routing, network administrator configures all the routes manually. So, for every new addition network administrator has to add new routing entry for the any addition. Whenever there is a new route or node added in the network, manual entries have to be made and if node has to be deleted, it has to be deleted manually as well. This is normally used for small networks. In static routing, the network has more control over the network. Static routing is simple to setup and less processor and memory intensive which is its one of the major benefit but problem arises when there is change in the topology and reconfiguring the route manually sometime become very problematic which is the drawback of static routing. In static routing network administrator has much more control and understanding of network because he is manually establishing the path and knows which of his path is more reliable and what path to choose for specific type of traffic. Whereas along with many advantages of dynamic routing protocol has some problem as well, in dynamic routing, routing tables are formed dynamically on the basis of routing protocol and its path calculation algorithms. The main drawback of dynamic routing protocols is they are more processor and memory intensive. Dynamic routing protocols have their own methods and technique of establishing the best path. Normally linked state and hybrid of advanced distance vector routing protocols maintains topology table in which all the possible path to destinations are exist which is huge advantage which any network administrator can utilize by the use of dynamic routing protocol.

2.6 Classfull Routing Protocols and Classless Routing Protocols

Based on the subnet mask, routing protocols are separated into two routing protocols such as

- Classless Routing Protocols
- Classful Routing Protocols

2.6.1 Classfull Routing

There are three major classes of IP address

1. Class A ranges from 1-126. In class A one octat is fixed for the network portion where as three potions are fixed for the host portion. Subnet mask of class A is 255.0.0.0.
2. Class B ranges from 128-191. In class B two octats are fixed for the network portion and two of the octact are reserved for the host porition . Subnet mask of class B is 255.255.0.0.
3. Class C ranges from 192-223. In Class C three octacts are reserved for the network portions and only one ocatacts is reserved for the host portions.

- Routers use the same subnet mask to understand the network address which is directly associated to the interface of the main network. When the router is not directly associated to the interface of the same main network, it applies Classfull subnet mask to the route. Classfull routing protocols have so many disadvantages and not used extensively in these days networks:
- This protocol doesn't support Variable Length Subnet Masks (VLSM).
- They are unable to support discontinuous networks.
- These protocols cannot clinch routing updates.
- These protocol cannot be used in sub-netted networks

Below figure depicts the example of network in which class routing is deployed with the same network mask in all the network locations.

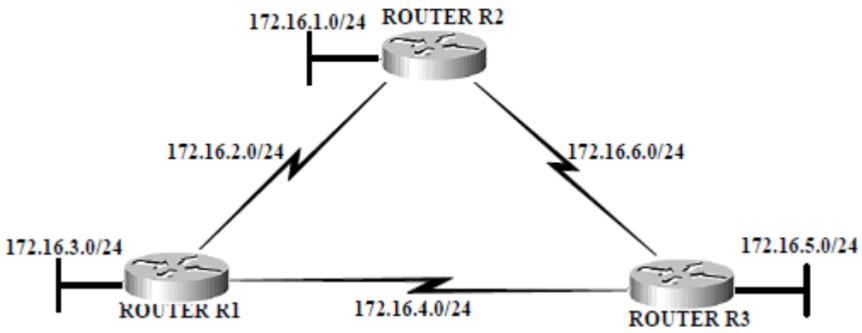

Figure 2.2: *Network Deployed with Classful Routing and Same Subnet Mask*

2.6.2 Classless Routing

As there is limitation with the IPV4 addresses and there are so many reasons of this shortage. Also commercial classes are not free of cost and anyone using these addresses have to pay for it. So it will be very difficult for anyone to have public

addresses at each of the locations as IPV4 address allocation and distributions is not good. Now days it has become a major quality of any routing protocol to support variable length subnet masking. Below figure depicts the classless network deployed by using variable length subnet masking at each of the location.

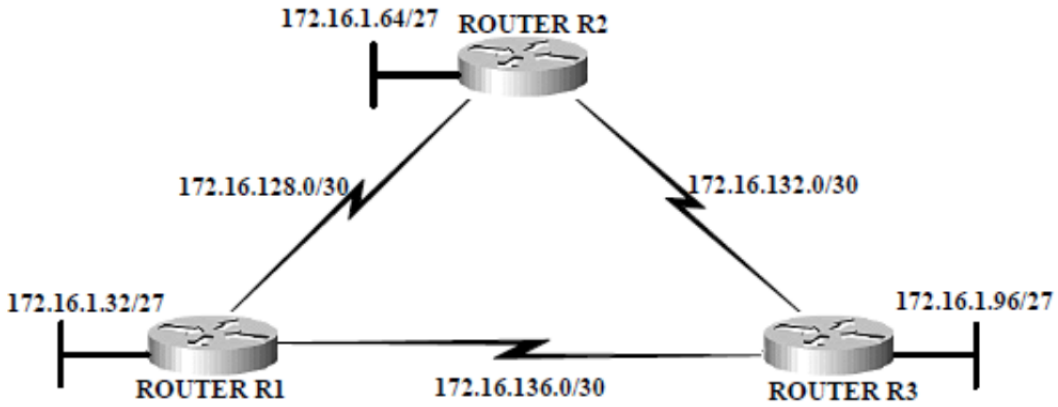

Figure 2.3: *Network Deployed with Classless Routing Protocol*

2.7 Linked-State Routing

The need to overcome the problem with the distance vector routing protocol led to the development of linked-stateorouting protocol. Link-state routing protocol have the following functionalities.

1. Respond quickly upon the change in the network, instead of periodic updates triggered updates are used in case of link-state routing protocol.
2. Respond quickly on any network change.
3. Self healing on network route not working.

Link-state routing protocol only send update only when there is any change occur in the network by this way not using the bandwidth unnecessarily. When there is change in the status of any link it sends any advertisement known as link state advertisement LSA.

By using LSA information is exchanged amongst all nodes. each LSA contains the information of neighboring device. Any change in link is communicated through LSA by flooding. All nodes can maintain a same database for all the routes known as topology table. These databases provide in sequence information of the link cost in the network. By this way routing table is formulated." There

- **Neighbor table:**
  - **Also known as the adjacency database**
  - **Contains list of recognized neighbors**
- **Topology table:**
  - **Typically referred to as LSDB**
  - **Contains all routers and their attached links in the area or network**
  - **Identical LSDB for all routers within an area**
- **Routing table:**
  - **Commonly named a forwarding database**
  - **Contains list of best paths to destinations**

Figure 2.4: *Link State Data Structure*

is a routing table which includes information regarding link costs, their paths and regarding all the neighboring nodes. Dijkstra algorithm is used for calculating the path and cost for each link. The link cost is set by the network operator and it is represented as the weight or length of that particular link." Loadobalancing performance is achieved after assigning the link cost. Therefore, link overcrowding of the network resources can be avoided. Therefore network operators can change the routing by changing the link cost. Usually the costs of the link are left with the default values and it is recommended to reverse the link's volume and then allocate the weight of a link on it." Though link state request protocols have better springiness, they are complex compared to the DV protocols.

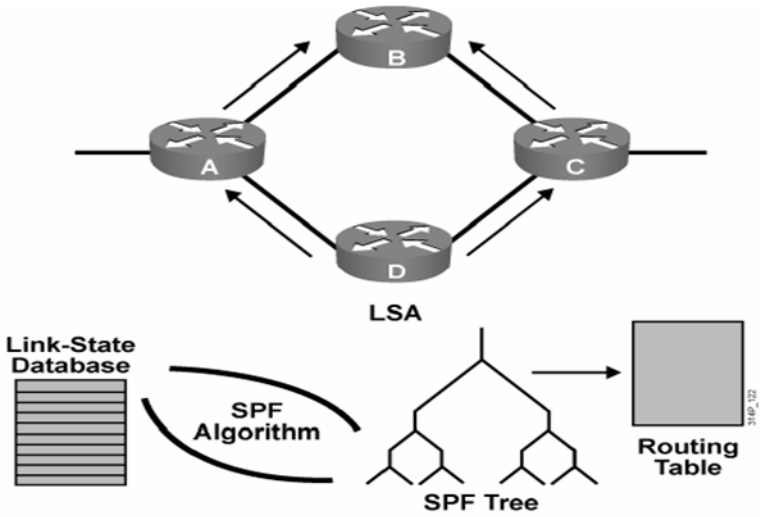

Figure 2.5: *Link State Routing [5]*

There are two linked-state routing protocols that is OSPF and integrated IS-IS. Link-state routing protocols use SPF (Shortest Path First Algorithm) knows as Dijkstra's Algorithm. Integrated IS-IS however uses SPF only.

2.7.1 Link-state protocol Characteristics

Link state protocol has the following characteristics.

- Each router possesses the identical database
- provides hierarchical structure
- Include and maintain several paths in the topology table for the destination
- Efficient and fast convergence without any loop
- Have much more precise metrics

2.7.2 Methods of Routing

These are the steps involved in the link-state routing.

- Every router acquires information of the directly connected neighboring networks and its directly connected links
- Every router stores information of link-state packet received from its neighbor
- Every router establishes the minimum cost path for the network topology
- Every router should have a connection with its directly connected adjacent networks and this is usually performed through ARP packet exchanges
- Every router must send a link-state information

2.7.3 Strength and Weaknesses of LSR

In Linked-state routing protocols, routers calculate routes autonomously and are autonomous of the calculation of intermediate routers. The strength of linked-state routing protocols are:

- They act fast to any change in connectivity.
- The packet size is very small.

Major disadvantages of link-state routing protocols are:

- memory intensive
- Hard to configure and understand
- Uses sophisticated algorithms

- More processor intensive
- Usually Unsuccessful under agility for link changes

2.8 Distance-Vector Routing

The Major example of Distance Vector Routing Protocols is Routing Information Protocol (RIP), Distance Vector protocols as the name suggests considers the two primary parameters to decide the best route; that are Distance and Vector. Distance means "How far" and Vector means which directions.RIP version 1 and RIP Version 2 uses Bellman Ford algorithms. Administrative distance of RIP is 120.Administrative Distance is the degree of reliability of any routing protocols. Smaller the administrative distance greater will be the reliability of routing protocols. Metric of Routing Information protocols is "hop-count". Metric is the decision making criteria of any routing protocol. RIP is normally used for smaller networks and its hop limit is 15. Distance vector routing protocols are also referred as routing by rumor. Distance vector routers have only information what neighboring router had passed on. Distance vector routing protocols uses the periodic update instead of triggered update. There are so many problems associated with the distance-vector routing protocol. One of the problems with the distance vector routing protocol is that they are not aware of the full topology. Below figure shows how the routes are learned by distance vector routing protocols and it's much easier to understand the problems associated with the distance vector routing protocols like split horizon, route poisoning etc.

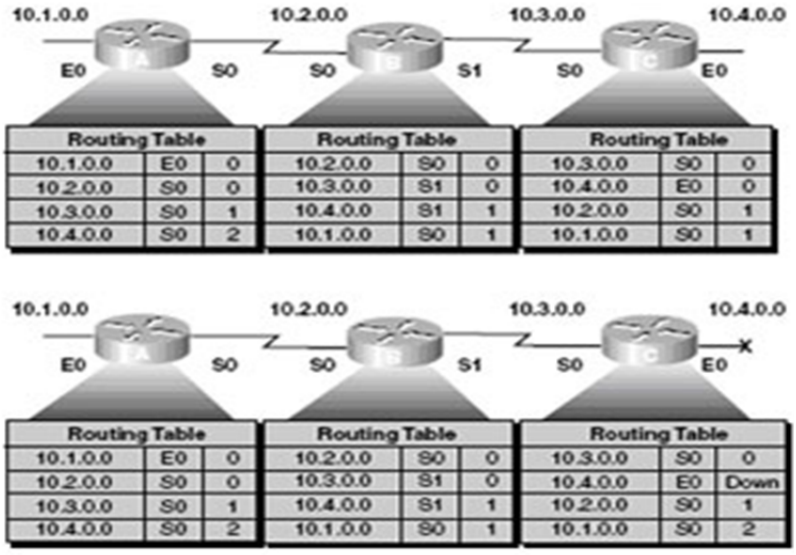

Figure 2.6: *Distance Vector Routing [5]*

2.8.1 Characteristics of Distance Vector Routing

The characteristics of Distance Vectorsrouting protocol are given below.

- Distance Vector routing protocol defines its routing table where all neighbours are directly connected with the table at a steady period
- New information should put in each routing table instantly when the routes become unreachable
- Distance Vector routing protocols are easy and effective in smaller networks and thus require little management
- Distance Vector routing is mainly based on hop counts vector
- The Distance Vector algorithm is iterative

2.8.2 Pros and Cons of DVR

The advantages of Distance Vector routing protocols are:

- Not using sophisticated algorithms, works very efficiently for smaller networks
- DVR are easy to implement
- Uses less memory and processor as compared to LSR

Distance Vector routing protocol experiences many problems like route poisoning, split horizon, counting to infinity and routing loops are the main drawbacks of DVRs. DVR uses Bellman Ford algorithms which isn't an efficient algorithms. Some of the most popular problems with DVR are:

- Possibility of routing loops
- Uses periodic updates and takes time to converge.
- DVR protocols have hop-limit
- Bellman Ford is not using rich metrics like Linked-state protocols.

Chapter 3
Dynamic Routing Protocols

3

Dynamic Routing Protocols

3.1 Routing Information Protocol

The RIP (Routing Information Protocol) is dynamic and a one of the distance-vector protocols which use the hop count as a metric. It was designed for smaller IP networks. For routing updates Routing Information use UDP port 520. It's Calculates the best path by counting the hops. Like rest of the distance-vector protocols its take some time to converge. RIP required less memory as compare to the link state protocols. It is good for a small network limited to few subnets and a small number of routers.

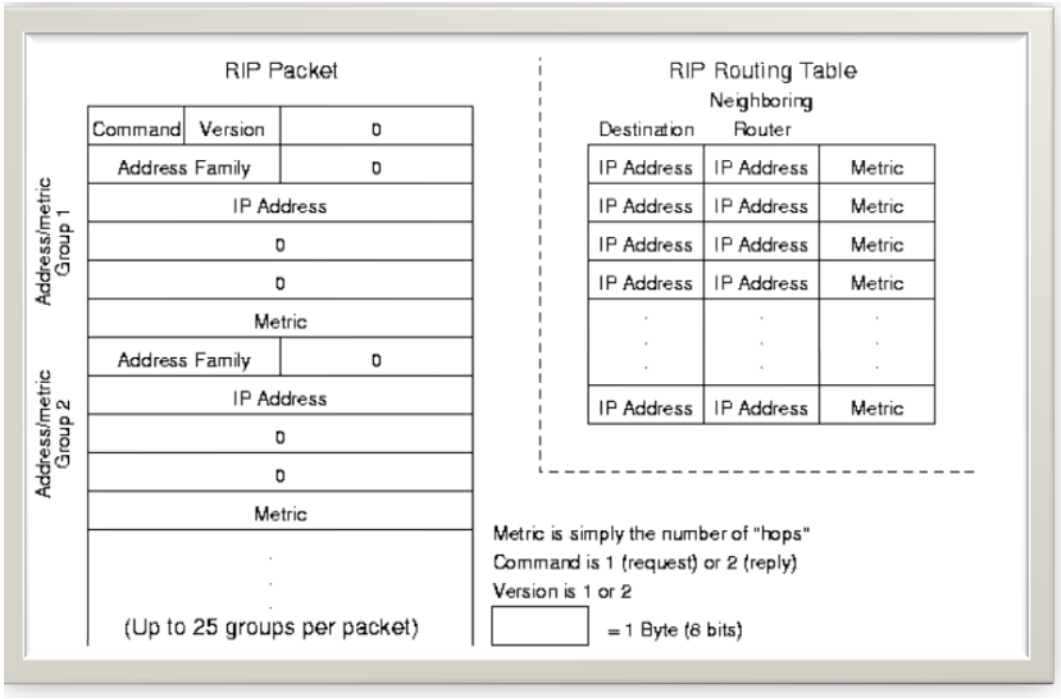

Figure 3.1: *RIP-Ver1 Packet Format [1]*

RIP go for 15 hops only. It cannot handle if number hops increases more than that infect it will not work. Anything more than 15 hops away it will consider unreachable if it found anything that is away more than 15 hops. This is way RIP use for loop prevention. Routing Information Protocol is class-full routing protocol. RIPv1 advertise all the networks that it knows about but without its subnets. This option is available in updated RIPv2 and RIP next generation (RIPng), defined in RFC 2080. RIP next generation (RIPng) is the extension of RIPv2 for IPv6 support. Packet formats are shown in Figures.

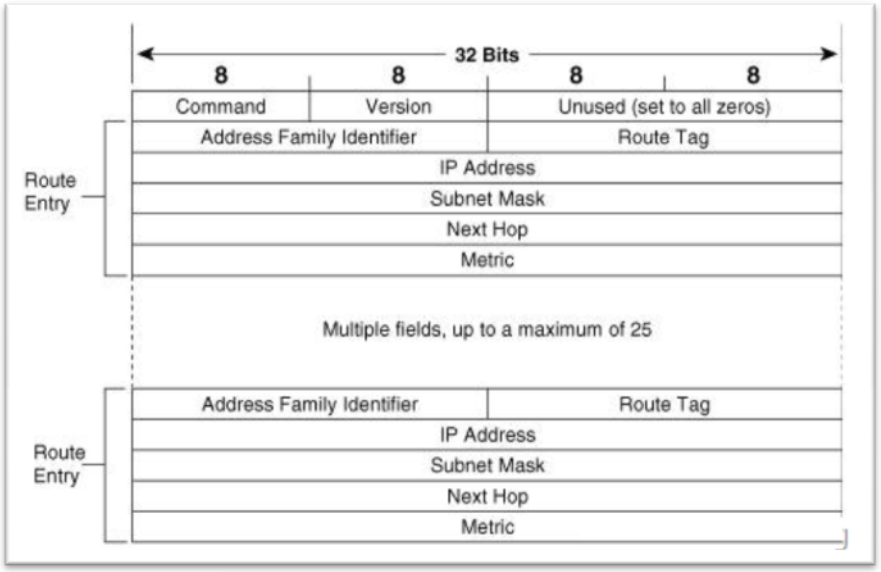

Figure 3.2: *RIP-Ver2 Packet Format [1]*

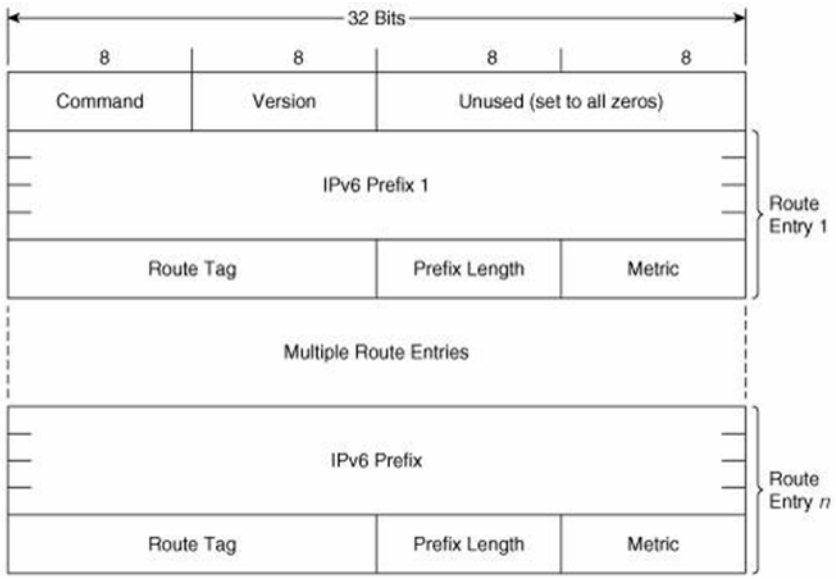

Figure 3.3: *RIPng Packet Format [1]*

RIP is considered is a good solution for small consistent networks. For larger network RIP will be considered more complicated and it will difficult for RIP to

run it in smooth fashion because it have to refresh it routing table after every 30 sec which is not good. RIP (Routing Information Protocol) exchanges complete routing after specific. Routing loops is one of the major problems in distance vector protocol. Below figure can best describe the possible loop occurrence when we have 10.4.0.0 network goes down.

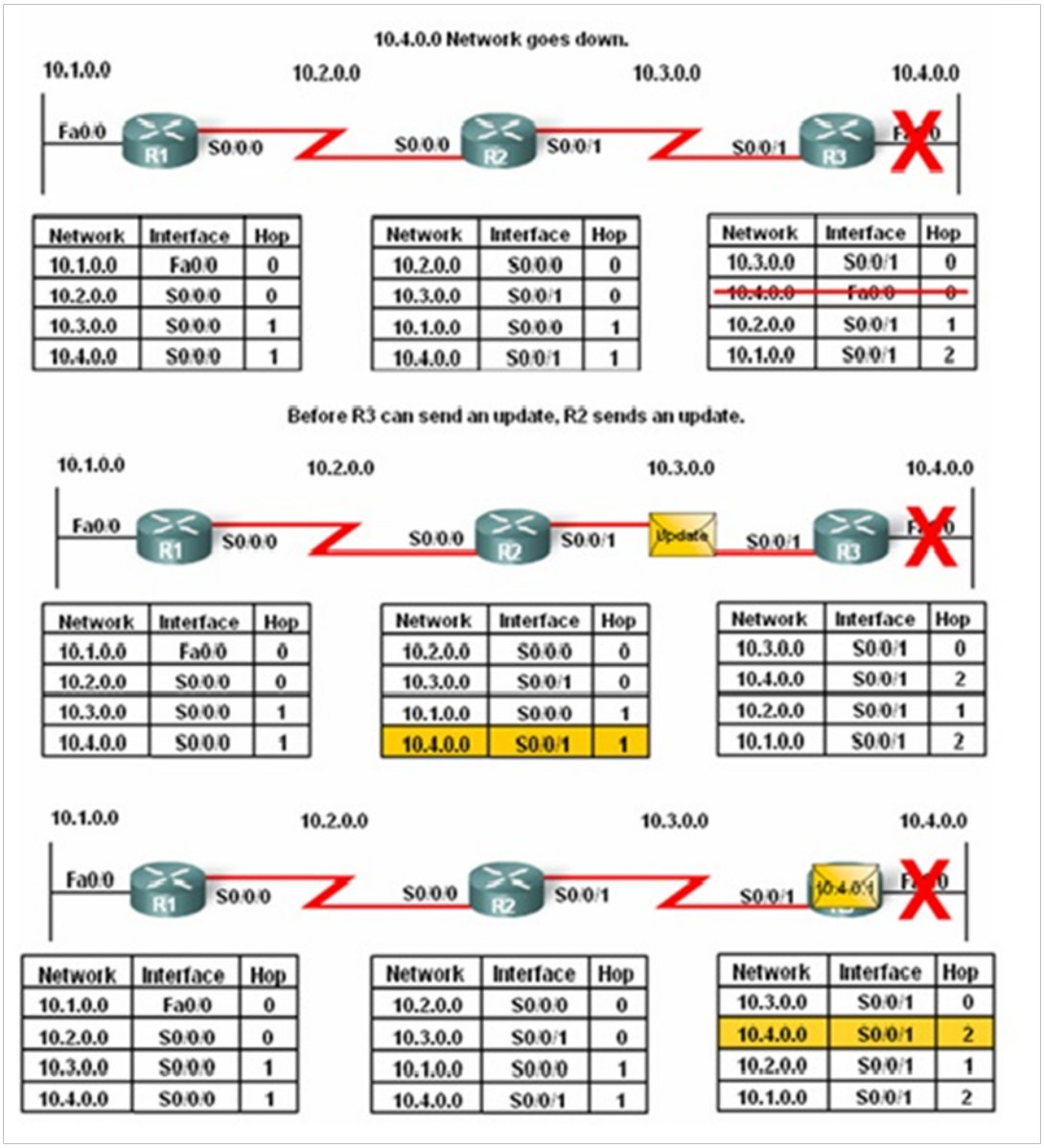

Figure 3.4: *Routing Loops in RIP [1]*

Above is the same condition in which packets travel across network without reaching to the final destination.

3.1.1 Split Horizon

If router sends back information to router from its get already is one the reason of loop occurrence. To avoid this Split Horizon is introduced. According to this rule router will never send information back to the router interface from where it learn already. Normally this happen when router A in a network sends some update to the router B on network and router B didn't get that information because of some failure. Split Horizon Rule for 10.4.0.0:

R2 only advertises 10.3.0.0 and 10.4.0.0 to R1.

R2 only advertises 10.2.0.0 and 10.1.0.0 to R3.

R1 only advertises 10.1.0.0 to R2.

R3 only advertises 10.4.0.0 to R2.

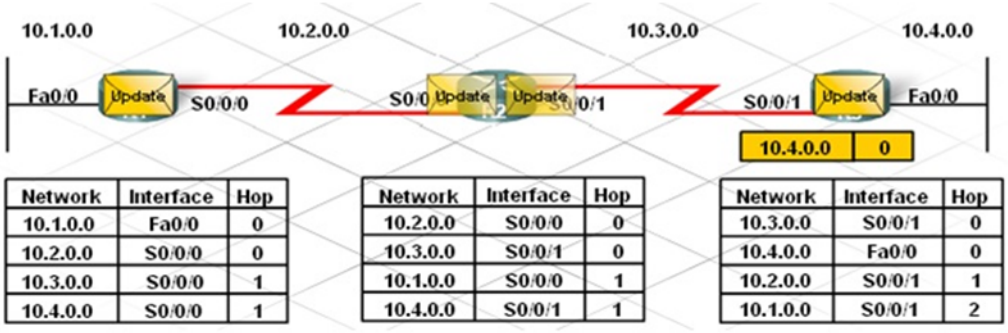

Figure 3.5: *Example of Split Horizon [1]*

To remove above problem from network Split Horizon rule is introduced.

3.1.2 Route Poisoning

Router will consider the route fail if it is advertised with infinite metric (that is metric: 16) instead of marking.

3.1.3 Poison Reverse

Poison reverse is a technique in which a router tells its neighbor routers that one of the link or router is no longer exist of failed. To do this, the notifying routers set the number of hops to the unconnected gateway to a number that indicates "infinite". AS Routing Information Protocol allows only up to 15 hops so

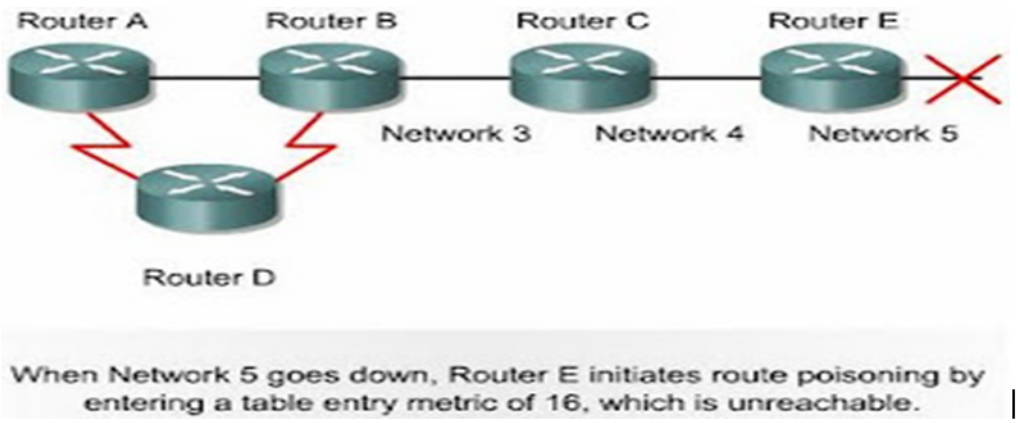

Figure 3.6: *Example of Route Poisoning [1]*

by setting the hop count to 16 would mean that this particular link of route is "infinite." Network 10.4.0.0 goes down. R3 Poisons route with an infinite metric.R3 sends triggered Poison update to R2:

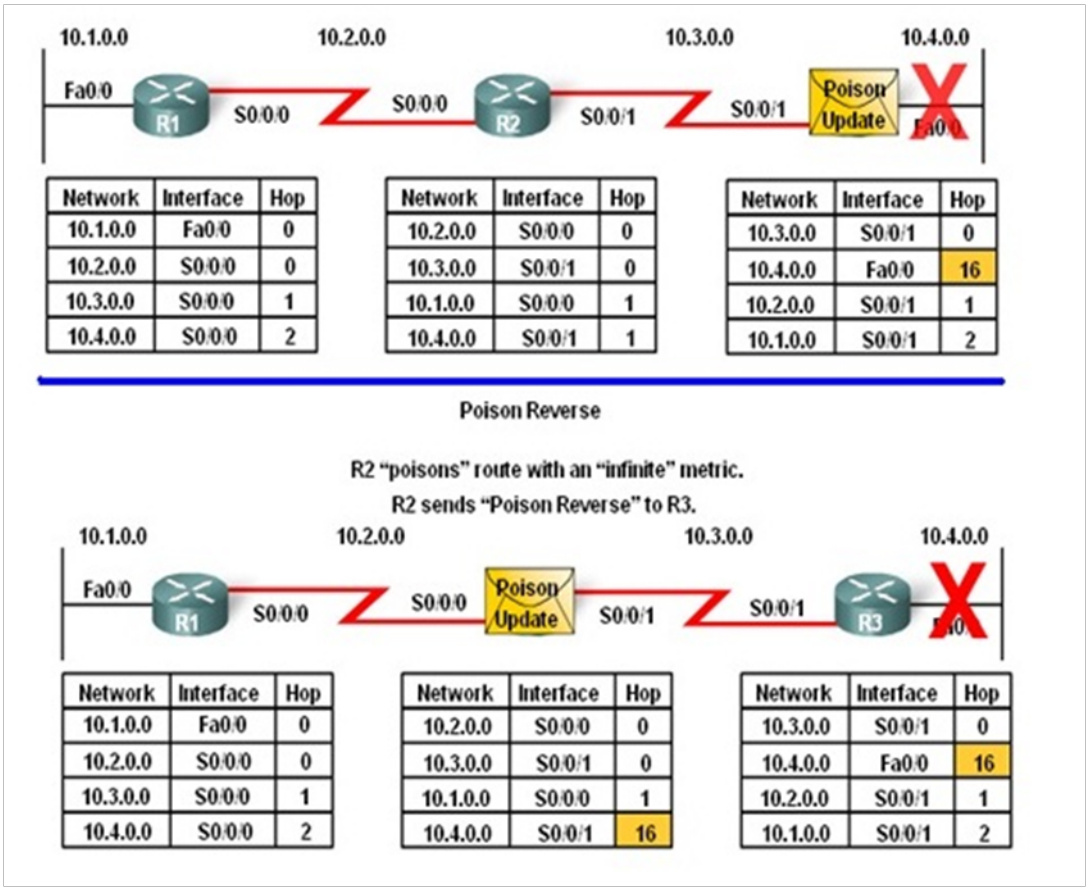

Figure 3.7: *Poison Reverse [1]*

3.1.4 Hold Down Timers

After a route poisoning, router stets a hold-down timer for that particular route and if gets any update with some kind of better metric then the recorded metric which was recorded earlier with in the period of hold down timer, In this case the hold down timer will be removed and will be possible to send the data across the network. . During this process hold-down timer, the "possibly down" will represent the "downed" route in the RIP routing table. Its default value is 180 sec. In below situation Hold down timer will take place.

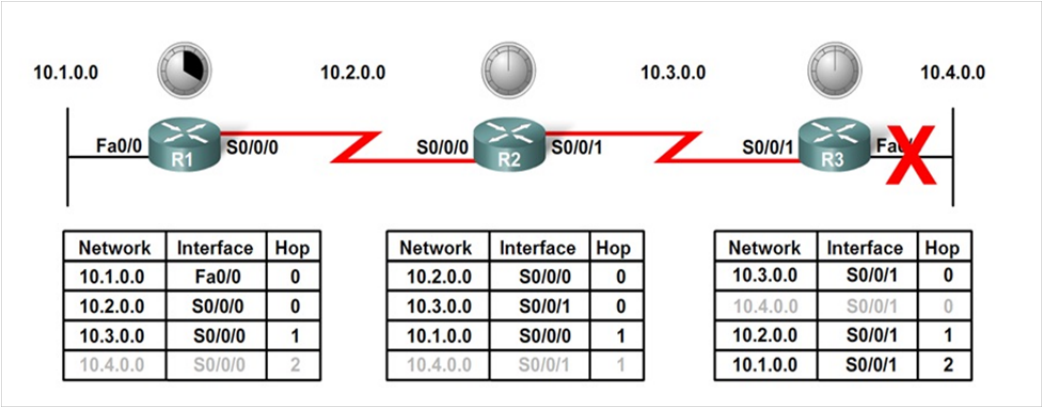

Figure 3.8: *Hold Down Timers [1]*

3.1.5 Triggered Updates

When in network any route failed and do not wait for coming next update, instead send immediate update by listing poison route. R2 Removes Route:

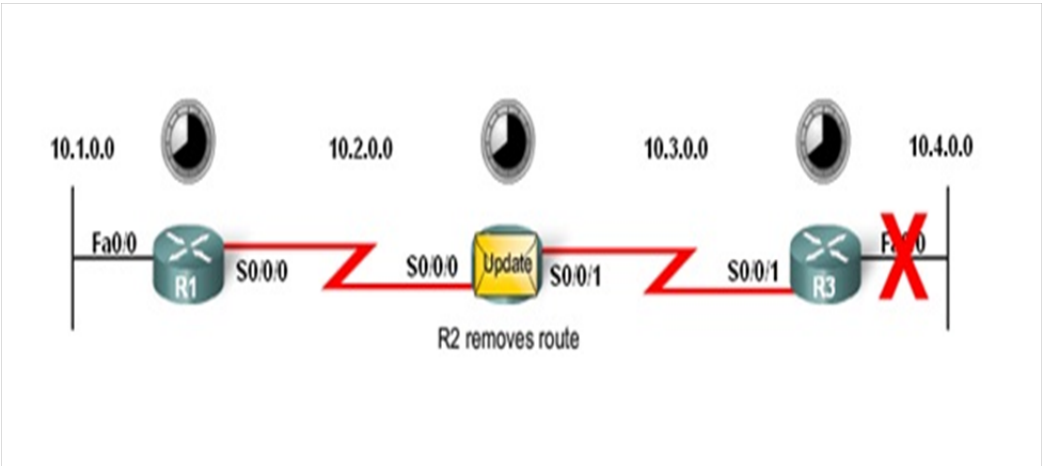

Figure 3.9: *Triggered Updates [1]*

3.1.6 Counting to Infinity

It will go to maximum up to 15 hops. After 15 hops it will be considered Unreachable.

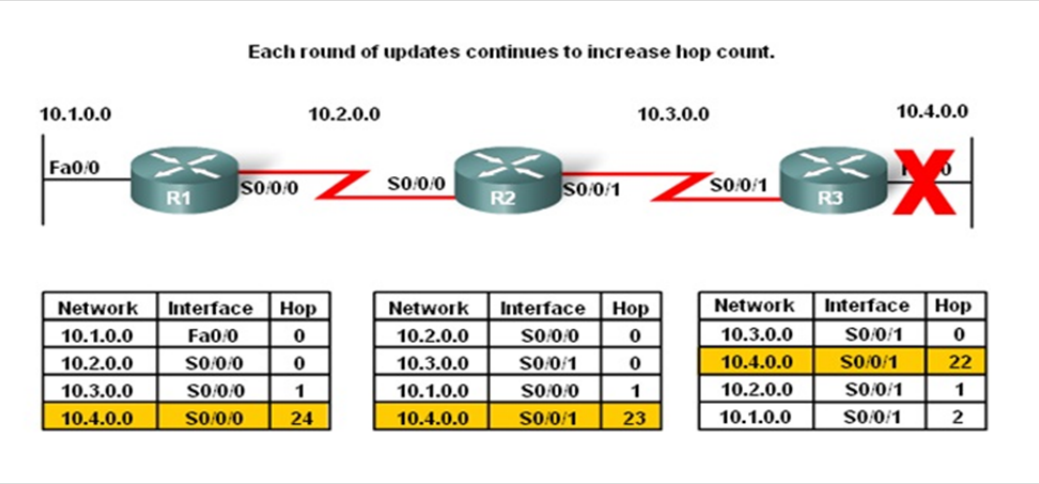

Figure 3.10: *Counting to Infinity [1]*

Hop Count is 16, 10.4.0.0 is unreachable:

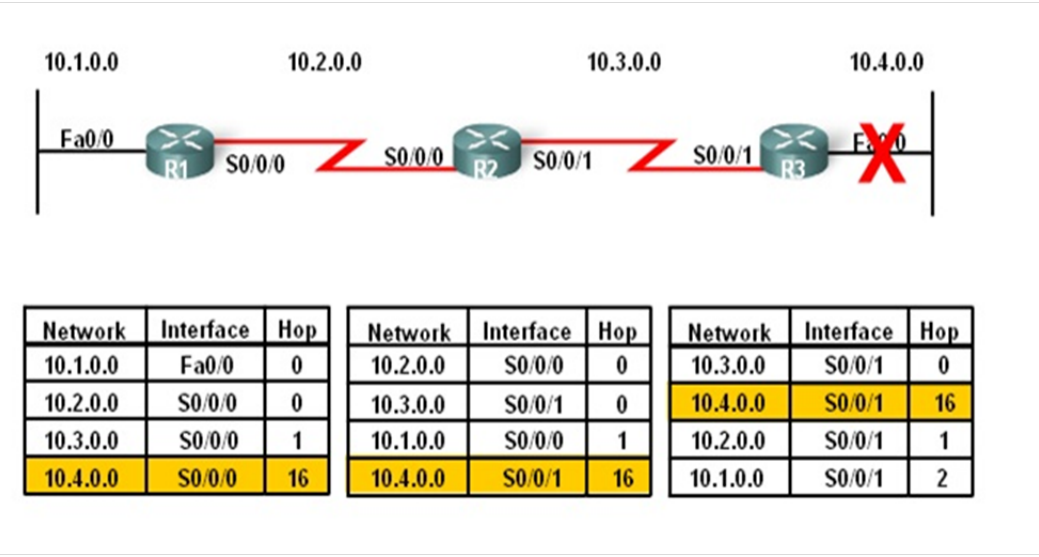

Figure 3.11: *Example of Counting to Infinity [1]*

3.1.7 Comparison

Factor used to determine that whether we go for RIP of other Distance vector protocol include the following.

- What is the network size?

- Compatibility between routers models
- Administrative knowledge.

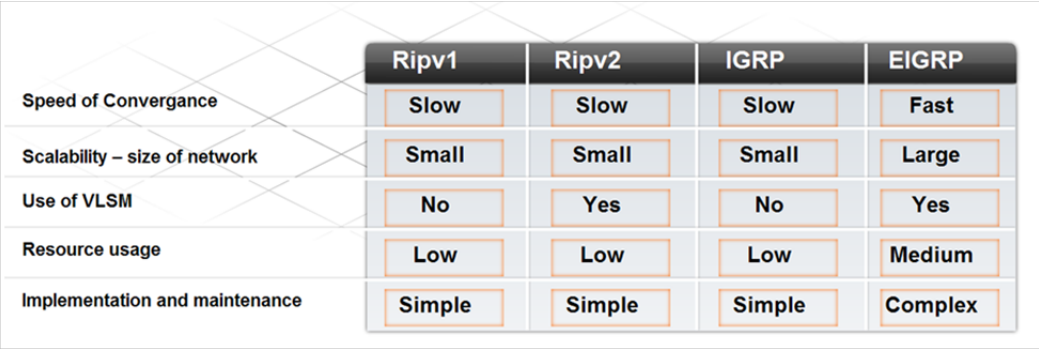

Figure 3.12: *RIP Comparison*

Above diagram can help to choose the Routing protocol for the parameter we interested more.

3.2 Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is one of the major examples of Hybrid routing protocols sometime referred as advanced DVR. EIGRP is Cisco's proprietary protocol. EIGRP provides much efficient route computation as compared to Distance Vector routing protocols. EIGRP is based on Diffusing update algorithm (DUAL). EIGRP maintains three different tables. That is

1. Neighbor Table
2. Topology Table
3. Routing Table

3.2.1 Neighbor Tables

Neighbor table contains the information of neighboring devices.

3.2.2 Topology Table

EIGRP maintains the topology table; topology table contains all the information of all the routes. For example if there are four five paths for the network

destinations, topology tables will have all the paths.

3.2.3 Routing Table

Routing table has the best path for the destination. For example if there are four or five paths in the topology table only one route out of four, five routes will be included in the routing table. EIGRP has many advantages over the link-state routing protocols because of its architecture.

EIGRP is very efficient routing protocol, it has the best of both the distance vector and link-state routing protocol. In EIGRP every router can perform route summarization, EIGRP is much simpler to implement. EIGRP has also the concept of Stub to restrict the unwanted routing updates. EIGRP uses very sophisticated routing algorithm DUAL. Just like link-state routing protocols EIGRP routing protocol is very memory and processor intensive.

3.2.4 EIGRP Features

1. EIGRP uses both the best of distance vector and liked-state routing protocols.
2. EIGRP is Class-less protocol.
3. There isn't any need of route redistribution with IGRP the predecessor of EIGRP.
4. EIGRP metric and IGRP metrics are directly translate able.
5. Convergence is very fast.
6. Uses partial updates when needed.
7. Consumes less bandwidths (no broadcasts, no periodic updates, updates contain only changes)
8. Supports multiple network layer protocols like IP,Apple Talk and IPX/SPX etc. EIGRP Operation

3.3 Open Shortest Path First (OSPF)

There are two routing protocols that link-state OSPF and integrated IS-IS. Link-state routing protocols use SPF (Shortest Path First Algorithm) knows as Di-

jkstra's Algorithm. Integrated IS-IS however uses SPF only for finding all routers in an area and runs Partial Route Calculation (PRC) algorithm for IP reach ability. On the other hand OSPF runs only Dijkstra's Algorithm. OSPF have the following detail in the packet.

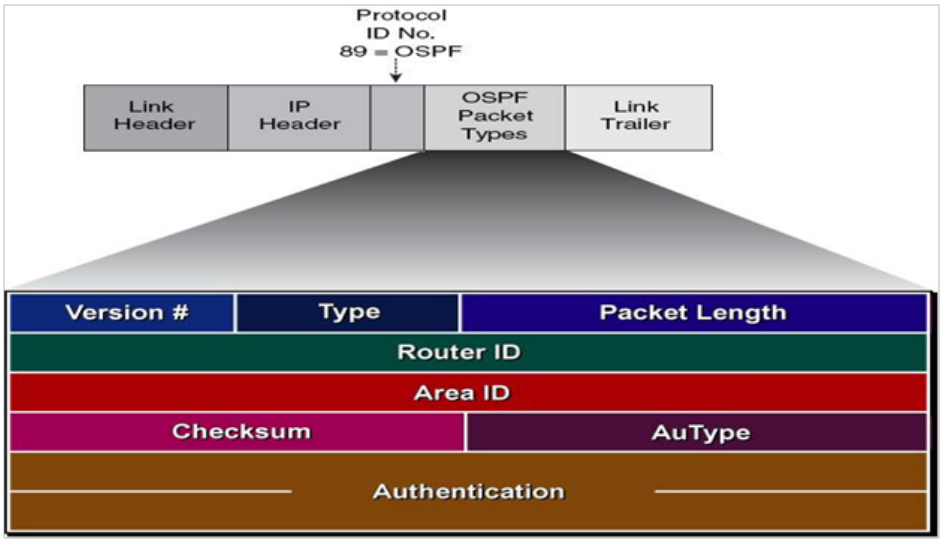

Figure 3.13: *OSPF Packet Format [8]*

OSPF maintains three tables which help OSPF to work efficiently:

- Routing Table
- Topology Table
- Neighbor Table

3.3.1 Routing Table

Routing table is a table that keeps the track of all Subnets so that it can transport packets to required destination. It uses the shortest path first (SPF) algorithm to populate the routing table.

3.3.2 Topology Table

Topology Table is also known as Link-stat table. This table has the information of every link in network. Keep the track of whole network. Below is the detail view of Topology Table.

3.3.3 Neighbor Table:

Neighbor Table has all the neighbor detail which is running OSPF. It contains all the required information about neighbor that is required for communication.

Updates in OSPF are triggered and incremental which means it will only send update LSU packet when there is a change in a network. However, OSPF sends complete routing table information to its like DV routing protocol after every 30min, also known as LS refresh.

3.3.4 OSPF Area Design and Principles

OSPF area design is hierarchical which means every area must connect to Backbone Area 0. Routers that connect two areas are termed as ABR and routers on which redistribution or other AS connect to be termed as ASBR. Routers in a particular area maintain a same topology table that is, they have same link-state database. Principle behind area design is to localize update within that area.

3.3.5 OSPF Neighbor Formation

OSPF neighbor formation is an eight step process.

1. OSPF router-id is determined. On an OSPF enabled router router-id is the highest IP address on the physical interface, loopback IP-address if configured beats the physical IP-address. Good design suggests that router-id should be hardcoded under the routing process.
2. OSPF adds the interface that is directed by a network command, in its link-state database.
3. DOWN state. In this state OSPF send hello packet on OSPF enabled interfaces. Hello packet contains information like Neighbor, authentication, Router-id, Area-id, Network mask, DR/BDR address, Hello and dead intervals.
4. INIT state. In this state OSPF check for the fields in hello packet that are Hello and Dead interval, Area-id, Authentication passwork and Network masks. If any of them do not match the relation between routers keeps bouncing between DOWN and INIT.
5. 2-WAY stat. In this OSPF checks the neighboring router-id and if they are already neighbors the simply reset their dead intervals. If they are not

neighbor already then the process to next state.

6. EX START state. In this DBD packets or exchanged. DBD contains cliff notes of all the networks that in the database. Master slave relation is formed first and after that master router sends its DBD packet first.

7. LOADING state. In this state DBD are saved and acknowledged. Both routers check for sequence number in DBD and check it against its database. If a prefix is missing a LSR is sent to the other router, SLAVE sends LSR first because it gets DBD first. LSU is sent back in response to LSR with detailed information of the missing prefix.

8. FULL state. In this neighbors are synchronized and after that Dijkstra's algorithm runs.

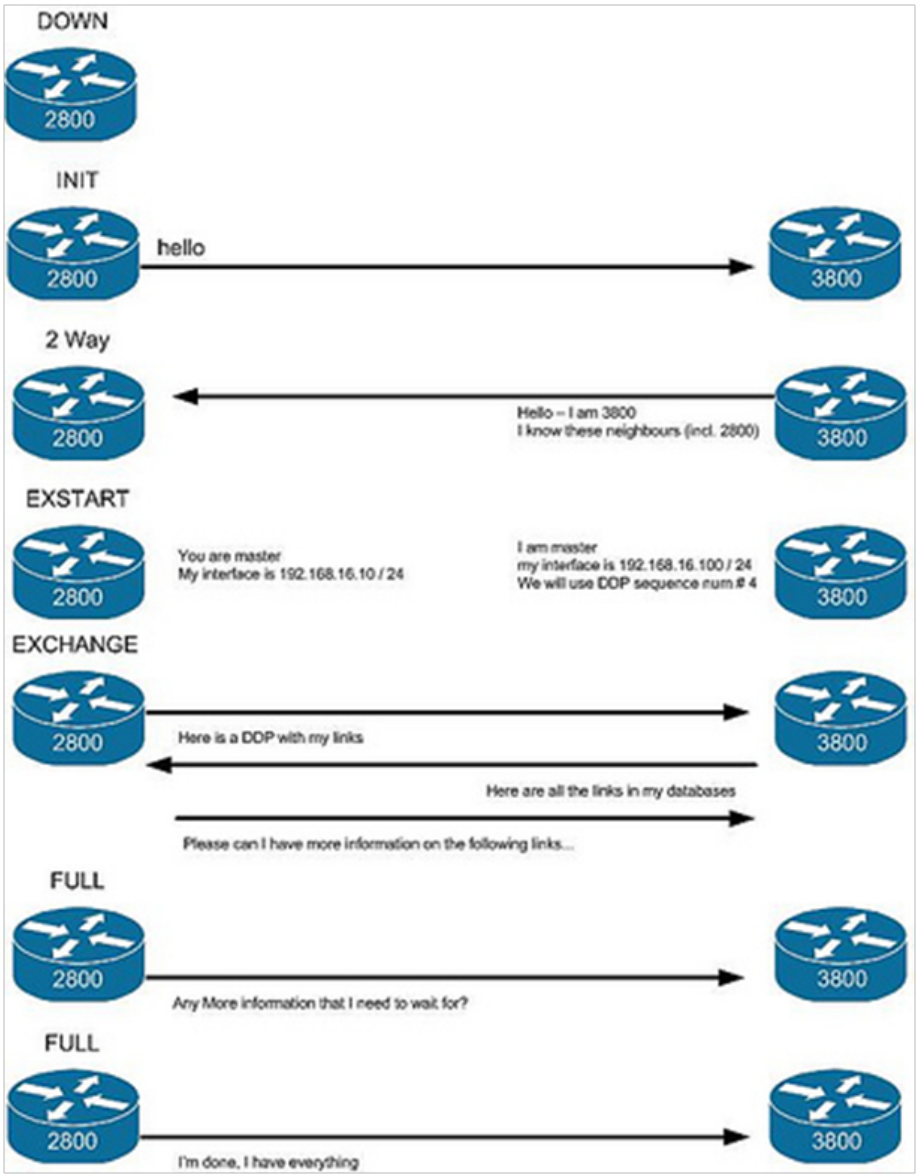

Figure 3.14: *OSPF Neighbor Formation [8]*

3.3.6 OSPF Packet Types

- Hello Packet
- Database Description Packet (DBD)
- Link-State Request (LSR)
- Link-State Advertisement (LSA)
- Link-State Update (LSU)
- Link-State Acknowledgement (LSACK)

Figure 3.15: *OSPF Packet Types [8]*

3.3.6.1 Types of LSAs

- LSA TYPE 1: Within area local routes are represent by type 1. These are just Hello packets that router exchange to each other after specific interval. Light green arrows in figure represent LSA TYPE 1.
- LSA TYPE 2: These are the packets that DR send to other routers in the Area. Light green arrows in figure represent LSA TYPE 2.
- LSA TYPE 3: ABR advertise these routes. These are inter-area routes. In routing table they represent by O IA. Blue arrows in figure represent LSA TYPE 3.

- LSA TYPE 4: ABR advertise Packets which is known is LSA type 4.It helps other router to know router ASBR location. Green broken arrows in figure represent LSA TYPE 4.
- LSA TYPE 5: Such types of routes are the external routes that are being advertised by ASBR to an area. Purple arrows in figure represent LSA TYPE 5.
-
- LSA TYPE 7: The Type 7 LSAs, NSSA, is when the Stub area is receiving routes that are redistributed within its area. Red arrows figure represent LSA TYPE 7.

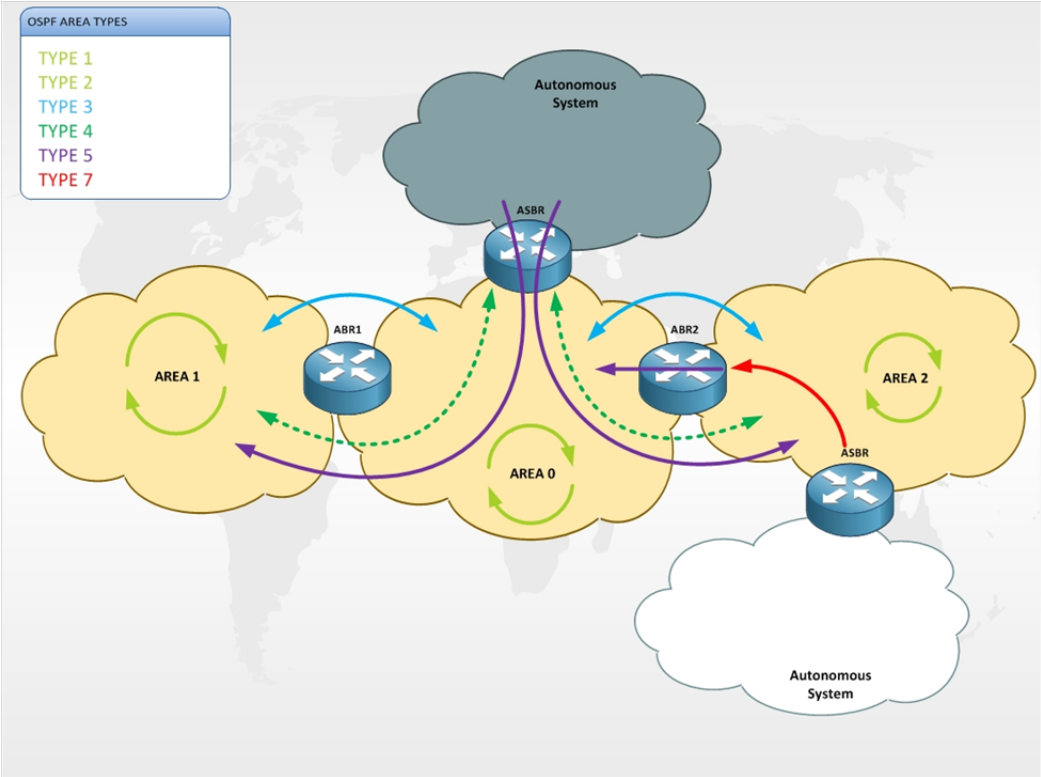

Figure 3.16: *LSA Types [8]*

3.3.7 OSPF Cost

OSPF finds cost of a particular based upon its bandwidth. Formula for cost calculation is 100/BW in Mbps, this means it has certain limitations e.g. Cost for 10 Meg link will be 10 and for 100 Meg will be 1 and 1 Gig will also be one 1. Auto cost reference changes that phenomena and allows us to adjust the cost formula.

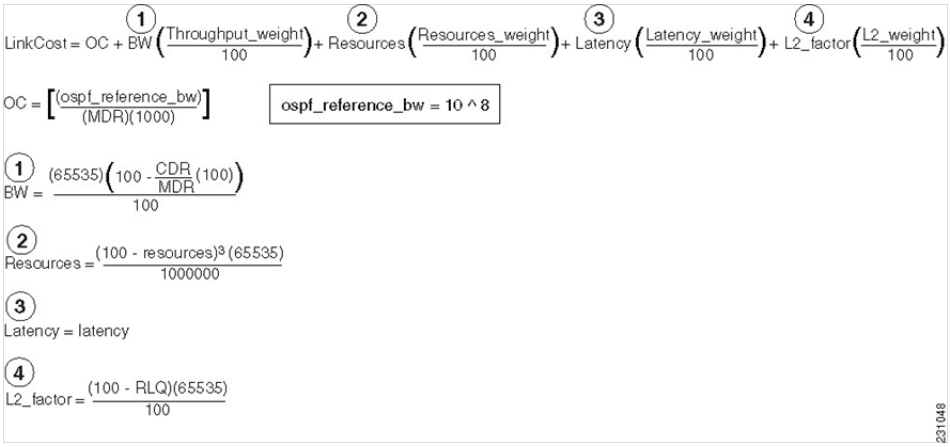

Figure 3.17: *OSPF Algorithm [8]*

3.3.8 Understanding DR and BDR

OSPF elects DR and a BDR on a shared segment. This is done on purpose to get rid of redundant network updates for a single update. DR is the router with the highest priority. DR and BDR role is critical when we into NBMA where particular router(hub) must be manually configured as DR. FULL relation-ship is formed between DR/BDR and every other router in a shared segment.2-way relation-ship is formed be other.224.0.0.5 and 224.0.0.6 are the two multicast address used to send update. Non-DR send updates on 224.0.0.6 which DR listens to , DR then sends that update on 224.0.0.5 which all routers listen.

3.3.9 OSPF Virtual Link

OSPF design requires all routers to be physically connected to Area 0. In this situation the routes of that areas are not advertise to any other area. If we run into a situation where our area does not connect to backbone we can use virtual links or GRE tunnels. Virtual link increases the domain to Area 0. Virtual link however, solve our problem but it is not a reliable solution so, re-designing should be done.

3.3.10 OSPF Summarization

Summarization in OSPF is restricted to two either ABR OR ASBR. It allows updates to be localized to a certain area. Summarization is done under the routing process. We can manually change the cost of summary routes. AREA RANGE XX command on ABR and SUMMARY-ADDRESS command on ASBR is used

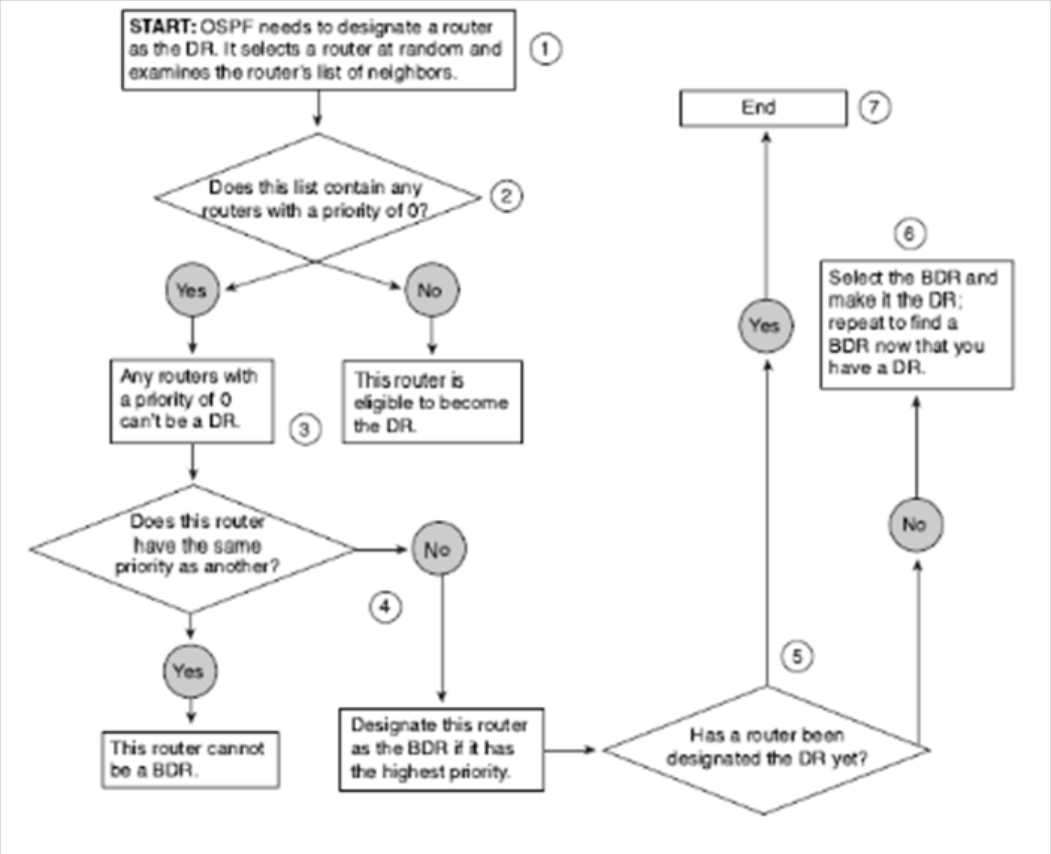

Figure 3.18: *DR, BDR Selection [8]*

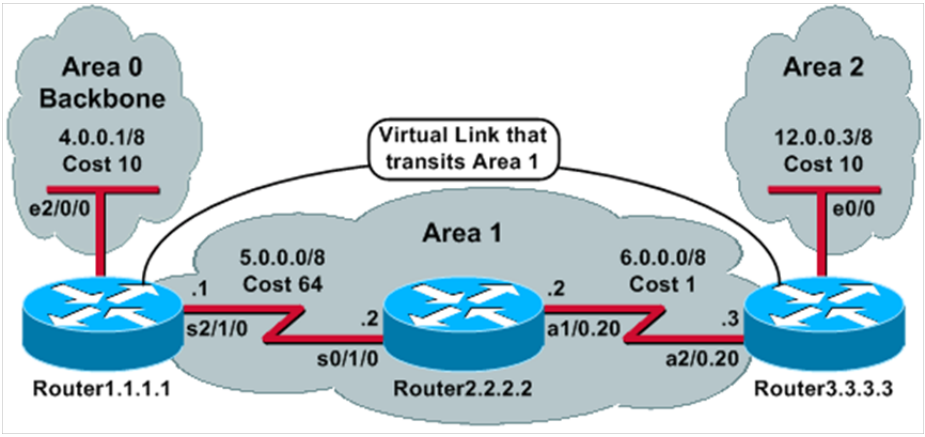

Figure 3.19: *OSFP Virtual Links [8]*

to summarize.

Redistribution on the other hand can be done on ASBR only. OSPF redistributes on class full boundary so subnet keyword must be entered while redistributing into OSPF. By default OSPF sets the cost of 20 and external type-2. Route-map can be referenced to tag routes as well as their default parameters can also be overridden.

3.3.11 OSPF Route Filtering

Filtering can be done using distribute-list on a router but this only removes a route from its routing table, OSPF database still retains and forwards the info to neighboring routers. Distribute-list if configured on ABR that connect area 0 to other areas removes a network not only from routing table but also link-state database. Only scenario where distribute list can be configured in out bound direction is ASBR for external redistributed routes, when it is done the routes are also removed from link-state database. LSA Type-3 summary routes cannot be filtered on an ABR. Database filtering can also is accomplished on a particular interface.

3.3.12 OSPF Area Types

There are different areas in OSPF depending upon the design requirements of a network.

- OSPF STUB AREA: LSA Type-4 and 5 routes will not be propagated into a stub area. ABR Installs a default routes into a stud for the reachability of external routes.
- OSPF TOTALLY STUB: LSA Type 3 in addition to type 4 and 5 is not propagated into this kind of area. This area will only maintain intra area routes and a default route injected from ABR.
- OSPF NSSA: LSA Type-4 and 5 are not allowed in this area but we can redistribute into this area. External routes will be propagated as LSA Type-7 (NS1 or NS2) and ABR converts those into LSA Type-5 (E1 OR E2) and advertise to other areas. Default route in not advertised but, we can make ABR advertise the default route.
- OSPF NSSA TOTALLY STUBBY AREA: LSA Type-3 in addition to LSA Type-4 and 5 are not propagated into these areas. This area will only maintain intra area route plus LSA Type-7 route.

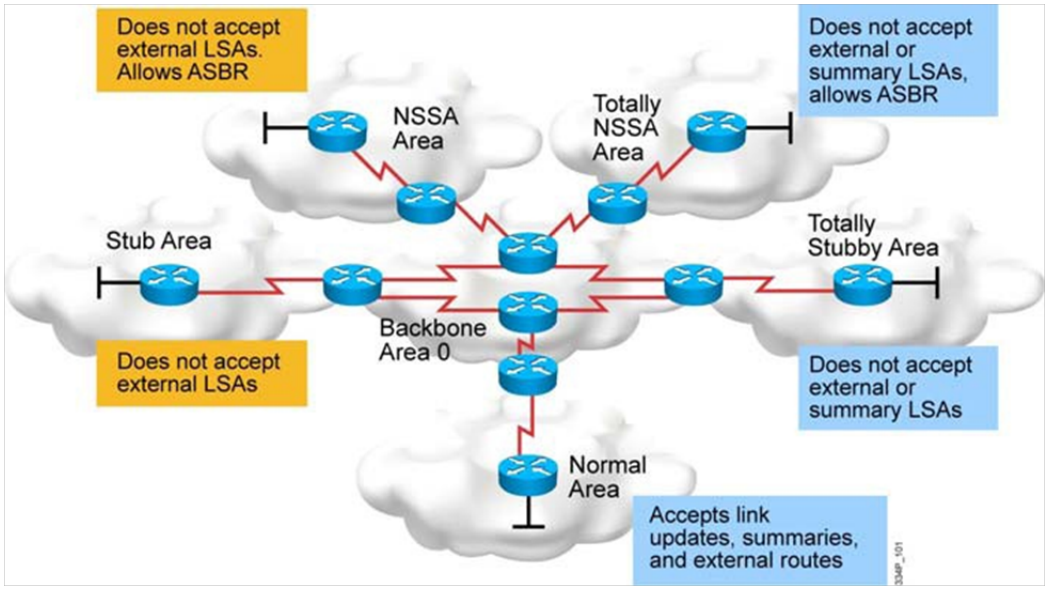

Figure 3.20: *OSFP Area Types [8]*

Chapter 4
Simulation Results

4

Simulation Results

4.1 Simulation Environment

In this thesis, network simulator, Optimized Network Engineering Tools (OPNET) modeler 14.0 has been used as a simulation environment. OPNET is a simulator built on top of discrete event system (DES) and it simulates the system behavior by modeling each event in the system and processes it through user defined processes [23]. OPNET is very powerful software to simulate heterogeneous network with various protocols.

4.1.1 OPNET Structure

OPNET is a high level user interface that is built as of C and C + + source code with huge library of OPNET function [24].

4.1.1.1 Hierarchical Structure

OPNET model is divided into three domains [24]. These are:

1. Network domain: Physical connection, interconnection and configuration can be included in the network model. It represents over all system such as network, sub-network on the geographical map to be simulated.
2. Node Domain: Node domain is an internal infrastructure of the network domain. Node can be routers, workstations, satellite and so on.
3. Process Domain: Process domain are used to specify the attribute of the processor and queue model by using source code C and C ++ which is inside

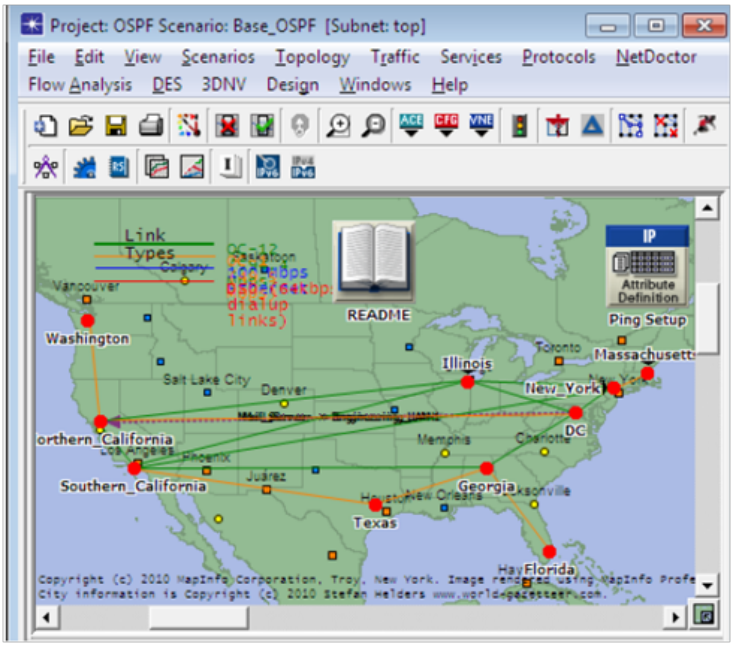

Figure 4.1: *Network Domain*

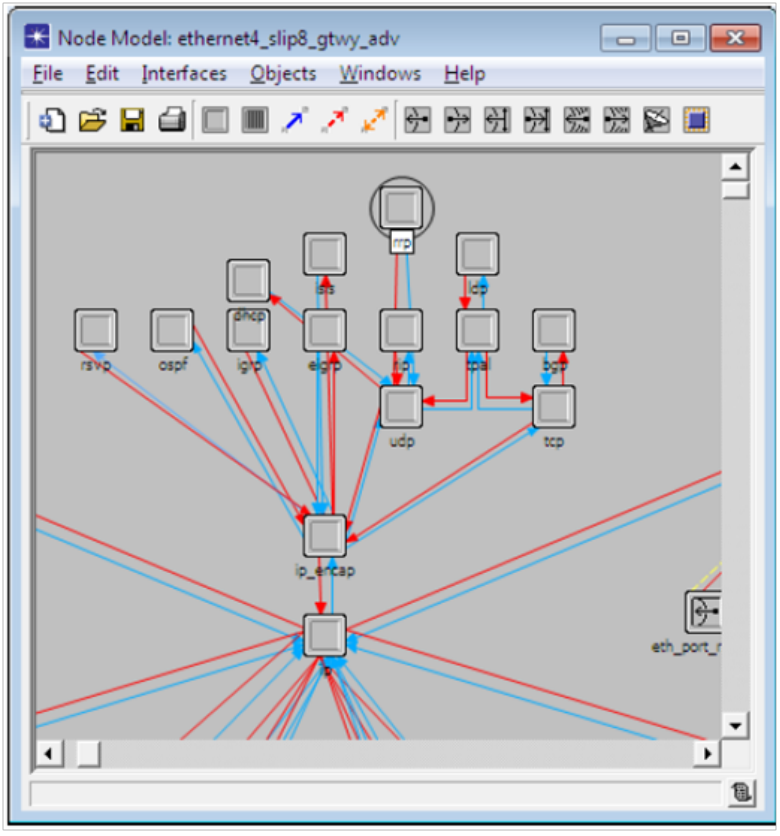

Figure 4.2: *Node Domain*

the node models.

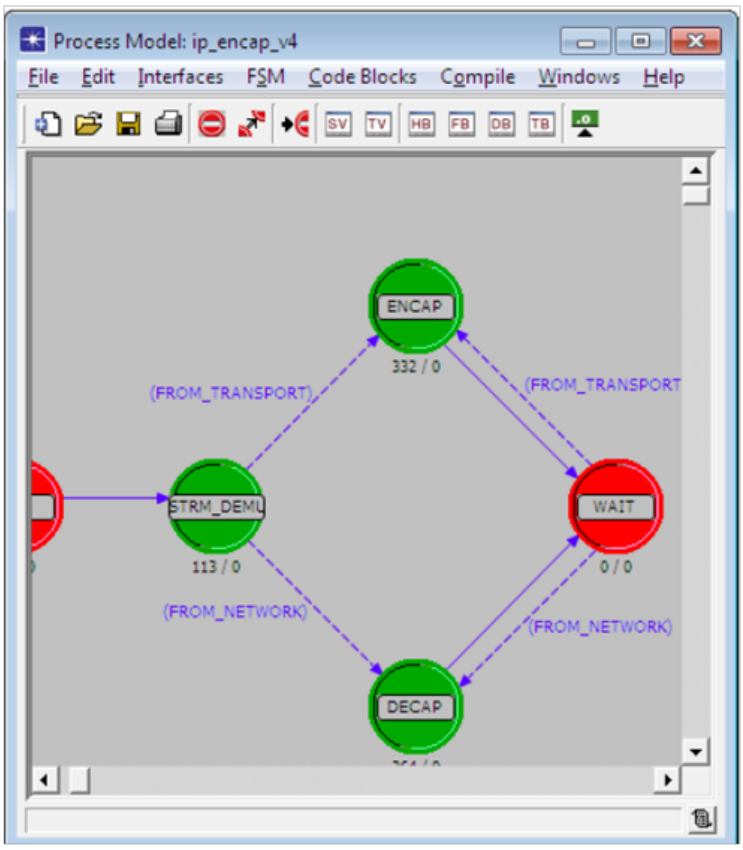

Figure 4.3: *Process Domain*

4.1.2 How to Analyze and Design in OPNET

When implementing a real model of the system in the OPNET, some steps are to be followed to design on simulator. Figure 5.1 shows a flow chart of the steps [3].

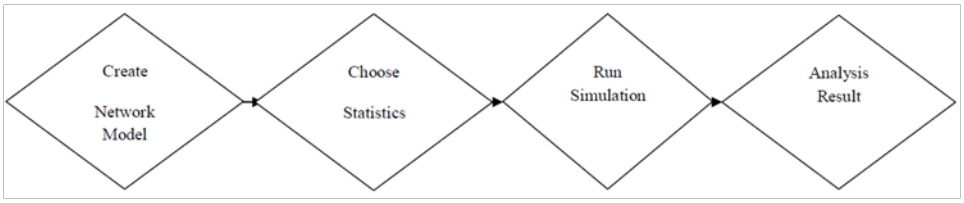

Figure 4.4: *Flow Chart of Design*

4.1.3 OPNET Environment

We used OPNET Modeler version 14.0.A for network simulations. OPNET is a comprehensive network simulation tool with a multitude of powerful functions. It enables simulation of heterogeneous networks by employing a various protocols [2].

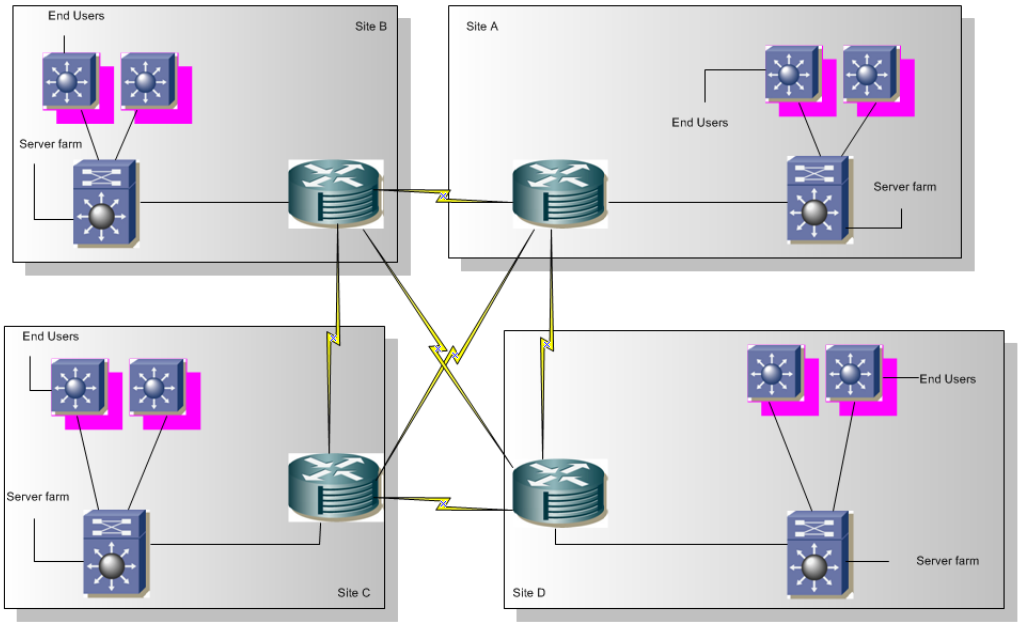

Figure 4.5: *Network Design*

We have simulated a real time network of Company XYZ. We have four offices connected together in full mesh topology. We have followed the Cisco's recommended three layer hierarchical model. That is

- Core
- Distribution
- Access

Cisco 7609 router is used as Core router at each office. All these offices connected using E1 connections. All the relevant configuration regarding the IP configurations and also routing related configuration done and tested. At each branch 6509 Core switch is deployed as Core Switch and 6506 used as aggregation switches. We have used Cisco 2960 Switch as an Access Switch. All the access switches configured with Hot Standby Routing Protocol to make sure the high availability.

The first simulated network employs the RIP routing. The same model is then used to simulate EIGRP and the OSPF routing protocol. The three scenarios are: "RIP no fail", "EIGRP no fail", and "OSPF no fail". We added the failure/recovery setting (the link between Subnet1 and Subnet5 fails at 300 s and recovers at 500 s) to each scenario and created three additional scenarios named: RIP, EIGRP, and OSPF

4.2 Simulation Results

We simulated the network convergence activity and protocol traffic using six simulation scenarios. The RIP, EIGRP, and OSPF protocol are chosen under global statistics.

Network Convergence: Our study of network convergence scenario concludes that EIGRP has the shortest convergence time whereas OSPF experience the longest convergence period. RIP convergence time is better than OSPF. It shows that EIGRP is much better due to its hybrid nature and DUAL algorithm. RIP is better than OSPF because it has a simple design and limited functionality. OSPF will take definitely need some time to calculate and convergence because it is design for big networks and using SPF algorithm and have sophisticated selection of DR and BDR in every LAN segment. The EIGRP and the OSPF protocol experience the shortest and the longest network convergence times, respectively.

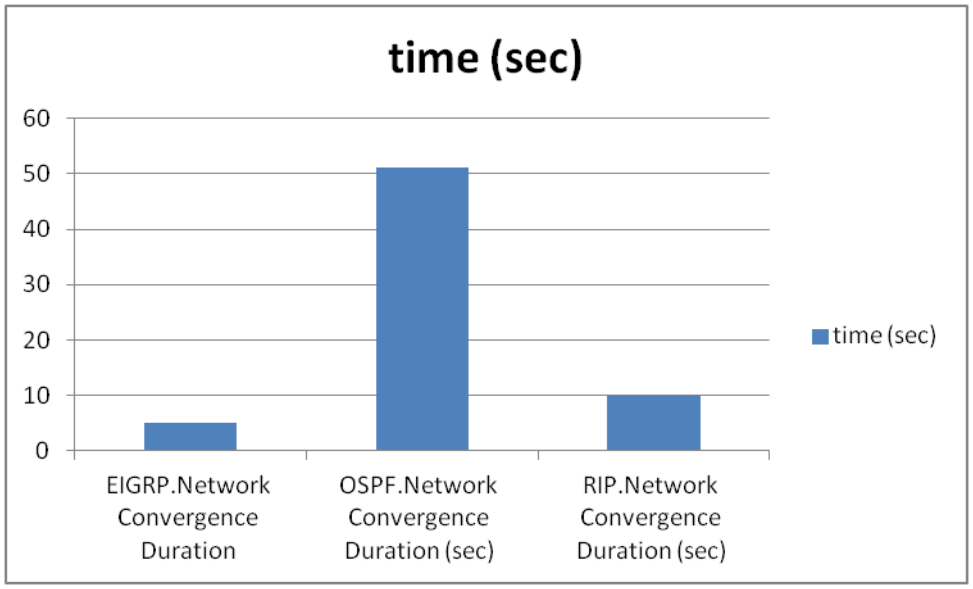

Figure 4.6: *Convergence Time*

EIGRP is very good in convergence because of its hybrid nature. OSPF take more time than the rest of two because of its hierarchical structure and complex criteria in selecting DR, BDR in every LAN segment. RIP need less time as compare to OSPF because it is a simple protocol ever exist. It follows really simple parameter and somehow its shows better result than OSPF. So above result can help in selecting protocol as our design demand.

In case of no link failure in OSPF shows the most traffic sent. The reason of this result is that due to packet header size and biggest conversion time OSPF took more time to send traffic update as compared with EIGRP and RIP. EIGRP

is the fastest routing protocol used in this simulation to sent traffic update because of its very fast convergence time; also RIP was the second to send traffic update because of its better convergence time than OSPF.

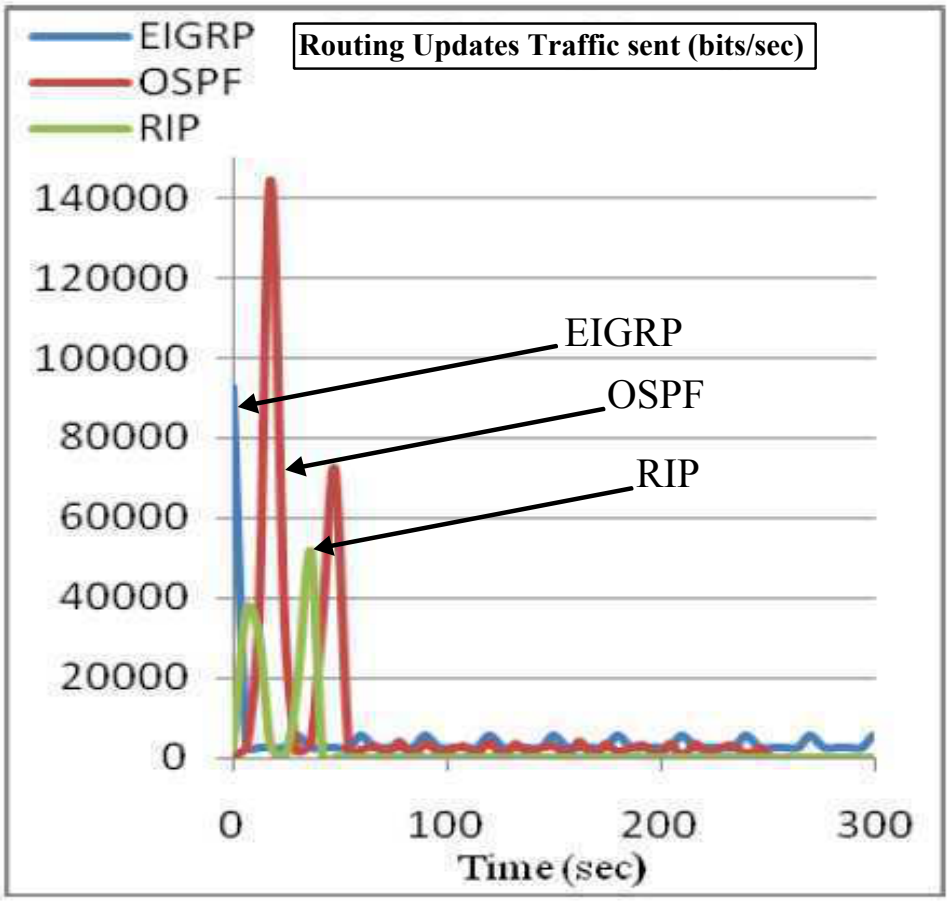

Figure 4.7: *Routing Updates Traffic Sent*

Same test was conducted with the node failure; with the node failure EIGRP provided better results than that of OSPF.

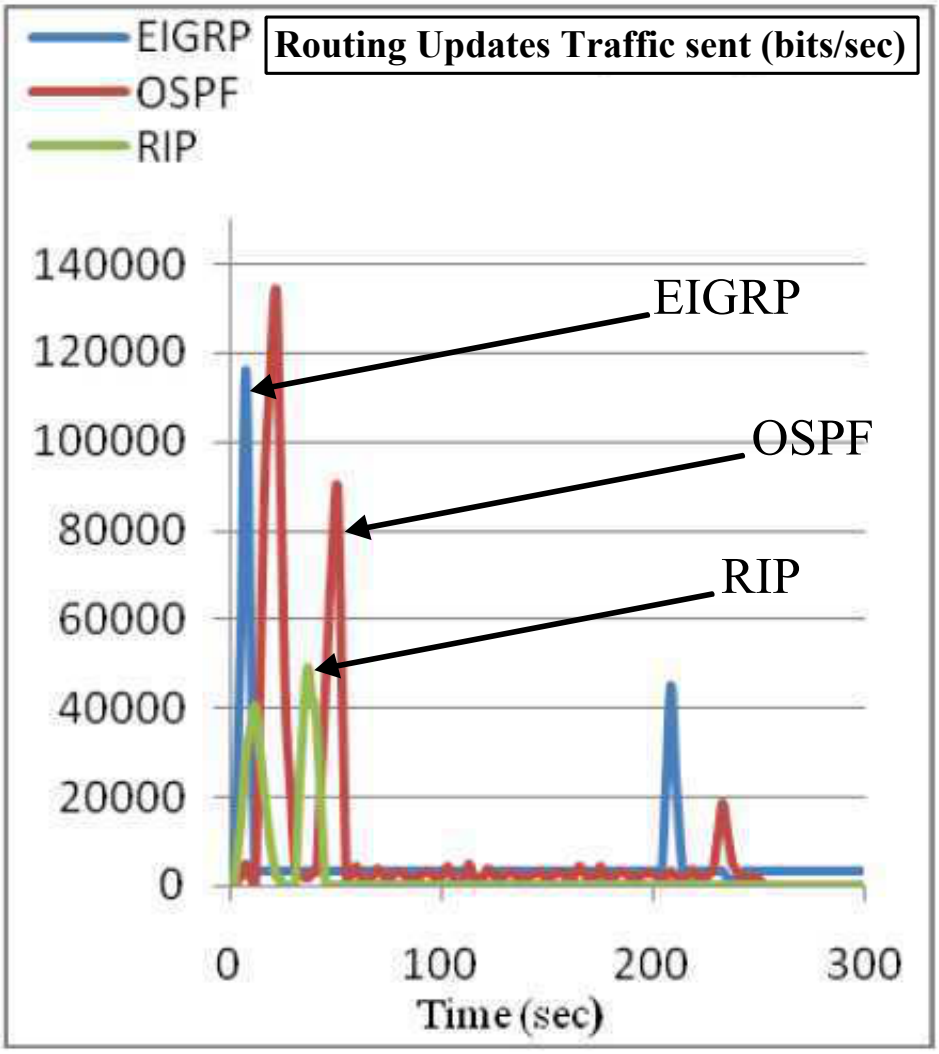

Figure 4.8: *Routing Updates Traffic Sent After Failure*

OSPF shown better results in case of delay variation. OSPF had better results for the end -to-end delay and RIP shows the worst results for end-to-end delay. EIGRP was slightly better than RIP for end-to-end delay. EIGRP delay was much closed to the OSPF delay. EIGRP and OSPF better results than RIP.

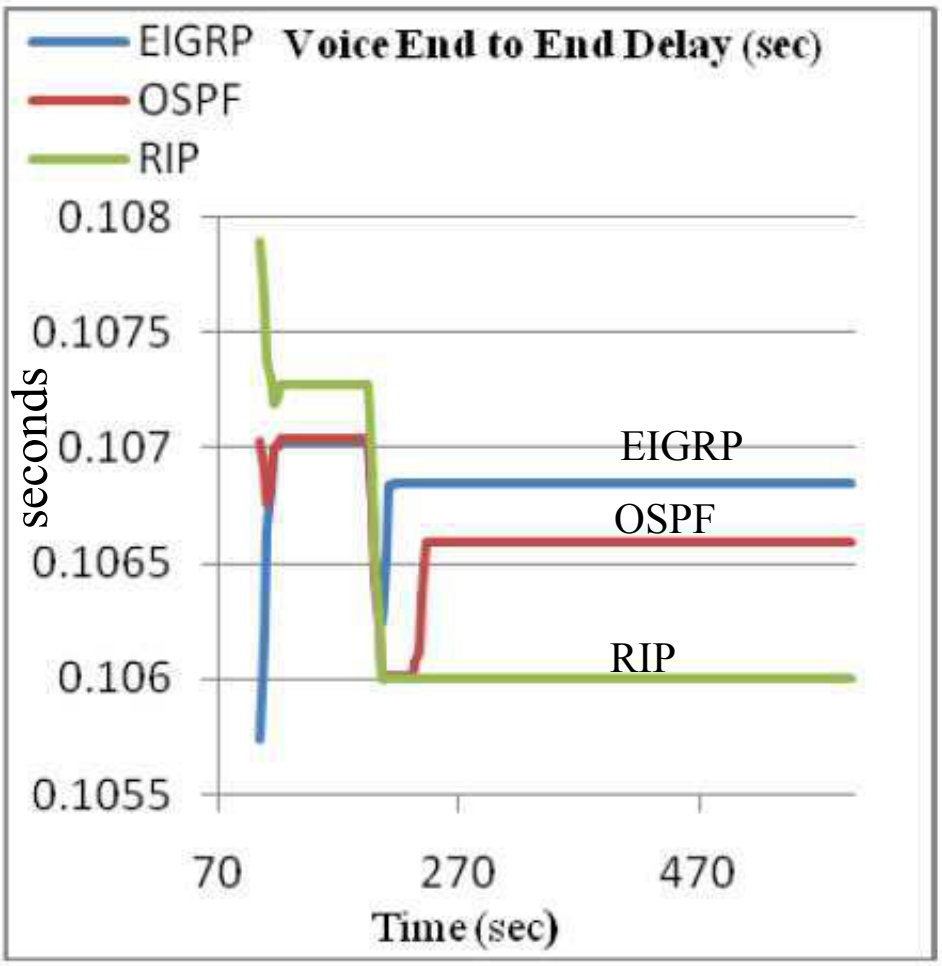

Figure 4.9: *Voice End-to-End Delay*

OSPF response after the link failure is less than the EIGRP.

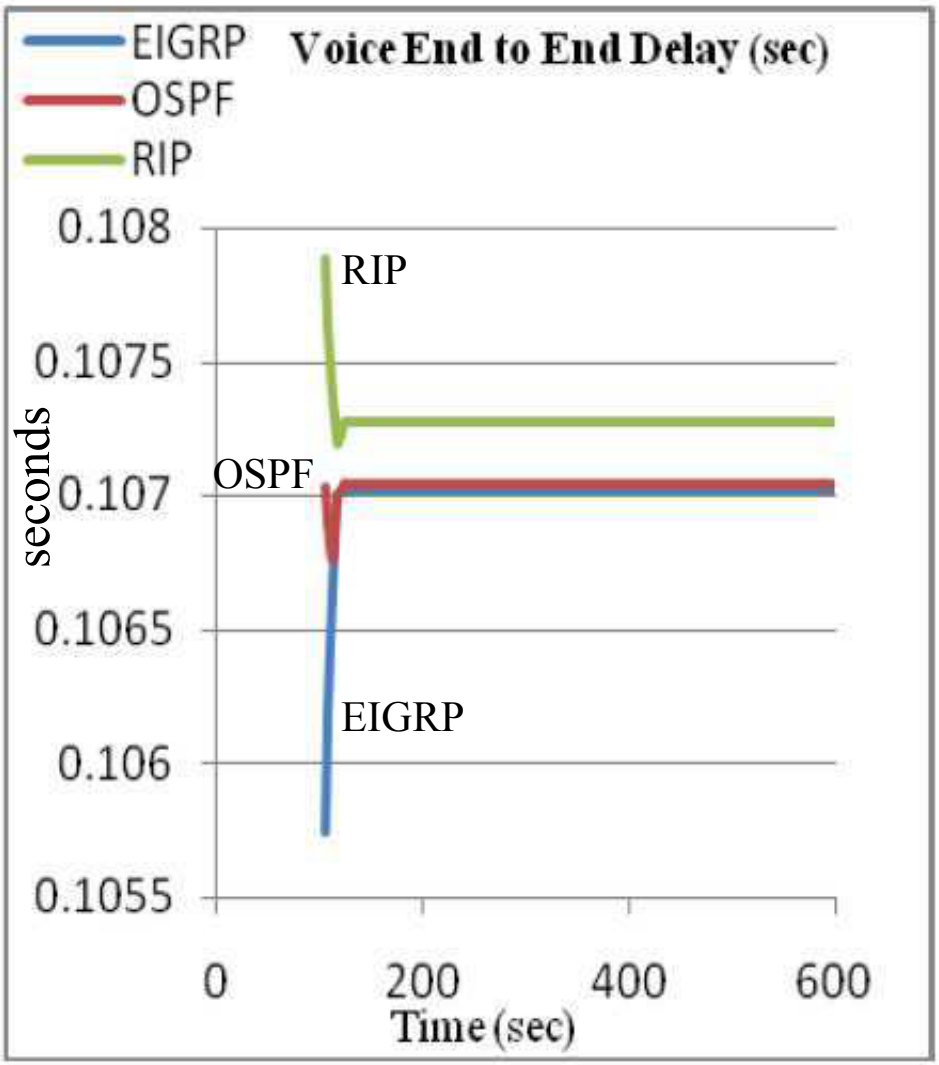

Figure 4.10: *Voice End-to-End Delay After Failure*

As for as delay variation results is concerned EIGRP and RIP shown almost similar results unlike OSPF which shows higher delay variations in the beginning but after the steady state achieved all these routing protocols shows similar sort of results.

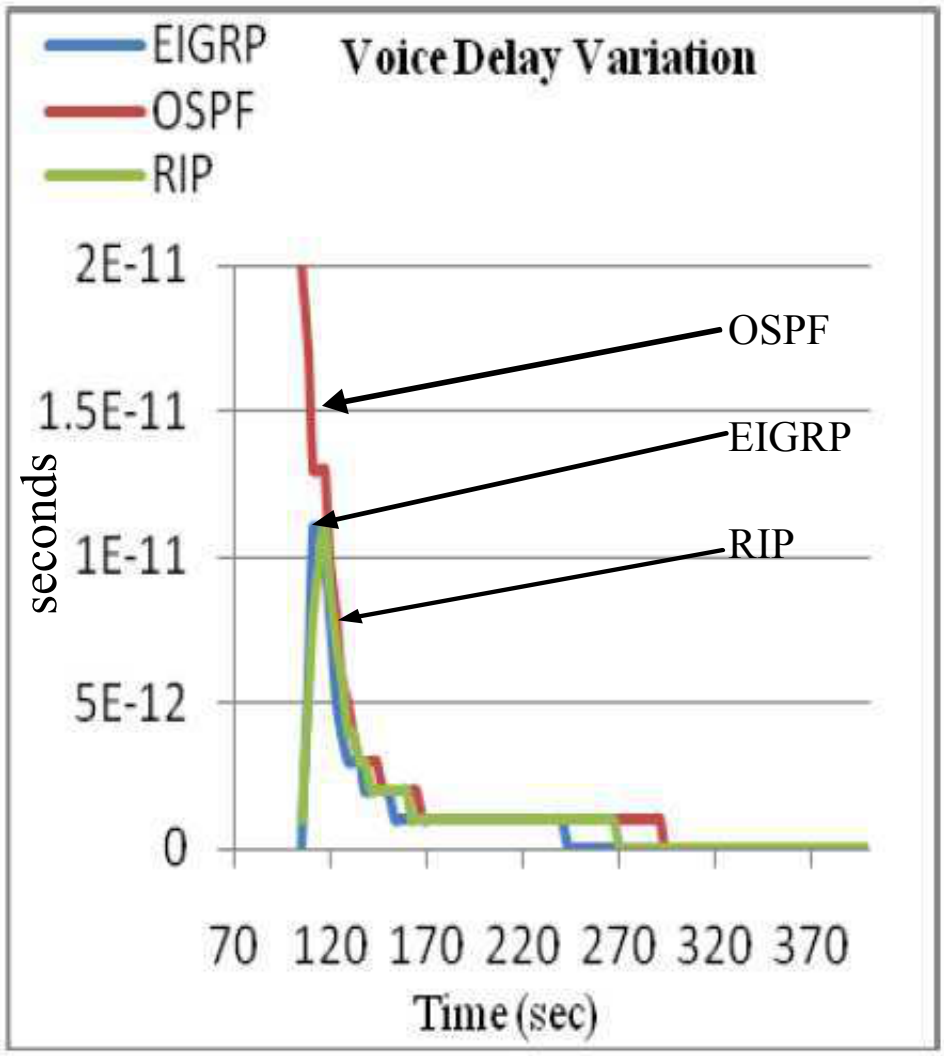

Figure 4.11: *Voice Packet Delay Variation*

For the Voice packet traffic sent; voice traffic sent activity is not affected by delay, jitter, and delay variation. All of these routing protocols shown similar results.

Chapter 5
Conclusions

5

Conclusions

Interior dynamic routing protocols like OSPF and EIGRP are heavily used in industry along with Routing information protocol (RIP). In this thesis we have analyzed the behavior of all these routing protocols using different test scenarios for the real time applications. Performance of all these protocols tested on the basis of attributes associated with these protocols to figure out which of the routing protocol best fit the industry requirements for the real time applications.

Enhanced Interior Gateway routing protocol (EIGRP) which is Cisco's propriety routing protocol has the best result in case of convergence duration and for the same topology EIGRP was the first to converge. EIGRP has the best way out in case of link or node failure, because of its topology database and concept of successor and feasible successor. Therefore we can say that EIGRP is much reliable for the real time applications. For routing traffic Enhanced Interior Gateway Routing Protocol was the first one to send traffic. Routing Information protocol had the slightest traffic. Because RIP only sends the number of hops information. Whereas, OSPF with the most traffic sent and was the last one to send routing traffic. EIGRP has the mechanism to send traffic very fast after link failure as compared with the OSPF. OSPF shown better results in case of delay variation. OSPF had better results for the end -to-end delay and RIP shows the worst results for end-to-end delay. EIGRP was slightly better than RIP for end-to-end delay.

One of the best things about OSPF is its area design and hierarchical structure, by doing so we can manage the routing table size, less amount of route processing and memory usage. On the contrary, areas increase the amount of configuration and also very sophisticated configuration required to obtain the best out of it. OSPF area design also help reducing the connectivity and increasing the traffic concentration. OSPF is widely used interior gateway routing protocols because of

its design and the amount of liberty in design and enhances the network efficiency by reducing the unwanted routing updates and by maintain the different tables.

References

References

[1] Rick Graziani and Allan Jonson, "Routing protocols and concepts: CCNA exploration companion guide," Pearson Education. London, 2008.

[2] Mohammad Nazrul Islam, Md. Ahsan Ullah Ashiqu, Simulation Based EIGRP over OSPF Performance Analysis, Master Thesis in Electrical Engineering Emphasis on Telecommunications Thesis no: 4983 May 14, 2010

[3] Dong (Don) Xu, OSPF, EIGRP AND RIP PEFORMANCE ANALYSIS BASED ON OPNET, ENSC835: COMMUNICATION NETWORKS, SPRING 2011

[4] Cisco Systems, I., Cisco Networking Academy Program CCNA 1 and 2 Companion Guide Third Edition.

[5] Routing Overview available at: http://networking.ringofsaturn.com/IP/Routing.php

[6] Moy, John. OSPF Anatomy of an internet routing protocol. May 200.

[7] Tanenbaum, Andrew s. Computer Networks. s.l.: Pearson Education, 2003.

[8] Berkowitz,Howard.http://www.certificationzone.com/cisco/studyguides/component.html?m OSPF Part 2: Using OSPF in Hierarchical Systems.

[9]] IKram Ud Din, Saeed Mahfooz and Muhammad Adnan ,Analysis of the Routing Protocols in Real Time Transmission, Global Journal of Computer Science and Technology, Vol. 10 Issue 5 Ver. 1.0 July 2010 p.18-22

[10]] Network Working Group at: http://www.ietf.org/rfc/rfc2328.txt

[11] Internetworking Technologies Handbook Fourth Edition

[12] Mohammed A. Aabed RoutingInOPNET(30/11/2008)