PERFORMANCE EVALUATION OF ROUTING PROTOCOLS

By
ELBADAWI GALAL ELBADAWI MOHAMMED
INDEX NO. 054020

Supervisor
Dr. HAMEED A. ALI

A REPORT SUBMITTED TO
University of Khartoum
In partial fulfillment of the requirements for the degree of
B. Sc (HONS) Electrical and Electronic Engineering
(COMMUNICATION ENGINEERING)
Faculty of Engineering
Department of Electrical and Electronic Engineering
July 2010
DEDICATION

To my father and mother

To my brothers and sisters

To all my friends
ACKNOWLEDGMENT

In the name of Allah, the Most Beneficent and the Most Merciful.
By Allah's will the completion of this work has become a reality. I start by thanking Allah for assisting and guiding me in this work. I thank Allah for giving me the confidence and patience to finish this work.

I want to thank Dr. Hamid A. Ali for supervising my project with all patience, authenticity, help, advice and leadership.

Also I want to thank my brother and project’s partner Zafir Al. shareef
ABSTRACT

Due to the huge number of routers and hosts in the internet, internet was divided into areas called (autonomous systems) or (ASs) each run under the same administrative authority. Inside the autonomous system the administrators have many choices of routing protocols to run. To select one among these choices, they must be compared with each to determine the best protocol to be used.

There are a lot of metrics to evaluate and compare the performance of routing protocols; the amount of traffic generated by each protocol, the traffic dropped by each protocol in case of link failure, the bandwidth consumed by the protocol, the delay caused by the protocol messages,…etc.

In this project, the OPNET modeler version 14 was used to evaluate and compare the performance of routing protocols.

First simulation compares the traffic generated by RIP, IGRP, OSPF and EIGRP, the second simulation evaluate the performance of distance vector protocols in the case of a topology changes, the third and fourth simulations show how the performance of the RIP can be improved by enabling the auto summary and the triggered extension mode .

From the simulation results it has been found that:

- The Enhanced Gateway Routing Protocol (IGRP) is the protocol that consumes the least bandwidth due to its small generated traffic when compared with the other routing protocols, and the EIGRP give the best performance in the case of topological changes due to its fast convergence time, the will make the EIGRP is the best choice to be used as an interior gateway routing protocol.

- The Enhanced Gateway Routing Protocol (IGRP) can only be used in CISCO routers, so in the case of the networks that use routers from other manufacturers, the OSPF will be a good choice because it has give the second best performance.
The routing information protocol RIP generate high periodic traffic that can cause congestion to the slow networks, but its performance can be improved by enabling the auto summary and the triggered extension mode which lead to a significant decrement in the traffic generated by the RIP.
المستخلص
نظرا للمدى الكبير من الموجهات في شبكة الإنترنت تم تقسيم الشبكة إلى مناطق أصغر تسمى مناطق الحكم الذاتي، وكل منطقة من مناطق الحكم الذاتي تخضع للسلطة الإدارية نفسها، وللسلطة الإدارية العديد من الخيارات المتاحة من بروتوكولات التسبيير، للحصول على الاختيار الأفضل يجب مقارنة اداء هذه البروتوكولات مع بعضها.

هناك العديد من المقاييس لمقارنة اداء هذه البروتوكولات منها مقدار البيانات المصادر عن كل بروتوكول الذي قد يؤدي إلى ازدحام الشبكة والتأثير الناجح عن هذه البيانات، والبيانات المفقودة في حالة حدوث تغير في الشبكة مثل فشل وصلة من الاتصالات.

استخدم برنامج محاكاة لمقارنة اداء هذه البروتوكولات مع بعضها.

في المحاكاة الأولى تم مقارنة حركة البيانات المصادر من كل بروتوكول وفي المحاكاة الثانية تم مقارنة البيانات المفقودة من كل بروتوكول في حالة فشل وصلة من الاتصالات. وفي المحاكاة الثالثة والرابعة تمت محاكاة طرق لتحسين اداء بروتوكول معلومات التسبيير من نتائج المحاكاة تم الوصول إلى الآتي:

يولد بروتوكول البوابة الداخلية المحسن قمية من البيانات ويفقد أقل كمية من البيانات في حالة فشل وصلة مما يجعله الخيار الأمثل.

يمكن تحسين اداء بروتوكول معلومات التسبيير بتفعيل حالة الاختصار التلقائي.

بروتوكول المسار المفتوح الأقصر أولا يمثل ثاني أفضل خيار ويمكن استخدامه في حالة استخدام موجهات من منتج آخر غير شركة سيسكو.
# TABLE OF CONTENTS

DEDICATION ......................................................................................................................... 2

ACKNOWLEDGMENT ............................................................................................................. 3

ABSTRACT ............................................................................................................................. 4

المستشار............................................................................................................................. 6

TABLE OF CONTENTS ......................................................................................................... 7

LIST OF FIGURES .................................................................................................................. 10

LIST OF ABBREVIATIONS .................................................................................................... 12

CHAPTER 1: INTRODUCTION .............................................................................................. 14

1.1 Overview ......................................................................................................................... 14

1.2 Problem Statement .......................................................................................................... 14

1.3 Methodology and tools .................................................................................................... 15

1.4 Project objectives: .......................................................................................................... 15

1.5 Thesis layout ................................................................................................................... 15

CHAPTER 2: COMPUTER NETWORKS INTRODUCTION .................................................... 16

2.1 Overview ......................................................................................................................... 16

2.2 Types of networks .......................................................................................................... 16

2.3 Network edge and network core .................................................................................... 17

2.3.1 Network edge ............................................................................................................. 17

2.3.2 The Network core ..................................................................................................... 18

2.3.2.1 Circuit switching .................................................................................................... 18

2.3.2.2 Packet Switching .................................................................................................. 18

2.3.2.3 Comparisons between circuit switching and packet switching............................ 19

2.4 Basic hardware components: ........................................................................................ 19

2.4.1 Network interface cards ............................................................................................ 19
2.4.2 Repeaters ................................................................. 19
2.4.3 Hubs ........................................................................ 19
2.4.4 Bridges ..................................................................... 19
2.4.5 Switches ..................................................................... 20
2.4.6 Routers ..................................................................... 20
2.5 Protocol layers .................................................................. 21
2.5.1 Application layer 7 ......................................................... 21
2.5.2 Presentation Layer 6 ....................................................... 21
2.5.3 Session Layer 5 ............................................................. 21
2.5.4 Transport layer 4 ............................................................ 21
2.5.5 Network layer 3 .............................................................. 22
2.5.6 Data Link Layer 2 .......................................................... 22
2.5.7 Physical Layer 1 ............................................................. 22

CHAPTER 3: ROUTING PROTOCOLS ........................................ 24
3.1 Overview ........................................................................ 24
3.2 Routing algorithms ........................................................... 24
3.2.1 Link state routing protocols ........................................ 25
3.2.2 Distance vector routing protocol ..................................... 26
3.3 Autonomous systems ......................................................... 27
3.4 Interior routing protocols: ................................................. 28
3.4.1 Routing information protocol (RIP): ................................ 28
3.4.2 Open shortest path first (OSPF): ..................................... 29
3.4.3 The Interior Gateway Routing Protocol (IGRP) .................. 29
3.4.4 Enhanced Interior Gateway Routing Protocol (EIGRP) ........... 30
3.5 Exterior gateway routing protocols: .................................... 32
LIST OF FIGURES

Figure 4.1 ………………… network topology for simulation 1

Figure 4.2 ………………… in side the subnet network topology for simulation 1

Figure 4.3 ………………… traffic sent when using RIP

Figure 4.4 ………………… Traffic sent when using IGRP

Figure 4.5 ………………… traffic sent when using EIGRP

Figure 4.6 ………………… traffic sent when using OSPF

Figure 4.7 ………………… point to point throughput

Figure 4.8 ………………… point to point utilization

Figure 4.9 ………………… the network topology for simulation 2 (link failure/recovery)

Figure 4.10 ………………… inside the subnet in network for simulation 2

Figure 4.11 ………………… the traffic sent in simulation 2 (link failure/recovery)

Figure 4.12 ………………… the traffic dropped in simulation 2 (link failure and recovery)

Figure 4.13 ………………… network for simulation 3

Figure 4.14 ………………… in side the office in network for simulation 3

Figure 4.15 ………………… the average RIP traffic sent

Figure 4.16 ………………… the average point to point throughput
Figure 4.17………………… network topology for simulation 4

Figure 4.18 …………………inside the subnet in the network for simulation 4

Figure 4.19………………… the RIP traffic sent

Figure 4.20…………………forwarding tables fir RIP v1

Figure 4.21…………………forwarding tables for RIP v2
## LIST OF ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARPANET</td>
<td>Advanced Research Projects Agency Network</td>
</tr>
<tr>
<td>AS</td>
<td>Autonomous Systems</td>
</tr>
<tr>
<td>BGP</td>
<td>Border gateway routing protocol</td>
</tr>
<tr>
<td>CIDR</td>
<td>Classless Inter-Domain Routing</td>
</tr>
<tr>
<td>EGP</td>
<td>Exterior Gateway Routing Protocol</td>
</tr>
<tr>
<td>EIGRP</td>
<td>Enhanced Interior Gateway Routing Protocol</td>
</tr>
<tr>
<td>FDM</td>
<td>Frequency Division Multiplexing</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GAN</td>
<td>Global Area Network</td>
</tr>
<tr>
<td>GloMoSim</td>
<td>Global Mobile Information System Simulator</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hyper Text Transfer Protocol</td>
</tr>
<tr>
<td>IGP</td>
<td>Interior Gateway Routing Protocols</td>
</tr>
<tr>
<td>IGRP</td>
<td>Interior Gateway Routing Protocol</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MD5</td>
<td>Message-Digest algorithm 5</td>
</tr>
<tr>
<td>Mbps</td>
<td>Mega bit per second</td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Card</td>
</tr>
<tr>
<td>NetSim</td>
<td>Network Simulator</td>
</tr>
<tr>
<td>OPNET</td>
<td>Optimized Network Engineering Tool</td>
</tr>
<tr>
<td>OSI</td>
<td>Open System Interconnection</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open shortest path firs</td>
</tr>
<tr>
<td>PAN</td>
<td>Personal Area Network</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>RIP</td>
<td>Routing information protocol</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>TCP</td>
<td>Transfer Control Protocol</td>
</tr>
<tr>
<td>TDM</td>
<td>Time division multiplexing</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>VPR</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WWW</td>
<td>World Wide Web</td>
</tr>
<tr>
<td>Wi-Max</td>
<td>Worldwide Interoperability for Microwave Access</td>
</tr>
</tbody>
</table>
CHAPTER 1: INTRODUCTION

1.1 Overview

During the last years networks have grown rabidly, internet as an example contain millions of host and routers, servicing millions of user and providing various kind of services. Today the internet plays an important role in each part of our life, health, education, industry ….etc. Because of the huge number of entities in today’s internet, internet was divided into areas called (autonomous systems) or (ASs) each run under the same administrative authority.

As the scale of the internet increased, the amount of data transmitted over it increased, different protocols introduced to control the propagation of these data in the internet, an important sort of this protocols is the routing protocols.

The main goal of routing protocols is to determine the best path should be followed by data from source to destination, the routing protocols can be broadly classified into two main categories: interior gateway routing protocols which used to perform routing process inside the AS, examples: RIP and EIGRP, and exterior gateway routing protocols which perform routing process between the ASs, example BGP.

There is many interior gateway routing protocols such as RIP, OSPF, IGRP and EIGRP. Each routing protocol has its weakness and strength points.

1.2 Problem Statement

There are many available routing protocols, each with its own advantages and limitations, so the selection of routing protocol to run it in a certain network is an important decision, the selection of routing protocol depends on the network, the applications in that network, the load on that network links and other factors that affect the selection of routing protocol.

To determine the most suitable routing protocol, the routing protocols should be compared with other, many metrics used in the comparison such as the
traffic generated by each protocol, throughput, delay and the traffic dropped in the case of a link failure.

1.3 Methodology and tools

Simulation software can be used to evaluate and compare the performance of routing protocols, in this thesis Optimized Network Engineering Tool (OPNET), OPNET v 14 will be used.

The simulation software give results used to evaluate the performance of routing protocols, the performance of different routing protocols will be compared, and techniques to improve the performance of these protocols will be simulated to determine how effective it will be.

1.4 Project objectives:

The project objective is to evaluate the performance of routing protocols using a simulation software to determine the which routing protocol is the best in a given network and the benefits and drawbacks of each protocol.

1.5 Thesis layout

Chapter 1: introduction

Chapter 2: introduction to computer networks

Chapter 3: routing protocols

Chapter 4: simulation

Chapter 5: conclusion.
CHAPTER 2: COMPUTER NETWORKS

INTRODUCTION

2.1 Overview

The network is a collection of computers devices connected to each other by connection channels that enable users to share resources with each other, these resources could be hardware, software or information.

Computer networks can be classified according to the connection method such as: optical fiber, Ethernet, Wireless LAN. or can be classified according to their scale such as: local area network (LAN), wide area network (WAN), metropolitan area network (MAN), personal area network (PAN), virtual private network (VPN), campus area network (CAN).or can be classified according to the network topology upon which the network is based, such as bus network, star network, ring network, mesh network, star-bus network, tree or hierarchical topology network.

2.2 Types of networks

The most common classification of the networks is according to their scale, networks can be classified as:

Personal area network

A personal area network: (PAN) is a computer network used for communication among computer and different information technological devices close to one person. Examples of devices that are used in a PAN are personal computers, printers, fax machines, telephones, PDAs, scanners, and even video game consoles. A PAN may include wired and wireless connections between devices.

Local area network: A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings. Each computer or device on the network is a node.

Wide area network: A wide area network (WAN) is a computer network that covers a large geographic area such as a city, country, or spans even
intercontinental distances, using a communications channel that combines many
types of media such as telephone lines, cables, and air waves. A WAN often uses
transmission facilities provided by common carriers, such as telephone companies.

**Global area network**: A global area network (GAN) is a network used for
supporting mobile communications across an arbitrary number of wireless LANs,
satellite coverage areas, etc.

**Enterprise Private Network** is a network build by an enterprise to interconnect
the various company sites (production sites, head offices, remote offices, shops
etc.) in order to share computer resources over the network.

**Virtual private network**: A virtual private network (VPN) is a computer network
in which some of the links between nodes are carried by open connections or
virtual circuits in some larger network (e.g., the Internet) instead of by physical
wires.

**Internet**: The Internet is a global system of interconnected governmental,
academic, corporate, public, and private computer networks. It is the successor of
the Advanced Research Projects Agency Network (ARPANET) developed by
DARPA of the U.S. Department of Defense. The Internet is also the
communications backbone underlying the World Wide Web (WWW).

### 2.3 Network edge and network core

#### 2.3.1 Network edge

Contain Clients and servers

Hosts are sometimes further divided into two categories, Clients and servers.
Generally, clients often tend to be desktop PC's or workstations, while servers are
more powerful machines. But the precise meaning of a client and a server in
computer networking, a client program running on one end system requests and receives information from a server running on another end system.

### 2.3.2 The Network core

The network core consists of the routers and physical links that interconnect end systems together. There are two approaches to implement the network core: circuit switching and packet switching.

#### 2.3.2.1 Circuit switching

In circuit switched networks, the resources needed along a path to provide for communication between the end systems are reserved for the duration of the session. In telecommunications, a circuit switching network is one that establishes a circuit or (channel) between nodes and terminals before the users may communicate, as if the nodes were physically connected with an electrical circuit. The bit delay is constant during a connection, as opposed to packet switching, where packet queues may cause varying packet transfer delay. Each circuit cannot be used by other callers until the circuit is released and a new connection is set up. Even if no actual communication is taking place in a dedicated circuit that channel remains unavailable to other users. Channels that are available for new calls to be setup are said to be idle. This method use TCP for communicates between the end systems.

#### 2.3.2.2 Packet Switching

In packet-switched networks, the resources are not reserved, a session's messages use the resource on demand, and as a consequence, may have to wait for access to a communication link. There are two broad classes of packet-switched networks: datagram networks and virtual-circuit networks. They differ according to whether they route packets according to host destination addresses or according to virtual circuit numbers. Packet switching features delivery of variable bit rate data streams over a shared network.

Two major packet switching modes exist; connectionless packet switching (datagram switching) and connection-oriented packet switching (virtual circuit switching). In the first case each packet includes complete addressing or routing information. The packets are routed individually, sometimes resulting in different paths and out-of-order delivery. In the second case a connection is defined and reallocated in each involved node before any packet is transferred. The packets include a connection identifier rather than address information, and are delivered in order. This method use UDP for communicates between end systems.
2.3.2.3 Comparisons between circuit switching and packet switching

Packet switching is not suitable for real-time services (e.g. telephone calls and video conference calls) due to its variable and unpredictable delays. And it offers better sharing of bandwidth than circuit switching and it is simpler, more efficient, and less costly to implement than circuit-switching.

2.4 Basic hardware components:

All networks are made up of basic hardware building blocks to interconnect network nodes, such as Network Interface Cards (NICs), Bridges, Hubs, Switches, and Routers. In addition, some method of connecting these building blocks is required.

2.4.1 Network interface cards

A network card, network adapter, or NIC (network interface card) is a piece of computer hardware designed to allow computers to communicate over a computer network. It provides physical access to a networking medium and often provides a low-level addressing system through the use of MAC addresses. [2]

2.4.2 Repeaters

A repeater is an electronic device that receives a signal, cleans it of unnecessary noise, regenerates it, and retransmits it at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation. Repeaters work on the Physical Layer of the OSI model.

2.4.3 Hubs

A network hub contains multiple ports. When a packet arrives at one port, it is copied unmodified to all ports of the hub for transmission. The destination address in the frame is not changed to a broadcast address. It works on the Physical Layer of the OSI model.

2.4.4 Bridges

A network bridge connects multiple network segments at the data link layer (layer 2) of the OSI model. Bridges do send broadcasts to all ports except the one on which the broadcast was received. However, bridges do not promiscuously copy traffic to all ports, as hubs do, but learn which MAC addresses are reachable.
through specific ports. Once the bridge associates a port and an address, it will send traffic for that address to that port only.

Bridges learn the association of ports and addresses by examining the source address of frames that it sees on various ports. Once a frame arrives through a port, its source address is stored and the bridge assumes that MAC address is associated with that port. The first time that a previously unknown destination address is seen, the bridge will forward the frame to all ports other than the one on which the frame arrived.

Bridges come in three basic types:

- **Local bridges**: Directly connect local area networks (LANs)
- **Remote bridges**: Can be used to create a wide area network (WAN) link between LANs. Remote bridges, where the connecting link is slower than the end networks, largely have been replaced with routers.
- **Wireless bridges**: Can be used to join LANs or connect remote stations to LANs.

### 2.4.5 Switches

A network switch is a device that forwards and filters OSI layer 2 datagrams (chunk of data communication) between ports (connected cables) based on the MAC addresses in the packets. This is distinct from a hub in that it only forwards the frames to the ports involved in the communication rather than all ports connected. Switches make forwarding decisions of frames on the basis of MAC addresses. A switch normally has numerous ports, facilitating a star topology for devices, and cascading additional switches. Some switches are capable of routing based on Layer 3 addressing or additional logical levels; these are called multi-layer switches.

### 2.4.6 Routers

A router is an internetworking device that forwards packets between networks by processing information found in the datagram or packet (Internet protocol information from Layer 3 of the OSI Model). In many situations, this information is processed in conjunction with the routing table (also known as forwarding table). Routers use routing tables to determine what interface to forward packets (this can include the "null" also known as the "black hole" interface because data can go into it, however, no further processing is done for said data).
2.5 Protocol layers

To reduce design complexity, network designers organize protocols and the network hardware and software that implement the protocols in layers. With layered protocol architecture, each protocol belongs to one of the layers. When taken together, the protocols of the various layers are called the protocol stack. The original protocol stack (protocol layers) are seven layers but defacto system were reduced seven layers to five layers by collecting Application layer, presentation layer and session layer into one layer called application layer.[1]

2.5.1 Application layer 7

This top layer defines the language and syntax that programs use to communicate with other programs. The application layer represents the purpose of communicating in the first place. For example, a program in a client uses commands to request data from a program in the server. The application layer includes many protocols, HTTP to support the Web, SMTP to support electronic mail, and FTP to support file transfer. An application layer protocol is distributed over multiple end system, with the application in one end system using the protocol to exchange packets of information with the application in another end system. We will refer to this packet of information (data) at the application layer as a message.

2.5.2 Presentation Layer 6

When data are transmitted between different types of computer systems, the presentation layer determines and manages the way data are represented and encoded. This layer is also used for encryption and decryption of the messages.

2.5.3 Session Layer 5

Provides coordination of the communications in an orderly manner. It determines one-way or two-way communications and manages the dialog between both parties; for example, making sure that the previous request has been fulfilled before the next one is sent. It also marks significant parts of the transmitted data with checkpoints to allow for fast recovery in the event of a connection failure. In practice, this layer is often not used or services within this layer are sometimes incorporated into the transport layer.

2.5.4 Transport layer 4

The transport layer is responsible for transporting application layer messages between the client and server sides of an application. In the Internet there are two transport protocols, TCP and UDP, either of which can transport application layer messages. TCP provides a connection-oriented service to its applications. This service includes guaranteed delivery of application layer messages to the
destination and flow control (i.e. sender/receiver speed matching). TCP also segments long messages into shorter segments and provides congestion control mechanism, so that a source throttles its transmission rate when the network is congested. The UDP protocol provides a connectionless service to its applications. This means that no reliability, no over flow control, and no congestion control.

2.5.5 Network layer 3

The network layer is responsible for routing datagrams from one host to another. The Internet's network Layer has two principle components. First it has a protocol that defines the fields in the IP datagram as well as how the end systems and routers act on these fields. This protocol is the celebrated IP protocol. There is only one IP protocol, and all Internet components that have a network layer must run the IP protocol. The Internet's network layer also contains routing protocols that determine the routes that datagrams take between sources and destinations. The Internet has many routing protocols. The Internet is network of networks and within a network, the network administrator can run any routing protocol desired. Although the network layer contains both the IP protocol and numerous routing protocols, it is often simply referred to as the IP layer, reflecting that fact that IP is the glue that binds the Internet together.

2.5.6 Data Link Layer 2

The data link is responsible for node to node validity and integrity of the transmission. The transmitted bits are divided into frames. In this layer the processes of checksum, parity flag, and error detection can take places. Layers 1 and 2 are required for every type of communications \[1\].

2.5.7 Physical Layer 1

The physical layer is responsible for passing bits onto and receiving them from the connecting medium. This layer has no understanding of the meaning of the bits, but deals with the electrical and mechanical characteristics of the signals and signaling methods. In this layer the processes of modulation, demodulation, TDM and FDM techniques for multiplexing data can tack places.
chapter 3: routing protocols

3.1 overview

Routing protocols are apart of network layer protocols, they mainly perform routing process which is the process of determining the path that the packets should take from source to destination.

A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network, the choice of the route being done by routing algorithms.

Routing algorithm chooses the best route between the source and destination, the best route is the one with the least cost, the cost have a various metrics. The routing protocols can be classified according to the routing algorithm used into two main classes:

- Link state routing protocols: like OSPF and IS-IS
- Distance vector routing protocols: like RIP, IGRP and EIGRP

- In the internet, The Internet is organized as a set of independent Autonomous Systems (AS) which is a collection of networks under single technical administration this give another classification of routing protocols classifying the routing protocols according to if they used inside the AS or outside it:
  - Interior gateway Routing Protocols (IGP) which used inside the AS, like RIP, OSPF
  - Exterior gateway Routing Protocol (EGP) which used between the Ass, like BGP V4

3.2 routing algorithms

The routing algorithm is algorithm used to determine the best route between the source and destination. The purpose of a routing algorithm is simple: given a set of routers, with links connecting the routers, a routing algorithm finds a "good" path from source to destination. Typically, a "good" path is one which has "least cost," but we will see that in practice, "real-world" concerns such as policy issues.
Routing algorithms can be classified into two main types:

- A global routing algorithm (link state) computes the least cost path between a source and destination using complete, global knowledge about the network. That is, the algorithm takes the connectivity between all nodes and all links costs as inputs. This then requires that the algorithm somehow obtain this information before actually performing the calculation. The calculation itself can be run at one site. In practice, algorithms with global state information are often referred to as link state algorithms, since the algorithm must be aware of the state (cost) of each link in the network.

- A decentralized routing algorithm (distance vector), the calculation of the least cost path is carried out in an iterative, distributed manner. No node has complete information about the costs of all network links. Instead, each node begins with only knowledge of the costs of its own directly attached links and then through an iterative process of calculation and exchange of information with its neighboring nodes (i.e., nodes which are at the "other end" of links to which it itself is attached) gradually calculates the least cost path to a destination, or set of destinations. It is called a distance vector algorithm because a node never actually knows a complete path from source to destination. Instead, it only knows the direction (which neighbor) to which it should forward a packet in order to reach a given destination along the least cost path, and the cost of that path from itself to the destination.

3.2.1-Link state routing protocols

Link-state protocol is performed by every switching node in the network (i.e. nodes that are prepared to forward packets; in the Internet, these are called routers). The basic concept of link-state routing is that 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. The collection of best paths will then form the node's routing table.

In the link state routing protocol there are 2 main stages [2]:

**Distributing maps:**

First main stage in the link-state algorithm is to give a map of the network to every node. This is done with several simple subsidiary steps:

- Determining the neighbors of each node: First, each node needs to determine what other ports it is connected to, over fully-working links; it does this using a simple reachability protocol which it runs separately with each of its directly-connected neighbors.
- Distributing the information for the map: Next, each node periodically and in case of connectivity changes makes up a short message, the link-state advertisement, which:

- Identifies the node which is producing it.

- Identifies all the other nodes to which it is directly connected.

- Creating the map

Finally, with the complete set of link-state advertisements (one from each node in the network) in hand, it is obviously easy to produce the graph for the map of the network.

The algorithm simply iterates over the collection of link-state advertisements; for each one, it makes links on the map of the network, from the node which sent that message, to all the nodes which that message indicates are neighbors of the sending node.

2- Calculating the routing table

The second main stage in the link-state algorithm is to produce routing tables, by inspecting the maps. This is again done with several steps:

- Calculating the shortest paths

Each node independently runs an algorithm over the map to determine the shortest path from itself to every other node in the network; generally Dijkstra's algorithm is used.

- Filling the routing table

With the shortest paths in hand, filling in the routing table is trivial.

3.2.2- Distance vector routing protocol

This type uses the distance vector algorithm which is iterative, asynchronous, and distributed. It is distributed in that each node receives some information from one or more of its directly attached neighbors, performs a Point-
to-Point Routing Algorithms Calculation and may then distribute the results of its
calculation back to its neighbors. It is iterative in that this process continues on
until no more information is exchanged between neighbors. [1]
The algorithm is asynchronous in that it does not require all of the nodes to operate
in lock step with each other.

The methods used to calculate the best path for a network are different
between different routing protocols but the fundamental features of distance-vector
algorithms are the same across all DV based protocols.

Distance Vector means that Routers are advertised as vector of distance and
Direction. Direction is simply next hop address and exit interface and Distance
means such as hop count.

Routers using distance vector protocol do not have knowledge of the entire
path to a destination. Instead DV uses two methods:

1. Direction in which or interface to which a packet should be forwarded.
2. Distance from its destination.

Updates are performed periodically in a distance-vector protocol where all or part
of a router's routing table is sent to all its neighbors that are configured to use the
same distance-vector routing protocol. Once a router has this information it is able
to make its own routing table to reflect the changes and then inform its neighbors
of the changes.

3.3 Autonomous systems

The internet now consist of large numbers of hosts and routers As the
number of routers grow larger and larger, the overhead involved in computing,
storing, and communicating the routing table information, Storing routing table
entries to huge number of routers would clearly require enormous amounts of
memory. The overhead required to broadcast link state updates among millions of
routers would leave no bandwidth left for sending the data packets! A distance
vector algorithm that iterated among millions of routers would surely never
converge! Clearly, something must be done to reduce the complexity of route
computation in networks as large as the public Internet.
Also every ISP or administrative organization should be able to run and administer
its network as it wishes, while still being able to connect its network to other
networks.

To deal with the huge number of hosts and routers and the administrative
authority problem the internet is divided into regions called autonomous systems
(Ass) each AS contain group of routers running the same routing algorithm.
This lead to another classification of routing protocols:
-interior routing protocols which is the protocol used inside the autonomous
system example: RIP, IGRP, EIGRP, OSPF
- exterior routing protocol which is used to connect two autonomous systems together
  Example BGP v4

### 3.4 Interior routing protocols:

#### 3.4.1 Routing information protocol (RIP):

RIP is interior routing protocol, that use distance vector algorithm, used in local and wide area networks. It was first defined in RFC 1058 (1988). The protocol has since been extended several times, resulting in RIP Version 2 (RFC 2453). Both versions are still in use today, however, they are considered to have been made technically obsolete by more advanced techniques such as Open Shortest Path First (OSPF) and IS-IS. RIP has also been adapted for use in IPv6 networks, a standard known as RIPng (RIP next generation), published in RFC 2080 (1997).

**Technical details**

RIP use hop count as a metric to compare the routes each link has a cost of 1. It also limits the maximum number of hops allowed in each path, the maximum allowed hops is 15 hops, a 16 hop count will considered inaccessible, also this will prevent routing loops it will also limits the use of RIP in ASs with maximum 15 hop diameter.

RIP transmits a complete update of routing information every 30 sec, this will generate a heavy traffic in the network every 30 sec. RIP v2 introduced in 1993 it has many new features:
- All RIP route entries now carry a subnet mask, effectively making it a classless protocol.
- A RIP route entry now specifies a next hop router. This allows a RIP router to advertise a network that is reachable via another router.
- Multicast addressing is now used for periodic broadcasts, reducing load on hosts that do not want to receive RIP messages.
- Authentication for RIP messages is now supported.

**Performance of RIP:**

RIP will generate high traffic in the network due to its periodic updates; this will make it not suitable for slow, crowded networks. The performance can be improved using auto summary and triggered extension mode which cause RIP to send information only when there has been an update to the routing database. Triggered extensions to IP RIP increase efficiency of RIP on point-to-point, serial interfaces. RIP routing traffic will be reduced on point-to-point, serial interfaces.
3.4.2 Open shortest path first (OSPF):

OSPF is interior gateway routing protocol that use link state routing algorithm, the most recent version of OSPF, version 2, is defined in RFC 2178 - a public document.

Technical details:

OSPF is a link-state protocol that uses flooding of link state information and a Dijkstra least cost path algorithm. With OSPF, a router constructs a complete topological map of the entire autonomous system. The router then locally runs Dijkstra's shortest path algorithm to determine a shortest path tree to all networks with itself as the root node. The router's routing table is then obtained from this shortest path tree. Individual link costs are configured by the network administrator.

OSPF support multi-path routing in which the traffic is shared among routes of equal costs.

As OSPF autonomous system can be configured into "areas." Each area runs its own OSPF link state routing algorithm, with each router in an area broadcasting its link state to all other routers in that area.. Intra-area routing involves only those routers within the same area. [1]

Performance of OSPF:

OSPF has very small convergence time which is the time needed by routers to agree on network topology after a change in network topology. [2]

OSPF use external metrics as a cost metrics, the cost of the links can be set according to distance of a router (round-trip time), network throughput of a link, or link availability and reliability, this give more control on the performance of the network, and provides a dynamic process of traffic load balancing between routes of equal cost.

3.4.3 The Interior Gateway Routing Protocol (IGRP)

IGRP is interior routing protocol that use the distance vector algorithm, The Interior Gateway Routing Protocol (IGRP) is a routing protocol that was developed in the mid-1980s by Cisco Systems, Inc. It is proprietary, which requires that you use Cisco routers only. [2]

Technical details:

IGRP uses distance vector algorithm, in which every router sends all or part of its routing database to neighboring routers, IGRP sends updates every 90 sec by default.

IGRP uses a combination (vector) of metrics. Internetwork delay, bandwidth, reliability, and load are all factored into the routing decision. Network
administrators can set the weighting factors for each of these metrics. IGRP uses either the administrator-set or the default weightings to automatically calculate optimal routes.

IGRP is considered a classful routing protocol. Because the protocol has no field for a subnet mask, the router assumes that all interface addresses within the same Class, This, classful protocols have become less popular as they are wasteful of IP address space.

IGRP is closely related to the RIP but they have many differences between them, the IGRP sends its updates every 90 sec, and the RIP sends it every 30 sec. and IGRP support multi path for equal costs routes which is not supported by the RIP, also IGRP has maximum hop count of 255 while RIP has a maximum hop count of 15.

**Performance of IGRP:**

The IGRP sends updates every 90 seconds, this will decrease the traffic in the network (when compared to the RIP).

The metrics used to compare routes calculated from the network delay, load, reliability and bandwidth; this will help improving the overall network performance and provide more flexibility.

IGRP is approximately replaced by another protocol which is enhanced IGRP.

3.4.4 Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is interior gateway routing protocol, that use Diffusing Update Algorithm (DUAL), it has characteristics of both distance vector routing protocols and link state routing protocols, developed by Cisco Systems, Inc.

**Technical details:**

EIGRP use the DUAL algorithm, DUAL finite-state machine embodies the decision process for all route computations by tracking all routes advertised by all neighbors. DUAL uses distance information to select efficient, loop-free paths and selects routes for insertion in a routing table based on feasible successors. A feasible successor is a neighboring router used for packet forwarding that is a least-cost path to a destination that is guaranteed not to be part of a routing loop. When a neighbor changes a metric, or when a topology change occurs, DUAL tests for feasible successors. If one is found, DUAL uses it to avoid recomputing the route unnecessarily. When no feasible successors exist but neighbors still advertise the
destination, recomputations (also known as a diffusing computation) must occur to
determine a new successor. Enhanced IGRP relies on four fundamental concepts:
neighbor tables, topology tables, route states, and route tagging. [5]
-Neighbor tables are used to record the neighbor’s addressed and interface of
neighboring routers.

- The topology table contains all destinations advertised by neighboring routers.

the Routing Table contains the best route to a destination, which is known as the
Successor. The Feasible Successor is a backup route to a destination which is kept
in the Topology Table.

- Route states: Topology-table entry for a destination can exist in one of two states:
active or passive. Destination is in the passive state when the router is not
performing a recomputation or in the active state when the router is performing a
recomputation.

To compare the routes EIGRP use metrics calculated from the network Delay,
Bandwidth, Reliability and Load.

Performance of EIGRP:

Enhanced IGRP stores all its neighbors’ routing tables so that it can quickly
adapt to alternate routes. If no appropriate route exists, Enhanced IGRP queries its
neighbors to discover an alternate route. These queries propagate until an alternate
route is found, this feature gives EIGRP the ability to handle the topology changes
as fast as possible, and provide much faster convergence.

Enhanced IGRP does not make periodic updates. Instead, it sends partial
updates only when the metric for a route changes. Propagation of partial updates is
automatically bounded so that only those routers that need the information are
updated. As a result of these two capabilities, Enhanced IGRP consumes
significantly less bandwidth.
EIGRP has totally replaced the obsolete IGRP it has many it has many capabilities
that are not found in IGRP:
- EIGRP support the classless routing where the IGRP does not
- EIGRP has much less convergence time than IGRP
- MD5 authentication can be used to authorize EIGRP packets. [2]
- EIGRP does not make periodic updates. Instead, it sends partial updates only
when the metric for a route changes. EIGRP consumes significantly less
bandwidth than IGRP. [2]
3.5 Exterior gateway routing protocols:

4.5.1 Border gateway routing protocol (BGP):

BGP is exterior gateway protocol, it provide routing between autonomous systems, it is the most common used exterior gateway routing protocol in today’s internet.

BGP is close to distance vector protocols but it differ in that the BGP do not propagate cost information, instead it propagates path information, these information include the sequence and the names of ASs on the route to destination.

Technical details:

As far as BGP is concerned, the whole Internet is a graph of ASs, and each AS is identified by an AS number the immediate neighbors in the graph of ASs are called peers. BGP information is prorogated through the network by exchanges of BGP messages between peers. The BGP protocol defines the four types of messages: OPEN UPDATE, NOTIFICATION and KEEPALIVE. [1]

When a BGP gateway wants to first establish contact with a BGP peer, an OPEN message is sent to the peer. The OPEN message allows a BGP gateway to identify and authenticate itself, and provide timer information. If the OPEN is acceptable to the peer, it will send back a KEEPALIVE.UPDATE message used to advertise a path to a given destination to the BGP peer. [1]

KEEPALIVE is used to let a peer know that the sender is alive but that the sender doesn't have other information to send. It also serves as an acknowledgment to a received OPEN message, NOTIFICATION message is used to inform a peer that an error has been or that the sender is about to close the BGP session. [1]

Very often an AS will have multiple gateway routers that provide connections to other ASs. Even though BGP is an exterior protocol, it can still be used inside an AS as a pipe to exchange BGP updates among gateway routers belonging to the same AS. BGP connections inside an AS are called Internal BGP (IBGP), whereas BGP connections between ASs are called External BGP (EBGP). [1]
CHAPTER 4: SIMULATION

4.1 Overview

network simulation is a method where a software program models (simulate) the behavior of a network either by calculating the interaction between the different network entities (hosts/routers, data links, packets, etc) using mathematical formulas, or actually capturing and playing back observations from a production network. Many conditions can be simulated to determine how the network would behave under these conditions.

A network simulator is a software program that imitates the working of a computer network. In simulators, the computer network is typically modeled with devices, traffic etc and the performance is analyzed. Typically, users can then customize the simulator to fulfill their specific analysis needs. Simulators typically come with support for the most popular protocols in use today, such as Wireless LAN, Wi-Max, UDP, and TCP.

There is a lot of network modelers like GloMoSim, NetSim. Here we use OPNET modeler version 14. Which is very large and powerful software with wide variety of possibilities enables the possibility to simulate entire heterogeneous networks with various protocols.

Development work was started in 1986 by MIL3 Inc. (nowadays OPNET Technologies Inc.). Originally the software was developed for the needs of military, but it has grown to be a world leading commercial network simulation tool. OPNET is quite expensive for commercial usage but there are also free licenses for educational purposes.

OPNET has Hierarchical structure, meaning that modeling is divided to three main domains:
• Network domain: Networks + sub-networks, network topologies, geographical coordinate mobility
• Node domain: Single network nodes (e.g., routers, workstations, mobile devices…)
• Process domain: Single modules and source code inside network nodes

OPNET also enable us to set network parameters as needed to provide a certain network environment to the network under test to determine the behavior of that network under these conditions like running certain routing protocol or run a certain application in the network (E-mail application for example) or link failure and recovery.

OPNET also provide metrics for the networks performance and give the results in a shape of tables or graphs.
Why the OPNET?
We choose the OPNET because OPNET give us sufficient control on the network environment characteristics, and have a large library of models can be used to design The desired network.( no need to design it from process layer ).

Also OPNET support all routing protocols needed for simulation .it also provide needed conditions such as link failure or recovery. Finally OPNET is easy to learn and use
4.2 SIMULATION: Comparison between routing protocols

4.2.1 Overview

Four routing protocols will be compared with each other:

RIP the Routing Information Protocol, use distance vector algorithm to mathematically compare routes to determine the best route use the hop count as a metric to compare routes with maximum cost 15 hop, update its entire routing tables every 30 seconds.

IGRP Interior Gateway Routing Protocol, distance vector based protocol, use a composite metric calculated by factoring weighted mathematical values for network delay, bandwidth reliability and load. Allow multi-path routing, update its tables every 90 seconds by default.

EIGRP Enhanced Interior Gateway Routing Protocol : use diffusing update algorithm in which routers share routes calculation and updates sent only when needed to neighbors who need it, use cost metric calculated from network delay, bandwidth, reliability and load.

OSPF the Open Shortest Path First which is a link state algorithm, each router have information about cost and network topology for the entire network, also provide multi-path routing

Every time we run single protocol, then observe how each protocol create traffic, and observe utilization and throughput of the network.

So we will have four scenarios ,one for each routing protocol .

4.2.2 Network Topology:

The network used in this scenario consists of:
- 50 subnet each consists of:

-2 LANs each have ten clients and one server.

-switch

-router

-internet cloud: model represents the internet and performs routing functions.

The network support E-mail application.

Figure 4.1: network topology for simulation 1
Figure 4.2: Inside the subnet, network topology for simulation 1
4.2.3 Results:

Scenario 1: RIP

Figure 4.3 traffic sent when using RIP
Scenario 2: IGRP

Figure 4.4 Traffic sent when using IGRP
Scenario 3: EIGRP

Figure 4.5 traffic sent when using EIGRP
Scenario 4: OSPF

Figure 4.6 traffic sent when using OSPF
Figure 4.7 point to point throughput
Utilization:

Figure 4.8 point to point utilization
4.2.4 Comments:

The traffic in the network when using RIP (figure 4.3) is really heavy compared to other routing protocols, this because RIP update its entire routing tables every 30 seconds and when the network topology change, and send this complete updates over the network creating high traffic every 30 seconds.

Figure 4.4 show traffic generated by IGRP it show that IGRP generate traffic every 90 sec To send updates to other routers in the network. we notice that the traffic is less than the one generated by RIP because IGRP send a part of its routing table every period.

Figure 4.5 show traffic generated by EIGRP which is really small traffic when compared to the others and this due to that EIGRP send updates only when there is topology change, (no periodic updates), and send these updates only to neighbors who need them. Notice there is small traffic every 30 seconds this come from small hello messages sent periodically to maintain adjacencies between neighboring routers.

Figure 4.6 show traffic generated by OSPF it is really high at the start of simulation because every router has to gain complete information about the entire network, these information flooded to all routers in the area. OSPF sends partial updates when a link-state change occurs.

RIP give higher utilization for the network links. on the other side EIGRP give the least utilization to the network leaving bandwidth space for transmitting data (Figure 4.8)
4.3 Simulation2: Link failure and recovery

4.3.1 Overview

This simulation examine the behavior of a network using a certain routing protocol when there is a link failure and recovery, we will run a single protocol every time and observe traffic dropped and traffic sent for each protocol, the results will be compared with each other.

In RIP if the router did not hear advertisement from neighbor router after 180 seconds, that neighbor will be considered dead and all routes use this dead router will be invalidated, updates sent to all neighbors to change their routing tables. This will take long time. The IGRP use the same mechanism. [2]

EIGRP implements DUAL (Diffusing Update Algorithm). DUAL allow EIGRP to converge very quickly. Each EIGRP router stores its neighbors routing tables. This allows the router to use a new route to a destination instantly if another feasible route is known. If no feasible route is known based upon the routing information previously learned from its neighbors, a router running EIGRP becomes active for that destination and sends a query to each of its neighbors asking for an alternate route to the destination. These queries propagate until an alternate route is found. Routers that are not affected by a topology change remain passive and do not need to be involved in the query and response. [4]

OSPF detects changes in the topology, such as link failures, very quickly and converges its routing structure within seconds. It computes the shortest path tree for each route using Dijkstra’s algorithm, a shortest path first algorithm.

The link-state information is maintained on each router as a link-state database (LSDB) which is a tree-image of the entire network topology. Identical copies of the LSDB are sent to all routers in the network.

In this simulation RIP, IGRP and EIGRP distance vector routing protocol will be compared against each other using the traffic generated by each protocol and the traffic dropped as metric for the comparison.
4.3.2 Network topology

The network consist of five subnets each have two sub-networks, switch and a router as shown in figure

Figure 4.9 the network topology for simulation 2 (link failure/recovery)
The link shown with the red color will be failed at time 5 min and recovered later in time 15 min. There will be three scenarios: RIP, IGRP and EIGRP. The traffic sent and the traffic dropped will be observed at each case.
4.3.3 Results

Figure 4.11 the traffic sent in simulation 2 (link failure /recovery)
Figure 4.12 the traffic dropped in simulation 2 (link failure and recovery)
4.3.4 Comments

Figure 4.11 show the traffic sent, the traffic increase at min 5 and min 15 because the routing protocols detect the link failure at time 5 min and update and send their updates to neighbor routers, and at time 15 min the failed link has been recovered so the traffic will increase due to the routing tables being updated.

RIP and IGRP generate high traffic compared to EIGRP as seen in simulation 1.

Figure 4.12 show the traffic dropped, IGRP and RIP give the higher dropped packets specially at time 5min (at the link failure time), this because the RIP and IGRP have long convergence times than EIGRP.

The results show that EIGRP has no traffic dropped because EIGRP use DUAL algorithm which search in the network topology for feasible successor and if it does not find feasible successor, and if it does not find a feasible successor, it enters in an active convergence state and sends request to neighbor routers for alternative route, neighboring routers reply with alternative route. all that done in a short time.

So EIGRP will have alternative routes ready to be used in the case of a link failure.
4.4 Simulation 3: Triggered extension mode in RIP

4.4.1 Overview

There were two problems using RIP to connect to a WAN [2]:
- Periodic broadcasting by RIP.
- Even on fixed, point-to-point links, the overhead of periodic RIP transmissions could seriously interrupt normal data transfer because of the quantity of information that hits the line every 30 seconds.

To overcome these limitations, triggered extensions to RIP cause RIP to send information on the WAN only when there has been an update to the routing database. Periodic update packets are suppressed over the interface on which this feature is enabled.

Triggered extensions to IP RIP increase efficiency of RIP on point-to-point, serial interfaces. RIP routing traffic will be reduced on point-to-point, serial interfaces. This simulation will examine if the triggered extension mode will be more efficient.

4.4.2 Network topology:

The network used in this simulation consists of two offices each have 3 backbone routers and LANs and 2 servers the two offices connected to each other via one link.
Figure 4.13 network for simulation 3
Figure 4.14 in side the office in network for simulation 3

This network will run the RIP, we will have two scenarios:

Scenario 1 triggered extension mode is off

Scenario 2 triggered extension mode is on

We will the observe the traffic sent and the throughput in each scenario and compare the results with each other
4.4.3 Results

Figure 4.15 the average RIP traffic sent
Figure 4.16 the average point to point throughput
4.4.4 Comments:

Figure 4.15 show the average RIP traffic sent, the traffic generated by RIP with triggered extension on is less than the one generated when the mode is off.

The same result can be obtained from figure 4.16 which show that the throughput is smaller when the triggered extension mode is on, leaving the rest of band width for the transmission of data.
4.5 Simulation 4: RIP v1 vs. RIP v2

4.5.1 Overview

RIP v2 introduce many new features: [2]

- included the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR)

- In an effort to avoid unnecessary load on hosts that do not participate in routing, RIPv2 multicasts the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast

- Authentication added using MD5

To maintain backward compatibility, the hop count limit of 15 remained

4.5.2 Network topology:

The network used in simulation consist of four fully meshed routers forming backbone routers connected to four subnets each has two sub-networks and a router.
Figure 4.17 network topology for simulation 4
Figure 4.18 inside the subnet in the network for simulation 4

There will be two scenarios:

Scenario using RIPv1

Scenario using RIP v2

In the simulator RIP v1 enabled to receive v2 updates by disabling the auto summary attribute in v1\textsuperscript{[6]}
4.5.3 Results:

Figure 4.19 the RIP traffic sent
### Performance IP Forwarding Table at End of Simulation for Campus Network Backbone East

<table>
<thead>
<tr>
<th>Destination</th>
<th>Source Protocol</th>
<th>Route Preference</th>
<th>Metric</th>
<th>Next Hop Address</th>
<th>Next Hop Node</th>
<th>Outgoing Interface</th>
<th>Outgoing LSP</th>
<th>Inversion Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>150.10.0.0/16</td>
<td>RIP</td>
<td>120</td>
<td>2</td>
<td>192.0.3.1</td>
<td>Campus Network Backbone North</td>
<td>IF11</td>
<td>N/A</td>
<td>8.580</td>
</tr>
<tr>
<td>150.30.0.0/16</td>
<td>RIP</td>
<td>120</td>
<td>2</td>
<td>192.0.6.1</td>
<td>Campus Network Backbone West</td>
<td>IF4</td>
<td>N/A</td>
<td>10.530</td>
</tr>
<tr>
<td>150.50.0.0/16</td>
<td>RIP</td>
<td>120</td>
<td>1</td>
<td>192.0.10.1</td>
<td>Campus Network EastNet Central</td>
<td>IF5</td>
<td>N/A</td>
<td>7.666</td>
</tr>
<tr>
<td>150.70.0.0/16</td>
<td>RIP</td>
<td>120</td>
<td>2</td>
<td>192.0.1.2</td>
<td>Campus Network Backbone South</td>
<td>IF10</td>
<td>N/A</td>
<td>6.496</td>
</tr>
<tr>
<td>192.0.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>192.0.1.1</td>
<td>Campus Network Backbone East</td>
<td>IF10</td>
<td>N/A</td>
<td>0.000</td>
</tr>
<tr>
<td>192.0.2.0/24</td>
<td>RIP</td>
<td>120</td>
<td>1</td>
<td>192.0.1.2</td>
<td>Campus Network Backbone South</td>
<td>IF10</td>
<td>N/A</td>
<td>6.496</td>
</tr>
<tr>
<td>192.0.3.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>192.0.3.2</td>
<td>Campus Network Backbone East</td>
<td>IF11</td>
<td>N/A</td>
<td>8.680</td>
</tr>
<tr>
<td>192.0.4.0/24</td>
<td>RIP</td>
<td>120</td>
<td>1</td>
<td>192.0.3.1</td>
<td>Campus Network Backbone North</td>
<td>IF11</td>
<td>N/A</td>
<td>6.496</td>
</tr>
<tr>
<td>192.0.5.0/24</td>
<td>RIP</td>
<td>120</td>
<td>1</td>
<td>192.0.1.2</td>
<td>Campus Network Backbone South</td>
<td>IF10</td>
<td>N/A</td>
<td>6.496</td>
</tr>
<tr>
<td>192.0.6.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>192.0.6.2</td>
<td>Campus Network Backbone East</td>
<td>IF4</td>
<td>N/A</td>
<td>0.000</td>
</tr>
<tr>
<td>192.0.7.0/24</td>
<td>RIP</td>
<td>120</td>
<td>1</td>
<td>192.0.3.1</td>
<td>Campus Network Backbone North</td>
<td>IF11</td>
<td>N/A</td>
<td>8.580</td>
</tr>
<tr>
<td>192.0.8.0/24</td>
<td>RIP</td>
<td>120</td>
<td>1</td>
<td>192.0.6.1</td>
<td>Campus Network Backbone West</td>
<td>IF4</td>
<td>N/A</td>
<td>8.769</td>
</tr>
<tr>
<td>192.0.9.0/24</td>
<td>RIP</td>
<td>120</td>
<td>1</td>
<td>192.0.1.2</td>
<td>Campus Network Backbone South</td>
<td>IF10</td>
<td>N/A</td>
<td>6.496</td>
</tr>
<tr>
<td>192.0.10.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>192.0.10.2</td>
<td>Campus Network Backbone East</td>
<td>IF5</td>
<td>N/A</td>
<td>0.000</td>
</tr>
</tbody>
</table>

15

16 Gateway of last resort is not set

17

---

Figure 4.20 forwarding tables fir RIP v1
### Figure 4.21 Forwarding Tables for RIP v2

<table>
<thead>
<tr>
<th>Destination</th>
<th>Source Protocol</th>
<th>Route Preference</th>
<th>Metric</th>
<th>Next Hop Address</th>
<th>Next Hop Node</th>
<th>Outgoing Interface</th>
<th>Outgoing LSP</th>
<th>Insertion Time (secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.10.0/24</td>
<td>RIP</td>
<td>120</td>
<td>2</td>
<td>192.0.0.2</td>
<td>Campus Network.Backbone_North</td>
<td>IF11</td>
<td>N/A</td>
<td>8.580</td>
</tr>
<tr>
<td>192.0.20.0/24</td>
<td>RIP</td>
<td>120</td>
<td>2</td>
<td>192.0.0.2</td>
<td>Campus Network.Backbone_North</td>
<td>IF11</td>
<td>N/A</td>
<td>8.580</td>
</tr>
<tr>
<td>192.0.30.0/24</td>
<td>RIP</td>
<td>120</td>
<td>2</td>
<td>192.0.0.2</td>
<td>Campus Network.Backbone_West</td>
<td>IF4</td>
<td>N/A</td>
<td>10.078</td>
</tr>
<tr>
<td>192.0.40.0/24</td>
<td>RIP</td>
<td>120</td>
<td>2</td>
<td>192.0.0.2</td>
<td>Campus Network.Backbone_West</td>
<td>IF4</td>
<td>N/A</td>
<td>10.078</td>
</tr>
<tr>
<td>192.0.50.0/24</td>
<td>RIP</td>
<td>120</td>
<td>1</td>
<td>192.0.0.2</td>
<td>Campus Network.EastNet_Central</td>
<td>IF5</td>
<td>N/A</td>
<td>7.666</td>
</tr>
<tr>
<td>192.0.60.0/24</td>
<td>RIP</td>
<td>120</td>
<td>1</td>
<td>192.0.0.2</td>
<td>Campus Network.EastNet_Central</td>
<td>IF5</td>
<td>N/A</td>
<td>7.666</td>
</tr>
<tr>
<td>192.0.70.0/24</td>
<td>RIP</td>
<td>120</td>
<td>2</td>
<td>192.0.0.2</td>
<td>Campus Network.Backbone_South</td>
<td>IF10</td>
<td>N/A</td>
<td>6.496</td>
</tr>
<tr>
<td>192.0.80.0/24</td>
<td>RIP</td>
<td>120</td>
<td>2</td>
<td>192.0.0.2</td>
<td>Campus Network.Backbone_South</td>
<td>IF10</td>
<td>N/A</td>
<td>6.496</td>
</tr>
<tr>
<td>192.0.90.0/24</td>
<td>RIP</td>
<td>120</td>
<td>1</td>
<td>192.0.0.2</td>
<td>Campus Network.Backbone_South</td>
<td>IF10</td>
<td>N/A</td>
<td>6.496</td>
</tr>
<tr>
<td>192.0.100/24</td>
<td>RIP</td>
<td>120</td>
<td>1</td>
<td>192.0.0.2</td>
<td>Campus Network.Backbone_South</td>
<td>IF10</td>
<td>N/A</td>
<td>6.496</td>
</tr>
<tr>
<td>192.0.110/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>192.0.0.2</td>
<td>Campus Network.Backbone_East</td>
<td>IF10</td>
<td>N/A</td>
<td>0.000</td>
</tr>
<tr>
<td>192.0.120/24</td>
<td>RIP</td>
<td>120</td>
<td>1</td>
<td>192.0.0.2</td>
<td>Campus Network.Backbone_South</td>
<td>IF10</td>
<td>N/A</td>
<td>6.496</td>
</tr>
<tr>
<td>192.0.130/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>192.0.0.2</td>
<td>Campus Network.Backbone_East</td>
<td>IF10</td>
<td>N/A</td>
<td>0.000</td>
</tr>
<tr>
<td>192.0.140/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>192.0.0.2</td>
<td>Campus Network.Backbone_East</td>
<td>IF10</td>
<td>N/A</td>
<td>0.000</td>
</tr>
<tr>
<td>192.0.150/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>192.0.0.2</td>
<td>Campus Network.Backbone_East</td>
<td>IF10</td>
<td>N/A</td>
<td>0.000</td>
</tr>
<tr>
<td>192.0.160/24</td>
<td>RIP</td>
<td>120</td>
<td>1</td>
<td>192.0.0.2</td>
<td>Campus Network.Backbone_North</td>
<td>IF11</td>
<td>N/A</td>
<td>8.580</td>
</tr>
<tr>
<td>192.0.170/24</td>
<td>RIP</td>
<td>120</td>
<td>1</td>
<td>192.0.0.2</td>
<td>Campus Network.Backbone_North</td>
<td>IF11</td>
<td>N/A</td>
<td>8.580</td>
</tr>
<tr>
<td>192.0.180/24</td>
<td>RIP</td>
<td>120</td>
<td>1</td>
<td>192.0.0.2</td>
<td>Campus Network.Backbone_West</td>
<td>IF4</td>
<td>N/A</td>
<td>8.769</td>
</tr>
</tbody>
</table>

Gateway of last resort is not set.
4.5.4 Comments

RIP V2 create greater traffic than v1 because we disable auto summary in v2 scenario so sub-networks are advertised out of their major networks. as we will see from routing tables

In the auto summary the major networks are summarized so they have only one entry in forwarding tables when the auto summary is disabled the major network will have 2 entries in the tables which will create greater traffic in the network.
CHAPTER 5: CONCLUSION

From the simulation results the EIGRP give the best performance when compared with RIP, IGRP and OSPF. EIGRP generate the least traffic and thus it will consume the least bandwidth, leaving enough bandwidth for transmission of data.

EIGRP also has the best performance in the case of topology changes; it has the least dropped traffic compared to the other distance vector routing protocols. So EIGRP should totally replace IGRP. But EIGRP is a CISCO proprietary protocol, which means that it can only be used on CISCO products.

The routing information protocol (RIP) has many limitations, it generates high traffic that can cause a congestion in slow networks, and it maximum hop count is 15 hop, that limits the use of RIP in a small, fast networks. RIP will be really bad choice in slow networks.

The performance of RIP can be improved using the triggered extension mode, which decrease the traffic generated by the RIP, enabling the auto summary will also decrease the traffic generated by the RIP.

The open shortest path first protocol (OSPF) has a short convergence time and have a maximum hop count of 255 hops; it can be perform efficiently in small and large networks that use routers from other manufacturers other than CISCO systems.
REFERENCES


[3] www.oscentre.co.nr


