Critical Analysis of the EIGRP Routing Protocol

Mr. Syed Islam
02027760
syi001@londonmet.ac.uk

Supervisor : Mr. Tarik Molalign
t.molalign@londonmet.ac.uk

A Dissertation submitted in partial fulfilment
of the requirements of London Metropolitan University for
the degree of Bachelor of Science in Computer Networking with Honours

May 2006

Department of Computing, Communications Technology and Mathematics (CCTM)

Acknowledgements

I would like to thank my project supervisor Mr. Tarik Molalign, senior lecturer CCTM, London Metropolitan University for his continuous support during the course of the project. Mr. Molalign provided valuable guidance and feed back during the research and implementation of the project. I would also like take this opportunity to express my gratitude to Dr. Nicholas Ioannides and Mr. Harry Benetatos for their support and guidance to ensure the success of this project.

Finally I would like thank all my fellow students who have provided ideas and have extended their support during the project.

Abstract

Routing Protocols are one of the key issues that influence the efficiency and availability of modern computer networks. EIGRP is a hybrid routing protocol that has been developed by Cisco Systems as an enhancement to its predecessor IGRP. The protocol has the ease of implementation as that of simple distance vector protocols but boasts abilities and features similar to those of complex link state protocols like OSPF. It uses newly developed key technologies to achieve fast convergence times and loop free routing. The protocol is becoming very popular and is being widely deployed in large-scale networks around the world. During the project the use of routed and routing protocols were researched. EIGRP was thoroughly researched and compared to other routing protocols. Capabilities and advanced features of the protocol were then tested and analyzed by its deployment in test networks. Evaluation of the test results and the research was carried out. This report outlines the requirements, needed to increase performance of networks which employ EIGRP. This final project report provides a good documentation on EIGRP which can be used for gaining understanding of the protocol.

Contents

Chapter 1 – Introduction

List of Figures

Chapter 3 – Routed Protocols

Chapter 4 – Routing Protocols

Chapter 5 – EIGRP (Theoretical Review)

Chapter 6 – Operational Analysis of EIGRP

List of Tables

Chapter 1 – Introduction

Chapter 3 – Routed Protocols

Chapter 4 – Routing Protocols

Chapter 5 – EIGRP (Theoretical Review)

Chapter 6 – Operational Analysis of EIGRP

Chapter 7 – Project Review

Abbreviations

AARP	AppleTalk Address Resolution Protocol
ADSP	AppleTalk Data Stream Protocol
AEP	AppleTalk Echo Protocol
AFI	Address Family Identifier
AFP	AppleTalk Filing Protocol
AS	Autonomous Systems
ASP	AppleTalk Session Protocol
ATP	AppleTalk Transaction Protocol
BGP	Border Gateway Protocol
BGP	Border Gateway Protocol
CIDR	Classless InterDomain Routing
CPU	Central Processing Unit
DDP	Datagram Delivery Protocol
DUAL	Diffusing Update Algorithm
EGP	Exterior Gateway Protocol
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
FDDI	Fiber Distributed Data Interface
FSM	Flexible Single Master Operations
FSM	Finite State Machine
HFS	Hierarchical File System

ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
IHL	Internet Header Length
InterNIC	Internet Network Information Center
IOS	Internetworking Operating System
IP	Internet Protocol
IPng	Internet Protocol Next Generation
IPX	Internetwork Packet Exchange
IS-IS	Intermediate System-Intermediate System
ISP	Internet Service Provider
LSA	Link State Advertisement
MTU	Maximum Transmission Unit
NBP	Name-Binding Protocol
NIC	Network Interface Card
OSI	Open Systems Interconnect
OSPF	Open Shortest Path First
OSPF	Open Shortest Path First
PAP	Printer Access Protocol
PDM	Protocol Dependent Modules

PDU	Protocol Data Unit
QoS	Quality of Service
RFC	Request For Comments
RIP	Routing Information Protocol
RTMP	Routing Table Maintenance Protocol
RTMP	Routing Table Maintenance Protocol
RTO	Retransmission Timeout
RTP	Real-Time Transport Protocol
SAF	System Authorization Facility
SIA	Stuck In Active
SPF	Shortest Path First
SRTT	Smooth Round Trip Time
TCP	Transmission Control Protocol
TLV	Type/Length/Value
UDP	User Datagram Protocol
VLSM	Variable Length Subnet Masking
WBS	Work Breakdown Structure
ZIP	Zone Information Protocol

CHAPTER 1 – INTRODUCTION

1.1 Background

Modern day Businesses rely very heavily on their computer systems to provide high productivity and to perform many services essential to making a profit. Computer Networks are always employed in large organizations so that data and resources can be centralized and shared. These systems are vital to the work that most large organizations carry out. When networks go down, it usually means a loss of productivity and performance for the company. The larger the company, the greater the loss, for some global companies network downtime is so critical that it can equate to millions of pounds of profit loss for each downtime hour or even each minute in some cases. Large organizations that have branches in different cities or even in different countries have extremely large networks. Due to the vast area that the networks cover and the great number of links in them they are more prone to failure. When network size is large and modern day applications are being used, a lot of traffic is generated on the network which needs to be handled and managed efficiently, for the network to be able to provide the level of performance required. It is vital to decrease network downtimes and increase its availability, so that the users are able to make full use of the facilities to increase productivity.

Routed Protocols are used to handle the encapsulation of the data that is transmitted on a network. There are many routed protocols available with IP, IPX and AppleTalk being the most common. IP is the most popular of the protocols and is most widely used around the world. The Internet is the largest network in the world and uses TCP/IP as its protocol. [1, 65]

Routers are devices that are primarily used to route traffic through networks [1]. Routers that connect different networks or different parts of a large network play a vital role in maintaining the efficiency of the network. To be able to efficiently forward traffic and increase network performance a router needs to know the best path through which a packet can be sent, in order to reach its destination. The protocols that routers use to exchange the path information or routing information is known as Routing Protocol. [1, 65]

Routing protocols have to be very efficient and need to provide routers with accurate and up-to-date information about routes. If there are any path changes in the network or a link becomes unavailable this information needs to be passed on to routers as quickly as possible. Incorrect routing information can cause routers to send traffic down wrong paths causing congestion in networks and ultimately reducing efficiency and availability of the network. Thus routing protocol and its performance is very closely related with routers performance, which in turn dictates network efficiency. Some of the most common routing protocols used are RIP, IGRP, OSPF and EIGRP, each having its own characteristics, advantage and disadvantage.

Enhanced IGRP is a hybrid routing protocol developed by Cisco Systems as an enhancement to IGRP. It is being widely employed by many large-scale organizations and companies in their networks. Some of the key improvements of EIGRP over IGRP include fast convergence, support for variable-length subnet mask, support for partial updates, and support for multiple network layer protocols. To provide superior routing performance, Enhanced IGRP employs four key technologies that combine to differentiate it from other routing protocols: neighbour discovery/recovery, reliable transport protocol (RTP), DUAL finite-state machine, and protocol-dependent modules. Although EIGRP is regarded as an interior gateway protocol (IGP) may also be used as an exterior gateway routing protocol for inter-domain routing due to its robustness and its capabilities to scale well in large networks. [1, 6, 22]

Routing protocols need to be conFigured on routers according to specific network requirements. Performance of routing protocol and the router depends largely on correct configuration settings being used on the routers. The configuration requirements are specific to the network requirements and dictate the configuration of the router. When deploying EIGRP in a network its advanced capabilities and features such as Load Balancing and Route Summarization can be used to increase network efficiency. It is therefore required to have a very good understanding of how EIGRP works and the configuration requirements that are needed to make use of these advanced features.

During the project different routing protocols were compared and EIGRP was be analyzed in depth. The knowledge gained from the analysis and research was used design test networks to test the capabilities of EIGRP. Evaluation of the test results and the research carried out and is being documented in the form of this report. The report will also outline major troubleshooting issues that exist for EIGRP deployment and give possible solutions to the problems.

1.2 Aim

The aim of the project is to perform critical analysis of EIGRP routing protocol and outline configuration requirements to gain optimum routing performance in EIGRP networks, by making use of advanced features of the protocol.

1.3 Objectives

1.3.1 Academic Objectives

The objectives of the project are:

- To explain the need for Routed protocols and briefly describe commonly used Routed Protocols.
- To explain the need for Routing Protocols and compare routing protocols in common usage.
- To provide a background to EIGRP and its evolution from IGRP.
- To provide detailed information about EIGRP along with its advanced technologies, key features and capabilities such as: fast convergence, support for variable-length subnet mask, support for partial updates, support for multiple network layer protocols, neighbour discovery/recovery, Reliable Transport Protocol (RTP,) DUAL finite-state machine, Load Balancing, topology Table, neighbour Table and routing Table.
- To discuss and produce the configuration process/ requirements for Implementation and Troubleshooting of EIGRP.
- To design a test network and the different testing scenarios to analyze and test capabilities of the protocol.
- To conduct analysis of the protocol by deploying it in the Test network under Lab conditions

- To use the test results and research to produce a report to show the actual capabilities of the protocol.

1.3.2 Personal Objectives:

Along with the other objectives of the project, the following personal objectives have been targeted to be fulfilled –

- Improve knowledge on the subject area.
- Develop and demonstrate written communication skills through the project report
- Further develop appreciation of different areas of project management
- Successfully follow the project plan to find the final recommendations for deployment
- Be aware of various research sources and methods to improve research skills
- Improve documentation and review skills
- Demonstrate abilities to identity key success elements of a project

1.4 Justification

The project will focus mainly on EIGRP routing protocol and its usage. There were several reasons for undertaking this project, some of which are briefly described below:

- EIGRP is the most recent routing protocol released by Cisco and is described as a hybrid protocol which is as easy to implement as IGRP but provides advanced capabilities such as link sate routing protocols. This project would allow for research of new technologies that were added to the protocol.

- One of the major problems with the implementation of EIGRP is lack of documentation available about it [5]. This is due to the fact that it is a proprietary protocol and the documentation provided by Cisco is all that can be found. This project would be used to produce a comprehensive report to the abilities, implementation and troubleshooting of the protocol which may be used during implementation of the protocol.

- Routing protocols are still being developed and new protocols are being researched and designed to increase routing efficiency. As the project would look in depth into EIGRP it is very possible that it may lead finding of flaws or possible enhancements that can be made to the protocol. This may lead to recommendations on improvements that can be made to the protocol and further research into new technologies.

- The project is being undertaken as the part of a degree in Computer Networking. This project will successfully show the knowledge gathered during the course and also enhance future development in academic knowledge. It will also enhance personal portfolio increasing opportunities of gaining career objectives. Network administrators and designer with sound knowledge of EIGRP protocols are in great demand, which will further enhance chances of meeting personal career goals.

1.5 Scope

Defining the scope of a project is of utmost importance to its success. The scope is generally very closely related with deliverables, time and cost of the project. These criteria are also normally used to measure the success of the failure of a project.

However, in the case of this particular project the criteria are different due to the nature of the project. As already mentioned the project is being undertaken as a part of degree course and has no cost issues related to it. The scope of the project is limited by the time and the strict deadline that have to be maintained to produce the required deliverables.

The scope of the project was limited to research about the relevant topics and the execution of the experiments that was used to perform analysis of the EIGRP routing protocol. Although research about EIGRP went into depth, the source code of the protocol was not analyzed or dealt with during the project. Areas directly related to the source code of the protocol were beyond the scope of this project. The practical experiments that were carried out were limited to the use and configuration of EIGRP using standard Cisco IOS. No special protocol analyzer or packets snuffers were used.

The functionality and behaviour of EIGRP were researched both theoretically and practically through experiment carried out on test networks. Research information, results from experiments and tests conducted were used to verify the findings of the research and to produce documentation related to the implementation and usage of the protocol.

1.6 Deliverables

The deliverables of projects vary according to the purpose of the project. The deliverable of a project can vary from gaining understanding, production of a report to manufacturing of a product. As this is an academic project that is being carried out as a part of a degree course it had set of defined variables each with specific requirements and deadlines. The deliverables of the project are detailed below.

1.6.1 Project Proposal Presentation

A presentation was given to the academic staff concerned with supervising the final year networking projects. This presentation was used to put forward the project proposal and to convey the idea of what is expected at the completion of the project. The deadline for this deliverable was 10th January 2006.

1.6.2 Project Development Website

A website was designed that held all related information about the project proposal. The website contained the project proposal, the presentation slides and details of the supervisor. The website also contained the proposed Table of contents of this final project report. The deadline for this was 17th January 2006.

1.6.3 Project Proposal Report

The project proposal was also delivered in the form of a report for approval by the supervisor. The report contained the project aim, objectives, methodology, and project planning and management details. The deadline for the submission of the proposal was 17th January 2006.

1.6.4 Journal Publication

A journal publication has also been produced. The publication outlines the finding of the research, experiments and analysis of the test results done during the project. The deadline for submission of the publication is 26th May 2006.

1.6.5 Project Implementation Website

This is an extension to the Project Development website to include the project implementation details. The website now also contains this project report, images from logbook that was used during the project, CV, updated WBS, Updated Gantt Chart and Updated Pert Chart. The deadline for submission of this deliverable is the 2nd June 2006.

1.6.6 Final Project Report

This final project report had to be produced to contain all the relevant details about the project. The deadline for the submission of this report is 19th May 2006.

1.7 Approach / Methodology

A modular approach has been used to break the project down into several stages. This methodology used allowed strict deadlines for each stage can be assigned and followed to ensure that the project gets completed within the given deadline. The approach used also ensured that each of the objectives set out for the project was met in order to achieve the aim of the project. The task carried out during the actual project was divided into four major phases with each phase having sub-stages to them. The major phases are given below and further task breakdown may be found in the next section.

1.7.1 Research

This first phase consisted of all the research that needed to be carried out for the project. The research method that was used is known as "Action Research" [42]. During the research primary, secondary and tertiary source of data was actively searched and related material was documented so that they could be later used during the design and the write up of this report. The research was carried out on three main areas which are described below.

1.7.1.1 Routed Protocols

Research and investigation was carried out using materials obtained from books, Internet and journals. Research carried out on this topic was not very through or did not go into much depth. It was used to gain an understanding and an overview of routed protocols. Chapter 3 of this report is dedicated to routed protocols, where their needs and relations with routing protocols are explained.

1.7.1.2 Routing Protocols

Research on routing protocols was carried out using materials found in books, journals, conference papers and the Internet. This research was elaborate then that carried out for the previous topic. The research allowed for comparison of the different routing protocols and also gain understanding about the evolution of

EIGRP from IGRP. The information obtained from this part of the research was used to dedicate a construct chapter 4 of this report about the routing protocols.

1.7.1.3 EIGRP

Books, conference papers, white papers, previous research materials and online material was used to carry out a through research of the EIGRP routing protocol. This was used to gain understanding of all the key technologies and advanced features of the protocol. Key technologies or areas that were researched in details were: support for VLSM, manual route summarization, automated route summarization, re-distribution with other routing protocols, convergence issues, partial updates, support for multiple network layer protocols using protocol dependant modules, neighbour discovery/recovery, usage of RTP, DUAL, route selection, Tables used, route tagging, bandwidth usage for updates, load balancing over equal cost paths, load balancing over unequal cost paths and SIA problem. Configuration, implementation and troubleshooting issues of the protocol were also researched to obtain a complete understanding of the capabilities and drawbacks of the protocol. This research was used to write chapter 5 in this final report outlining key factors associated with EIGRP and also helped in the design of the test network.

1.7.2 Design of Experiments

At completion of the research phase enough knowledge the next phase of the project was put into action. This is the Design of Experiments phase. During this phase of the project the knowledge gained from the research previously carried out was used to design the experiments used to analyze EIGRP. Firstly the materials gathered from the research were used to determine the features of the protocol that need to be analyzed and then the design of the scenarios and the test network were done which needed to be simulated to execute the experiments. Details of the experiments are given in the chapter 6 of this report.

1.7.3 Practical Work

After the network was designed and the experiments that were to be carried out had been decided upon the next phase of the project was undertaken. During this phase practical work was carried out using the NETLAB and simulation networks setup in the labs. The configuration requirements for the scenarios were taken from the research that had been done on EIGRP configuration and implementation. These different scenarios were manipulated to provide the situation that was to be analyzed to ascertain the capabilities of the protocol under certain situations. NETLAB was used extensively to perform experiments and obtain relevant results. The results of the experiments and their evaluation and analysis can be found in chapter 7 of this report.

1.7.4 Analysis of Results and Evaluation

The final phase of the project was to analyze the results from the experiments conducted. During this stage the final project report, journal and project development website were also produced. This project report used the research that had been carried out and the experiment results to provide an analysis of the EIGRP routing protocol along with supporting evidence and draw appropriate conclusions.

1.8 Project Plan & Management

“Project Management is the discipline of defining and achieving targets while optimizing the use of resources (time, money, people, materials, energy, space, etc) over the course of a project (a set of activities of finite duration).” [69]

1.8.1 Overview

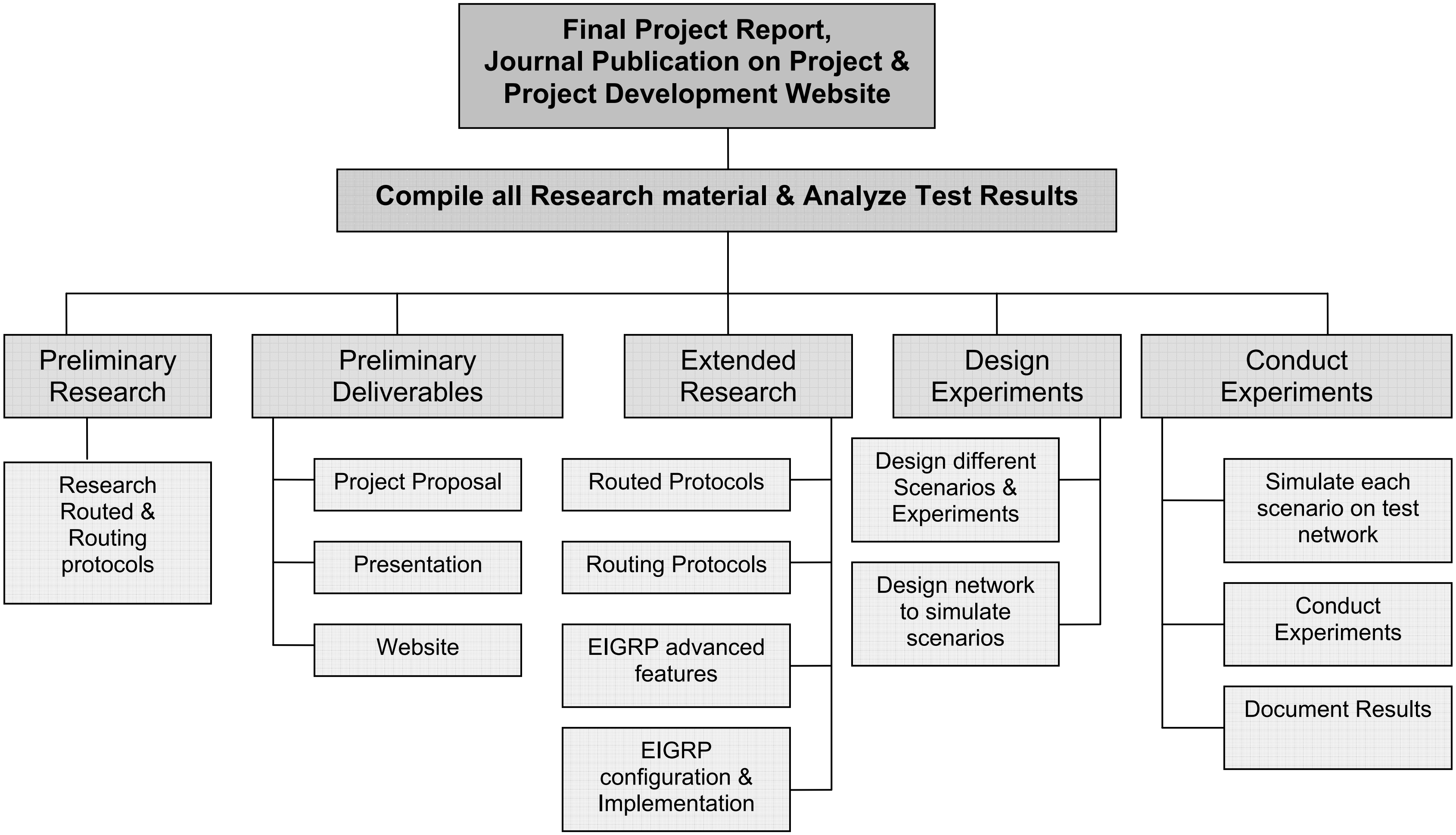
Project management is the use of knowledge, skills, tools and techniques to a wide range of activities in order to meet the requirements of the particular project [67]. The objectives of project management are to:

- Ensure Projects are Delivered within the Budgeted Cost
- Ensure Projects are Delivered within Schedule Commitments
- Deliver Quality Solutions

    - Reduced Errors
    - Improved Effectiveness
    - Appropriate Risk Management and Internal Controls
- Continuous Project Improvement through Collaboration
- Develop and Manage Project Communications and Oversight [67]

A project plan is "A formal, approved document used to guide both project execution and project control. The primary uses of the project plan are to document planning assumptions and decisions, facilitate communication among stakeholders, and document approved scope, cost, and schedule baselines.” [10]

1.8.2 Work Breakdown Structure



Final Project Report, Journal Publication on Project & Project Development Website
Compile all Research material & Analyze Test Results
Preliminary Research
Research Routed & Routing protocols
Preliminary Deliverables
Project Proposal
Presentation
Website
Extended Research
Routed Protocols
Routing Protocols
EIGRP advanced features
EIGRP configuration & Implementation
Design Experiments
Design different Scenarios & Experiments
Design network to simulate scenarios
Conduct Experiments
Simulate each scenario on test network
Conduct Experiments
Document Results

1.8.3 Project Scheduling

Project scheduling is the process of identifying when project activities will occur depending on defined durations and project activities [68]. Many IT projects are failures on meeting project scope, time and cost estimations [66]. Hence it is vital to produce a project schedule that would not only deliver the project in due time, but also to closely resemble the actual timing of activities in the project.

1.8.3.1 Initial Task List

Table 1.1 – Initial Task List

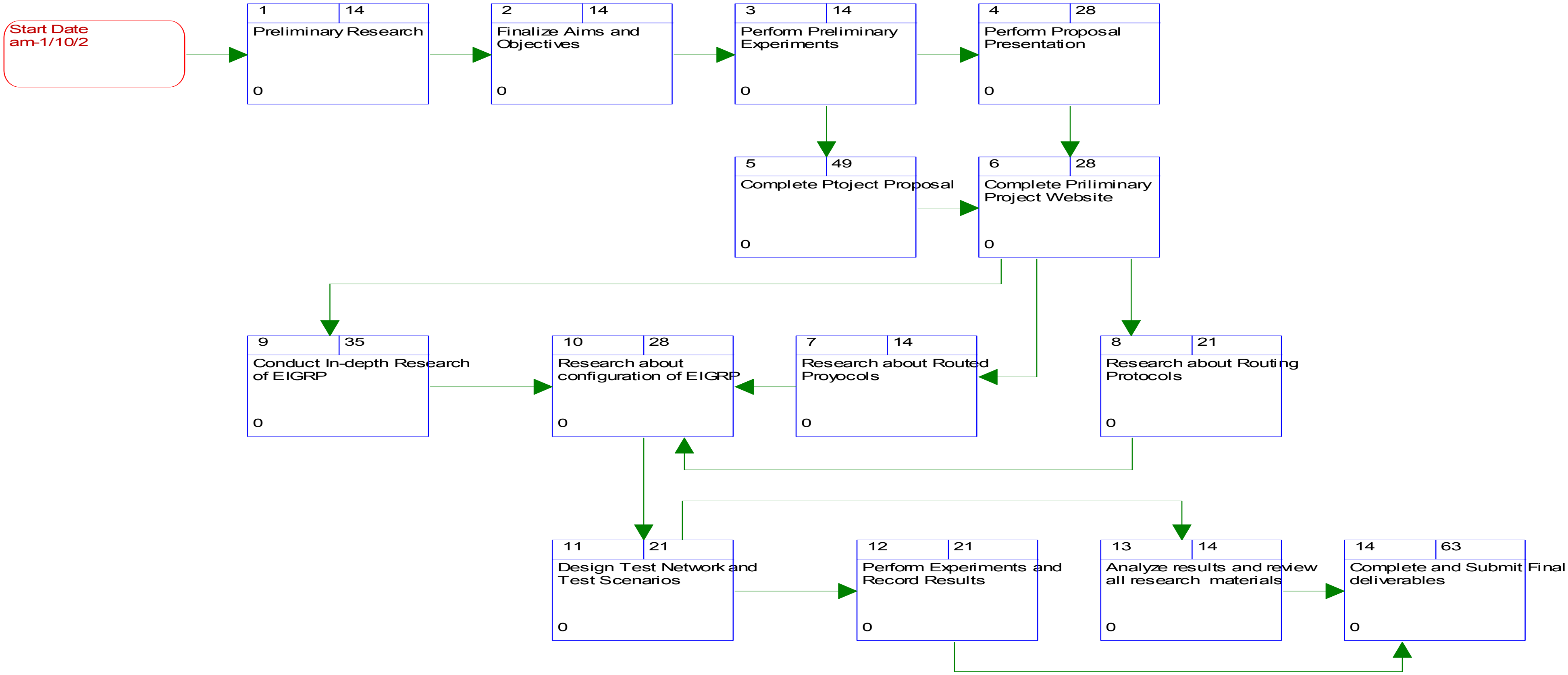
Task ID	Task Description	Duration (Weeks)	Dependency
A	Preliminary Research	2	-
B	Finalize of Aim and Objectives	2	A
C	Perform Preliminary Experiments	2	B
D	Presentation of Proposal	4	C
E	Project Proposal Completion	5	A,B,C
F	Project Proposal Website	4	A,B,C
G	Research about Routed Protocols	2	E,F
H	Research about Routing Protocols	3	F
I	Conduct in-depth research on EIGRP	3	G,H
J	Research about EIGRP Configuration, Implementation and Troubleshooting	3	I
K	Design Test Network and Test Scenarios	2	J
L	Perform Experiments and Record Results	3	K
M	Analyze results and review all research material	2	K
N	Compile, complete and submit final deliverables.	3	L,M

1.8.3.2 Initial Gantt Chart

Task	November ’05 (Weeks)				December ‘05 (Weeks)				January ‘06 (Weeks)				February ‘06 (Weeks)				March ’06 (weeks)				April ‘06 (Weeks)				May ‘06 (Weeks)			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
A - Preliminary Research		▨	■																									
B - Finalize Aims & Objectives			▨	■																								
C - Perform Preliminary experiments					▨	■																						
D - Project Proposal Presentation							▨	▨	▨	■																		
E - Complete Project Proposal							▨	▨	▨	▨	■																	
F - Complete Preliminary Project Website											■																	
G - Research about Routed Protocols.												▨	■															
H - Research about Routing Protocols												▨	▨	■														
I – Conduct In-depth research of EIGRP															▨	▨	■											
J - Research about configuration of EIGRP																		▨	▨	■								
K - Design Test Network & Test Scenarios																					▨	■						
L - Perform Experiments & Record results																							▨	▨	■			
M – Analyze results and review all research materials																							▨	■				
N - Complete and Submit final deliverables																										▨	▨	■

▨ - Task Ongoing ■ - Completion of Task

1.8.3.3 Initial Pert Chart


Start Date
am-1/10/2
1
14
Preliminary Research
0
2
14
Finalize Aims and Objectives
0
3
14
Perform Preliminary Experiments
0
4
28
Perform Proposal Presentation
0
5
49
Complete Ptoject Proposal
0
6
28
Complete Priliminary Project Website
0
9
35
Conduct In-depth Research of EIGRP
0
10
28
Research about configuration of EIGRP
0
7
14
Research about Routed Proyocols
0
8
21
Research about Routing Protocols
0
11
21
Design Test Network and Test Scenarios
0
12
21
Perform Experiments and Record Results
0
13
14
Analyze results and review all research materials
0
14
63
Complete and Submit Final deliverables
0

1.8.3.4 Updated Task List

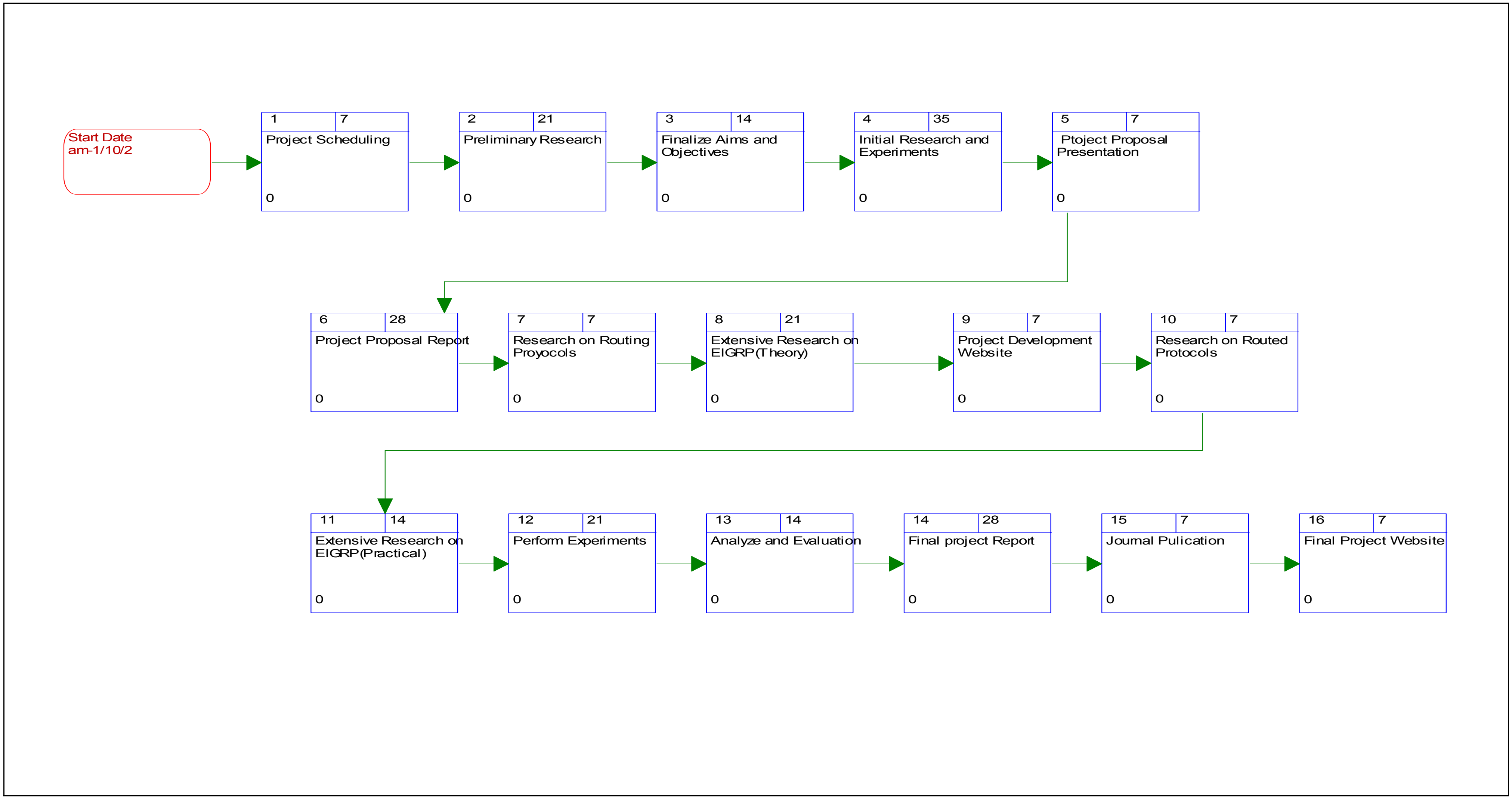
Table 1.2 – Final Task List

Task ID	Task Description	Duration (Weeks)	Dependency
A	Project Scheduling	1	-
B	Preliminary Research	3	A
C	Finalization of Aim and Objectives	2	B
D	Initial Research and Experiments	5	C
E	Project Proposal Presentation	1	D
F	Project Proposal Report	4	E
G	Project Development Website (Initial Version)	1	F
H	Research about Routed Protocols	1	G
I	Research about Routing Protocols	1	H
J	Extensive Research on EIGRP (Theory)	3	I
K	Extensive Research on EIGRP Configuration and Troubleshooting	2	J
L	Perform Experiments in the Lab environment	3	K
M	Analysis and Evaluation of Results	2	L
N	Compilation and Production of Final Report	4	M
O	Production of Journal Publication	1	N
P	Completion of the Project Website (Final)	1	O

1.8.3.5 Updated Gantt chart

ID	Task	Oct ’05 Weeks				Nov ’05 Weeks				Dec ‘05 Weeks				Jan ‘06 Weeks				Feb ‘06 Weeks				Mar ’06 Weeks				Apr ‘06 Weeks				May ‘06 Weeks			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
A	Project Scheduling	■																															
B	Preliminary Research		■	■	■																												
C	Finalizing Aim and Objectives					■	■																										
D	Initial Research and Experiments							■	■	■	■	■																					
E	Project Proposal Presentation												■																				
F	Project Proposal Report												■	■	■	■																	
G	Project Development Website															■																	
H	Research on Routed Protocols																■																
I	Research on Routing Protocols																	■															
J	Extensive Research on EIGRP (Theory)																		■	■	■												
K	Extensive Research on EIGRP (Practical)																				■	■											
L	Perform Experiments																						■	■	■								
M	Analysis & Evaluation																									■	■						
N	Final Project Report																											■	■	■	■		
O	Journal Publication																															■	
P	Final Project Website.																																■

1.8.3.6 Updated Pert Chart



1.9 Chapter Preview

A brief description about the contents of each chapter of this report can be found below.

1.9.1 Chapter 1 – Introduction

This chapter is used to provide background information related to the project along with aim, objectives, scope, approach, deliverables and project planning. It describes the direction of the project along with the way in which the project will be conducted.

1.9.2 Chapter 2 – Literature Review

This chapter is used to put forward all the material that was reviewed and used during the research. Summaries of information obtained from the sources are provided along with the relevancy of the information that is obtained from the source. The sources of the material include books, internet websites, published journals and white papers.

1.9.3 Chapter 3 – Routed Protocols

To understand EIGRP initial understanding of routed protocols are necessary. This chapter gives an overview of routed protocol. Explaining the need for routed protocols and gives more details about the major routed protocols, IP, Novell IPX and Apple Talk. It also marks the difference between routed and routing protocols.

1.9.4 Chapter 4 – Routing Protocols

After talking about routed protocols brief explanation is given about routing and how it works. The chapter also explains the way in which routing is achieved and the need for routing protocols. It goes further to describe some of the commonly used Distance vector, link state and hybrid routing protocols. This chapter cover protocols such as RIP, RIPv2, IGRP, OSPF and IS-IS in brief.

1.9.5 Chapter 5 – EIGRP

After providing a brief description about routed and routing protocols this chapter is used to describe EIGRP routing protocol in detail. It start of with a background to it evolution from IGRP and moves on to the principles of the protocols and its underlying technologies. It then goes on to describe and explain the advanced feature of the protocol, issues of designing networks with the protocol, troubleshooting issues and finally configuration requirements.

1.9.6 Chapter 6 – Operational Analysis of EIGRP

This chapter first outlines the functionalities, capabilities and issues of EGIRP that will be analyzed through its deployment in different scenarios. Experiments that were carried out along with the requirements for the experiments, tools and devices used and the expected outcomes are also given in the chapter. Analysis and evaluations of the results from the experiments are also present at the end of each experiment. This chapter gives details about all practical work that was carried out on EIGRP.

1.9.7 Chapter 7 – Conclusion

This chapter summarizes the work carried out during the project and the analysis of the protocol.

CHAPTER 2 – LITERATURE REVIEW

The literature review carried out focused on three main research areas Router Protocols, Routing Protocols and EIGRP. The sources of the literature include books, published white papers and the Internet. Some of the major literatures that have been reviewed during the course of the project are detailed below:

2.1 Books and White Papers Reviewed

- **Cisco Systems, Inc. (2003)** *CCNA 1 and2 – Companion Guide,* Cisco Press, 3rd ed. ISBN - 1587131102

  Summary: Chapter 7, 11, 15 and 16 of this book were used to learn about TCP/IP Protocol Suite and IP Addressing, Router Fundamentals, Routing Protocols and Distance vector routing protocols respectively. The book covers all the mentioned areas in details.

  The information available from the book was sufficient to write about distance vector protocols in the report. TCP/IP protocol suite and IP addressing was also covered by the book in details. Routing and Routing protocols were not covered in details which later had to be retrieved from other sources available.

- **Cisco Systems, Inc. (2003)** *CCNA 3 and4 – Companion Guide,* Cisco Press, 3rd ed. ISBN 1587131137.

  Summary: Chapter 4 (page 115-146) of this book is about EIGRP. The chapter provides a comparison of EIGRP to IGRP, conceptual overview of EIGRP, convergence and basic operations of DUAL, EIGRP terminology, EIGRP data structures, route summarization, basic configuration and troubleshooting.

  This book provides a simplified overview of the routing protocols and does not go into depth on any of the features or topics of the protocol. This source was able to provide a good overview of the protocol.

- **Malhotra, R. (2002)** *IP Routing,* O'Reilly, 1st ed. ISBN 0596002750.

  Summary: This book offers basic concepts of IP routing, free of hype and jargon. It begins with the simplest routing protocol, RIP, and then proceeds, in order of complexity, to IGRP, EIGRP, RIP2, OSPF, and finally to BGP. There is also quiet a lot of references to test networks with diagrams which help in understanding fundamental concepts behind each protocol. The chapter on EIGRP focuses on enhancements over IGRP: the use of DUAL; and the use of subnet masks in updates, which in turn allow VLSM and route summarization at arbitrary bit boundaries. It also gives comprehensive explanation of EIGRP Metric, Neighbour Relationship, Reliable Transport Protocol, EIGRP Packet Format, Route Summarization, configuration and troubleshooting.

The book provides a good background over development of EIGRP from IGRP and gives information about its advanced features. It is based more from a theoretical point of view and lacks the configurations for the advanced features. It however gives comprehensive overview and explanation of the other routing protocols, which allows them to be compared to EIGRP.

- **Pepelnjak, I. (1999)** *EIGRP Network Design Solution,* Cisco Press, ed. 1st ISBN 1578701651

Summary: *EIGRP Network Design Solutions* uses case studies and real-world configuration examples to help gain an in-depth understanding of the issues involved in designing, deploying, and managing EIGRP-based networks. It details proper designs that can be used to build large and scalable EIGRP-based networks, and documents possible ways each EIGRP feature can be used in network design, implementation, troubleshooting, and monitoring. It also gives detailed coverage of all EIGRP technologies, including DUAL, transport protocol, and topology database. In addition there is extensive coverage of EIGRP deployment over WAN and dial-up networks and information on such features as filter lists, route maps, summarization, EIGRP pacing, and MD5 authentication.

- **Aziz, Z. & Liu, J. (2002)** *Troubleshooting IP Routing Protocols (CCIE Professional Development Series),* Cisco Press, ed. 1st ISBN 1587050196.

  Extraction of chapter "Troubleshooting EIGRP" available on the Internet at http://www.ciscopress.com/articles/article.asp?p=27839&seqNum=5&rl=1

  Date of access: 18/11/2005 22:07

  Summary: This article provides extensive, hands-on guide for troubleshooting EIGRP. It explains how to solve complex routing problems through methodical, easy-to-follow flowcharts and step-by-step scenario instructions for troubleshooting. It also provides numerous protocol-specific debugging tricks that speed up problem resolution

- EIGRP – White paper available at http://www.ssuet.edu.pk/~amkhan/cisco/EIGRP_white_paper.pdf

  Date of access: 18/11/2005 23:31

  The white paper is also available from authenticated CISCO sites.

  Summary: The white paper provides detailed explanation on most EIGRP related topics. It gives details of EIGRP theory of operation, Split Horizon and Poison Reverse issues, Troubleshooting SIA, Redistribution, Route Summarization, Query Process and Range, Bandwidth configuration, Load

Balancing, Metric configuration, using Administrative Tags and detailed usage of show IP EIGRP Topology.

2.2 Web-Based Resources Reviewed

- http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2017.htm

  Date of access: 18/11/2005 22:29

  The above URL provides the link to the chapter titled “Integrating Enhanced IGRP into Existing Networks” which is a part of the Cisco “Internetwork Design Guide”. The website and its contents are maintained by CISCO Sys.

  Summary: This chapter provides a detailed guide to configuring EIGRP integration with other protocols. It provides various scenarios where the configuration is being done and also provides detailed explanations of how the integration is achieved. It covers adding EIGRP to a single IGRP network, adding EIGRP to multiple IGRP networks, adding EIGRP to a Novell IPX network and also adding EIGRP to an AppleTalk Network.

- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/en_igrp.htm#xtocid0

  Date of access: 18/11/2005 22:49

The above URL provides the link to the chapter titled "Enhanced IGRP" which is a part of the Cisco "Internetwork Design Guide". The website and its contents are maintained by CISCO Sys.

Summary: This chapter provides a brief history into the making of EIGRP and outlines the four key technologies that are employed by EIGRP along with simple explanation of DUAL, redistribution and migration to EIGRP.

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/np1_c/1cprt1/1ceigrp.htm *Date of access: 18/11/2005 23:09*

The above URL provides the link to the chapter titled "Configuring EIGRP" which is a part of the Cisco "Part2: IP Routing Protocols". The website and its contents are maintained by CISCO Sys.

Summary: This chapter describes how to conFigure Enhanced Interior Gateway Routing Protocol (E IGRP). It describes Cisco's EIGRP Implementation, EIGRP benefits, Configuration Task List, Common Configuration commands and provides scenarios to show common configuration mistakes that occur.

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fiprrp_r/1rfeigrp.htm *Date of access: 18/11/2005 23:23*

The above URL provides the link to the chapter titled "EIGRP Commands" which is a part of the Cisco "Command Reference". The website and its contents are maintained by CISCO Sys.

Summary: This page provides all the EIGRP command available with examples. This can be a very useful resource, which can be used when performing EIGRP configuration

- http://www.rhyshaden.com/eigrp.htm *date of access: 18/11/2005 21:53.*

Summary: This webpage gives brief information on EIGRP routing metrics but provides a comprehensive reference to EIGRP packets, Neighbour discovery and adjacencies, the DUAL Finite State Machine and Diffusing Computation.

- http://www.unix.org.ua/cisco/CCNP-CCDP/CID-Sybex/ewtoc.html *date of access: 19/11/2005 19:23.*

The above URL provides a link to the CCDP: Cisco Internetwork Design Study Guide.

Summary: Chapter 4 of this guide is concerned with designing networks for IP routing protocols. It has a subsection that is concerned with the network design for network using EIGRP. Although the guide doesn't provide much information about the protocol it highlights some design issues that need to be considered when designing networks for EIGRP. It gives an overview of the DUAL mechanism and provides an explanation with diagram about the convergence of EIGRP. It discusses other factors such as RTP, SIA, Load balancing and bandwidth usage.

- http://www.cisco.com/warp/public/105/46.html *date of access: 19/11/2005 20:17.*

The above URL provides a link to the document titled "How does Load Balancing work?" with the document id 5212 on the Cisco website.

Summary: The document provides a simple overview of the idea behind load balancing in networks. It also explains how the Cisco IOS on routers support load balancing by default. It then provides links to IGRP metrics and Explanations. It also provides another link to a document that details the method by which the metric of EIGRP can be manipulated to set preferred routes.

- http://www.cisco.com/warp/public/103/19.html *date of access: 19/11/2005 21:48*

The above URL provides a link to the document titled "How does Unequal cost path load balancing (Variance) work in IGRP and EIGRP?" with the document id 13677 authored by *Syed Faraz Shamim* on the Cisco website.

Summary: The document provides detailed information on how to perform load balancing on unequal cost path on a network. The document also provides significant explanation and diagrams of test networks that may be used during the course of the project. The document also outlines some of the required commands that are needed to perform load balancing with unequal cost paths.

- http://www.cisco.com/warp/public/103/18.html *date of access: 19/11/2005 22:24.*

The above URL provides a link to the document titled "What does EIGRP DUAL-3-SIA Error message mean?" with the document id 13676 on the Cisco website.

Summary: This document provides complete information about the EIGRP Stuck in Active issue. This is one of the major issues of EIGRP that a network administrator needs to have complete knowledge of in order to be able to reduce downtime. It give complete background information to the problem, the reasons for which the problem may occur and also the solutions to this problem.

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt2/1cdeigrp.htm *date of access: 19/11/2005 23:12.*

  Summary: This document provides information about Cisco EIGRP implementation. If provides the configuration commands that are needed for the deployment of EIGRP. This document also explains some configuration setting in details with the aid of diagrams and different scenarios. The configuration provided in this document mainly concerns transition to EIGRP from IGRP, adjusting EIGRP metric, disabling route summarization, manual route summarization, authentication, changing hold time , changing hello packet intervals, disabling split horizon and stub networks. It contains various examples of configuration to provide a better understanding of the related issues.

- http://www.ciscopress.com/articles/article.asp?p=24090&seqNum=3 *Last Date of Access: 12-05-2006 17:24*

  The above URL provides a link to the document titled “Dynamic Routing Protocols” found on the Cisco Press website.

  Summary: The document discusses in details Routing Protocol basics, Distance Vector Routing Protocols, Link state routing protocols, Interior and Exterior Routing Protocols, Static Routing and Dynamic Routing. This document was particularly useful during the report preparation. The various topics present on the article gives in dept explanation which was found very useful during the report. In the report this article has been referenced at several places marking the importance of the article to this report.

- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/netwarep.htm

  Last Date of Access: 12-05-2006 15:30

  The above URL provides a link to the document titled "Introduction to Netware IPX/SPX" found on the Cisco website.

  Summary: The document discusses in details IPX networks and their main features. The use of IPX and integration of EIGRP into IPX is also explained in details. This document was used to produce the section about IPX of this report.

- http://www.ciscopress.com/articles/article.asp?p=27839&seqNum=5&rl=1

  Last Date of Access: 13-05-2006 15:35.

  The above URL provides a link to the document titled "Troubleshooting EIGRP" found on the Cisco Press website.

  Summary: The article provides a comprehensive guide to troubleshooting Cisco EIGRP. It gives various scenarios and routing configurations where problems may occur. It also gives detailed explanation and solution to the problems. Each of the major troubleshooting steps is described using diagrammatic notation (Flowcharts).

- http://www.cisco.com/warp/public/103/trouble_eigrp.html

  Last Date of access: 11-05-2006 08:22.

  The above URL provides a link to the document titled "Troubleshooting EIGRP" found on the Cisco website.

  Summary: The documentation gives the steps to checking major problems and giving solution to them. The troubleshooting is divided into main areas such as: neighbour relationship, routing and redistribution problems. Main and sub flowchart for problems are provided and possible solutions are also indicated.

CHAPTER 3 – ROUTED PROTOCOLS

Prior to discussion about EIGRP and Routing protocols it is important to have a sound understanding of Routed protocols as they are closely related to the process of routing. This chapter is used to provide an understanding of how routed protocols relate to the system and describe routed protocols that are supported by EIGRP.

3.1 Overview

Protocols that are used to transfer data from one host to another across a network are called routed protocol. [1]. Routed protocols have the following two functions:

- They provide enough addressing information through the network layer so that packets can be routed to their desired destination.
- They define the format and use of the fields within a packet. Packets generally sent form end system to end system. [1]

Routed protocols are transported by routing protocols across an internetwork. Routed protocols are sometimes also are referred to as network protocols or routable protocols. These network protocols perform a variety of functions required for communication between user applications in source and destination devices, and these functions can differ widely among protocol suites. Network protocols occur at the upper five layers of the OSI reference model: the network layer, the transport layer, the session layer, the presentation layer, and the application layer. Routed protocols are protocols that are routed over an internetwork. [1, 65]

Some of the routed protocols are given below:

- Internet Protocol
- Novell IPX
- Open Standards Institute networking protocol
- DECnet
- Appletalk
- Banyan Vines
- Xerox Network System (XNS)

Packets that travel outside its originating network need to be routed by routers. However all routed protocols are not routable. Other then the ones mentioned above there are also non-routable protocols which cannot survive being routed. Non-routable protocols presume that all hosts they will ever communicate between are from the same network. That is the host or the sender is on the same subnet as the receiver and the data packets sent does not have to cross the network or the network segment boundary. Modern networks are almost always linked to the internet. Internet is made up of several thousands of networks all interconnected with each other. Any traffic sent through the internet has to travel through multiple routers. Modern networks including the internet are not tolerant of protocols that do not understand the concept of a multi-segment networks. This is why non-routable protocols have almost become obsolete [45]. Some of the non-routable protocols are given below:

- NetBEUI
- DLC
- LAT
- DRP
- MOP

3.2 Internet Protocol

The Internet Protocol (IP) is a part of the TCP/IP Protocol suit that is used on the Internet. It is one of the most successful and popular protocols in use today. It is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be routed through networks. IP is documented in RFC 791 IP has two primary functionality: providing connectionless, best-effort delivery of datagrams through an internetwork; and providing fragmentation and reassembly of datagrams to support data links with different maximum-transmission unit (MTU) sizes. As the name best effort suggests, IP does not guarantee delivery of datagrams. Reliability when using IP must be handled by an upper layer protocol. [46]

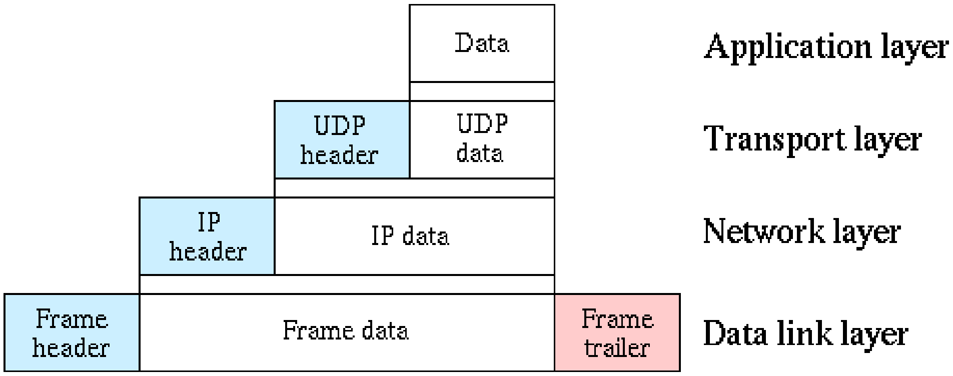


Figure 3.1 – Data Encapsulation

Figure 3.1 shows the encapsulation of data by the different layer of the OSI model. It can be seen that in the network layer UDP Datagrams are given IP header and converted to IP Packets. These IP Packets can be routed by routers in an internetwork. When a router receives an IP packet it uses the address information present in the IP header to route the packet towards its destination. The layered design also allows IP to be used over heterogeneous networks without making a difference to the upper layer protocols. There are two version of the Internet Protocol, the IP v4 and the IPv6. IP version four is the current and the most popular network layer protocol in use today. The current addressing scheme on the internet uses v4 of the protocol. Due to the massive boost in internet users IPv4 addressing scheme is not able to provide the number of required addresses. The updated version of the protocol which is IPv6 will be able to provide the addresses needed and fill the gap. IPv5 although invented was never deployed and was used only for experimental purposes. [46]

3.2.1 Internet Protocol V4

IPv4 is version 4 of the Internet Protocol which is also the first version that was deployed for commercial use. It is the most common of the routed protocols and is most widely used in the networks. It was also the only protocol that was used on the internet until recently. IPv6 which is Internet Protocol version 6 can also be found on a small portion of the internet. As with any other network-layer protocol, the IP addressing scheme is integral to the process of routing IP datagrams through an internetwork. Each IP address has specific components and follows a fundamental format. [46]

Each host on a TCP/IP network is assigned a unique 32-bit logical address that is divided into two main parts: the network number and the host number. The network number identifies a network. This must be unique and has to be assigned by the Internet Network Information Center (InterNIC) for the network to be part of the Internet. An Internet Service Provider (ISP) can obtain blocks of network addresses from the InterNIC and can itself assign address space as necessary. The host number identifies a host on a network and is assigned by the local network administrator. [46]

It uses a 32 bit addressing scheme gives a total of 4,294,967,296 unique IP addresses. All of these addresses are not usable as some them have been reserved for special purposes such as research. The 32-bit IP address is grouped eight bits at a time each group is separated by dots. To make the number more readable by humans they are also represented in decimal format (known as *dotted decimal notation*). The minimum and the maximum value of a group known as an octet are 0 and 255 respectively. Figure 3.1 gives a representation of the Dotted Decimal notation address and how its breaks into the four octet. The Figure shows 16 bits being allocated for the network address and 16 bits for the host address. This is just a general representation and is not true for the case of all IPv4 address. This classification will be explained in the later section.

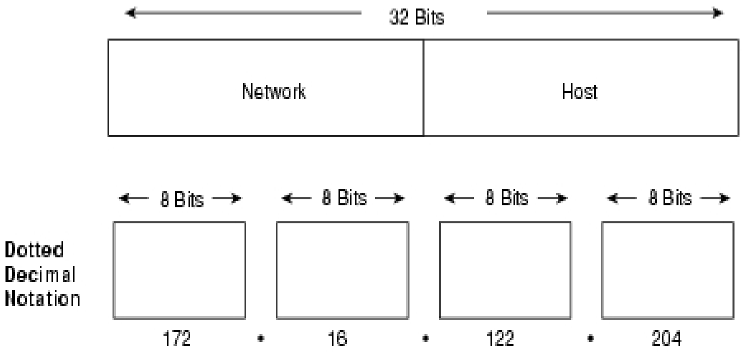


Figure 3.2 – Ipv4 Address Format [46]

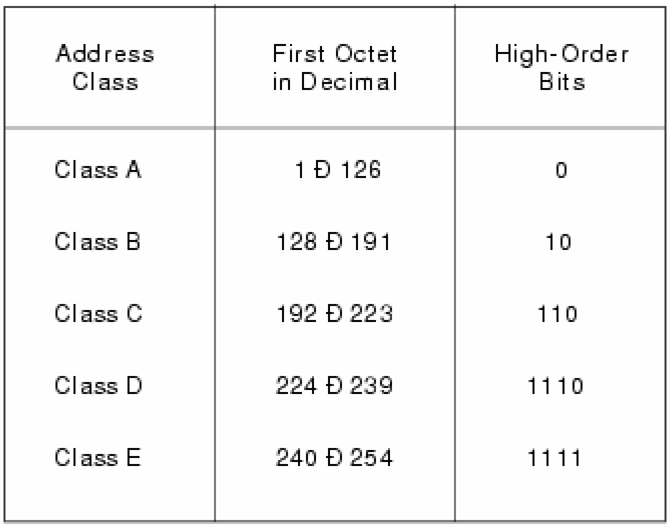
IPv4 addressing supports five different address classes: A, B, C, D, and E. Only classes A, B, and C are available for commercial use. Addresses from class D and E are reserved for experimental purposes. The high order bits of the first octet of an address are used to derive its class.

Table 3.1 that follows shows the address range and the format that are available in the different classes.

Table 3.1 IPv4 Address Range

IP Address Class	Format	Address Range	No. Bits Network/Host	Max. Hosts
A	N.H.H.H	1.0.0.0 to 126.0.0.0	7/24	16777214 (2^{24} - 2)
B	N.N.H.H	128.1.0.0 to 191.254.0.0	14/16	65534 (2^{16} - 2)
C	N.N.N.H	192.0.1.0 to 223.255.254.0	21/8	254 (2^{8} - 2)
D	N/A	224.0.0.0 to 239.255.255.255	N/A	N/A
E	N/A	240.0.0.0 to 254.255.255.255	N/A	N/A

As already mentioned above the class of the address is decided using the high order bits of the first octet of an address. Figure 3.3 shows the classification addresses according to their high order bits.



Address Class	First Octet in Decimal	High-Order Bits
Class A	1 Ð 126	0
Class B	128 Ð 191	10
Class C	192 Ð 223	110
Class D	224 Ð 239	1110
Class E	240 Ð 254	1111

Figure 3.3 – Classification of IPv4 Addresses. [46]

Figure 3.4 shows the difference is size of the network and the host portion depending on the class of the address. In this case it should be noted that each class has different number of octets assigned to its network address. Class A has a network address of 1 octet whereas class B and C have 2 and 3 octets respectively.

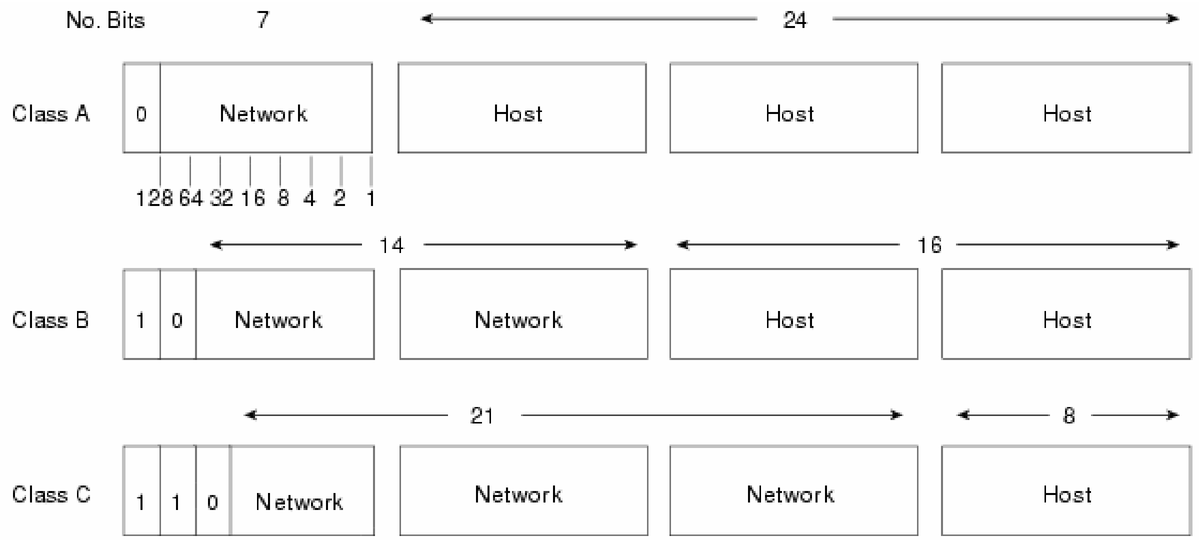


Figure 3.4 – Network and Host Division [46]

As already mentioned IPv4 is the most popular routed protocol currently found on the internet. The IP packet structure is flexible and can be of different length. The most common length found on the internet is 1500 bytes as this is the maximum allowed by most routers on the internet.

Figure 3.5 shows the format of the IPv4 Packets.

Figure 3.5 - IPv4 Packet Format [46]

0	Version	Header length	Type of Service (now DiffServ and ECN)	Total Length		
32	Identification			Flags	Evil Bit	Fragment Offset
64	Time to Live		Protocol	Header Checksum		
96	Source Address					
128	Destination Address					
160	Options					
160/192+	Data					

The following discussion describes the IP packet fields illustrated in Figure 3.5:

- *Version*—version of IP being used.

- *IP Header Length (*IHL) — Indicates the datagram header length in 32-bits

- *Type-of-Service*— Specifies how an upper-layer protocol would like a current datagram to be handled, and assigns datagrams various levels of importance.

- *Total Length*— Total length of the entire IP packet in bytes

- *Identification*—integer that identifying the current datagram. This field is used to correctly sequence fragmented datagrams

- *Flags*—3 bit field, with the LSB specifying if the packet can be fragmented. The middle bit specifies if this is the last fragment. MSB is not used.

- *Fragment Offset*— indicates the position of the fragment's data relative to the beginning of the data in the original datagram.

- *Time-to-Live*— a counter which is decremented by each hop that the packet passes. This is an inbuilt system to stop IP packets from endless looping.

- *Protocol*— upper layer protocol that the packet belongs to

- *Header Checksum*— used to check integrity of header.

- S*ource Address*— IP address of source host.

- *Destination Address*—IP address of destination host

- *Options*—Allows IP to support various options, such as security.

- *Data*—Contains upper-layer information.

There was a concern about the exhaustion of addresses available from IPv4 due to the tremendous growth of the internet. Around 1993, the classful networks were replaced with a Classless Inter-Domain Routing (CIDR) scheme. The new scheme allowed subdivision of networks to let entities sub-allocate IPs. This reduced the amount of wasted addresses on networks greatly reducing the number of IP address needed.

Some methods that were used to mitigate the IPv4 address exhaustion are:

- Network address translation or Port Address Translation
- Use of private network address
- Dynamic Host Configuration Protocol
- Virtual hosting
- Tighter control by Regional Internet Registries on the allocation of addresses to Local Internet Registries
- Network renumbering to reclaim large blocks of address space allocated in the early days of the Internet

The solutions were however just a means to delay the exhaustion and gave no real solution to the problem. IPv6 was developed which would allow 18 quintillion addresses (3.4e38 total addresses) as it uses 128 bits instead of 32 bits for each address. [46]

3.2.2 Internet Protocol V6

The primary goal of IPv6 was to provide more addresses to meet demands that would not be met by IPv4. In recent years mobile networking has really taken off and devices such as PDA, laptops and even mobile phones require IP addresses. It is predicted that in smart homes of the future everyday electronic devices that we use will be networked and will require IP addresses. IPv4 supports 4.3 billion addresses, whereas IPv6 supports up to 50 octillion addresses. Invented by Steve Deering and Craig Mudge at Xerox PARC, IPv6 was adopted by the Internet Engineering Task Force in 1994, when it was called "IP Next Generation" (IPng). [70]

In December 2005 IPv6 was deployed on the internet for the first time. At present, IPv6 accounts for a tiny percentage of the live addresses in the publicly-accessible Internet, which is still dominated by IPv4. The adoption of IPv6 has been slowed because of technologies mentioned, that partially alleviates address exhaustion. IPv4 is expected to be running alongside IPv6 for the foreseeable future. [70]

IPv6 is a conservative extension to IPv4. Most transport and application layer protocols need little or no change to work over IPv6. There are exceptions are Applications protocols that embed network-layer addresses (such as FTP or

NTPv3) however can not change over to IPv6 that easily due to change of the addressing format.[70]

The main characteristics of IPv6 are given below:

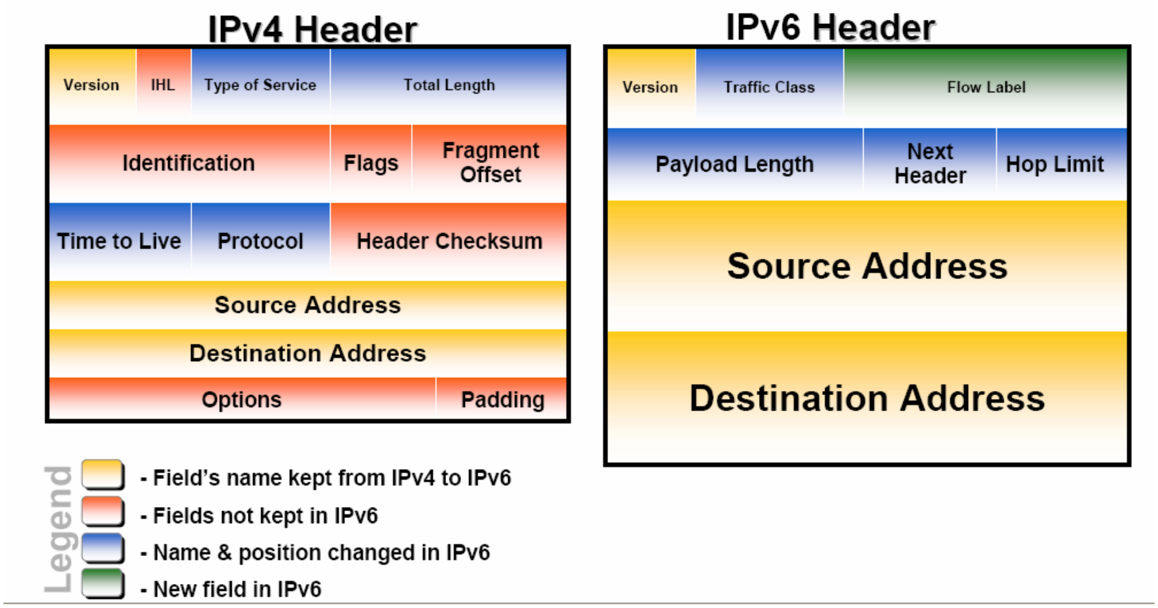
- Larger address space- It uses 128 bits to represent IP addresses giving it more addresses then IPv4
- Less Vulnerable to scanning
- More tolerant to malicious traffic
- Stateless auto configuration of hosts using DHCPv6
- Multicast abilities on both local link and across routers
- Jubmograms – Size of packet supported by IPv6 is more the 64kB increasing the network performance.
- Faster Routing – Simpler and Systematic header structure allows for faster routing
- Network-layer-security – IP network-layer encryption and authentication is available.

The primary and the most significant change from IPv4 to IPv6 is the length of network addresses. IPv6 addresses are 128 bits long (as defined by RFC 2373 and RFC 2374), whereas IPv4 addresses use 32 bits. IPv6 addresses are typically composed of two logical parts: a 64-bit network portion and a 64-bit host portion, which is either automatically generated from the interface's MAC address or assigned sequentially. They are normally written as eight groups of four hexadecimal digits.

For example, 2001:0db8:85a3:08d3:1319:8a2e:0370:7334.

An IPv6 network (or subnet) is a contiguous group of IPv6 addresses the size of which must be a power of two. The initial bits of addresses which are identical for all hosts in the network are called the network's prefix. There are no address ranges reserved for broadcast in IPv6 and applications use multicast to the all-hosts group instead. [70]

Figure 3.6 – IPv4 and IPv6 Packet Format [71]



The IPv6 packet shown in Figure 3.6 is composed of two main parts:

- Header - The header is the first 40 octets of the packet and contains both source and destination addresses (128 bits each), as well as the version (4-bit IP version), traffic class (8 bits, Packet Priority), flow label (20 bits, QoS management), payload length (16 bits), next header (8 bits), and hop limit (8 bits, time to live).
- Payload - The payload can be up to 64k in size in standard mode, or larger with a "jumbo payload" option which is discussed later.

Fragmentation of IPv6 packets are only done by the sending host. Routers in the network do not fragment IPv6 packets unlike IPv4 packets. The protocol field of IPv4 is replaced with a Next Header field for IPv6. This field usually specifies the transport layer protocol that the data contained belongs to.

In February 1999, The IPv6 Forum was founded by the IETF to drive deployment worldwide. On 20 July 2004 ICANN announced that the root DNS servers for the Internet had been modified to support both IPv6 and IPv4. [70]

A number of transition mechanisms are available that can be used for IPv6-only hosts to reach IPv4 services and to allow isolated IPv6 hosts and networks to reach the IPv6 Internet over the IPv4 infrastructure. The technologies are briefly described below:

- Dual stack - IPv6 is an extension of IPv4 which allows same network stack to support both IPv4 and IPv6. An implementation shared code network stack is called a dual stack, and a host implementing a dual stack is called a dual-stack host. This approach is described in RFC4213. Most implementations of IPv6 use a dual stack.

- Tunnelling - In order to reach the IPv6 Internet, an isolated host or network must be able to use the existing IPv4 infrastructure to carry IPv6 packets. This is done using a technique called tunnelling. Using this technique IPv6 packets are encapsulated within IPv4 so that transport can take place over the network. IPv6 packets can be directly encapsulated within IPv4 packets using a protocol called 41. Some routers on the internet block NAT stopping protocol 41 from traversing. UDP encapsulation can be used in such cases to overcome this problem. There are two types of tunnelling techniques that can be used to encapsulate IPv6 packets within IPv4 packets. They are:

    - Automatic Tunnelling – Tunnel endpoints are automatically determined by the routing infrastructure
    - Configured tunnelling - Tunnel endpoints are configured explicitly, either by a human operator or by an automatic service known as a Tunnel Broker. [70]

Although IPv6 provides many advantages, migration has proved to be a challenge and has raised many complications. A complete Internet adoption of IPv6 is unlikely and IPv4 is predicted to continue for may more years to come.

3.3 Novell IPX

Internetwork Packet Exchange (IPX) is a legacy network protocol used by the Novell NetWare operating systems. This is a layer three protocol and is similar to IP in the TCP/IP suite. IPX is a datagram protocol used for connectionless communications and similar to IP higher-level protocols, such as SPX and NCP, are used error control and recovery services. IPX uses the services of a dynamic distance vector routing protocols or a link-state routing protocol (NetWare Link-State Protocol [NLSP]). Cisco EIGRP provides support for IPX networks.

.Novell IPX network addresses are unique and are represented in hexadecimal format that consist of two parts: a network number and a node number. The IPX network number, which is assigned by the network administrator, is 32 bits long. The node number is usually the MAC address of the machine that is being addressed. [63]

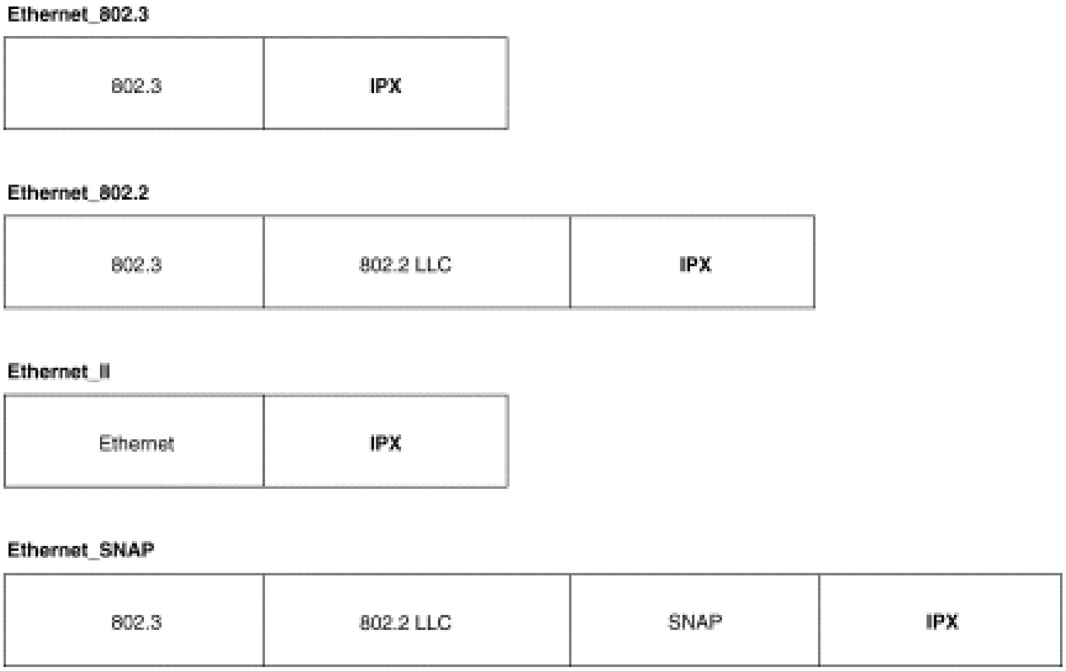
Novell NetWare IPX supports four encapsulation schemes on a single router interface as given below:

- Novell Proprietary - This serves as the initial encapsulation scheme. It is also known as 802.3 raw or Novell Ethernet_802.3.
- 802.3 – This is the standard IEEE 802.3 frame format and is also known as Novell_802.2,

- Ethernet version 2- Also called Ethernet-II or ARPA, Ethernet version 2 includes the standard Ethernet Version 2 header, which consists of Destination and Source Address fields followed by an EtherType field.
- SNAP- Also called Ethernet_SNAP, SNAP extends the IEEE 802.2 header by providing a type code similar to that defined in the Ethernet version 2 specifications. [21]

The four IPX encapsulation types are shown in Figure 3.6.

Figure 3.7 - Types of IPX encapsulation [63]



The length of an IPX packet is not fixed and can vary. The header of the packet is has a length of 30 bytes. Figure 3.7 shows the format of an IPX header. The payload varies according to the data that is being carried by the datagram.

Figure 3.8- IPX Packet Header Format [21]

8	16bit
Checksum	
Packet Length	
Transport control	Packet Type
Destination Network (4 bytes)	
Destination node (6 bytes)	
Destination socket (2 bytes)	
Source network (4 bytes)	
Source node (6 bytes)	
Source socket (2 bytes)	
Upper Layer Data	

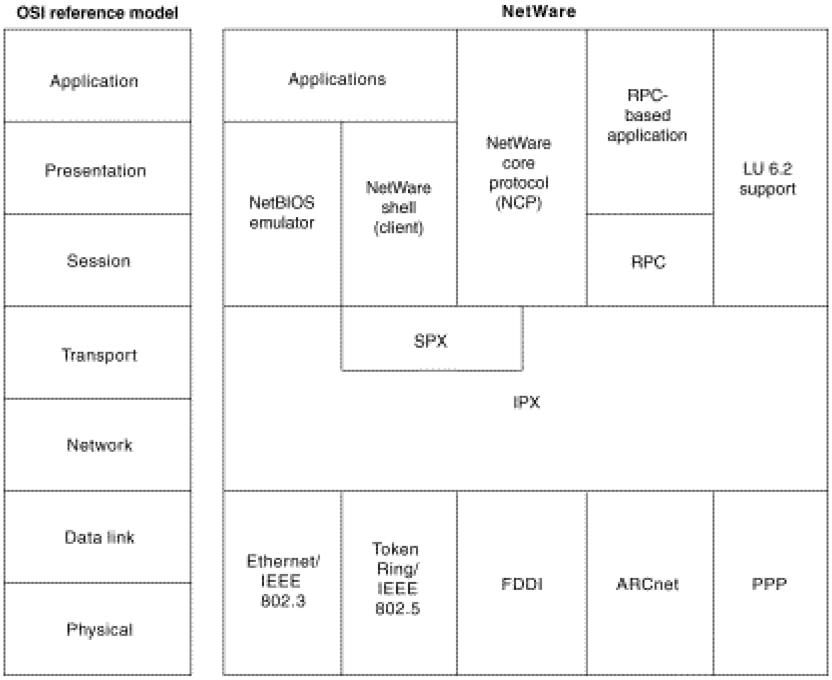
The header fields are explained below:

- *Checksum* – Contain the checksum for the header. Indicates that the checksum is not used when this 16-bit field is set to 1s (FFFF).
- *Packet length* - Specifies the length, in bytes,
- *Transport control* – Number of routers traversed by the packet

- Packet type- Specifies which upper-layer that the packet belongs to. It has two common values:
  - 5- Specifies Sequenced Packet Exchange (SPX)
  - 17- Specifies NetWare Core Protocol (NCP)
- *Destination network, Destination node, and Destination socket* - Specify destination information.
- *Source network, Source node, and Source socket* - Specify source information.
- *Upper-Layer data* — Contains information for upper-layer processes.

Figure 3.9 shows the Netware protocols and how the map to protocols in the OSI model.

Figure 3.9 - The NetWare Protocol Suite Map [63]



The Sequenced Packet Exchange (SPX) protocol is the most common NetWare transport protocol mapping to Layer 4 of the OSI model and resides on top of IPX in the NetWare Protocol Suite. SPX is a reliable, connection-oriented protocol that provides necessary reliability for IPX. Novell also provides support for IP in the form of UDP. IPX datagrams can be encapsulated inside UDP/IP headers for transport across IP-based networks. [63, 21]

IPX is still installed in millions of computers in the NetWare networks. However, due to the dominance of IP there has been a switchover from IPX to IP in many of the networks. Cisco EIGRP routing protocols has built in support for IPX networks.

3.4 AppleTalk

AppleTalk is a proprietary protocol architecture developed by Apple Computer Inc. AppleTalk has many characteristics as that of IP and IPX. AppleTalk transport and application services operate over a best effort delivery datagram protocol (Datagram Delivery Protocol, DDP). It provides reliable delivery by using the AppleTalk Data Stream Protocol (ADSP). AppleTalk is a multi-layered protocol providing internetwork routing, transaction and data stream service, naming service, and comprehensive file and print sharing. RTMP is a distance vector routing protocol used by AppleTalk. It is similar to IP and IPX RIP and uses hop count as its routing metric. [15]

AppleTalk addresses are 4 bytes long consisting of a two-byte network number, a one-byte node number, and a one-byte socket number. Apple injects hierarchy to its addressing scheme by assigning a given network a range of 16 bit network numbers, where each number in that range is capable of supporting 254 nodes. The network numbers on the routers need to be configured manually. Each node dynamically chooses its own node number using AARP protocol. All application-level protocols use dynamically-assigned socket numbers at both the client and server end which is also done automatically. [15]

Services in AppleTalk networks are defined using names rather then addresses. The names of the services are long to avoid duplication. A name in AppleTalk maps directly to a service being provided by a machine. In contrast DNS only translates names to address of machines disregarding the services that are provided by the host. A network-visible entity (NVE) is an AppleTalk network-addressable service, such as a socket. Each NVE must have at least one name and also has an attribute list associated with it. AppleTalk networks are logically divided into areas called zones. Each node in an AppleTalk network belongs to one and only one zone. Extended networks can have multiple zones. [15]

The design of AppleTalk closely resembles that of OSI model. To extend the addressing capability of AppleTalk networks and provide compliance with the IEEE 802 standard, Apple Computer introduced AppleTalk Phase 2 in 1989.

AppleTalk Phase 2 differs primarily in the range of available network layer addresses and the use of the IEEE 802.2 Logical Link Control (LLC) protocol at the Data Link Layer [15]. Figure 3.10 and Table 3.2 shows the mapping of the AppleTalk protocols to that of OSI model.

Figure 3.10 – AppleTalk protocols. [15]

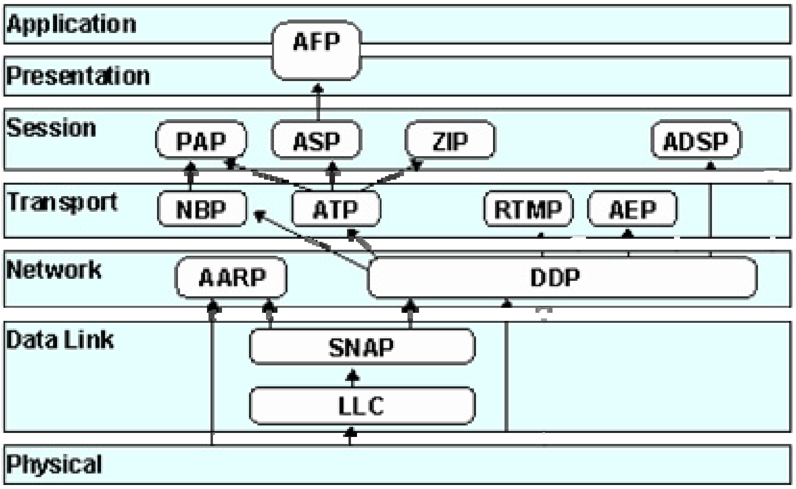


Table 3.2 – AppleTalk Protocols

OSI Model	Corresponding AppleTalk layers
Application	Apple Filing Protocol (AFP)
Presentation	Apple Filing Protocol (AFP)
Session	Zone Information Protocol (ZIP) AppleTalk Session Protocol (ASP) AppleTalk Data Stream Protocol (ADSP)
Transport	AppleTalk Transaction Protocol (ATP) AppleTalk Echo Protocol (AEP)

	Name Binding Protocol (NBP) Routing Table Maintenance Protocol (RTMP)
Network	Datagram Delivery Protocol (DDP)
Data link	EtherTalk Link Access Protocol (ELAP) LocalTalk Link Access Protocol (LLAP) TokenTalk Link Access Protocol (TLAP) Fibre Distributed Data Interface (FDDI)
Physical	LocalTalk driver Ethernet driver Token Ring driver FDDI driver

Brief explanation of the major protocols is given below:

- **AARP (AppleTalk Address Resolution Protocol)** - AppleTalk has plug and play architecture. When new nodes are connected they acquire a unique AppleTalk address, learn of resources and their locations dynamically. Nodes accomplish dynamic address configuration by using a feature of the AppleTalk Address Resolution Protocol (AARP) called Probe. A node proposes an AppleTalk address for itself, broadcasts the address over the network, and waits for a reply from any other node on the network claiming that the address in the probe is already in use. If the node doesn't receive a response, then it concludes that the address is unique on the network and assigns the address to its interface. If a response to a probe is received (i.e., another node has claimed the proposed address), the node proposes a new address, and repeats the probe process until it succeeds in acquiring an unused address, or until all assignable addresses are exhausted.

- **DDP (Datagram Delivery Protocol)** provides a datagram delivery and routing service to higher layer protocols. DDP is the lowest-level data-link-independent transport protocol. Like IP it does not provide a guarantee for delivery of data.

- **ZIP (Zone Information Protocol) -** Once an end node acquires an address, it uses ZIP during network initialization to choose a zone and to acquire internetwork zone information. An end node obtains zone and internetwork information from routers on the network by broadcasting ZIP messages requesting this information. Routers supply the zone name to network range bindings in ZIP replies.

- **RTMP (Routing Table Maintenance Protocol)** manages routing information for AppleTalk networks. RTMP can be regarded as a routing protocol for AppleTalk. It is similar to a distance vector routing protocol and maintains routing Table. It uses hop count as its metric similar to RIP.

- **AEP (AppleTalk Echo Protocol)** provides an echo service to AppleTalk hosts. It can specify up to 585 bytes of data for an echo transaction.

- **ATP (AppleTalk Transaction Protocol)** provides reliable delivery service for transaction-oriented operations. ATP uses a bitmap token to handle acknowledgement and flow control and a sequence of reserved bytes for use by higher level protocols.

- **NBP (Name Binding Protocol)** is a dynamic, distributed system for managing the use of names on AppleTalk networks. NBP maintains a names directory that includes names registered by hosts and bound to socket addresses. This can be compared to a DNS service only works in contrast.

- **ASP (AppleTalk Session Protocol)** manages sessions for higher layer protocols such as AFP. ASP issues a unique session identifier for each logical connection and continuously monitors the status of each connection. It maintains idle sessions by periodically exchanging keepalive frames in order to verify the session status.

- **PAP (Printer Access Protocol)** manages the virtual connection to printers and other servers. PAP is also used to convey connection status and coordinate data transfer.

- **ADSP (AppleTalk Data Stream Protocol)** provides reliable connection-oriented transport.

- **AFP (Apple Filing Protocol)** is the protocol for communicating with AppleShare file servers. It provides services for authenticating users and for performing operations specific to the Macintosh HFS file system.

- **PAP** is a protocol used in AppleTalk networks for communication with PostScript printers.

Like IP and IPX, routers forward data packets from source nodes to destination nodes across heterogeneous media. When a router receives a DDP packet, it checks to see if the packet's destination network number is the local network. If it is, the router passes the packet down to the data link layer which forwards the packet toward the destination node. If the destination network number is a different network, the router refers to its routing Tables to determine the next hop on the shortest path toward the destination. [15]

To forward a DDP packet to a directly connected node over a given medium, a router must know the hardware-specific address that corresponds to the destination node. Just as IP hosts and routers maintain an IP-to-hardware address cache and use IP ARP to maintain that cache, an AppleTalk router maintains list of mappings between AppleTalk and corresponding hardware addresses and uses AARP to maintain an Address Mapping Table. When the router attempts to send a packet to a given AppleTalk address, it scans its local AARP cache to find the corresponding hardware address. If the hardware address is not known, the router broadcasts a single AARP packet requesting the address mapping. The node whose AppleTalk address matches that specified in the request packet replies with the hardware address that corresponds to the AppleTalk address. The router then updates its address Table with this new information. [15]

AppleTalk is a remarkably easy network system to install and operate. The routing, naming, and addressing support system are demanding on the routed infrastructure: they consume CPU cycles and bandwidth, and rely heavily on the features of multi-access broadcast LANs such as Ethernet. AppleTalk is now deprecated by Apple in favour of TCP/IP networking. AppleTalk is now also considered clunky and often called 'chatty', notably on larger networks and WANs where the naming services generate considerable unwanted traffic. Today AppleTalk support is provided for backward compatibility in many products, but even the default networking on the Mac is TCP/IP. [15]

3.5 Chapter Summary

In this chapter routed protocols and their needs were described. Common Routed protocols such as IP, IPX and AppleTalk were also outlined briefly. IPv4 and IPv6 was described separately to provide and understanding of the complications with the current IP addressing system. IPX and AppleTalk protocols and their relation to OSI models were also discussed. This understanding of the routed protocols is particularly necessary before gaining an understanding of EIGRP and its functionalities.

The following project objectives have been achieved through this chapter:

- To explain the need for Routed protocols and briefly describe commonly used Routed Protocols.

The next chapter of this report will move the focus of the discussion from routed protocols to routing protocols. Prior to explanation of routing protocols, the chapter will provide and over view of routing and the different types of routing. Once routing process has been explained, routing protocols, classification of routing protocols will be explained. Later some of the common routing protocols that are in use will be explained at the completion which the routing protocols will be compared.

CHAPTER 4 – ROUTING PROTOCOLS

This chapter will explain routing, routing protocols and the different ways in which they can be classified. The chapter goes on further to provide a brief description of common routing protocols such as RIP, RIPv2, IGRP and OSPF. Detailed discussion on EIGRP will follow in the next chapter of this report. Classification of distance vector and link state routing protocols are explained. The idea of hybrid routing protocols are introduced and explained. This chapter provides the knowledge and background information necessary to appreciate and understand the technologies and functions of EIGRP.

4.1 Routing

Routing is the process of finding the most efficient path from one device to another and moving data through the path. Routing is an OSI layer 3 function that is performed by network devices known as routers. Data packets usually have to travel through many nodes or routers to go from the originating network to a remote destination. During the routing process, routers check destination address on packets and forward them through the routes that can be used to reach the desired destination. This forwarding is done on the basis of routing

Tables within the routers, which maintain a record of the best routes to various network destinations. [28, 29, 65]

Routing involves two basic activities:

- Determining optimal routing paths – There may be multiple paths that can be taken to reach a particular destination. Using special algorithms known as routing protocols routers decide the optimal path for each destination.
- Transporting packets through an Internetwork. – Once the router has decided on the path that the packet should be sent on, the packet is sent to the interface that is connected to the route.[65]

Routing can be classified into the following types which will be explained in the following sections:

- Static Routing
- Dynamic Routing

4.1.1 Dynamic Routing

Dynamic routing is a process in which routers automatically adjust to changes in network topology or traffic. The routers can adapt to any changes in the network very quickly without and intervention from an administrator. Routers that use dynamic routing exchange special packets containing their routing information with other routers on the network. These exchanges of routing information allow routers to learn of new routes and keep track of changes that occur in the network. The contents of the packets and their timing depend on the specific routing protocol that is being used. [64, 65]

4.1.2 Static Routing

The other type of routing is known as static routing where the system network administrator would manually configure network routers with all the information necessary for successful packet forwarding. The administrator constructs the routing Table in every router by putting in the entries for every network that could be a destination. Routers simply forward packets on the links that are defined for respective destinations. Such process does not offer any adaptability or fault tolerance because any changes of the network will not be reflected on the routing Tables automatically. The changes to the routes have to be made by manual correction of the routing Table. Static routing is based on routing Tables manually updated by network administrators. Modern networks are generally large and have many routes available through them. Manual Configuration of large networks is near impossible and leads to static routing being rarely used. However, there are circumstances where they offer significant advantage of dynamic routing. Complete static routing is never used due to the numerous possible destination networks. Static routes are generally used along side dynamic routing in order to define routes such as gateway of last resort. [1, 64, 65]

4.1.3 Dynamic Routing Versus Static Routing

Dynamic and Static routing can be differentiated using many criteria. Table 4.1 shows the difference between the two types of routing according to the various criteria.

Table 4.1 – Dynamic Routing Versus Static Routing

Criteria	Dynamic Routing	Static Routing
Scalability	Automatic	Routes need to be added
Adaptability	Automatic	Changes need to be made manually
Ease of Implementation	Medium	Easy
Bandwidth Usage	Ranges from low to high depending of protocol	Does not use any bandwidth to share routing information
Processing Power	Ranges from medium to high again depending on protocol	Low processing needed power needed
Compatibility		
Secure	Not secure as routes are sent via updates	Secure as route information is not shared
Efficiency	Efficient as it adapts to any changes	Not efficient as changes are not automated

4.2 Routing Protocols

Routing protocols facilitate the exchange of routing information between networks, allowing routers to build routing Tables dynamically. That is routing protocols enable routers to communicate and share information about available routes so that data can be routed. The exchange of routing information is done using special packets. Specifics of the packets, their contents and timing all depend on the particular routing protocol that is being used. Routing protocols use metrics to evaluate what path will be the best for a packet to reach its destination. A metric is a standard of measurement, such as path bandwidth or number of hops that is used by routing algorithms to determine the optimal path to a destination. To aid the process of path determination, routing protocols initialize and maintain routing Tables, which contain route information. Route information also varies depending on the routing algorithm used.

Routing protocols have the following functions:

- To provide process for sharing routing information
- Allow routers to update and maintain routing Tables based on information from other routers using specific algorithms. [1, 24, 64, 65]

A routing protocol describes the following:

- How updates are sent
- What knowledge is contained in the updates
- When to send updates
- How to locate recipients of the updates.[65]

Routing protocols can be differentiated based on several key characteristics. They can be differentiated using the following characteristics:

- **Optimality -** The capability of the routing algorithm to select the best route, which depends on the metrics and metric weightings used to make the calculation
- **Simplicity and low overhead –** Ease of configuration and maintenance. Overhead refers to the amount of CPU, memory and the bandwidth that the protocol consumes.
- **Robustness and stability –** The ability of protocols to function properly in the face of unusual or unforeseen circumstances, such as hardware failures, high load conditions, and incorrect implementations.
- **Convergence Times** – The time that routing protocols take to adapt themselves to network changes. Difference between the time a network change occurs and the time all of the routers have adjusted to it in a consistent manner is known as convergence time.

- **Flexibility-** The ability to adapt to any changes that occur within the network to find new routes to destinations.
- **Metrics-** Metrics are criteria used by routing protocols to identify the best path. There are different metrics that are used by protocols that differentiate them. Some of the commonly used metrics are:
  - Path length
  - Reliability
  - Delay
  - Bandwidth
  - Load
  - Communication cost [64]

Routing Protocols can be classified depending on where they are used. They can be classified into the following two types depending on whether they are used between networks or within one autonomous system:

- **IGP (Interior Gateway Protocol):** An IGP is a protocol for exchanging routing information between gateways within an autonomous network. RIP, RIPv2, IGRP, EIGRP and OSPF are example of Interior gateway routing protocol. [1, 64, 65]
- **EGP (Exterior Gateway Protocol)**: EGP is a protocol for exchanging routing information between two neighbour gateways of different autonomous systems. It carries routing information between two

independent administrative entities. Each of these entities maintains an independent network infrastructure and uses an EGP to communicate routing information to the other. The most common exterior protocol is the Border Gateway Protocol (BGP). It is the primary exterior protocol used between networks connected to the Internet, and was designed specifically for such purposes. [1, 64, 65]

While it is possible to use an interior protocol as an exterior protocol, and vice versa, it is not a good idea. Exterior protocols are designed to scale to the largest of networks and are very complex. Their overheads can quickly overwhelm a small or medium-sized network. On the other hand, while interior protocols are fairly simple and have little inherent overhead, they do not offer the scalability needed to maintain huge number of routes and neighbors. [64]

Depending on how routers interact with each other, Interior gateway routing protocols can be classifies as one of the three basic types of routing protocols. They are:

- Distance-Vector Routing Protocols
- Link-State Routing Protocols
- Balanced-Hybrid Protocol.

4.2.1 Distance Vector Routing Protocols

Distance vector protocols as their name suggests make use of distance and vector to make routing decisions. Distance is measure in term of hops and vector relates to the next hop address. They can also be described as simple routing protocols that use distance or hop count as its primary metric for determining the best forwarding path. Distance-vector protocols periodically send all or some portion of their routing Table to their adjacent neighbours. Routers running a distance-vector routing protocols send periodic updates even if there are no changes in the network. By receiving a neighbour's routing Table, a router can verify all the known routes and make changes to the local routing Table based on updated information received from the neighbouring router. Distance vector algorithms are based on the work done of R. E. Bellman, L. R. Ford, and D. R. Fulkerson and for this reason they are occasionally referred to as *Bellman-Ford* or *Ford-Fulkerson* algorithms. Such algorithms date back to the ARPAnet network in the early 1970s. [1, 14, 64]

Some common characteristics of distance vector routing algorithms are given below:

- **Periodic Updates -** At the end of a certain time period, updates containing full routing information of each router is transmitted by respective routers to all its neighbours. This period typically ranges from 10 seconds for AppleTalk's RTMP to 90 seconds for Cisco's IGRP. The continuous timed updates regardless of any change can cause network congestion. This can decrease networking efficiency especially in a large network involving numerous routers.

- **Neighbours** - Routers directly connected using a link is regarded as neighbours. Routing updates are sent to all neighbours, which is why distance vector routing is said to use hop-by-hop updates.
- **Route Invalidation Timers-** This is the amount of time a router waits before marking routes as unreachable on which an update has not been received. Typical periods for route timeouts range from three to six update periods.
- **Split Horizon-** Routers using distance vector routing protocols send updates as broadcast out all of their active interfaces. *Split horizon* is a technique that prevents routers from advertising routes on to links from which they were learned. This first of all reduces the number of updates being sent on the network but the most important reason for not sending route information back to the router from which the information was learned is to avoid routing loop. Split horizon is of two types: “Simple Split Horizon” or “Split Horizon with Poison Reverse”.
- **Maximum Hop Count / Count to infinity –** Distance-vector routing protocols are simple to configure and deploy. Most of the protocols have a limit to the number of routers that can be used within the network. For example: RIP has a maximum hop count of 16. [64, 65]

The main problems associated with distance vector routing protocols are given below:

- **Long Convergence Time** – As routing updates are sent periodically, routers have to wait for updates from neighboring router to learn of route changes. After receiving updates routers make necessary changes to their own routing Tables and then broadcast their own routing Table to other neighbours. In theory, a network with 6 routers using a protocol with an update interval of 30 seconds can take up to 3 minutes to converge.
- **Periodic updates** are always used by DV protocols to send out their entire routing Tables as broadcasts. This process consumes a lot of network bandwidth and routers processing power which have to check and analyze each broadcast to find out about changes to the topology. Even when then network is sTable DV protocols consume a lot of bandwidth and processing power.
- **Routing Loops** – As DV protocols do not have a full view of the network and have slow convergence they are prone to routing loops.

So, while distance-vector protocols are simple to understand and configure they have various problems associated with them. Use of extra technology to lessen the problems of the protocol has made it more complex but keeps many of its limitations in place.

The most common distance vector routing protocols are RIP, RIPv2 and IGRP. These protocols will be briefly described later during this chapter.

4.2.1.1 RIP (Routing Information Protocol)

The Routing Information Protocol, or RIP, as it is more commonly called, is one of the most enduring of all routing protocols. These algorithms emerged from academic research that dates back to 1957. Today's open standard version of RIP, sometimes referred to as IP RIP, is formally defined in two documents: Request For Comments (RFC) 1058 and Internet Standard (STD) 56. [1]

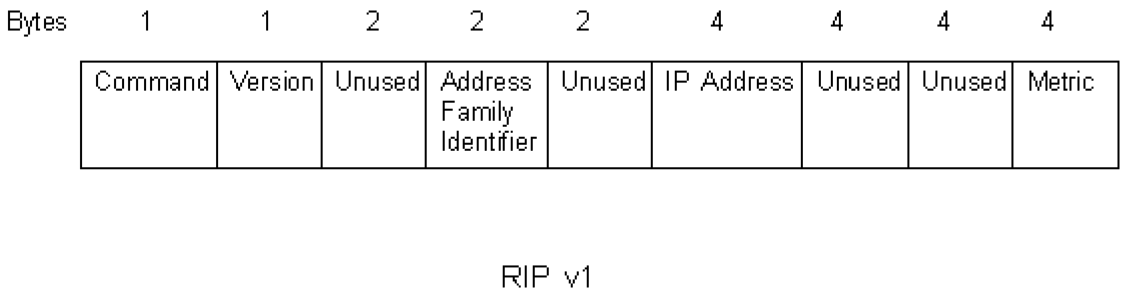
RIP sends routing update messages at regular intervals and when there are changes to the network topology. When a router receives a routing update that includes changes to an entry, it updates its routing Table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (path with the least hop count) to a destination. After updating its routing Table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send and are known as triggered updates.

RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops in a path is 15. If a router receives a routing update that contains a new or changed entry, and if increasing the metric value by 1 causes the metric to be infinity (that is, 16), the network destination is considered unreachable. The downside of this stability feature is that it limits the maximum diameter of a RIP network to less than 16 hops. [1, 64]

RIP includes a number of other stability features that are common to many routing protocols. These features are designed to provide stability despite potentially rapid changes in a network's topology. For example, RIP implements the split horizon and hold-down mechanisms to prevent incorrect routing information from being propagated.

RIP uses numerous timers to regulate its performance. These include a routing-update timer, a route-timeout timer, and a route-flush timer. The routing-update timer clocks the interval between periodic routing updates. Generally, it is set to 30 seconds, with a small random amount of time added whenever the timer is reset. This is done to help prevent congestion, which could result from all routers simultaneously attempting to update their neighbours. Each routing Table entry has a route-timeout timer associated with it. When the route-timeout timer expires, the route is marked invalid but is retained in the Table until the route-flush timer expires. [1, 65]

Figure 4.1 – RIP Packet Format [72]



Bytes	1	1	2	2	2	4	4	4	4
	Command	Version	Unused	Address Family Identifier	Unused	IP Address	Unused	Unused	Metric

RIP v1

The following descriptions summarize the IP RIP packet format fields illustrated in Figure 4.1:

- **Command**— indicates whether the packet is a request or a response. The request asks that a router send all or part of its routing Table. The response can be an unsolicited regular routing update or a reply to a request. Responses contain routing Table entries. Multiple RIP packets are used to convey information from large routing Tables.
- **Version number**—specifies the RIP version used. This field can signal different potentially incompatible versions.
- **Zero**— this field is not actually used by RFC 1058 RIP; it was added solely to provide backward compatibility with pre standard varieties of RIP.
- **Address-family identifier (AFI)**—Specifies the address family used. RIP is designed to carry routing information for several different protocols. Each entry has an address-family identifier to indicate the type of address being specified. The AFI for IP is 2.
- **Address**—Specifies the IP address for the entry.
- **Metric**—Indicates how many internetwork hops (routers) have been traversed in the trip to the destination. This value is between 1 and 15 for a valid route, or 16 for an unreachable route. [65]

RIP uses hop count to determine the direction and distance to any link the internetwork. If there are multiple paths to a destination, RIP selects the path with the fewest hops. However, because hop count is the only routing metric RIP uses, it does not necessarily select the fastest path to a destination. RIP v1 uses only classful routing. This means that all devices in the network must use the same subnet mast because RIP v1 does not include subnet information in its updates.

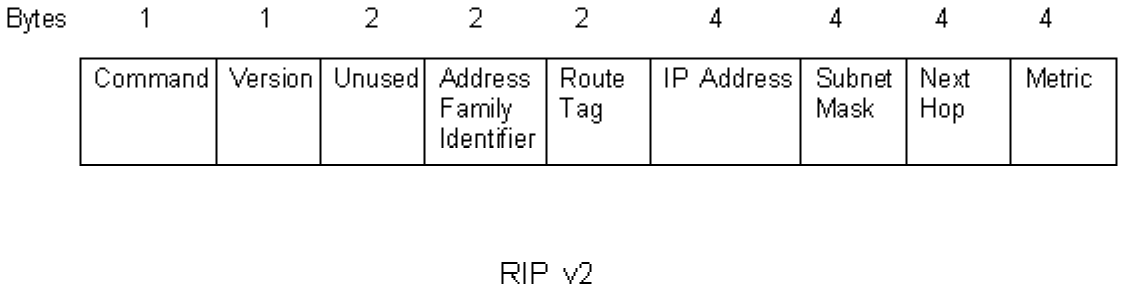
RIPv1 can be summarized as:

- Distance-vector protocol.
- Classful protocol (no support for VLSMs or CIDR).
- Metric is router hop count.
- Maximum hop count is 15; unreachable routes have a metric of 16.
- Periodic route updates broadcast (255.255.255.255) every 30 seconds.
- Implements split horizon with poison reverse.
- Implements triggered updates.
- No support for authentication.
- Administrative distance for RIP is 120.
- Used in small, flat networks or at the edge of larger networks. [65]

4.2.1.2 RIP Version 2

Updated version of RIP known as RIPv2 (second version of RIP) was released in January 1994 by IETF. RIPv2 enabled RIP messages to carry more information, which permitted the use of a simple authentication mechanism to secure Table updates. But, the most important update made enabled RIPv2 to provide support for VLSM. This was a crucial feature that the original RIP lacked. The support for subnets was achieved by including the subnet mask information in routing updates. With classless routing protocols, different subnet within the same network can have different subnet masks. The use of different subnet masks within the same network is called variable length subnet masking VLSM. Figure 4.2 shows the updated RIP packet format.

Figure 4.2 – RIPv2 Packet format [72]



Bytes	1	1	2	2	2	4	4	4	4
	Command	Version	Unused	Address Family Identifier	Route Tag	IP Address	Subnet Mask	Next Hop	Metric

RIP v2

The following descriptions summarize the IP RIPv2 packet format fields illustrated in Figure 4.2:

- **Command**—indicates whether the packet is a request or a response. The request asks that a router send all or part of its routing Table. The response can be an unsolicited regular routing update or a reply to a request. Responses contain routing Table entries. Multiple RIP packets are used to convey information from large routing Tables.

- **Version**—Specifies the RIP version used. In a RIP packet implementing any of the RIP 2 fields or using authentication, this value is set to 2.
- **Unused**—has a value set to zero.
- **Address-family identifier (AFI)**—Specifies the address family used. RIPv2's AFI field functions identically to RFC 1058 RIP's AFI field, with one exception: If the AFI for the first entry in the message is 0xFFFF, the remainder of the entry contains authentication information. Currently, the only authentication type is simple password.
- **Route tag**—provides a method for distinguishing between internal routes (learned by RIP) and external routes (learned from other protocols).
- **IP address**—specifies the IP address for the entry.
- **Subnet mask**—contains the subnet mask for the entry. If this field is zero, the default subnet mask is assumed.
- **Next hop**—indicates the IP address of the next hop to which packets for the entry should be forwarded.

- **Metric**—Indicates how many internetwork hops (routers) have been traversed in the trip to the destination. This value is between 1 and 15 for a valid route, or 16 for an unreachable route.[65]

Despite being one of the oldest routing protocols to have been released RIP is still used in many networks. RIP is mature, stable, widely supported, and most importantly easy to configure. It is simple and has very low demands on routers in terms of memory and processing power. Its simplicity is well suited for use in stub networks and in small autonomous systems that do not have many redundant paths requiring sophisticated routing protocols to be implemented.

RIPv2 can be summarized as:

- Distance-vector protocol.
- Classless protocol (support for CIDR).
- Supports VLSMs.
- Metric is router hop count.
- Maximum hop count is 15; infinite (unreachable) routes have a metric of 16.
- Periodic route updates sent every 30 seconds to multicast address 224.0.0.9.
- Supports authentication.
- Implements split horizon with poison reverse.
- Implements triggered updates.

- Subnet mask included in route entry.
- Administrative distance for RIPv2 is 120.
- Used in small, flat networks or at the edge of larger networks.

4.2.1.3 IGRP (Interior Gateway Routing Protocol)

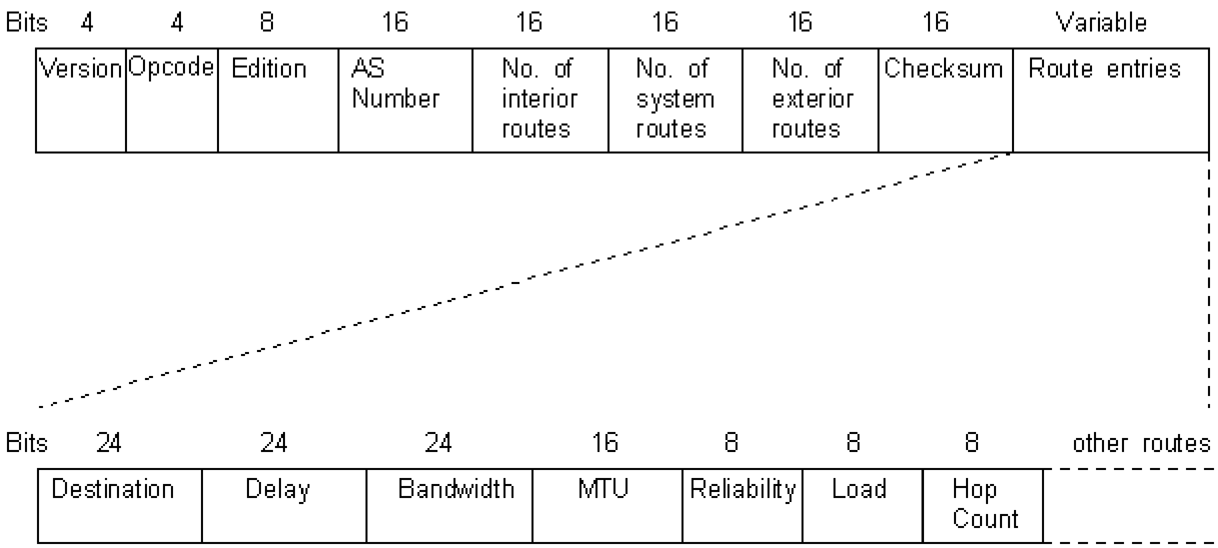
The Interior Gateway Routing Protocol (IGRP) is a routing protocol that was developed in the mid-1980s by Cisco Systems, Inc. Cisco's principal goal in creating IGRP was to provide a robust protocol for routing within an autonomous system (AS). In the mid-1980s, the most popular Interior Gateway Routing Protocol was the Routing Information Protocol (RIP). As, explained earlier although RIP was quite useful for routing within small networks, relatively homogeneous internetworks, its limits were being pushed by growth in the size of networks. RIP had a maximum hop count of 16 which means there could be no more than 15 routers in one network. IGRP supported larger network by allowing a maximum hop count of 255. This made IGRP very popular and was widely deployed in networks which had Cisco equipment. [1, 65, 71]

Unlike RIP, IGRP uses a composite metric to calculate the cost of a route. Despite using a composite metric IGRP is still regarded as a distance vector routing protocol because it sends periodic updates just as RIP. The metric or cost is calculated by factoring weighted mathematical values for internetwork delay, bandwidth, reliability, and load. Network administrators have the privilege set the weighting factors for each of these metrics to manipulate route selection. The use of the composite also allowed IGRP to make better route selection then RIP.

Like RIP, IGRP automatically load balances over equal cost paths that are available for a destination. IGRP however provides additional flexibility by allowing load balancing over unequal cost paths. Due to the fact that IGRP uses a composite metric the router calculates a cost for each route to the destination. The route with the least cost is installed in the routing Table and is used as the primary path to forward traffic. Using the **Variance** command, it is possible to enable routing over multiple paths that do not have the same cost. Only routes with metrics that are within a certain range or variance of the best route are used as multiple paths. The variance value can be defined by the network administrator and by default is 1. [1, 65, 71]

Like all other distance vector routing protocols IGRP send period updates by broadcast every 90 seconds. The packet format for IGRP is shown in Figure 4.3.

Figure 4.3 – IGRP Packet Format [71]



Bits	4	4	8	16	16	16	16	16	Variable
	Version	Opcode	Edition	AS Number	No. of interior routes	No. of system routes	No. of exterior routes	Checksum	Route entries

Bits	24	24	24	16	8	8	8	other routes
	Destination	Delay	Bandwidth	MTU	Reliability	Load	Hop Count	

The respective field descriptions of the IGRP packet shown in Figure 4.3 are as follows:

- **Version** - Always 0x01
- **Opcode** - 0x01 for a Request (a header with no entries) and 0x02 for an Update
- **Edition** - This number is incremented by the sender so that the receiving router does not use an old update
- **Autonomous System number** - The IGRP process ID
- **Number of Interior routes** - indicates how many of the routing entries in this update are subnets of a directly connected network.
- **Number of System routes** - indicates how many of the routing entries in this update are not from a directly connected network.
- **Number of Exterior routes** - indicates how many of the routing entries in this update are default networks.
- **Checksum** - calculated on the header and the entries. With his field set to **0**, the 16-bit one's complement sum is calculated and then inserted into

this field. At the other end, the 16-bit one's complement is calculated again by the other router but this time including the already calculated value in the Checksum field. The result on a good packet will be 0xFFFF.

- **Destination** - Destination network, just containing the last three octets for interior routes (e.g. 24.5.0 for the network 10.24.5.0) since the first octet will be known. For System and External routes, the routes would have been summarized so the last octet will always be zero (e.g. 10.24.5.0 will be entered as 10.24.5).
- **Delay** - The number of 10 microsecond chunks which is the sum of delays
- **Bandwidth** - IGRP bandwidth
- **MTU** - The smallest MTU encountered along the route to this particular destination network.
- **Reliability** - A number between 0x01 and 0xFF to indicate the error rates along the route. 0xFF is reliable.
- **Load** - A number between 0x01 and 0xFF expressing the total load along a route where 0xFF is totally loaded.
- **Hop Count** - A number between 0x00 (directly connected network) and 0xFF. [71]

IGRP has proven to be one of the most successful routing protocols of all time. It preserved all the capabilities of RIP and got rid of its limitation to become a robust routing protocol. But IGRP does not have the ability to provide support for variable length subnet masks or VLSM. This is a big issue in modern day networks because almost all networks now use VLSM to conserve IP addresses.

IGRP can be summarized as:

- Distance-vector protocol.
- Uses IP protocol 9.

- Classful protocol (no support for CIDR).
- No support for VLSMs.
- Composite metric of bandwidth and delay.
- Route updates broadcast every 90 seconds.
- No support for authentication.
- Implements split horizon with poison reverse.
- Implements triggered updates.
- Administrative distance is 100.
- Previously used in large networks; now replaced by EIGRP.

4.2.2 Link State Routing Protocols

Link state routing protocols were designed to overcome the limitation of distance-vector routing protocols. Link-state routing protocols respond quickly to network changes, send trigger updates only when a network change has occurred, and send periodic updates (called link-state refreshes) at long interval times such as every 30 minutes. Link-state routing communicates changes in network topology incrementally. Link state protocols are also known as *shortest path first* or *distributed database* protocols, are built around a well-known algorithm from graph theory, E. W. Dijkstra'a shortest path algorithm. [64, 65]

When a change in the topology occurs, the device that detects the change creates a link-state advertisement (LSA) and sends it out to its neighbours. The LSA consists of only updates or changes to the network. Each routing device takes a copy of the LSA, updates its link-sate (topological) database, and forwards the LSA to all its neighbouring devices. This flooding of the LSA is required to ensure that all routing devices update their database before creating an updated routing Table that reflects the new topology. The objective of this method is that every router has identical information about the internetwork, and each router will independently calculate its own best paths.

These protocols are more complex then DV. The link-state database is used to calculate the best paths through the network. Link-state routers find the best paths to destinations by applying the Dijkstra Shortest Path First (SPF) algorithm against the link-state database to build the SPF tree. The best (shortest) paths are then selected from the shortest-path-first tree and are placed in the routing Table. [65]

Link state routing protocols have the following characteristics:

- **Neighbours -** Neighbour discovery is the first process that takes place in order for router to share information. Special Packets called Hello Packets are sent by routers out all interfaces when they are first turned on. When two routers have discovered each other as neighbours by exchanging information using hello packets, they build adjacencies. Hello packets are also used to maintain and monitor the adjacency. If Hello packets are not received from an adjacent neighbour within a certain established time, the neighbour is considered unreachable and the adjacency is broken.

- **Link State Flooding -** After the adjacencies are established, the routers may begin sending out LSAs. Each router sends LSA to all its neighbours that it has formed an adjacency with. Each router also keeps a copy of every LSA received and forwards it to every neighbour except the one that sent the LSA. LSAs are forwarded almost immediately, whereas distance vector must run its algorithm and update its routing Table before sending routing updates to its neighbours. As a result, link state protocols converge much faster than distance vector protocols converge when the topology changes. The flooding process of the LSA is a complex function of the link state protocol. There are several ways by which flooding is made more efficient and more reliable, such as using unicast and multicast addresses, checksums, and positive acknowledgments. The procedures used are specific to each protocol, but there are two vital common procedures of the flooding process: sequencing and aging. The advertisements must be sent in sequence so that each router has an up to date view of the entire network and does not use an old update which may cause the topology view to be in error. There are various methods of sequencing used. The LSA packet has an age field which is set to zero by the router creating the packet. Each router that the packet passes through increments the age by one. This aging value is also used to ensure the sequencing of the LSA packets.

- **The Link State Database –** This database is a collection of information from the LSA's that is received by a router. It contains complete information obtained from all updates allowing the router to have a consistent topological view of the entire network.

- **Areas -** An area is a subset of the routers that make up an internetwork. Link state protocols make use of areas to divide internetworks into smaller zones due to the following reasons:

  - Topological database used by link state protocols use a lot of memory. Holding topological view of an area takes much less space then that of the entire network.

  - The complex algorithm used to calculate the shortest path is very CPU intensive. Naturally, the bigger the database the more CPU power is needed. Thus reducing the size of the database by splitting the internetwork into areas reduces the amount of CPU power needed for processing.

  - The flooding of link state packets adversely affects available bandwidth, particularly in unstable internetwork. Advertisement packets are confined to their respective areas thus reducing the overall traffic traversing the network.

During forwarding of packets to destination routers use the routing Table to look up the link that the packets need to be sent upon to reach their final destination. Different metrics are used during the calculations of the routes. In case of link sate protocols metric may include the bandwidth of the link, the current load on the link, administrative weights, or even policy information restricting which packets may traverse the link

Link-state protocols have some important advantages. Because a link-state protocol computes its routes based on the topology of the network as indicated by the link-state updates, it can't form a loop in response to a partial network failure, like a distance-vector protocol might. Further, because a change in link-state gets flooded throughout the network immediately and causes all routers to update their topology map and routing Tables, convergence time is minimal. Finally, because most link-state protocols are designed to send link-state updates only when the state of a link changes, they tend to conserve network bandwidth and router processing power during periods of network stability. [1, 64, 65]

The following are some of the problems that are related to link state routing protocols:

- Complexity – Link state routing protocols use complex algorithms to calculate the paths for each destination within the network. For each of the protocols this might be drastically different. They are generally harder to configure as they require more parameters and are not very tolerant towards mismatches in the configuration.
- Processing power and memory – A lot of memory is needed for the routers to store all the LSA's and to perform complex calculation using the topology Table and the various metrics.
- Initial Flooding – When link state network routers first come on there is an initial flooding of LSA and updates throughout the network. This flooding can consume all of the network bandwidth and can render it unusable.

[1, 64, 65]

Both link-state and distance-vector protocols have their advantages and disadvantages. If the complexity of link-state protocols is not needed, or if there is a concern over the consumption of router resources, distance-vector protocols would be a better choice for deployment. On the other hand, if fast convergence and low bandwidth consumption of a link-state protocol, or the network size is large and then a protocol from the link-state family should be selected.

The most popular link state protocol is OSPF which will be briefly described in the later section.

4.2.2.1 OSPF (Open Shortest Path First)

Open Shortest Path First (OSPF*)* is a routing protocol developed for IP networks by the IGP working group of the IETF. The working group was formed in 1988 to design an IGP based on the Shortest Path First (SPF) algorithm for use in the Internet. Just like IGRP OSPF was also developed to address the problems with RIP. OSPF was derived from various researches that was carried out previously and was based on the shortest path algorithm. The algorithm is sometimes referred to as the Dijkstra algorithm, name after the creator of the algorithm. [73]

OSPF is a link-state routing protocol that uses Link state advertisements (LSA) to share information with routers in the same area. Information about attached interfaces, metrics used, and other variables are included in LSAs. As OSPF routers accumulate link-state information, they use the SPF algorithm to calculate the shortest path to each node. Being a link state protocol OSPF only advertises changes in the link as and when they occur. It does not use any periodic updates like that of distance vector protocols for convergence. There is a periodic update for OSPF which takes place every 30 minutes on a stable converged network. OSPF as the name suggest is open structure which means its specification is in the public domain. [73]

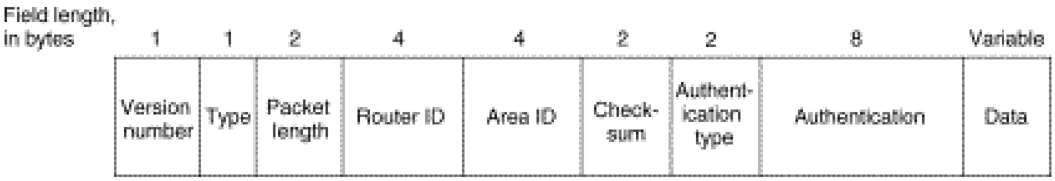
Unlike RIP, OSPF can operate within a hierarchy. The largest entity within the hierarchy is the autonomous system (AS), which is a collection of networks under a common administration that share a common routing strategy. OSPF is an IGP but is capable of functioning as an EGP. An AS can be divided into a number of areas with contiguous networks forming each area. Routers with multiple interfaces can be a part of multiple areas. Routers that belong to multiple areas are called Area Border Routers and maintain separate topological databases for each area. As topologies for each area are separate, OSPF passes less routing traffic than it would if the AS were not partitioned. [73]

A topological database contains collection of LSAs received from all routers in the same area. This allows routers in the same are to have an identical view of the entire network. Area partitioning creates two different types of OSPF routing, depending on whether the source and the destination are in the same or different areas. All Area border routers in an OSPF network from a special area called the backbone. This is depicted as area 0 in an OSPF configuration. The backbone area routes information or traffic between the different areas of an OSPF network. The backbone topology is invisible to all intra area routers, as are individual area topologies to the backbone.

The Shortest Path First (SPF) routing algorithm is the basis for OSPF operations. When an OSPF router becomes active it sends hello packets out all its interfaces trying to find out about other directly connected routers. A router sends hello packets to its neighbours and receives their hello packets. Hello packets are used to detect and form relationship with neighbours. Other then forming relationship with neighbours, hello packet is also used to maintain the relationship and let neighbours know that the router is functional. When the link-state databases of two neighbouring routers are synchronized, the routers are said to be adjacent. On multi-access networks, the Hello protocol elects a designated router and a backup designated router. Designated router is responsible for generating and sending of LSAs to each router on a multi-access network. Having the designated router system allows a reduction in network traffic as fewer advertisements need to traverse the network. The designated router also determines which routers should become adjacent. This allows greater control over the flow of advertisement packets.

All OSPF packets begin with a 24-byte header and the format for the packet can be found in Figure 4.4

Figure 4.4 – OSPF Packet Format. [73]



Field length, in bytes	1	1	2	4	4	2	2	8	Variable
	Version number	Type	Packet length	Router ID	Area ID	Check-sum	Authent-ication type	Authentication	Data

The packet form of OSPF found in Figure 4.4 is explained below:

- **Version number**—identifies the OSPF version used.
- **Type**—Identifies the OSPF packet type as one of the following:
    - **Hello**—Establishes and maintains neighbour relationships.

- **Database description**—describes the contents of the topological database. These messages are exchanged when an adjacency is initialized.
- **Link-state request**—Requests pieces of the topological database from neighbour routers. Such requests are sent when a router determines that its topology information is out of date.
- **Link-state update**— response to a link-state request packet. LSAs are also sent using this packet. Multiple LSAs can be included within a single link-state update packet.
- **Link-state acknowledgment**—Acknowledges link-state update packets.

- **Packet length**—specifies the length of the entire packet in bytes
- **Router ID**—identifies the source of the packet.
- **Area ID**—identifies the area to which the packet belongs.
- **Checksum**— used to verify integrity of a packet
- **Authentication type**—contains the authentication type. All OSPF protocol exchanges are authenticated and can be different for each area.
- **Authentication**—Contains authentication information.
- **Data**—Contains encapsulated upper-layer information. [73]

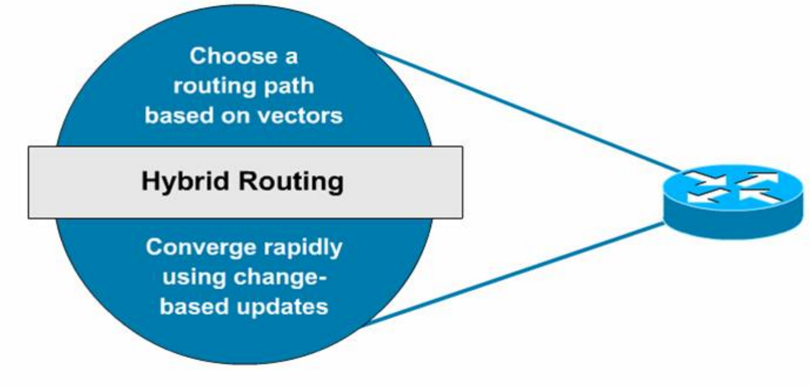
OSPF by defaults allows equal cost path load balancing over up to 6 links. Single of multiple metrics can be use by OSPF with line speed being the most common metric used. TOS-based routing supports those upper-layer protocols that can specify particular types of service. An application, for example, might specify that certain data is urgent. If OSPF has high-priority links at its disposal, these can be used to transport the urgent datagram. Routing in OSPF can also be done using policy. For these reasons OSPF works well as an EGP. OSPF provides support for VLSM and uses authentication for messages sent across the network. [73]

OSPF is a link state protocol which makes very efficient use of bandwidth and CPU processing power of router during stable conditions. However during computation of routes the algorithm is very CPU intensive. During initial flooding of the network with LSA almost all the bandwidth is consumed making the network unavailable. OSPF scales very well and is appropriate for large networks that require complex routing policies and support VLSM. However, OSPF should not be implemented in small networks where resources are very limited. Configuration and troubleshooting of the protocol is also quiet complex and the protocol is not tolerant of erroneous configuration. It should only be implemented by administrator with sound knowledge of it processes.

4.2.3 Hybrid Routing Protocols

The third classification of Interior Gateway Routing Protocols is known as Hybrid Routing protocols. They use combination of link-state and distance-vector routing techniques to give better overall performance. It is also regarded as balanced-hybrid routing protocol because it uses techniques from both sides.

Figure 4.5 – Hybrid Routing Scheme. (Ref: Buchanan W, Distributed Systems And Networks, Page 386)


Choose a routing path based on vectors
Hybrid Routing
Converge rapidly using change-based updates

Balanced hybrid routing protocols are distance vector protocols with more accurate metrics to determine the best paths to destinations. However, they differ from most distance vector protocols by only sending topology change to other neighbour as and when they occur. Periodic updates contains partial of complete routing Tables are not sent by hybrid protocols.

Balanced hybrid routing protocols have convergence times and stability comparable to Links state protocols but require less memory and CPU power. EIGRP is regarded as a Balanced-hybrid routing protocols.

4.3 Chapter Summary

Routing in the process by which data is routed through networks. Routing protocols are used by routers to share data about routes. Routing protocols can be classified as Interior Gateway Routing Protocols or Exterior Gateway Routing Protocols. Interior Gateway Routing protocols can be further classified into distance vector, link state and hybrid routing protocols. RIP, RIPv2, IGRP and OSPF were briefly described in this chapter. Hybrid routing protocol background was explained to form a platform for detailed discussion about EIGRP.

The following project objectives have been achieved through this chapter:

- To explain the need for Routing Protocols and compare routing protocols in common usage.

This knowledge provided in the chapter allows for enough understanding about different routing protocols to be able to appreciate the capabilities and technologies of EIGRP protocols which will be explained in details during the rest of this report.

The next chapter of this report will explain in details the theoretical aspects of the EIGRP routing protocol followed by operational analysis of the protocol.

CHAPTER 5 – EIGRP

5.1 Background

The Enhanced Interior Gateway Routing Protocol (EIGRP) was released by Cisco in 1994 as an improvement to its previous proprietary routing protocol IGRP. Enhanced IGRP just as the name suggests is an evolution from its predecessor IGRP. This evolution was brought about by the changes in networking and the demands of diverse, large-scale internetworks. EIGRP was introduced to meet many of the shortfalls of its predecessor IGRP.

Improvements that were made to EIGRP over IGRP are as follows:

- DUAL
- Incremental updates
- Loop-free networks
- Reduced bandwidth usage
- Support for multiple network layer protocols (IP, IPX, AppleTalk)
- Support for variable-length subnet masks (VLSMs), discontiguous networks, and classless routing
- Advanced distance vector capabilities
- Automatic route summarization on major network boundaries

5.2 Overview

EIGRP is an interior gateway protocol suited for many different topologies and media. In a well designed network, EIGRP scales well and provides extremely quick convergence times with minimal bandwidth usage. Although the protocol is regarded as an interior gateway protocol (IGP), it has also been used extensively as an exterior gateway protocol for inter-domain routing due to its scalability. [5, 13]

EIGRP integrates the capabilities of link-state protocols and distance vector protocols. Additionally, EIGRP contains several important technologies that greatly increase its operational efficiency compared to other routing protocols. *Diffusing update algorithm (DUAL)* developed at SRI International by Dr. J.J. Garcia-Luna-Aceves is the most important technology of the protocol. DUAL enables EIGRP routers to determine whether a path advertised by a neighbour is looped or loop-free, and also allows routers to find alternate paths quickly during link failures. EIGRP is a highly efficient routing protocol consisting of two primary components: the Protocol Engine and the Protocol-Dependent Modules. [1, 13, 25, 65]

Although EIGRP was built as an enhancement to IGRP the two protocols share little in common except the use of same metrics. Unlike IGRP, which is a classful routing protocol, EIGRP supports classless interdomain routing (CIDR) and variable-length subnet mask (VLSM), which allows efficient use of IP addresses. Compared to IGRP, EIGRP boasts faster convergence times, improved scalability, and superior handling of routing loops. EIGRP also provides support for multiple routing protocols. It can replace Novell Routing Information Protocol (RIP) and AppleTalk Routing Table Maintenance Protocol (RTMP), serving both IPX and AppleTalk network with powerful efficiency. [1, 5]

EIGRP is often described as a hybrid routing protocol that combines the best features of distance-vector and link-sate protocols. Strictly speaking, EIGRP is an advanced distance-vector routing protocol that has features that are commonly associated with link-state protocols. EIGRP uses features such as partial updates and neighbour discovery that are found in OSPF. Although EIGRP provides capabilities of link state protocols, it is much easier to configure then Open Shortest Path First (OSPF). EIGRP is and ideal choice for large, multiprotocol networks that are built primarily of Cisco routers. EIGRP maintains separate routing Tables and uses separate hello packets for neighbour discovery for each routed protocol in use. For this reason, EIGRP is considered a “ships-in-the-night” (SIN) protocol. [1, 13, 25]

5.3 EIGRP Features

The main features of EIGRP are given below:

- It is relatively simple to configure compared to Link-State protocols.
- It is virtually free of routing loops and has a fast convergence time as a result of DUAL.
- It consumes considerably less bandwidth and router internal resources than other protocols.
- It supports variable-length subnet mask (VLSM) and automatic route aggregation.
- It uses a system of neighbour discovery and management, enabling a router running EIGRP to automatically detect and exchange routing updates with other EIGRP routers on the network as well as detecting when a neighbour becomes unavailable.
- It employs a reliable transport protocol (RTP) to ensure that routing updates are successfully exchanged between neighbours.
- EIGRP supports multiple network protocols, maintaining separate neighbour, topology, and routing Tables for each protocol, and
- Allows for automatic route redistribution between IGRP, IPX RIP, SAP, and RTMP. [1, 13]

Each of these capabilities and functionalities will be dealt with in this chapter. They will be discussed in the explanation of the topic which they are associated with.

5.4 EIGRP Terminologies

In this section of the report the key terminologies associated with EIGRP will be explained.

5.4.1 Neighbour Table

Each EIGRP router maintains neighbour Table that lists adjacent routers which have formed adjacencies with the local router. This Table is comparable to the adjacency database that OSPF uses. Separate neighbour Tables are kept for each routed protocol running on a router. When new neighbours are discovered, the address and interface of the neighbour are recorded and stored in this Table. When a neighbour sends a hello packet it advertises a hold time. The hold time is that amount of time that a router treats a neighbour as operational even without having any hello packets from it. In other words, if a hello packet is not heard within the hold time the neighbour is regarded as down.

The neighbour-Table entry also includes information required by Reliable Transport Protocol (RTP). Sequence numbers are employed to match acknowledgments with data packets, and the last sequence number received from the neighbour is recorded so that out-of-order packets can be detected. A transmission list is used to queue packets for possible retransmission on a per-neighbour basis. Round-trip timers are also kept in the neighbour-Table entry to estimate an optimal retransmission interval. [1]

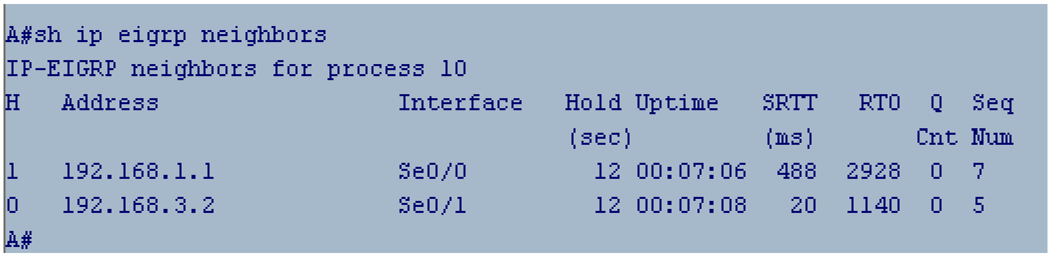
The **show ip eigrp neighbours** command can be used in EXEC mode to view the neighbour Table of an EIGRP router. The command and its syntax description are given below:

show ip eigrp neighbours [*interface-type* | *as-number* | static| details]

Syntax Description [19]

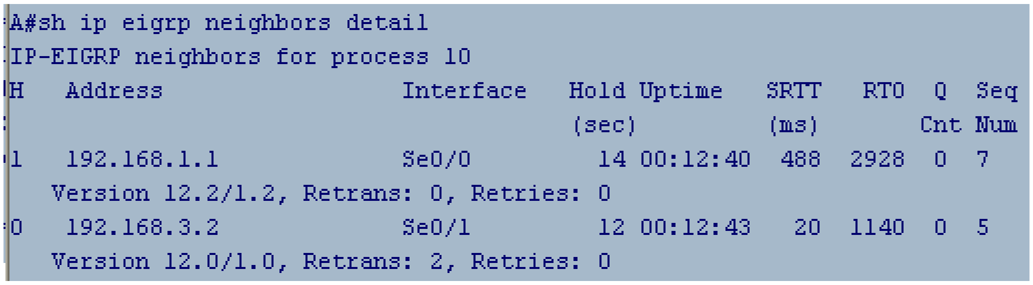
interface-type (Optional) Interface type.
as-number (Optional) Autonomous system number.
static (Optional) Static routes.
Details Shows details about neighbours including their IOS version, number of retries and retransmissions.

Figure 5.1 – EIGRP Neighbour Table.



```
A#sh ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq
                                        (sec)         (ms)       Cnt Num
1   192.168.1.1             Se0/0         12 00:07:06  488  2928  0  7
0   192.168.3.2             Se0/1         12 00:07:08   20  1140  0  5
A#
```

Figure 5.2 – EIGRP Neighbour Table (Full Details)



```
A#sh ip eigrp neighbors detail
IP-EIGRP neighbors for process 10
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq
                                        (sec)         (ms)       Cnt Num
1   192.168.1.1             Se0/0         14 00:12:40  488  2928  0  7
   Version 12.2/1.2, Retrans: 0, Retries: 0
0   192.168.3.2             Se0/1         12 00:12:43   20  1140  0  5
   Version 12.0/1.0, Retrans: 2, Retries: 0
```

Figure 5.1 and Figure 5.2 shows the neighbour Table of the EIGRP router showing different details due to use of different commands. The contents shown on the screenshot are explained below:

- **H** is the order in which the neighbours were discovered.
- **Neighbour Address** – The IP address of the neighbour router.
- **Interface** on which the neighbour is connected to.
- **Hold time**– The interval to wait without receiving anything from a neighbour before considering the link unavailable and neighbour down.
- **Up Time**- The time for which the neighbour has been operational.
- **Smooth Round Trip Time (SRTT)** - The average time that it takes to send and receive packets from a neighbour.
- **Retransmission Timeout (RTO)** - The time in milliseconds that a router waits for an acknowledgement of a reliably sent packet before retransmitting the packet again.
- **Queue Count (Q Cnt)** – The number of packets that are waiting in queue to be sent.
- **Sequence Number**– This is used to detect out of sequence packets that arrive from a neighbour. The sequence numbers are also used to send acknowledgements for particular packet.[1]

5.4.2 Topology Table

EIGRP routers also maintain a topology Table for each configured routed protocol. The topology Table includes route entries for all destinations learned by the router. All learned routes to a destination are maintained in the topology

Table regardless of whether they meet the feasibility condition or not. This Table is constructed from all the updates that are received from routers within the same Autonomous System. During route calculations DUAL uses information from this Table and the neighbour Table to calculate the best path to a destination. As this Table contains all routes to a destination it allows EGIRP routers to maintain a complete topological view of the entire network. [1]

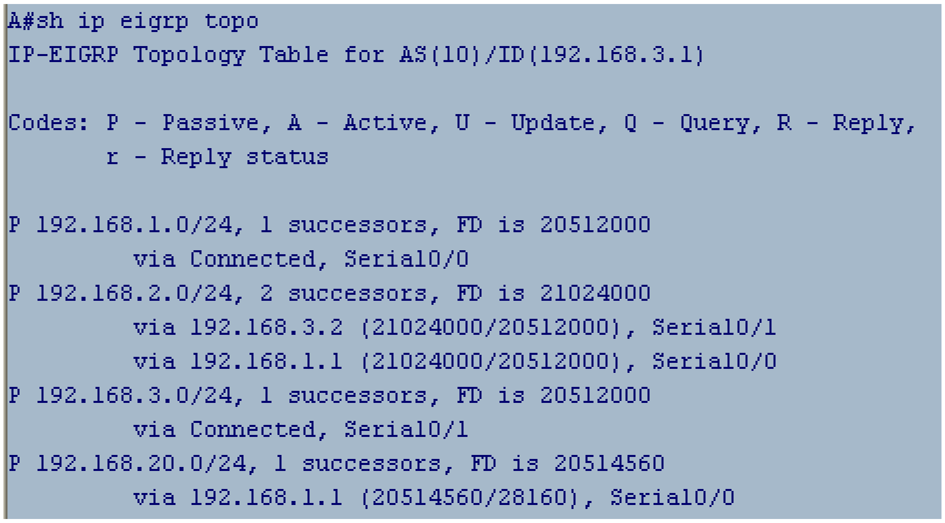
The **show ip eigrp topology** command can be used in EXEC mode of EIGRP routers to view the topology Table. The command syntax and its description are given below:

show ip eigrp topology [*as-number* | [[*ip-address*] *mask*]] [**active** | **all-links** | **pending** | **summary** | **zero-successors**]

Syntax Description [19]

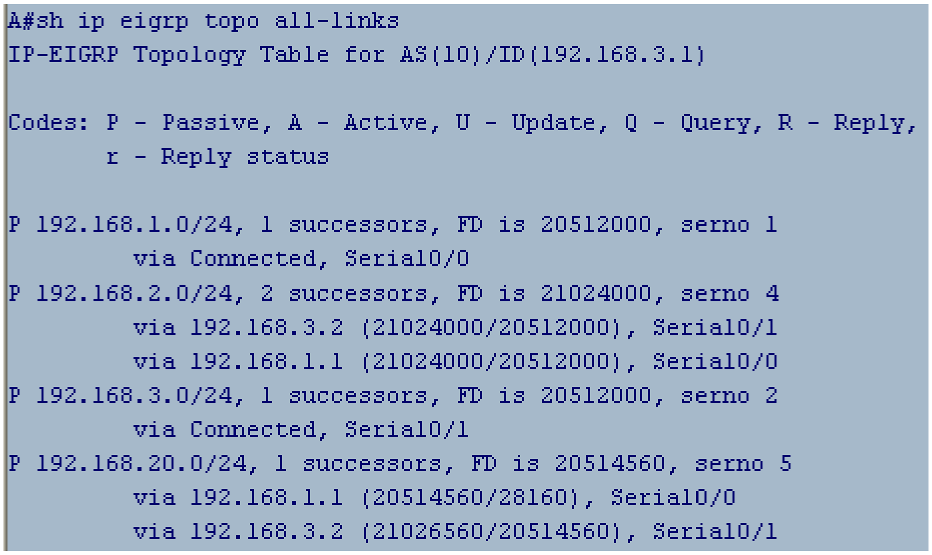
as-number	(Optional) Autonomous system number.
ip-address	(Optional) IP address. When specified with a mask, a detailed description of the entry is displayed.
mask	(Optional) Subnet mask.
active	(Optional) Displays only active entries in the EIGRP topology Table.
all-links	(Optional) Displays all entries in the EIGRP topology Table.
pending	(Optional) Displays all entries in the EIGRP topology Table that are waiting for an update from a neighbour or are waiting to reply to a neighbour.
summary	(Optional) Displays a summary of the EIGRP topology Table.
zero-successors	(Optional) Displays available routes in the EIGRP topology Table.

Figure 5.3 – Topology Table



```
A#sh ip eigrp topo
IP-EIGRP Topology Table for AS(10)/ID(192.168.3.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.1.0/24, 1 successors, FD is 20512000
         via Connected, Serial0/0
P 192.168.2.0/24, 2 successors, FD is 21024000
         via 192.168.3.2 (21024000/20512000), Serial0/1
         via 192.168.1.1 (21024000/20512000), Serial0/0
P 192.168.3.0/24, 1 successors, FD is 20512000
         via Connected, Serial0/1
P 192.168.20.0/24, 1 successors, FD is 20514560
         via 192.168.1.1 (20514560/28160), Serial0/0
```

Figure 5.4 – Topology Table (All links)



```
A#sh ip eigrp topo all-links
IP-EIGRP Topology Table for AS(10)/ID(192.168.3.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.1.0/24, 1 successors, FD is 20512000, serno 1
         via Connected, Serial0/0
P 192.168.2.0/24, 2 successors, FD is 21024000, serno 4
         via 192.168.3.2 (21024000/20512000), Serial0/1
         via 192.168.1.1 (21024000/20512000), Serial0/0
P 192.168.3.0/24, 1 successors, FD is 20512000, serno 2
         via Connected, Serial0/1
P 192.168.20.0/24, 1 successors, FD is 20514560, serno 5
         via 192.168.1.1 (20514560/28160), Serial0/0
         via 192.168.3.2 (21026560/20514560), Serial0/1
```

Figure 5.3 and Figure 5.4 show the EIGRP topology Table of an EIGRP router with partial and all links respectively. The topology Table in Figure 5.3 only shows successor and feasible successor routes or in other words routes that are believed to be loops free. Where as Figure 5.4 shows all links learned by the router.

The contents of the topology Table as shown in Figure 5.3 and Figure 5.4 are explained below:

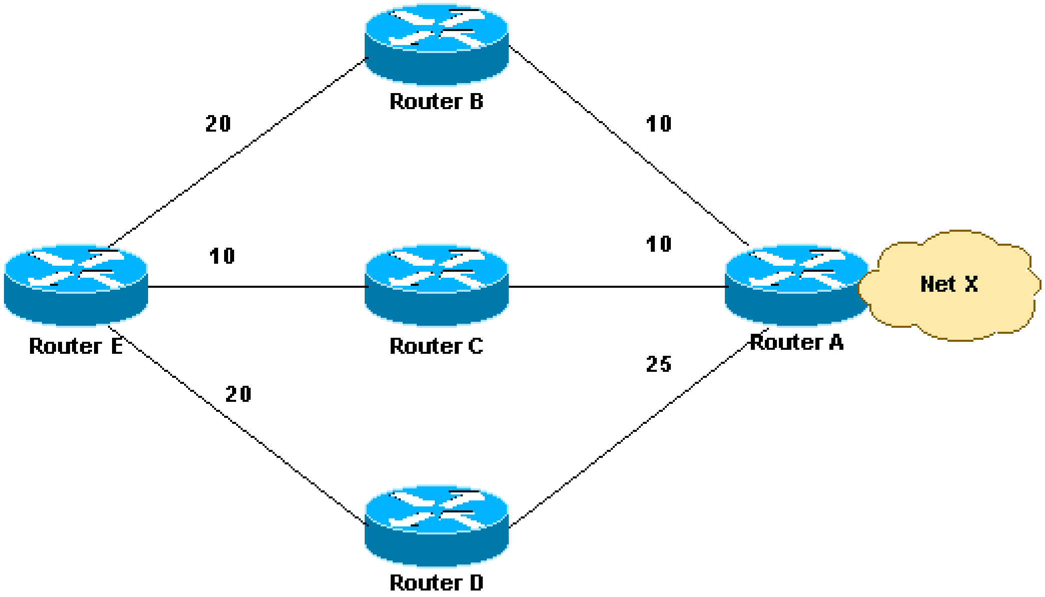
- **Feasible distance** – The cost of the best path to the destination
- **Route source** – This field is only used when storing external routes. It contains ID of the router advertising the route information.
- **Reported Distance** – The cost of the path to the destination from the next hop or router.
- **Interface information –** This is the interface on the router through which the destination is reachable.
- **Route Status**– EIGRP routes can either be in active (A) or passive state (P). Routes that are stable and can be currently used are denoted as passive. Routes to destinations that are being currently calculated are marked as active. [1]

EIGRP sorts the topology Table so that the successor routes (best routes for destination) are at the top, followed by the feasible successor. Routes that the algorithm believes to be loops are listed at the bottom of the Table.

Maintaining a Topology Table also allows a router to make sure that all its own metrics to destination networks are larger than its neighbours, thereby avoiding any routing loops. EIGRP therefore does not need Hold Down or Flush timers since loops are avoided by maintaining a full view of the entire network.

Figure 5.5 shown below will be used to explain some terminologies that are specific to EIGRP. The diagram shows 5 routers running EIGRP within the same Autonomous system. The links on the diagram are marked with number depicting the cost of the link calculated by EIGRP composite metric. It should be noted that the diagram is assuming simplified costs of links for ease of explanation. Actual metric calculation done by EIGRP will be explained later in this chapter.

Figure 5.5 – Simple Network Topology [8]



5.4.3 Feasible Distance

The metric or the cost of the best path from the local router to a destination is known as the feasible distance. [1] In Figure 5.5 it can be seen that there are three routes to destination X from router A. The routes are along with their costs are given below:

20 10

- E --------------- B -----------– A - X (30)

10 10

- E –------------- C –---------- A - X (20)

20 25

- E –------------ D ------------– A – X (45)

During route calculations Router A will choose route E-C-A-X as the best route because it has the least cost to the destination. So the feasible distance for router A to destination X using route E-C-A-X will be 20. The feasible distance of a route can be seen by issuing the EIGRP EXEC command **show ip route** *destination IP address.* The displayed screen will use the format as shown in Figure 5.8.

5.4.4 Reported Distance

The metric or the cost of the best path from the next hop (router) is known as the reported distance. This is also sometimes regarded as the *Advertised Cost* of the route as the cost is being reported or advertised by the router present at the next hop. For valid routes that do not have routing loops, the reported distance will always be less then the feasible distance of the route. In Figure 5.5 router C will advertise a reported distance of 10 to Router E for destination X.

5.4.5 Successor

Successor is defined as the best route or the route with the least cost to reach a destination. In simpler words in can be regarded as the route that is selected as the primary route for a destination. DUAL identifies the route from the information held in the neighbour Table and topology Table. As successor routes are used for forwarding data to destination they are placed in the routing Table. By default there can be up to 4 successor routes for a destination. Using the command **maximum-paths** this can be increase to 6. A copy of the successor route is also kept in the topology Table. [1]

As already explained for the network shown in Figure 5.5, Router E will choose route E-C-A-X to reach destination X as it has the least cost. This route is therefore called the Successor route for destination X in EIGRP terms.

5.4.6 Feasible Successor

A feasible successor route is a backup route that may be used to reach a destination in the event of successor route failure. It can also be regarded as a route with the second least cost for a particular destination. These routes are identified at the same time the successors are identified. Feasible successor routes are only stored in the topology Table as they are not actively used for forwarding data. Multiple feasible successors for a destination can also be retained in the topology Table.

To become a feasible successor it is not enough for a route to just have the second least cost for a destination. A route must satisfy the *feasibility condition* to become a feasible successor for the destination. Any route that has a reported distance that is less than the feasible distance of the current successor is said to have met the feasibility condition. Meeting the feasible condition ensures that the route is not part of a loop which traverses back through the local router. [1]

Considering Figure 5.5 again, router E has three possible routes to destination X. As earlier explained, route E-C-A-X will be selected as the successor owing to it being the least cost route. The other two routes that router E has for destination x are E-B-A-X and E-D-A-X. In this case route E-B-A-X will qualify as a feasible successor because it has a reported distance of 10 which is less then the feasible distance of the successor (20). However route E-D-A-X will not qualify as feasible successor because it has a reported distance of 25 which is more then the feasible distance of the successor. At this point it should also be noted that even it the reported distance of route E-D-A-X was 20 it sill would not qualify for a feasible successor. This is because for a route to meet the feasibility condition the reported distance of the route has to be less then the feasible distance of the current successor.

5.4.7 Passive Routes

A Route that is feasible and currently can be used for forwarding traffic to a destination is said to be in passive state. During normal EIGRP operations a fully converged network will have all of its routes in passive state [1]. The state of a route can be checked by viewing the topology Table. As shown in Figure 5.3 and 5.4 routes that are passive are marked with a "P" in a displayed topology Table.

5.4.8 Active Routes

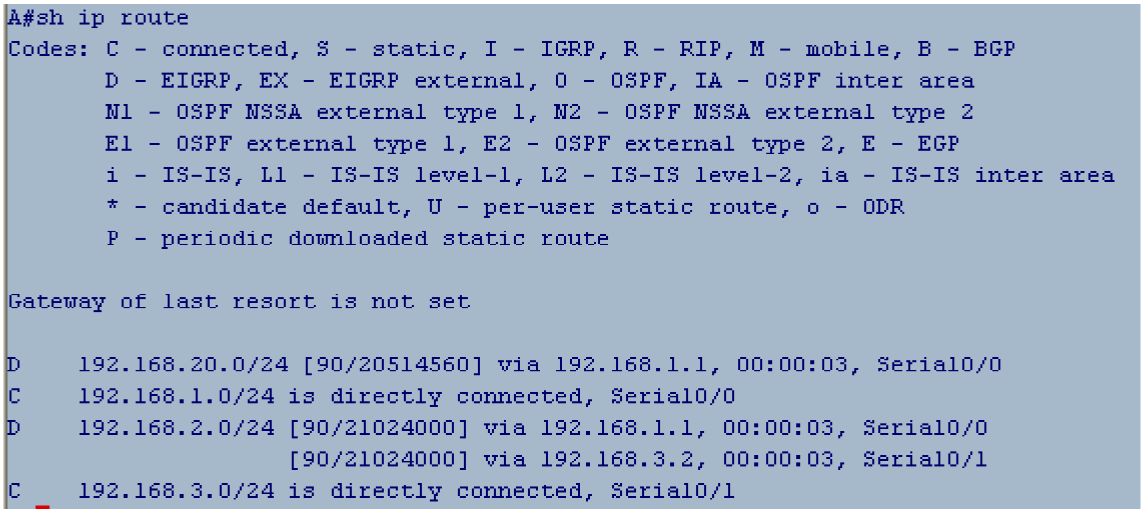
When a route is being recalculated by DUAL it is said to be in Active state and is known as Active Route. The recalculation can be due to various reasons which will be discussed later in this chapter. The state of a route can be checked by viewing the topology Table. As shown in Figure 5.3 and Figure 5.4 routes that are active are marked with an "A" in a displayed topology Table.

5.4.9 Routing Table

The routing Table holds all best/successor routes for destinations. EIGRP uses DUAL to perform route calculations and stores the successor routes in this Table. The routing Table will automatically hold up to 4 equal cost routes for each destination. When a packet arrives at a router to be routed to a particular destination, the router checks the entries in the routing Table to find a route for the destination. Once found the specified route is used to forward the packet to the destination. Routers can only forward packets to a destination, if routes for the destination are present in the routing Table. Figure 5.7 shows a routing Table being displayed by an EIGRP router. The **show ip route** command can be used in the EXEC mode of a router to view its routing Table. The command and its syntax are given below:

Show ip route [*ip address of particular destination.]*

Figure 5.7 – Routing Table



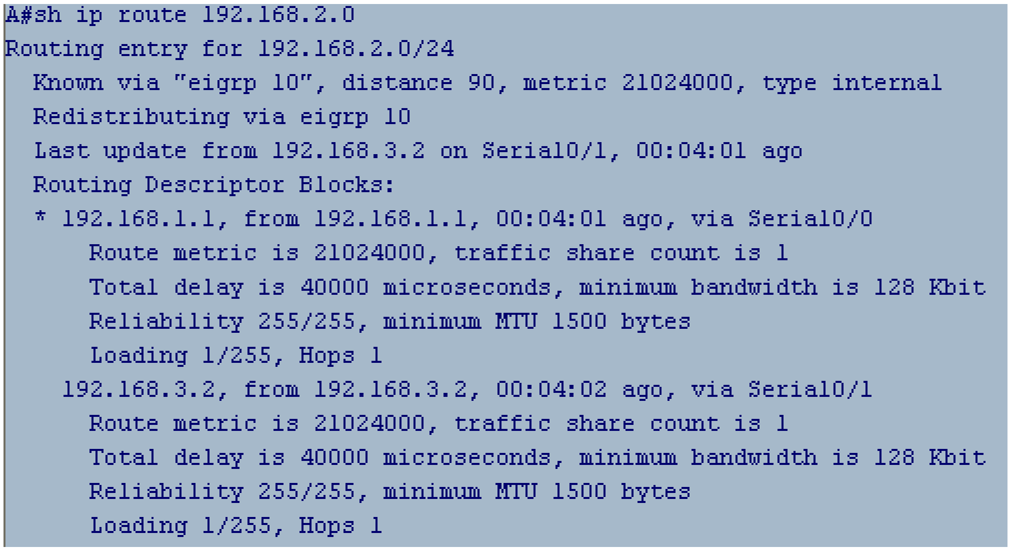
```
A#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
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

Gateway of last resort is not set

D    192.168.20.0/24 [90/20514560] via 192.168.1.1, 00:00:03, Serial0/0
C    192.168.1.0/24 is directly connected, Serial0/0
D    192.168.2.0/24 [90/21024000] via 192.168.1.1, 00:00:03, Serial0/0
                    [90/21024000] via 192.168.3.2, 00:00:03, Serial0/1
C    192.168.3.0/24 is directly connected, Serial0/1
```

The routing Table shown in Figure 5.7 shows information about the following:

- The protocol from whom the route was learnt. D refers to EIGRP while C refers to a directly connected route.
- The destination IP address and the subnet mask.
- Administrative distance for route and the feasible distance (cost) of route.
- The address of the next hop that can be used to reach the destination
- The amount of time for which the route has been known
- The interface connecting the next hop on route

Route to a particular destination can also be viewed by specifying the IP address of the destination host or network. Figure 5.8 show the information that is displayed when viewing a particular route. The route information shown in Figure 5.8 is the route information for destination 192.168.2.0 as found in the routing Table shown in Figure 5.7

Figure 5.8 – Route Information



```
A#sh ip route 192.168.2.0
Routing entry for 192.168.2.0/24
  Known via "eigrp 10", distance 90, metric 21024000, type internal
  Redistributing via eigrp 10
  Last update from 192.168.3.2 on Serial0/1, 00:04:01 ago
  Routing Descriptor Blocks:
  * 192.168.1.1, from 192.168.1.1, 00:04:01 ago, via Serial0/0
      Route metric is 21024000, traffic share count is 1
      Total delay is 40000 microseconds, minimum bandwidth is 128 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
    192.168.3.2, from 192.168.3.2, 00:04:02 ago, via Serial0/1
      Route metric is 21024000, traffic share count is 1
      Total delay is 40000 microseconds, minimum bandwidth is 128 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

The route information shown in Figure 5.8 shows the following:

- Protocol using which the route was learnt.
- Administrative distance of route (classified based on how it is learnt)
- Metric or total cost of the route.
- Information about who sent the last update received about the route and when.
- Delay, Bandwidth, Reliability, loading and MTU metric values are also displayed.
- Traffic share is displayed if multiple routes are present for the destination.
- If multiple routes are present, the route that will be used to send the next packet on is marked by “*”.

5.5 Key Technologies

EIGRP employs four key technologies as given below:

- Neighbour Discovery, Maintenance and Recovery
- Reliable Transport Protocol - Utilizes Reliable Transport Protocol (RTP) for delivery of EIGRP packets.
- DUAL Finite State Machine
- Protocol Dependant Modules [1]

5.5.1 Neighbour Discovery, Maintenance and Recovery

Simple distance vector routing protocols such as RIP and IGRP do not establish a relationship with their neighbours. RIP and IGRP routers merely broadcast or multicast updates on configured interfaces to all neighbours. In contrast EIGRP routers actively establish relationships with their neighbours. The neighbour relationship that EIGRP establishes can be compared to that used by OSPF. EIGRP routers establish adjacencies with their neighbour routers by using small hello packets. [13]

By forming neighbour relationship with adjacent routers, EIGRP is able to achieve the following:

- Dynamically learn of new routes that join the network
- Identify routes that become either unreachable of inoperable
- Rediscover routers that had previously been unreachable [1]

EIGRP routers send out small hello packet on all of its configured interfaces. A router discovers a neighbour when it receives its first hello packet on a directly connected link. The router requests DUAL to send full route information as update to the new neighbour. In response, the neighbour sends its full route information as an update. When both routers have exchanged hello packets and routing information they are regarded as neighbours and are said to be converged. A new neighbour relationship between two adjacent routers A and B can be established in the following steps:

1. When a router *A* receives a hello packet from a new neighbour *B*, *A* sends its topology Table to router *B* in unicast updates with the initialization bit turned on.
2. Upon receipt of the update router B sends an acknowledgement.
3. Router B then sends its topology Table to router *A* using a unicast update.
4. Route A acknowledges the update and the two routers from a neighbour relationship. Each router adds information about its neighbour in the neighbour Table used by EIGRP. [1]

EIGRP does not build neighbour relationships over secondary addresses as all EIGRP traffic is sourced from the primary address of the interfaces. Also when EIGRP is configured for use over a multi-access Frame Relay network (point-to-multipoint, and so on), the **broadcast** keyword in the **frame-relay map** statements must be used. Without the **broadcast** keyword the adjacencies would not establish between two EIGRP routers on such networks. [1, 11, 13, 19]

After neighbour relationship has been established between the two routers, hello packets are sent periodically by each router to maintain the relationship. As long as a router receives hello packets from its neighbour, it assumes that the neighbour is functioning, and the two can exchange routing information. By default hello packets are sent every 5 seconds on high-bandwidth links and 60 seconds on low-bandwidth links. Hello packets are very small and act as keepalives only. They do not contain any routing information allowing them to consume minimal bandwidth. Through the use of hello packet EGIRP routers advertise hold-time*.* Hello-time is the amount of time that a router regards a neighbour as functional without having obtained any packets from it. The default hold-time is three times that of the hello interval, which is 15 seconds and 180 seconds for high-bandwidth and low-bandwidth links respectively. The hello-interval can be changed with the following command in interface configuration mode:

ip hello-interval eigrp *autonomous-system-number seconds*

Increasing the hello-interval increases the route convergence time as detection of new neighbours is also delayed. However, a longer hello-interval may be needed on a congested network with many EIGRP routers to conserve bandwidth of the network. [1, 13, 19]

Modification to the hello-interval does not modify the hold-time automatically. It needs to be manually modified separately. Hold time should be configured to be three times of the hello interval as per Cisco recommendation. The hold-time can be changed with the following command in interface configuration mode:

ip hold-time eigrp *autonomous-system-number seconds*

The hello-interval and hold-time do not have to be the same for all routers on an EIGRP network. Each router advertises its own hold-time, which is recorded in its neighbours Table and used by the neighbour to time the advertising router out. This is different from OSPF where all routers in a particular area have to use the same hello times in order to be able to converge. [1, 13, 19]

If no hello packets are received for the duration of the hold-time, DUAL start computation to make the necessary changes to the neighbour, topology and the routing Tables depicting the loss of the neighbour that failed to send hello packets. Subsequently DUAL sends updates the other routers of the failed link. Thus, in addition to detecting new neighbour, hello packets are also used to maintain and detect the loss of a neighbour. When a downed neighbour comes back up it sends hello packets again to from new relationship with adjacent routers. [1]

There are no limitations on the number of neighbours that EIGRP can support, however the recommended number of neighbour relationship is 30. The actual number of supported neighbours depends on the capability of the routers, such as:

- memory capacity
- processing power
- amount of exchanged information, such as the number of routes sent
- topology complexity
- network stability [5]

5.5.2 Reliable Transport Protocol

Reliable Transport Protocol is a transport-layer protocol that can guarantee ordered deliver of EIGRP packets to all neighbours. On an IP network, hosts use TCP to sequence packets and ensure their timely delivery. As EIGRP was designed to support multiple routed protocols, it cannot reply on TCP/IP to exchange routing information like RIP, IGRP and OSPF. To stay independent of IP specific protocols, EGIRP uses Reliable Transport Protocol (RTP) as its proprietary transport-layer protocol to guarantee delivery of routing information. [1]

RTP can provide both reliable and unreliable transport service as and when required. It supports both multicast and unicast transmission of packets. For efficiency, only certain EIGRP packets are transmitted reliably. RTP contains a provision for sending multicast packets quickly when unacknowledged packets are pending, which helps ensure that convergence time remains low in the presence of varying speed links. The IP multicast address used is 224.0.0.10 with port number 88. [1, 13]

EIGRP requires guaranteed and sequenced delivery for some transmissions. This is achieved using acknowledgments and sequence numbers. The sequence number (seq num) of the last packet from each neighbour is recorded in the neighbours Table to ensure that packets received are in sequence. Packets that are sent reliably have unique sequence numbers. Acknowledgment packet with the correct sequence number is expected from the receiving router. After transmission of a reliable packet EIGRP puts the packet in queue because it may require retransmission. If an acknowledgment with the correct sequence number is not received from the receiving router, the packet is retransmitted as a unicast. The number of packets in the queue that may require retransmission is shown as a queue count (QCnt) in the neighbour Table. Smooth round trip time (SRTT) which is an estimate of the time its takes a packet to travel to and from the receiving router is used to calculate the retransmission timeout (RTO). RTO shows the amount of time a router will wait for an acknowledgment before retransmitting. [13]

The different packets used by EIGRP are discussed in details later in the report.

5.5.3 Dual Finite State Machine

Diffusing algorithm more commonly known as DUAL is used by EIGR track all routing updates and perform route calculations. The full name of this technology is DUAL finite-state machine (FSM). An FSM is an abstract machine, not a mechanical device with moving parts. FSM is an algorithm that defines a set of possible states that something can go through, what events cause those states, and what events result from those states. The DUAL FSM contains all the logic used to calculate and compare routes in an EIGRP network. The principles that DUAL relies on to function properly as outlined below:

- Neighbour loss or detection will occur within a finite time.
- Messages are received in an orderly and correct manner, within a finite time.
- Messages are processed in the order in which they are received, within a finite time. [1, 8, 13]

DUAL tracks all routing information that is received from neighbours and stores them in the topology Table. It then uses a composite metric to calculate the cost for each route to destinations. It finds the route with the least cost according to the metric and places a copy of the route in the routing Table. If there are multiple paths with the lowest cost DUAL allows multiple successor routes to be put into the routing Table. There can be up to four successor routes by default which can be increased to six. DUAL also checks other routes that are available to reach the same networks but are not the least cost. The second best path to the destination is designated as the feasible successor route provided it meets the feasibility condition. It is not compulsory to have a feasible successor route but DUAL tries to calculate it each time as having a feasible successor significantly decreases network convergence times during successor failures. There can be multiple feasible successor routes as well and are placed only in the topology Tables. These routes are backup routes and are not used to forward traffic until there is a problem with the successor routes. [1]

DUAL also guarantees that each path is loop free. The feasibility condition which each feasible successor must meet is also a test for loops. If the feasibility condition is met, the router advertising the reported distance must have a path to the destination which does not go through the router checking the feasibility condition. If it did, the reported distance would have been higher than the feasibility distance.

After a network has converged only hello packets are used to maintain neighbour relationships. No updates are sent or received unless there is a change in the network topology which conserves link bandwidth. Any of the following events can cause DUAL to re-evaluate the routes:

- The transition in the state of a directly connected link
- A change in the metric of a directly connected link
- An update from a neighbour

There are two types of DUAL computation that can take place depending on whether a feasible successor is present for the destination that has been affected by the link failure. If there is a feasible successor route present for the destination then the type of computation that takes place is known as Local Computation. Alternatively if there are no feasible successor present for the destination then the type of computation that takes place is known is Diffusing Computation. [1, 8, 13, 25]

5.5.3.1 Local Computation

As already mentioned feasible successor routes are backup routes that can be used in the event of a successor route failure. Local computation takes place when there is a feasible successor present for a destination whose successor route has gone down. As information about the feasible successor is already present in the topology Table, the local router does not need to send query to other routers regarding routes to the destination. The router simply takes the information about the feasible successor from the topology Table and puts it into the routing Table changing the route status to successor. The change over process is instantaneous as all the data are already present in Tables held by the local router. This type of computation takes less then a second and causes minimal disruption to the network. The local router then sends out update to all its neighbours informing them of the change to the route. This feature of EIGRP greatly decreases its convergence times and enhances its efficiency during change in the network topology.

The list of Feasible Successors for a particular route are also reassessed locally if there is a change to the cost of the link, a change of state or if update, query or reply packets are received. Depending on the particular case re-computation can lead to feasible successor being changed to successor, successor being changed to feasible successor or addition of new routes. [1, 8, 13, 25]

5.5.3.2 Diffusing Computation

During failure of a successor route, Diffusing Computation takes place when there is no feasible successor present for the destination. When performing Diffusing Computation, queries are sent to all the neighbours regarding the path information for the destination network. The network is said to be in an active state during this type of computation. The originating router does not consider the

Diffusing Computation to be complete until replies have been received from all the neighbours. If the neighbour that is being queried does not have a successor route to the destination in question it queries all its neighbours before sending a reply. The *query range* and its issues are discussed in details later in this chapter. Queries to neighbour are sent reliably using RTP. A time known as **Active Timer** is used to detect the amount of time that is being taken by each neighbour to reply. On a large network with many routers, it can take a considerable amount of time before the originating router receives reply to all its queries. If reply to a query is not received from a neighbour within 3 minutes, then the route is said to be **Stuck-in-Active (SIA)**. The neighbour from whom a reply was not received is removed from the neighbour Table and the metric for that route set to infinity so that another neighbour can meet the Feasibility Condition and become a Successor. SIA is a major issue with EIGRP networks especially if they are large size networks. SIA and its concerning issues are discussed in details later in this chapter.

Most well functioning EIGRP networks convergence within couple of seconds even during this type of computation. However, in the worst case even a properly working EIGRP process can take up to 16 seconds. This convergence estimate is based on the detection of a link failure and the time necessary to respond with a new route calculation. [1, 5, 13]

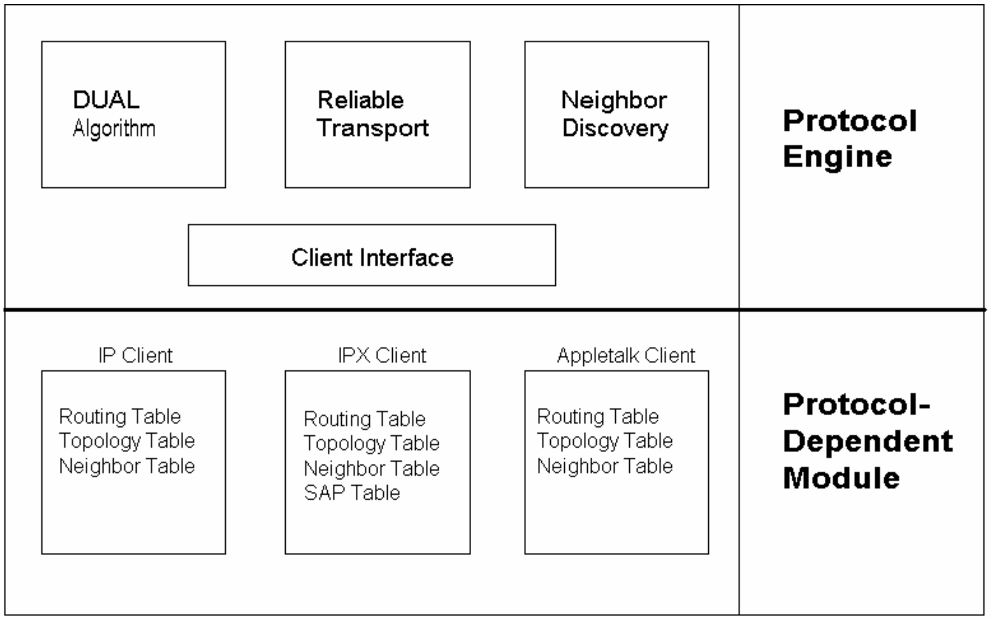
5.5.4 Protocol Dependant Module

One of the most attractive features of EIGRP is its modular design. Modular layered designs prove to be the most scalable and adaptable. Support for routed protocols such as IP IPX and AppleTalk is included in EIGRP through Protocol Dependant Modules (PDM). In theory EIGRP can be easily made to adapt to new or revised routed protocols (for example IPv6) by addition of extra PDM.

There are three PDM that EIGRP employs with each being responsible for all functions related its specific routed protocol. The IP-EIGRP module is responsible for the following:

- Sending and receiving EIGRP packets that bear IP data
- Notifying DUAL of new IP routing information that is received
- Maintaining the results of DUAL’s routing decisions in the IP routing Table.
- Redistribution routing information that was learned by other IP-Capable routing protocols.

Figure 5.9 – PDM layered structure



The IP protocol-dependent module (PDM) handles the transfer of information between the Tables. After DUAL calculates successor routes it is the responsibility of PDM to transfer the route information from the topology Table to the routing Table. The PDM may also carry information in the reverse direction that is from the routing Table to the topology Table. This occurs when routes are being redistributed into EIGRP from another protocol. The IP PDM is also responsible for encapsulating EIGRP messages in IP packets.

As mentioned before, each plug-in module handles the network protocol is responsible for services to specific routed protocol. This is particularly useful because routing protocols for different routed protocols use different metrics for route calculations. For example, although there is a form of RIP for IPX called IPX RIP, it uses a slightly different method of metric calculation than IP RIP. IP RIP uses hop count as its metric, whereas IPX RIP uses a delay expressed as ticks. [13]

5.6 EIGRP Packets

EIGRP packets are encapsulated directly in IP with the protocol field set to 88. The destination IP address of EIGRP packets depend on the type of the packet. Some packets are sent as multicast (with an address of 224.0.0.10) and others are sent as unicast. The source IP address is the IP address of the interface from which the packet is issued.

EIGRP uses the following packet types:

- hello
- acknowledgment
- update
- query
- reply [13]

5.6.1 Hello Packets

Hello packets are used for neighbour form and maintain neighbour relationships. They are sent as multicasts and do not require acknowledgment. EIGRP hello packets are sent out by each router to their neighbours at regular intervals to maintain neighbour relationship. The hello packet is vital for both establishing a neighbour relationship between routers and determining whether or not a neighbour has died or is no longer available. If a hello packet is not received from a neighbour before its hold time expires, that neighbour is regarded as unreachable.

EIGRP by default sends hello packets every 5 seconds on high bandwidth links and every 60 on low bandwidth links. The following are classified as high bandwidth links by EIGRP:

- broadcast media, such as Ethernet, Token Ring, and FDDI
- point-to-point serial links, such as PPP or HDLC leased circuits, Frame Relay point-to-point sub-interfaces, and ATM point-to-point sub-interface
- high bandwidth (greater than T1) multipoint circuits, such as ISDN PRI and Frame Relay [1, 13, 22]

5.6.1 Acknowledgment Packets

An acknowledgment packet is an EIGRP hello packet with no data inside it. Acknowledgment packets contain a nonzero acknowledgment number. This is the number of the message whose receipt is being acknowledged. Acknowledgement packets are sent using the unicast address of the router that sent the message which is being acknowledged. A neighbour is declared dead if it fails to acknowledge 16 consecutive unicast packets which it received using the reliable delivery method. As explained earlier, Routers normally re-transmit packets that need to be sent reliably if their acknowledgement is not received within the specified RTO. [1, 13, 22]

5.6.3 Update Packets

Update packets are used to send changes in routing information. When a new neighbour is discovered, unicast update packets are sent so that the neighbour can build up its topology Table. The updates are forwarded by neighbours to their neighbours as soon as they are received. This allows for quick convergence and allows each router to have a complete view of the entire network. Unlike other distance vector routing protocols EIGRP does not send updates periodically. It only sends updates when there are changes in the network topology such as routes becoming unavailable. Updates contain only the essential information concerning the route in question and are sent only to neighbours that are affected by the change. In other words, they are bounded updates, sent only to neighbours that need the information. If this update information is required by several neighbours, a multicast packet is sent. If the change affects only one router, however, a unicast packet is sent. Update packets always use reliable delivery require and require acknowledgments. When an update is sent to a neighbour, the router then expects a response, indicating that the update was received. Unicast updates are sent to routers that fail to acknowledge updates. RTO is used to determine the waiting period before a router starts retransmission of updates. If a neighbour fails to acknowledge 16 consecutive unicast updates that router is marked as unreachable. All routes through the router are recalculated using DUAL. [1, 13, 22]

5.6.4 Query Packet

When a router looses the successor route for a destination and is unable to locate a feasible successor it sends out query packets to all its neighbours enquiring about the destination in question. If a neighbour has a route to the intended destination it replies with its route information. If the neighbour does not have a route it in turn enquires its neighbours. Initial Query packets are always multicast. These packets are sent reliably and require an acknowledgement. The query process in EIRGP is unique and can lead to complications in large networks. Issues related to EIGRP query process and range of queries is later dealt with in a separate section of this chapter.

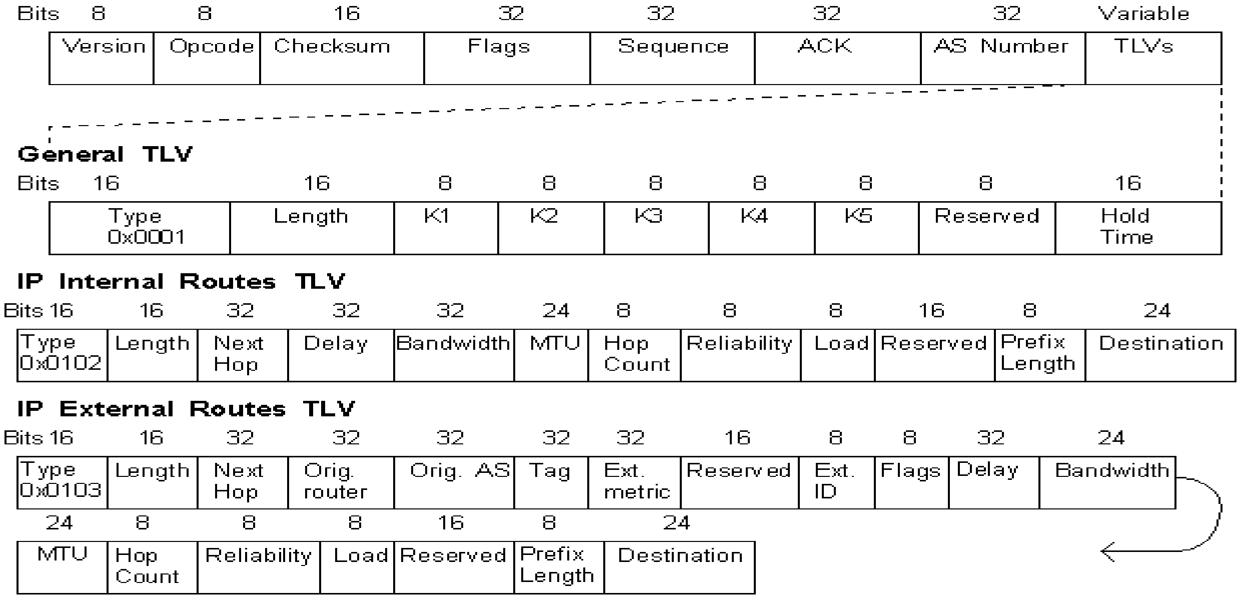
5.6.5 Reply Packet

Reply packets are sent in response to query packets to instruct the originator of route information for the queried path. Reply packets are unicast to the originator of the query. Reply packets are also transmitted reliably and require acknowledgement.

5.6.6 Packet Format

All the packet types use the same packet format, but there is a slight difference in TLV of the packets depending whether the route was learnt internally or externally. Figure 5.10 show the format of an EIGRP packet.

Figure 5.10 – EIGRP Packet format. [72]



Bits	8	8	16	32	32	32	32	Variable
	Version	Opcode	Checksum	Flags	Sequence	ACK	AS Number	TLVs

General TLV

Bits 16	16	8	8	8	8	8	8	16
Type 0x0001	Length	K1	K2	K3	K4	K5	Reserved	Hold Time

IP Internal Routes TLV

Bits 16	16	32	32	32	24	8	8	8	16	8	24
Type 0x0102	Length	Next Hop	Delay	Bandwidth	MTU	Hop Count	Reliability	Load	Reserved	Prefix Length	Destination

IP External Routes TLV

Bits 16	16	32	32	32	32	32	16	8	8	32	24
Type 0x0103	Length	Next Hop	Orig. router	Orig. AS	Tag	Ext. metric	Reserved	Ext. ID	Flags	Delay	Bandwidth

24	8	8	8	16	8	24
MTU	Hop Count	Reliability	Load	Reserved	Prefix Length	Destination

The EIGRP packet shown in Figure 5.10 is explained below:

- **Version** - there has only been one version
- **Opcode** - this is the EIGRP packet type:
  - **1** - Update
  - **3** - Query
  - **4** - Reply
  - **5** - Hello
  - **6** - IPX SAP
- **Checksum** – The checksum applies to the entire EIGRP packet excluding the IP header.
- **Flags** - The LSB (0x00000001) is the **Init** bit meaning that the route in this packet is the first in a new neighbour relationship. The next bit (0x00000002) is the **Conditional Receive** bit used in Cisco's Reliable Multicasting algorithm.
- **Sequence** - the 32-bit sequence number used by RTP.
- **ACK** - the 32-bit sequence last heard from the neighbour. A Hello packet with a non-zero value is an ACK.
- **AS Number** - the Autonomous System number of the EIGRP domain.
- **Type/Length/Value (TLV)** - There are a number of TLVs, all of them begin with a 16 bit Type field and a 16 bit Length field. There then follows a number of fields that vary depending on the type as given below.
  - General TLVs

    - **0x0001** - General EIGRP parameters (applies to any EIGRP packet regardless of protocol)
    - **0x0003** - Sequence (used by Cisco's Reliable Multicast)
    - **0x0004** - EIGRP software version, the original version being **0** and the current version being **1** (used by Cisco's Reliable Multicast)
    - **0x0005** - Next Multicast Sequence (used by Cisco's Reliable Multicast)
  - IP TLVs
    - **0x0102** - IP internal routes
    - **0x0103** - IP external routes
  - AppleTalk TLVs
    - **0x0202** - AppleTalk internal routes
    - **0x0203** - AppleTalk external routes
    - **0x0204** - AppleTalk cable setup
  - IPX TLVs
    - **0x0302** - IPX internal routes
    - **0x0303** - IPX external routes

The Figure 5.10 also illustrates the General TLV (containing the 'K' values) and the IP TLVs (containing details such as the five metrics). IP TLV is the most common and important. The formal to IP TLV is explained below:

Type 0x0102 IP internal routes TLV

- **Type 0x0102**
- **Length** - Length of the TLV
- **Next Hop** - The next hop route for this route
- **Delay** - The number of 10 microsecond chunks which is the sum of delays
- **Bandwidth** - 256 * IGRP bandwidth
- **MTU** - The smallest MTU encountered along the route to this particular destination network.
- **Hop Count** - A number between 0x00 (directly connected network) and 0xFF.
- **Reliability** - A number between 0x01 and 0xFF to indicate the error rates totalled along the route. 0xFF is reliable.
- **Load** - A number between 0x01 and 0xFF expressing the total load along a route where 0xFF is totally loaded.
- **Reserved** - 0x0000 and not used.
- **Prefix Length** - The number of bits used for the mask
- **Destination** - Destination network

Type 0x0103 IP external routes TLV

- **Type 0x0103**
- **Length** - Length of the TLV
- **Next Hop** - The next hop route for this route
- **Originating Autonomous System** - The AS from where the route came

- **Tag** - Used with Route Maps to track routes
- **External Protocol Metric** - The metric for this route used by the external routing protocol e.g. IGRP, OSPF, RIP
- **Reserved** - 0x0000 and not used.
- **External Protocol ID** - identifies the external protocol advertising this particular route
    - **0x01** - IGRP
    - **0x02** - EIGRP (a different AS)
    - **0x03** - Static Route
    - **0x04** - RIP
    - **0x05** - Hello
    - **0x06** - OSPF
    - **0x07** - IS-IS
    - **0x08** - EGP
    - **0x09** - BGP
    - **0x0A** - IDRP
    - **0x0B** - directly connected
- **Flags** - **0x01** means the route is an external route whereas **0x02** means that the route could be a default route.
- **Delay** - The number of 10 microsecond chunks which is the sum of delays
- **Bandwidth** - 256 * IGRP bandwidth
- **MTU** - The smallest MTU encountered along the route to this particular destination network.

- **Hop Count** - A number between 0x00 (directly connected network) and 0xFF.
- **Reliability** - A number between 0x01 and 0xFF to indicate the error rates totalled along the route. 0xFF is reliable.
- **Load** - A number between 0x01 and 0xFF expressing the total load along a route where 0xFF is totally loaded.
- **Reserved** - 0x0000 and not used.
- **Prefix Length** - The number of bits used for the mask
- **Destination** - Destination network [72]

The Table 5.1 provides a summary for the EIGRP packets outlining their type, function and how they are sent.

Table 5.1 - EIGRP Packet Summary

Type	Transmit	Reliable / Unreliable	Function
Hello	Multicast	Unreliably	Neighbour discovery/recovery
Acknowledgement	Unicast	Reliably	Zero byte acknowledgement (with ACK number)
Updates	Unicast	Reliably	Neighbour discovery
	Multicast	Reliably	Link cost or metric change updates
Queries	Multicast	Reliably	When feasible successor not present for active rotate
Replies	Unicast	Reliably	Sent to originator of a query.
Requests	Multicast or Unicast	Unreliably	Request specific information from neighbours

5.7 Route Tagging

EIGRP topology Tables hold additional information about routes showing how and where they were learned from. EIGRP classifies routes as either internal or external. Routes that have originated within the same EIGRP Autonomous system are regarded as Internal Routes. External routes are ones that have been learned from another routing protocol such as RIP, OSPF and IGRP. Static routes that reside in the routing Table are also classified as external. The routes are tagged individually with the identity of their origination.

External routes are tagged with the following information:

- The router ID of the EIGRP router that redistributed the route.
- The AS number where the destination resides.
- A configurable administrator tag.
- Protocol ID of the external protocol.
- The metric from the external protocol.
- Bit flags for default routing.

The Figure 5.4 shows topology entry for an external route that was learnt by EIGRP by redistribution with IGRP.

EIGRP also allows administrative tags to be configured as any number between 0 and 255. Tags can be used to deploy special routing policies. External routes from other networks can be accepted, rejected or propagated based on any of the routing tag information held by EIGRP. The configured Administrative tag can also be used as a base for decisions. Using EIGRP customized route tagging can give a network administrator control and flexibility in enforcing routing policies. Route tagging is particularly useful in when EIGRP interacts with Border Gateway Routing Protocol (BGP) which performs policy based routing. [1]

5.8 Query Processing and Range

When a router looses routes to a particular destination due to failure of its neighbouring router, it first checks its topology Table to find feasible successor for each of the destinations whose routes were lost. If it is not able to find routes to that destination it will send queries to all its current neighbours asking about routes to the destinations that were just lost. If the neighbour has routes to the destination network that was affected by the loss of the link then the neighbour replies with information about its route to the destination. If the neighbour does not have a route to the destination it queries all its neighbours to find routes to the destination. This process goes on until all the routers in the AS have been checked to find a route to the destination. Whether or not a route is found to the destination through any neighbour, the querying router must wait for all its queries to be replied before it can start DUAL computation to choose the best path. This is because until the router has information about routes from each of its neighbouring routers it will not be able to choose the optimal route for the destination.

This query process used by EIGRP can lead to problems as a neighbour will not reply to a query until it has checked with all its neighbours and so on. In large networks with a large number of routers this can lead to a convergence problem.

When replying to a query from a neighbour EIGRP routes act according the rules shown in Table 5.2

Table 5.2 – Query Procedure [22]

Query from	Route state	Action
neighbour (not successor)	Passive	Reply with current successor information.
successor	Passive	Checks for Feasible successor. If FS is not available then queries are sent to other neighbours requesting route information. If a route is found through other neighbours route is installed. The querying neighbour is updated with the new route information. If no route is found then the message is sent to the querying router.

any neighbour	no path through this neighbour before query	Send successor route information
any neighbour	not known before query	Send Reply saying that the destination is unreachable
neighbour (not the current successor)	Active	if there is no current successor to this destinations reply with an unreachable message
		if there is a good successor, reply with the current path information
successor	Active	Attempt to find new successor; if successful, reply with new information; if not successful, mark destination unreachable and query all neighbours except the previous successor. Update the querying neighbour after route information is verified.

The affects of the query process and the range of query on the network depend greatly on the number of routers on the network and their configuration.

5.8.1 Issues Affecting Query Range

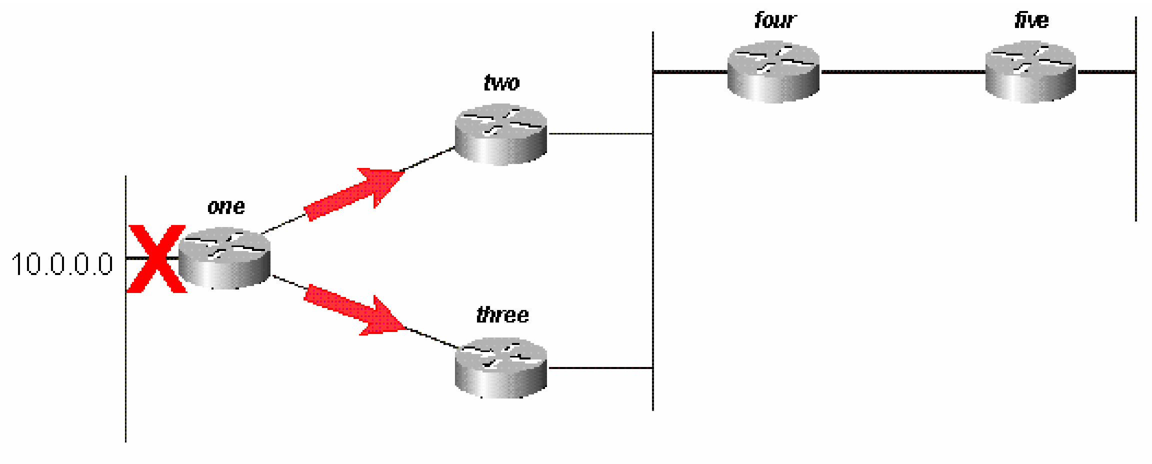
Route Summarization, Autonomous system boundary and distribution lists affect the range of an EIGRP query. These issues will be discussed in the next few section of this report.

5.8.1.1 Route Summarization

Any form of summarization done by routers will stop queries from traversing through the router. Automatic summarization done by EIGRP or Manual summarization both have the same affect on the query range. The router performing the summarization will not forward any query packets to its neighbours.

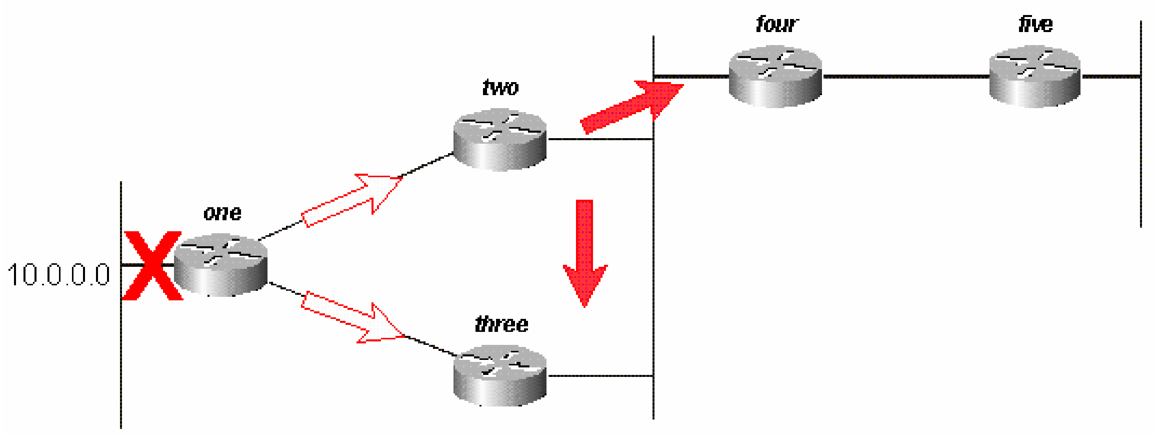
To understand the affect let us consider Figure 5.12 shown below. In the network shown below router four summarizes routes before passing them on to router five. The link to Network 10.0.0.0 which is directly connected to router one goes down. Router one checks to see that there is no alternative route for the destination and send out query to all its neighbours to find a route to the destination.

Figure 5.12 – Affect of Route summarization on Query Range (1) [22]



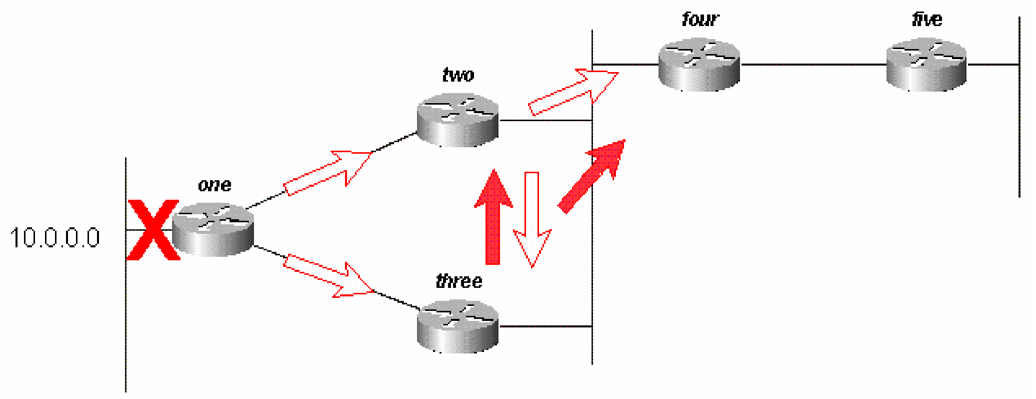
When router two gets the query it checks its topology Table to see that router one was the successor to the destination network and it does not have any alternative routes to the destination network 10.0.0.0. It sends out query to all its neighbours which are shown in Figure 5.13.

Figure 5.13 – Affect of Route summarization on Query Range (2) [22]



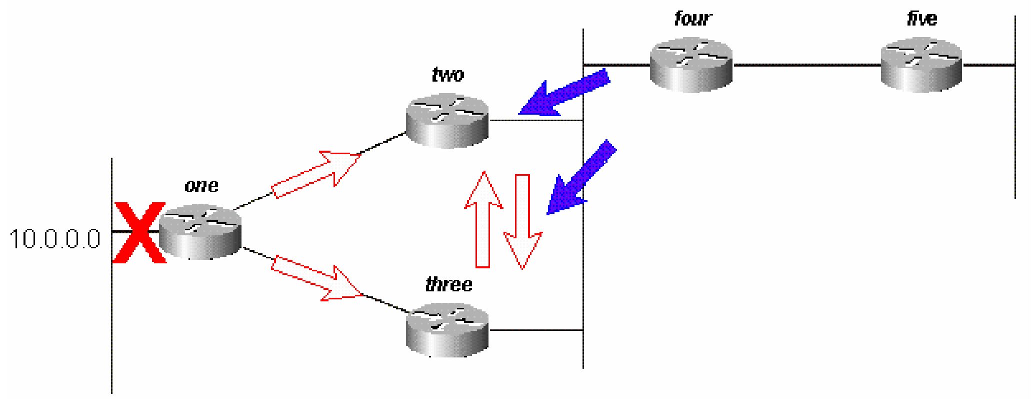
When router three gets the query from router one it does the same thing as router two shown in Figure 5.13.

Figure 5.14 – Affect of Route summarization on Query Range (3) [22]



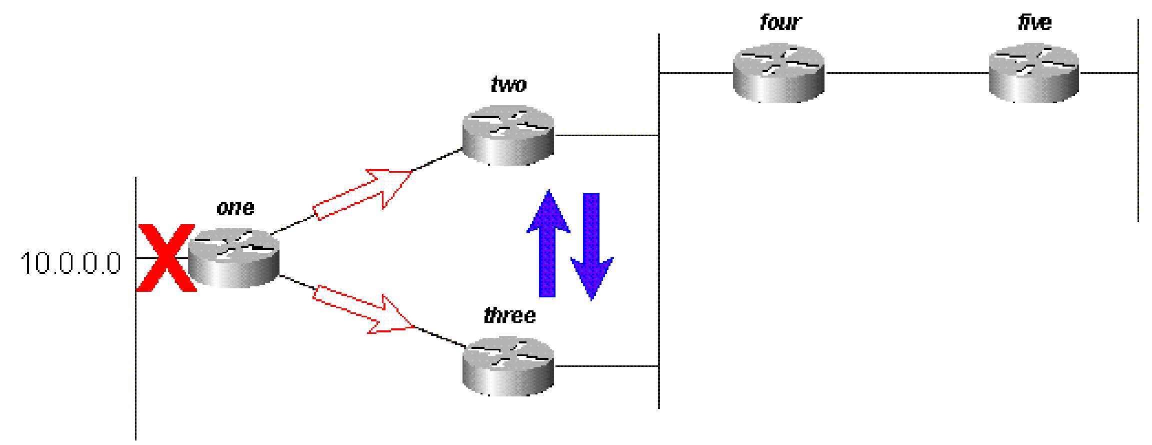
Once router four receives the queries from router two and three it instantly replies with information telling both routers it does not have a route to the destination 10.0.0.0. It does not pass the query on as it summarizes the routes advertised by router one, two and three before passing them on to router five. The Figure 5.15 shows the reply from router four coming back to router two and three.

Figure 5.15 – Affect of Router summarization on Query Range (4) [22]



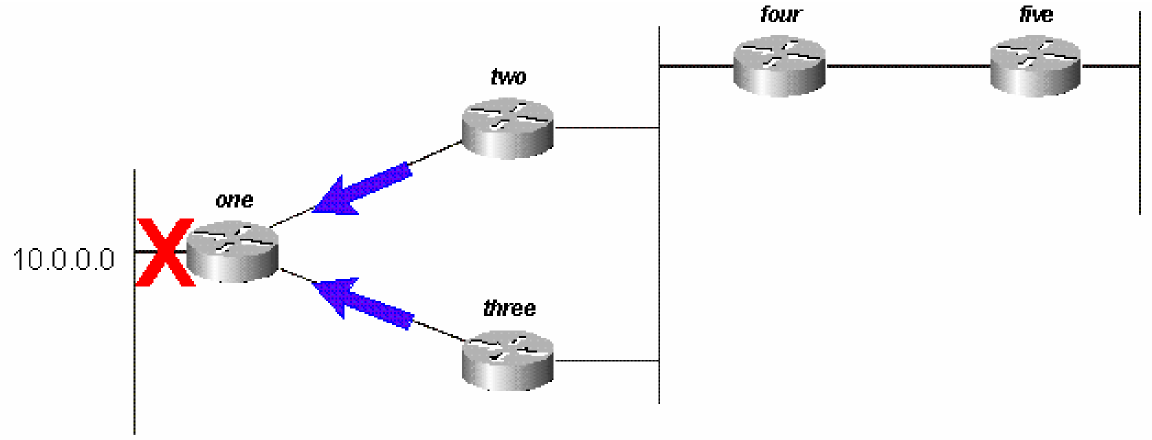
Once router two and three obtain a reply from router four they send replies to the queries that the sent to each other. This is shown in Figure 5.16

Figure 5.16 – Affect of Route summarization on Query Range (5) [22]



Finally after getting reply from both router two and router four, router three becomes certain it does not have any routes to the destination 10.0.0.0. Similarly, router two having got replies to its query from router three and four determines that it also does not have a route to destination 10.0.0.0. As all queries sent by both router two and router three have been answered, they now send reply to the original query from router one. This can be seen in Figure 5.17

Figure 5.17 – Affect of Route summarization on Query Range (6) [22]



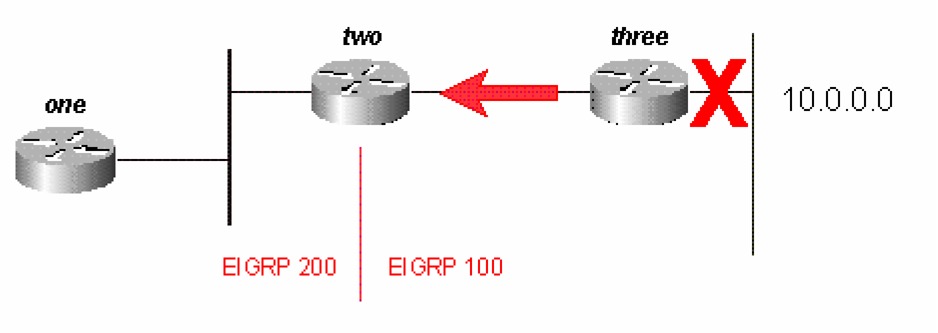
Thus, summarization of routes by routers is able to stop queries from traversing through them and can be used to control the range of queries on EIGRP networks.

5.8.1.2 Autonomous System Boundaries

If a router that is redistributing routes between two EIGRP autonomous systems receives a query it replies to the query using the procedures outlined in Table 5.2. According to the rules found in the Table, if the router does not have a valid route it queries its neighbours about routes to the destination. The boundary router will send a reply to the querying router saying the destination is unreachable. Although the original query does not propagate throughout the network, it leaks into the second autonomous system in the form of a new query. This technique helps to prevent stuck in active (SIA) problems in a network by limiting the number of routers a query must pass through before being answered, but it does not solve the overall problem that each router must process the query. [22]

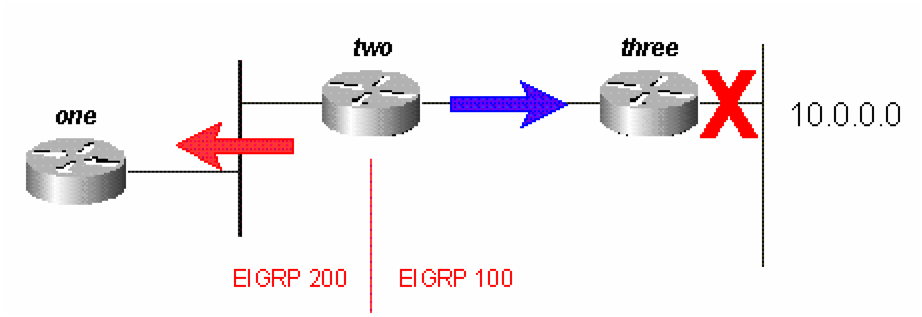
The network shown in Figure 5.18 consists of three routers. Router two is a border router for both EIGRP 200 AS and EIGRP 100 AS. Router three belongs to AS 100 and router one belongs to AS 200. When router three looses its link to network 10.0.0.0 it send a query about the route to its neighbour (router two).

Figure 5.18 – Affect of Autonomous System Boundary on Query Range (1) [22]



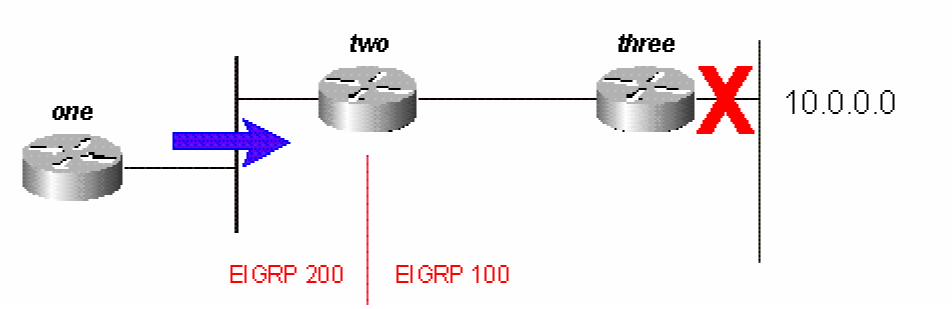
As router two does not readily have an alternative route to network 10.0.0.0 it replies to router three with a replying saying that network 10.0.0.0 is unreachable. Router two then send a query to its neighbours enquiring about a route to network to 10.0.0.0. These two aspects are shown in Figure 5.19 As router two replies to the query of route three instantly without waiting for router one to reply to its query, the reply time of query sent by router three is minimal.

Figure 5.19 – Affect of Autonomous System Boundary on Query Range (2) [22]



Finally Router two also get an update from router one telling it that network 10.0.0.0 is unreachable through router one. This can be seen in Figure 5.20.

Figure 5.20 – Affect of Autonomous System Boundary on Query Range (3) [22]

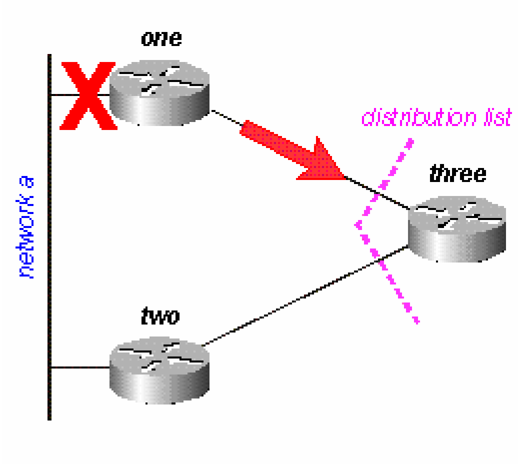


5.8.1.3 Distribution List

Distribution lists have somewhat the same affect as Autonomous system boundaries. The router implementing a distribution list will always reply to a query from a neighbour showing the destination network as unreachable. Even if the router receiving the query has a valid route to the queried network due to distribution list being applied on it, the router will reply to the query saying that the network is unreachable.

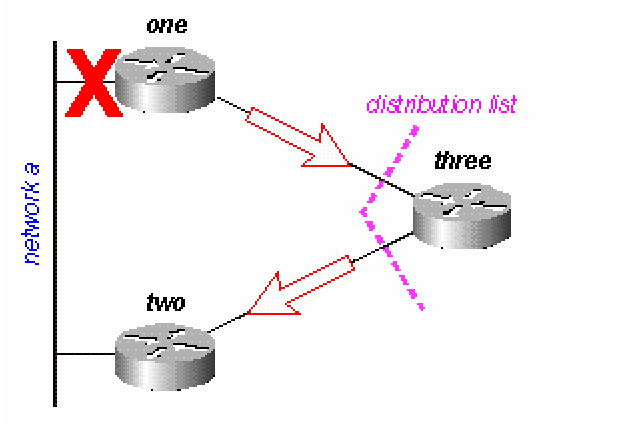
Figure 5.21 show a network where a distribution list has been configured on router three. The distribution allows router three to only advertise certain networks out its interfaces. The distribution list does not permit router three to advertise network a. Router one only knows of the directly connected route that it has to network a. It is not able to see a route through router three as router three does not advertise network a. When the directly connected link of Router one to network a goes down it queries its neighbour (router three) about a route to the destination network a.

Figure 5.21 – Affect of Distribution list on Query Range (1) [22]



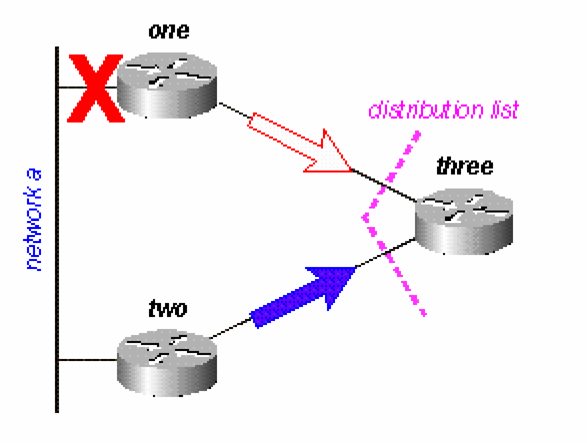
Upon receipt of the query from router one, router three behaves according to the procedures defined in Table 5.2. As it does not have a valid route to network a, it queries its neighbour (router two). This can be seen in Figure 5.22.

Figure 5.22 – Affect of Distribution list on Query Range (2) [22]



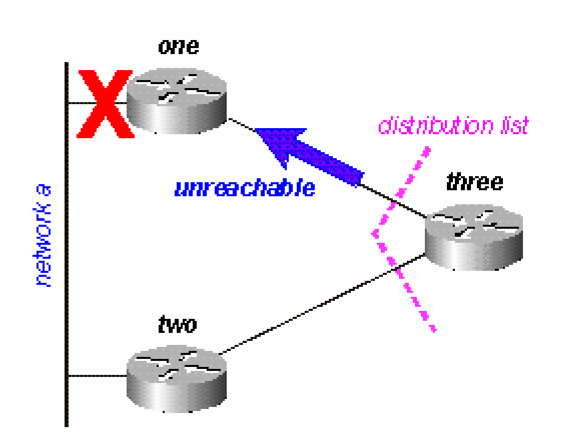
When router two receives a query from router three it replies to the query with a valid route to network a. This can be seen in Figure 5.23.

Figure 5.23 – Affect of Distribution list on Query Range (3) [22]



Although router three now has a reply from router two giving it a valid route for network a, it will reply to router one with an unreachable message due to the configuration of the distribution list. This effect can be seen in Figure 5.24

Figure 5.24 – Affect of Distribution list on Query Range (4) [22]



5.9 Metric

When a router advertises its route information, it includes its metric and calculated total delay in the update. The receiving router then adds its local delay to the total received for use in its metric calculation. This then is regarded as the total cost for the links. By default EIGRP uses the minimum bandwidth on the path to a destination network and the total delay to compute routing metrics.

EIGRP can use the following metrics to calculate the cost of its routes:

- Bandwidth
- Load
- Delay
- Reliability
- MTU

Bandwidth - The bandwidth metric is based on the bandwidth statement on an interface in the routing path. The bandwidth value used in the calculation of the cost for a route takes into account the lowest bandwidth of any link of the route. The value is cumulative and static.

Delay - The delay metric is also static and is an accumulation of the entire path delay. For each link on the route it is inversely proportional to bandwidth of the link.

Reliability - Calculated from keepalives, the reliability metric is dynamic and represents the reliability of the path over time. A link with lower reliability would become less desirable. Reliability values range from 0 to 255, with the default 255 being 100 percent reliable. This metric is not enabled by default.

Loading - Loading is a dynamic measure of the utilization of the link, expressed as a value from 0 to 255, with the default 0 being 0 percent load. This can be used to avoid congestion. However, doing so could result in significant changes to the routing Table and these changes may occur too slowly to improve real-time data transfers. The loading metric is not enabled by default.

MTU - The maximum transmission unit (MTU) portion of the metric takes into account the fact that some media can support larger packet sizes. For example, Ethernet can support only 1500-byte packets, whereas FDDI, ATM, and Token Ring can all easily exceed that value. By the same measure, some serial interfaces cannot support MTUs greater than 576 bytes. Because fragmentation and header overhead are reduced with a larger MTU, these routes are preferable. MTU metric is also not enabled by default. [1, 22]

In default settings EIGRP only uses bandwidth and delay for metric calculation. These five metric components are signified by constants used in the EIGRP metric calculation formula. These constants, known as K values, are named K1 through K5. The k values can be manipulated to control the affect that it has on the metric calculations. Table 5.3 shows the default K values setting on EIGRP.

Table 5.3 – K-value default setting.

K Value	Default Value
K1	1
K2	0
K3	1
K4	0
K5	0

The default values may be modified by use of the metric weights router configuration command in the EIGRP router configuration mode, which enables EIGRP to include the K values' corresponding constants in its metric calculations. However, it is strongly recommended by Cisco not to change the default settings for these values. For routers to form an adjacency through establishment of neighbour relationships they must have the same K values. If two routers with different try to from an adjacency, EIGRP will generate an error message showing that there is a mismatch of the K values of the concerned routers.

After the router receives an update from its neighbour, it performs metric calculations based on the metric passed to it from that neighbour, and it compares the result to the metrics calculated by its other neighbours, as well as its own self-calculated metric. The metric is also considered the cost of the given path to the destination. The lowest cost path is then chosen is chosen as the best route for the destination. Figure 5.25 shows the formula that is used for the metric calculation. [13]

Figure 5.25 – EIGRP Metric Calculation Formula [13]

$$\text{metric} = \left[(\text{K1} \times \text{bandwidth}) + \left[\frac{(\text{K2} \times \text{bandwidth})}{(256 - \text{load})} \right] + (\text{K3} \times \text{delay}) \right] + \left[\frac{\text{K5}}{(\text{reliability} + \text{K4})} \right]$$

This is the same formula used for IGRP so the values need to be scaled by a factor of 256 as EIGRP uses 32 bits rather then 24bits like IGRP.

For EIGRP default operation, however, only K1 and K3 are used, so this formula can be very much simplified down to the following:

Metric = Bandwidth + Delay

The **show interface** command shows the configured bandwidth and delay on the link. During calculation of cost for a route the minimum bandwidth on the path to a destination network needs to be taken into consideration.

The bandwidth from the **show interface** command needs to be scaled using the following formula to give the cost for the bandwidth:

Cost *[Bandwidth]* = (10000000/Bandwidth) x 256

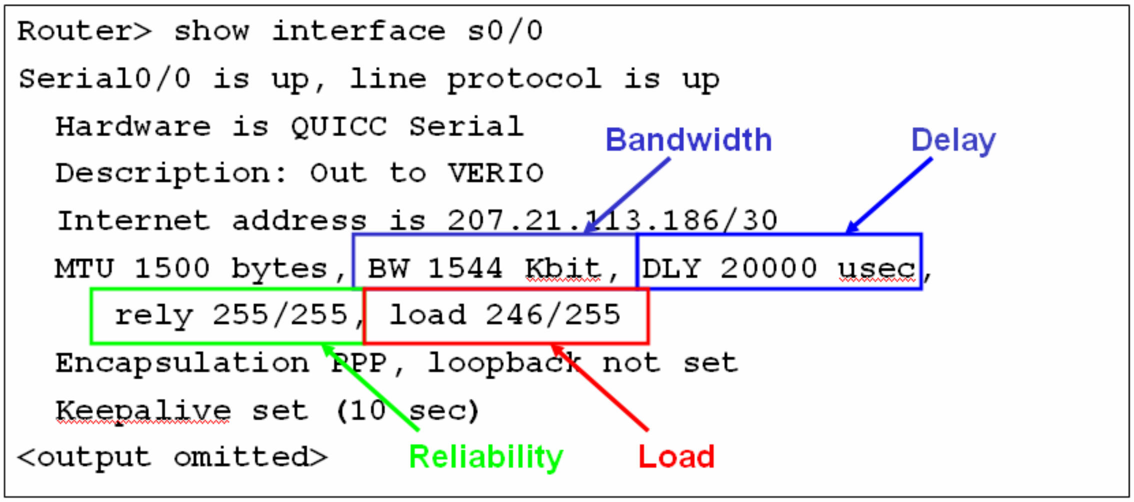
The delay from the **show interface** command needs to be scaled using the following formula to give the cost for the delay:

Cost *[Delay]* = Delay /10 x 256

To give the cost or metric for an entire path, the sum of cost of all delays to the destination need to be taken and then added to the cost of the minimum bandwidth configured along the path to the destination.

Figure 5.26 shows the show interface output from a route.

Figure 5.26 – Show interface output of router. [65]



```
Router> show interface s0/0
Serial0/0 is up, line protocol is up
  Hardware is QUICC Serial
  Description: Out to VERIO
  Internet address is 207.21.113.186/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     rely 255/255, load 246/255
  Encapsulation PPP, loopback not set
  Keepalive set (10 sec)
<output omitted>
```

The k values that influence the metric calculation can be changed by using the following command:

Router(config-router)# **metric weights** *tos k1 k2 k3 k4 k5*

5.10 Load Balancing

Load balancing is the capability of a router to distribute traffic over multiple routes that can be used to reach a destination. Load balancing increases the utilization of the routes that are available, thus giving a greater bandwidth and increasing the overall network efficiency. There are two types of load balancing:

- Equal cost path
- Unequal cost path [65]

5.10.1 Equal Cost Path Load Balancing

Every routing protocol supports equal cost path load balancing. Equal path load balancing is an automatic feature of Cisco IOS. By default, if there are multiple equal-cost paths to a destination the router will share the traffic across up to four paths. Depending on the version of the IOS the number of paths may be increase to six with the command **maximum-paths.** In the default setting each path will receive an equal amount of traffic. [65]

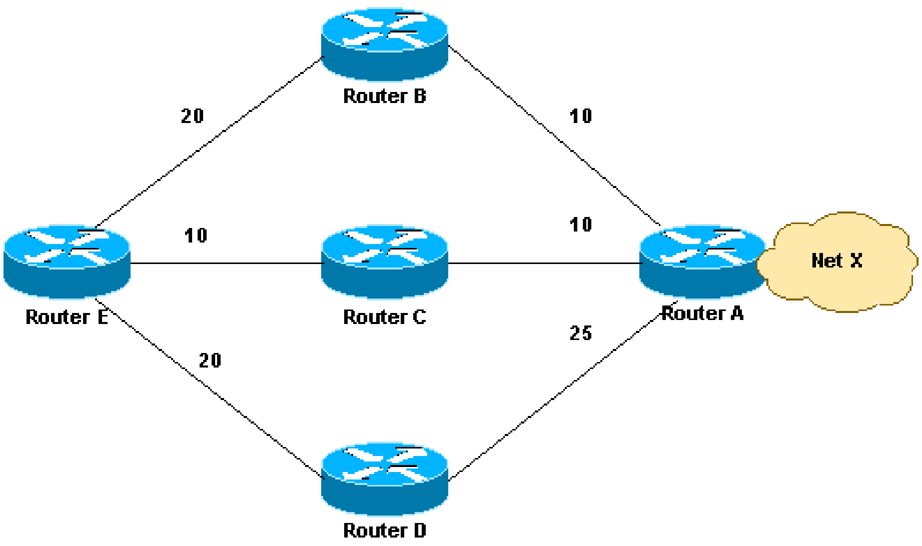
This feature of the protocol will be tested and analyzed in the next chapter of this report.

5.10.2 Unequal Cost Path Load Balancing

EIGRP also supports unequal cost path load balancing. EIGRP needs to be configured to for this type of load balancing. It is required to tell EIGRP which of the non optimal routes should be used to load balance. This is done in regards to the least cost path. The least cost path will have been already selected by EIGRP and put in the routing Table. The **variance *n*** command needs to be used to instruct the router to include routes with a cost less than ***n*** times the minimum cost route for that destination. The variable ***n*** can take a value between 1 and 128. The default is 1, which allows the equal cost path load balancing.

To avoid routing loops EIGRP will only load balance over successor and feasible successor routes. Any known route that does not meet the feasibility condition will not be used to forward traffic as these routes may contain routing loops.

Figure 5.27 – EIGRP unequal path load balancing [8]



In the network shown in Figure 5.27, there are three ways to get to Network X from router E:

- E-B-A with a cost of 30
- E-C-A with a cost of 20
- E-D-A with a cost of 45

During DUAL calculations E-C-A with a metric of 20 will be chosen as the successor because it has the least cost. Using the command **variance 2** in the network configuration interface will instruct the router to use paths which have cost less then twice that of the successor route. Thus any path which meets the feasibility condition and has cost less then 40 will be used to perform load balancing. From the above Figure it can be seen that route E-B-A has a cost of 30. Router E will therefore use both routes E-C-A and E-B-A to forward traffic to network X. Route E-D-A will not be used because it has a cost higher than 40. If the variance command was changed to **variance 3** which would allow EIGRP to include routes with cost up to 60 the route E-D-A would still not be used by EIGRP to forward traffic as the route does not meet the feasibility condition. That is the reported distance of router D (25) is not less then the Feasible distance (20) of the current successor route which is E-C-A.

This feature of the protocol will be tested and analyzed in the next chapter of this report.

5.10.2.1 Traffic Sharing

EIGRP not only provides unequal cost path load balancing, but also intelligent load balancing, such as traffic sharing. By default EIGRP will divide traffic over the links according to the ratio of the cost of the paths. Paths with higher cost will get less traffic where as paths with lower cost will get more traffic. This feature can be controlled using the **traffic-share balanced** command. By default this feature is turned on. If this feature was disabled EIGRP would share traffic equally even over the paths with different cost. This would decrease the efficiency of the network as both high and low cost paths would get the same amount of traffic sent through them.

A special feature which is available on the new IOS is the command **traffic-share min across-interfaces**. When this feature is used EIGRP forwards traffic through the best path only. This is identical to the forwarding behaviour without use of the **variance** command. However, when the **traffic-share min** command and the **variance** command is used, even though traffic is sent over the minimum-cost path only, all feasible routes get installed into the routing Table. This means during a link failure the router instantly sends packet through the other routes to the destination. The 1 sec. or so time needed by DUAL for a Local Computation is not needed and the convergence is instant. There are also no packet losses owing to the instant switching. [8, 15]

If **traffic-share min command** was configured along with **variance 3** on router E shown in Figure 5.27, router E would forward traffic only using route E-C-A although both routes E-C-A and E-B-A will be present in the routing Table. If a link failure occurred on route E-C-A the router would be instantly able to forward traffic using route E-B-A giving spontaneous convergence.

5.11 Variable Length Subnet Mask

Unlike RIP and IGRP, EIGRP updates carry subnet mask information. This allows the protocol to support variable length subnet masking. The network designer or the administrator can use a wide range of IP addressing schemes to make efficient use of the available addresses. Using subnet with sizes that reflect the size of the host population on the subnet conserves addresses and can increase network efficiency if a hierarchy is maintained. [1]

This feature of the protocol will be tested and analyzed in the next chapter of this report.

5.12 Route Summarization

Route summarization in EIGRP is automatic across major network boundaries, but many administrators disable this feature in order to take advantage of manual summarization on all boundaries and gain more control. EIGRP provides support for VLSM and some designs have dis-contiguous subnets. In such cases the auto summarization feature must be disabled. The best EIGRP designs yield very small core routing Tables divided at a very high level based on summarization. The default behaviour of EIGRP is to summarize on network-number at boundaries. [1, 15, 22]

This feature of the protocol will be tested and analyzed in the next chapter of this report.

5.12.1 Automatic Summarization

Summarizing on network-number boundaries is an easy way to reduce the size of routing Tables and the complexity of the network. Disabling route summarization should be undertaken only when necessary.

The auto summarization feature of the protocol can be turned off using the command **no auto-summary**. To re-enable the feature the command **auto-summary** needs to be used in the router configuration mode. [13, 15]

This feature of the protocol will be tested and analyzed in the next chapter of this report.

5.12.2 Manual Summarization

EIGRP allows for the summarization of (external or internal) routes on any boundary. Manual summarization can be used to reduce the size of routing Tables. This feature is needed when there are dis-contagious subnets within the network which cannot be summarized automatically. The following command can be used to perform manual summarization.

ip summary-address eigrp *network address* subnet mask

This feature of the protocol will be tested and analyzed in the next chapter of this report.

5.13 Split Horizon and Poison reverse

Split Horizon and Poison reverse are methods used by distance-vector routing protocols to avoid routing loops. Split Horizon is a routing technique in which information about routes are not sent back through the interface on which they were received. This stops neighbours from advertising routes between them that they learnt from each other. Poison reverse is another technique where routers advertise routes with large hop counts so that they are regarded as unreachable through the advertising router. Distance-vector routing protocols do not build or have a complete overview of the network. Thus, the need to use these techniques to eliminate routing loops.

As EIGRP uses DUAL to ensure a loop free topology and does not send periodic updates out all interfaces split horizon and poison reverse are not needed for its convergence operations. By default it is enabled in Cisco routers and EIGRP uses split horizon or advertises a route as unreachable when:

- two routers are in start-up mode (exchanging topology Tables for the first time)
- advertising a topology Table change
- sending a query

When two routers first become neighbours, they exchange topology Tables during start-up mode. For each Table entry a router receives during start-up mode, it advertises the same entry back to its new neighbour with a maximum metric (poison route).

Split horizon controls the sending of EIGRP update and query packets. When split horizon is enabled on an interface, these packets are not sent for destinations for which this interface is the next hop. This reduces the possibility of routing loops. [1, 13, 22, 65]

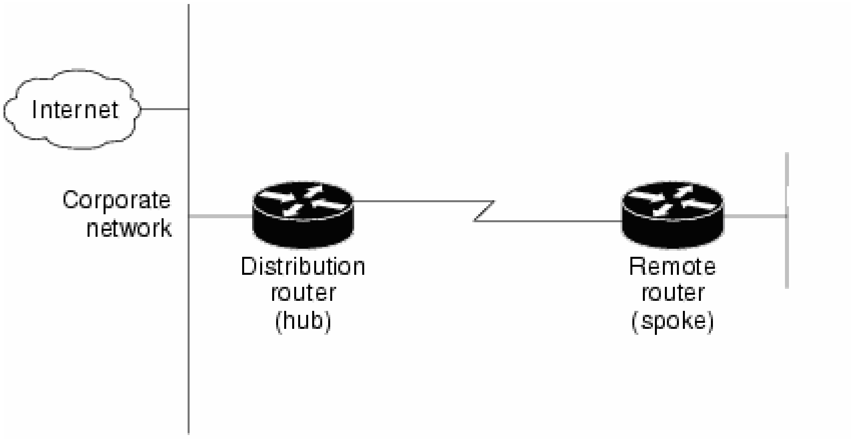
5.14 Stub Routing

Stub routing is mainly used for hub-spoke network topology. In a hub and spoke network, one or more end (stub) networks are connected to a remote router (the spoke) that is connected to one or more distribution routers (the hub). The remote router is adjacent only to one or more distribution routers. The only route for IP traffic to follow into the remote router is through a distribution router. A network that has only one route to get to outside networks is regarded as a stub network. This type of configuration is commonly used in WAN topologies where the distribution router is directly connected to a WAN. The distribution router can be connected to many more remote routers. Often, the distribution router will be connected to 100 or more remote routers in large networks. In a hub and spoke topology, the remote router must forward all non-local traffic to a distribution router, so it becomes unnecessary for the remote router to hold a complete routing Table. This is achieved by the use of default routes, so that all traffic are forwarded to the distribution router unless it is meant to the network segment directly connected to the remote router. [20]

Only the remote routers on an EIGRP hub and spoke network needs to be configured as a stub router. Only specified routes are advertised from the stub router to the local router. The router responds to queries for summaries, connected routes, redistributed static routes, external routes, and internal routes with the message "unreachable." This is similar to behaviours of routers with distributed list explained in the section about query processing. A stub router sends special peer packets to notify its neighbours of its status. [20]

EIGRP routers do not send queries to stub routers. The stub router will depend on the distribution router to send the proper updates to all peers.

Figure 5.28 – Stub Routing Network [20]



In the network shown in Figure 5.28 the remote router can access the corporate network and the Internet through the distribution router only. Bandwidth and memory can be conserved by summarizing and filtering routes on the distribution router. All spokes or remote routers should be configured with default routes so that they send all non-local traffic to the distribution router. The distribution router can then forward traffic to destination through the appropriate routes. The spoke router does not need to learn of routes to networks that are not local as all data will be forwarded to distribution router.

If stub features were not used on such networks, the hub on the network could send queries to the spokes about link failures. Using route summarization on the router would not stop it from sending out queries about lost routes. In large scale networks where there are hundreds of spokes connected to a hub this can lead to sever network congestions. Without the stub routing feature large EIGRP networks become very unstable if a hub and spoke topology is used. The stub feature stops the distribution router from sending queries to the internal spoke routers. This reduces the SIA problems that EIGRP has considerably. Thus the, EIGRP Stub Routing feature improves network stability, reduces resource utilization, and simplifies stub router configuration. [20]

5.14.1 Dual-Homed Remote

Simple hub and spoke networks have each remote router connecting to only one distribution router. There are topologies where remote router is connected to multiple distribution routers. This kind of topology is said to have Dual-Home

Remote. This configuration adds redundancy and introduces unique issues, and the stub feature helps to address some of these issues. Although a dual-homed remote will have two or more distribution routers connected to it, the principles of stub routing are the same as they are with a hub and spoke topology. This allows for redundancy as there are multiple paths available to reach the internal network.

5.14.2 Benefits

5.14.2.1 Greater Network Stability

During changes to the network topology, the EIGRP Stub Routing feature prevents EIGRP queries from being sent over limited bandwidth links to non-transit routers. Instead, distribution routers to which the stub router is connected replies to the query on behalf of the stub router. This feature greatly reduces the chance of further network instability due to congested or problematic WAN links.

5.14.2.2 Simplified Stub Router Configuration

The EIGRP Stub Routing feature greatly simplifies the configuration and maintenance of hub and spoke networks. When stub routing is enabled in dual-homed remote configurations, it is no longer necessary to configure filtering on remote routers to prevent those remote routers from appearing as transit paths to the hub routers. [22]

5.14.3 Restrictions

5.14.3.1 Supports Only Stub Routers

A router connected to the network core or distribution layer is regarded as a Stub Router. Core or transit traffic should not flow through a stub router. A stub router also can not have any EIGRP neighbours other than distribution routers. If stub routers are allowed to have EIGRP neighbours other than distribution routers, network becomes unstable can lead to complications. Finally, the stub router configuration should only be used on stub routers.

5.14.3.2 Multi-Access Interfaces

Multi-access interfaces, such as ATM, Ethernet, Frame Relay, ISDN PRI, and X.25, are supported by the EIGRP Stub Routing feature only when all routers on that interface, except the hub, are configured as stub routers. [22]

5.14.4 Configuring EIGRP Stub Routing

The steps show in Table 5.4 can be used to configure Stub feature on EIGRP routers.

Table 5.4 – Stub feature configuration steps

Command		Purpose
Step 1	router(config)# **router eigrp** as-number	Configures a remote or distribution router to run an EIGRP process.
Step 2	router(config-router)# **network** network-number	Specifies the network address of the EIGRP distribution router.
Step 3	router(config-router)# **eigrp stub** [**receive-only** | **connected** | **static** | **summary**]	Configures a remote router as an EIGRP stub router.

A router that is configured as a stub with the **eigrp stub** command shares connected and summary routing information with all neighbour routers by default. Four optional keywords can be used with the **eigrp stub** command to modify this behaviour:

- receive-only
- connected

- static

- summary

The **eigrp stub** command can be modified with several options, and these options can be used in any combination except for the **receive-only** keyword. The **receive-only** keyword will restrict the router from sharing any of its routes with any other router in that EIGRP autonomous system, and the **receive-only** keyword will not permit any other option to be specified because it prevents any type of route from being sent. The three other optional keywords (**connected**, **static**, and **summary**) can be used in any combination but cannot be used with the **receive-only** keyword. If any of these three keywords is used individually with the **eigrp stub** command, connected and summary routes will not be sent automatically.

The **connected** keyword will permit the EIGRP Stub Routing feature to send connected routes. If the connected routes are not covered by a network statement, it may be necessary to redistribute connected routes with the **redistribute connected** command under the EIGRP process. This option is enabled by default.

The **static** keyword will permit the EIGRP Stub Routing feature to send static routes. Without the configuration of this option, EIGRP will not send any static routes. Internal static routes that would normally be automatically redistributed will also not be advertised. The **redistribute static** command needs to be used to solve this problem.

The **summary** keyword will permit the EIGRP Stub Routing feature to send summary routes. Summary routes can be created manually with the summary address command or automatically take place automatically at a major network border router with the **auto-summary** command enabled. This option is also enabled by default.

There is no way to tell whether a router is acting as a stub or not from itself other then using then checking the running configuration. However, to verify the operation of a stub router **show ip eigrp neighbour detail** should be used on one of the spoke routers. [22]

The **debug eigrp packet stub** command may be used to display debug information about the stub status of peer routers. [22]

5.15 Integrating EIGRP in to IP Networks

When integrating EIGRP into existing networks a phased approach is best. First EIGRP should be added at the periphery of the network by configuring EIGRP on a boundary router on the backbone off the core network. Then EIGRP can be integrated into the core network.

The key considerations for integrating EIGRP into an IP network running IGRP are as follows:

- Route selection
- Metric handling
- Redistribution from IGRP to EIGRP and vice versa
- Route summarization

5.15.1 Redistribution between EIGRP and IGRP

Route Selection

EIGRP can be added to both single area and multiple are IGRP processes. EIGRP classifies its routes as internal, external, and summary. Internal routes are routes that are learned from the same EIGRP AS. External routes are routes that have been redistributed into EIGRP from other routing protocols. Summary routes are routes that EIGRP may dynamically create due to auto summarization, or due to an explicit summary route configuration. Route selection is based on administrative distance. The default administrative distance for EIGRP is 90 (internal), 170 (external), or 5 (summary). For IGRP, the default administrative distance is 100 because internal EIGRP routes take precedence over IGRP routes, and IGRP routes are preferred to external EIGRP routes.

One of the most unique features in EIGRP is the concept of an external route, which is how IGRP routes are tagged in EIGRP upon redistribution. External routes are learned from one of the following:

- A static route injected into the protocol
- A route learned from redistribution from another EIGRP AS
- Routes learned from other protocols, including IGRP

All routes tagged as external are given a higher administrative distance than internal EIGRP routes. This also means that during selection of best route, internal routes are given preference over external routes.

When EIGRP tags a route as external, it includes additional information about the route in the topology Table. This information includes the following:

- The router ID of the router that redistributed the route (EIGRP redistribution) and the AS number of that router
- The protocol used in the external network
- The metric or cost received with the route
- An external route tag that the administrator can use for filtering [19]

By default EIGRP will prefer internal routes to forward traffic rather then IGRP routes. This can however be changed by manually configuring administrative tags as explained earlier.

Metric Handling

The formula and default K values used for cost calculation of routes are the same for IGRP and EIGRP. By default, the composite metric is the sum of the segment delays and the lowest segment bandwidth (scaled and inverted) for a given route. Although this can be adjusted the default value with the **metric weights** command, the defaults were carefully selected by the proprietor Cisco to provide excellent operation in most networks.

Although, EIGRP and IGRP share the same composite routing metrics and mathematical weights, EIGRP supports metrics up to 32 bits. In contrast, IGRP only uses only 24 bits for the metric. EIGRP will automatically handle this issue, and after conversion metrics from either protocol are interchangeable. [19]

Redistribution

EIGRP can be added to an IGRP network in two ways: using the same IGRP AS number or using a new AS number. If EIGRP uses the same AS number as IGRP, redistribution of IGRP into EIGRP and redistribution of EIGRP into IGRP occurs automatically. If EIGRP uses a different AS number, the **redistribute** command needs to be configured manually on the border routers to redistribute routs. The **default-metric** command also needs to be used in conjunction with the redistribution command. IGRP routes redistributed into EIGRP are marked as external but, IGRP is not able to distinguish between IGRP and EIGRP routes.

Manual redistribution gives extra control allowing more control over routes and policy application. [19]

Route Summarization

With EIGRP, routing information advertised out an interface is often automatically summarized at major network number boundaries. The summarization is more evident for those routes whose major network number differs from the major network number of the interface to which the advertisement is being sent. Unless turned off, due to automatic summarization features, EIGRP will advertise summarized routes to IGRP. [19]

5.15.2 Redistribution between EIGRP and RIP

During redistribution between EIGRP and RIP the major for the boundary routers needs to be configured so that routes from RIP are advertised into EIGRP and vice versa. Particular care needs to be taken to ensure that protocols do not advertise routes learned from other protocols back to them.

The **passive-interface** command needs to be applied the interface of the RIP route connecting to the EIGRP router to address this issue. The **redistribute eigrp** router configuration command must be used on the RIP router. This would specify to the router that routing information derived from EIGRP should be advertised in RIP routing updates.

The **default-metric** router configuration command causes RIP to use the same metric value for all routes obtained from EIGRP. The default metric command helps solve the problem of redistributing routes between the protocols as they have different metrics. The **passive-interface** router configuration command disables the sending of routing updates from RIP route to EIGRP router. The RIP router will however still process updates that it receives on that interface and learns of networks that are behind a passive interface. For the EIGRP router the **default-metric** router configuration command assigns an EIGRP metric to all RIP derived routes. The minimum bandwidth, a route delay in tens of microseconds, connection reliability, the effective bandwidth of the route and the maximum transmission unit (MTU) of the route must be specified manually for the metric to function. When used with EIGRP, the **passive-interface** router configuration command has a different effect than it has when used with RIP or IGRP. When the **passive-interface** command is used with EIGRP, the router does not send out any updates including hello messages on the interface. This is done because routers running RIP will not be able to recognize EIGRP hello packets. This also means that the router does not learn about networks that are behind a passive interface.

In such cases Access-list needs to be configured with the networks that are available on the RIP network and distributed into the EIGRP network using a distribution list. [19]

5.16 Integrating EIGRP into Novell IPX Network

The key considerations for integrating EIGRP into an IPX network running RIP and SAP are as follows:

- Route selection
- Redistribution metric handling
- Redistribution from IPX RIP to EIGRP and vice versa
- Reducing SAP traffic

Adding EIGRP to a Novell IPX Network

EIGRP for a Novell IPX network has the same fast convergence and incremental update capabilities as EIGRP for IP. In addition, EIGRP provides several features that are designed to facilitate the building of large, robust Novell IPX networks. [22]

The first capability is support for incremental SAP updates. Novell IPX RIP routers send out large RIP and SAP updates every 60 seconds. This consumes a large amount of the available network bandwidth. In contrast, EIGRP for IPX sends out SAP updates only when changes occur and sends only changed information similar to that of IP EIGIRP.

The second capability that EIGRP adds to IPX networks is the ability to build large networks. IPX RIP networks have a diameter limit of 15 hops whereas; EIGRP networks can have a diameter of 224 hops.

The third capability that EIGRP for Novell IPX provides is optimal path selection. The RIP metric for route determination is based on ticks with hop count used as a tie-breaker. If more than one route has the same value for the tick metric, the route with the least number of hops is preferred. As already explained, routes selected based on hop count of purely distance may not be the optimal route. Instead of ticks and hop count, IPX EIGRP uses a combination of these metrics: delay, bandwidth, reliability, and load. [22]

Route Selection

IPX EIGRP routes are automatically preferred over RIP routes regardless of metrics unless a RIP route has a hop count which is less than the external hop count of an EIGRP advertised route.

Redistribution and Metric Handling

Redistribution is automatic between RIP and EIGRP, and vice versa. Automatic redistribution can be turned off using the **no redistribute** command.

The metric handling for integrating RIP into EIGRP is bandwidth plus delay, left shifted by 8 bits. The metric handling for EIGRP to RIP is the external metric plus 1. An IPX EIGRP router that is redistributing RIP into EIGRP takes the RIP metric associated with each RIP route, increments it, and stores that metric in the EIGRP routing Table as the external metric.

The EIGRP metric is created using the RIP ticks for the delay vector. The hop count is incremented and stored as the external metric. The external delay is also stored. [22]

Reducing SAP Traffic

Novell IPX RIP routers send out large RIP and SAP updates every 60 seconds containing full routing Tables regardless of whether a change to the network topology has occurred or not. These larger periodic updates consume a lot of the available network bandwidth. As, IPX EIGRP on sends incremental updates showing the changes in the network as and when they occur, it conserves bandwidth. [22]

5.17 Integration of EIGRP into AppleTalk Network

The key considerations for integrating EIGRP into an AppleTalk network are as follows:

- Route selection
- Metric handling
- Redistribution from AppleTalk to EIGRP and vice versa

Route Selection

AppleTalk EIGRP routes are automatically preferred over Routing Table Maintenance Protocol (RTMP) routes. AppleTalk metric for route determination is based on hop count only similar to that of distance vector routing protocols. In contrast AppleTalk EIGRP uses a combination of these configurable metrics: delay, bandwidth, reliability, and load. [19]

Metric Handling

The formula for converting RTMP metrics to AppleTalk EIGRP metrics is hop count multiplied by 252524800. This is a constant based on the bandwidth for a 9.6-Kbps serial line and includes an RTMP factor. An RTMP hop distributed into EIGRP has a relative higher cost than an EIGRP-native, 9.6-Kbps serial link. The formula for converting EIGRP to RTMP is the value of the EIGRP external metric plus 1. [19]

Redistribution

Redistribution between AppleTalk and EIGRP and vice versa is also automatic by default. Redistribution involves converting the EIGRP metric back into an RTMP hop count metric. In practice, there is no conversion of an EIGRP composite metric into a RTMP metric.

There is no conversion of an EIGRP metric back into an RTMP metric because, in reality, what RTMP uses as a metric (the hop count) is carried along the EIGRP metric all the way through the network. This is true of EIGRP derived routes and routes propagated through the network that were originally derived from an RTMP route. [19]

5.18 EIGRP Network Design Considerations

Although it may seem that networks using Cisco equipment should use EIGRP as it provides extremely fast convergence, relatively easy configuration, and variable-length subnetting there are factors that can cause significant problems in

EIGRP deployment. The most significant problem arises from the amount of memory and CPU power needed by routers for large networks. [5]

The simplest recommendations for deploying EIGRP fall into four basic areas and are as follows:

- Maximum possible amount of memory should be made available on each router. The amount of memory should be increased in proportion to the increase in number of neighbours.
- Each router should be allowed to have a limited number of neighbours. Passive interfaces can be configured on routers to stop them from building neighbour relationships. This would however significantly diminish the overall benefits of EIGRP. The generic guidelines recommend that EIGRP neighbours be kept to fewer than 30.This however depends on the amount of memory and the number of routes.
- Automatic redistribution feature should not be used unless the network is very simple. Automatic redistribution is a feature Cisco provides in order to make IGRP-to-EIGRP migration easier but provides very little control over the routes which are often needed for migration.
- Route summarization features of the protocol should be extensively used to reduce the size of the routing Tables which can further enhance stability and convergence. [5]

The major advantages of EIGRP compared to other distance-vector routing protocols that generally lead to migration are given below:

- **Low bandwidth consumption -** When the network is stable, the protocol relies only on hello packets. This greatly reduces the amount of bandwidth needed for updates.
- **Efficient use of bandwidth during convergence**- When a change occurs in the routing topology, EIGRP enters a period of active convergence. During this time, the routers attempt to rebuild their routing Tables to account for the change. To conserve bandwidth, EIGRP communicates only changes in the topological database to other routers in the AS, as opposed to communication of the entire routing Table, which consumes a great deal of bandwidth, especially in larger networks.
- **Support for VLSM**- As noted previously, EIGRP supports variable-length subnet masks. This support, along with support for classless Inter-net domain routing (CIDR), can greatly assist the network designer by offering greater flexibility and conservation in IP addressing. [19]

5.19 Pacing Packets Feature

By default, EIGRP is configured to use up to 50% of available link bandwidth. EIGRP however bases its usage on the configured bandwidth of the link rather then the actual bandwidth. There are two major reasons for controlling this feature of EIGRP as given below:

1. Generating more traffic than the interface can handle would cause drops, thereby impairing EIGRP performance.
2. Generating a lot of EIGRP traffic would result in little bandwidth remaining for user data.

As mentioned, EIGRP uses the bandwidth that is configured on an interface to decide how much EIGRP traffic to generate. If the bandwidth configured on an interface does not match the physical bandwidth, EIGRP may be generating too little or too much traffic. Both scenarios would cause a lot of problems. On large scale network if, EIGRP is not able to converge quickly enough or is unable to maintain convergence then the amount of bandwidth allocated to EIGRP must be increased, as it may not have been allocated enough bandwidth to be able to send all necessary message within a period of time. On smaller networks the amount of bandwidth available can be decreased because not much traffic will be generated by EIGRP on regular basis. There is however a risk of slower convergence times if EIGRP is not able to send all DUAL updates due to being allocated small bandwidth. [1, 5, 65]

The following command can be used to change the amount of bandwidth allocated to EIGRP for a link.

ip bandwidth-percent eigrp *as-number percent* [19]

5.20 Troubleshooting EIGRP

EIGRP can be difficult to troubleshoot because of its complexity. The best preparation for troubleshooting is to be familiar with the normal operations of the protocol. The second-best preparation for troubleshooting a network is the ability to track network implementations and changes.

Although significant literature was found and reviewed during the course of the project, a full list of troubleshooting issues and their solutions are outside the scope of this report. The literature found on troubleshooting has been referenced and can be used as necessary.

Cisco systems provides significant amount of troubleshooting advice and technical support for EIGRP implementation. In this section flow charts found at Cisco website will be used to briefly describe how troubleshooting should be attempted and classified. Major troubleshooting issues associated with the protocol and their solution will be discussed in details. Figure 5.29 show the main troubleshooting flowchart. Using this flowchart the problem can be identified to be either of the following:

- Neighbour Relationship issues.
- Redistribution issues
- Routing Issues
- Load balancing and
- Stuck in active issues.

Figure 5.29 – Main Troubleshooting Flowchart. [10]

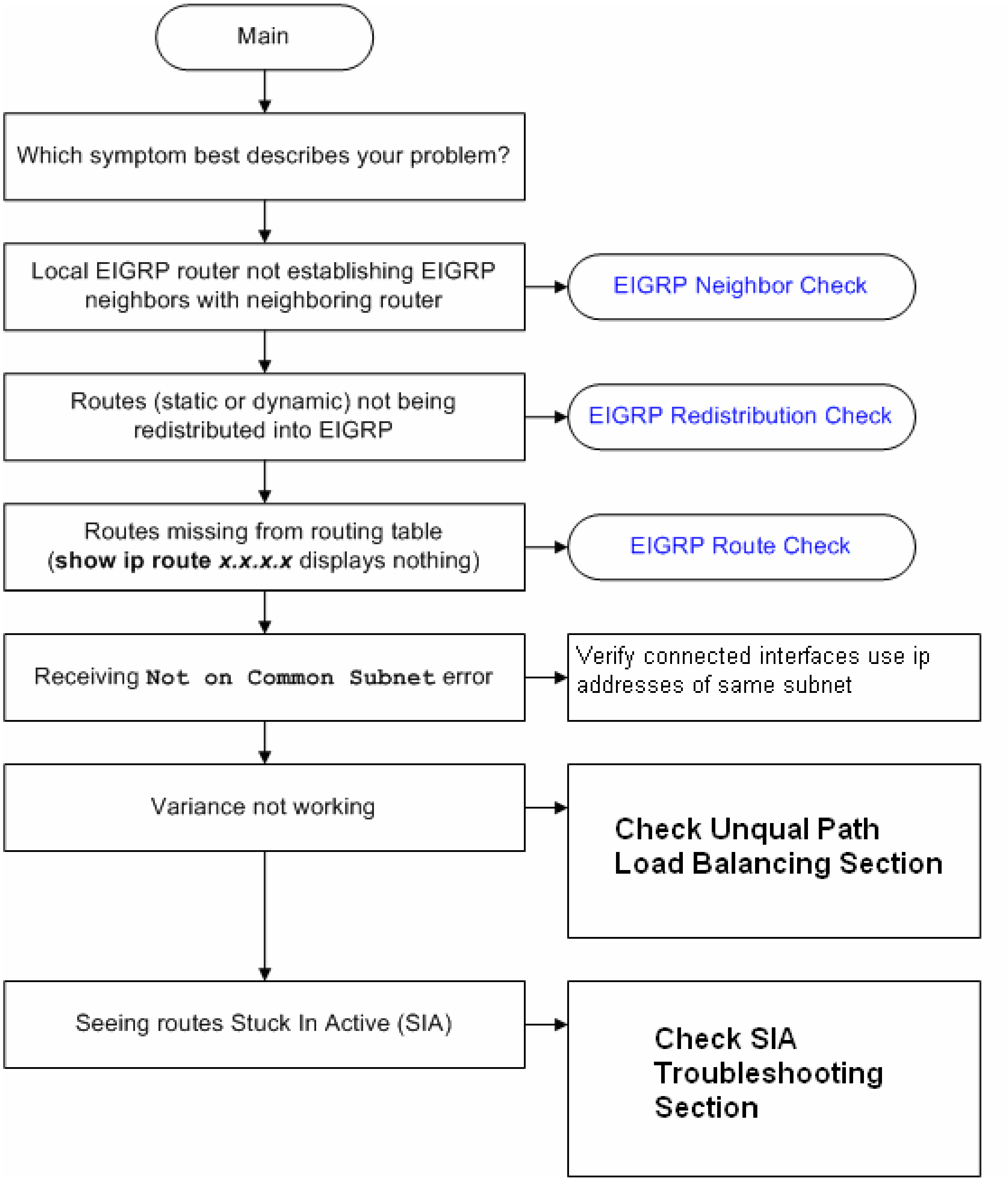

Main
Which symptom best describes your problem?
Local EIGRP router not establishing EIGRP neighbors with neighboring router
EIGRP Neighbor Check
Routes (static or dynamic) not being redistributed into EIGRP
EIGRP Redistribution Check
Routes missing from routing table (show ip route x.x.x.x displays nothing)
EIGRP Route Check
Receiving Not on Common Subnet error
Verify connected interfaces use ip addresses of same subnet
Variance not working
Check Unqual Path Load Balancing Section
Seeing routes Stuck In Active (SIA)
Check SIA Troubleshooting Section

Figure 5.30 shows the neighbour check flowchart. Figure 5.31 shows redistribution flowchart and Figure 5.32 shows flowchart for checking routes.

Figure 5.30(a) - Neighbour Check Flowchart [10]

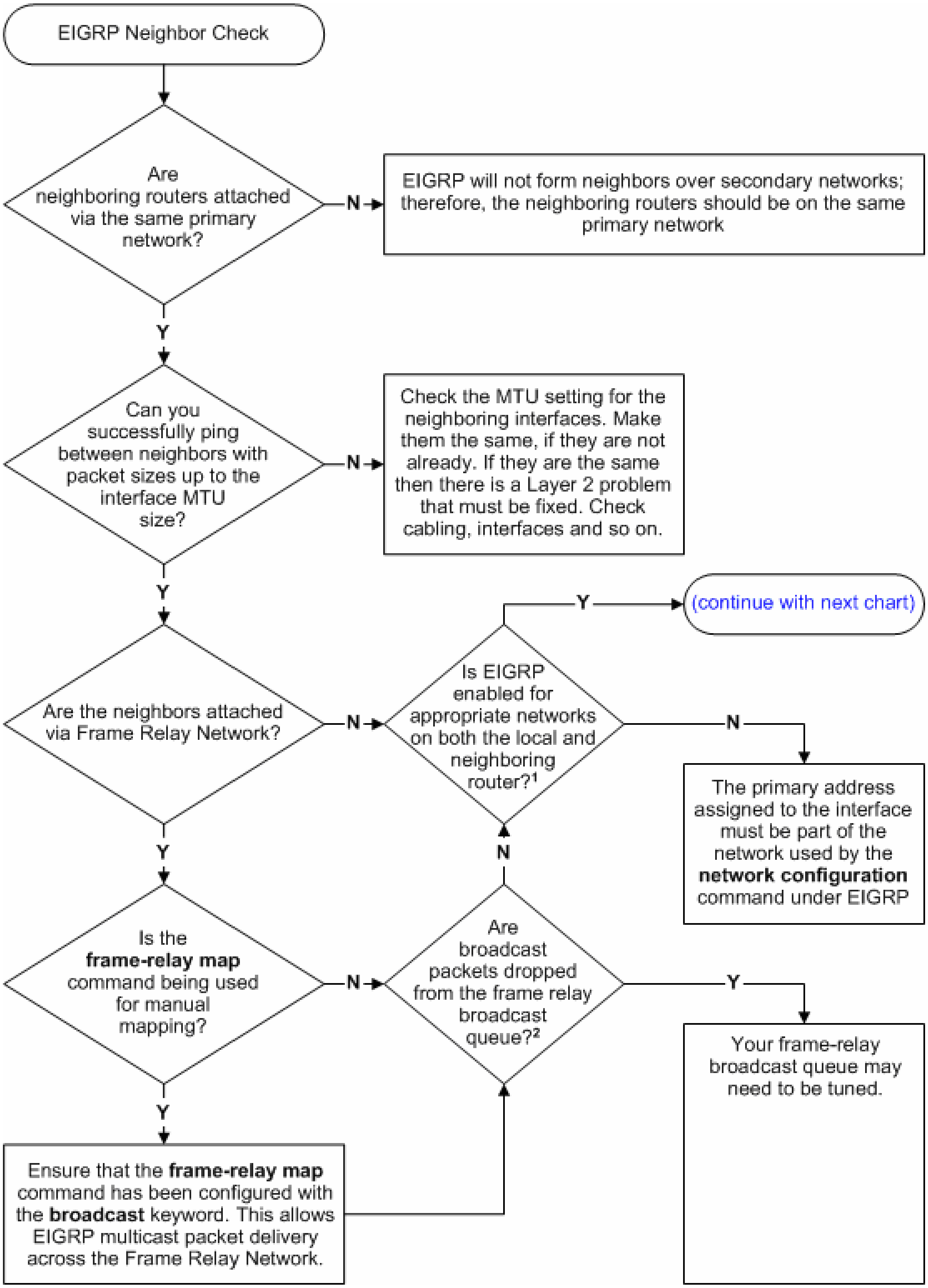

EIGRP Neighbor Check
Are neighboring routers attached via the same primary network?
N
EIGRP will not form neighbors over secondary networks; therefore, the neighboring routers should be on the same primary network
Y
Can you successfully ping between neighbors with packet sizes up to the interface MTU size?
N
Check the MTU setting for the neighboring interfaces. Make them the same, if they are not already. If they are the same then there is a Layer 2 problem that must be fixed. Check cabling, interfaces and so on.
Y
Are the neighbors attached via Frame Relay Network?
N
Is EIGRP enabled for appropriate networks on both the local and neighboring router?¹
Y
(continue with next chart)
N
The primary address assigned to the interface must be part of the network used by the **network configuration** command under EIGRP
Y
Is the **frame-relay map** command being used for manual mapping?
N
Are broadcast packets dropped from the frame relay broadcast queue?²
N
Y
Your frame-relay broadcast queue may need to be tuned.
Y
Ensure that the **frame-relay map** command has been configured with the **broadcast** keyword. This allows EIGRP multicast packet delivery across the Frame Relay Network.

Figure 5.30(b) - Neighbour Check Flowchart Continued [10]

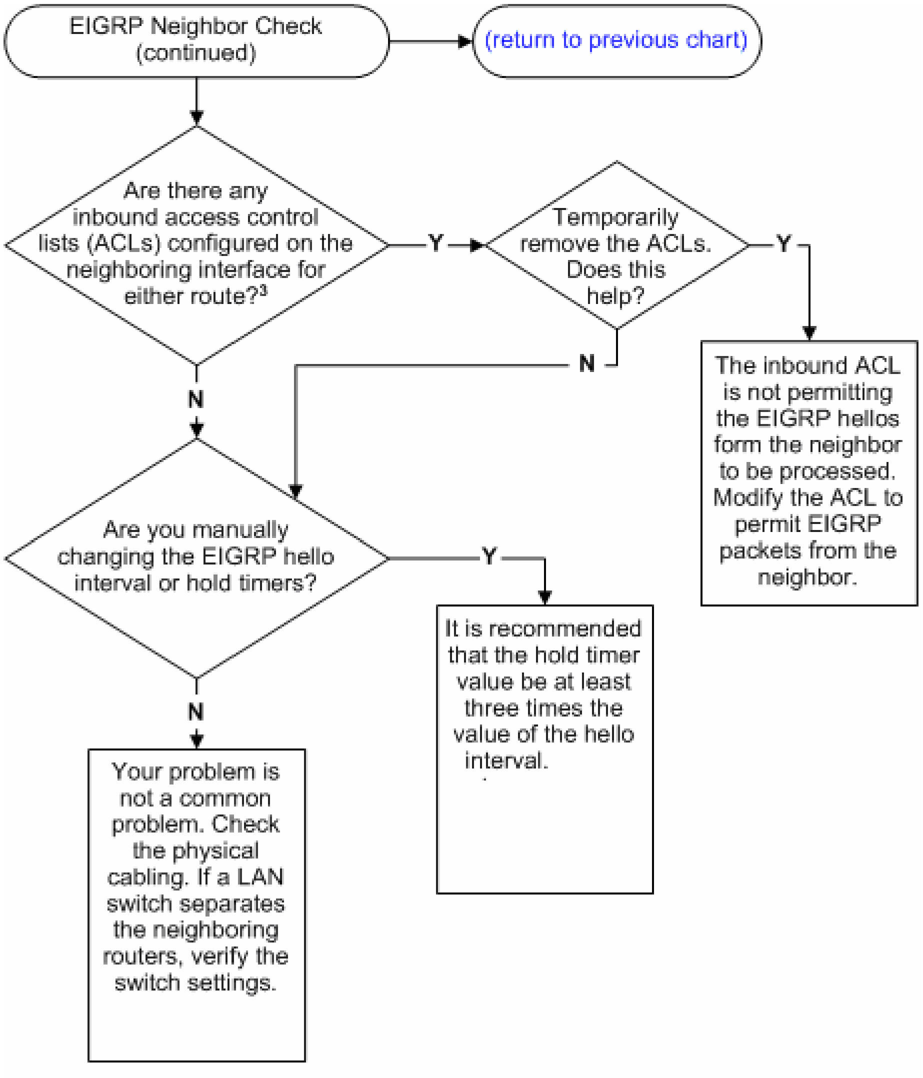

EIGRP Neighbor Check (continued)
(return to previous chart)
Are there any inbound access control lists (ACLs) configured on the neighboring interface for either route?3
Y
Temporarily remove the ACLs. Does this help?
Y
The inbound ACL is not permitting the EIGRP hellos form the neighbor to be processed. Modify the ACL to permit EIGRP packets from the neighbor.
N
N
Are you manually changing the EIGRP hello interval or hold timers?
Y
It is recommended that the hold timer value be at least three times the value of the hello interval.
N
Your problem is not a common problem. Check the physical cabling. If a LAN switch separates the neighboring routers, verify the switch settings.

Figure 5.31 - Redistribution Check Flowchart [10]

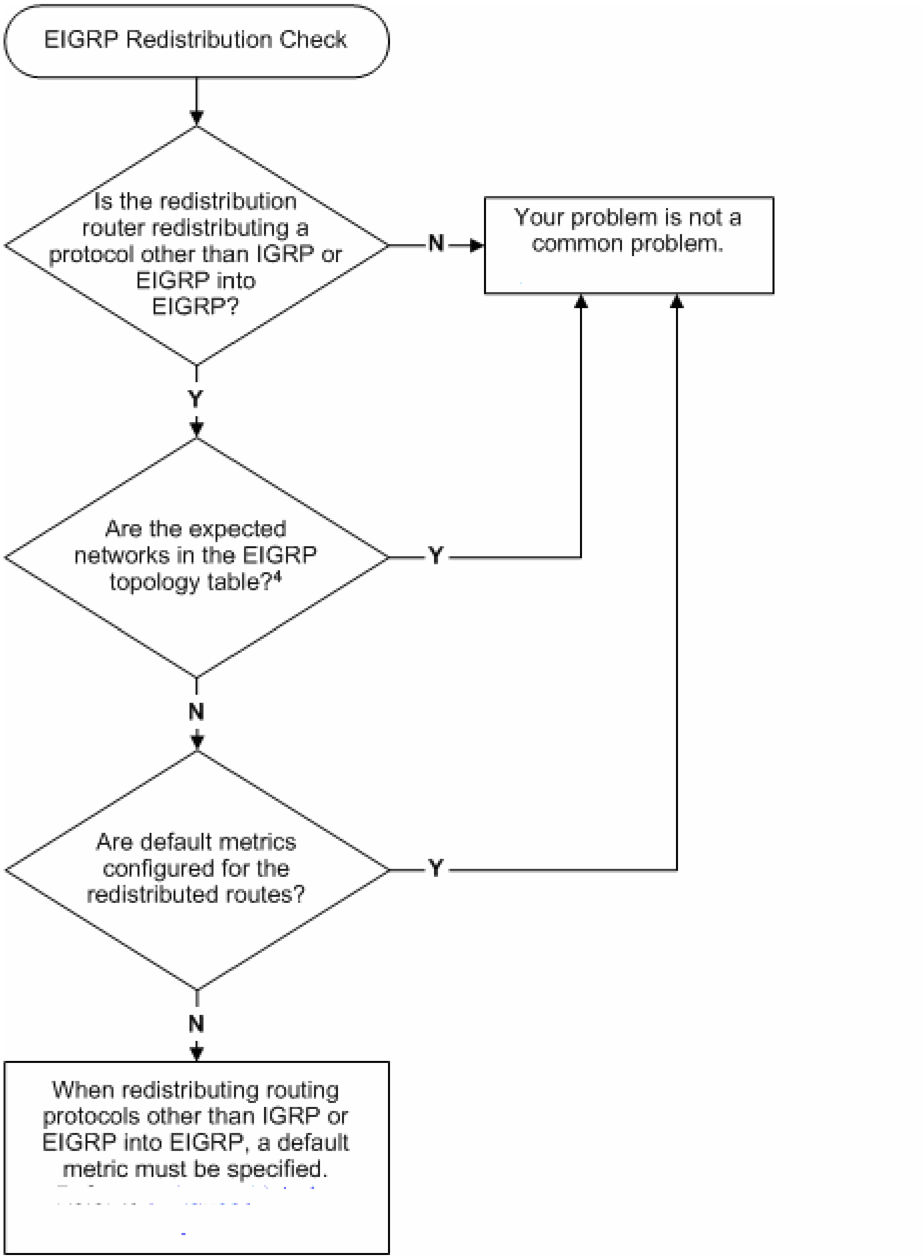

EIGRP Redistribution Check
Is the redistribution router redistributing a protocol other than IGRP or EIGRP into EIGRP?
N
Your problem is not a common problem.
Y
Are the expected networks in the EIGRP topology table?4
Y
N
Are default metrics configured for the redistributed routes?
Y
N
When redistributing routing protocols other than IGRP or EIGRP into EIGRP, a default metric must be specified.

Figure 5.32(a) - EIGRP Route Check Flowchart [10]

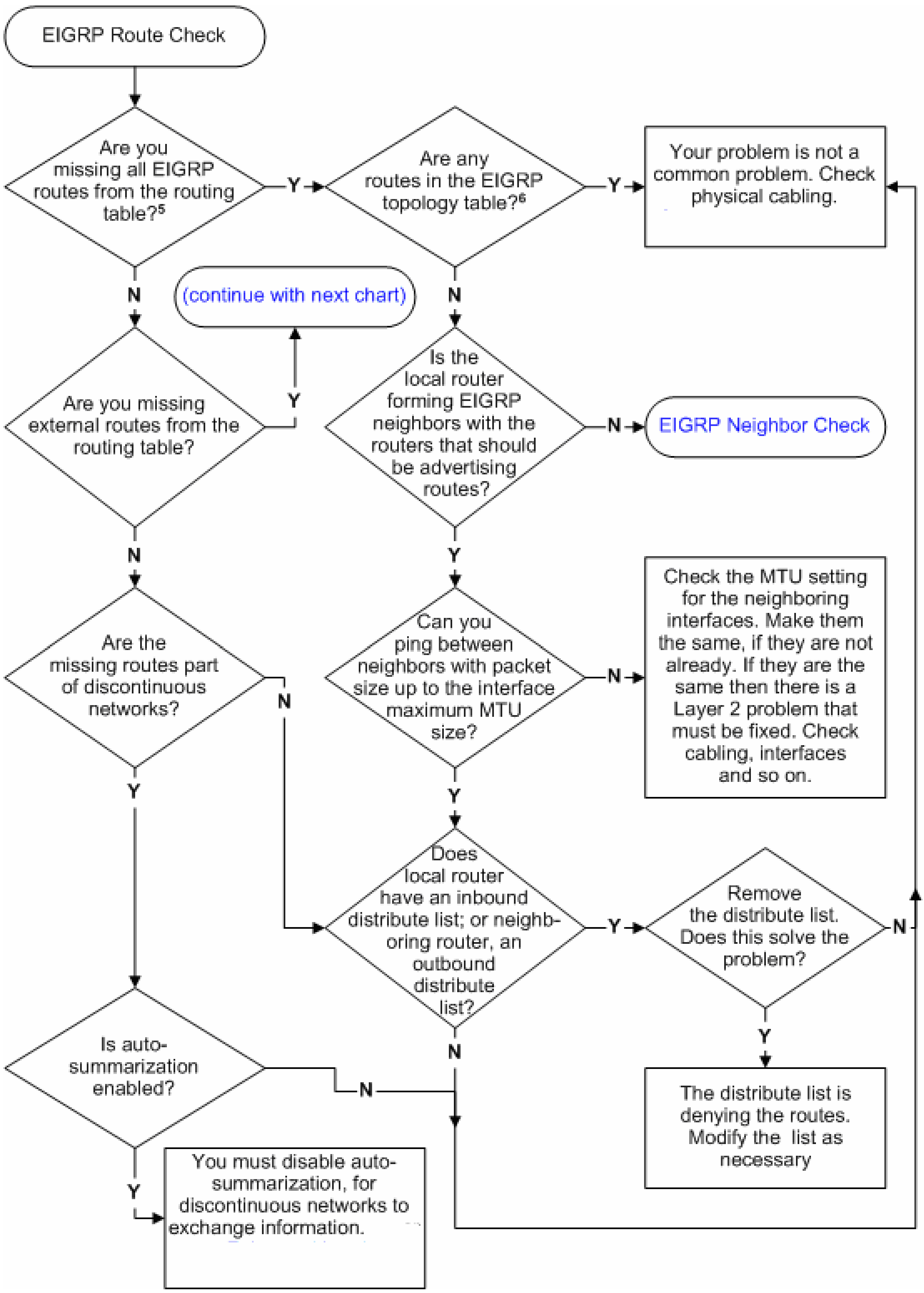
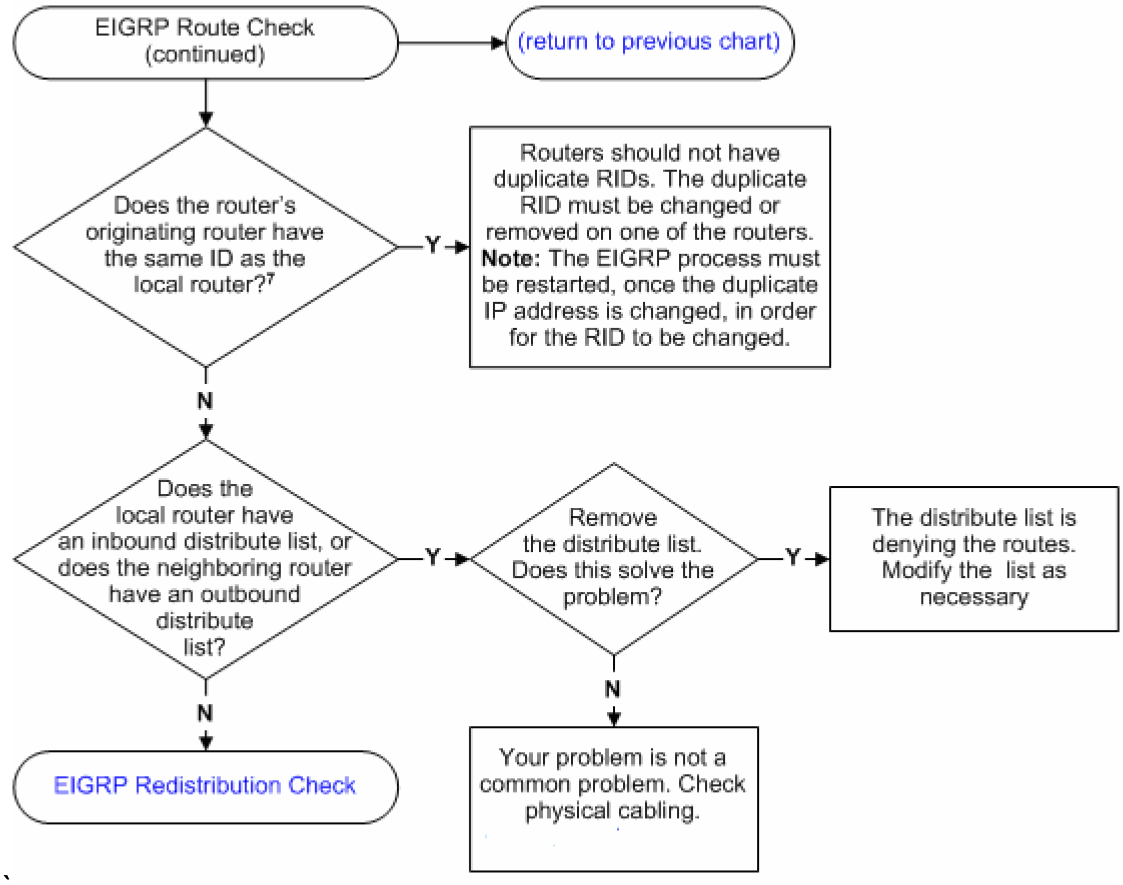

EIGRP Route Check
Are you missing all EIGRP routes from the routing table?5
Y
Are any routes in the EIGRP topology table?6
Y
Your problem is not a common problem. Check physical cabling.
N
(continue with next chart)
N
Are you missing external routes from the routing table?
Y
Is the local router forming EIGRP neighbors with the routers that should be advertising routes?
N
EIGRP Neighbor Check
N
Y
Are the missing routes part of discontinuous networks?
N
Can you ping between neighbors with packet size up to the interface maximum MTU size?
N
Check the MTU setting for the neighboring interfaces. Make them the same, if they are not already. If they are the same then there is a Layer 2 problem that must be fixed. Check cabling, interfaces and so on.
Y
Y
Does local router have an inbound distribute list; or neighboring router, an outbound distribute list?
Y
Remove the distribute list. Does this solve the problem?
N
Y
N
Is auto-summarization enabled?
N
The distribute list is denying the routes. Modify the list as necessary
Y
You must disable auto-summarization, for discontinuous networks to exchange information.

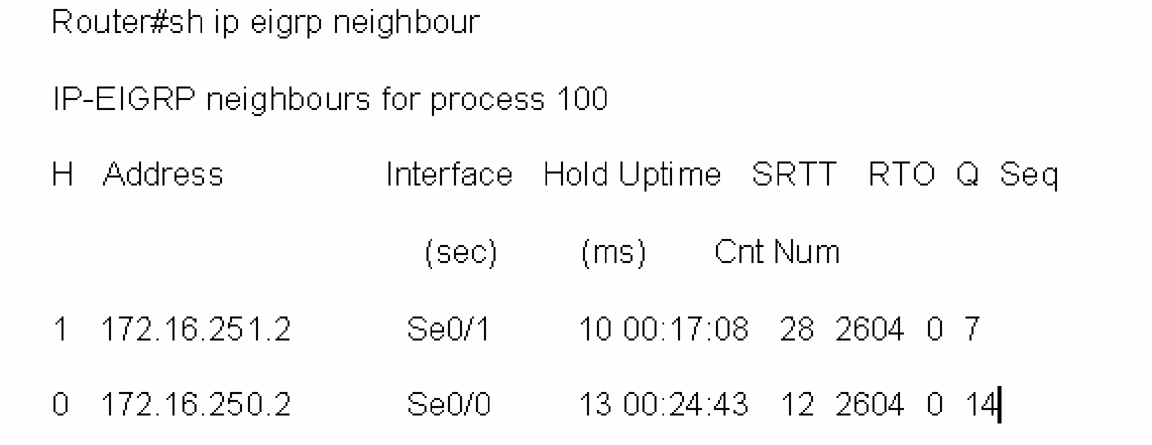
Figure 5.32(b) - EIGRP Route Check Flowchart Continued


EIGRP Route Check (continued)
(return to previous chart)
Does the router's originating router have the same ID as the local router?[7]
Y
Routers should not have duplicate RIDs. The duplicate RID must be changed or removed on one of the routers. Note: The EIGRP process must be restarted, once the duplicate IP address is changed, in order for the RID to be changed.
N
Does the local router have an inbound distribute list, or does the neighboring router have an outbound distribute list?
Y
Remove the distribute list. Does this solve the problem?
Y
The distribute list is denying the routes. Modify the list as necessary
N
Your problem is not a common problem. Check physical cabling.
N
EIGRP Redistribution Check

5.20.1 Troubleshooting Neighbour Relationships

Building and maintaining is one of the key aspects of EIGRP. The protocol can not function properly if it not able to build and make use of neighbour relationships. The operation of the neighbour relationship of an EIGRP router can be verified by using the **show ip eigrp neighbour** command. The command displays the neighbour Table of the router. Figure 5.33 shows example of usage of the command to view the neighbour Table.

Figure 5.33 – EIGRP neighbour Table [10]



```
Router#sh ip eigrp neighbour

IP-EIGRP neighbours for process 100

H   Address              Interface   Hold Uptime   SRTT   RTO  Q  Seq

                            (sec)        (ms)       Cnt Num

1   172.16.251.2          Se0/1        10 00:17:08   28  2604  0  7

0   172.16.250.2          Se0/0        13 00:24:43   12  2604  0  14
```

The first step is to verify that the router has recognized all directly connected routers as neighbours and formed relationship with them. If there are adjacent directly connected routers not showing on the neighbour Table, there may be a problem with the physical connection between the routers. [11, 15]

Due to network congestion if neighbour router is not able to send hello packets within 15 seconds it will be declared as unreachable. Although increasing the hello-interval/hold-time will solve this issue, it is not a proper solution. In such cases the network should be thoroughly analyzed to find problems causing the network congestion.

The uptime for each router shown in the routing Table should reflect the duration that the routers have been up. A low uptime indicates that the neighbour relationship was lost and has been re-established. This is not a problem if it occurs rarely. If this problem persists, then it means that the router is having problems maintaining relationship with its neighbours.

The QCnt which shows the number of packets waiting to be sent should constantly 0. This may change during period of high activity but should not be more then 0 during sTable network operations. Having a queue count greater then 0 can also mean that a neighbour has not responded to unicast packets sent to it. This could be because of a route getting stuck in active mode. [10]

In summary, if a problem is found in the neighbour relationship, the following should be done:

1. Physical connection should be checked and verified
2. Ensure connectivity between routers and hubs.
3. Ensure that configuration commands or filters are not blocking EIGRP packets.
4. Verify router configurations by checking IP addresses, masks, EIGRP AS numbers, and the network numbers defined under EIGRP.
5. Increase the hello interval/hold-time on congested networks. [10, 15]

The command to clear and re-establish neighbour relationships is:

clear ip eigrp neighbours [ip address | interface]

Table 5.5 shows common messages that are related to neighbour relationships.

Table 5.5 – Common Neighbour Relationship IOS messages [10, 11, 15, 23]

Log Message	Meaning
NEW ADJACENCY	Indicates that a new neighbour has been established.
PEER RESTARTED	Indicates that the other neighbour initiates the reset of the neighbour relationship. The router getting the message is not the one resetting the neighbour.
HOLD TIME EXPIRED	Indicates that the router has not heard any EIGRP packets from the neighbour within the hold-time limit.
RETRY LIMIT EXCEEDED	Indicates that EIGRP did not receive the acknowledgement from the neighbour for EIGRP reliable packets and that EIGRP already has tried to retransmit the reliable packet 16 times without any success.
ROUTE FILTER CHANGED	Indicates that the EIGRP neighbour is resetting because there is a change in the route filter (`distribute-list` command under router EIGRP).
INTERFACE DELAY CHANGED	Indicates that the EIGRP neighbour is resetting because there is a manual configuration change in the delay parameter on the interface.
INTERFACE	Indicates that the EIGRP neighbour is resetting because there is

BANDWIDTH CHANGED	a manual configuration change in the interface bandwidth on the interface.
STUCK IN ACTIVE	Indicates that the EIGRP neighbour is resetting because EIGRP is stuck in active state. The neighbour getting reset is the result of stuck in active.

5.20.2 Debug Commands

The following is a list of debug commands that can be used on the router to check the operation of EIGRP.

- **debug eigrp fsm** (Shows DUAL calculation taking place)
- **debug eigrp neighbours** (for neighbour-relationship activity)
- **debug eigrp packet** (shows all EIGRP packets)
- **debug eigrp transmit** (shows all transmissions)

Most of the debug command has optional criteria's that can be set. For example the type or types of packet that is to be displayed by the debug packet command can be specified. Using specific command would allow troubleshooting process easier and will also conserve router resources.

Debug commands are very intensive and only be used for the duration they are required for. Debug command should not be used during normal network usage. All debug command currently running on a router can be turned off using the **Undebug all** command. Individual debugs can be turned off by using the no form of the command that was used to turn it on.

5.20.3 EIGRP Show commands

Some of the EIGRP show commands that can be used to check the operation of the protocol are listed below:

- **Show ip eigrp interfaces** [address] [as-number] [details]
- **Show ip eigrp neighbours** [address] [details]
- **Show ip eigrp topology** [as-number] [active] [pending] [zero-successor] [all-links]
- **Show ip eigrp traffic**

5.20.4 Common EIGRP Error Messages

The most common EIGRP errors and a brief description are given below:

- **DUAL-3-SIA**— this message denotes that some of the routes were stuck in active mode during route re-computation. This will be explained in details later as this is one of the major issues affecting large EIGRP networks

- **Neighbour not on common subnet** — this message indicates that the router has received a hello packet from a neighbour that is not on the same subnet as the local router. This generally means that there must be an error in configuration of IP address and subnet mask on either the local router or the neighbour.
- **DUAL-3-BADCOUNT**—Bad count means that EIGRP believes that it knows of more routes for a given network than actually exist. It's typically (not always) seen in conjunction with DUAL-3-SIAs, but it is not believed to cause any problems by it.
- **Unequal, <route>, dndb=<metric>, query=<metric>**—This message is used for information only. It indicates that the metric the router had at the time of the query does not match the metric that it had when it received the reply. This can well be because of change in the network topology and seldom creates a problem.
- **DUAL-3-INTERNAL: IP-EIGRP Internal Error** — This message indicates that there is an EIGRP internal error. However, the router is coded to fully recover from this internal error. The EIGRP internal error is caused by software problem and should not affect the operation of the router. Experts are needed to check the logs and find the errors. Router software may need to be upgraded to remove the internal bug.

- **IP-EIGRP: Callback: callbackup_routes** — this message indicates that at some point, EIGRP attempted to install routes to the destinations and failed, because of the existence of a route with a better administrative distance. When this occurs, EIGRP registers its route as a backup route. When the better route disappears from the routing Table, EIGRP is called back through callbackup_routes so that it can attempt to reinstall the routes that it is holding in the topology Table.
- **Error EIGRP: DDB not configured on interface—** If a routers interface is not configured for EIGRP but receives EIGRP hello packets, and then this error message is displayed.
- **Poison squashed—** The router turns a topology Table entry as a poison in reply to an update. While the router is building the packet that contains the poison reverse, the router realizes that it does not need to send it because of further updates from the neighbour. In such cases the message is shown.[11]

5.21 EIGRP Stuck in Active Issues

After DUAL performs its calculation successor routes for all destinations are stored in the routing Table. Routes that have a valid successor are said to be in a “passive” state. If, for some reason, a router loses route to a destination through its successor and does not have a feasible successor for that destination, then the route transitions to an “active” state. In the active state, a router sends queries out to its neighbours requesting a path to the lost destination.

When an EIGRP neighbour receives a query for a route, it behaves as follows:

- If the EIGRP topology Table does not currently contain an entry for the route, then the router immediately replies to the query with an unreachable message, stating that there is no path for this route through this neighbour.
- If the EIGRP topology Table lists the querying router as the successor for this route and a feasible successor exists, then the feasible successor is installed and the router immediately replies to the query.
- If the EIGRP topology Table lists the querying router as the successor for this route and a feasible successor does not exist, then the router queries all of its EIGRP neighbours except those sent out the same interface as its former successor. The router will not reply to the querying router until it has received a reply to all queries that it originated for this route.
- If the query was received from a neighbour that is not the successor for this destination, then the router replies with its successor information.

As explained earlier when a router sends out a query, it has to wait for each of the queries to be answered prior to starting DUAL calculations to install a new route. In large networks this can lead to problems as some neighbours who do not have a feasible successor to the destination will enquire their neighbours and so on. [1, 11, 15, 17]

When the `SIA` error message occurs, it indicates that the EIGRP routing protocol failed to converge for the specified route. Routes can get stuck in active mode due to multiple reasons which will be discussed shortly. The routing to other destinations is not affected while the EIGRP process is in active state for the specified route. When the SIA timer (3 minutes) for the neighbour that did not reply expires, the neighbour is removed from the topology. As a result, all routes through the neighbour are also removed. This cause DUAL to start computation for the new routes that have lost their routes to destinations. This means that the forwarding Table can be affected by an SIA, and those packets can be dropped while the network is converging. Usually, an active route gets stuck for one of the following reasons:

- Broken links
- Network Congestion
- Low router resources, such as low memory or high CPU on the router
- Routing loops
- Primary address mismatch
- Long query range
- Excessive redundancy [1, 11]

5.21.1 Resolving SIA Issue

Although there are many reasons why a route can get stuck in Active mode, there is only one approach that needs to be taken in order to rectify the problem. The first step in the process is to identify the neighbour that did not reply to the query. This can be hard to do because no error message will be provided while the route is in active mode. Error message will be shown by EIGRP only once the neighbour has failed to reply to the query within an allocated time. However, the **show ip eigrp topology active** command can be used to view routes that are currently in active mode on a router. The display will show the time for which the route has been active and the number of replies that were received. The neighbours queried will be listed. A lowercase r next the neighbour indicates that the router is waiting for a reply from the neighbour. A capital R next to the neighbour indicates a reply from this neighbour has been received. List of neighbours that have not replied to the query can also be seen here. This can be used to determine the neighbour that has not replied to the query. Some of the reasons for which a route can get stuck in active mode are outlined in the following sections. The possible reasons for which the SIA problem occurs and their solution are given below. [11, 17]

5.21.1.1 Broken Link

If the link between router sending the query and the neighbour receiving the query goes down after the query has been sent but before it has been replied to, it can cause a SIA issue. Although this will rarely happen as the failure of the link in most cases will be detected before the SIA timer expires. This is however a possibility in the event that the link goes off just before the SIA times expires and the neighbour can send a reply to the query.

This problem is more related to loosing a link the problem with the query process. Troubleshooting steps should be followed to bring the link up with the neighbour. [11, 17]

5.21.1.2 Network Congestion

Due to severe network congestion during peak network usage, the time taken by routers to reply to queries may be significantly increased causing the SIA timer to time out.

This issue needs to be dealt with by bringing in a solution to the congestion problem. However the amount of Bandwidth available to EIGRP for transmission of messages can be increased using the **ip eigrp bandwidth-percentage** command. Although this may provide a temporary solution it should not be used as a permanent fix to the issue. [11, 17]

5.21.1.3 Low Router Resources

A lack of system resources such as CPU, memory, or buffers can also prevent a router from replying to queries or from processing packets of any type. EIGRP requires a lot of memory to run DUAL and maintain neighbour relationships. If the network is very congested and busy, the neighbour may be occupied with processing packets and may not have enough resources available to reply to the query. This can cause SIA timer to expire as well.

If this problem is persistent it would mean that the resources of the routers on the network are not sufficient to deal with the utilization of the network. The recourses of the routers need to be increased proportionally to the size of the network. [11, 17]

5.21.1.4 Routing loops

Routing loops can also cause SIA errors. This will be a very rare case as EIGRP is not prone to routing loop problems. However, if a routing loop is present within the network and the queried router is part of the routing loop, the route being queried will get stuck in active mode.

The solution of the problem again lies in finding a solution to the looping problem using DUAL.

5.21.1.5 Mismatched primary and secondary addresses

If two neighbours have not been configured with IP address from the same subnet, query from one router will not be answered by the other as they cannot form a neighbour adjacency. In newer versions of the Cisco IOS this problem is detected and separate appropriate messages are given to the administrator. SIA problems due to this error are very rare but do take place in networks using routers with old Cisco IOS. [39]

5.21.1.6 Long Query Range

Range of queries, especially in some Hub and spoke designs are very long as the query traverses each router in the network to reach the end router before getting replied to.

There are configuration settings that can be used to limit the range of a query which have already been discussed in the section related to query range and processing. Possible solutions to this problem have also been outlined in the same section.

5.21.1.7 SIA Active timer

The SIA active timer is used by EIGRP to calculate the time that a neighbour takes to reply to a query. This timer has a default value of 3 minutes which causes all routes whose queries have not been answered with in the time to get stuck in active. DUAL computation also takes place, as the neighbour that failed to reply to the query is also removed from the topology Table along with all routes through the neighbour.

The default 3 minutes setting for time out can be changed using the command **timers active-time *minutes.*** Although this should be used in cases where the network is so large that all queries can not be replied to within 3 minutes, it should not be used as a quick solution to the problem The changing of the default should be done after careful consideration, as it will increase the network convergence time. For the change to be effective, the active timer must be modified on every router in the path of the query. [[11, 17]

The best and the easiest method for controlling and limiting the query range are through the use of router summarization.

5.22 Security

Almost all routing protocols provide some type of security in the form of authentication of the messages that they receive from other routers. Authentication is required in routing protocols so that routers can verify that updates being received are being sent from legitimate network routers. If some outsider is able to gain access to the link between routers, it is possible to read and send updates on the links. This can lead to serious issues and the hacker may learn of the internal network structure which can then be used to exploit vulnerabilities of the network. Authentication allows routers to verify the received updates and is some cases protect updates from being accessed and read by unauthorized personnel. There are two types of authentication that are commonly supported by routing protocols. They are:

- Plaintext password authentication
- MD5 Digest Authentication

Plaintext password authentication

Just as the name sounds, plain text passwords are used in this form of authentication. A password is sent embedded within packets in plain text format. The format of the password is however specific to the protocol that is being used. This type of authentication is not very useful because using a sniffer software can be used to read packets, in which case the password can be also be read. Spoofed packets can be sent using the learnt password embedded in them which would then be regarded by receiving routers as authentic. This however offers protection against situations when packets accidentally that leak into the network. If an update packet not belonging to the network gets advertised, the routers can recognize that the packet does not belong to the network because the packet will not correct passwords required for authentication.

MD5 Digest Authentication

This is the other form of authentication that is supported by routing protocols. This technique is very popular and is used in EIGRP and OSPF. MD5 digest works by creating a 16-byte hash of routing message and combines them with a secret key or password that is configured by administrators on the routers. The 16-byte value which is hashed is specific to the message that it is embedded into. Only the hashed packets are sent by routers using the secret password as a key to perform the hashing. Even if a packet is spoofed or altered in any way the 16 byte digest becomes invalid. This allows routers to recognize packets that have been changed or not been sent by legitimate sources. This technique also stops some one from reading the packets using a packet sniffer as packets cannot be decoded and reconstructed without the secret password. The secret key is only stored in the routers and are never sent over the link. It is not possible to find out the secret key without having authorized and unrestricted access of the router.

EIGRP routers provide support for MD5 authentication and use it successfully to authenticate packets sent to them. The Table 5.6 shows the steps involved in configuring authentication on EIGRP routers.

Table 5.6 – EIGRP Authentication Configuration Steps.

	Command	Purpose
Step 1	Router(config)# **interface** *type number*	Configure an interface type and enter interface configuration mode.
Step 2	Router(config-if)# **ip authentication mode eigrp** *autonomous-system* **md5**	Enable MD5 authentication in EIGRP packets.
Step 3	Router(config-if)# **ip authentication**	Enable authentication of EIGRP

	key-chain eigrp *autonomous-system key-chain*	packets.
Step 4	Router(config-if)# **exit** Router(config)#	Exit to global configuration mode.
Step 5	Router(config)# **key chain** *name-of-chain*	Identify a key chain. (Match the name configured in Step 1.)
Step 6	Router(config-keychain)# **key** *number*	In key chain configuration mode, identify the key number.
Step 7	Router(config-keychain)# **key-string** *text*	In key chain key configuration mode, identify the key string.
Step 8	Router(config-keychain)# **accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}	Optionally specify the time period during which the key can be received.
Step 9	Router(config-keychain)# **send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}	Optionally specify the time period during which the key can be sent.

5.23 Basic EIGRP Configuration

5.23.1 Enabling EIGRP

To enable EIGRP on a router the steps shown in Table 5.7 can be followed. These steps should be performed after the interfaces of the router have been configured with correct IP addresses.

Table 5.7 – EIGRP Enabling Steps

	Command	Purpose
Step 1	Router(config)# **router eigrp** *autonomous-system*	Enable an EIGRP routing process in global configuration mode.
Step 2	Router(config-router)# **network**	Associate networks with an

	network-number	EIGRP routing process in router configuration mode.

EIGRP will only send updates on the interfaces that are specified by the network command to be under the EIGRP AS.

5.23.2 Logging EIGRP Neighbour Adjacency Changes

As already explained earlier, proper EIGRP neighbour relationships are vital to the stability of the network. The changes to neighbour relationship can be logged in EIGRP for later review. The command to turn on logging of neighbour adjacencies is given in Table 5.8.

Table 5.8 – Enabling Neighbour Adjacency logging

Command	Purpose
Router(config)# **eigrp log-neighbour-changes**	Enable logging of EIGRP neighbour adjacency changes.

5.24 EIGRP Theoretical Summary

EIGRP is one of the most feature-rich and robust routing protocols to ever be developed by Cisco. Its unique combination of features uses the best attributes of distance vector protocols and the best attributes of link-state protocols. The result is a hybrid routing protocol with great many features.

EIGRP is remarkably easy to configure and deploy. It is very efficient and secure in operation. It is regarded as a hybrid protocol because of its ease of configuration but provides capabilities similar to that of OSPF and other link state protocols. However, for large networks EIGRP can not be used as plug and play and must be configured according to specific requirements. EIGRP makes use of DUAL, to select best loops free paths to destination. The selection of routes is done using a composite metric which can be configured to give maximum performance in complex networks. EIGRP also provides support for variable-length subnets with in the network and route summarization to make addressing scheme and routing Tables more efficient. In addition it also has built in modules that provide support for Novell IPX and AppleTalk protocols. EIGRP is a very robust protocols and scales well to medium and large networks. The addable modules will allow for an easy extension of EIGRP to provide support for IPv6. Due to the protocols robustness and scalability features it can also be used as an EGP.

These benefits provided by EIGRP come at the price of higher memory requirements and processing power. DUAL is complex and can be very CPU-intensive, especially during periods of network instability when CPU resources are already low. EIGRP is a Cisco proprietary protocol which also leads to vendor compatibility problems. EIGRP networks need to be built using Cisco equipment which can be more expensive then other brands available in the market. [1, 15, 22, 65, 73]

5.25 Routing Protocol Summary Table

Table 5.9 – Routing Protocol Comparison Table [1, 15, 22, 65, 73]

Protocol	RIP	OSPF	IGRP	EIGRP
Type	distance-vector	link-state	distance-vector	distance-vector
Convergence Time	slow	fast	slow	fast
VLSM	No	yes	no	yes
Bandwidth Consumption	high	low	high	low
Resource Consumption	Low	high	low	low
Multi-path Support	No	yes	yes	yes
Scales Well	No	yes	yes	yes
Proprietary	No	no	yes	yes
Routers Non-IP Protocols	No	no	no	yes

5.26 Chapter Summary

This chapter discussed the theory related to EGIRP in details. Some aspects such as configuration, commands, redistribution, integration and troubleshooting are very broad topics. These topics have been briefly outlined and a complete discussion of these topics is beyond the scope of this project. The chapter dealt with all the theoretical research that was carried out in relation to the protocol.

The following project objectives have been achieved through this chapter:

- To provide a background to EIGRP and its evolution from IGRP.
- To provide detailed information about EIGRP along with its advanced technologies, key features and capabilities such as: fast convergence, support for variable-length subnet mask, support for partial updates, support for multiple network layer protocols, neighbours discovery/recovery, Reliable Transport Protocol (RTP,) DUAL finite-state machine, Load Balancing, topology Table, neighbours Table and routing Table.
- To discuss and produce the configuration process/ requirements for Implementation and Troubleshooting of EIGRP.

The next chapter will include details about operation analysis of EIGRP. The experiments range from simple features to complex ones and are used to analyze the protocol under different scenarios. Some of the experiments also show the capabilities and functionalities of EIGRP and outlines their configuration requirements. Analysis of the experiments and the recommendations for EIGRP deployment can also be found in the next chapter.

CHAPTER 6 – Operational Analysis of EIGRP

6.1 Overview

In the previous chapters, Routing, Routed Protocols, Routing Protocols and particularly EIGRP were theoretically reviewed. This chapter will be a continuation of the last chapter in the sense that the last chapter was based on theoretical research carried out on EIGRP and this chapter will include operational analysis of EIGRP. The main objective of this chapter is to show configuration requirements, show capabilities and features of the protocol. Each of the experiments has been carefully chosen to show a certain aspect of the protocol. Analysis and evaluation of the experiment results will also be carried out within the chapter.

6.2 Operational Analysis

The operational components of EIGRP that will be dealt with through practical experiments are given below:

- Basic EIGRP Network Configuration
- Estimated Convergence time (for a small network)
- Affect of Bandwidth availability on EIGRP operation
- Hello packet exchanges to form neighbour relationships and rediscover failed neighbours
- Periodic exchange of hello packets to maintain relationship.
- The use of update packets during changes in network topology.
- Successor Selection Process
- Feasible Successor Selection
- Equal path Load Balancing
- Unequal path load balancing
- Local Computation
- Diffusing Computation
- Query Range and Process
- Effect of K-value changes and mismatch
- Route Summarization
- EIGRP integration with IGRP network.

6.2.1 Basic EIGRP Network Configuration

Aim: To demonstrate the configuration requirements for EIGRP deployment and it ease.

Figure 6.1 – Network topology for experiment 6.2.1

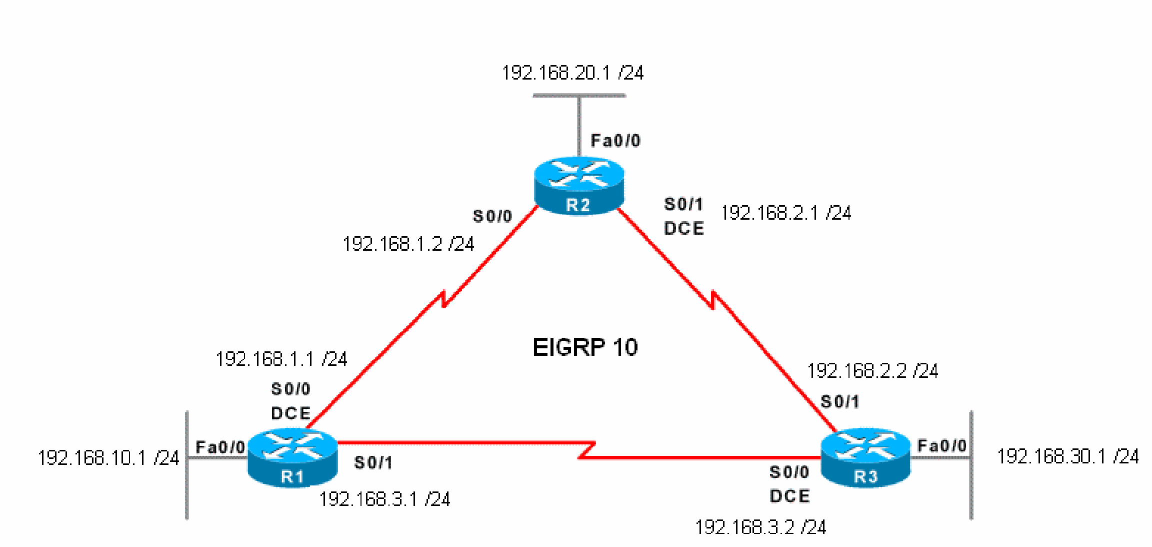


Table 6.1 – Router Configuration for Experiment 6.2.1

Configuration for Router R1

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R1
R1(config)#interface serial 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)#clockrate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/1
R1(config-if)# ip address 192.168.3.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fa 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router eigrp 10
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.3.0
R1(config-router)#network 192.168.10.0
```

Configuration for Router R2

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R2
R2(config)#interface serial 0/0
R2(config-if)# ip address 192.168.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface serial 0/1
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)#clockrate 64000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface fa 0/0
R2(config-if)# ip address 192.168.20.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router eigrp 10
R2(config-router)#network 192.168.1.0
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.20.0
```

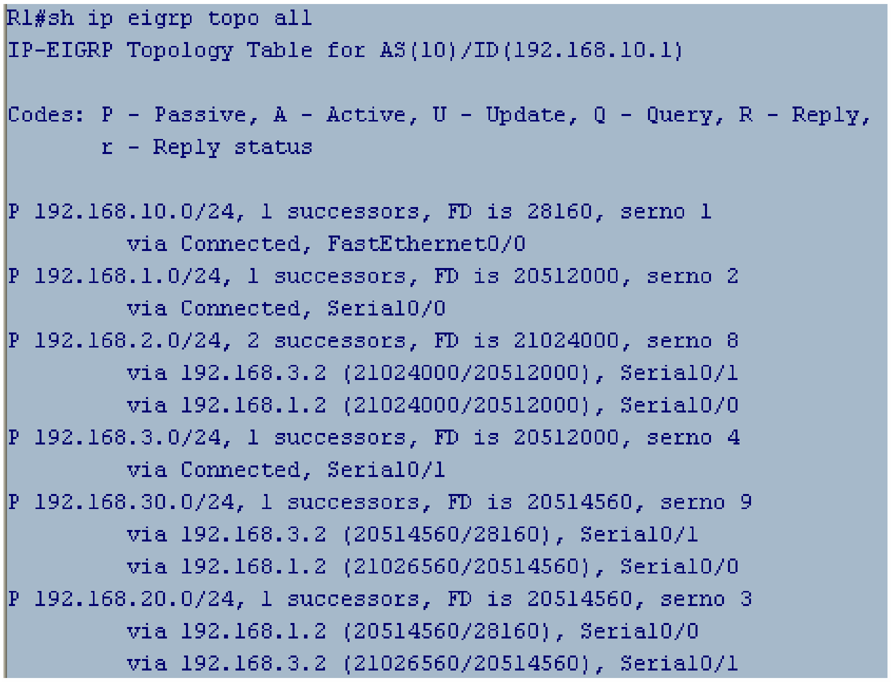
Configuration for Router R3

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R3
R3(config)#interface serial 0/0
R3(config-if)# ip address 192.168.3.2 255.255.255.0
R3(config-if)#clockrate 64000
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface serial 0/1
R3(config-if)# ip address 192.168.2.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface fa 0/0
R3(config-if)# ip address 192.168.30.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router eigrp 10
R3(config-router)#network 192.168.2.0
R3(config-router)#network 192.168.3.0
R3(config-router)#network 192.168.30.0
```

Description/Procedure: This experiment was designed to show the ease of configuration of an EIGRP network. The experiment involved configuration of the three routers according to Table 6.1. The topology diagram for the experiment can also be found in Figure 6.1. Once the network was configured routing

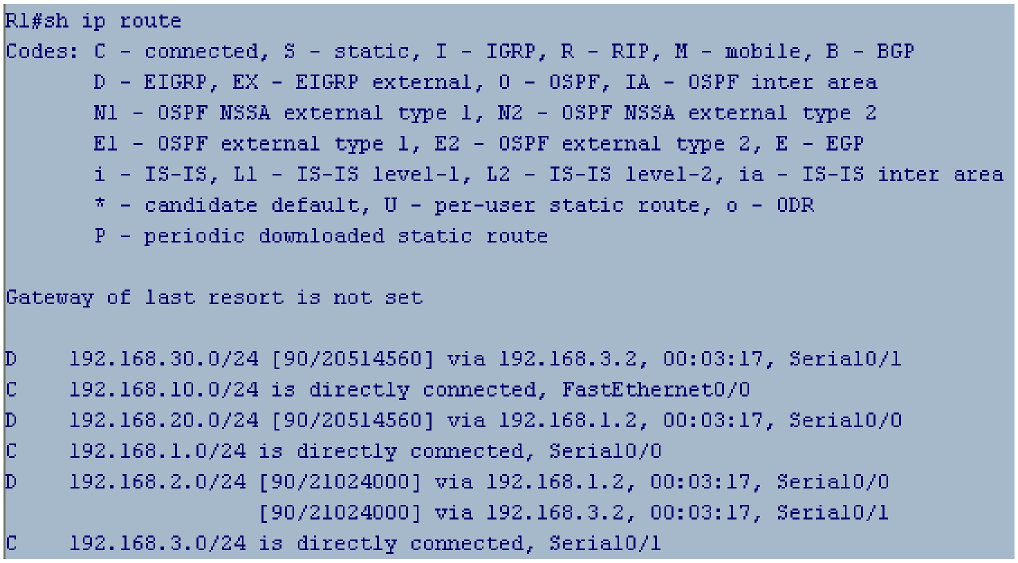
Tables, topology Tables and neighbour Tables on each router was checked to verify that the network had successfully converged using EIGRP.

Results: The following screenshot shows the topology Table of Router R1 which contains all routes learned by the router. From this it can be seen that all routes within the network had been advertised properly to Router R1.



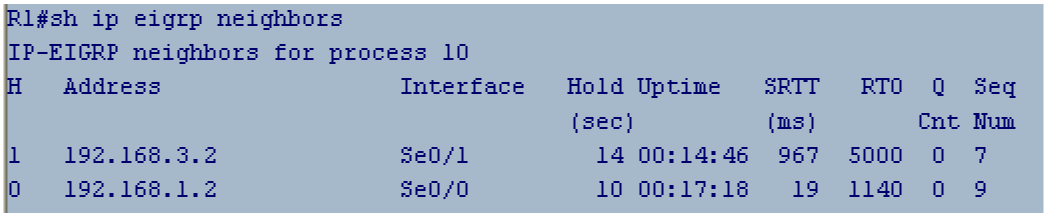
```
R1#sh ip eigrp topo all
IP-EIGRP Topology Table for AS(10)/ID(192.168.10.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.10.0/24, 1 successors, FD is 28160, serno 1
         via Connected, FastEthernet0/0
P 192.168.1.0/24, 1 successors, FD is 20512000, serno 2
         via Connected, Serial0/0
P 192.168.2.0/24, 2 successors, FD is 21024000, serno 8
         via 192.168.3.2 (21024000/20512000), Serial0/1
         via 192.168.1.2 (21024000/20512000), Serial0/0
P 192.168.3.0/24, 1 successors, FD is 20512000, serno 4
         via Connected, Serial0/1
P 192.168.30.0/24, 1 successors, FD is 20514560, serno 9
         via 192.168.3.2 (20514560/28160), Serial0/1
         via 192.168.1.2 (21026560/20514560), Serial0/0
P 192.168.20.0/24, 1 successors, FD is 20514560, serno 3
         via 192.168.1.2 (20514560/28160), Serial0/0
         via 192.168.3.2 (21026560/20514560), Serial0/1
```

The following screenshot verifies that the Router R1 has successfully performed DUAL computation to find successor routes for each destination.



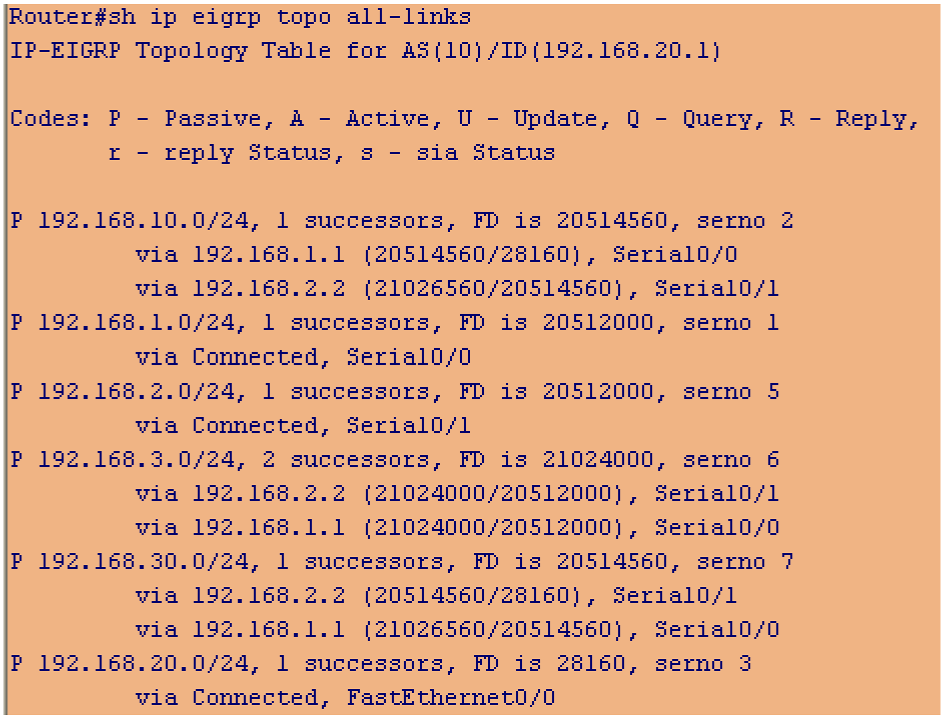
```
R1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D    192.168.30.0/24 [90/20514560] via 192.168.3.2, 00:03:17, Serial0/1
C    192.168.10.0/24 is directly connected, FastEthernet0/0
D    192.168.20.0/24 [90/20514560] via 192.168.1.2, 00:03:17, Serial0/0
C    192.168.1.0/24 is directly connected, Serial0/0
D    192.168.2.0/24 [90/21024000] via 192.168.1.2, 00:03:17, Serial0/0
                    [90/21024000] via 192.168.3.2, 00:03:17, Serial0/1
C    192.168.3.0/24 is directly connected, Serial0/1
```

The following screenshot shows that Router R1 successfully formed neighbour relationships with Router R2 and Router R3.

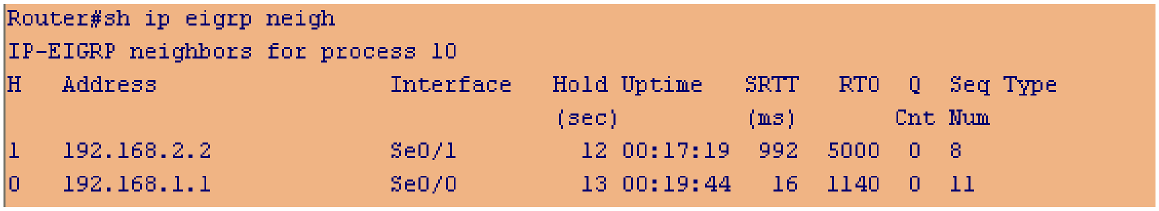


```
R1#sh ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   192.168.3.2             Se0/1             14 00:14:46  967  5000  0  7
0   192.168.1.2             Se0/0             10 00:17:18   19  1140  0  9
```

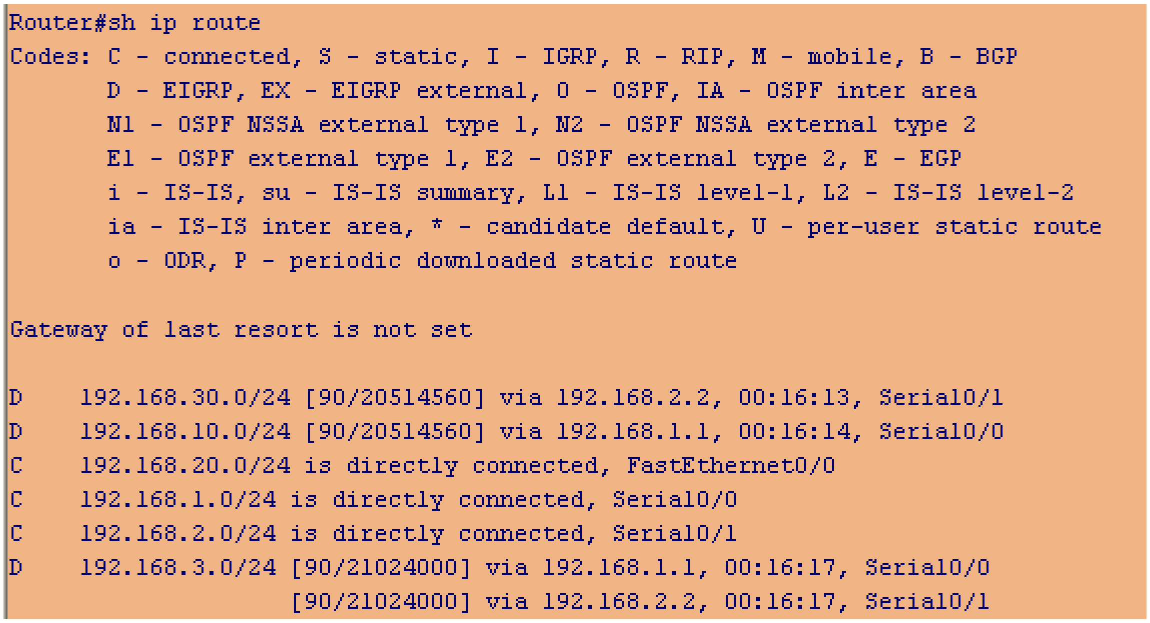
The following screenshots show the topology Table, routing Table and neighbour Table of Router R2. These Tables verify the fact that Router R2 has also learned of all routes to destinations and successfully used DUAL to calculate successor routes and formed adjacency with router R1 and R3.



```
Router#sh ip eigrp topo all-links
IP-EIGRP Topology Table for AS(10)/ID(192.168.20.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.10.0/24, 1 successors, FD is 20514560, serno 2
         via 192.168.1.1 (20514560/28160), Serial0/0
         via 192.168.2.2 (21026560/20514560), Serial0/1
P 192.168.1.0/24, 1 successors, FD is 20512000, serno 1
         via Connected, Serial0/0
P 192.168.2.0/24, 1 successors, FD is 20512000, serno 5
         via Connected, Serial0/1
P 192.168.3.0/24, 2 successors, FD is 21024000, serno 6
         via 192.168.2.2 (21024000/20512000), Serial0/1
         via 192.168.1.1 (21024000/20512000), Serial0/0
P 192.168.30.0/24, 1 successors, FD is 20514560, serno 7
         via 192.168.2.2 (20514560/28160), Serial0/1
         via 192.168.1.1 (21026560/20514560), Serial0/0
P 192.168.20.0/24, 1 successors, FD is 28160, serno 3
         via Connected, FastEthernet0/0
```

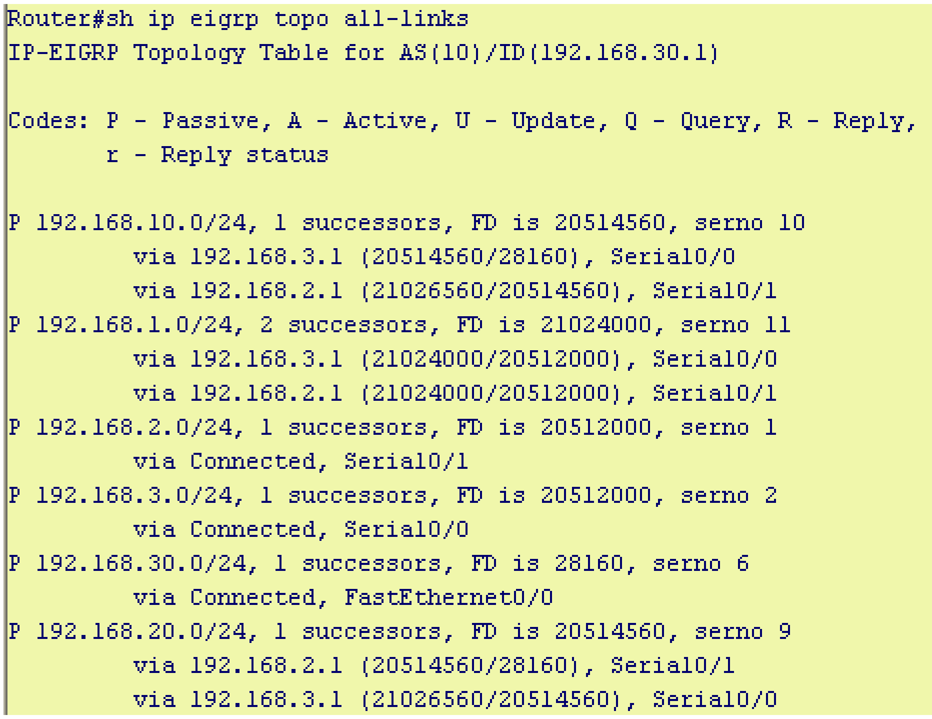


```
Router#sh ip eigrp neigh
IP-EIGRP neighbors for process 10
H   Address                 Interface     Hold Uptime   SRTT   RTO  Q  Seq Type
                                          (sec)         (ms)       Cnt Num
1   192.168.2.2             Se0/1           12 00:17:19  992  5000  0  8
0   192.168.1.1             Se0/0           13 00:19:44   16  1140  0  11
```

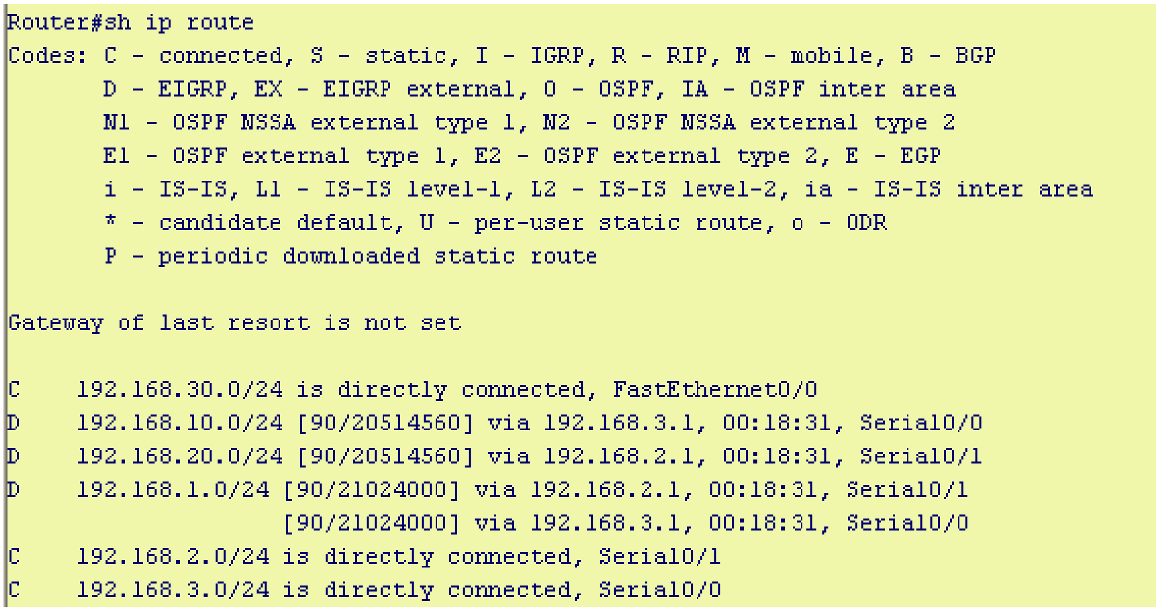


```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -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

Gateway of last resort is not set

D    192.168.30.0/24 [90/20514560] via 192.168.2.2, 00:16:13, Serial0/1
D    192.168.10.0/24 [90/20514560] via 192.168.1.1, 00:16:14, Serial0/0
C    192.168.20.0/24 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, Serial0/0
C    192.168.2.0/24 is directly connected, Serial0/1
D    192.168.3.0/24 [90/21024000] via 192.168.1.1, 00:16:17, Serial0/0
                    [90/21024000] via 192.168.2.2, 00:16:17, Serial0/1
```

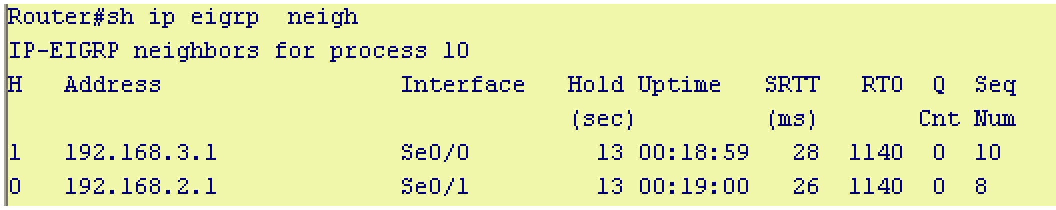
The following screenshots show the topology Table, routing Table and neighbour Table of router R3. These Tables verify the fact that Router R3 has also learned off all routes to destinations and has successfully used DUAL to calculate successor routes and formed adjacency with router R1 and R2.



```
Router#sh ip eigrp topo all-links
IP-EIGRP Topology Table for AS(10)/ID(192.168.30.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.10.0/24, 1 successors, FD is 20514560, serno 10
         via 192.168.3.1 (20514560/28160), Serial0/0
         via 192.168.2.1 (21026560/20514560), Serial0/1
P 192.168.1.0/24, 2 successors, FD is 21024000, serno 11
         via 192.168.3.1 (21024000/20512000), Serial0/0
         via 192.168.2.1 (21024000/20512000), Serial0/1
P 192.168.2.0/24, 1 successors, FD is 20512000, serno 1
         via Connected, Serial0/1
P 192.168.3.0/24, 1 successors, FD is 20512000, serno 2
         via Connected, Serial0/0
P 192.168.30.0/24, 1 successors, FD is 28160, serno 6
         via Connected, FastEthernet0/0
P 192.168.20.0/24, 1 successors, FD is 20514560, serno 9
         via 192.168.2.1 (20514560/28160), Serial0/1
         via 192.168.3.1 (21026560/20514560), Serial0/0
```



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

Gateway of last resort is not set

C    192.168.30.0/24 is directly connected, FastEthernet0/0
D    192.168.10.0/24 [90/20514560] via 192.168.3.1, 00:18:31, Serial0/0
D    192.168.20.0/24 [90/20514560] via 192.168.2.1, 00:18:31, Serial0/1
D    192.168.1.0/24 [90/21024000] via 192.168.2.1, 00:18:31, Serial0/1
                    [90/21024000] via 192.168.3.1, 00:18:31, Serial0/0
C    192.168.2.0/24 is directly connected, Serial0/1
C    192.168.3.0/24 is directly connected, Serial0/0
```



```
Router#sh ip eigrp  neigh
IP-EIGRP neighbors for process 10
H   Address                 Interface    Hold Uptime    SRTT   RTO  Q  Seq
                                         (sec)          (ms)       Cnt Num
1   192.168.3.1             Se0/0          13 00:18:59   28   1140  0  10
0   192.168.2.1             Se0/1          13 00:19:00   26   1140  0  8
```

Analysis: The screenshots taken show that the network was fully converged and all routers within the network had a full view of the entire network. This network has redundant routes which can form a routing loop but DUAL was used successfully to select successor and feasible successor routes by all routers which allowed a loop-free fully converged network. The configuration requirement of such simple networks is really small when deploying EIGRP. The network converged sharing routes between the routers with very little configuration.

Conclusion: This experiment successfully demonstrated the ease of configuration and simplicity of configuring an EIGRP network.

6.2.2 Estimate network convergence time.

Aim: To estimate the time convergence time of a small EIGRP network.

Figure 6.2 – Network topology for experiment 6.2.2

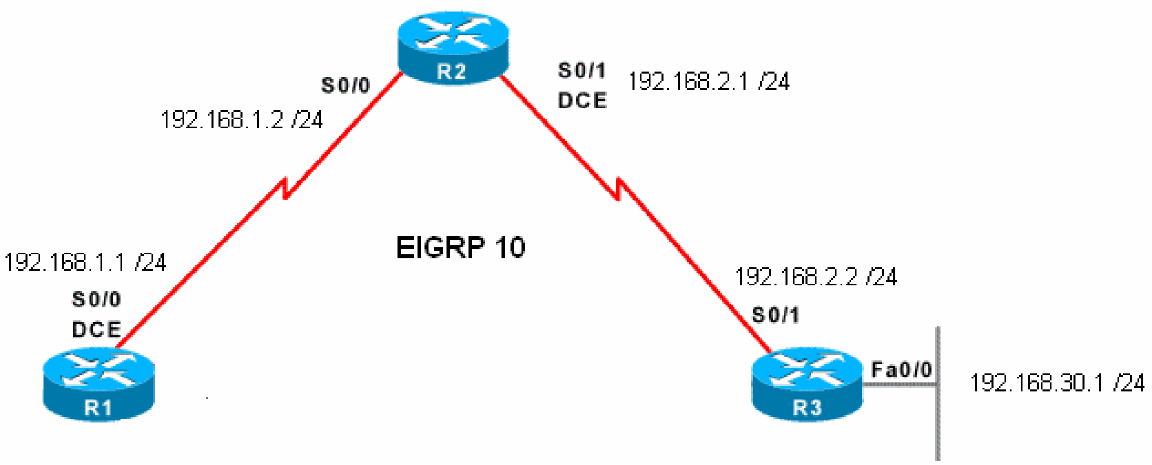


Table 6.2 – Router Configuration for Experiment 6.2.2

Configuration for Router R1

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R1
R1(config)#interface serial 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)#clockrate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router eigrp 10
R1(config-router)#network 192.168.1.0
```

Configuration for Router R2

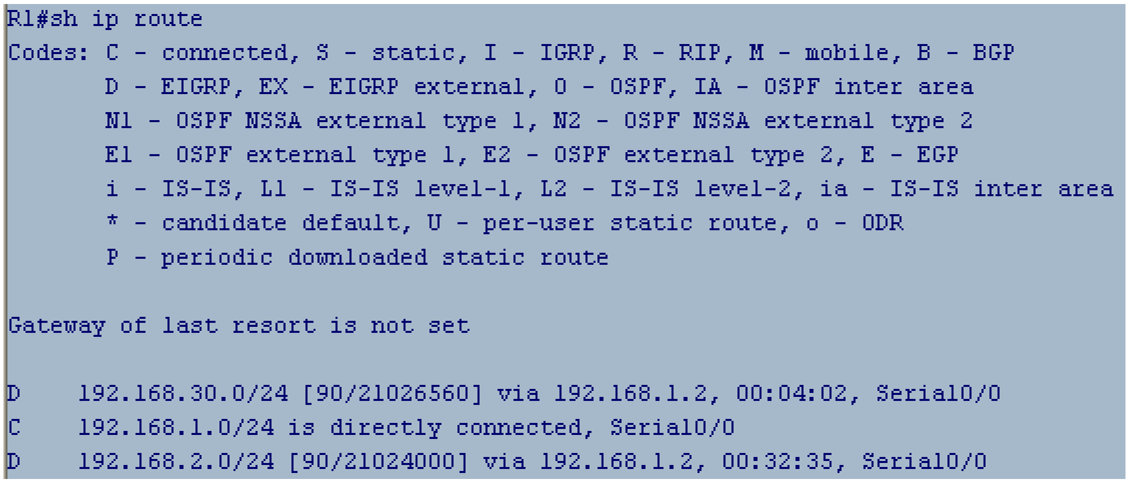
```
Router>enable
Router#conFigure terminal
Router(config)#hostname R2
R2(config)#interface serial 0/0
R2(config-if)# ip address 192.168.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface serial 0/1
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)#clockrate 64000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router eigrp 10
R2(config-router)#network 192.168.1.0
R2(config-router)#network 192.168.2.0
```

Configuration for Router R3

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R3
R3(config)#interface serial 0/1
R3(config-if)# ip address 192.168.2.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface fa 0/0
R3(config-if)# ip address 192.168.30.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router eigrp 10
R3(config-router)#network 192.168.2.0
R3(config-router)#network 192.168.30.0
```

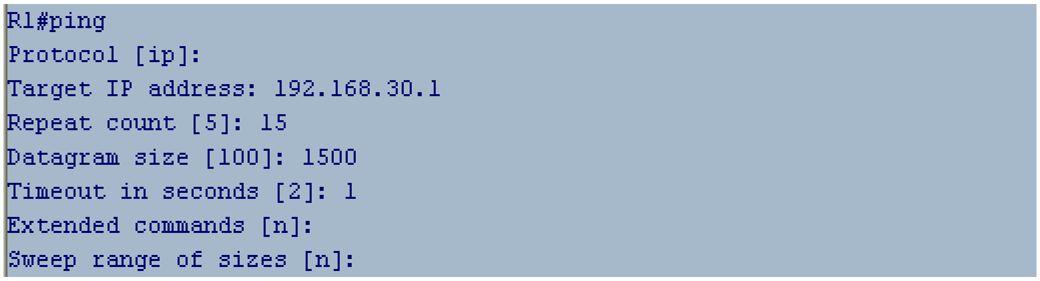
Description/Procedure: The network diagram for the experiment can be found above in Figure 6.2. The configuration of router used in the experiment can also be found above in Table 6.2. After the routers have been configured and the network has converged, average round trip time of 1500 byte ICMP ping packet to network 192.169.30.0 from Router R1 will be measured using extended ping and debugging options. After measuring the extended ping times, another extended ping to network 192.168.30.0 will be carried out. However, this time failure of Router R2 serial link will be simulated. This will be done by administratively turning the router serial interface off and then consecutively turning it back on again. This will be done very quickly so the delay in issuing of the commands does not affect the outcome of the experiment. Router R3 will be configured with EIGRP debug commands to see the reported convergence times by EIGRP. The failure of the link will cause some of the packets of the extended ping to be lost. An estimate of the time the network takes to converge will be made from the number of packets lost during the link failure and the DUAL messages confirming new link establishment.

Result: The screenshot below shows that the network is converged and router R1 knows of a valid routed to destination 192.168.30.1 through router R2.



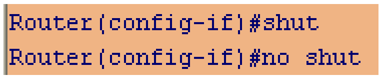
```
R1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D    192.168.30.0/24 [90/21026560] via 192.168.1.2, 00:04:02, Serial0/0
C    192.168.1.0/24 is directly connected, Serial0/0
D    192.168.2.0/24 [90/21024000] via 192.168.1.2, 00:32:35, Serial0/0
```

The following screenshot shows the configuration used for the extended ping.



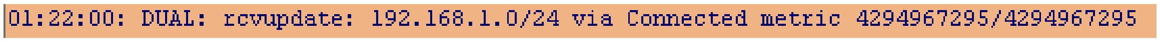
```
R1#ping
Protocol [ip]:
Target IP address: 192.168.30.1
Repeat count [5]: 15
Datagram size [100]: 1500
Timeout in seconds [2]: 1
Extended commands [n]:
Sweep range of sizes [n]:
```

The simulation of the links is done consecutively and very quickly. Both the commands were issued even before the router was able to show a message for the link failure. The following screen shows the issuing of the packets.



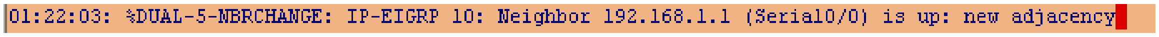
```
Router(config-if)#shut
Router(config-if)#no shut
```

The following screenshot show the time at which the DUAL process starts of Router R2 after it the link was turned back on.



```
01:22:00: DUAL: rcvupdate: 192.168.1.0/24 via Connected metric 4294967295/4294967295
```

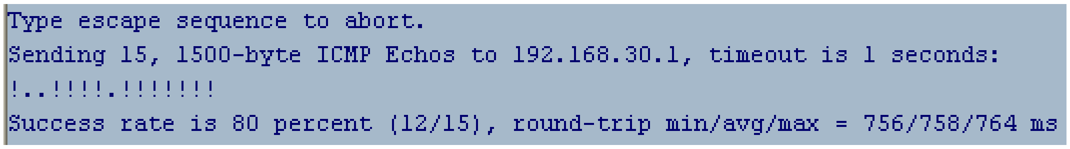
The following screenshot show the time at which the DUAL computation ends at Router R2.



```
01:22:03: %DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.1.1 (Serial0/0) is up: new adjacency
```

From the above screenshots it can be seen that the DUAL calculation lasted for about 3 seconds.

The following screenshot shows the results of the extended ping.



```
Type escape sequence to abort.
Sending 15, 1500-byte ICMP Echos to 192.168.30.1, timeout is 1 seconds:
!..!!!!.!!!!!!!
Success rate is 80 percent (12/15), round-trip min/avg/max = 756/758/764 ms
```

Analysis: From the screenshots that shows DUAL calculations it can be seen that the DUAL calculation went on for three seconds. The result of the extended ping shows that three packets were lost in transit, which also took three to be detected seconds. The network was not converged during DUAL calculations or for the period of time that Router R1 did not have a route to Router R3, thus ICMP packets were lost. As both DUAL required three seconds to complete computation and packets were lost for 3 seconds, it can be ascertained that the network was converged for three seconds. In other words the convergence time of the network used in the experiment is three (3) seconds.

Conclusion: The experiment was successfully used to find the convergence time for the network shown in Figure 6.3. It was found to be three seconds. At this point it should be noted that the three seconds estimated convergence time only applies to the network with the given configuration. Changes to the network may impact the convergence times.

6.2.3 Effect of Bandwidth Change

Aim: To show the effect of bandwidth availability to EIGRP.

Figure 6.3 – Network topology for experiment 6.2.3

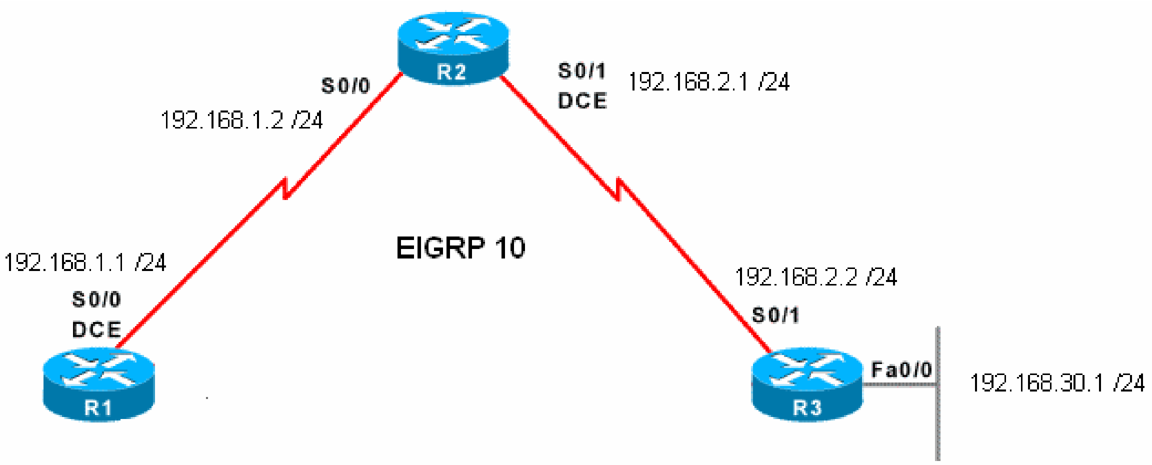


Table 6.3 – Router Configuration for Experiment 6.2.3

Configuration for Router R1

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R1
R1(config)#interface serial 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)#clockrate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router eigrp 10
R1(config-router)#network 192.168.1.0
```

Configuration for Router R2

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R2
R2(config)#interface serial 0/0
```

```
R2(config-if)# ip address 192.168.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface serial 0/1
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)#clockrate 64000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router eigrp 10
R2(config-router)#network 192.168.1.0
R2(config-router)#network 192.168.2.0
```

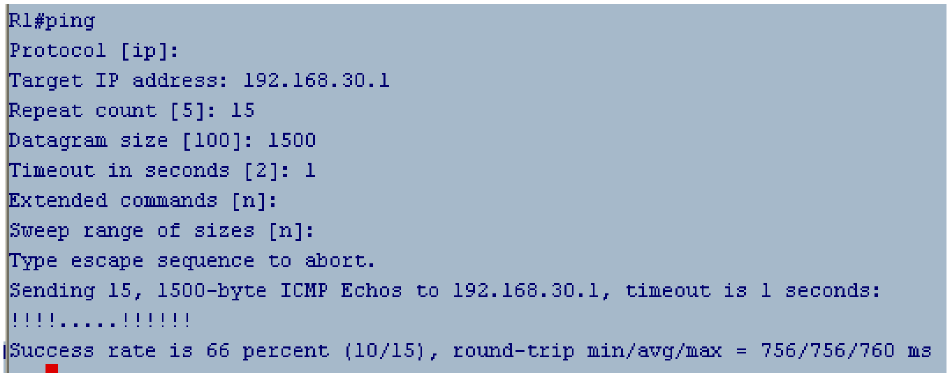
Configuration for Router R3

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R3
R3(config)#interface serial 0/1
R3(config-if)# ip address 192.168.2.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface fa 0/0
R3(config-if)# ip address 192.168.30.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router eigrp 10
R3(config-router)#network 192.168.2.0
R3(config-router)#network 192.168.30.0
```

Description/Procedure: The network topology and the configuration of the routers used for the experiment can be found in Figure 6.3 and Table 6.3. During the last experiment, the convergence time for the network had been estimate and was found to be three seconds. The configuration used for the last experiment and this experiment is the same and so the results of the experiment will be comparable. By default EIGRP is allowed to use up to 50% of the link bandwidth to exchange routing information. So, during the last experiment it was estimated at using 50% bandwidth allocation the network takes 3 seconds to converge. During this experiment the bandwidth available to EIGRP will be set at different levels. Each time the convergence time will be noted. The different percentages of bandwidth that EIGRP will be allocated are: 1%, 10%, 20%, 30%, 40%, and

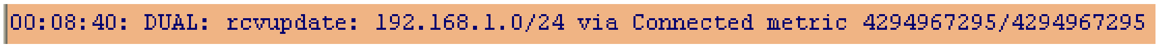
100%. Because the network is of small size it is expected that a difference in the convergence time will not be evident until the available bandwidth has been made drastically low.

Result: The following screenshot shows the result of the extended ping with EIGRP allocated only 1% of the configured link bandwidth for usage.



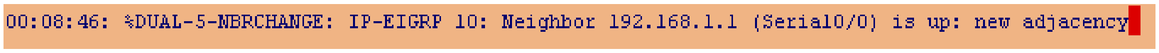
```
R1#ping
Protocol [ip]:
Target IP address: 192.168.30.1
Repeat count [5]: 15
Datagram size [100]: 1500
Timeout in seconds [2]: 1
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 15, 1500-byte ICMP Echos to 192.168.30.1, timeout is 1 seconds:
!!!!.....!!!!!!
Success rate is 66 percent (10/15), round-trip min/avg/max = 756/756/760 ms
```

The following screenshot shows the start time of DUAL calculation with EIGRP configured to use up to 1% of the configured link bandwidth.



```
00:08:40: DUAL: rcvupdate: 192.168.1.0/24 via Connected metric 4294967295/4294967295
```

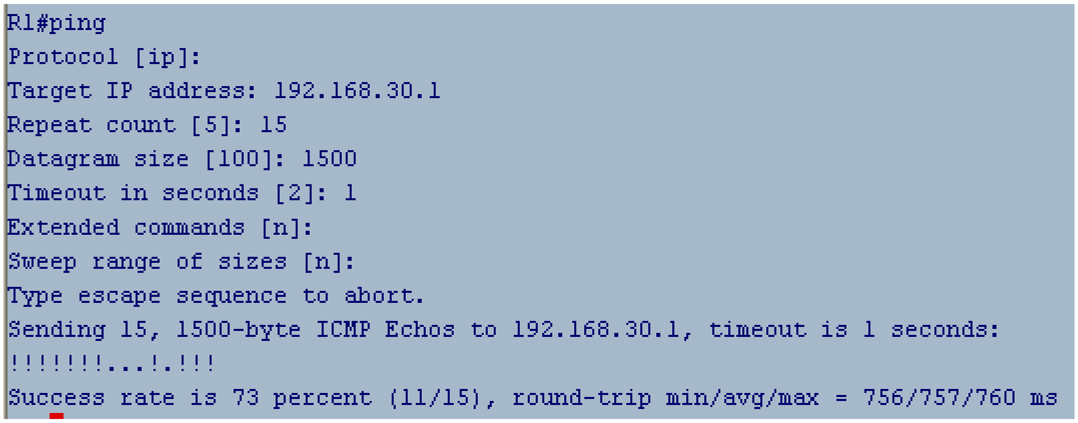
The following screenshot shows the finish time of DUAL calculation with EIGRP configured to use up to 1% of the configured link bandwidth.



```
00:08:46: %DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.1.1 (Serial0/0) is up: new adjacency
```

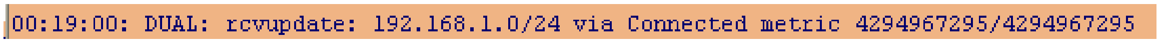
From the above screenshots it can be seen that DUAL took 6 seconds to converge when allocate to use only 1% of the configured link bandwidth.

The following screenshot shows the result of the extended ping with EIGRP allocated up to10% of the configured link bandwidth for usage.



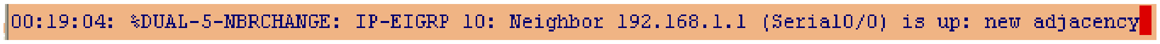
```
R1#ping
Protocol [ip]:
Target IP address: 192.168.30.1
Repeat count [5]: 15
Datagram size [100]: 1500
Timeout in seconds [2]: 1
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 15, 1500-byte ICMP Echos to 192.168.30.1, timeout is 1 seconds:
!!!!!!!...!.!!!
Success rate is 73 percent (11/15), round-trip min/avg/max = 756/757/760 ms
```

The following screenshot shows the start time of DUAL calculation with EIGRP configured to use up to 10% of the configured link bandwidth.



```
00:19:00: DUAL: rcvupdate: 192.168.1.0/24 via Connected metric 4294967295/4294967295
```

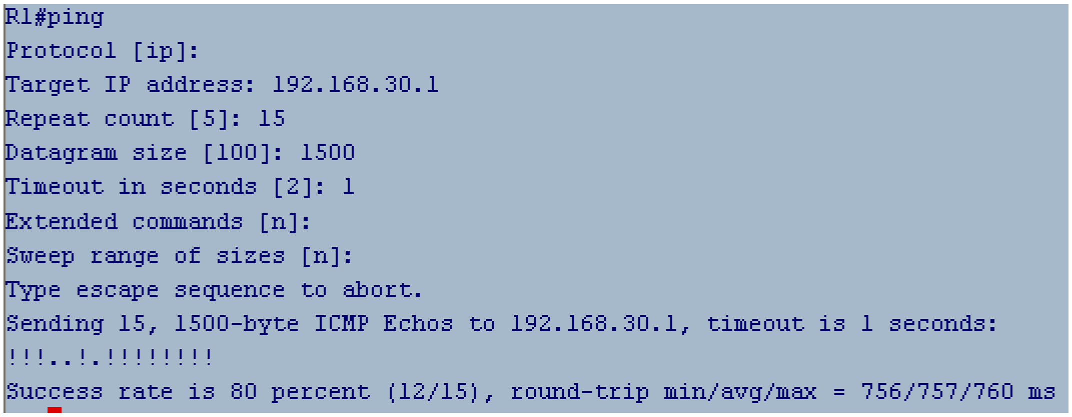
The following screenshot shows the finish time of DUAL calculation with EIGRP configured to use up to 10% of the configured link bandwidth.



```
00:19:04: %DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.1.1 (Serial0/0) is up: new adjacency
```

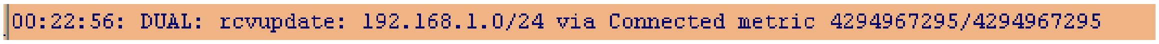
From the above screenshots it can be seen that DUAL took 4 seconds to converge when allocate to use only 10% of the configured link bandwidth.

The following screenshot shows the result of the extended ping with EIGRP allowed to use up to 20% of the configured link bandwidth.



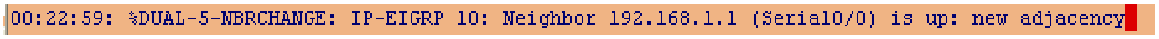
```
R1#ping
Protocol [ip]:
Target IP address: 192.168.30.1
Repeat count [5]: 15
Datagram size [100]: 1500
Timeout in seconds [2]: 1
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 15, 1500-byte ICMP Echos to 192.168.30.1, timeout is 1 seconds:
!!!..!.!!!!!!!!
Success rate is 80 percent (12/15), round-trip min/avg/max = 756/757/760 ms
```

The following screenshot shows the start time of DUAL calculation with EIGRP configured to use up to 20% of the configured link bandwidth.



```
00:22:56: DUAL: rcvupdate: 192.168.1.0/24 via Connected metric 4294967295/4294967295
```

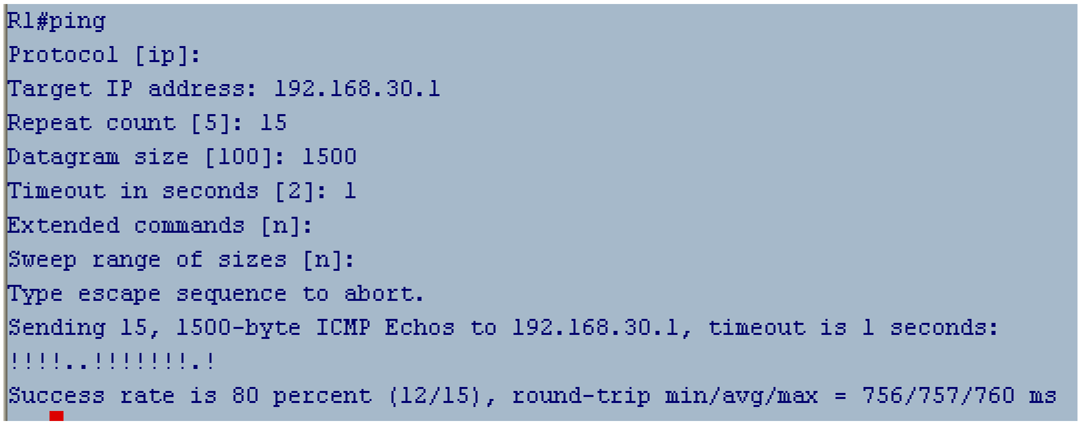
The following screenshot shows the finish time of DUAL calculation with EIGRP configured to use up to 20% of the configured link bandwidth.



```
00:22:59: %DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.1.1 (Serial0/0) is up: new adjacency
```

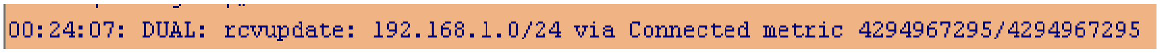
From the above screenshots it can be seen that DUAL took 3 seconds to converge when allocate to use only 20% of the configured link bandwidth.

The following screenshot shows the result of the extended ping with EIGRP allowed to use only 30% of the configured link bandwidth.



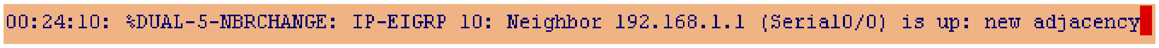
```
R1#ping
Protocol [ip]:
Target IP address: 192.168.30.1
Repeat count [5]: 15
Datagram size [100]: 1500
Timeout in seconds [2]: 1
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 15, 1500-byte ICMP Echos to 192.168.30.1, timeout is 1 seconds:
!!!!..!!!!!!!.!
Success rate is 80 percent (12/15), round-trip min/avg/max = 756/757/760 ms
```

The following screenshot shows the start time of DUAL calculation with EIGRP configured to use up to 30% of the configured link bandwidth.



```
00:24:07: DUAL: rcvupdate: 192.168.1.0/24 via Connected metric 4294967295/4294967295
```

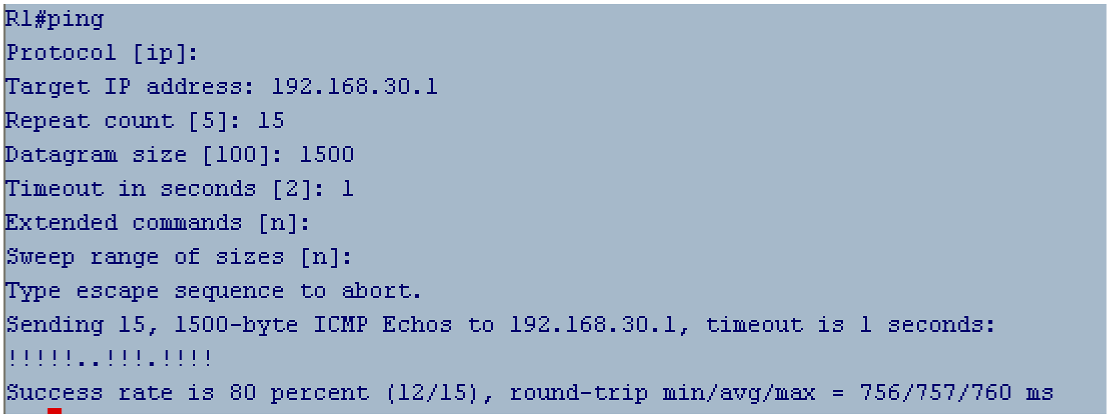
The following screenshot shows the finish time of DUAL calculation with EIGRP configured to use up to 30% of the configured link bandwidth.



```
00:24:10: %DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.1.1 (Serial0/0) is up: new adjacency
```

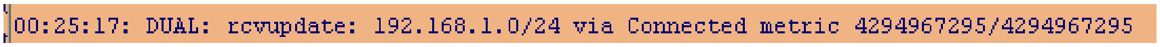
From the above screenshots it can be seen that DUAL took 3 seconds to converge when allocate to use only 30% of the configured link bandwidth.

The following screenshot shows the result of the extended ping with EIGRP allowed to use only 40% of the configured link bandwidth.



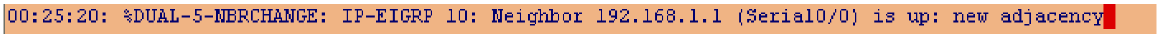
```
R1#ping
Protocol [ip]:
Target IP address: 192.168.30.1
Repeat count [5]: 15
Datagram size [100]: 1500
Timeout in seconds [2]: 1
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 15, 1500-byte ICMP Echos to 192.168.30.1, timeout is 1 seconds:
!!!!!..!!!.!!!!
Success rate is 80 percent (12/15), round-trip min/avg/max = 756/757/760 ms
```

The following screenshot shows the start time of DUAL calculation with EIGRP configured to use up to 40% of the configured link bandwidth.



```
00:25:17: DUAL: rcvupdate: 192.168.1.0/24 via Connected metric 4294967295/4294967295
```

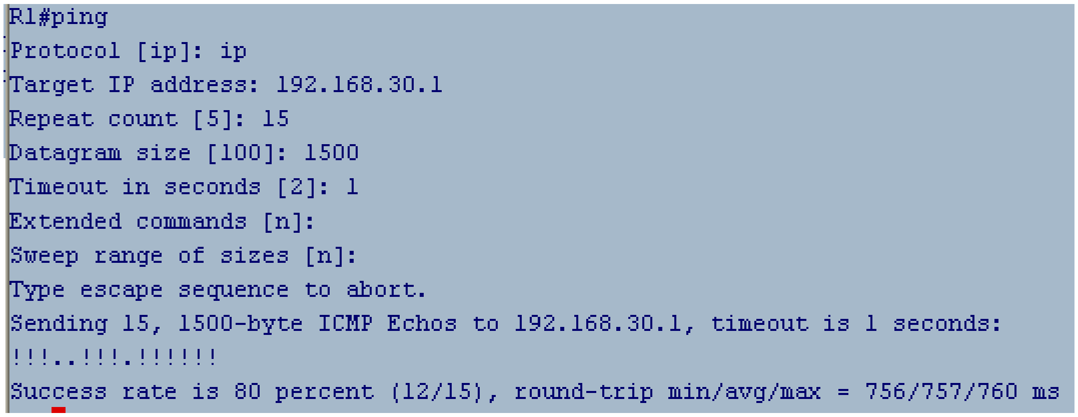
The following screenshot shows the finish time of DUAL calculation with EIGRP configured to use up to 40% of the configured link bandwidth.



```
00:25:20: %DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.1.1 (Serial0/0) is up: new adjacency
```

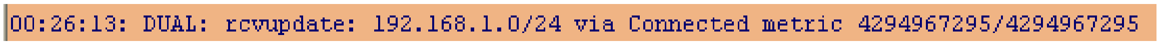
From the above screenshots it can be seen that DUAL took 3 seconds to converge when allocate to use only 40% of the configured link bandwidth.

The following screenshot shows the result of the extended ping with EIGRP allowed to use only 100% of the configured link bandwidth.



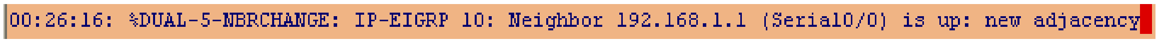
```
R1#ping
Protocol [ip]: ip
Target IP address: 192.168.30.1
Repeat count [5]: 15
Datagram size [100]: 1500
Timeout in seconds [2]: 1
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 15, 1500-byte ICMP Echos to 192.168.30.1, timeout is 1 seconds:
!!!..!!!.!!!!!!
Success rate is 80 percent (12/15), round-trip min/avg/max = 756/757/760 ms
```

The following screenshot shows the start time of DUAL calculation with EIGRP configured to use up to 100% of the configured link bandwidth.



```
00:26:13: DUAL: rcvupdate: 192.168.1.0/24 via Connected metric 4294967295/4294967295
```

The following screenshot shows the finish time of DUAL calculation with EIGRP configured to use up to 100% of the configured link bandwidth.

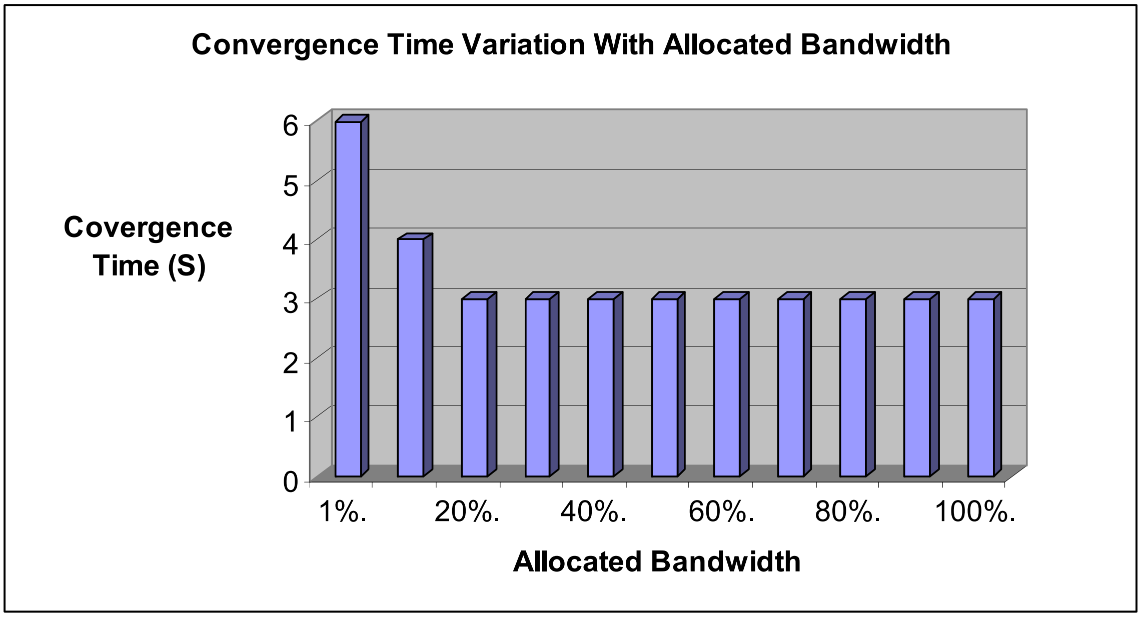


```
00:26:16: %DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.1.1 (Serial0/0) is up: new adjacency
```

From the above screenshots it can be seen that DUAL took 3 seconds to converge when allocate to use only 100% of the configured link bandwidth.

Analysis: From the experiment results it can be seen that the convergence time of the network changes once the amount of bandwidth available to EIGRP is reduced to 10%. Above 10% there is no significant change because on a small network like this EIGRP requires around 10% of the bandwidth to have the best convergence times.

The graph below shows the effect of allocated bandwidth on the network convergence time.



It should however be noted the convergence time and the effect of the change of allocated bandwidth depends on the size of the network and its complexity. This graph gives a representation of the network that was used for the experiment.

Conclusion: The experiment successfully shows the variations in convergence times of the network due to different allocation of Bandwidth to EIGRP process.

6.2.4 Hello packet exchanges to form neighbour relationship and rediscover failed neighbours.

Aim: To show the exchange of hello packets between two adjacent routers to form a neighbour relationship.

Figure 6.4 – Network topology for experiment 6.2.4

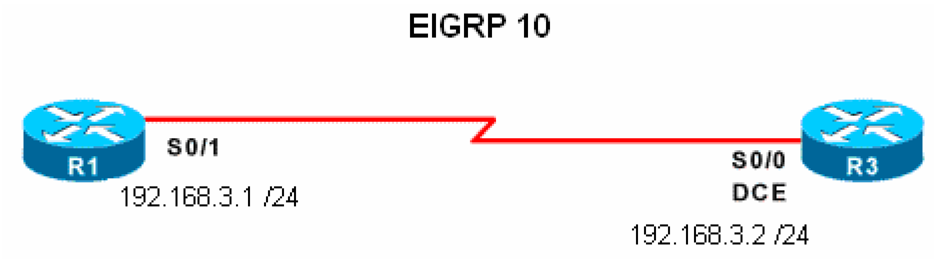


Table 6.4 – Router Configuration for Experiment 6.2.4

Configuration for Router R1

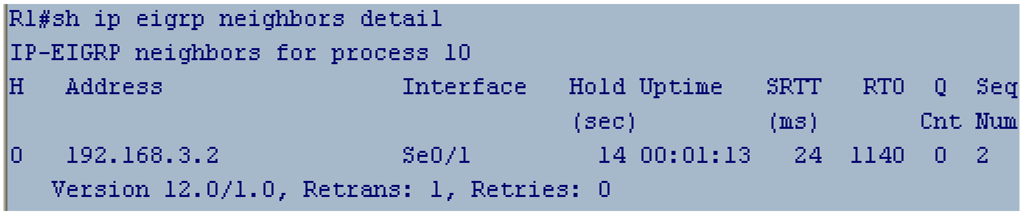
```
Router>enable
Router#conFigure terminal
Router(config)#hostname R1
R1(config)#interface serial 0/1
R1(config-if)# ip address 192.168.3.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router eigrp 10
R1(config-router)#network 192.168.3.0
```

Configuration for Router R3

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R3
R3(config)#interface serial 0/0
R3(config-if)# ip address 192.168.3.2 255.255.255.0
R3(config-if)#clockrate 64000
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router eigrp 10
R3(config-router)#network 192.168.3.0
```

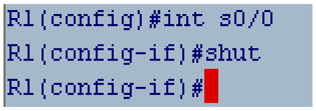
Description/Procedure: The two routers on the network will be configured according the topology shown Figure 6.4 and the configuration given in Table 6.4. Neighbour Table of each router will then be checked to verify that the routers have formed adjacency. EIGRP neighbour debugging feature will be used on one of the routers and the EIGPR packet debugging feature will be used on the other router. Link failure between the routers will be simulated, by turning the serial interface of a router off and then back on again. When the link comes back up again, the enabled debug features on both routers will show outputs showing the hello packets that were exchanged and the forming of a neighbour relationship. Once the relationship has been re-established the routing Tables on both routers will be checked to verify that routing information was shared between then when they formed the neighbour relationship. An estimated time needed to establish neighbour relationship will also be measured.

Result: The following screenshot shows the neighbour Table of Router R1



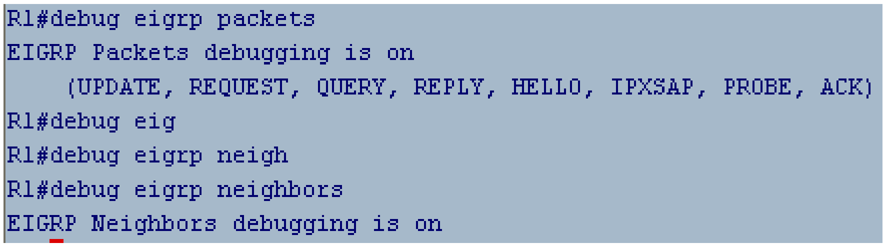
```
R1#sh ip eigrp neighbors detail
IP-EIGRP neighbors for process 10
H   Address                 Interface    Hold Uptime   SRTT   RTO  Q  Seq
                                         (sec)         (ms)       Cnt Num
0   192.168.3.2             Se0/1          14 00:01:13   24   1140  0  2
   Version 12.0/1.0, Retrans: 1, Retries: 0
```

The failure of link Serial 0/0 of Router R1 is being simulated by administratively shutting it down. The following screenshot shows the command used to administratively shut the link down.



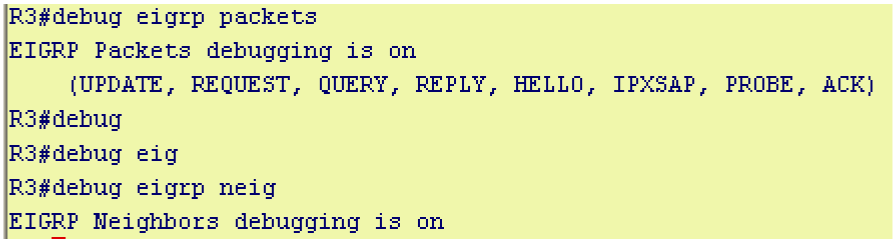
```
R1(config)#int s0/0
R1(config-if)#shut
R1(config-if)#
```

The following screenshots show the debugging neighbour and the debugging of EIGRP packets feature being turned on for Router R1.



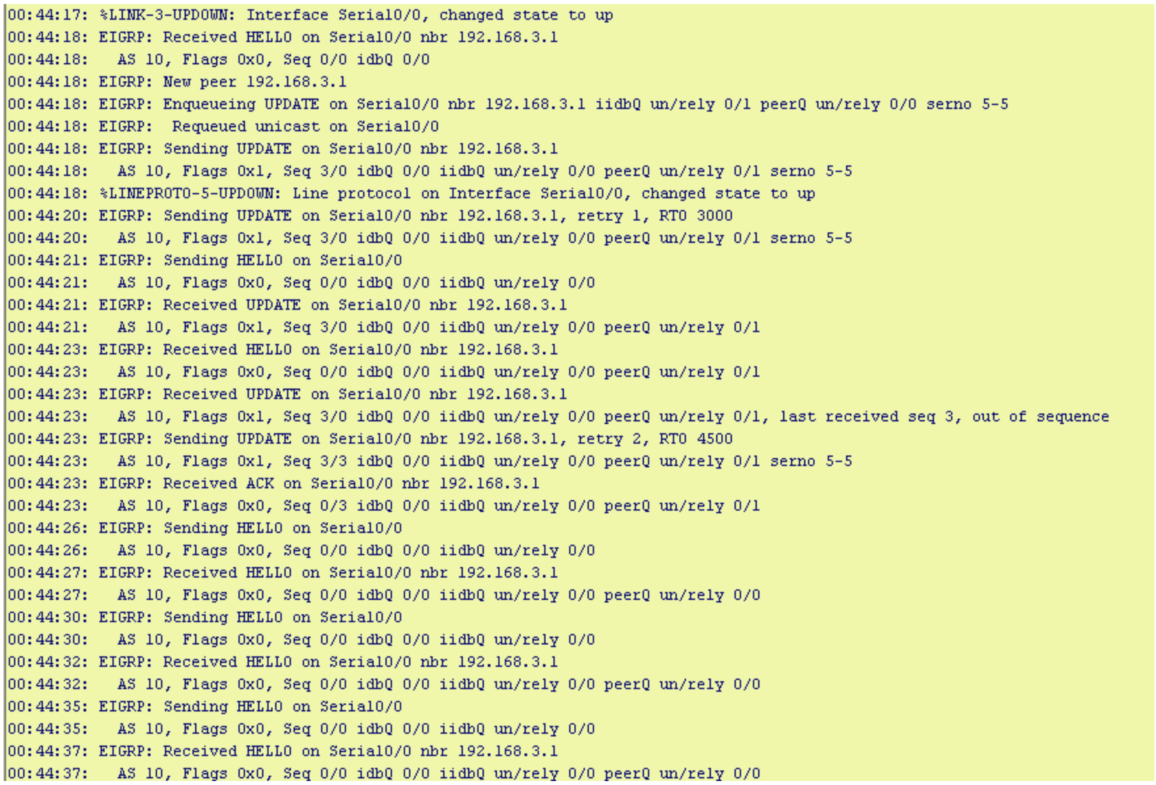
```
R1#debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK)
R1#debug eig
R1#debug eigrp neigh
R1#debug eigrp neighbors
EIGRP Neighbors debugging is on
```

The following screenshots show the debugging neighbour and the debugging of EIGRP packets feature being turned on for Router R3.



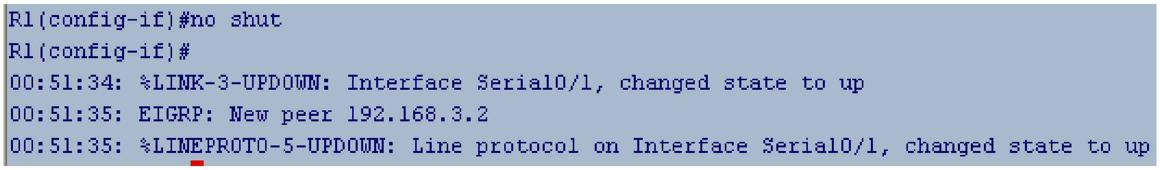
```
R3#debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK)
R3#debug
R3#debug eig
R3#debug eigrp neig
EIGRP Neighbors debugging is on
```

The following screenshot shows the output of the debug screen once the serial link is re-instantiated. It can be observed EIGRP neighbour process starts by receiving of hello packet by Router R3 at 00:44:18 and completes neighbour establishment by receiving of the last acknowledgement for the updates sent at 00:44:23. However the detection of the new peer occurs at 00:44:18.



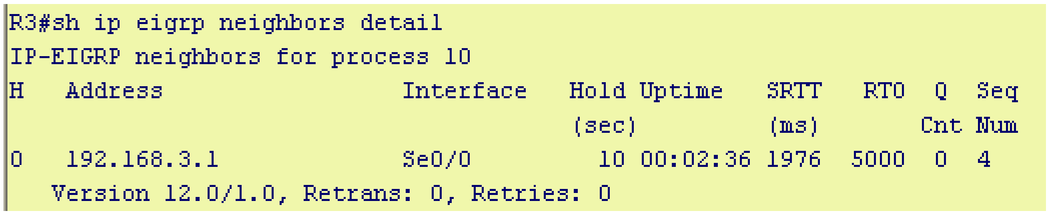
```
00:44:17: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
00:44:18: EIGRP: Received HELLO on Serial0/0 nbr 192.168.3.1
00:44:18:   AS 10, Flags 0x0, Seq 0/0 idbQ 0/0
00:44:18: EIGRP: New peer 192.168.3.1
00:44:18: EIGRP: Enqueueing UPDATE on Serial0/0 nbr 192.168.3.1 iidbQ un/rely 0/1 peerQ un/rely 0/0 serno 5-5
00:44:18: EIGRP:  Requeued unicast on Serial0/0
00:44:18: EIGRP: Sending UPDATE on Serial0/0 nbr 192.168.3.1
00:44:18:   AS 10, Flags 0x1, Seq 3/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1 serno 5-5
00:44:18: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
00:44:20: EIGRP: Sending UPDATE on Serial0/0 nbr 192.168.3.1, retry 1, RTO 3000
00:44:20:   AS 10, Flags 0x1, Seq 3/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1 serno 5-5
00:44:21: EIGRP: Sending HELLO on Serial0/0
00:44:21:   AS 10, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
00:44:21: EIGRP: Received UPDATE on Serial0/0 nbr 192.168.3.1
00:44:21:   AS 10, Flags 0x1, Seq 3/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1
00:44:23: EIGRP: Received HELLO on Serial0/0 nbr 192.168.3.1
00:44:23:   AS 10, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1
00:44:23: EIGRP: Received UPDATE on Serial0/0 nbr 192.168.3.1
00:44:23:   AS 10, Flags 0x1, Seq 3/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1, last received seq 3, out of sequence
00:44:23: EIGRP: Sending UPDATE on Serial0/0 nbr 192.168.3.1, retry 2, RTO 4500
00:44:23:   AS 10, Flags 0x1, Seq 3/3 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1 serno 5-5
00:44:23: EIGRP: Received ACK on Serial0/0 nbr 192.168.3.1
00:44:23:   AS 10, Flags 0x0, Seq 0/3 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1
00:44:26: EIGRP: Sending HELLO on Serial0/0
00:44:26:   AS 10, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
00:44:27: EIGRP: Received HELLO on Serial0/0 nbr 192.168.3.1
00:44:27:   AS 10, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
00:44:30: EIGRP: Sending HELLO on Serial0/0
00:44:30:   AS 10, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
00:44:32: EIGRP: Received HELLO on Serial0/0 nbr 192.168.3.1
00:44:32:   AS 10, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
00:44:35: EIGRP: Sending HELLO on Serial0/0
00:44:35:   AS 10, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
00:44:37: EIGRP: Received HELLO on Serial0/0 nbr 192.168.3.1
00:44:37:   AS 10, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
```

The following screenshot shows the output from the neighbour debugging after the link was turned back on.

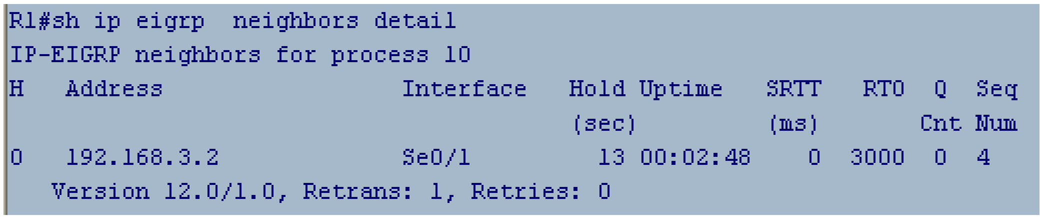


```
R1(config-if)#no shut
R1(config-if)#
00:51:34: %LINK-3-UPDOWN: Interface Serial0/1, changed state to up
00:51:35: EIGRP: New peer 192.168.3.2
00:51:35: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to up
```

The following screenshots showing neighbour Tables of router R3 and router R1 confirms that the adjacent routers were able to re-establish their neighbour relationship once the link was turned back on.



```
R3#sh ip eigrp neighbors detail
IP-EIGRP neighbors for process 10
H   Address                 Interface    Hold Uptime   SRTT   RTO  Q  Seq
                                         (sec)         (ms)       Cnt Num
0   192.168.3.1             Se0/0          10 00:02:36 1976   5000  0  4
   Version 12.0/1.0, Retrans: 0, Retries: 0
```



```
R1#sh ip eigrp  neighbors detail
IP-EIGRP neighbors for process 10
H   Address                 Interface    Hold Uptime   SRTT   RTO  Q  Seq
                                         (sec)         (ms)       Cnt Num
0   192.168.3.2             Se0/1          13 00:02:48    0   3000  0  4
   Version 12.0/1.0, Retrans: 1, Retries: 0
```

Analysis: From the experiment it can be seen that hello packets are used to detect and form neighbour relationships by EIGRP. It is also observed that once the failed link is re-instantiated, the adjacent router takes about a second before it recognizes the new peer and starts the relationship forming process. The relationship is formed and the two routers are fully converged after they have shared information about their routes. This time taken for routers to form relationship will also depend somewhat on the network, its size and its configurations.

Conclusion: The experiment successfully demonstrates the use of hello packets to form new neighbour relationships and also to rediscover neighbours that were previously unavailable.

6.2.5 Periodic exchange of hello packets to maintain relationship

Aim: To confirm and analyze the use of hello packet in neighbour relationship maintenance

Figure 6.5 – Network topology for experiment 6.2.5

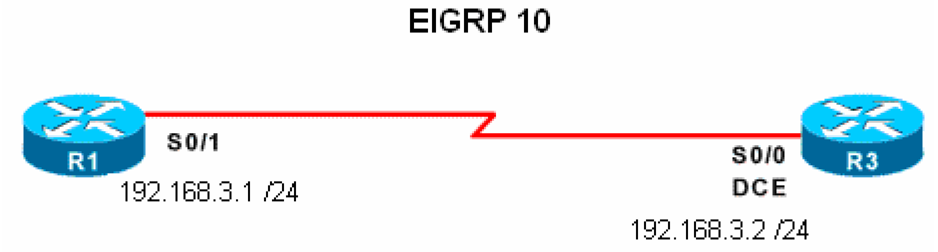
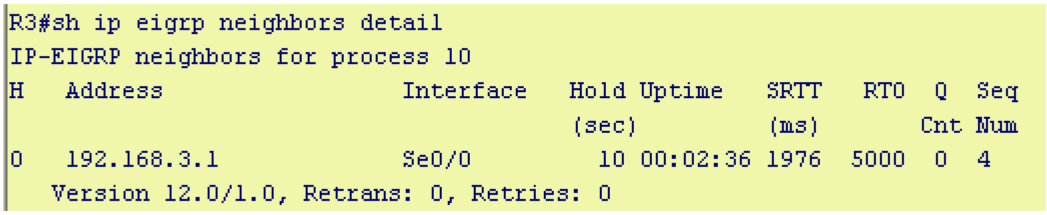


Table 6.5 – Router Configuration for Experiment 6.2.5

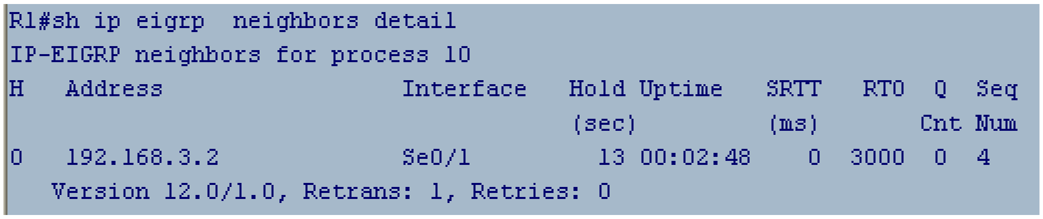
Configuration for Router R1
Router>enable
Router#conFigure terminal
Router(config)#hostname R1
R1(config)#interface serial 0/1
R1(config-if)# ip address 192.168.3.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router eigrp 10
R1(config-router)#network 192.168.3.0
Configuration for Router R3
Router>enable
Router#conFigure terminal
Router(config)#hostname R3
R3(config)#interface serial 0/0
R3(config-if)# ip address 192.168.3.2 255.255.255.0
R3(config-if)#clockrate 64000
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router eigrp 10
R3(config-router)#network 192.168.3.0

Description/Procedure: The two routers on the network will be configured according the topology shown in the network diagram and the configuration given Figure 6.5 and Table 6.5. Neighbour Table of each router will then be checked to verify that the routers have formed adjacency. Through the use of debug EIGRP packets command, the exchange of hello packets to maintain relationship will be shown. The interval between the packets will also be shown. Hello interval will be re-configured to be more than the hold-time. Expected neighbour relationship failures in such case will be noted. The hold-time of the routers will also be increase and the process carried out in 6.2.4 will be done again to estimate the time taken to form the neighbour relationship with the increase hello interval.

Result: The following screenshots show the neighbour Table of the two routers verifying that they have formed neighbour relationship.

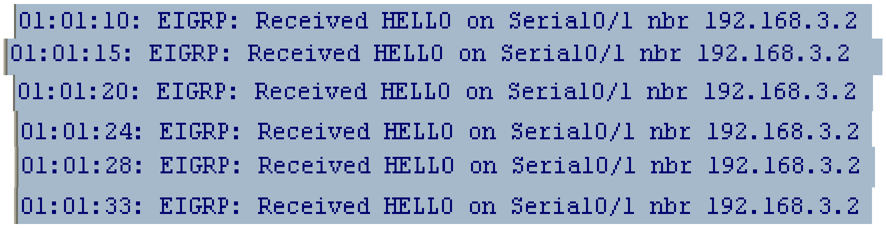


```
R3#sh ip eigrp neighbors detail
IP-EIGRP neighbors for process 10
H   Address                 Interface    Hold Uptime   SRTT   RTO  Q  Seq
                                         (sec)         (ms)       Cnt Num
0   192.168.3.1             Se0/0          10 00:02:36 1976   5000  0  4
   Version 12.0/1.0, Retrans: 0, Retries: 0
```



```
R1#sh ip eigrp  neighbors detail
IP-EIGRP neighbors for process 10
H   Address                 Interface    Hold Uptime   SRTT   RTO  Q  Seq
                                         (sec)         (ms)       Cnt Num
0   192.168.3.2             Se0/1          13 00:02:48    0   3000  0  4
   Version 12.0/1.0, Retrans: 1, Retries: 0
```

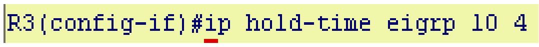
The following screenshot shows the Hello packets that are being sent by Router R1.



```
01:01:10: EIGRP: Received HELLO on Serial0/1 nbr 192.168.3.2
01:01:15: EIGRP: Received HELLO on Serial0/1 nbr 192.168.3.2
01:01:20: EIGRP: Received HELLO on Serial0/1 nbr 192.168.3.2
01:01:24: EIGRP: Received HELLO on Serial0/1 nbr 192.168.3.2
01:01:28: EIGRP: Received HELLO on Serial0/1 nbr 192.168.3.2
01:01:33: EIGRP: Received HELLO on Serial0/1 nbr 192.168.3.2
```

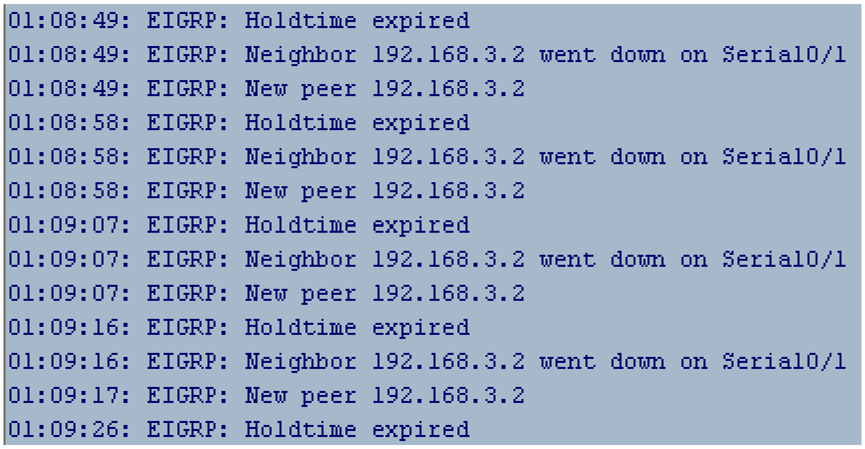
From the above screen it can be seen that hello packet interval is still the default value of 5 seconds. If the screenshot is looked at closely it can be seen that the packets are not sent at exactly 5 seconds. There is a random time which EIGRP either adds or subtract from the configured hello time to avoid situations where each router sends out hello packets at the same time.

The following screenshot shows the hold-time for Router R1 on Router R3 is being reduced to 4 seconds.



```
R3(config-if)#ip hold-time eigrp 10 4
```

The following screenshot reveals the affect of the decreased hold time. As the hello interval is currently 5 seconds but the hold-time is currently 4 seconds, Router R3 times Router R1 out and drops it from the neighbour Table. After receiving the next hello packet it tries to establish the neighbour relationship but the neighbour times out again.



```
01:08:49: EIGRP: Holdtime expired
01:08:49: EIGRP: Neighbor 192.168.3.2 went down on Serial0/1
01:08:49: EIGRP: New peer 192.168.3.2
01:08:58: EIGRP: Holdtime expired
01:08:58: EIGRP: Neighbor 192.168.3.2 went down on Serial0/1
01:08:58: EIGRP: New peer 192.168.3.2
01:09:07: EIGRP: Holdtime expired
01:09:07: EIGRP: Neighbor 192.168.3.2 went down on Serial0/1
01:09:07: EIGRP: New peer 192.168.3.2
01:09:16: EIGRP: Holdtime expired
01:09:16: EIGRP: Neighbor 192.168.3.2 went down on Serial0/1
01:09:17: EIGRP: New peer 192.168.3.2
01:09:26: EIGRP: Holdtime expired
```

Analysis: The experiment is used to show the consequences of incorrect configuration of the hello interval and the hold time. This situation should be avoided because each time a neighbour is lost DUAL tries to recalculate all routes that were lost. Also, each time a neighbour is found DUAL does calculations for new route. Conditions like above can lead to very intense use of processing power rendering the router inactive. This situation can also happen in highly congested networks where hello packets may not be received within the hold time. In such cases hold time may be increased to address the problem but, that would increase the time needed for the network to converge.

Conclusion: The experiments addresses issues related to mis-configuration of hello interval and hold time. It also discusses related issues and possible solutions.

6.2.6 Successor Selection

Aim: To demonstrate the Successor Selection Process

Figure 6.6 – Network topology for experiment 6.2.6

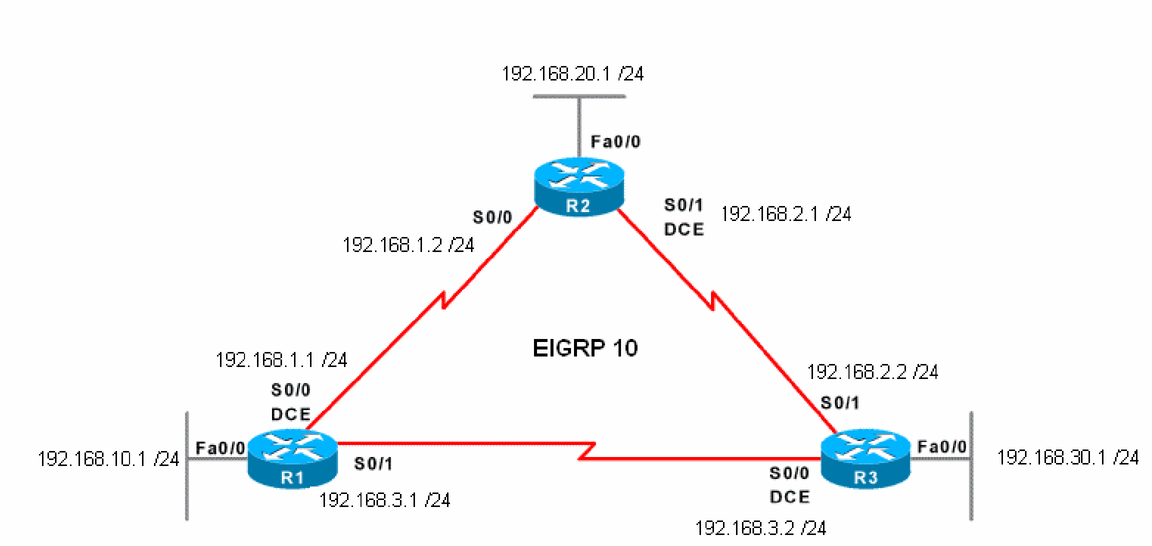


Table 6.6 – Router Configuration for Experiment 6.2.6

Configuration for Router R1

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R1
R1(config)#interface serial 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)#clockrate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/1
R1(config-if)# ip address 192.168.3.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fa 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router eigrp 10
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.3.0
R1(config-router)#network 192.168.10.0
```

Configuration for Router R2

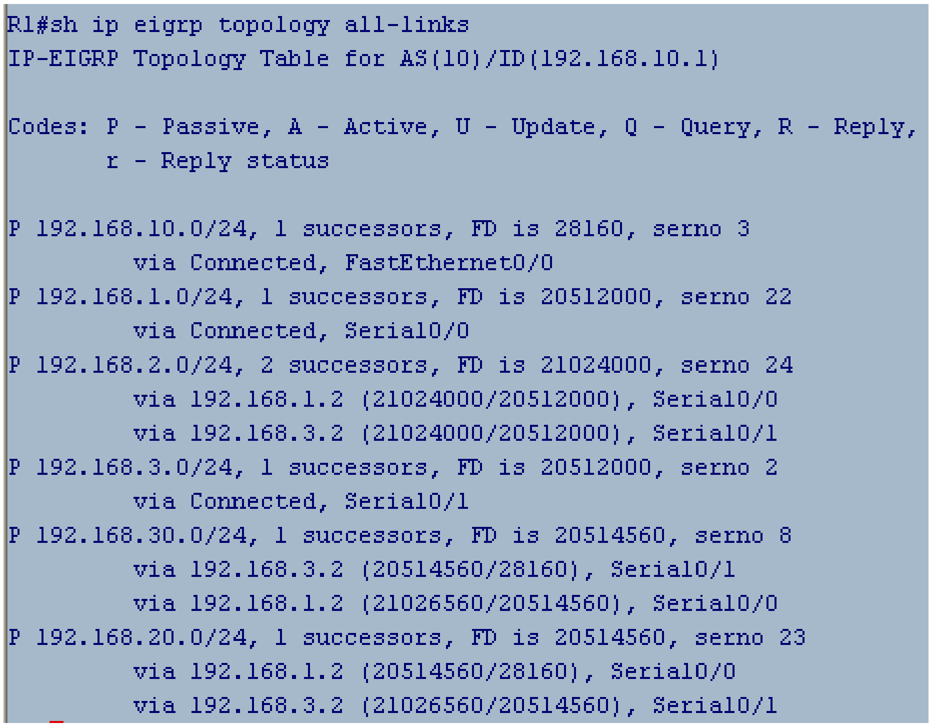
```
Router>enable
Router#conFigure terminal
Router(config)#hostname R2
R2(config)#interface serial 0/0
R2(config-if)# ip address 192.168.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface serial 0/1
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)#clockrate 64000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface fa 0/0
R2(config-if)# ip address 192.168.20.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router eigrp 10
R2(config-router)#network 192.168.1.0
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.20.0
```

Configuration for Router R3

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R3
R3(config)#interface serial 0/0
R3(config-if)# ip address 192.168.3.2 255.255.255.0
R3(config-if)#clockrate 64000
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface serial 0/1
R3(config-if)# ip address 192.168.2.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface fa 0/0
R3(config-if)# ip address 192.168.30.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router eigrp 10
R3(config-router)#network 192.168.2.0
R3(config-router)#network 192.168.3.0
R3(config-router)#network 192.168.30.0
```

Description/Procedure: The routers will be configured according to the network topology diagram and the configurations given in Figure 6.6 and Table 6.6. Once the network has converged the show IP route and Show IP EIGRP Topology all-link commands will be used to show the possible routes to destinations and theirs costs. Debug outputs will be used to show the route computation done by DUAL FSM during change of links status.

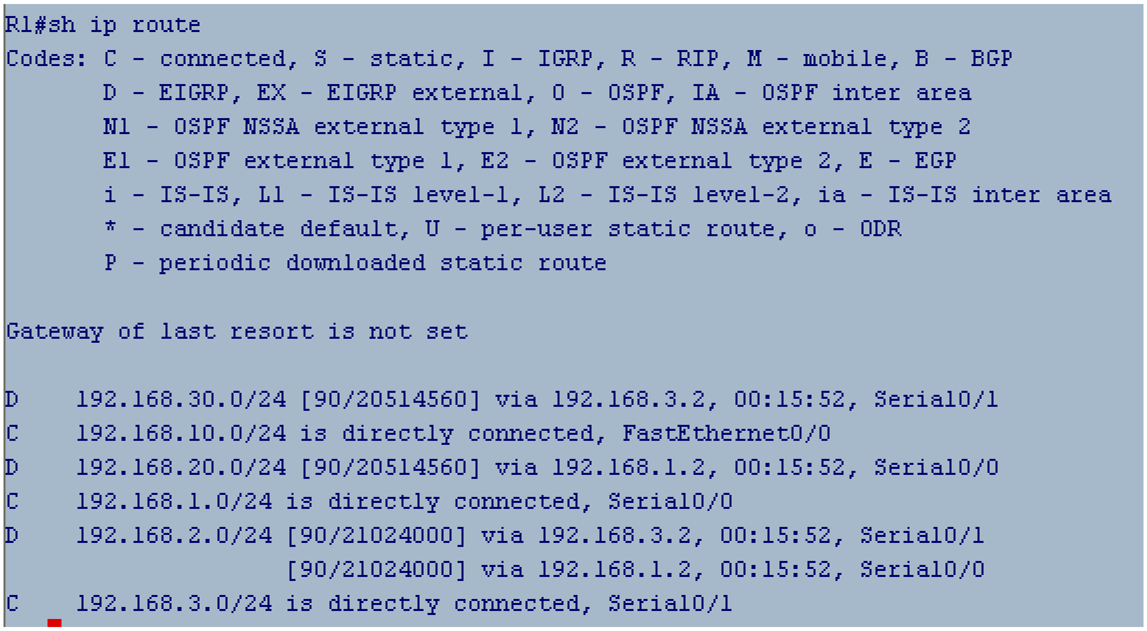
Result: The following screenshot show all the topology Table of Router R1, which contains all the routes learned by the router.



```
R1#sh ip eigrp topology all-links
IP-EIGRP Topology Table for AS(10)/ID(192.168.10.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.10.0/24, 1 successors, FD is 28160, serno 3
         via Connected, FastEthernet0/0
P 192.168.1.0/24, 1 successors, FD is 20512000, serno 22
         via Connected, Serial0/0
P 192.168.2.0/24, 2 successors, FD is 21024000, serno 24
         via 192.168.1.2 (21024000/20512000), Serial0/0
         via 192.168.3.2 (21024000/20512000), Serial0/1
P 192.168.3.0/24, 1 successors, FD is 20512000, serno 2
         via Connected, Serial0/1
P 192.168.30.0/24, 1 successors, FD is 20514560, serno 8
         via 192.168.3.2 (20514560/28160), Serial0/1
         via 192.168.1.2 (21026560/20514560), Serial0/0
P 192.168.20.0/24, 1 successors, FD is 20514560, serno 23
         via 192.168.1.2 (20514560/28160), Serial0/0
         via 192.168.3.2 (21026560/20514560), Serial0/1
```

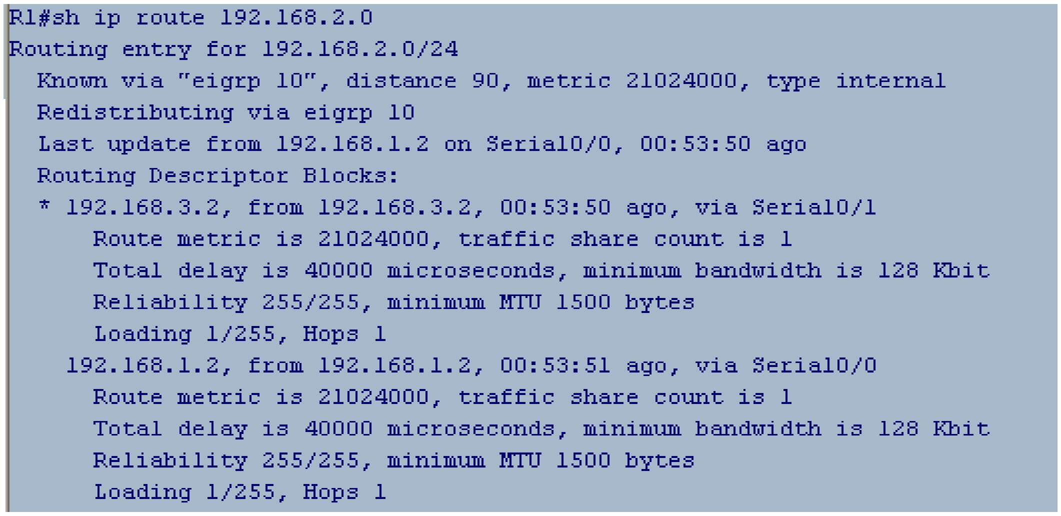
From the topology able shown above the total cost for each route is given in brackets next to the next hop address for the destination. The first number in the bracket is the total cost of the link. The path with the least cost will be chosen as the successor and installed into the routing Table by DUAL. It can also be observed that for destination 192.168.2.0 there are two links, via serial 0/0 and via serial0/1 from router R1. Both the routes have the same cost so DUAL should install both routes into the routing Table automatically.

The following screenshot shows the routing Table of the router, which confirms that the cheapest path for each destination was selected and installed into the routing Table by DUAL. For destination 192.169.2.0 as there were two equal least cost paths, both of them were installed.



```
R1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D    192.168.30.0/24 [90/20514560] via 192.168.3.2, 00:15:52, Serial0/1
C    192.168.10.0/24 is directly connected, FastEthernet0/0
D    192.168.20.0/24 [90/20514560] via 192.168.1.2, 00:15:52, Serial0/0
C    192.168.1.0/24 is directly connected, Serial0/0
D    192.168.2.0/24 [90/21024000] via 192.168.3.2, 00:15:52, Serial0/1
                    [90/21024000] via 192.168.1.2, 00:15:52, Serial0/0
C    192.168.3.0/24 is directly connected, Serial0/1
```

The following screenshot shows the routes for destination 192.168.2.0 from Router R1.



```
R1#sh ip route 192.168.2.0
Routing entry for 192.168.2.0/24
  Known via "eigrp 10", distance 90, metric 21024000, type internal
  Redistributing via eigrp 10
  Last update from 192.168.1.2 on Serial0/0, 00:53:50 ago
  Routing Descriptor Blocks:
  * 192.168.3.2, from 192.168.3.2, 00:53:50 ago, via Serial0/1
      Route metric is 21024000, traffic share count is 1
      Total delay is 40000 microseconds, minimum bandwidth is 128 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
    192.168.1.2, from 192.168.1.2, 00:53:51 ago, via Serial0/0
      Route metric is 21024000, traffic share count is 1
      Total delay is 40000 microseconds, minimum bandwidth is 128 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

Analysis: The result of the DUAL computation shows that it picks the least cost loop free paths to each destination and puts them in the routing Table. These paths are then used by the router to forward packets to the intended destinations. The experiment also successfully demonstrates that if there is multiple least cost paths present for a destination, they are automatically installed into the routing Table.

Conclusion: This experiment shows that DUAL chooses the path with the least metric cost to reach a destination. This path is known as the successor route in EIGRP terminology.

6.2.7 Feasible Successor Selection

Aim: To demonstrate the Feasible Successor Selection Process

Figure 6.7 – Network topology for experiment 6.2.7

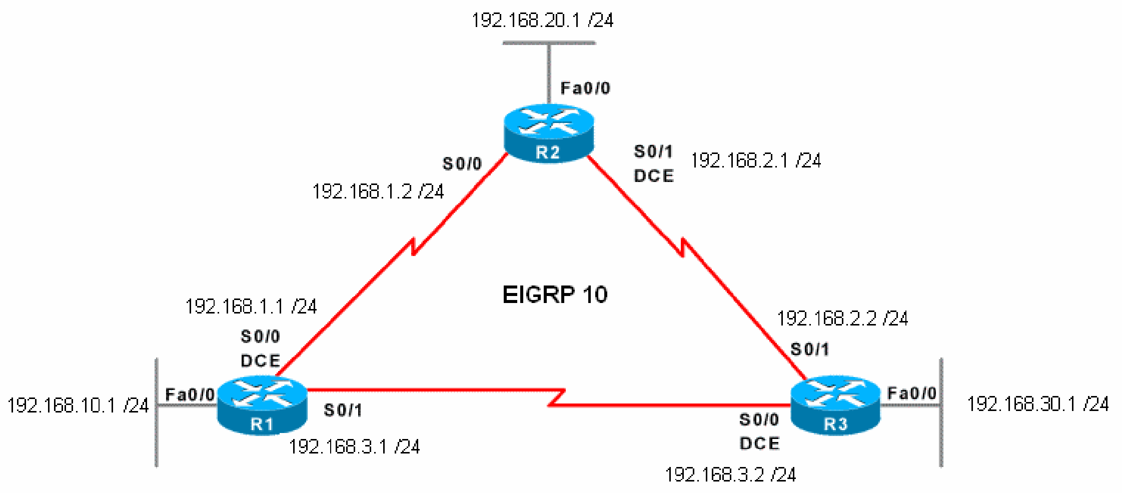


Table 6.7 – Router Configuration for Experiment 6.2.7

Configuration for Router R1

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R1
R1(config)#interface serial 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)#clockrate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/1
R1(config-if)# ip address 192.168.3.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fa 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router eigrp 10
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.3.0
R1(config-router)#network 192.168.10.0
```

Configuration for Router R2

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R2
R2(config)#interface serial 0/0
R2(config-if)# ip address 192.168.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface serial 0/1
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)#clockrate 64000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface fa 0/0
R2(config-if)# ip address 192.168.20.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router eigrp 10
R2(config-router)#network 192.168.1.0
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.20.0
```

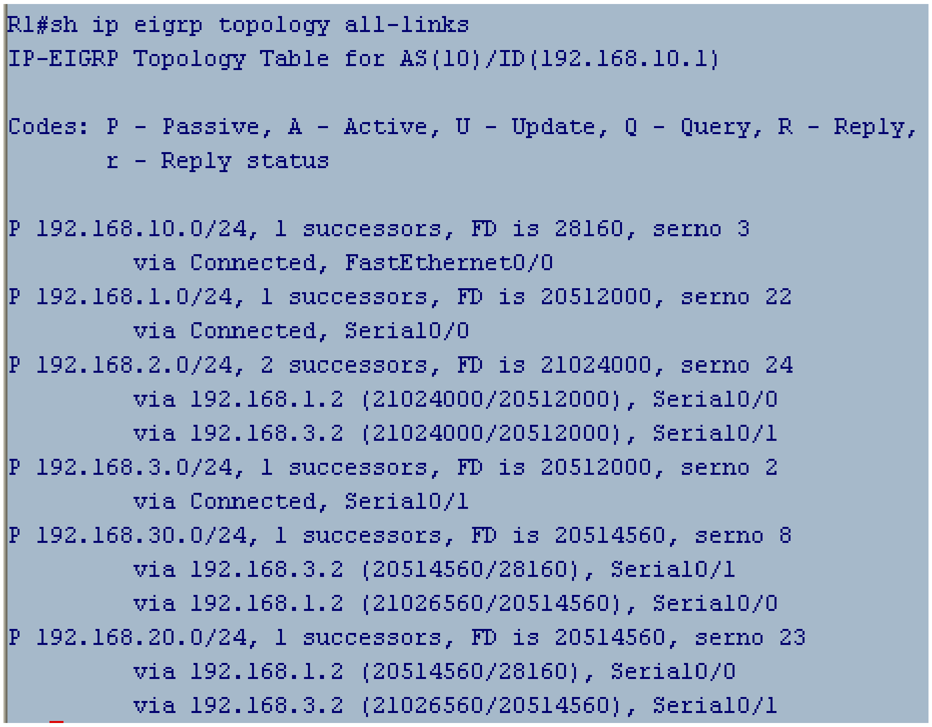
Configuration for Router R3

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R3
R3(config)#interface serial 0/0
R3(config-if)# ip address 192.168.3.2 255.255.255.0
R3(config-if)#clockrate 64000
R3(config-if)#no shutdown
R3(config-if)#exit
```

```
R3(config)#interface serial 0/1
R3(config-if)# ip address 192.168.2.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface fa 0/0
R3(config-if)# ip address 192.168.30.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router eigrp 10
R3(config-router)#network 192.168.2.0
R3(config-router)#network 192.168.3.0
R3(config-router)#network 192.168.30.0
```

Description/Procedure: The routers will be configured according to the network topology diagram and the configurations given Figure 6.7 and Table 6.7. However, this standard network configuration cannot be used to demonstrate the process for selection of feasible successor due to the nature of the topology and the links. The cost of routes will be manually manipulated to get the required reported distance that has to be advertised by a neighbour to meet the feasibility condition and be selected as a feasible successor. Once the metric costs have been calculated, they will be configured on appropriate links to enable the selection of a feasible successor. The confirmation for the presence of both successor and feasible successor for a destination will be achieved by checking the routing and the topology Table of routers. It will also be verified that the feasible successor is not used to forward any traffic until the successor link remains viable.

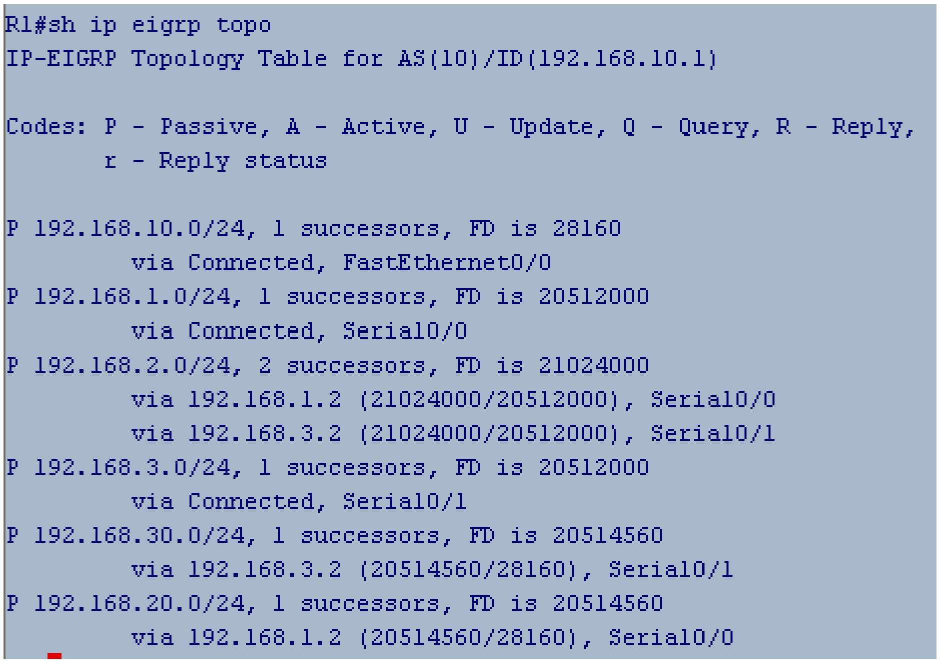
Result: The screenshot given below shows the topology Table of Router R1 with all links learned by the router.



```
R1#sh ip eigrp topology all-links
IP-EIGRP Topology Table for AS(10)/ID(192.168.10.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.10.0/24, 1 successors, FD is 28160, serno 3
         via Connected, FastEthernet0/0
P 192.168.1.0/24, 1 successors, FD is 20512000, serno 22
         via Connected, Serial0/0
P 192.168.2.0/24, 2 successors, FD is 21024000, serno 24
         via 192.168.1.2 (21024000/20512000), Serial0/0
         via 192.168.3.2 (21024000/20512000), Serial0/1
P 192.168.3.0/24, 1 successors, FD is 20512000, serno 2
         via Connected, Serial0/1
P 192.168.30.0/24, 1 successors, FD is 20514560, serno 8
         via 192.168.3.2 (20514560/28160), Serial0/1
         via 192.168.1.2 (21026560/20514560), Serial0/0
P 192.168.20.0/24, 1 successors, FD is 20514560, serno 23
         via 192.168.1.2 (20514560/28160), Serial0/0
         via 192.168.3.2 (21026560/20514560), Serial0/1
```

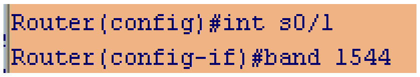
From the topology Table shown above it can be seen that for network 192.168.30.0 there are two links available. The first link is via 192.168.3.2 with a total cost of 20514560 and advertised cost of 28160. The other link via 192.168.1.2 has a total cost of 21026560 and advertised cost of 20514560. According feasibility conditions rule which feasible successors must satisfy, the advertised or reported distance of the route has to be less then the current feasible distance. For this reason the second link does not qualify as a feasible successor.

This is why it is not present in the topology Table with only successor and feasible successor routes.



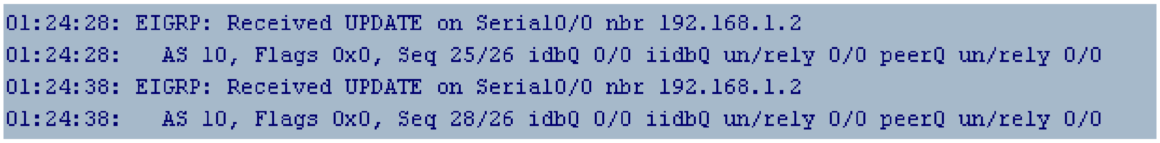
```
R1#sh ip eigrp topo
IP-EIGRP Topology Table for AS(10)/ID(192.168.10.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.10.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 192.168.1.0/24, 1 successors, FD is 20512000
         via Connected, Serial0/0
P 192.168.2.0/24, 2 successors, FD is 21024000
         via 192.168.1.2 (21024000/20512000), Serial0/0
         via 192.168.3.2 (21024000/20512000), Serial0/1
P 192.168.3.0/24, 1 successors, FD is 20512000
         via Connected, Serial0/1
P 192.168.30.0/24, 1 successors, FD is 20514560
         via 192.168.3.2 (20514560/28160), Serial0/1
P 192.168.20.0/24, 1 successors, FD is 20514560
         via 192.168.1.2 (20514560/28160), Serial0/0
```

To make the second route satisfy the feasibility condition the reported distance must be reduced. This is done by changing the bandwidth of the link to a higher one. This is done using the following command:



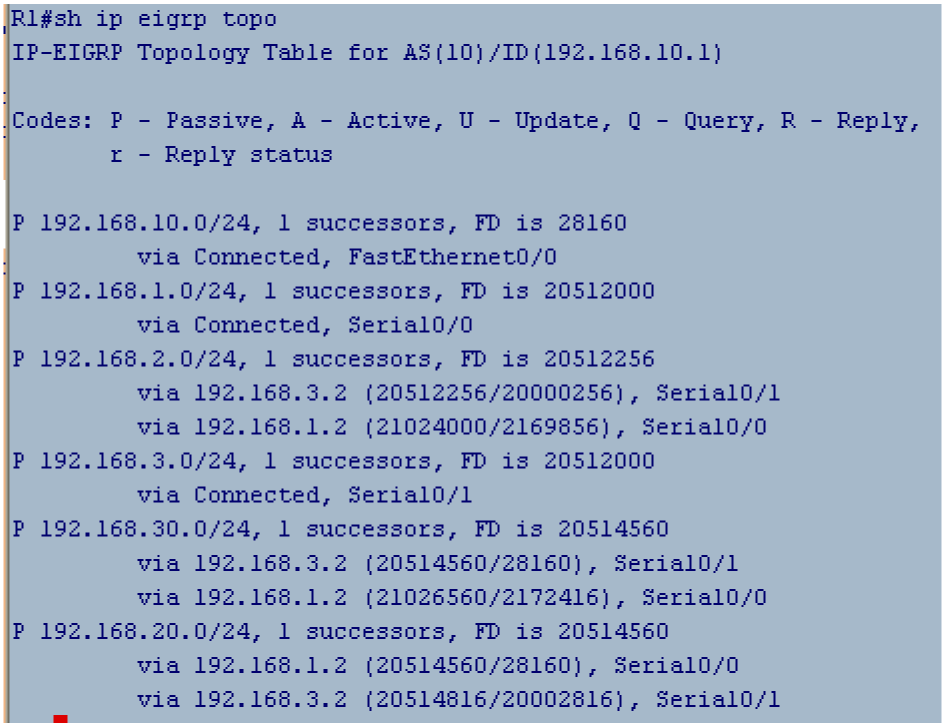
```
Router(config)#int s0/1
Router(config-if)#band 1544
```

Once the bandwidth of the link has been altered, Router R1 gets and update from router R2 giving it the new cost for the route. This is show in the screenshot given below:



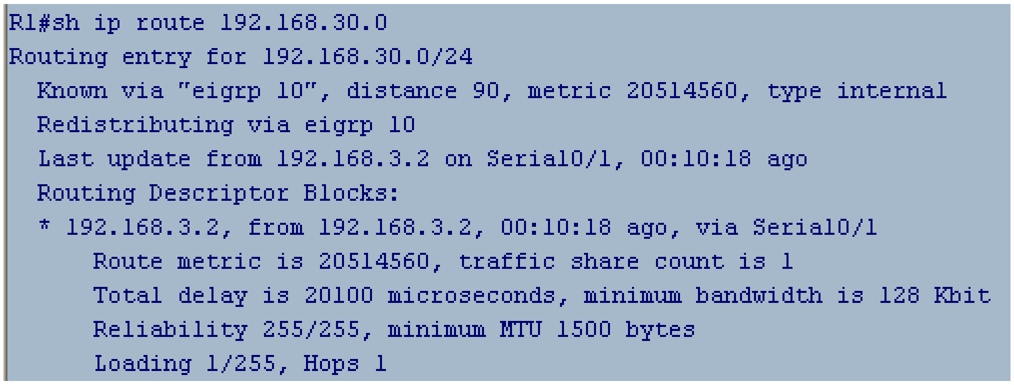
```
01:24:28: EIGRP: Received UPDATE on Serial0/0 nbr 192.168.1.2
01:24:28:   AS 10, Flags 0x0, Seq 25/26 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
01:24:38: EIGRP: Received UPDATE on Serial0/0 nbr 192.168.1.2
01:24:38:   AS 10, Flags 0x0, Seq 28/26 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
```

DUAL performs calculation and changes the metric for the routes. Now the second link qualifies as a feasible successor as its reported distance is less then the current feasible distance.



```
R1#sh ip eigrp topo
IP-EIGRP Topology Table for AS(10)/ID(192.168.10.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.10.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 192.168.1.0/24, 1 successors, FD is 20512000
         via Connected, Serial0/0
P 192.168.2.0/24, 1 successors, FD is 20512256
         via 192.168.3.2 (20512256/20000256), Serial0/1
         via 192.168.1.2 (21024000/2169856), Serial0/0
P 192.168.3.0/24, 1 successors, FD is 20512000
         via Connected, Serial0/1
P 192.168.30.0/24, 1 successors, FD is 20514560
         via 192.168.3.2 (20514560/28160), Serial0/1
         via 192.168.1.2 (21026560/2172416), Serial0/0
P 192.168.20.0/24, 1 successors, FD is 20514560
         via 192.168.1.2 (20514560/28160), Serial0/0
         via 192.168.3.2 (20514816/20002816), Serial0/1
```

The following screenshot shows the route entry for the destination network 192.168.30.0 proving that feasible successor is not automatically used to forward traffic.



```
R1#sh ip route 192.168.30.0
Routing entry for 192.168.30.0/24
  Known via "eigrp 10", distance 90, metric 20514560, type internal
  Redistributing via eigrp 10
  Last update from 192.168.3.2 on Serial0/1, 00:10:18 ago
  Routing Descriptor Blocks:
  * 192.168.3.2, from 192.168.3.2, 00:10:18 ago, via Serial0/1
      Route metric is 20514560, traffic share count is 1
      Total delay is 20100 microseconds, minimum bandwidth is 128 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

Analysis: The feasible successor process was shown during the experiment. The method of changing cost for a route through manipulation of link bandwidth was also demonstrated. It was also shown that feasible successor routes are not used to forward traffic automatically.

Conclusion: This experiment demonstrates the feasible successor selection process. It further shows how link cost can be modified to influence the selection process.

6.2.8 Equal path Load Balancing

Aim: To demonstrate Equal Path Load Balancing

Figure 6.8 – Network topology for experiment 6.2.8

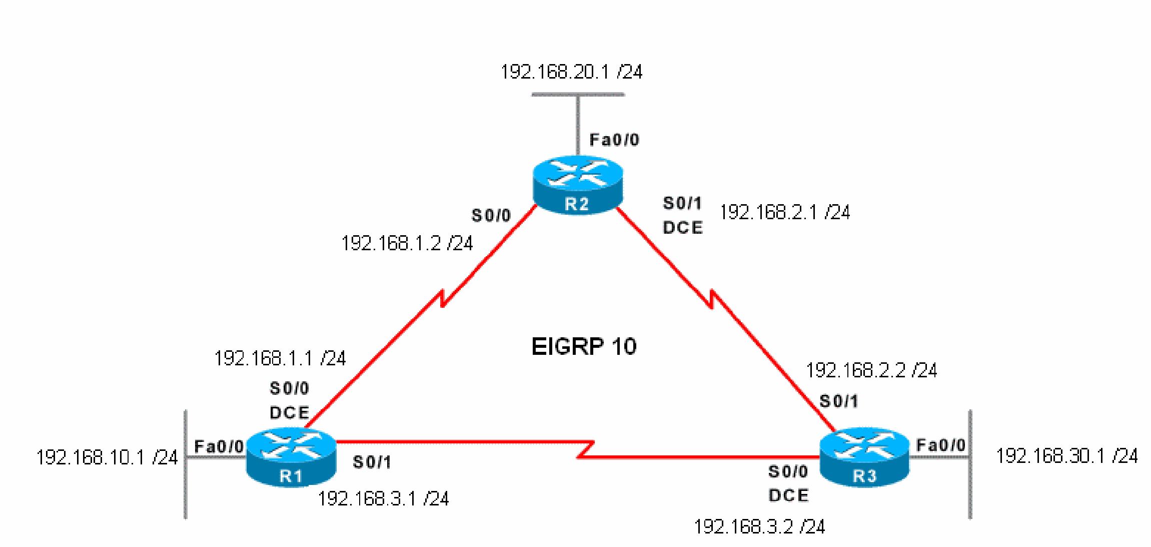


Table 6.8 – Router Configuration for Experiment 6.2.8

Configuration for Router R1

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R1
R1(config)#interface serial 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)#clockrate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/1
R1(config-if)# ip address 192.168.3.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fa 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router eigrp 10
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.3.0
R1(config-router)#network 192.168.10.0
```

Configuration for Router R2

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R2
R2(config)#interface serial 0/0
R2(config-if)# ip address 192.168.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface serial 0/1
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)#clockrate 64000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface fa 0/0
R2(config-if)# ip address 192.168.20.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router eigrp 10
R2(config-router)#network 192.168.1.0
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.20.0
```

Configuration for Router R3

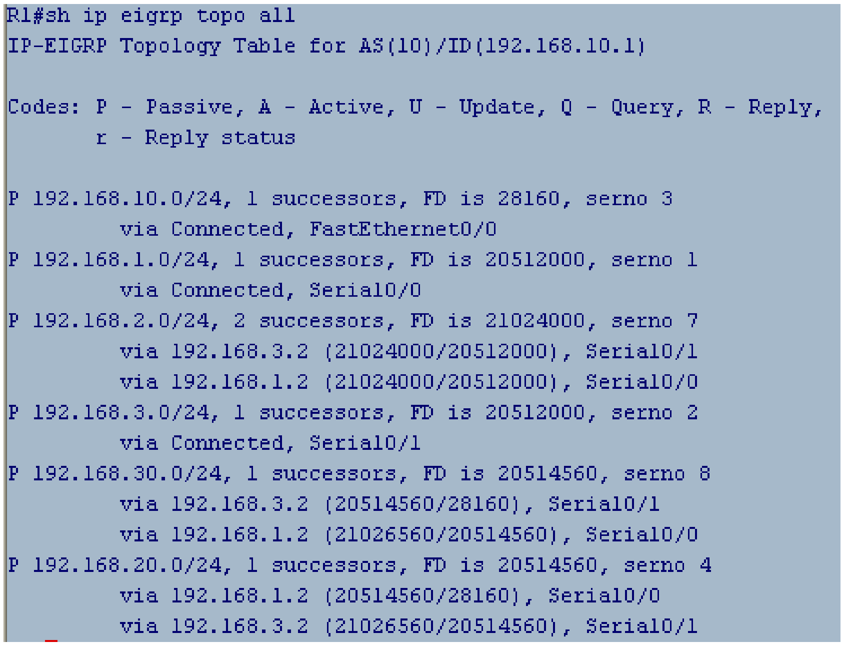
```
Router>enable
Router#conFigure terminal
Router(config)#hostname R3
R3(config)#interface serial 0/0
R3(config-if)# ip address 192.168.3.2 255.255.255.0
```

```
R3(config-if)#clockrate 64000
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface serial 0/1
R3(config-if)# ip address 192.168.2.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface fa 0/0
R3(config-if)# ip address 192.168.30.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router eigrp 10
R3(config-router)#network 192.168.2.0
R3(config-router)#network 192.168.3.0
R3(config-router)#network 192.168.30.0
```

Description/Procedure: The routers will be configured according to the network topology diagram and the configurations given in Figure 6.8 and Table 6.8. Once the network has converged the show IP route and Show IP EIGRP Topology all-link commands will be used to show the possible routes to destinations and theirs costs. As show in the topology Router R1 has two routes via which it can get to network 192.168.2.0. As both routes have only one hop and the links are the same the cost for both routes will also be the same. This fact will be verified using the outputs obtained from the router. Show IP route will be used to show that both routes are automatically installed into the routing Table because they have the same cost. Multiple packets will be sent to a destination on 192.168.2.0 network to show that EIGRP uses both the links to forward packets.

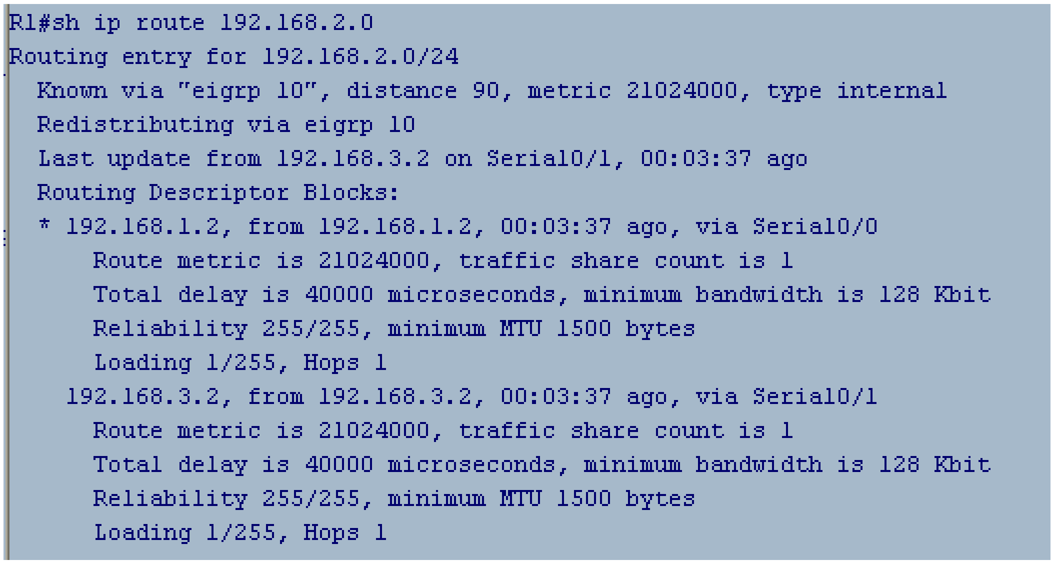
Result: The following screenshot shows the topology Table of Router R1 along with all the links that were learned by the router. It can be seen that destination

192.168.2.0 has two routes that can be used to reach it. Both of the routes have the same cost.



```
R1#sh ip eigrp topo all
IP-EIGRP Topology Table for AS(10)/ID(192.168.10.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.10.0/24, 1 successors, FD is 28160, serno 3
         via Connected, FastEthernet0/0
P 192.168.1.0/24, 1 successors, FD is 20512000, serno 1
         via Connected, Serial0/0
P 192.168.2.0/24, 2 successors, FD is 21024000, serno 7
         via 192.168.3.2 (21024000/20512000), Serial0/1
         via 192.168.1.2 (21024000/20512000), Serial0/0
P 192.168.3.0/24, 1 successors, FD is 20512000, serno 2
         via Connected, Serial0/1
P 192.168.30.0/24, 1 successors, FD is 20514560, serno 8
         via 192.168.3.2 (20514560/28160), Serial0/1
         via 192.168.1.2 (21026560/20514560), Serial0/0
P 192.168.20.0/24, 1 successors, FD is 20514560, serno 4
         via 192.168.1.2 (20514560/28160), Serial0/0
         via 192.168.3.2 (21026560/20514560), Serial0/1
```

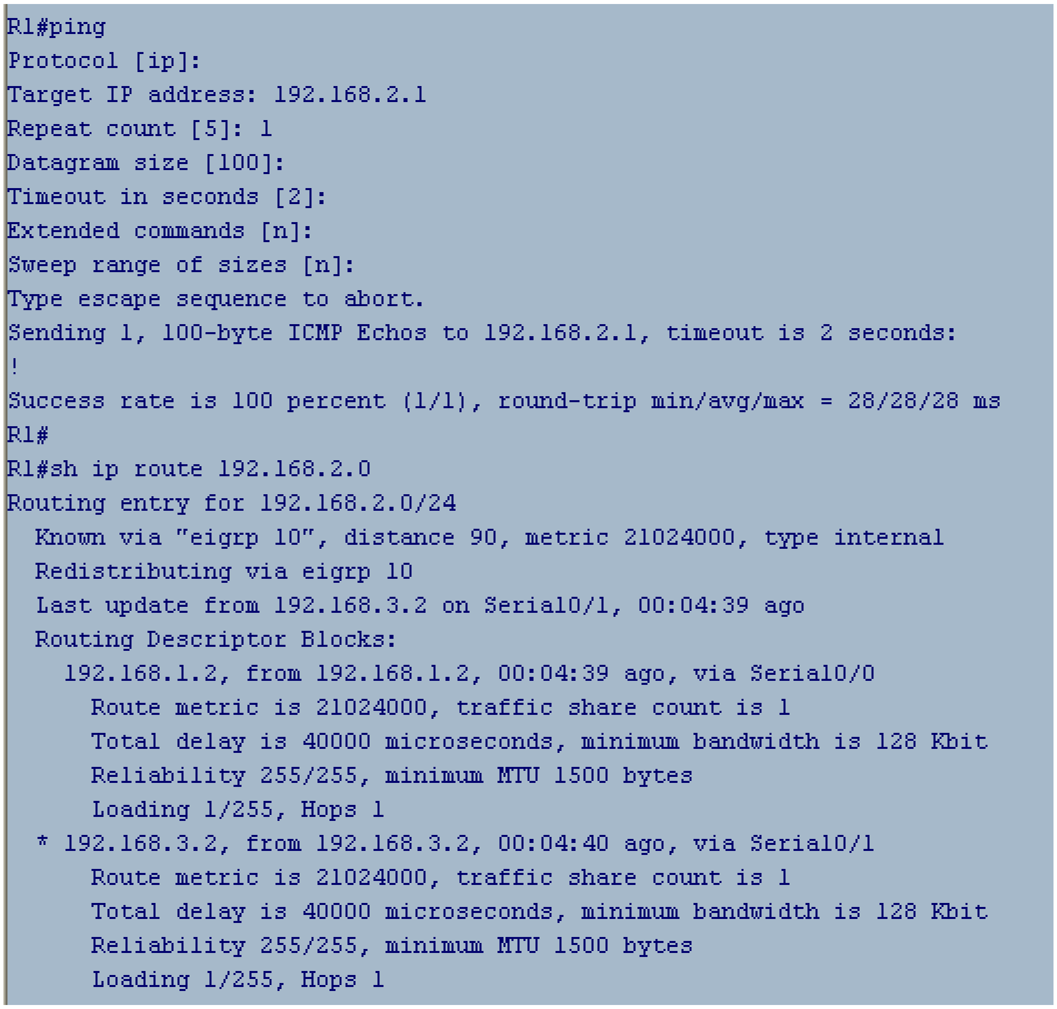
The following screenshot shows the routes to destination network 192.168.2.0 from Router R1. This proves that DUAL selected both equal path routes designate the successor routes and placed them in the routing Table.



```
R1#sh ip route 192.168.2.0
Routing entry for 192.168.2.0/24
  Known via "eigrp 10", distance 90, metric 21024000, type internal
  Redistributing via eigrp 10
  Last update from 192.168.3.2 on Serial0/1, 00:03:37 ago
  Routing Descriptor Blocks:
  * 192.168.1.2, from 192.168.1.2, 00:03:37 ago, via Serial0/0
      Route metric is 21024000, traffic share count is 1
      Total delay is 40000 microseconds, minimum bandwidth is 128 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
    192.168.3.2, from 192.168.3.2, 00:03:37 ago, via Serial0/1
      Route metric is 21024000, traffic share count is 1
      Total delay is 40000 microseconds, minimum bandwidth is 128 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

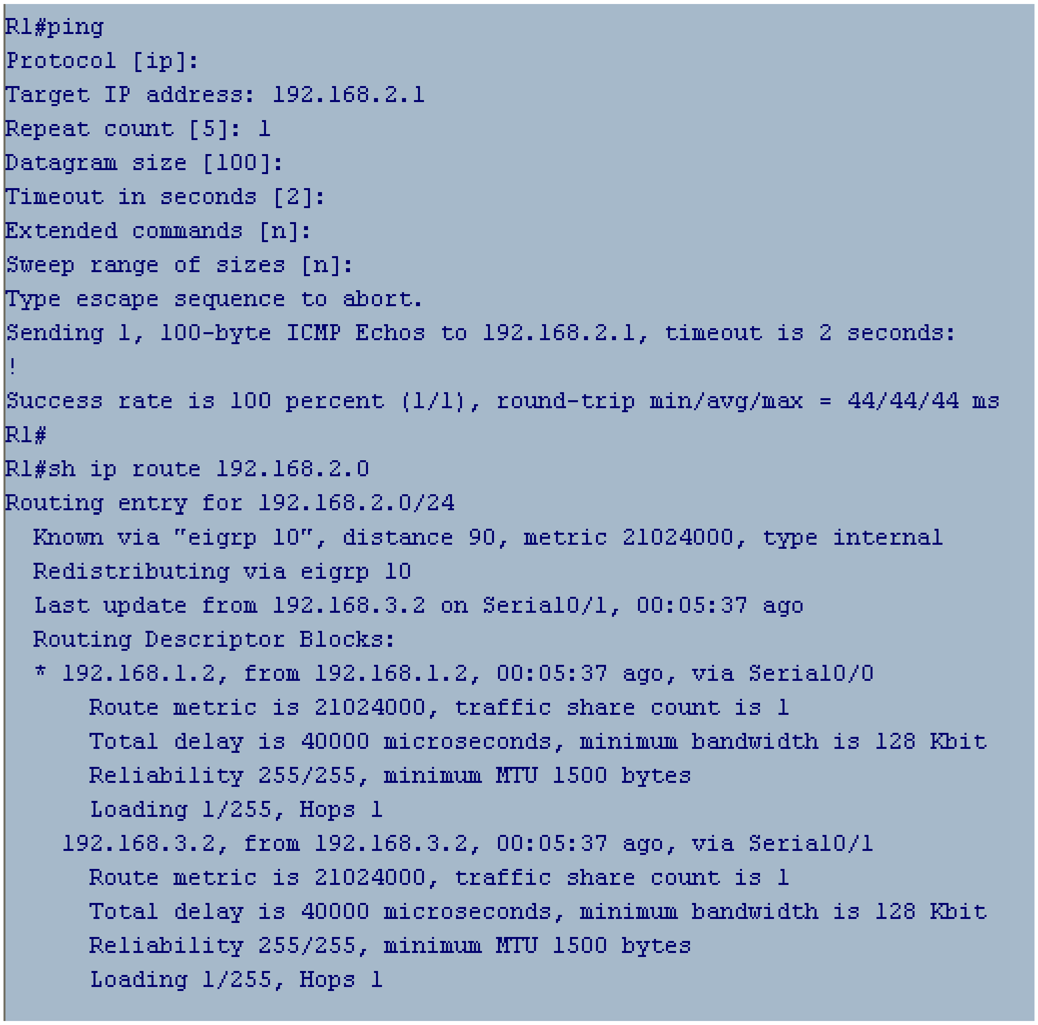
In the above screen it can be seen that the traffic share count for both routes is 1. Traffic share count it the proportion of traffic each route will get. This is decided by EIGRP on the cost of the route. As both routes have equal cost they will get an equal share of the traffic.

The followings screen shows then after a packet is sent the router marks the other route with the "*", meaning that this route will now be used.



```
R1#ping
Protocol [ip]:
Target IP address: 192.168.2.1
Repeat count [5]: 1
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 28/28/28 ms
R1#
R1#sh ip route 192.168.2.0
Routing entry for 192.168.2.0/24
  Known via "eigrp 10", distance 90, metric 21024000, type internal
  Redistributing via eigrp 10
  Last update from 192.168.3.2 on Serial0/1, 00:04:39 ago
  Routing Descriptor Blocks:
    192.168.1.2, from 192.168.1.2, 00:04:39 ago, via Serial0/0
      Route metric is 21024000, traffic share count is 1
      Total delay is 40000 microseconds, minimum bandwidth is 128 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
  * 192.168.3.2, from 192.168.3.2, 00:04:40 ago, via Serial0/1
      Route metric is 21024000, traffic share count is 1
      Total delay is 40000 microseconds, minimum bandwidth is 128 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

The following screenshot shows that sending another packet to the destination causes the router to use to the other route. Router is giving a 1:1 share of traffic to each of the routes.



```
R1#ping
Protocol [ip]:
Target IP address: 192.168.2.1
Repeat count [5]: 1
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 44/44/44 ms
R1#
R1#sh ip route 192.168.2.0
Routing entry for 192.168.2.0/24
  Known via "eigrp 10", distance 90, metric 21024000, type internal
  Redistributing via eigrp 10
  Last update from 192.168.3.2 on Serial0/1, 00:05:37 ago
  Routing Descriptor Blocks:
  * 192.168.1.2, from 192.168.1.2, 00:05:37 ago, via Serial0/0
      Route metric is 21024000, traffic share count is 1
      Total delay is 40000 microseconds, minimum bandwidth is 128 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
    192.168.3.2, from 192.168.3.2, 00:05:37 ago, via Serial0/1
      Route metric is 21024000, traffic share count is 1
      Total delay is 40000 microseconds, minimum bandwidth is 128 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

Analysis: This experiment shows that EIGRP routers select load balance of equal cost paths by default. The traffic between the two paths is divided as a ratio of 1:1 because both routes have the same cost.

Conclusion: Load balancing over equal cost paths happens automatically in EIGRP and the traffic is shared equally between them.

6.2.9 Unequal path load balancing

Aim: To demonstrate Unequal Path load balancing requirements and process of EIGRP

Figure 6.9 – Network topology for experiment 6.2.9

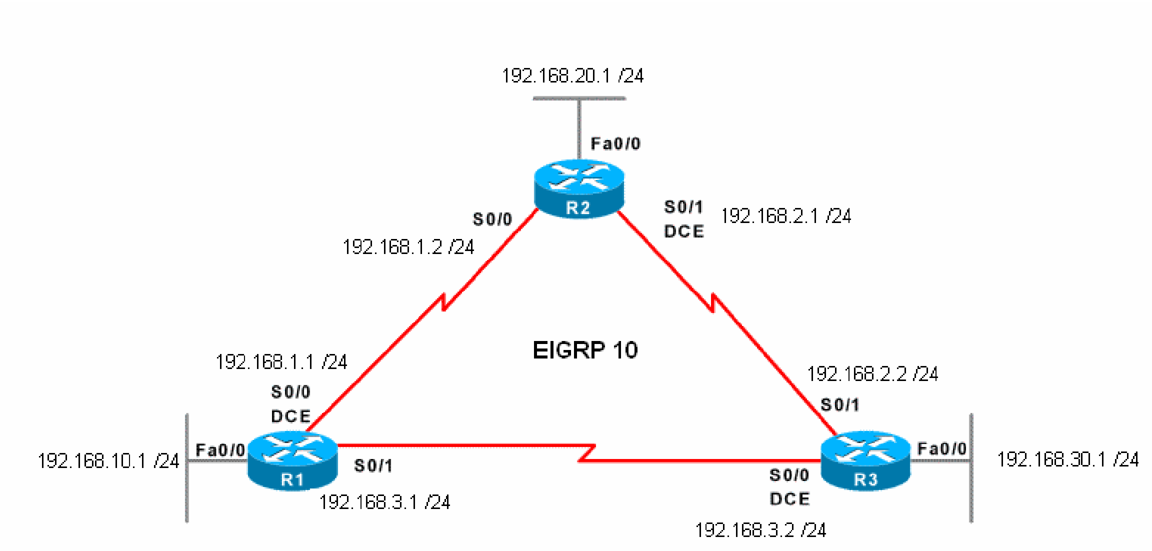


Table 6.9 – Router Configuration for Experiment 6.2.9

Configuration for Router R1

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R1
R1(config)#interface serial 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)#clockrate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/1
R1(config-if)# ip address 192.168.3.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fa 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router eigrp 10
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.3.0
R1(config-router)#network 192.168.10.0
```

Configuration for Router R2

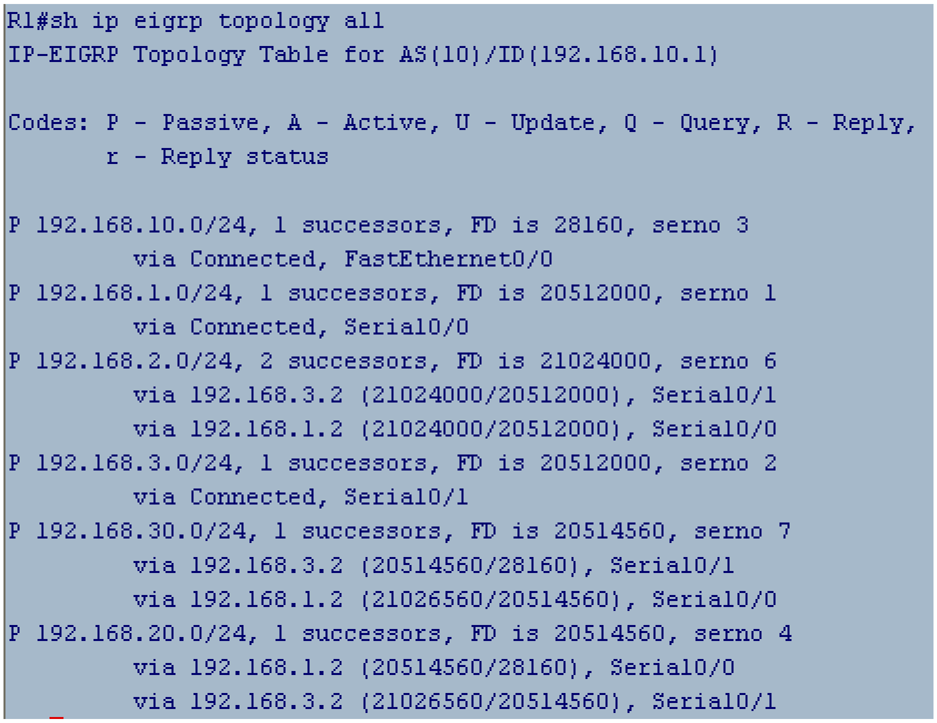
```
Router>enable
Router#conFigure terminal
Router(config)#hostname R2
R2(config)#interface serial 0/0
R2(config-if)# ip address 192.168.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface serial 0/1
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)#clockrate 64000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface fa 0/0
R2(config-if)# ip address 192.168.20.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router eigrp 10
R2(config-router)#network 192.168.1.0
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.20.0
```

Configuration for Router R3

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R3
R3(config)#interface serial 0/0
R3(config-if)# ip address 192.168.3.2 255.255.255.0
R3(config-if)#clockrate 64000
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface serial 0/1
R3(config-if)# ip address 192.168.2.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface fa 0/0
R3(config-if)# ip address 192.168.30.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router eigrp 10
R3(config-router)#network 192.168.2.0
R3(config-router)#network 192.168.3.0
R3(config-router)#network 192.168.30.0
```

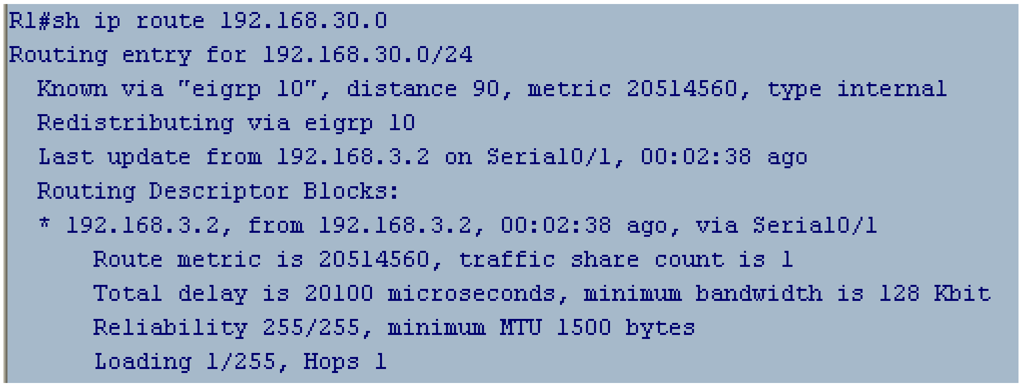
Description/Procedure: The routers will be configured according to the network topology diagram and the configurations given in Figure 6.9 and Table 6.9. Once the network has converged the show IP route and Show IP EIGRP Topology all-link commands will be used to show the possible routes to destinations and theirs costs. It will be seen that Router R1 has two paths to the destination 192.168.30.1 and chooses the link through Router R3 to reach the destination. The link through R2 will not be selected as the FS because it does not meet the feasibility condition. The reported distance to destination 192.168.30.1 through Router R2 is equal to the feasible distance. EIGRP requires the reported distance of a route to be less then the current feasible distance to meet the feasibility condition. After this has been shown, the total cost to destination 192.168.30.1 through R2 will be calculated. Appropriate variance N value would be used so that EIGRP takes any route up to the cost of route through Router R2. It will however be seen that the route through R2 will not be used to load balance or be installed into the routing Table. This is because EIGRP will only load balance using Successor and feasible successor even with variance command configured. This feature of EIGRP allows it to avoid and loops in the network. The reported distance of R2 will be changed so that the route through R2 become meets the feasibility condition and becomes a feasible successor. Once route through R2 becomes feasible successor, EIGRP should install this route and start load balancing over it. The traffic share between the routes will be proportional to the cost of the routes. At this point the metric can be changed to verify that the traffic share over the links change.

Result: The following screenshot shows the topology Table of Router R1 along with all the routes learnt by the router. From the Table it can be seen that there are two routes for destination network 192.169.30.0. The first route has a total cost of 20514560 and the second route has a total cost of 212026560. The second route is 1.03 times more expansive then the first route.



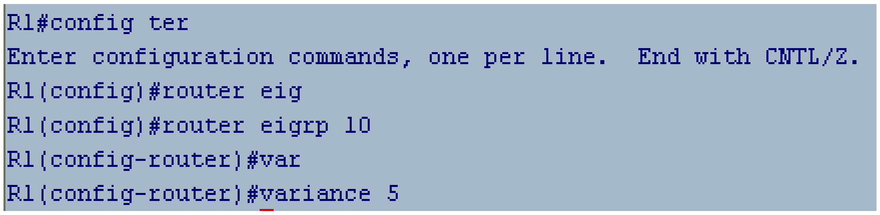
```
R1#sh ip eigrp topology all
IP-EIGRP Topology Table for AS(10)/ID(192.168.10.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.10.0/24, 1 successors, FD is 28160, serno 3
         via Connected, FastEthernet0/0
P 192.168.1.0/24, 1 successors, FD is 20512000, serno 1
         via Connected, Serial0/0
P 192.168.2.0/24, 2 successors, FD is 21024000, serno 6
         via 192.168.3.2 (21024000/20512000), Serial0/1
         via 192.168.1.2 (21024000/20512000), Serial0/0
P 192.168.3.0/24, 1 successors, FD is 20512000, serno 2
         via Connected, Serial0/1
P 192.168.30.0/24, 1 successors, FD is 20514560, serno 7
         via 192.168.3.2 (20514560/28160), Serial0/1
         via 192.168.1.2 (21026560/20514560), Serial0/0
P 192.168.20.0/24, 1 successors, FD is 20514560, serno 4
         via 192.168.1.2 (20514560/28160), Serial0/0
         via 192.168.3.2 (21026560/20514560), Serial0/1
```

The following screenshot shows that the least cost path route has been installed by DUAL into the routing Table which is being used to forward traffic to the destination.



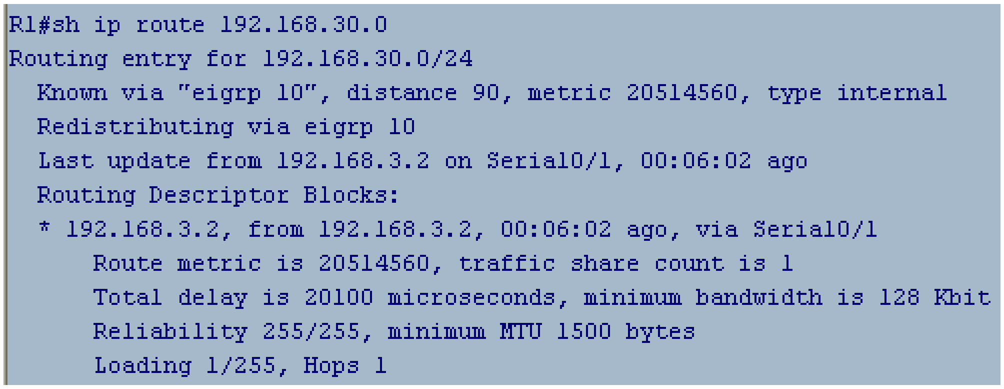
```
R1#sh ip route 192.168.30.0
Routing entry for 192.168.30.0/24
  Known via "eigrp 10", distance 90, metric 20514560, type internal
  Redistributing via eigrp 10
  Last update from 192.168.3.2 on Serial0/1, 00:02:38 ago
  Routing Descriptor Blocks:
  * 192.168.3.2, from 192.168.3.2, 00:02:38 ago, via Serial0/1
      Route metric is 20514560, traffic share count is 1
      Total delay is 20100 microseconds, minimum bandwidth is 128 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

The variance command is configured on the router as show below with the value of n as 5. This should allow all routes up to 5 times the least cost route to be selected.



```
R1#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router eig
R1(config)#router eigrp 10
R1(config-router)#var
R1(config-router)#variance 5
```

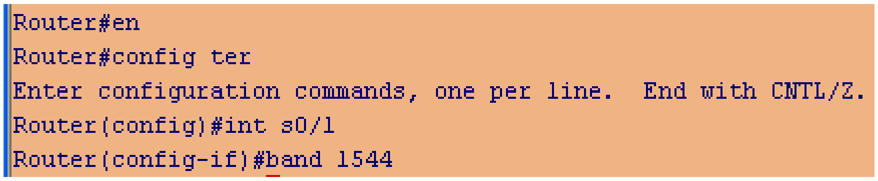
After the variance command was issued the route installed for destination 192.169.30.0 is checked. The screenshot below shows the installed route.



```
R1#sh ip route 192.168.30.0
Routing entry for 192.168.30.0/24
  Known via "eigrp 10", distance 90, metric 20514560, type internal
  Redistributing via eigrp 10
  Last update from 192.168.3.2 on Serial0/1, 00:06:02 ago
  Routing Descriptor Blocks:
  * 192.168.3.2, from 192.168.3.2, 00:06:02 ago, via Serial0/1
      Route metric is 20514560, traffic share count is 1
      Total delay is 20100 microseconds, minimum bandwidth is 128 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

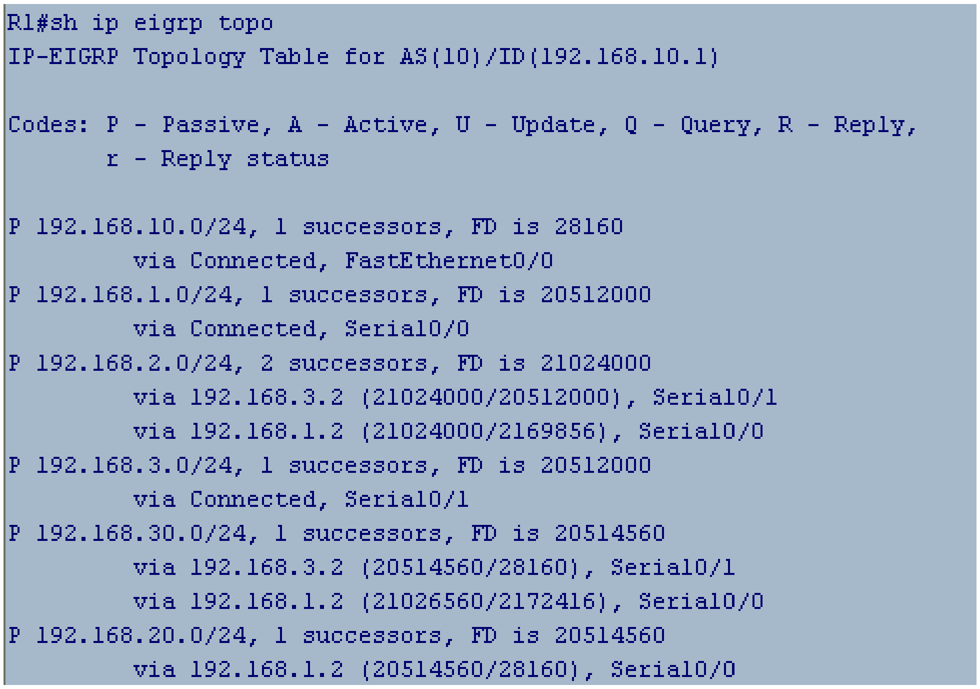
Despite being with in the range of the variance command the second route has not been installed because it does not meet the feasibility condition and does not qualify as a feasible successor.

The following screenshot shows the configuration that is used to change the bandwidth of the link on Router R2 to the destination so that the second route through router R2 qualifies as feasible successor.



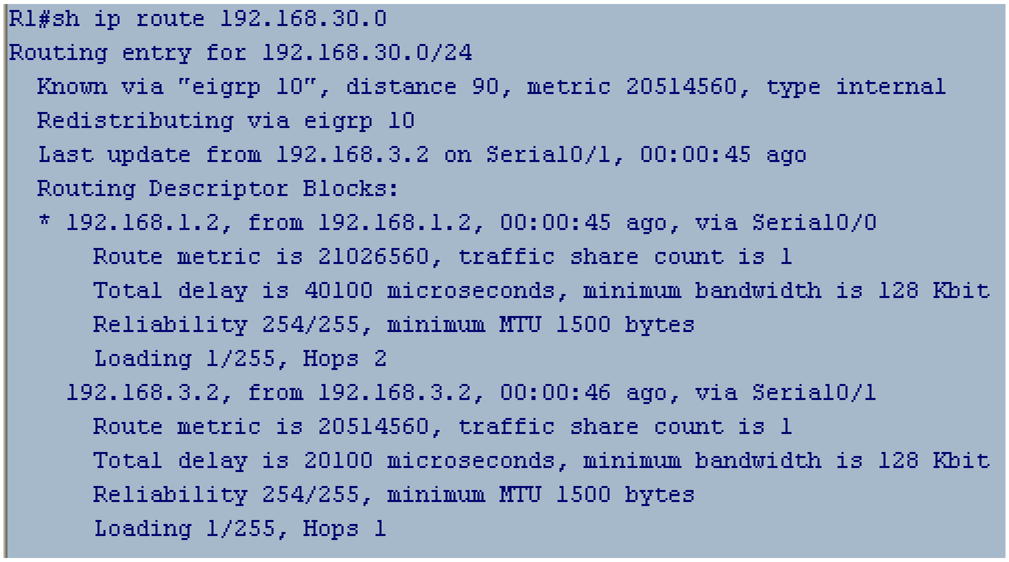
```
Router#en
Router#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int s0/1
Router(config-if)#band 1544
```

The screenshot shown below confirms that the cost of the second route has changed and now it qualifies as a feasible successor.



```
R1#sh ip eigrp topo
IP-EIGRP Topology Table for AS(10)/ID(192.168.10.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.10.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 192.168.1.0/24, 1 successors, FD is 20512000
         via Connected, Serial0/0
P 192.168.2.0/24, 2 successors, FD is 21024000
         via 192.168.3.2 (21024000/20512000), Serial0/1
         via 192.168.1.2 (21024000/2169856), Serial0/0
P 192.168.3.0/24, 1 successors, FD is 20512000
         via Connected, Serial0/1
P 192.168.30.0/24, 1 successors, FD is 20514560
         via 192.168.3.2 (20514560/28160), Serial0/1
         via 192.168.1.2 (21026560/2172416), Serial0/0
P 192.168.20.0/24, 1 successors, FD is 20514560
         via 192.168.1.2 (20514560/28160), Serial0/0
```

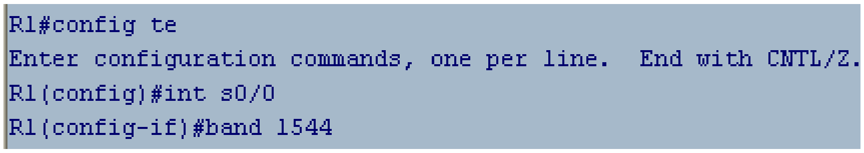
The next screenshot shows that after the route qualifies as a feasible successor it gets installed into the routing Table and there are now two routes available to router R2 to reach destination.



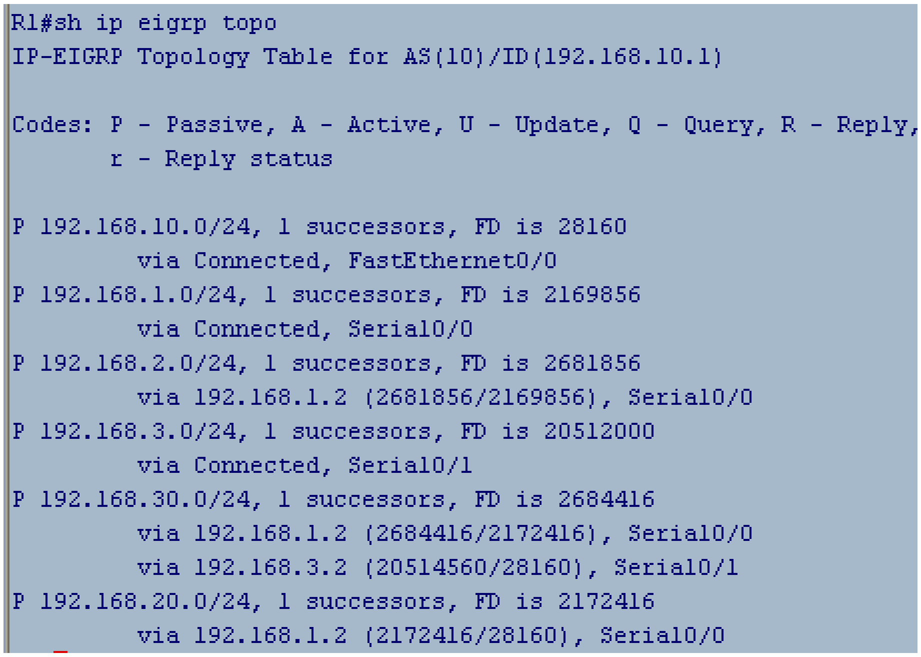
```
R1#sh ip route 192.168.30.0
Routing entry for 192.168.30.0/24
  Known via "eigrp 10", distance 90, metric 20514560, type internal
  Redistributing via eigrp 10
  Last update from 192.168.3.2 on Serial0/1, 00:00:45 ago
  Routing Descriptor Blocks:
  * 192.168.1.2, from 192.168.1.2, 00:00:45 ago, via Serial0/0
      Route metric is 21026560, traffic share count is 1
      Total delay is 40100 microseconds, minimum bandwidth is 128 Kbit
      Reliability 254/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2
    192.168.3.2, from 192.168.3.2, 00:00:46 ago, via Serial0/1
      Route metric is 20514560, traffic share count is 1
      Total delay is 20100 microseconds, minimum bandwidth is 128 Kbit
      Reliability 254/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

The above screenshot shows that both routes have been installed and are being actively used by the router to forward packet. As they both have a cost ratio of 1:1 (rounded to the nearest integer) they will have equal share of traffic. This is shown by the traffic share proportion shown next to the routes.

The following screen shows manipulation of the route costs to change the successor and the feasible successor. In the screenshot shown below it can be seen that there is a successor and feasible successor present. The cost of the feasible successor route is 7 times more then the cost of the successor route.

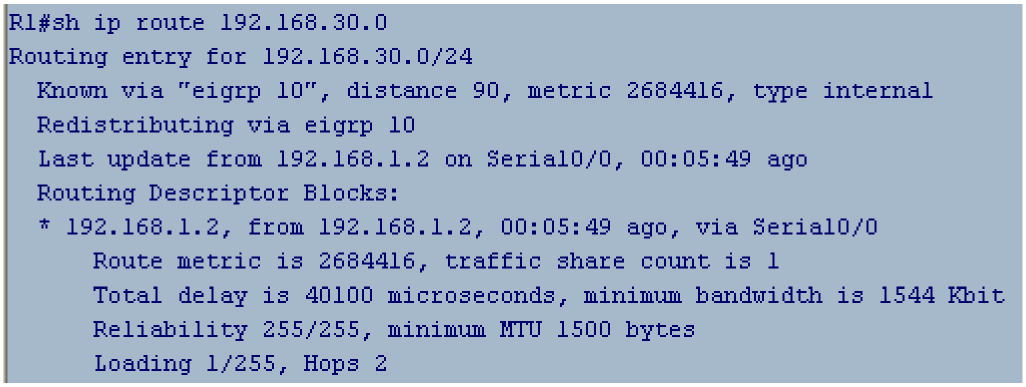


```
R1#config te
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int s0/0
R1(config-if)#band 1544
```



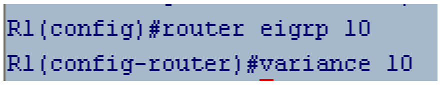
```
R1#sh ip eigrp topo
IP-EIGRP Topology Table for AS(10)/ID(192.168.10.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.10.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 192.168.1.0/24, 1 successors, FD is 2169856
         via Connected, Serial0/0
P 192.168.2.0/24, 1 successors, FD is 2681856
         via 192.168.1.2 (2681856/2169856), Serial0/0
P 192.168.3.0/24, 1 successors, FD is 20512000
         via Connected, Serial0/1
P 192.168.30.0/24, 1 successors, FD is 2684416
         via 192.168.1.2 (2684416/2172416), Serial0/0
         via 192.168.3.2 (20514560/28160), Serial0/1
P 192.168.20.0/24, 1 successors, FD is 2172416
         via 192.168.1.2 (2172416/28160), Serial0/0
```

Although the route via router R3 to destination qualifies as a feasible successor it will not be added to the routing Table because it has 7 times higher cost then the successor. The variance command currently configured will load balance using routes up to 5 times the cost of the successor route.



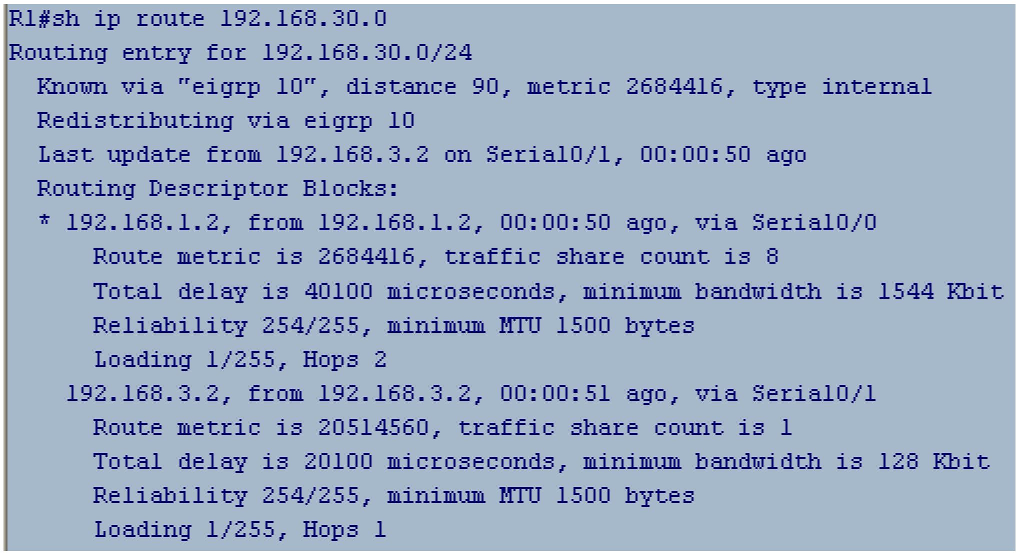
```
R1#sh ip route 192.168.30.0
Routing entry for 192.168.30.0/24
  Known via "eigrp 10", distance 90, metric 2684416, type internal
  Redistributing via eigrp 10
  Last update from 192.168.1.2 on Serial0/0, 00:05:49 ago
  Routing Descriptor Blocks:
  * 192.168.1.2, from 192.168.1.2, 00:05:49 ago, via Serial0/0
      Route metric is 2684416, traffic share count is 1
      Total delay is 40100 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2
```

The following screenshot shows the variance command being increased so that the router load balanced using routes up to 10 times the cost of the successor.



```
R1(config)#router eigrp 10
R1(config-router)#variance 10
```

The following screenshot shows that once the variance 10 command has been issued the FS with 8 times the cost of the successor is also added to the routing Table. By default the traffic share will be proportional to the route cost. In the screen it can be seen that the successor will get 8 times more traffic through its route because it is 8 times cheaper then the feasible successor.



```
R1#sh ip route 192.168.30.0
Routing entry for 192.168.30.0/24
  Known via "eigrp 10", distance 90, metric 2684416, type internal
  Redistributing via eigrp 10
  Last update from 192.168.3.2 on Serial0/1, 00:00:50 ago
  Routing Descriptor Blocks:
  * 192.168.1.2, from 192.168.1.2, 00:00:50 ago, via Serial0/0
      Route metric is 2684416, traffic share count is 8
      Total delay is 40100 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 254/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2
    192.168.3.2, from 192.168.3.2, 00:00:51 ago, via Serial0/1
      Route metric is 20514560, traffic share count is 1
      Total delay is 20100 microseconds, minimum bandwidth is 128 Kbit
      Reliability 254/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

Analysis: The experiment shows that unequal path load balancing can be done using EIGRP routing protocol. To be selected as one of the routes which will be used for load balancing, a route must satisfy the feasibility condition. By default EIGRP shares traffic proportionate to the cost of the route. This can however be changed by issuing **traffic-share balanced** command. The **min-traffic share** command can also be used to install all the routes according to the variance rule but, traffic will only be sent using the least cost path. This is useful because is case of successor failure the router can switch to the alternate route already present in the routing Table.

Conclusion: The experiment successfully shows the requirement a route must meet to become one of the load balanced paths. The process and the configuration that can be used to manipulate the outcomes have also been explained.

6.2.10 Local Computation

Aim: The demonstrate the local computation process taking place on an EIGRP network

Figure 6.10 – Network topology for experiment 6.2.10

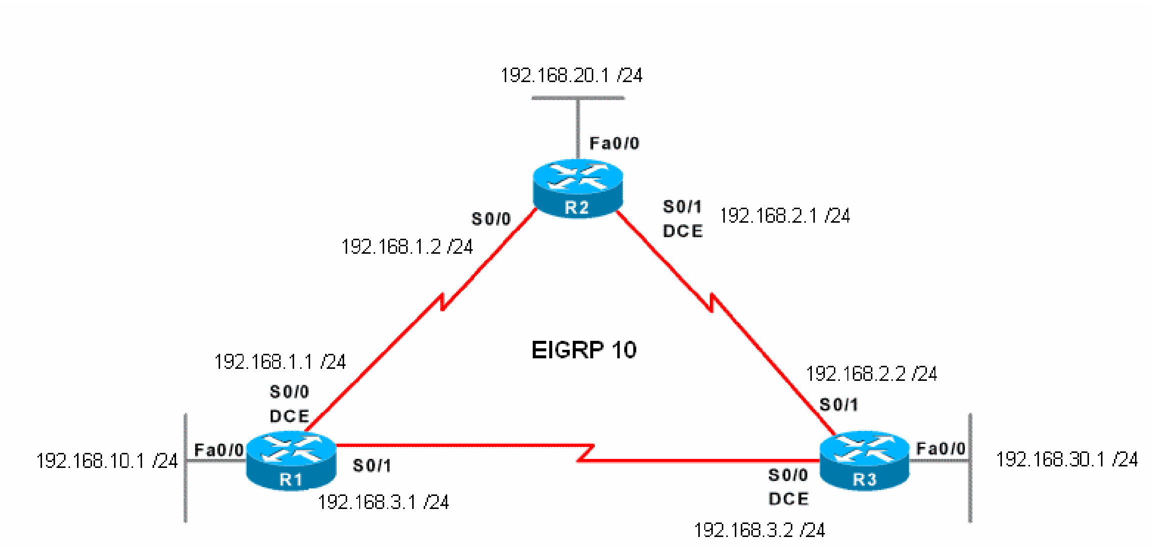


Table 6.10 – Router Configuration for Experiment 6.2.10

Configuration for Router R1

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R1
R1(config)#interface serial 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)#clockrate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/1
R1(config-if)# ip address 192.168.3.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fa 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router eigrp 10
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.3.0
R1(config-router)#network 192.168.10.0
```

Configuration for Router R2

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R2
R2(config)#interface serial 0/0
R2(config-if)# ip address 192.168.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface serial 0/1
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)#clockrate 64000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface fa 0/0
R2(config-if)# ip address 192.168.20.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router eigrp 10
R2(config-router)#network 192.168.1.0
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.20.0
```

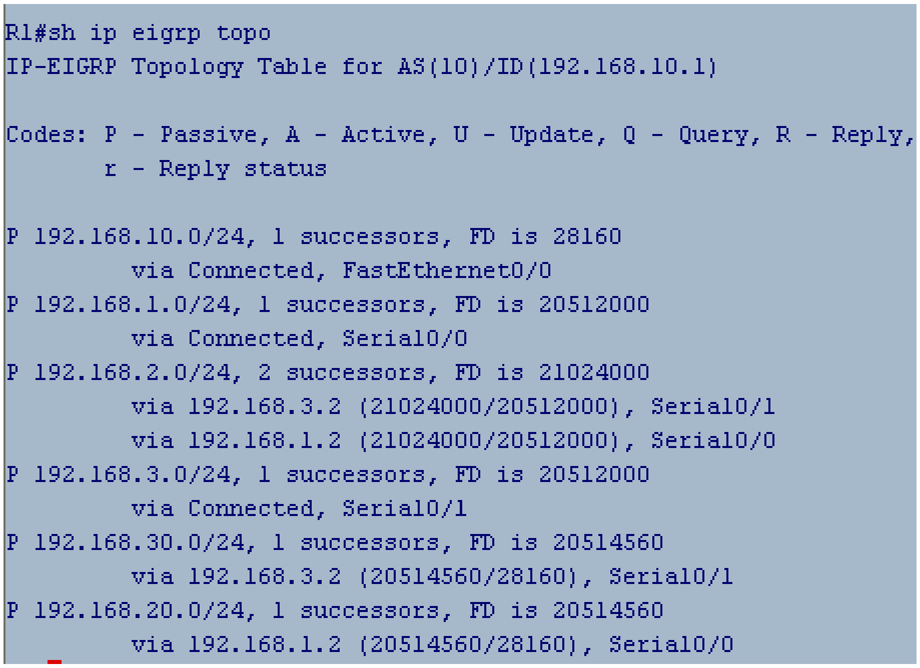
Configuration for Router R3

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R3
R3(config)#interface serial 0/0
R3(config-if)# ip address 192.168.3.2 255.255.255.0
R3(config-if)#clockrate 64000
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface serial 0/1
```

```
R3(config-if)# ip address 192.168.2.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface fa 0/0
R3(config-if)# ip address 192.168.30.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router eigrp 10
R3(config-router)#network 192.168.2.0
R3(config-router)#network 192.168.3.0
R3(config-router)#network 192.168.30.0
```

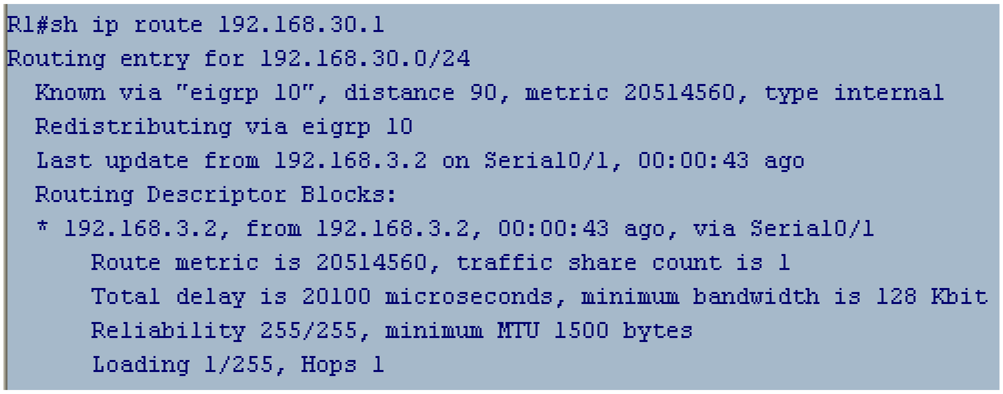
Description/Procedure: The configuration for the routers and the network topology are given in Table 6.10 and Figure 6.10. Once the network has converged the show IP route and Show IP EIGRP Topology all-link commands will be used to show the possible routes to destinations and theirs costs. It will be seen that Router R1 has two paths to the destination 192.168.30.1 and chooses the link through Router R3 to reach the destination. The link through R2 will not be selected as the FS because it does not meet the feasibility condition. The reported distance to destination 192.168.30.1 through Router R2 is equal to the feasible distance. EIGRP requires the reported distance of a route to be less then the current feasible distance to meet the feasibility condition. Once the destination 192.168.30.1 has a feasible successor, extended ping will be done from router R1 to destination. While the ping is taking place a simulated failure of the successor link will be done. This will cause EIGRP to perform recalculations for the route. It will be shown that because a FS was present EIGRP instantly switches over with minimum packet loss. Router R1 also does not send out any queries to router R2 for route information to destination 192.168.30.1. Debug commands will be used to estimate re-convergence times. Ping outputs will be used to show the number of packets lost and total time taken to send and receive reply for all the packets.

Result: The following screenshot shows the topology Table of Router R1 with all the successor and feasible successor routes for destinations known to the router. The Table shows that for destination 191.168.30.0 there is no feasible successor present.



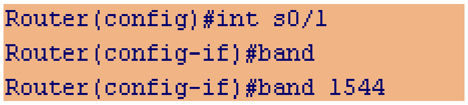
```
R1#sh ip eigrp topo
IP-EIGRP Topology Table for AS(10)/ID(192.168.10.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.10.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 192.168.1.0/24, 1 successors, FD is 20512000
         via Connected, Serial0/0
P 192.168.2.0/24, 2 successors, FD is 21024000
         via 192.168.3.2 (21024000/20512000), Serial0/1
         via 192.168.1.2 (21024000/20512000), Serial0/0
P 192.168.3.0/24, 1 successors, FD is 20512000
         via Connected, Serial0/1
P 192.168.30.0/24, 1 successors, FD is 20514560
         via 192.168.3.2 (20514560/28160), Serial0/1
P 192.168.20.0/24, 1 successors, FD is 20514560
         via 192.168.1.2 (20514560/28160), Serial0/0
```

The following screenshot showing the route to the destination also reveals this fact.



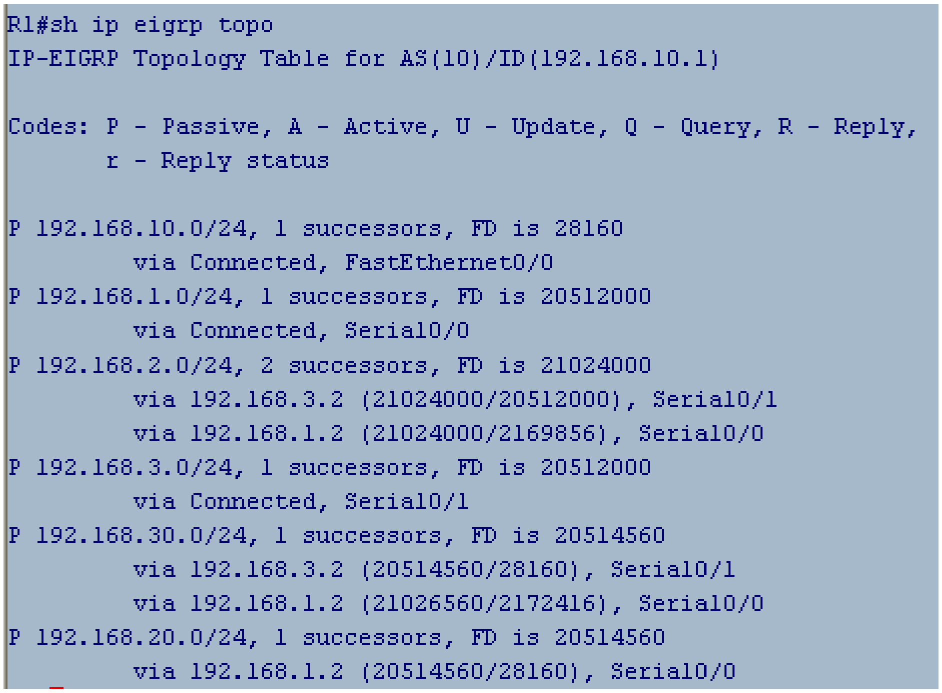
```
R1#sh ip route 192.168.30.1
Routing entry for 192.168.30.0/24
  Known via "eigrp 10", distance 90, metric 20514560, type internal
  Redistributing via eigrp 10
  Last update from 192.168.3.2 on Serial0/1, 00:00:43 ago
  Routing Descriptor Blocks:
  * 192.168.3.2, from 192.168.3.2, 00:00:43 ago, via Serial0/1
      Route metric is 20514560, traffic share count is 1
      Total delay is 20100 microseconds, minimum bandwidth is 128 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

The metric on serial 0/1 link of router R2 is changed so that the route to destination 192.168.30.0 through router R2 qualifies as a feasible successor. The configuration used the metric change is given below



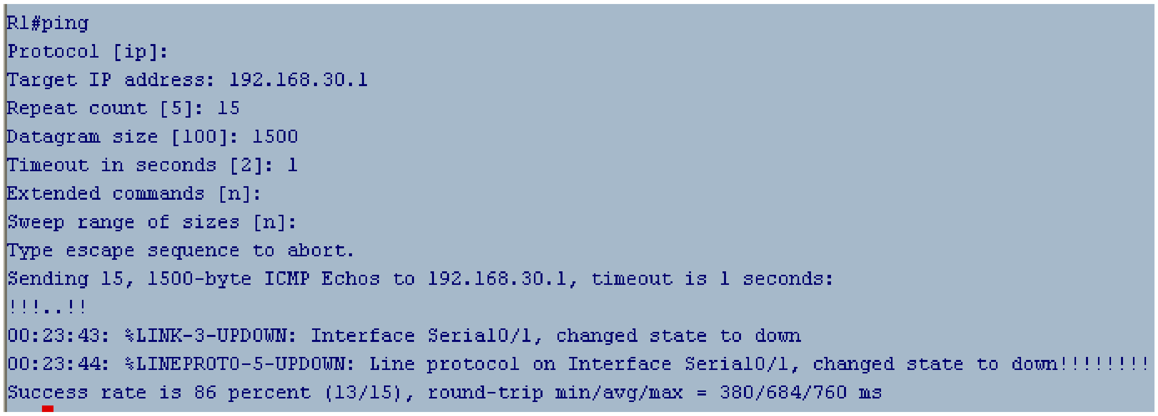
```
Router(config)#int s0/1
Router(config-if)#band
Router(config-if)#band 1544
```

The topology Table of Router R1 shown below confirms that due to the metric change, the route through Router R2 now qualifies as the feasible successor.



```
R1#sh ip eigrp topo
IP-EIGRP Topology Table for AS(10)/ID(192.168.10.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.10.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 192.168.1.0/24, 1 successors, FD is 20512000
         via Connected, Serial0/0
P 192.168.2.0/24, 2 successors, FD is 21024000
         via 192.168.3.2 (21024000/20512000), Serial0/1
         via 192.168.1.2 (21024000/2169856), Serial0/0
P 192.168.3.0/24, 1 successors, FD is 20512000
         via Connected, Serial0/1
P 192.168.30.0/24, 1 successors, FD is 20514560
         via 192.168.3.2 (20514560/28160), Serial0/1
         via 192.168.1.2 (21026560/2172416), Serial0/0
P 192.168.20.0/24, 1 successors, FD is 20514560
         via 192.168.1.2 (20514560/28160), Serial0/0
```

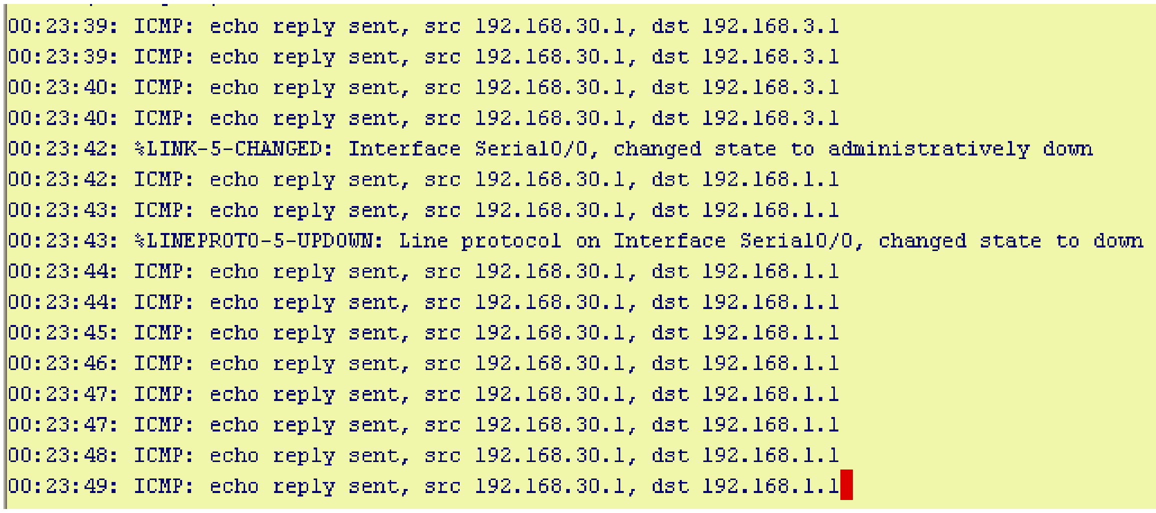
The following screen shot shows and extended ping is being sent to the destination from router R1. During the extended ping the successor route was made unavailable by administratively shutting the link down.



```
R1#ping
Protocol [ip]:
Target IP address: 192.168.30.1
Repeat count [5]: 15
Datagram size [100]: 1500
Timeout in seconds [2]: 1
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 15, 1500-byte ICMP Echos to 192.168.30.1, timeout is 1 seconds:
!!!..!!
00:23:43: %LINK-3-UPDOWN: Interface Serial0/1, changed state to down
00:23:44: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to down!!!!!!!!
Success rate is 86 percent (13/15), round-trip min/avg/max = 380/684/760 ms
```

The failure of the successor link caused the router to look for alternative route.

The following screen shows the debug output of the ICMP reply on router R3.



```
00:23:39: ICMP: echo reply sent, src 192.168.30.1, dst 192.168.3.1
00:23:39: ICMP: echo reply sent, src 192.168.30.1, dst 192.168.3.1
00:23:40: ICMP: echo reply sent, src 192.168.30.1, dst 192.168.3.1
00:23:40: ICMP: echo reply sent, src 192.168.30.1, dst 192.168.3.1
00:23:42: %LINK-5-CHANGED: Interface Serial0/0, changed state to administratively down
00:23:42: ICMP: echo reply sent, src 192.168.30.1, dst 192.168.1.1
00:23:43: ICMP: echo reply sent, src 192.168.30.1, dst 192.168.1.1
00:23:43: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to down
00:23:44: ICMP: echo reply sent, src 192.168.30.1, dst 192.168.1.1
00:23:44: ICMP: echo reply sent, src 192.168.30.1, dst 192.168.1.1
00:23:45: ICMP: echo reply sent, src 192.168.30.1, dst 192.168.1.1
00:23:46: ICMP: echo reply sent, src 192.168.30.1, dst 192.168.1.1
00:23:47: ICMP: echo reply sent, src 192.168.30.1, dst 192.168.1.1
00:23:47: ICMP: echo reply sent, src 192.168.30.1, dst 192.168.1.1
00:23:48: ICMP: echo reply sent, src 192.168.30.1, dst 192.168.1.1
00:23:49: ICMP: echo reply sent, src 192.168.30.1, dst 192.168.1.1
```

Analysis: From the above screenshots it can be seen that during the extended ping when the route failure was simulated, two of the packets were lost. This is the time that was taken by DUAL to switch over to the feasible successor route that was already present and installed. This two second delay is also confirmed by the fact that in the debug ICMP reply there is a two second gap between packets replied to at 00:23:40 and 00:23:42 by router R3.

Conclusion: From the experiment it was concluded that Local computation of DUAL took 2 seconds to find and install the feasible successor as successor so that the route could be used to forward traffic to the destination.

6.2.11 Diffusing Computation

Aim: The demonstrate the Diffusing computation taking place on an EIGRP network

Figure 6.11 – Network topology for experiment 6.2.11

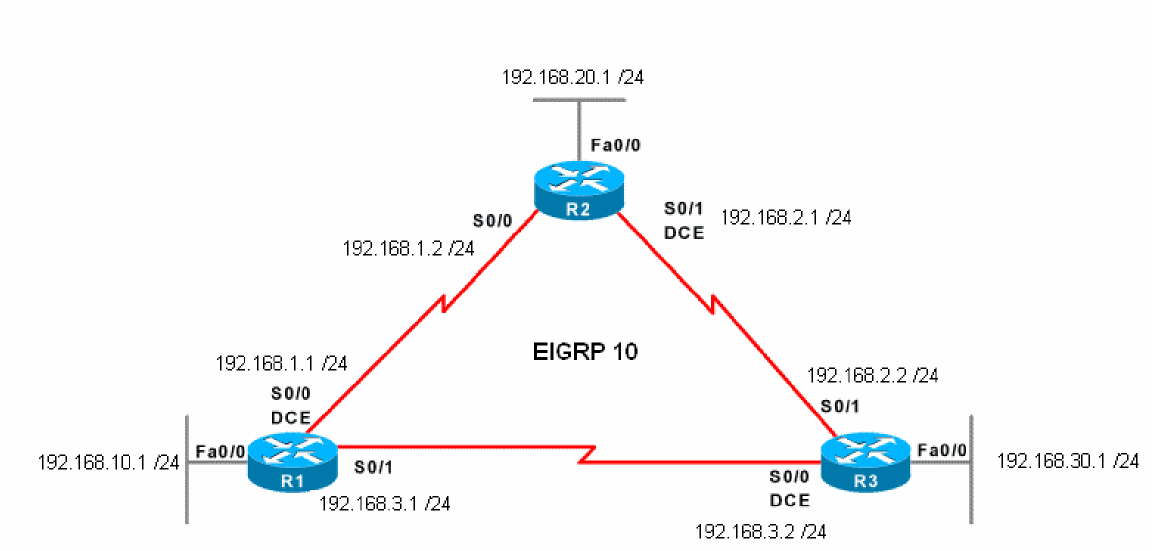


Table 6.11 – Router Configuration for Experiment 6.2.11

Configuration for Router R1

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R1
R1(config)#interface serial 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)#clockrate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/1
R1(config-if)# ip address 192.168.3.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fa 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router eigrp 10
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.3.0
R1(config-router)#network 192.168.10.0
```

Configuration for Router R2

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R2
R2(config)#interface serial 0/0
R2(config-if)# ip address 192.168.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface serial 0/1
R2(config-if)# ip address 192.168.2.1 255.255.255.0
```

```
R2(config-if)#clockrate 64000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface fa 0/0
R2(config-if)# ip address 192.168.20.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router eigrp 10
R2(config-router)#network 192.168.1.0
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.20.0
```

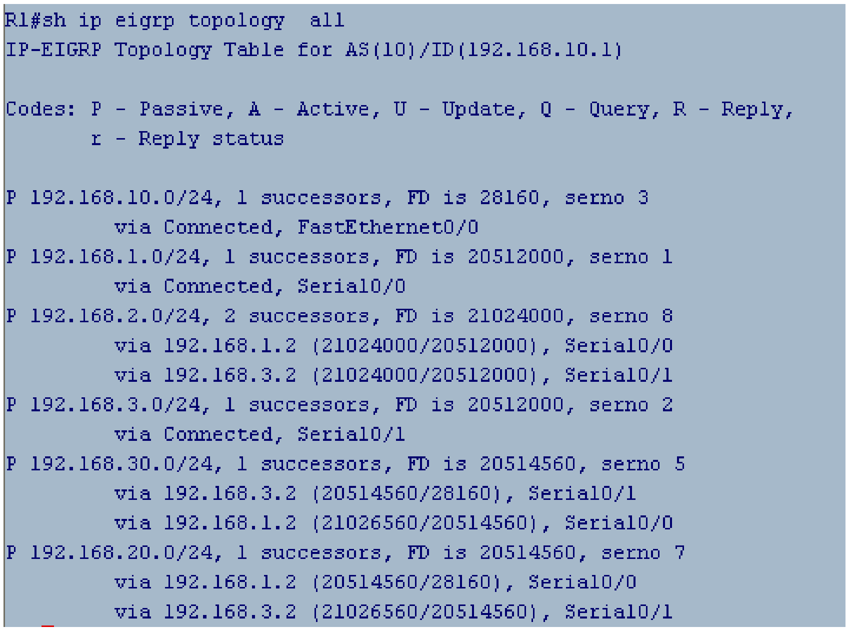
Configuration for Router R3

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R3
R3(config)#interface serial 0/0
R3(config-if)# ip address 192.168.3.2 255.255.255.0
R3(config-if)#clockrate 64000
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface serial 0/1
R3(config-if)# ip address 192.168.2.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface fa 0/0
R3(config-if)# ip address 192.168.30.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router eigrp 10
R3(config-router)#network 192.168.2.0
R3(config-router)#network 192.168.3.0
R3(config-router)#network 192.168.30.0
```

Description/Procedure: The routers will be configured according to the network topology diagram and the configurations given in Figure 6.11 and Table 6.11. Once the network has converged the show IP route and Show IP EIGRP Topology all-link commands will be used to show the possible routes to destinations and theirs costs. It will be seen that for the destination 192.168.30.1 from router R1, there only a successor route present through router R3. The Route through Router R2 does not meet the feasibility condition is not a feasible successor. Extended ping will be done from Router R1 to destination

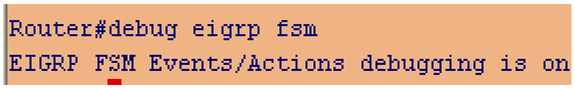
192.168.30.1 and simulation failure of the successor will be done. Through debug command placed on both router R1 and R3, the time taken for route re-computation will be estimated. The time taken for all the ICMP packets to be replied to and the number of packet losses will also be documented. These values will then be compared with the values obtained from previous experiment to see the difference in network convergence and performance during local and diffusing computation.

Result: The following screenshot of the topology Table of Router R1 shows that there is no feasible successor present for destination 192.168.30.0

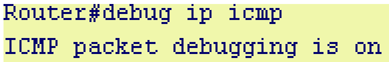


```
R1#sh ip eigrp topology  all
IP-EIGRP Topology Table for AS(10)/ID(192.168.10.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.10.0/24, 1 successors, FD is 28160, serno 3
         via Connected, FastEthernet0/0
P 192.168.1.0/24, 1 successors, FD is 20512000, serno 1
         via Connected, Serial0/0
P 192.168.2.0/24, 2 successors, FD is 21024000, serno 8
         via 192.168.1.2 (21024000/20512000), Serial0/0
         via 192.168.3.2 (21024000/20512000), Serial0/1
P 192.168.3.0/24, 1 successors, FD is 20512000, serno 2
         via Connected, Serial0/1
P 192.168.30.0/24, 1 successors, FD is 20514560, serno 5
         via 192.168.3.2 (20514560/28160), Serial0/1
         via 192.168.1.2 (21026560/20514560), Serial0/0
P 192.168.20.0/24, 1 successors, FD is 20514560, serno 7
         via 192.168.1.2 (20514560/28160), Serial0/0
         via 192.168.3.2 (21026560/20514560), Serial0/1
```

The debugging command that shows FSM calculations and ICMP packets are turned on as shown in the screen below.

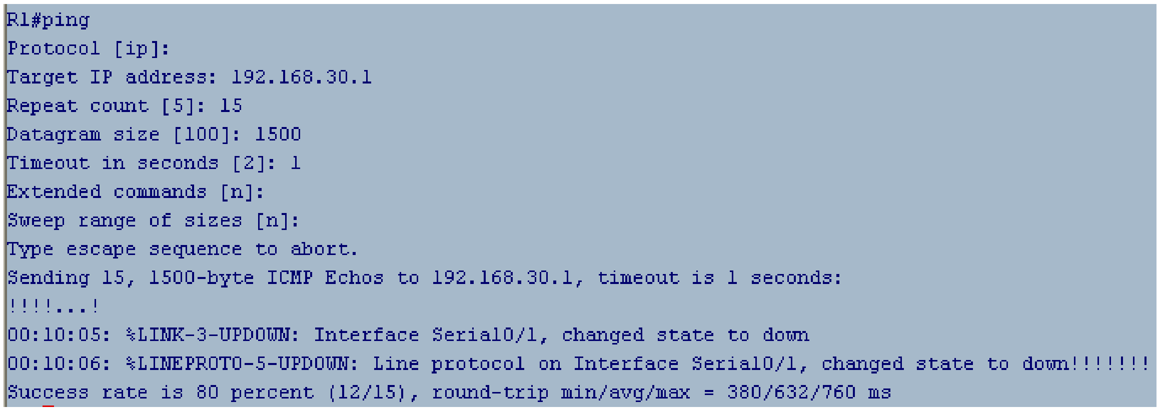


```
Router#debug eigrp fsm
EIGRP FSM Events/Actions debugging is on
```



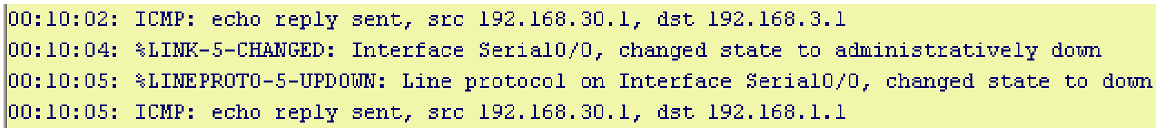
```
Router#debug ip icmp
ICMP packet debugging is on
```

Extended ping is done from router R1 to destination 192.169.30.1. Link failure of the successor route was simulated after the extended ping was started.



```
R1#ping
Protocol [ip]:
Target IP address: 192.168.30.1
Repeat count [5]: 15
Datagram size [100]: 1500
Timeout in seconds [2]: 1
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 15, 1500-byte ICMP Echos to 192.168.30.1, timeout is 1 seconds:
!!!!...!
00:10:05: %LINK-3-UPDOWN: Interface Serial0/1, changed state to down
00:10:06: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to down!!!!!!!
Success rate is 80 percent (12/15), round-trip min/avg/max = 380/632/760 ms
```

The following screenshot shows the ICMP packets sent from Router R1 being replied to by router R3.



```
00:10:02: ICMP: echo reply sent, src 192.168.30.1, dst 192.168.3.1
00:10:04: %LINK-5-CHANGED: Interface Serial0/0, changed state to administratively down
00:10:05: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to down
00:10:05: ICMP: echo reply sent, src 192.168.30.1, dst 192.168.1.1
```

Analysis: From the above screenshots it can be seen that there are three packets that get lost during the computation process. The debug ICMP also confirms the three second delay. During this experiment there was no feasible successor present for the destination. When the successor route failed EGIRP DUAL had to query other routers, find route and install it before sending further packets. This process in this case took three seconds.

Analyzing the previous and the current experiment it has been shown that Local Computation is quicker then Diffusing Computation. The difference between them would have been more evident if, this was a large network where are lot of routers would have had to reply to the query.

Conclusion: This experiment successful showed the process involved in diffusing computation. In this case it was found that for this particular network and EIGRP router takes roughly three seconds to perform diffusing calculation.

6.2.12 Query Processing and Range

Aim: The demonstrate the Query and reply process and its range

Figure 6.12 – Network topology for experiment 6.2.12

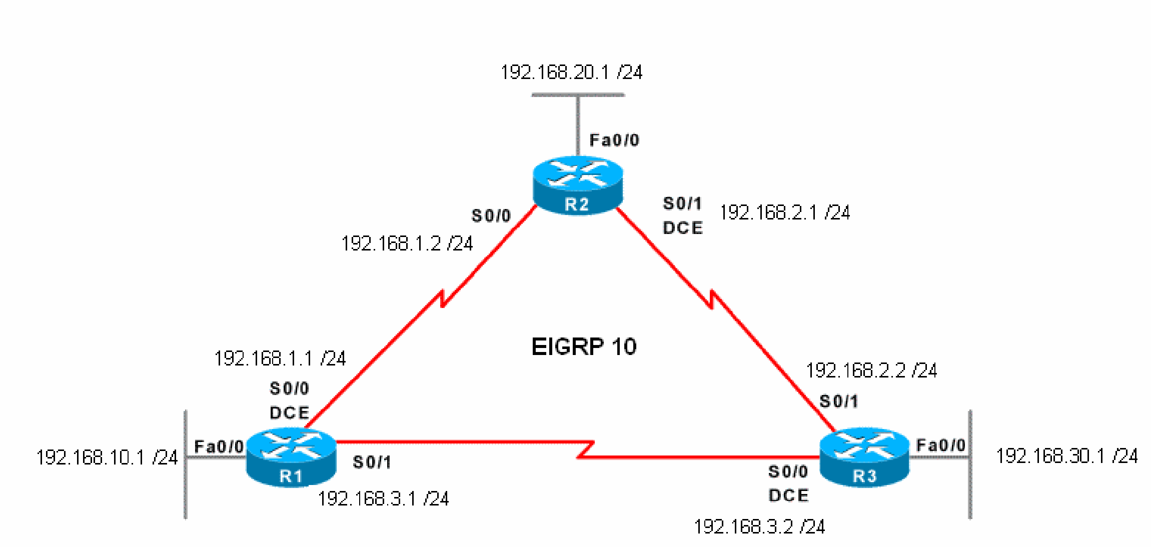


Table 6.12 – Router Configuration for Experiment 6.2.12

Configuration for Router R1

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R1
R1(config)#interface serial 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)#clockrate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/1
R1(config-if)# ip address 192.168.3.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fa 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router eigrp 10
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.3.0
R1(config-router)#network 192.168.10.0
```

Configuration for Router R2

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R2
R2(config)#interface serial 0/0
R2(config-if)# ip address 192.168.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface serial 0/1
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)#clockrate 64000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface fa 0/0
R2(config-if)# ip address 192.168.20.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router eigrp 10
R2(config-router)#network 192.168.1.0
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.20.0
```

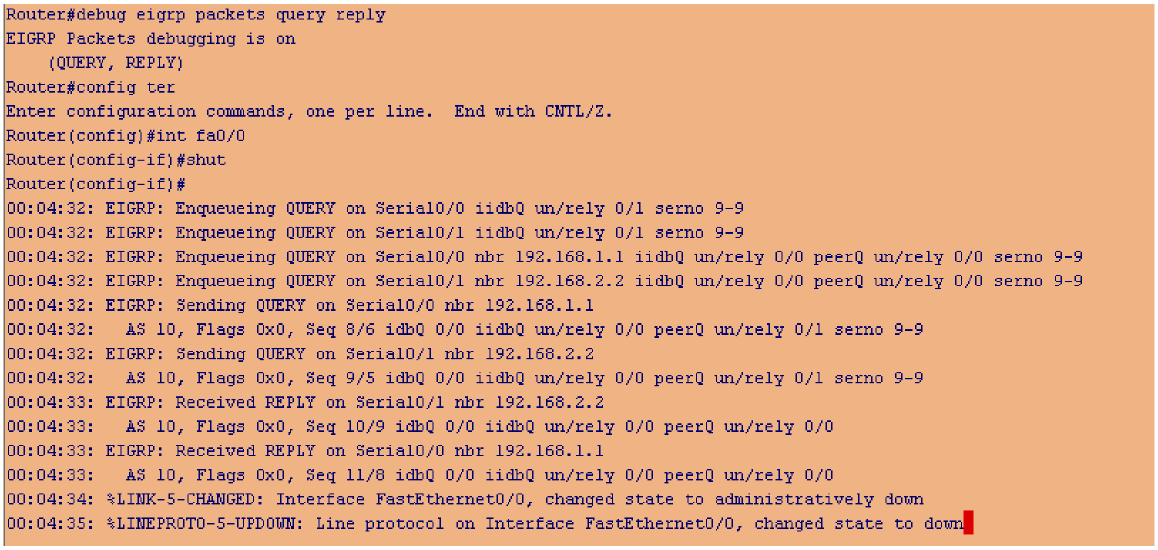
Configuration for Router R3

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R3
R3(config)#interface serial 0/0
R3(config-if)# ip address 192.168.3.2 255.255.255.0
R3(config-if)#clockrate 64000
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface serial 0/1
```

```
R3(config-if)# ip address 192.168.2.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface fa 0/0
R3(config-if)# ip address 192.168.30.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router eigrp 10
R3(config-router)#network 192.168.2.0
R3(config-router)#network 192.168.3.0
R3(config-router)#network 192.168.30.0
```

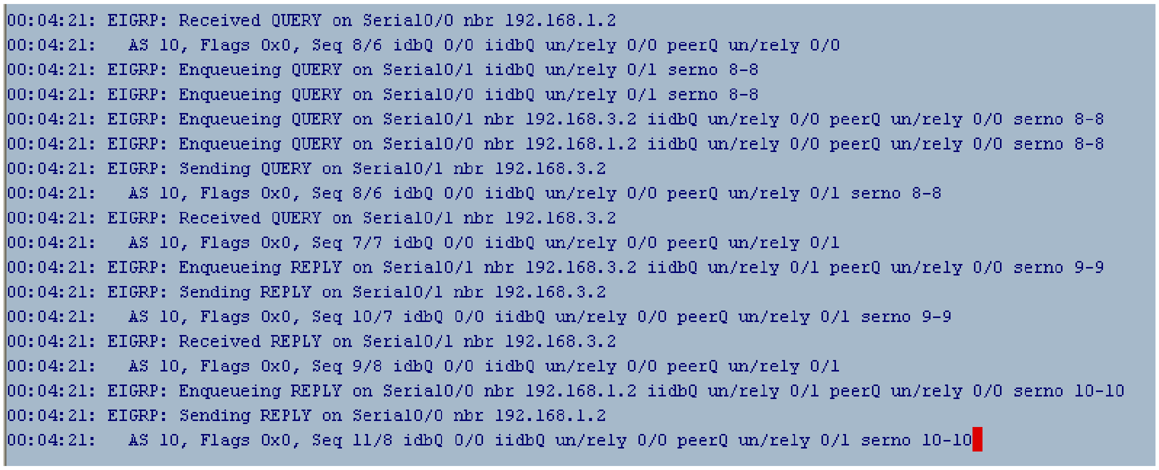
Description/Procedure: The network was configured using the network diagram shown in Figure 6.12 and the router configuration present in Table 6.12. Link failure between R1 and R2 is simulated. Query and reply exchange between three routers was observed using the debugging commands.

Result: The following screenshot shows debugging EIGRP query and reply packets being issued on Router R2. The fa0/0 link of the router is administratively disabled to simulate link failure. Upon link failure it can be seen that router R2 sends query to find route information about the lost link to router R1 and router R3.



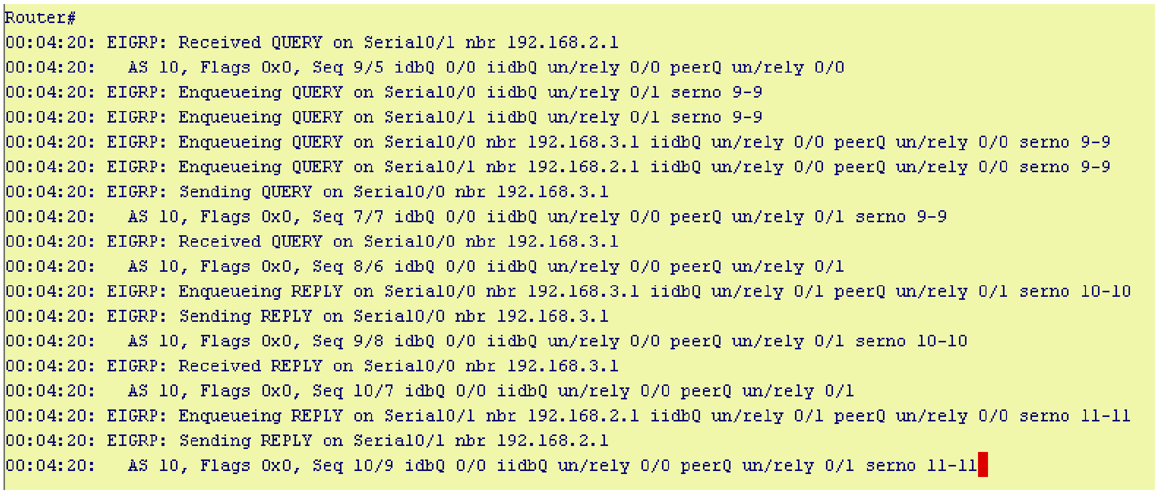
```
Router#debug eigrp packets query reply
EIGRP Packets debugging is on
    (QUERY, REPLY)
Router#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#shut
Router(config-if)#
00:04:32: EIGRP: Enqueueing QUERY on Serial0/0 iidbQ un/rely 0/1 serno 9-9
00:04:32: EIGRP: Enqueueing QUERY on Serial0/1 iidbQ un/rely 0/1 serno 9-9
00:04:32: EIGRP: Enqueueing QUERY on Serial0/0 nbr 192.168.1.1 iidbQ un/rely 0/0 peerQ un/rely 0/0 serno 9-9
00:04:32: EIGRP: Enqueueing QUERY on Serial0/1 nbr 192.168.2.2 iidbQ un/rely 0/0 peerQ un/rely 0/0 serno 9-9
00:04:32: EIGRP: Sending QUERY on Serial0/0 nbr 192.168.1.1
00:04:32:   AS 10, Flags 0x0, Seq 8/6 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1 serno 9-9
00:04:32: EIGRP: Sending QUERY on Serial0/1 nbr 192.168.2.2
00:04:32:   AS 10, Flags 0x0, Seq 9/5 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1 serno 9-9
00:04:33: EIGRP: Received REPLY on Serial0/1 nbr 192.168.2.2
00:04:33:   AS 10, Flags 0x0, Seq 10/9 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
00:04:33: EIGRP: Received REPLY on Serial0/0 nbr 192.168.1.1
00:04:33:   AS 10, Flags 0x0, Seq 11/8 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
00:04:34: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
00:04:35: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
```

The following screenshot has been taken from the router Console of Router R1. It shows that R1 receives the query from router R2. As R1 does not have a viable route to the destination it in turn enquires router R3. Note that it does not reply to the original query until getting reply from R3.



```
00:04:21: EIGRP: Received QUERY on Serial0/0 nbr 192.168.1.2
00:04:21:   AS 10, Flags 0x0, Seq 8/6 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
00:04:21: EIGRP: Enqueueing QUERY on Serial0/1 iidbQ un/rely 0/1 serno 8-8
00:04:21: EIGRP: Enqueueing QUERY on Serial0/0 iidbQ un/rely 0/1 serno 8-8
00:04:21: EIGRP: Enqueueing QUERY on Serial0/1 nbr 192.168.3.2 iidbQ un/rely 0/0 peerQ un/rely 0/0 serno 8-8
00:04:21: EIGRP: Enqueueing QUERY on Serial0/0 nbr 192.168.1.2 iidbQ un/rely 0/0 peerQ un/rely 0/0 serno 8-8
00:04:21: EIGRP: Sending QUERY on Serial0/1 nbr 192.168.3.2
00:04:21:   AS 10, Flags 0x0, Seq 8/6 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1 serno 8-8
00:04:21: EIGRP: Received QUERY on Serial0/1 nbr 192.168.3.2
00:04:21:   AS 10, Flags 0x0, Seq 7/7 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1
00:04:21: EIGRP: Enqueueing REPLY on Serial0/1 nbr 192.168.3.2 iidbQ un/rely 0/1 peerQ un/rely 0/0 serno 9-9
00:04:21: EIGRP: Sending REPLY on Serial0/1 nbr 192.168.3.2
00:04:21:   AS 10, Flags 0x0, Seq 10/7 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1 serno 9-9
00:04:21: EIGRP: Received REPLY on Serial0/1 nbr 192.168.3.2
00:04:21:   AS 10, Flags 0x0, Seq 9/8 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1
00:04:21: EIGRP: Enqueueing REPLY on Serial0/0 nbr 192.168.1.2 iidbQ un/rely 0/1 peerQ un/rely 0/0 serno 10-10
00:04:21: EIGRP: Sending REPLY on Serial0/0 nbr 192.168.1.2
00:04:21:   AS 10, Flags 0x0, Seq 11/8 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1 serno 10-10
```

The following screenshot has been taken from the router Console of Router R3. It shows that R3 receives the query from router R2. As R3 does not have a viable route to the destination it in turn enquires router R1. Note that it does not reply to the original query until getting reply from R1.



```
Router#
00:04:20: EIGRP: Received QUERY on Serial0/1 nbr 192.168.2.1
00:04:20:   AS 10, Flags 0x0, Seq 9/5 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
00:04:20: EIGRP: Enqueueing QUERY on Serial0/0 iidbQ un/rely 0/1 serno 9-9
00:04:20: EIGRP: Enqueueing QUERY on Serial0/1 iidbQ un/rely 0/1 serno 9-9
00:04:20: EIGRP: Enqueueing QUERY on Serial0/0 nbr 192.168.3.1 iidbQ un/rely 0/0 peerQ un/rely 0/0 serno 9-9
00:04:20: EIGRP: Enqueueing QUERY on Serial0/1 nbr 192.168.2.1 iidbQ un/rely 0/0 peerQ un/rely 0/0 serno 9-9
00:04:20: EIGRP: Sending QUERY on Serial0/0 nbr 192.168.3.1
00:04:20:   AS 10, Flags 0x0, Seq 7/7 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1 serno 9-9
00:04:20: EIGRP: Received QUERY on Serial0/0 nbr 192.168.3.1
00:04:20:   AS 10, Flags 0x0, Seq 8/6 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1
00:04:20: EIGRP: Enqueueing REPLY on Serial0/0 nbr 192.168.3.1 iidbQ un/rely 0/1 peerQ un/rely 0/1 serno 10-10
00:04:20: EIGRP: Sending REPLY on Serial0/0 nbr 192.168.3.1
00:04:20:   AS 10, Flags 0x0, Seq 9/8 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1 serno 10-10
00:04:20: EIGRP: Received REPLY on Serial0/0 nbr 192.168.3.1
00:04:20:   AS 10, Flags 0x0, Seq 10/7 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1
00:04:20: EIGRP: Enqueueing REPLY on Serial0/1 nbr 192.168.2.1 iidbQ un/rely 0/1 peerQ un/rely 0/0 serno 11-11
00:04:20: EIGRP: Sending REPLY on Serial0/1 nbr 192.168.2.1
00:04:20:   AS 10, Flags 0x0, Seq 10/9 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1 serno 11-11
```

Analysis: It can be seen that upon querying about a failed route to routers which do not have a route to the failed destination causes the router queried to send out queries to their neighbours. This can go on until the end of the AS or all routers have applied to a query. This is an issue about EIGRP which can be controlled using features that were described in chapter 5 of this report. Network designs that have a large number of routers involved must take this factor into account otherwise it can lead to sever SIA problems.

Conclusion: The experiment successfully demonstrates the issue with EIGRP query range and processing.

6.2.13 Effect of K-value changes to influence metrics

Aim: To show the effect of mismatched K values

Figure 6.13 – Network topology for experiment 6.2.13

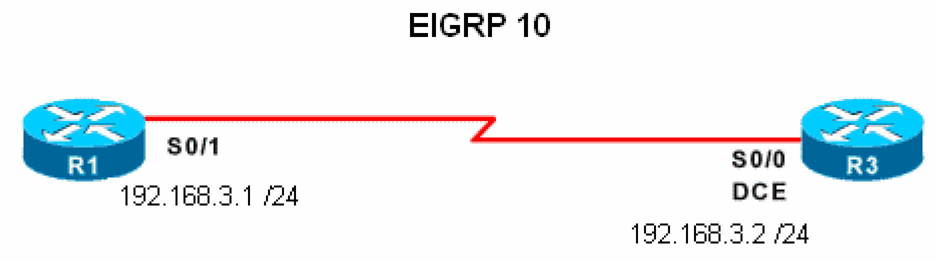


Table 6.13 – Router Configuration for Experiment 6.2.13

Configuration for Router R1

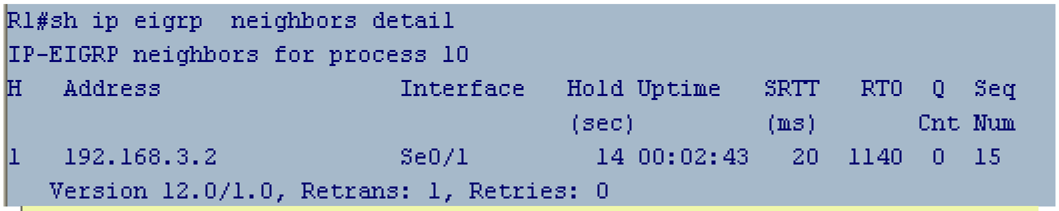
```
Router>enable
Router#conFigure terminal
Router(config)#hostname R1
R1(config)#interface serial 0/1
R1(config-if)# ip address 192.168.3.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router eigrp 10
R1(config-router)#network 192.168.3.0
```

Configuration for Router R3

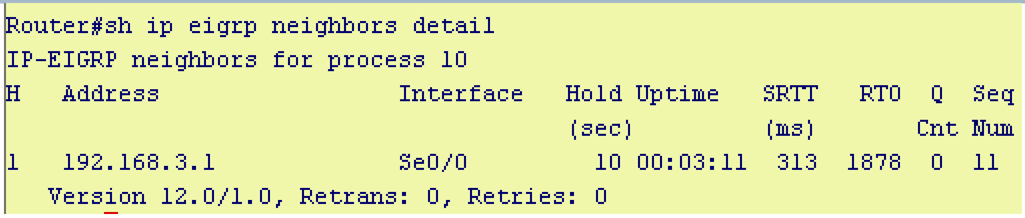
```
Router>enable
Router#conFigure terminal
Router(config)#hostname R3
R3(config)#interface serial 0/0
R3(config-if)# ip address 192.168.3.2 255.255.255.0
R3(config-if)#clockrate 64000
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router eigrp 10
R3(config-router)#network 192.168.3.0
```

Description/Procedure: For the purpose of this experiment the routers and the network was configured using the router configuration found in Table 6.12 and the network topology found in Figure 6.12. The experiment will involve verification of neighbour relationship between two routers and then changing the K values on one of the routers to see the effect.

Result: The following screenshots showing neighbour Tables from both the routers verify the fact that neighbour relationship was established.

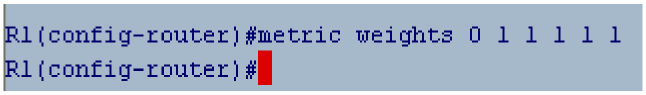


```
R1#sh ip eigrp  neighbors detail
IP-EIGRP neighbors for process 10
H   Address                 Interface     Hold Uptime    SRTT   RTO  Q  Seq
                                          (sec)          (ms)       Cnt Num
1   192.168.3.2             Se0/1           14 00:02:43   20   1140  0  15
   Version 12.0/1.0, Retrans: 1, Retries: 0
```



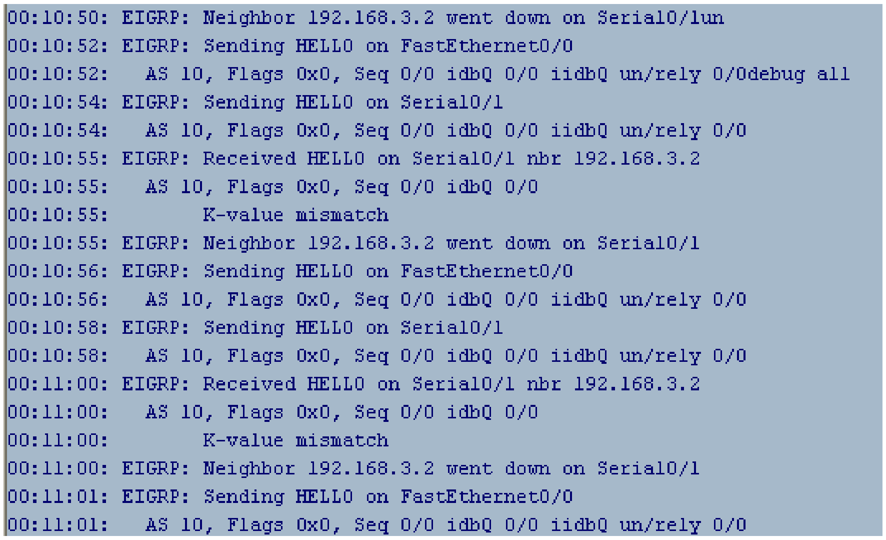
```
Router#sh ip eigrp neighbors detail
IP-EIGRP neighbors for process 10
H   Address                 Interface     Hold Uptime    SRTT   RTO  Q  Seq
                                          (sec)          (ms)       Cnt Num
1   192.168.3.1             Se0/0           10 00:03:11  313   1878  0  11
   Version 12.0/1.0, Retrans: 0, Retries: 0
```

Using the configurations shown in the screenshot below, the k values that influence the metric calculations are given below.



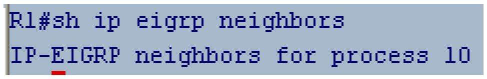
```
R1(config-router)#metric weights 0 1 1 1 1 1
R1(config-router)#
```

The following screen shows the error message received from debug sources about mismatch of K values. The routers loose their relationship with each other.



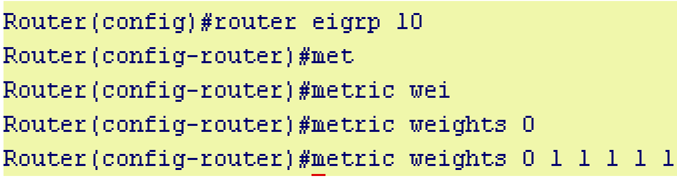
```
00:10:50: EIGRP: Neighbor 192.168.3.2 went down on Serial0/lun
00:10:52: EIGRP: Sending HELLO on FastEthernet0/0
00:10:52:   AS 10, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0debug all
00:10:54: EIGRP: Sending HELLO on Serial0/1
00:10:54:   AS 10, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
00:10:55: EIGRP: Received HELLO on Serial0/1 nbr 192.168.3.2
00:10:55:   AS 10, Flags 0x0, Seq 0/0 idbQ 0/0
00:10:55:        K-value mismatch
00:10:55: EIGRP: Neighbor 192.168.3.2 went down on Serial0/1
00:10:56: EIGRP: Sending HELLO on FastEthernet0/0
00:10:56:   AS 10, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
00:10:58: EIGRP: Sending HELLO on Serial0/1
00:10:58:   AS 10, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
00:11:00: EIGRP: Received HELLO on Serial0/1 nbr 192.168.3.2
00:11:00:   AS 10, Flags 0x0, Seq 0/0 idbQ 0/0
00:11:00:        K-value mismatch
00:11:00: EIGRP: Neighbor 192.168.3.2 went down on Serial0/1
00:11:01: EIGRP: Sending HELLO on FastEthernet0/0
00:11:01:   AS 10, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
```

The following screenshot verifies that neighbour relationship is lost due to mismatch of K values.



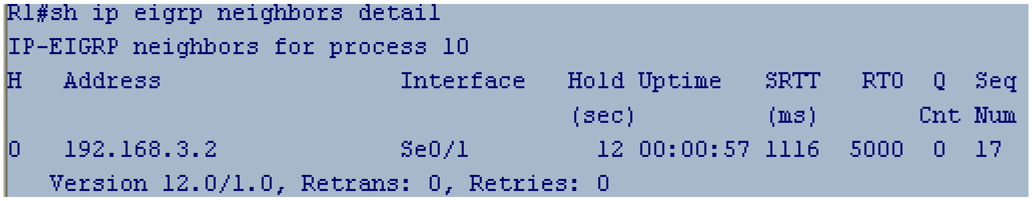
```
R1#sh ip eigrp neighbors
IP-EIGRP neighbors for process 10
```

The following screenshot show the configuration command used to configure router R3 with the same K values as that Router R1 was configured with.

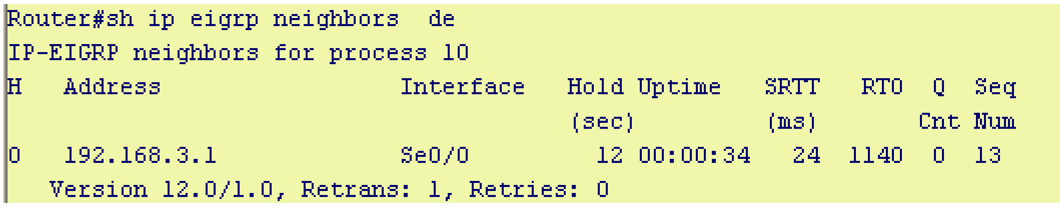


```
Router(config)#router eigrp 10
Router(config-router)#met
Router(config-router)#metric wei
Router(config-router)#metric weights 0
Router(config-router)#metric weights 0 1 1 1 1 1
```

The following screenshots showing the neighbour Tables of both routers confirm that the neighbour relationship was re-established.



```
R1#sh ip eigrp neighbors detail
IP-EIGRP neighbors for process 10
H   Address                 Interface      Hold Uptime   SRTT   RTO  Q  Seq
                                           (sec)         (ms)       Cnt Num
0   192.168.3.2             Se0/1            12 00:00:57 1116  5000  0  17
   Version 12.0/1.0, Retrans: 0, Retries: 0
```



```
Router#sh ip eigrp neighbors  de
IP-EIGRP neighbors for process 10
H   Address                 Interface      Hold Uptime   SRTT   RTO  Q  Seq
                                           (sec)         (ms)       Cnt Num
0   192.168.3.1             Se0/0            12 00:00:34   24  1140  0  13
   Version 12.0/1.0, Retrans: 1, Retries: 0
```

Analysis: From this experiment it was ascertained that the K values for all routers on an AS have to be the same, so that the metrics calculated for routes are compatible with each other. The convergence time experiments carried out earlier were redone using updated K values. The results of the experiment were same as the ones done before.

Conclusion: This experiment successfully shows the issues related to K values.

6.2.14 Route Summarization

Figure 6.14 – Network topology for experiment 6.2.14

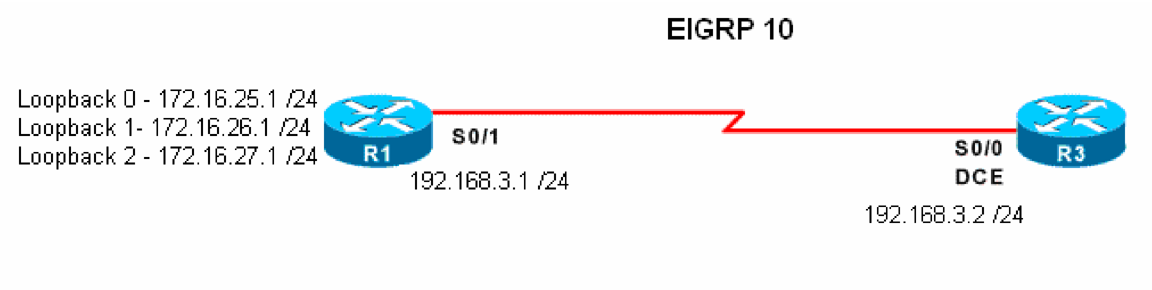

EIGRP 10
Loopback 0 - 172.16.25.1 /24
Loopback 1- 172.16.26.1 /24
Loopback 2 - 172.16.27.1 /24
R1
S0/1
192.168.3.1 /24
S0/0
DCE
R3
192.168.3.2 /24

Table 6.14 – Router Configuration for Experiment 6.2.14

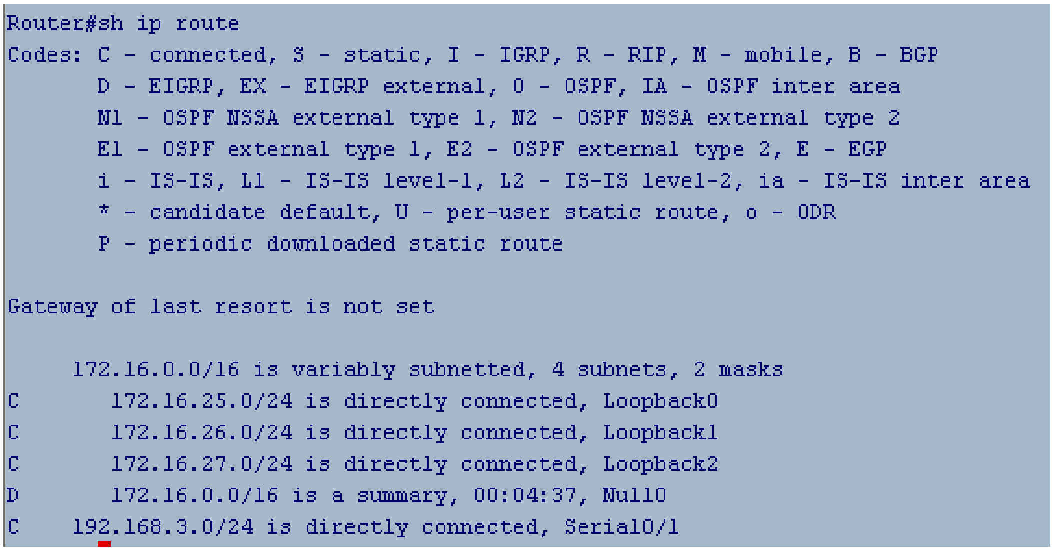
Configuration for Router R1

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R1
R1(config)#interface serial 0/1
R1(config-if)# ip address 192.168.3.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface loopback0
R1(config-if)# ip address 172.16.25.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface loopback1
R1(config-if)# ip address 171.16.26.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface loopback2
R1(config-if)# ip address 172.16.26.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router eigrp 10
R1(config-router)#network 192.168.3.0
R1(config-router)#network 172.16.0.0
```

Configuration for Router R3

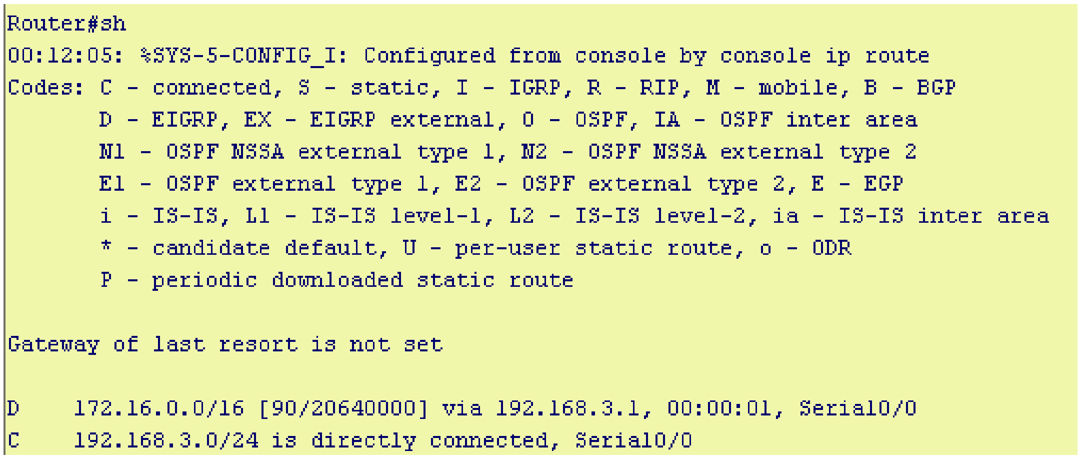
```
Router>enable
Router#conFigure terminal
Router(config)#hostname R3
R3(config)#interface serial 0/0
R3(config-if)# ip address 192.168.3.2 255.255.255.0
R3(config-if)#clockrate 64000
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router eigrp 10
R3(config-router)#network 192.168.3.0
```

Results: The following screenshot verifies the configured route on Router R1



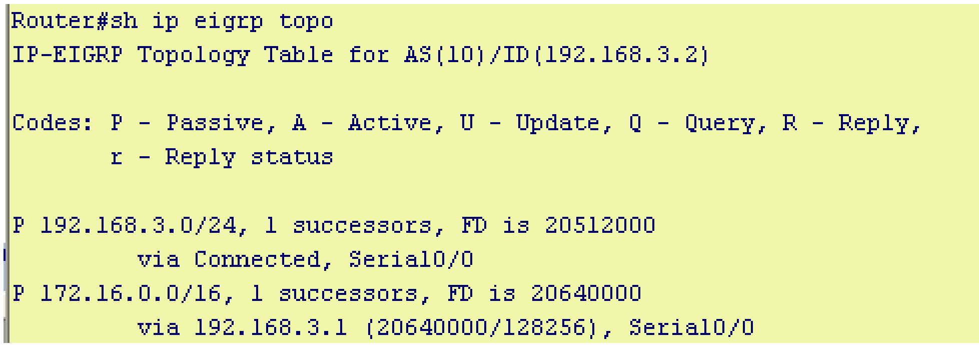
```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -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

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.16.25.0/24 is directly connected, Loopback0
C       172.16.26.0/24 is directly connected, Loopback1
C       172.16.27.0/24 is directly connected, Loopback2
D       172.16.0.0/16 is a summary, 00:04:37, Null0
C    192.168.3.0/24 is directly connected, Serial0/1
```

The following screenshot shows that router R3 was only receiving a summarized advertisement of routes from router R1. This is automatically done by EIGRP at major network boundaries.



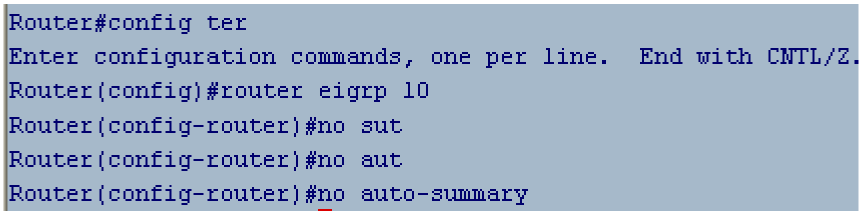
```
Router#sh
00:12:05: %SYS-5-CONFIG_I: Configured from console by console ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D    172.16.0.0/16 [90/20640000] via 192.168.3.1, 00:00:01, Serial0/0
C    192.168.3.0/24 is directly connected, Serial0/0
```

The following screenshot show the topology Table present on Router R3. Even the topology Table contains entries for the summarized network.



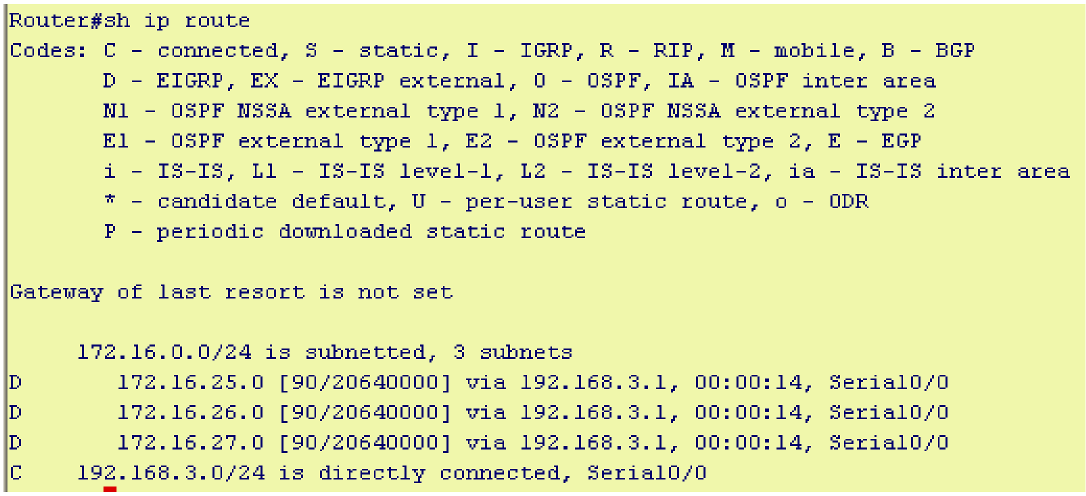
```
Router#sh ip eigrp topo
IP-EIGRP Topology Table for AS(10)/ID(192.168.3.2)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.3.0/24, 1 successors, FD is 20512000
         via Connected, Serial0/0
P 172.16.0.0/16, 1 successors, FD is 20640000
         via 192.168.3.1 (20640000/128256), Serial0/0
```

The following screenshot shows the automatic address summarization feature of the protocol being turned off.



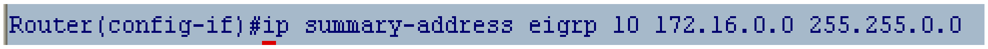
```
Router#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router eigrp 10
Router(config-router)#no sut
Router(config-router)#no aut
Router(config-router)#no auto-summary
```

The following screenshot shows that all networks are advertised separately by router R1 once the auto summarization feature has been turned off.



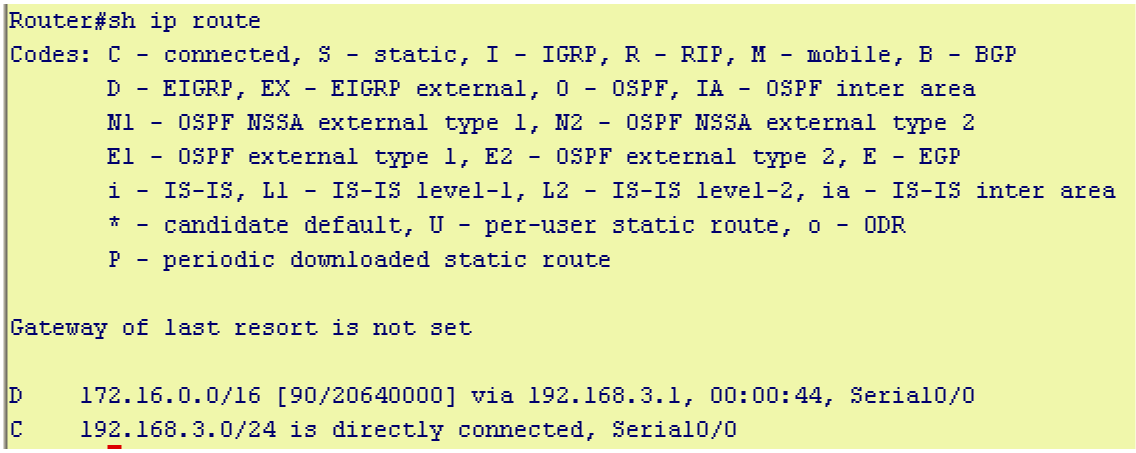
```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -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

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
D       172.16.25.0 [90/20640000] via 192.168.3.1, 00:00:14, Serial0/0
D       172.16.26.0 [90/20640000] via 192.168.3.1, 00:00:14, Serial0/0
D       172.16.27.0 [90/20640000] via 192.168.3.1, 00:00:14, Serial0/0
C    192.168.3.0/24 is directly connected, Serial0/0
```

The following screenshot shows the configuration command used to manually summarize the routes. The command is placed on the interface connected to router R3. Instead of sending regular updated router R1 will just send the defined summary route.



```
Router(config-if)#ip summary-address eigrp 10 172.16.0.0 255.255.0.0
```

The following screenshot shows the effect of manual summarization to be same as automatic.



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

Gateway of last resort is not set

D    172.16.0.0/16 [90/20640000] via 192.168.3.1, 00:00:44, Serial0/0
C    192.168.3.0/24 is directly connected, Serial0/0
```

Analysis: The network was configured with subnets connected to Router R1. By default EIGRP summarized the routes and advertised a summarized route to router R3. This was verified by checking the routing Table of router R3. The automatic summarization feature was then disabled to show that EIGRP is able to advertise subnets separately. This also proves that EIGRP provides support for VLSM. The summarization was then configured manually so that EIGRP advertised a desirable summary address. This manual configuration feature is of the necessary when there are discontiguous subnets within a network. Automatic summarization does not work when there discontiguous networks present.

Conclusion: The route summarization feature of EIGRP is very powerful and useful. It allows more efficient routing because there are fewer entries in the routing Table when route summarization is being used. In large networks proper router summarization can increase performance and efficiency significantly.

6.2.15 IGRP and EIGRP Redistribution

Aim: To show the process and configuration requirements for EIGRP – IGRP redistribution.

Figure 6.15 – Network topology for experiment 6.2.15

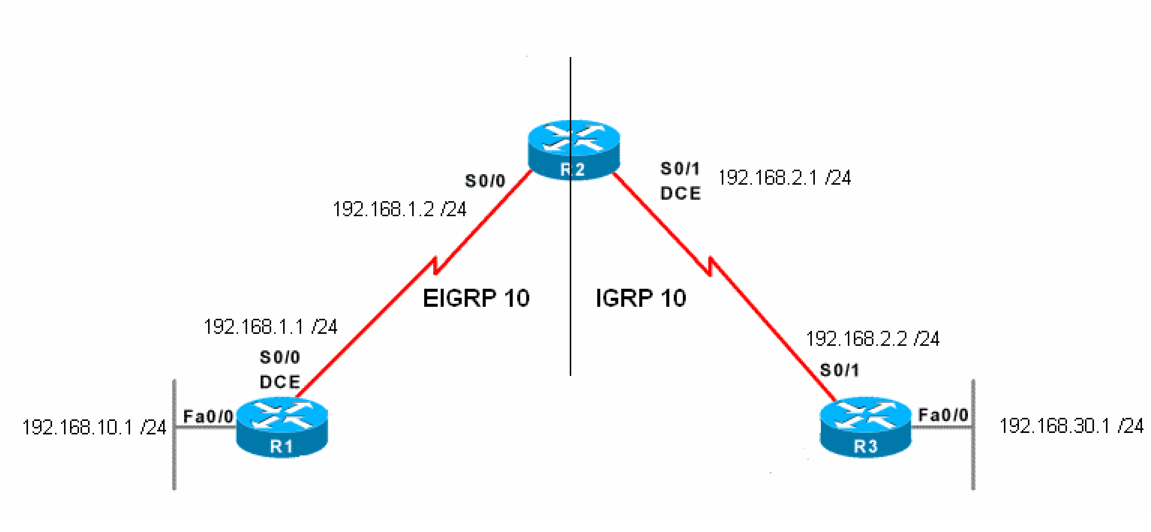


Table 6.15 – Router Configuration for Experiment 6.2.15

Configuration for Router R1

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R1
R1(config)#interface s0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)#clockrate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fa0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router eigrp 10
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.10.0
```

Configuration for Router R2

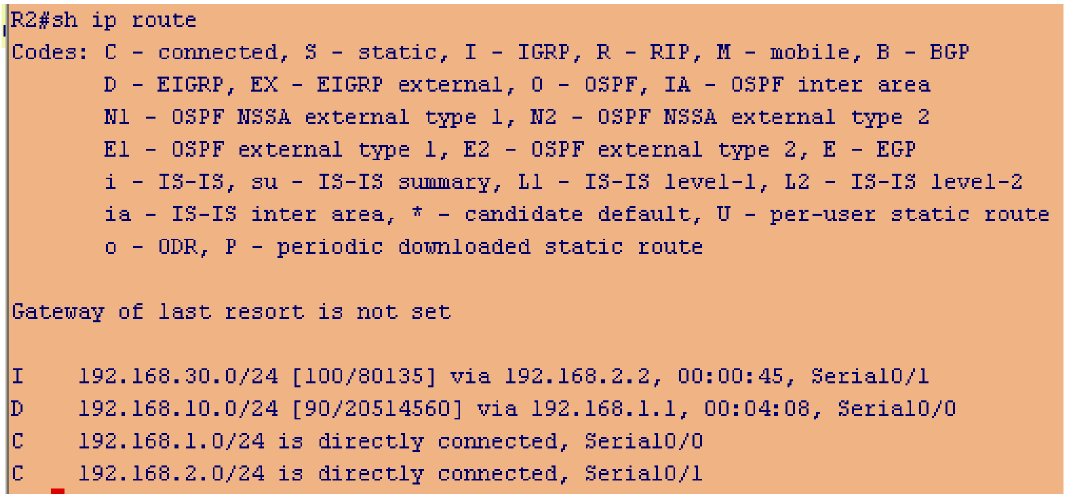
```
Router>enable
Router#conFigure terminal
Router(config)#hostname R2
R1(config)#interface s0/0
R1(config-if)# ip address 192.168.1.2 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface s0/1
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# clockrate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router eigrp 10
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.10.0
R1(config)#router igrp 10
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.10.0
```

Configuration for Router R3

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R3
R3(config)#interface serial 0/1
R3(config-if)# ip address 192.168.2.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface fa 0/0
R3(config-if)# ip address 192.168.30.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router igrp 10
R3(config-router)#network 192.168.30.0
R3(config-router)#network 192.168.2.0
```

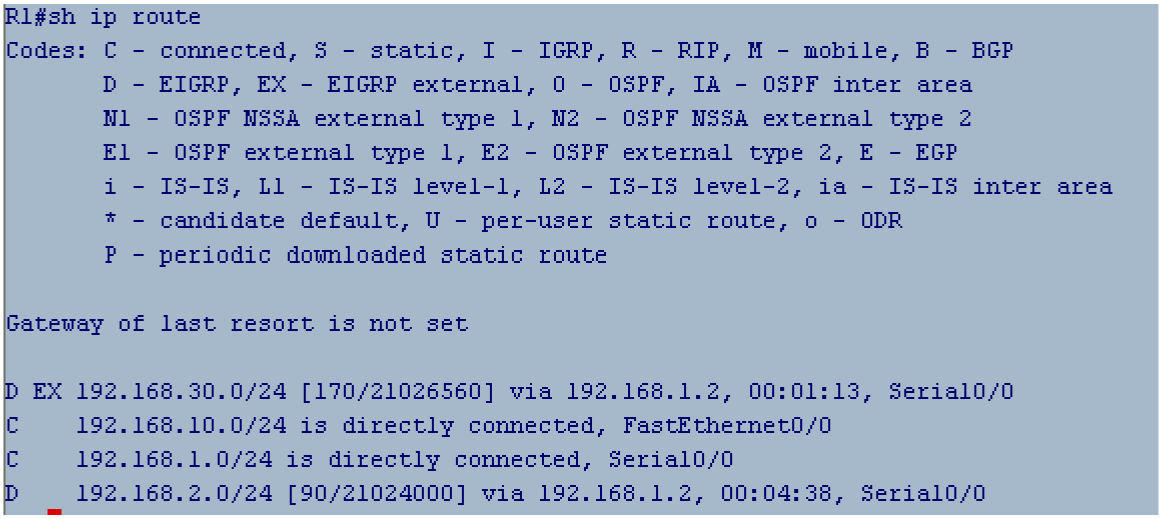
Description/Procedure: The network was configured according to the configuration found in Figure 6.15 and Table 6.15. Redistribution between the two protocols happens with very little configuration.

Results: The following screenshot shows routing Table of router R2. The routing Table shows 1 route was learned form IGRP and 1 was learned through EIGPR.



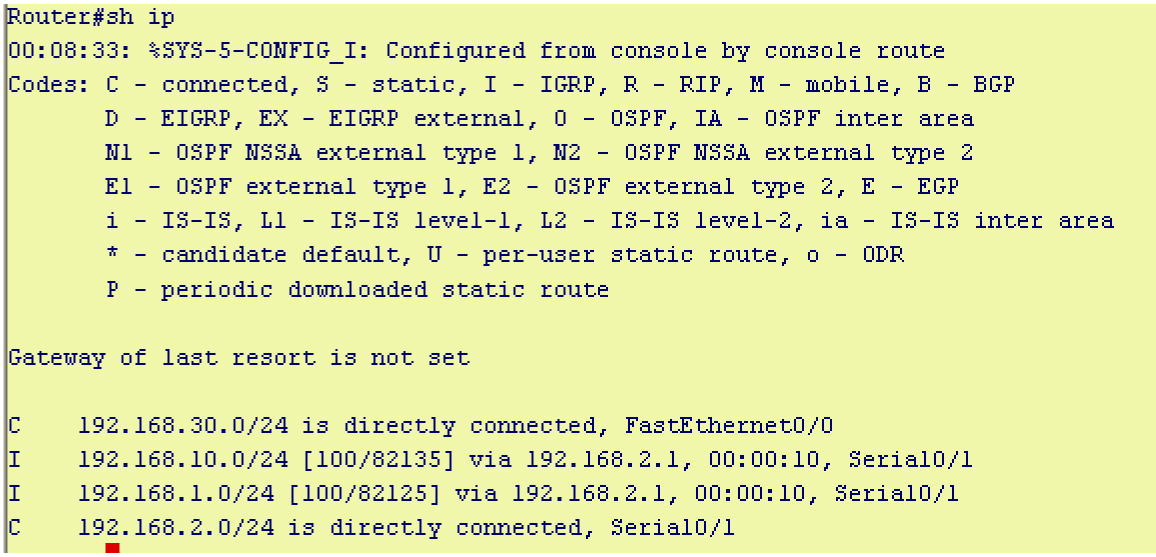
```
R2#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

I    192.168.30.0/24 [100/80135] via 192.168.2.2, 00:00:45, Serial0/1
D    192.168.10.0/24 [90/20514560] via 192.168.1.1, 00:04:08, Serial0/0
C    192.168.1.0/24 is directly connected, Serial0/0
C    192.168.2.0/24 is directly connected, Serial0/1
```

The following screenshot show the routing Table of router R1. Here the EIGRP router identifies routes learned through IGRP and marks them as external routes.



```
R1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D EX 192.168.30.0/24 [170/21026560] via 192.168.1.2, 00:01:13, Serial0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, Serial0/0
D    192.168.2.0/24 [90/21024000] via 192.168.1.2, 00:04:38, Serial0/0
```

The following screenshot shows the routing Table on router R3. The IGRP router is not able to differentiate between routes learned through EIGRP and IGRP.



```
Router#sh ip
00:08:33: %SYS-5-CONFIG_I: Configured from console by console route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.30.0/24 is directly connected, FastEthernet0/0
I    192.168.10.0/24 [100/82135] via 192.168.2.1, 00:00:10, Serial0/1
I    192.168.1.0/24 [100/82125] via 192.168.2.1, 00:00:10, Serial0/1
C    192.168.2.0/24 is directly connected, Serial0/1
```

Analysis: The redistribution process between EIGRP and IGRP is very simple. For simplified redistribution both IGRP and EIGRP have to be running the same autonomous system numbers. The border router needs to list all directly connected networks under both EIGRP and IGRP. Although the metric used by both protocols are different, conversion of the metric is automatic and does not require any configuration.

Conclusion: The experiment shows that IGRP and EIGRP networks can be integrated with each other if they are running the same AS number. Furthermore the experiment also shows the route tagging that each protocol uses for routes learned from the other.

6.2.16 Update Packet due to change in network topology

Aim: To confirm that update packets are only used during topology changes

Figure 6.16 – Network topology for experiment 6.2.16

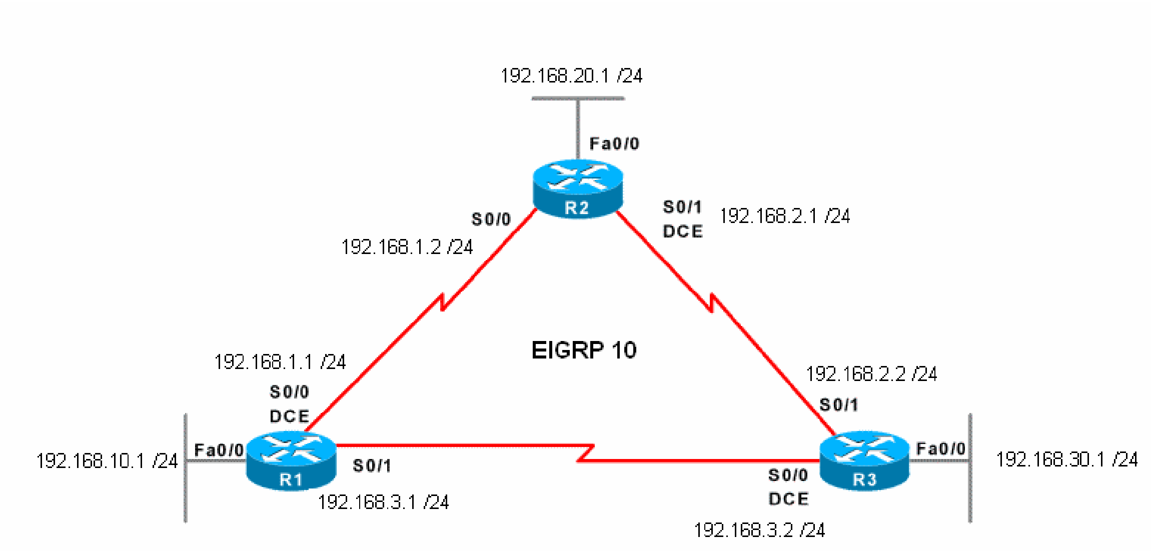


Table 6.16 – Router Configuration for Experiment 6.2.16

Configuration for Router R1

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R1
R1(config)#interface serial 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)#clockrate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/1
R1(config-if)# ip address 192.168.3.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fa 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router eigrp 10
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.3.0
R1(config-router)#network 192.168.10.0
```

Configuration for Router R2

```
Router>enable
```

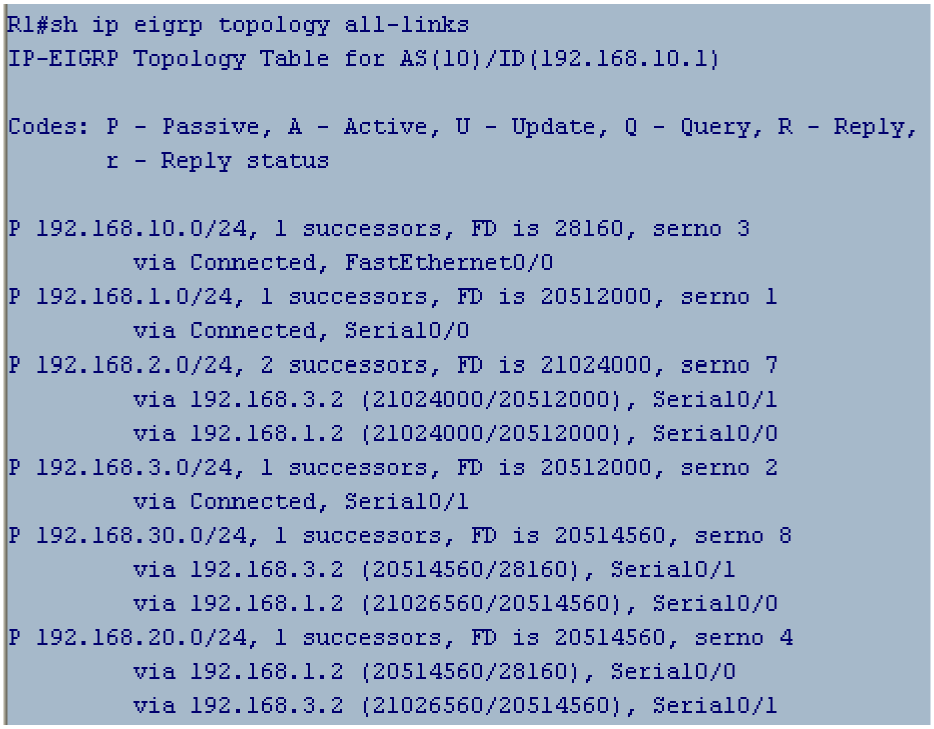
```
Router#conFigure terminal
Router(config)#hostname R2
R2(config)#interface serial 0/0
R2(config-if)# ip address 192.168.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface serial 0/1
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)#clockrate 64000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface fa 0/0
R2(config-if)# ip address 192.168.20.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router eigrp 10
R2(config-router)#network 192.168.1.0
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.20.0
```

Configuration for Router R3

```
Router>enable
Router#conFigure terminal
Router(config)#hostname R3
R3(config)#interface serial 0/0
R3(config-if)# ip address 192.168.3.2 255.255.255.0
R3(config-if)#clockrate 64000
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface serial 0/1
R3(config-if)# ip address 192.168.2.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface fa 0/0
R3(config-if)# ip address 192.168.30.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router eigrp 10
R3(config-router)#network 192.168.2.0
R3(config-router)#network 192.168.3.0
R3(config-router)#network 192.168.30.0
```

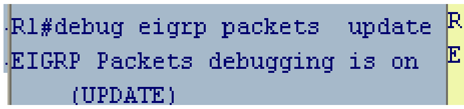
Description/Procedure: The routers will be configured according to the network topology diagram and the configuration given in Figure 6.6 and Table 6.6. Debugging of EIGRP Update packets will be turned on the routers to view packets that are being exchanged between them. The debugging outputs will be used to verify that no update packets are exchanged during normal network operations. Link failure of the serial link on one of the router will be simulated. The output from the debugging screens on the other routers will be used to verify the exchange of packets that take place.

Result: The following screenshot shows that the network is fully converged and Router R1 has a complete view of the entire network.

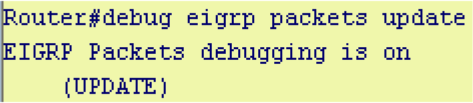


```
R1#sh ip eigrp topology all-links
IP-EIGRP Topology Table for AS(10)/ID(192.168.10.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.10.0/24, 1 successors, FD is 28160, serno 3
         via Connected, FastEthernet0/0
P 192.168.1.0/24, 1 successors, FD is 20512000, serno 1
         via Connected, Serial0/0
P 192.168.2.0/24, 2 successors, FD is 21024000, serno 7
         via 192.168.3.2 (21024000/20512000), Serial0/1
         via 192.168.1.2 (21024000/20512000), Serial0/0
P 192.168.3.0/24, 1 successors, FD is 20512000, serno 2
         via Connected, Serial0/1
P 192.168.30.0/24, 1 successors, FD is 20514560, serno 8
         via 192.168.3.2 (20514560/28160), Serial0/1
         via 192.168.1.2 (21026560/20514560), Serial0/0
P 192.168.20.0/24, 1 successors, FD is 20514560, serno 4
         via 192.168.1.2 (20514560/28160), Serial0/0
         via 192.168.3.2 (21026560/20514560), Serial0/1
```

The following screenshot shows the EIGRP debug commands to view the update packets are being used on both routers.

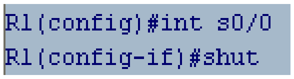


```
R1#debug eigrp packets  update
EIGRP Packets debugging is on
    (UPDATE)
```



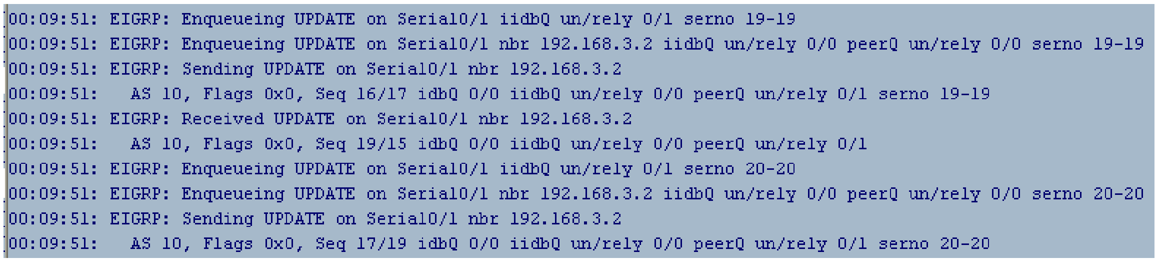
```
Router#debug eigrp packets update
EIGRP Packets debugging is on
    (UPDATE)
```

The following screen shot shows the serial link is be simulated for link failure.

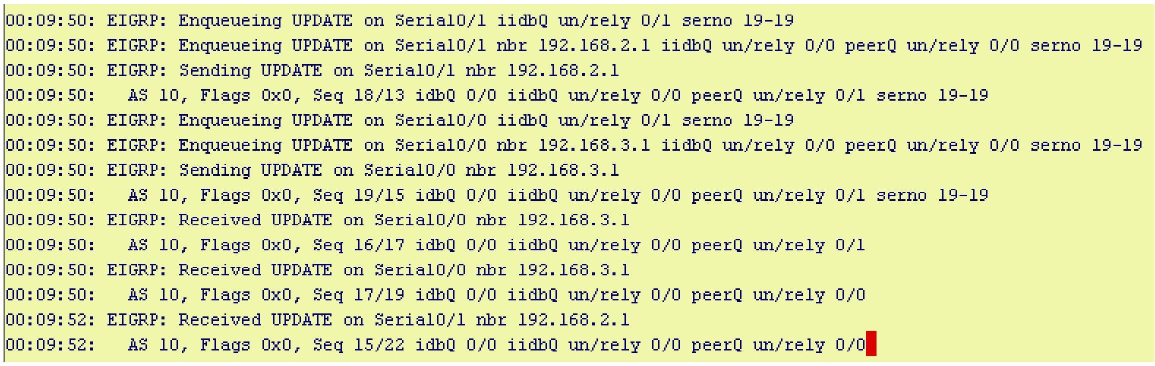


```
R1(config)#int s0/0
R1(config-if)#shut
```

The following screenshot shows the routers on the link send out updates as soon as they detect the link failure.



```
00:09:51: EIGRP: Enqueueing UPDATE on Serial0/1 iidbQ un/rely 0/1 serno 19-19
00:09:51: EIGRP: Enqueueing UPDATE on Serial0/1 nbr 192.168.3.2 iidbQ un/rely 0/0 peerQ un/rely 0/0 serno 19-19
00:09:51: EIGRP: Sending UPDATE on Serial0/1 nbr 192.168.3.2
00:09:51:   AS 10, Flags 0x0, Seq 16/17 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1 serno 19-19
00:09:51: EIGRP: Received UPDATE on Serial0/1 nbr 192.168.3.2
00:09:51:   AS 10, Flags 0x0, Seq 19/15 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1
00:09:51: EIGRP: Enqueueing UPDATE on Serial0/1 iidbQ un/rely 0/1 serno 20-20
00:09:51: EIGRP: Enqueueing UPDATE on Serial0/1 nbr 192.168.3.2 iidbQ un/rely 0/0 peerQ un/rely 0/0 serno 20-20
00:09:51: EIGRP: Sending UPDATE on Serial0/1 nbr 192.168.3.2
00:09:51:   AS 10, Flags 0x0, Seq 17/19 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1 serno 20-20
```



```
00:09:50: EIGRP: Enqueueing UPDATE on Serial0/1 iidbQ un/rely 0/1 serno 19-19
00:09:50: EIGRP: Enqueueing UPDATE on Serial0/1 nbr 192.168.2.1 iidbQ un/rely 0/0 peerQ un/rely 0/0 serno 19-19
00:09:50: EIGRP: Sending UPDATE on Serial0/1 nbr 192.168.2.1
00:09:50:   AS 10, Flags 0x0, Seq 18/13 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1 serno 19-19
00:09:50: EIGRP: Enqueueing UPDATE on Serial0/0 iidbQ un/rely 0/1 serno 19-19
00:09:50: EIGRP: Enqueueing UPDATE on Serial0/0 nbr 192.168.3.1 iidbQ un/rely 0/0 peerQ un/rely 0/0 serno 19-19
00:09:50: EIGRP: Sending UPDATE on Serial0/0 nbr 192.168.3.1
00:09:50:   AS 10, Flags 0x0, Seq 19/15 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1 serno 19-19
00:09:50: EIGRP: Received UPDATE on Serial0/0 nbr 192.168.3.1
00:09:50:   AS 10, Flags 0x0, Seq 16/17 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1
00:09:50: EIGRP: Received UPDATE on Serial0/0 nbr 192.168.3.1
00:09:50:   AS 10, Flags 0x0, Seq 17/19 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
00:09:52: EIGRP: Received UPDATE on Serial0/1 nbr 192.168.2.1
00:09:52:   AS 10, Flags 0x0, Seq 15/22 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
```

Analysis: The results from the experiment show that EIGRP does not send updates periodically. During normal operation of the network updates are not exchanged. When an EIGRP router detects a change in one of its links, it sends out updates containing information about the changes to its neighbours.

Conclusion: The experiment successfully shows the use of EIGRP update packet in an EGIRP network.

6.3 Recommendations for Deployment

The experiments that were performed to check various features and capitalises to EIGRP of which some were described in this chapter have been used to derive the following general recommendation to improve network performance through EIGRP Configuration.

Recommendations are as follow:

1. EIGRP is very easy to configure especially when the network size is small. In small networks EIGRP also tends to be efficient because it does not use up much memory in route calculations. However, if routers do not have sufficient processing power and memory deployment of the protocol should be avoided. On the other hand, if sufficient resources are available, EIGRP would be a very good choice for a small network.
2. Network convergence time of EIGRP varies from 1 -16 seconds even on good designs depending on the network scenario. However, convergence time of most small to medium networks should be less then 6 seconds. These Figures should be checked and matched during deployment to ascertain the efficiency of the design.
3. During experiment it was found that the default bandwidth percentage allocated to EIGRP is 50%. EIGRP however does not require all this bandwidth most of the time to converge. On small to medium size networks it works efficiently with 20% bandwidth allocated to it. This

however does not mean that the allocation should be reduced. The allocation should only be changed if it is seen that there is not enough bandwidth remaining for data packet to use the network. Reducing the EIGRP bandwidth allocation will have a negative affect on network convergence times during congestion.

4. Hello packets are exchanged by EIGRP to form neighbour relationships and to re-discover adjacent routers that were previously unreachable. These hello packets are very small and have little effect on the network. The forming of the relationship of end of a relationship however generally starts a DUAL computation that is memory intensive. It should always be made certain that neighbour relationships are not regularly lost due to factors that can be controlled, such as power loss.
5. Hello packets are exchanged every 5 seconds with EIGRP neighbours. This acts as a default and generally suits all small to medium networks. The hold-time on EIGRP routers by default is 15 seconds, which is three times the hello interval. Increasing the hello interval will increase the network convergence time. This may however be necessary if very congested networks. If the hello interval is increased, the hold time also needs to be increased manually. The hold time does not change automatically. The hold time should be kept at 3 times that of hello interval as this reflects the best failure detection.
6. Selection of Successor and Feasible successor is automated in EIGRP. The selection process should not be influenced by changing the metric

cost of routes and this can lead to routing loops. Changing of metric to influence route selection should not be done unless certain of the fact that new routes will not cause routing loops.

7. EIGRP only selects routes as feasible successor if the route has a reported distance that is less then the current feasible distance. If the route has a reported distance which is equal to the feasible distance EIGRP still does not install the route as feasible successor.
8. The bandwidth and delay on a route should be configured to reflect the actual bandwidth and delay of link. EIGRP paces its packet depending on the link bandwidth and delay. A higher then actual configuration can lead to network congestion due to frequent EIGRP packet exchange.
9. Equal cost path load balancing on EIGRP occurs automatically over up to 4 routes. If there are more then 4 equal cost routes, appropriate commands should be used as explained to increase the number of router over which the traffic is shared.
10. Unequal path load balancing on EIGRP has to be configured using the ***variance*** command. An integer number has to be issued along with variance command. EIGRP will load balance over paths whose cost are n times that of the least cost path. The paths have to meet the feasibility condition before they are selected for load balancing.
11. Local computation of DUAL is faster then Diffusing computation but when using load balancing over unequal cost paths a command ***traffic share min*** can be used. This will cause the router to only forward traffic using

the best link but will keep all the other feasible routes stored in the routing Table. This can cause an instant switchover during link failure. This will be quicker then local computation and use up virtually no router resources. This command is very useful in large network where a computation may take significant amount of time.

12. Query range of an EIGRP network is very important as it can affect network convergence. The query range, process and its affects have already been discussed in earlier chapters. Limiting the range of the query is also very important to have good network convergence times.
13. The K values are the constants that can be used to influence the cost of routes. Changing K-values does not increase the efficiency of the network or decrease the network convergence times. The default K-values have been selected by Cisco to provide best performance on most networks. The K-values should not be changed until the administrator is absolutely sure of positive outcome. Furthermore, although EIGRP does not require hello timers and hold down timers of adjacent routers to be the same, it does need the K-values of the neighbouring routers should be same. Until the K-values of adjacent routers are same they will not form neighbour relationship.
14. Route summarization of routes at major network boundaries is automatic when using EIGRP. This feature may be disabled for greater control if required. Manual summarization of routes is also possible, which will be needed where there are discontiguous networks within the design. Route

summarization is a powerful feature and makes routing more efficient by reducing the size of routing Table. This feature should be used in large networks to reduce the routing Table and entry and make the process more efficient.

15. Integration of EIGRP into IGRP is very simple and can be done with very little configuration. Undertaking an integration project where EIGRP needs to be added to an IGRP network can be done with ease.
16. During deployment of EIGRP in large network limiting of query range, route summarization, tired network design and routers with sufficient memory and processing power should be used.

6.4 Chapter summary

The chapter was concerned with the operational analysis of the protocol. EIGRP is a protocol with many functionalities and capabilities. Detailed examination and analysis of all its capabilities are outside the scope of this project but, most of the major issues, capabilities and functionalities of the protocol were analyzed during the operation analysis of the protocol.

This chapter contains aim, network topology, router configuration, description, results, analysis of the results and the conclusion that was derived from each experiment that was carried out. Through experiments it was ascertained that EIGRP is a very robust protocols which when configured properly in relation to the deployment scenario, it performs extremely well. Specific recommendation that was derived from the experiments can also be found within this chapter.

The chapter satisfied the following project objectives:

- To conduct analysis of the protocol by deploying it in the Test network under Lab conditions
- To use the test results and research to produce a report to show the actual capabilities of the protocol.

This chapter concludes the research and analysis that was carried out on EIGRP. The next chapter summarizes the project, evaluates the outcome of the project and draws a conclusion.

CHAPTER 7 – PROJECT REVIEW

This chapter will conclude the report by summarizing the project outcomes, outlining further work that can be undertaken and providing a personal reflection and conclusion for the overall project.

7.1 Project Achievements

The objectives that were set out at the beginning of the project were all satisfied and the aim of the project was also achieved at its completion. The objectives of the project and its achievements are shown in Table 7.1, Table 7.2 and Table 7.3.

Table 7.1 – Project Achievements (Defined Academic)

Defined Project Objective (Academic)	Achieved
To explain the need for Routed protocols and briefly describe commonly used Routed Protocols.	✓
To explain the need for Routing Protocols and compare routing protocols in common usage.	✓
To provide a background to EIGRP and its evolution from IGRP	✓
To provide detailed information about EIGRP along with its advanced technologies, key features and capabilities such as: fast convergence,	✓

support for variable-length subnet mask, support for partial updates, support for multiple network layer protocols, neighbour discovery/recovery, Reliable Transport Protocol (RTP,) DUAL finite-state machine, Load Balancing, topology Table, neighbour Table and routing Table.	
To discuss and produce the configuration process/ requirements for Implementation and Troubleshooting of EIGRP.	✓
To design a test network and the different testing scenarios to analyze and test capabilities of the protocol.	✓
To conduct analysis of the protocol by deploying it in the Test network under Lab conditions	✓
To use the test results and research to produce a report to show the actual capabilities of the protocol.	✓

Table 7.2 – Project Achievements (Defined Personal)

Defined Project Objective (Personal)	Achieved
Improve knowledge on the subject area.	✓
Develop and demonstrate written communication skills through the project report	✓
Further develop appreciation of different areas of project management	✓

Successfully follow the project plan to find the final recommendations for deployment	✓
Be aware of various research sources and methods to improve research skills	✓
Improve documentation and review skills	✓
Demonstrate abilities to identity key success elements of a project	✓

Table 7.3 – Project Achievements (Additional Academic)

Additional Project Objective (Academic)	Achieved
Recommendation for EIGRP Deployment	✓

All of the above academic project objectives were achieved and combined together to deliver the final project aim

> **Perform critical analysis of EIGRP routing protocol and outline configuration requirements to gain optimum routing performance in EIGRP networks, by making use of advanced features of the protocol.**

7.2 Further Work

The operational analysis of the project was done by its deployment in a test network. Although the test network successfully simulated many of the scenarios it can never give the same problems and complexity of a real life network.

During further work, operational analysis of EIGRP can done using statistics of a large scale live network. Data from such a network would be more reliable and would allow better analysis of the protocol. The scenarios such as redistribution and router summarization which could not be dealt with during the project due to its vastness can then be further analyzed.

7.3 Personal reflection

During the research and development of the project, various sources of information have been used to conduct a thorough and complete research. It has taught me to look up and information over the Internet, library and books much more quickly as I now know where and how to look. My knowledge of the networking subject area in general and regarding network protocol has increased to a much higher level due to the research of this project. I learnt to look up journals, white papers and articles for information during the literature review phase which brought my knowledge and understandings of the information technology up to date. This information is crucial in the job market and where everyone is looking to get a competitive edge over one another.

A great deal of research data was collected during the research phase. This information required to be sorted, grouped and structured to find the underlying process and technologies of network routing protocols. This process helped me to improve my organizational skills and to work with a schedule to meet deadlines

My aim in life is to be highly ranked information systems developer. This career pathway requires me to carry out and analyze research data and produce or recommend efficient solutions just like in this project. When I would go for job interviews, the companies would be more interested to see my achievements through the final year project. The key to a good project is to carry out a good research to understand the technologies involved. When my employers will be seeing my abilities through this project, they would not hesitate to offer me my dream job.

7.4 Project Conclusion

Routed protocols were reviewed and their needs and types were explained. Common routed protocols such as IP, IPX and AppleTalk were outlined. IPv4 and IPv6 were outlined separately showing their addressing schemes and packet format. Information given about routed protocols provided a background routing.

Types of routing and the method used for routing were explained in details. Advantages, disadvantages and comparison of static and dynamic routing were done. Classification of routing protocols was explained according to where they are deployed or how they perform their operation. Link-state and distance-vector routing protocols were explained and outlined. Common protocols such as RIP, RIPv2, IGRP, OSPF and IS-IS were also shown. Summary Table was provided showing the comparison of the routing protocols.

Theoretical review of EIGRP routing protocol was carried out in details. Common terminologies of EIGRP were given and explained. Calculation of routes and metric were also explained in details. Selection process involving successor and feasible successor were also explained details. Technologies used by EIGRP such as neighbour relationship, RTP, DUAL, and PDM are explained in details. The different types of packets used by EIGRP and their formats have been explained and shown in details. Route tagging, metric calculations and integration processes of EIGRP into IP, IPX and Apple talk have also been shown and explained. Features such as Load balancing, route tagging, stub routing and troubleshooting issues have bee discussed in details. EIGRP issues such as network design considerations, SIA, Query processing and stub routing has been described in details. Operational analysis of the protocol was then carried out on issues that were identified during the protocol through its deployment on test networks. Analysis of the results from the operation deployment was done. Conclusion and results of each experiment was also provided. After completion of the experiments critical analysis of all research and results were carried out to come up with specific recommendation that can be used to enhance network performance during EIGRP deployment. All the above were used to finally satisfy the project objectives and met the aim.

Glossary

Adjacent neighbour: Two directly connected routers that participate in the exchange of routing information are said to be adjacent.

Algorithm: A well-defined rule or process for arriving at a solution to a problem. In networking, algorithms are commonly used to determine the best route for traffic from a particular source to a particular destination.

AS (Autonomous system): Collection of routers under a single administrative authority using a common Interior Gateway Protocol (IGP) for routing packets.

Authentication: The process of identifying an individual, usually base on an user name and password

Authorization: The process of granting or denying access to a service or resource.

Backbone: A backbone is a part of a network that acts as the primary path for traffic that is most often sources from, and destined for, other networks.

Balanced hybrid routing protocol: Routing protocols that utilize elements of distance vector and link-state routing protocols.

Bandwidth: The amount of information that can flow through a network connection in a given period of time.

Cisco Internetworking Operating System (IOS) Software: Software stored as an image file in Flash memory on the router that, when loaded into RAM, provides the operating system that runs the router.

Classless interdomain routing (CIDR): Ability to support variable length subnets and perform router aggregation.

Congestion: Traffic that is excess of network capacity.

Convergence: The speed and capability of a group of internetworking devices running a specific routing protocol to determine network topology.

Datagram: A logical grouping of information sent as a network layer unit over a transmission medium without prior establishment of a virtual circuit. IP datagrams are the primary information units in the Internet.

Debugging: To find and remove error from a program or a design.

***Distance-vector routing protocol**:* A routing protocol that uses the number of hops in a route to decide on the shortest path to a destination.

Dotted-decimal format: In this notation, each IP address is written as four parts separated by periods, or dots.

DUAL (Diffusing Update Algorithm): Convergence algorithm used in EIGRP that provides loop-free operation at every instant throughout a route computation and allows routers involved in a topology to synchronize completely.

Dynamic Routing: Routing that adjusts automatically to network topology or traffic change.

EIGRP (Enhanced Interior Gateway Routing Protocol): An advanced version of IGRP developed by Cisco that has superior convergence properties and operating efficiency and combines the advantages of link-state protocols with those of distance-vector protocols.

Exterior Gateway Protocol (EGP): A routing protocol designed for use between networks that are controlled by two different organizations.

Exterior Route: Routes to networks outside the autonomous system that are considered when identifying a gateway of last resort.

FD (feasible distance): The lowest calculated metric to each destination.

FS (feasible successor): A backup route that is identified at the same time as the successor but is kept only in the topology Table.

Header: Control information placed before data when encapsulating that data for network transmission.

Hop: the passage of a data packet from one network node, typically a router, to another.

Hop-count: A routing metric used to measure the distance between a source and a destination using number of routers present on the link.

Hybrid-protocol: A protocol that combines aspects of the link-state and distance-vector protocols.

ICMP: Network layer protocol tat reports errors and provides other information relevant to IP packet processing.

IGP (Interior Gateway Protocol): Protocols used to perform internal routing of large heterogeneous network.

IGRP (Interior Gateway Routing Protocol): A protocol developed by Cisco to address the problems associated with routing in large-scale networks.

Interface: Connection between two system and devices. In routing terms this is regarded as a network connection.

Interior Routes: Routers between subnets of a network attached to a router interface.

Link-state routing protocol: A complex routing protocol that allows a consistent view of the entire network on all the routers in the AS.

Load sharing: Use of multiple paths to send data to a destination.

Neighbour Table: The Table that routers running EIGRP use to maintain lists of adjacent routers.

OSPF (Open Shortest Path First) protocol: A link-state routing protocol that uses cost as its routing metric.

RD (reported distance): The distance that an adjacent neighbour reports for a specific destination.

RTP (Reliable Transport Protocol): A transport-layer protocol that guarantees ordered and reliable delivery of EIGRP packets.

Route Authentication: A form of authentication that is used when a router must pass criteria before another router accepts its routing updates.

Route summarization: Consolidation of addresses by advertisement of a single summary route to be advertised to other areas by an area border router.

Routed protocols: A protocol that can be routed by a router. Examples of routed protocols include IP, IPX, Apple Talk and DECnet.

Router: A network layer device that forward packets from one network to another based on network layer information also known as a gateway.

Routing protocol: Protocol used by routers to share route information. Examples of routing protocols include RIP, IGRP, EIGRP and OSPF.

Routing Table: A Table that stores routes to destination networks and in some cases metrics that are associated with those routes.

Shortest path first (SPF) algorithm: Routing algorithm that iterates on length of path to determine a shortest-path spanning tree. Commonly used in link-state routing algorithms.

Static route: A route that is fixed and is not capable of action or change.

Static routing: Routing that is explicitly configured and entered into the routing Table.

Stub network: A network that has only a single connection to a router.

Stuck in Active: A route that a router has been trying to gather information about but has not had a reply for a long period of time.

Successor: A route that is selected as the primary route to use to reach a destination.

Topology Table: The Table is made up of all EIGRP routing Tables in the autonomous system to provide the router with knowledge of all the destination routers within the AS.

Tunnelling: A vehicle that encapsulates packets inside a protocol that is understood at the entry and exit points of a given network.

VLSM (variable-length subnet mask): The ability to specify a different subnet mask for the same network number on different subnets. VLSM helps optimize available address space.

[1, 65]

References and Bibliography

[1] **Cisco Systems**. **(2003)** *CCNA 3 and4 – Companion Guide,* Cisco Press, 3rd ed. ISBN 1587131137.

[2] **Malhotra, R**. **(2002)** *IP Routing,* O'Reilly, 1st ed. ISBN 0596002750.

[3] **Pepelnjak, I. (1999)** *EIGRP Network Design Solution*, Cisco Press, 1st ed. ISBN 1578701651.

[4] **Aziz, Z. & Liu, J. (2002)** *Troubleshooting IP Routing Protocols (CCIE Professional Development Series)*, Cisco Press, 1st ed. ISBN 1587050196.

[5] *CCDP: Cisco Internetwork Design Study Guide.* URL : http://www.unix.org.ua/cisco/CCNP-CCDP/CID-sybex/ewtoc.html
Last Date of access: 15-05-2006 15:33.

[6] How does Load Balancing work?(Data Network Resource)
URL: http://www.cisco.com/warp/public/105/46.html
Last Date of access: 15-05-2006 02:25.

[7] Enhanced IGRP. (Cisco Systems Website) URL: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/en_igrp.htm Last Date of access: 13-05-2006 17:14.

[8] How does Unequal cost path load balancing (Variance) work in IGRP and EIGRP? (Cisco Systems Website) URL: http://www.cisco.com/warp/public/103/19.html Last Date of access: 12-05-2006 12:53. authored by **Syed Faraz Shamim.**

[9] Integrating Enhanced IGRP into Existing Networks. URL: http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2017.htm Last Date of access: 11-05-2006 07:59.

[10] Troubleshooting EIGRP. (Cisco Systems Website) URL: http://www.cisco.com/warp/public/103/trouble_eigrp.html Last Date of access: 11-05-2006 08:22.

[11] Troubleshooting EIGRP (Cisco Press Article). URL: http://www.ciscopress.com/articles/article.asp?p=27839&seqNum=5&rl=1 Last Date of access: 13-05-2006 15:35.

[12] Enhanced Interior Gateway Routing Protocol (EIGRP) – Chapter 4. (O'Reilly online Catalogue). URL: http://www.oreilly.com/catalog/iprouting/chapter/ch04.html#31695 Last Date of access: 11-05-2006 16:31.

[13] EIGRP Operations and Configuration. (CCNP online material) URL: http://www.it-123.co.uk/ebook/chapter_six.htm Last Date of access: 12-05-2006 16:18.

[14] Routing Protocol Selection - Chapter 5. (O'Reilly online Catalogue). URL: http://www.oreilly.com/catalog/cisco/chapter/ch05.html Last Date of access: 11-05-2006 13:21.

[15] Apple Talk Networking: A lower layer Primer URL: http://www.corecom.com/html/appletalk.html Last Date of access: 14-05-2006 21:07.

[16] **Aziz, Z. (2002)** *Troubleshooting IP Routing Protocols (CCIE Professional Development Series),* Cisco Press. ISBN 1587050196.

[17] What doest the EIGRP DUAL-3-SIA Error Message Mean? URL: http://www.cisco.com/warp/public/103/18.html Last Date of access: 16-05-2006 22:24

[18] EIGRP Configuration Documentation (Cisco Systems Website) URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt2/1cdeigrp.htm Last Date of access: 16-04-2006 12:14.

[19] EIGRP Commands (Cisco Systems Website) URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fiprrp_r/1rfeigrp.htm Last Date of access: 10-05-06 23:23

[20] EIGRP Stub Routing (Cisco Systems Website) URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s15/eigrpstb.htm Last Date of access: 12-05-06 12:46

[21] Understanding IPX-EIGRP (Cisco Tech Notes) URL: http://www.cisco.com/warp/public/473/57.html Last Date of access: 11-05-06 10:30

[22]Enhanced Interior Gateway Routing Protocol (Cisco Tech Notes) Document ID: 16406 URL: http://www.cisco.com/warp/public/103/eigrp-toc.html Last Date of access: 11-05-06 12:10

[23] Hybrid Routing Protocol. URL: http://homepages.uel.ac.uk/u0220856/Hybrid/Hybrid%20%20Protocol.html Last Date of access: 12-05-06 09:25

[24] EIGRP (Data Network Resources) URL: http://www.rhyshaden.com/eigrp.htm Last Date of access: 12-05-06 10:50

[25] EIGPR Introduction (Cisco Systems Website) URL: http://www.cisco.com/en/US/products/ps6630/products_ios_protocol_option_home.html. Last Date of access: 10-05-06 21:14

[26]Troubleshooting EIGRP Networks URL: http://www.cisco.com/application/pdf/en/us/guest/products/ps6630/c1161/cdccont_0900aecd80310efb.pdf Last Date of access: 10-05-06 23:22

[27] Deploying IGRP / EIGRP URL: http://www.cisco.com/application/pdf/en/us/guest/products/ps6630/c1161/cdccont_0900aecd80310f03.pdf Last Date of access: 14-05-06 13:15

[28]Route Selection in Cisco Routers (Cisco Documentation) URL: http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094823.shtml Last Date of access: 13-05-06 17:13

[29] Routing Basics (Cisco Documentation) URL: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/routing.htm
Last Date of access: 10-05-06 23:02

[30] What Do EIGRP "Not On Common Subnet" Messages Mean? (Cisco Documentation) URL: http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080093f09.shtml Last Date of access: 12-05-06 10:39

[31] EIGRP – White paper. URL: http://www.ssuet.edu.pk/~amkhan/cisco/EIGRP_white_paper.pdf Last Date of access: 12-05-06 10:58

[32] Technical Writing (Example). URL: http://www.egr.msu.edu/%7Emisrakir/projects/InternetRouters.PDF

[33] Technical Report Writing Notes. URL: http://owl.english.purdue.edu/workshops/hypertext/reportW/index.html Last Date of access: 14-05-06 09:50

[34] Some Advice on technical report writing. URL: http://www.csee.umbc.edu/%7Esherman/Courses/documents/TR_how_to.html Last Date of access: 14-05-06 09:50

[35]Written and Oral Presentation of Data. URL: http://biology.nebrwesleyan.edu/empiricist/sources/tips/present.html Last Date of access: 14-05-06 09:50

[36] **Kirkman, J. (1999)** *Full Marks: Advice on Punctuation for Scientific and Technical Writing* 3rd ed, Ramsbury Books.

[37] **Kirkman, J (1992)** Good Style – Writing for Science and Technology, Spon.

[38] **Van Emden, J (2001)** Effective Communication for Science and Technology, Palgrave.

[39] **Gowers, E. (1997)** The complete Plain Words, Pelican. revised 1997

[40] **Fraser, J (1995)** Professional Proposal Writing, Gower, 1995

[41] Technical Report writing Notes by Dr. Saeed R Taghizadeh. URL: http://homepages.unl.ac.uk/~taghizas/Digital%20Systems/Microprocessors/EE203/EE203.html Last Date of access: 14-05-06 09:50

[42] Report writing and Project Management Notes by Dr. N. Ioannides. URL:http://homepages.unl.ac.uk/~ioannidn/EE249.htm
Last Date of access: 14-05-06 09:50

[43] About the internet glossary. URL: http://compnetworking.about.com/od/networkprotocolsip/l/bldef_ip.htm Last Date of Access: 10-05-2006 14:25

[44] CCNA for Dummies. URL: http://www.dummies.com/WileyCDA/DummiesArticle/id-2267.html Last date of Access: 04-05-2006 14:45

[45] Routed Protocols. URL: http://www.inetdaemon.com/tutorials/internet/ip/routing/routing_vs_routed.shtml Last Date of Access: 25-04-2006 15:30

[46] Internet Protocol. URL: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ip.htm Last Date of Access: 25-04-2006 15:30

[63] Netware Protocols. URL: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/netwarep.htm Last Date of Access: 12-05-2006 15:30

[64] Dynamic Routing Protocols http://www.ciscopress.com/articles/article.asp?p=24090&seqNum=3 Last Date of Access: 12-05-2006 17:24

[65] **Cisco Systems**. **(2003)** *CCNA 1 and2 – Companion Guide,* Cisco Press, 3rd ed. ISBN – 1587131102

[66] Project management - Wikipedia, the free encyclopedia http://en.wikipedia.org/wiki/Project_management Date Last Accessed: 15-12-2005 07:43

[67] Project Management Activities

http://www.fin.ucar.edu/presentations/nsfbp_it/sld015.htm

Date Last Accessed: 15-12-2005 08:27

[68] Project Management Definition

http://scrc.ncsu.edu/public/DEFINITIONS/P%20-%20R.html

Date Last Accessed: 14-12- 2005 08:13

[69] Project Plan Definition http://en.wikipedia.org/wiki/Project_plan

Date Last Accessed: 11-05-2006 07:24

[70] **SANOG, V.** SANOG5-IPv6-tutorial

http://www.sanog.org/resources/sanog5-pfs-ipv6-tutorial.pdf

Date Last Accessed: 13-05-2006 8:18

[71] IGRP

http://www.rhyshaden.com/igrp.htm

Date Last Accessed: 13-05-2006 8:18

[72] IP-RIP

http://www.rhyshaden.com/iprip.htm

Date Last Accessed: 13-05-2006 8:18

[73] OSPF – Cisco Website article

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ospf.htm

Date Last Accessed: 12-05-2006 10:45

APPENDIX - A

Critical Analysis of the EIGRP Routing Protocol

(Project Proposal)

Abstract

Routing Protocols are one of the key issues that influence the efficiency and availability of modern computer networks. EIGRP is a hybrid routing protocol that has been developed by Cisco Systems as an enhancement to its predecessor IGRP. The new protocol has the same ease of implementation as simple distance vector protocols but boasts abilities and features similar to those of complex link state protocols like OSPF. It uses newly developed key technologies to achieve fast convergence times and loop free routing. The protocol is becoming very popular and is being widely deployed in large-scale networks around the world. During the project EIGRP will be researched and compared to other routing protocols. Capabilities and advanced features of the protocol will then be tested and analysed by its deployment in test network. Evaluation of the test results and the research will be carried out to produce an outline of configuration requirements, needed to increase performance of networks which employ EIGRP. This project proposal will outline the aim, objectives, scope, methodology, project plan and the deliverables of the project.

Acknowledgement

I would like to thank my project supervisor Mr. Tarik Molalign, senior lecturer CCTM, London Metropolitan University for his continuous support during the preliminary research and preparation of the project proposal. I would also like to thank Dr. Nicholas Ioannides for his support with overall project management and his lecture materials to ensure the success of the proposal.

Table of Contents

Table of Figures

Introduction

Modern day Businesses rely very heavily on their computer systems to provide high productivity and to perform many services essential to making a profit. Computer Networks are always employed in large organizations so that data and resources can be centralized and shared. These systems are vital to the work that most large organizations carry out. When networks go down, it usually means a loss of productivity and performance. The larger the company, the greater the loss, for some global companies network downtime is so critical that it can equate to millions of pounds of profit loss for each downtime hour or even each minute in some cases. Large organizations that have branches in different cities or even in different countries have extremely large networks. Due to the vast area that the networks cover and the great number of links in them they are more prone to failure. When network size is large and modern day applications are being used, a lot of traffic is generated on the network which needs to be handled and managed efficiently, for the network to be able to provide the level of performance required. It is vital to decrease network downtimes and increase their availability, so that the users are able to make full use of them and increase productivity.

Routed Protocols are used to handle the encapsulation of the data that is moved around in the network. There are various types of routed protocols, the major ones which will be considered during the project is IP, IPX and Apple Talk. IP is the most popular of the protocols and is most widely used around the world. The Internet is the largest network in the world and uses TCP/IP as its protocol.

Routers are devices that are primarily used to route traffic through the networks. Routers that connect different networks or different parts of a large network play a vital role in maintaining the efficiency of the network. To be able to efficiently forward traffic and increase network performance a router needs to know the best path through which a packet can be sent, in order to reach its destination. The protocols that routers use to exchange the path information or routing information is known as Routing Protocol.

Routing protocols have to be very efficient and need to provide routers with accurate up-to-date information about routes. If there are any path changes in the network or a link becomes unavailable this information needs to be passed on to routers as quickly as possible. Incorrect routing information can cause routers to send traffic down wrong paths causing congestion in networks and ultimately reducing efficiency and availability of the network. Thus routing protocol and its performance is very closely related with routers performance, which in turn dictates network efficiency. Some of the most common routing protocols used are RIP, IGRP, OSPF and EIGRP, each having its own characteristics, advantage and disadvantage.

Enhanced IGRP is a hybrid routing protocol developed by Cisco Systems as an enhancement to IGRP. It is being widely employed by many large-scale organizations and companies in their networks. Some of the key improvements of EIGRP over IGRP include fast convergence, support for variable-length subnet mask, support for partial updates, and support for multiple network layer protocols. To provide superior routing performance, Enhanced IGRP employs four key technologies that combine to differentiate it from other routing protocols: neighbour discovery/recovery, reliable transport protocol (RTP), DUAL finite-state machine, and protocol-dependent modules. Although EIGRP is regarded as an interior gateway protocol (IGP) it is also extensively used as an exterior gateway protocol for inter-domain routing due to its robustness and its capabilities to scale well in large networks.

Routing protocols need to be configured on routers according to specific network requirements. Performance of routing protocol and the router depends largely on correct configuration settings being used on the routers. The configuration requirements are specific to the network requirements and dictate the configuration of the router. When deploying EIGRP in a network its advanced capabilities and features such as Load Balancing and Route Summarisation can be used to increase network efficiency. It is therefore required to have a very good understanding of how EIGRP protocols works and the configuration requirements that are needed to make use of these features.

During the project different routing protocols will be compared and EIGRP will be analyzed in depth. The knowledge gained from the analysis and research will be used design test networks to test the capabilities of EIGRP. Evaluation of the test results and the research will be carried out and will also be documented in the form of a report. It will also outline major troubleshooting issues that exist for EIGRP deployment.

Aim

The aim of the project is to perform critical analysis of EIGRP routing protocol and outline configuration requirements to gain optimum routing performance in EIGRP networks, by making use of advanced features of the protocol.

Objectives

The objectives of the project are:

- To explain the need for Routed protocols and briefly describe commonly used Routed Protocols.
- To explain the need for Routing Protocols and compare routing protocols in common usage.
- To provide a background to EIGRP and its evolution from IGRP.
- To provide detailed information about EIGRP along with its advanced technologies, key features and capabilities such as: fast convergence, support for variable-length subnet mask, support for partial updates, support for multiple network layer protocols, neighbour discovery/recovery, Reliable Transport Protocol (RTP,) DUAL finite-state machine, Load Balancing, topology Table, neighbour Table and routing Table.
- To discuss and produce the configuration process/requirements for Implementation and Troubleshooting of EIGRP.
- To design a test network and the different testing scenarios to analyse and test capabilities of the protocol.
- To conduct analysis of the protocol by deploying it in the Test network under Lab conditions
- To use the test results and research to produce a report to show the actual capabilities of the protocol, along with the configuration requirements to enhance routing performance.

Justification

The project that is being undertaken will focus mainly on EIGRP routing protocol and its usage. There are several reasons for undertaking this project, some of which are briefly described below:

- EIGRP is one of the newly released routing protocols by Cisco and is described as a hybrid protocol which is as easy to implement as IGRP but provides advanced capabilities such as of OSPF and other link sate routing protocols. This project will allow for research into its newly added technologies and also analyse its capabilities, which makes it superior then its predecessor. This will lead to greater understanding of the newly added mechanisms, which makes this protocol superior to others.

- One of the major problems with the implementation of EIGRP is that there is not much documentation available about it. This is due to the fact that it is a proprietary protocol and the documentation provided by Cisco is all that can be found. During preliminary research it was also ascertained that there is very limited number of research carried out on the protocol and the documentation available is also very limited. This project will be used to produce a comprehensive report to the abilities, implementation and troubleshooting of the protocol which may be used during implementation of the protocol.

- Routing protocols are still being developed and new protocols are being researched and designed to increase routing efficiency. As the project will look in depth into EIGRP it is very possible that it may lead finding of flaws or possible enhancements that can be made to the protocol. This may lead to recommendations on improvements that can be made to the protocol and further research into new technologies.

- The project is being undertaken as the part of a degree in Computer Networking. This project will successfully show the knowledge gathered during the course and also enhance future development in academic knowledge. It will also enhance personal portfolio allowing excellent chances of gaining career objectives. Network administrators and designer with sound knowledge of EIGRP protocols are in great demand, which will further enhance my chances of meeting my career goals.

Scope

Defining the scope of a project is very important to its success. The scope is generally very closely related with deliverables, time and cost. In this case however it is different due to the nature of the project. The project is being undertaken as a part of degree course and has no cost issues related to it. The scope of the project is however greatly related to time and the required deliverables.

The objectives of the project have already been outlined and will need to be fulfilled for its successful completion. The final deliverable is in the form of a report, which will be discussed later during this proposal. A schedule has to be maintained, if all the objectives and the aim of the project are to be achieved within the given deadline.

The scope of the project will be only to achieve the objectives already defined, in order to fulfil the aim of the project and produce the report within the given deadline. As the deadline is fixed the project will not have any more tasks added to it. Any ideas or areas that may be researched will be documented separately and will be dealt with in future when provisions are available.

During the course of the project EIGRP routing protocol will be analysed. The analysis and test will be carried out on performance related issues of EIGRP. However, the source code of the protocol will not be analyzed or dealt with during the project. Areas directly related to the source code of the protocol are beyond the scope of this project. The functionality and behaviour of EIGRP will be researched both theoretically and practically through experiment carried out on test networks. Results from experiments and tests conducted will be used to verify the findings of the research and to make specific recommendations.

The supervisor has already agreed upon the Aim, Objectives and the deliverables of the project that define the scope and any changes will also have to be acknowledged.

Approach

A modular approach has been used to break the project down into several stages. This methodology used will ensure that a strict deadline for each stage can be assigned and followed to ensure that the project is completed within the deadline. The approach used will also ensure that each of the objectives set out for the project is met in order to achieve the aim of the project. The task carried out during the actual project will be divided into four major phases with each phase having sub-stages to them.
The phases that will be followed along with their sub-stages given below:

Research

This phase will consist of all the research that needs to be carried out during the project. The research method that will be used is known as "Action Research". Here primary, secondary and tertiary source of data will be actively searched and related material will be documented so that they may be used during the design and the write up of the report. The research will be carried out on three main areas that are detailed below:

- Routed Protocols: The research and investigation will be carried out using materials obtained from books, Internet and journals. This section of the research will not be very through or will not go into much depth. It will be used to gain an understanding and an overview of routed protocols. In the final report this research will be used to produce a section about Routed Protocols.
- Routing Protocols: Research on routing protocols will be carried out using materials found in books, journals, conference papers and the Internet. This research will be elaborate and will look into the subject area more deeply. This will allow for the comparison of the different routing protocols and also to understand the evolution of EIGRP from IGRP. This information obtained from this part of the research will be used to write a chapter in the final report about the routing protocols and the evolution of EIGRP from IGRP.

- EIGRP routing protocol: Books, conference papers, white papers, previous research materials and online material will be used to carry out a through research of the EIGRP routing protocol. This will allow for an understanding of all the key technologies and advanced feature of the protocol. Key technologies or areas that will be researched in details are: support for VLSM, manual route summarization, automated route summarization, re-distribution with other routing protocols, convergence issues, partial updates, support for multiple network layer protocols using protocol dependant modules, neighbour discovery/recovery, usage of RTP, DUAL, route selection, Tables used, route tagging, bandwidth usage for updates, load balancing over equal cost paths, load balancing over unequal cost paths and SIA problem. Configuration, implementation and troubleshooting issues of the protocol will also be researched to obtain a complete understanding of the capabilities and drawbacks of the protocol. This research will be used to write chapters in the final report about EIGRP and will also help in the design of the test network.

Design

This phase of the project will be used to design the experiments that need to be carried out for the analysis of EIGRP. The phase is divided into two smaller sections to make the task simpler and easier to handle.

- Firstly the materials gathered from the research will be used to determine the features of the protocol that are to be analysed. Depending on these scenarios will be drawn out which would have to be simulated in order for the tests to take place. Some of the areas that may be analysed are: convergence times and issues, DUAL and its functionality, neighbour discovery, neighbour relationship maintenance, neighbour recovery, Tables used and their contents, selection of successor, selection of feasible successor, route selections, effects of failure of links on network in different circumstances, local computation, diffusing computation, load balancing on both equal and unequal cost paths, usage of bandwidth by EIGRP, redistribution with other protocols, support for VLSM, automatic route summarization, manual route summarisation, issues with EIGRP in stub networks, issues with EIGRP in hub and spoke networks, SIA issues of EIGRP and overall efficiency. Additional tests may be carried out on issues that may come to light during further research of EIGRP.
- After the different experiment scenarios have been drawn up, a network will be designed for implementation of the scenarios. This network design will have to take into account all the scenarios that are to be tested and also the availability of the equipment for the test. A preliminary design of the test network has been drawn up (Figure 4) which can be found on page 46 of this proposal.

Experiment / Test

- After the network has been designed it will be set up in the Lab and the required scenarios will be simulated using different configuration. The configuration requirements for the scenarios will be taken from the research that has been done on EIGRP configuration and implementation. These different scenarios will be manipulated to provide the situation that is to be analysed to ascertain the capabilities of the protocol under the situation. These results of the tests will be documented in a logical order so that they may be analyzed later.

Production of the Final Deliverables

- This is the final task that will be carried out during the course of the project. During this stage the final project report, journal and project development website will be produced. The project report will use the research that has been carried out and the experiment results to provide an analysis of the EIGRP routing protocol along with supporting evidence. The results of the experiment will be shown in a form that is suiTable for a technical report and will support the conclusions drawn from the completion of the project.

Deliverables

The deliverables of projects vary according to the purpose of the project. The deliverable of a project can vary from gaining understanding, production of a report to manufacturing of a product. The project that is being proposed is an academic project and has defined deliverables. Due to the fact that this is an academic project that is being carried out as a part of a degree course it has additional deliverables other then the final project report.

All the major deliverables for this project are detailed below:

- **Presentation of Project Proposal-** A presentation needs to be given to the academic staff concerned with supervising the final year projects. This presentation will be used to present the project proposal and to convey the idea of what is expected at the completion of the project.

- **Project Proposal Website –** A website will have to be designed which will hold all related information about this project. The website will contain the project proposal, the presentation slides, details of the supervisor, details and CV of the person undertaking the project. The website will also contain the proposed Table of contents of the final project report. At the completion of the project this website will be updated with the final project report and related information.

- **Project Proposal -** This project proposal is also a deliverable concerned with the project.

- **Journal Publication on Project –** This will be the publication of a technical journal about the project

- **Final Project Report-** The final project report will be the main deliverable that will be produced. Completion and submission of this report will mark the ending of the project. This will consist of all the research carried during the project and give balanced arguments and opinion on each aspect that was researched. The report will also contain test results and all other information to meet the objectives and the aim of the project. The documentation will also draw a conclusion with supporting results from the project and discuss the necessary requirements to enhance network performance when using EIGRP.

- **Project Development Website –** This will include all information and documentation related to the project.

Milestones and Evaluation

The work that is to be carried out during the project has already been defined and described in the previous sections. The objectives of the project have been laid out and the approach to achieve those objectives has also been described. The approach will be followed in the stages they were laid out and this will allow for the objectives to be achieved in order.

Each of the objectives is regarded as a milestone of the project. Some of the objectives are very closely related and may be achieved through completion of inter-related tasks. At completion of each milestone the project will be evaluated and compared to the project plan to make certain that the project is on schedule and none of the tasks are lacking behind schedule. The plan and the time schedule for the project will be outlined in the project plan and management section of this proposal.

Each of the six deliverables may be regarded as major milestones of the project. The final project report is the final milestone of the project at the completion of which the project would have ended.

The four deliverables and their deadline are given below:

- Presentation of Project Proposal – 10th of January 2006
- Project Proposal Website – 17th of January 2006

- Submission of Project Proposal – 17th of January 2006
- Journal Publication on Project – 23rd May 2006.
- Project Development Website – 23rd May
- Submission of Final Project Report – 23rd of May 2006

A complete evaluation of the project along with its achievement will be done during the Viva Voce Examination.

Constraints & Assumptions

The project involves analysis of features of EIGRP routing protocol such as Load balancing, convergence times, DUAL and troubleshooting issues. For these analyses, EIGRP protocol needs to be configured on to a network and the performance of the routers would need to be tested. Various scenarios need to be created on the network to test all the features of the protocol. The experiment will be carried out on a test network that will be designed during the course of the project. The network designed will have to be such that it is able to exploit all weaknesses and capabilities of the protocol.

The remote lab access present at the university does not provide a complex enough topology that may be used to perform the experiments. It would have been much easier to conduct the whole experiment using remote lab, as this would save vital time that will now be wasted in setting up equipment every time experiments are to be conducted. Equipments that are available at the labs will also have to be taken into consideration during the design of the network. This may somewhat limit the design of the network. To make sure that the required equipment is available a proposed test network (Figure 4) was designed. The design of the network can be found in later section of this report.

All the tests and experiments carried out during the project will be performed on the test network that will be set up in the lab. The results from these tests will be used to validate and support findings during the project. Results from experiments done on real life networks may vary somewhat to that of the lab environment. However, in this case it is assumed that the lab network will produce similar results and will be able to simulate real life networks sufficiently so that correct conclusions can drawn from results obtained from the experiments.

Resources & Qualifications

As already discussed the project will involve experiments being carried out. To do the experiments a network will have to be designed and built in the labs. The institution where the project will be carried out has networking labs, which have more then sufficient equipment to support the project. Routers and other networking equipment are available at suiTable times to carry out the experiments. Remote Lab access is also available from the institution. Although the remote lab does not provide a complex enough topology to carry out the whole experiment it may however be useful during preliminary stages to test the methods that will be used to perform the experiments.

Previous studies undertaken by me related to networking have given me an overview of routed protocols, routing protocols, network configuration, troubleshooting and the TCP/IP layers. This background will allow for the required research to be undertaken and also for successful completion of the project in due course.

Project Plan & Risk Assessment

The only risk associated with this project is that it has to be made sure that there is no deviation from the project plan, that is all work carried out are within the scope of the project. This is why a project plan has been drawn up so that work carried out can be evaluated regularly to reduce the risk of deviation from the scope.

Project management plays the most important role in the success of any project. To be successful a project must have a plan to abide by. This is because most projects have to achieve all its objectives within a certain time period. In most projects cost is also associated with the objectives. However in the case of this particular project time is the only major concern. There are strict deadlines for each deliverable of the project that cannot be altered or extended.

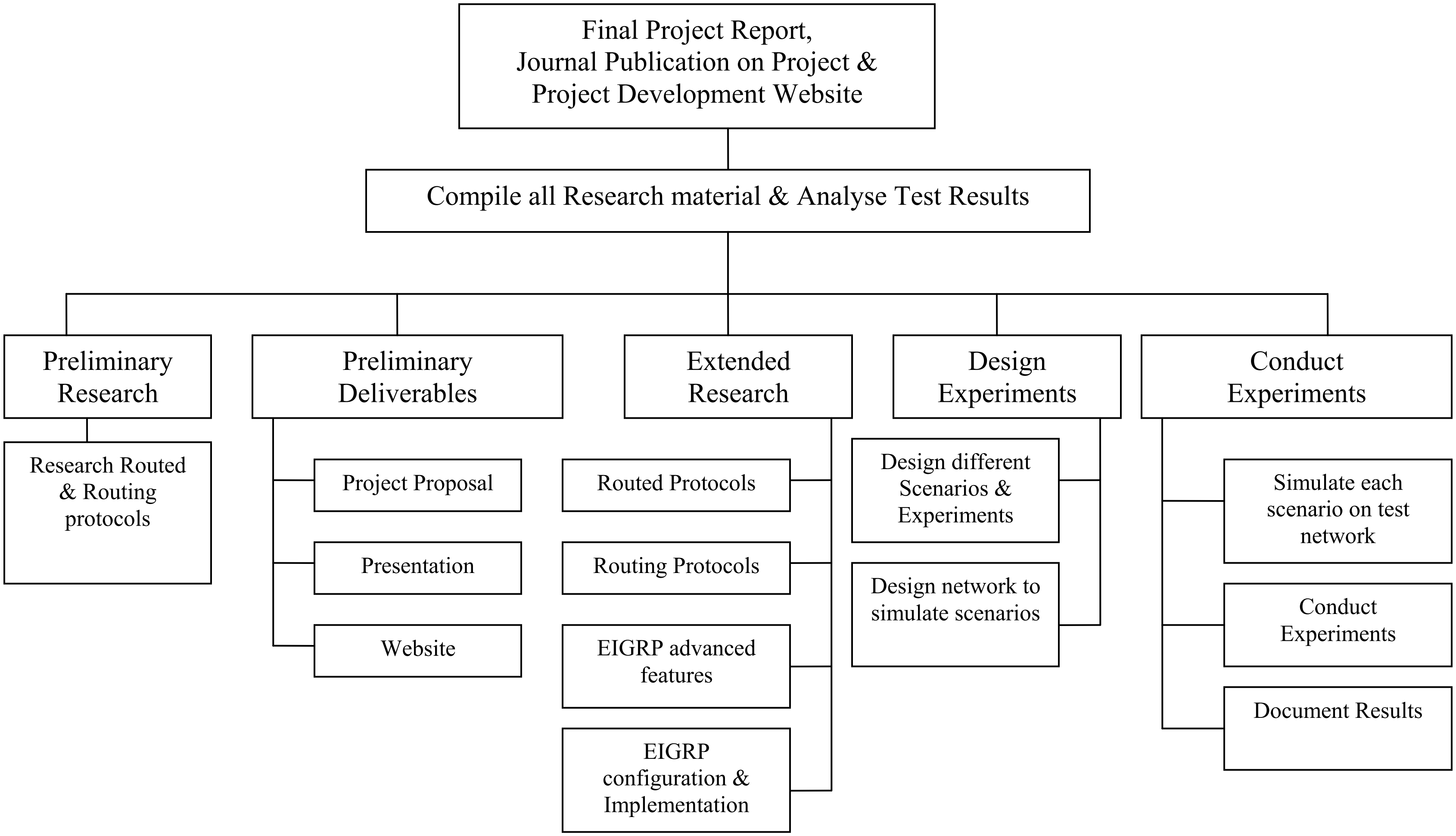
For a project to be successful and the project to be managed successfully all the objectives of the project must be SMART that is they must be specific, measurable, agreed up, realistic and time framed. The objectives of the project were chosen keeping this rule in mind. All the objectives of the project are specific, agreed upon, realistic and measurable.

The project is a big endeavour and will need to be divided up into tasks that may be carried out individually. These tasks can then be scheduled to make sure that the overall aim and the objectives of the project are met within the allocated time.

Each task will be carried out in a scheduled time frame so that the project is completed on time. The tasks are very closely related to the methodology being used and upon completion of each task objectives of the project will be met. A structure will be used to break the whole project down into more manageable smaller tasks.

A very effective way of representing the work that needs to be carried out during the project is through the use of Work Breakdown Structure Diagram (WBS). WBS doesn't show task dependencies or the time line by which a particular task must be completed. It only gives a structure that breaks down the project into phases and shows the task associated with each phase. In the case of this project the WBS diagram is very closely related to the methodology that is being used to achieve the aim of the project. WBS for the project (Figure 1) can be found on the next page.

Figure 1 - Work Breakdown Structure (WBS)


Final Project Report, Journal Publication on Project & Project Development Website
Compile all Research material & Analyse Test Results
Preliminary Research
Research Routed & Routing protocols
Preliminary Deliverables
Project Proposal
Presentation
Website
Extended Research
Routed Protocols
Routing Protocols
EIGRP advanced features
EIGRP configuration & Implementation
Design Experiments
Design different Scenarios & Experiments
Design network to simulate scenarios
Conduct Experiments
Simulate each scenario on test network
Conduct Experiments
Document Results

The WBS for the project has been used to identify the major tasks that need to be carried out for the completion of the project. The tasks are refined and detailed below in the logical order in which they should be carried out. Each task will also be assigned a task number for the ease of future referencing.

A - Preliminary Research
This consisted of preliminary research that was carried out on routed protocols, routing protocols and EIGRP.

B - Finalise Aims and Objectives
The information and knowledge gained from the preliminary research were used to finalise the aim and the objectives of the project.

C – Perform Preliminary Experiment
Preliminary experiments were carried out in the lab and using remote lab access to prove that the actual planned experiments to perform analysis of the protocol can be carried out. This also shows that the methodology/approach taken for the project can be followed and will be able to meet all the objectives and the aim of the project.

D – Presentation of Project Proposal
This will be done to present the project proposal to an audience consisting of lecturers and students of the university. The presentation will be used to convey the objectives, aim, approach and outcomes of the project.

E –Project Proposal Submission
The project proposal is to be drawn up and submitted in a written form by the given deadline.

F – Project Proposal Website
A website has to be designed and published containing the details of the project. The site will contain: details of student undertaking the project, details of project supervisor, project proposal, presentation slides, scanned images of the project logbook, proposed Table of contents of the final project report and the CV of the student.

G – Research about Routed Protocols.
Research will be carried out on routed protocols and materials found will be documented for later use and report write up.

H – Research about Routing Protocols
Elaborate research will be conducted on routing protocols. Information and material found will be documented for later use and report write up.

I – Conduct In-Depth Research on EIGRP
This will be a through research in to the key features and technologies used in EIGRP. Different scenarios where the protocols may be used will also be researched. This will also include detailed study of the abilities and capabilities of the protocol.

J – Research about EIGRP configuration, Implementation and Troubleshooting:
Here the configuration requirements for implementation of EIGRP will be researched in details. All its configuration commands will be documented. Examples of configuration usage for different scenarios will also be investigated.

K - Design Test Network and Test Scenarios
Knowledge gained from the completion of the above tasks will be used to design scenarios that may be used to test various functionalities and capabilities of the protocol. After the scenarios have been decided upon, a network will be designed where the scenarios may be simulated to give the desired environment for the relative experiments.

L – Perform Experiments and Record results
The experiments that are required to perform analysis of the protocol will be carried out. The designed scenarios and the designed test networks will be used for the purpose of the experiments. The results of the experiments will be documented so that they may be analysed later during the project report.

M - Analyse results and review all research materials
This task will consist of gathering of all the test results and the research materials in a logical order. Analysis of the test results from the experiments will be carried out and documented. The research material and the analysis of the results will be compared and conclusion will be drawn from both. This will be used to provide a balanced judgement during the final project report writing.

N – Compile, Complete and Submit the Final Deliverables
This is the final task that needs to be carried out for the completion of the project. During the previous task all related research material would have been sorted the test results would have been analysed. In this final task all the related materials and arguments will be put in the form of a technical report. After formatting the technical report to suit the needs of the final project report it will be submitted before the deadline marking the end of the project. Journal Publication on Project and the Project Development website will also be created.

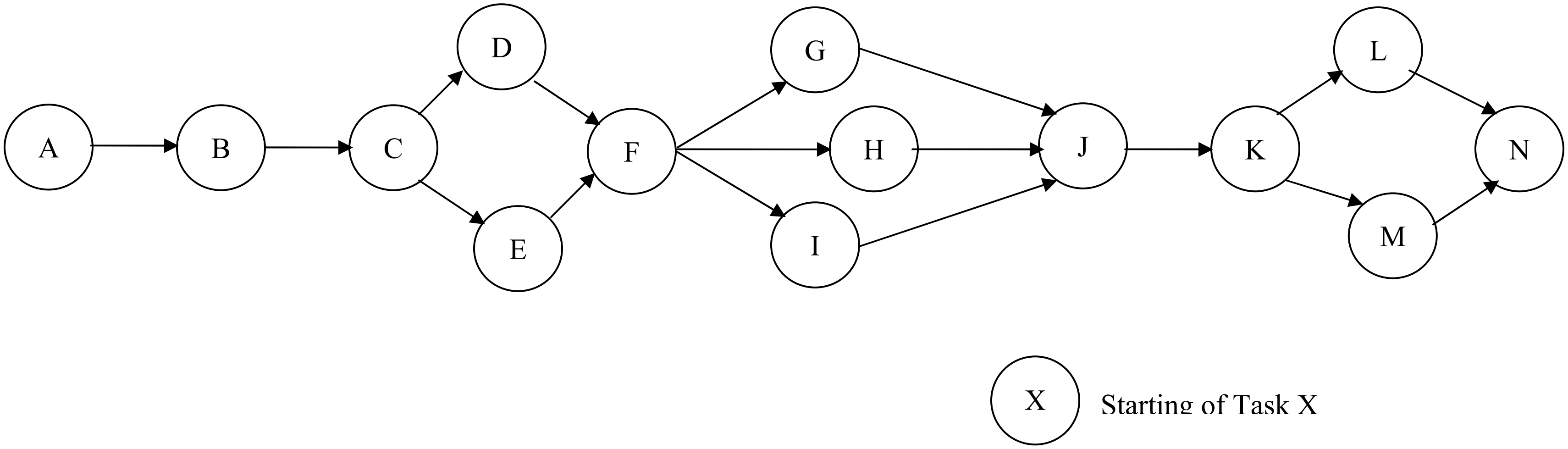
The Gantt chart (Figure 2) that is found on the next page shows all the tasks with respect to the timeline. The deliverables of the project can also be found in the Gantt chart that is being designed. This will allow the deadlines for both the tasks and the deliverables to be met. Pert chart (Figure 3) showing the task dependencies can be found on page 33 of this proposal.

Figure 2 - Gantt chart

Task	November ’05 (Weeks)				December ‘05 (Weeks)				January ‘06 (Weeks)				February ‘06 (Weeks)				March ’06 (weeks)				April ‘06 (Weeks)				May ‘06 (Weeks)			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
A - Preliminary Research		▒	█																									
B - Finalise Aims & Objectives			▒	█																								
C - Perform Preliminary experiments					▒	█																						
D - Project Proposal Presentation							▒	▒	▒	█																		
E - Complete Project Proposal					▒	▒	▒	▒	▒	▒	█																	
F - Complete Preliminary Project Website								▒	▒	▒	█																	
G - Research about Routed Protocols.												▒	█															
H - Research about Routing Protocols												▒	▒	█														
I – Conduct In-depth research of EIGRP													▒	▒	▒	▒	█											
J - Research about configuration of EIGRP																	▒	▒	▒	█								
K - Design Test Network & Test Scenarios																				▒	▒	█						
L - Perform Experiments & Record results																							▒	▒	█			
M – Analyze results and review all research materials																									▒	█		
N - Complete and Submit final deliverables																				▒	▒	▒	▒	▒	▒	▒	▒	█

Figure 3 - Port chart

▒ - Task Ongoing █ - Completion of Task


A
B
C
D
E
F
G
H
I
J
K
L
M
N
X
Starting of Task X

Although from the Gantt chart it may seem that the schedule that needs to be maintained during the project is very tight and missing the planned finishing time for any task could lead to significant problems, it is however not the case. Just like any project all the variables that affect the completion of a task can never be taken into account. This is why each task on the chart is allocated a generous estimate of the time when in reality the time needed for the task should be less then allocated. This leaves a small buffer in the event of failure to complete a task on time due to rise of any unavoidable circumstances.

From the Gantt chart it can be seen that just like most projects all the tasks do not need to be completed in a sequential manner. There are tasks that run at the same time and there are some tasks that are dependent on the completion of other tasks. The inter relation and dependencies of the task are shown in the Pert chart for the project. Each node in the pert chart marks the start of one of the tasks that have been defined previously. The notation of the node is the same as the task number of the task, whose starting is marked by the node. The tasks numbers used in the Gantt chart and the pert chart are the same as that assigned initially to each task. This makes it easier to relate each task to the different tools.

Preliminary Literature Review

The preliminary literature review carried out focused mostly on EIGRP. This was due to the fact that the aim and the objectives of the project are related to EIGRP. Some research was also carried out on other routing protocols and routed protocols in order to gain background information.

The sources of the literature include books, published white papers and the Internet. The literatures that have been reviewed are detailed below:

- **Cisco Systems, Inc. (2003)** *CCNA 3 and4 – Companion Guide,* Cisco Press, 3rd ed. ISBN 1587131137.
  Summary: Chapter 4 (page 115-146) of this book is about EIGRP. The chapter provides a comparison of EIGRP to IGRP, conceptual overview of EIGRP, convergence and basic operations of DUAL, EIGRP terminology, EIGRP data structures, route summarization, basic configuration and troubleshooting.
  This book provides a simplified overview of the routing protocols and does not go into depth on any of the features or topics of the protocol. This source was able to provide a good overview of the protocol.
- **Amphora, R. (2002)** *IP Routing,* O'Reilly, 1st ed. ISBN 0596002750.
  Summary: This book offers basic concepts of IP routing, free of hype and jargon. It begins with the simplest routing protocol, RIP, and then proceeds, in order of complexity, to IGRP, EIGRP, RIP2, OSPF, and finally to BGP. There is also quiet a lot of references to test networks with diagrams which help in understanding fundamental concepts behind each protocol. The chapter on EIGRP focuses on enhancements over IGRP: the use of DUAL; and the use of subnet masks in updates, which in turn allow VLSM and route summarization at arbitrary bit boundaries. It also gives comprehensive explanation of EIGRP Metric, Neighbour Relationship, Reliable Transport Protocol, EIGRP Packet Format, Route Summarization, configuration and troubleshooting.

The book provides a good background over development of EIGRP from IGRP and gives information about its advanced features. It is based more from a theoretical point of view and lacks the configurations for the advanced features. It however gives comprehensive overview and explanation of the other routing protocols, which allows them to be compared to EIGRP.

- **Popinjay, I. (1999)** *EIGRP Network Design Solution,* Cisco Press, ed. 1st ISBN 1578701651

  Summary: *EIGRP Network Design Solutions* uses case studies and real-world configuration examples to help gain an in-depth understanding of the issues involved in designing, deploying, and managing EIGRP-based networks. It details proper designs that can be used to build large and scalable EIGRP-based networks, and documents possible ways each EIGRP feature can be used in network design, implementation, troubleshooting, and monitoring. It also gives detailed coverage of all EIGRP technologies, including DUAL, transport protocol, and topology database. In addition there is extensive coverage of EIGRP deployment over WAN and dial-up networks and information on such features as filter lists, route maps, summarization, EIGRP pacing, and MD5 authentication.

- **Aziz, Z. & Liu, J. (2002)** *Troubleshooting IP Routing Protocols (CCIE Professional Development Series),* Cisco Press, ed. 1st ISBN 1587050196.

  Extraction of chapter "Troubleshooting EIGRP" available on the Internet at
  http://www.ciscopress.com/articles/article.asp?p=27839&seqNum=5&rl=1
  Date of access: 18/11/2005 22:07

  Summary: This article provides extensive, hands-on guide for troubleshooting EIGRP. It explains how to solve complex routing problems through methodical, easy-to-follow flowcharts and step-by-step scenario instructions for troubleshooting. It also provides numerous protocol-specific debugging tricks that speed up problem resolution

- http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2017.htm

  Date of access: 18/11/2005 22:29

  The above URL provides the link to the chapter titled "Integrating Enhanced IGRP into Existing Networks" which is a part of the Cisco "Internetwork Design Guide". The website and its contents are maintained by CISCO Sys.

  Summary: This chapter provides a detailed guide to configuring EIGRP integration with other protocols. It provides various scenarios where the configuration is being done and also provides detailed explanations of how the integration is achieved. It covers adding EIGRP to a single IGRP network, adding EIGRP to multiple IGRP networks, adding EIGRP to a Novell IPX network and also adding EIGRP to an AppleTalk Network.

- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/en_igrp.htm#xtocid0
  Date of access: 18/11/2005 22:49

  The above URL provides the link to the chapter titled "Enhanced IGRP" which is a part of the Cisco "Internetwork Design Guide". The website and its contents are maintained by CISCO Sys.

  Summary: This chapter provides a brief history into the making of EIGRP and outlines the four key technologies that are employed by EIGRP along with simple explanation of DUAL, redistribution and migration to EIGRP.

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/np1_c/1cprt1/1ceigrp.htm *Date of access: 18/11/2005 23:09*

  The above URL provides the link to the chapter titled "Configuring EIGRP" which is a part of the Cisco "Part2: IP Routing Protocols". The website and its contents are maintained by CISCO Sys.

  Summary: This chapter describes how to configure Enhanced Interior Gateway Routing Protocol (E IGRP). It describes Cisco's EIGRP Implementation, EIGRP benefits, Configuration Task List, Common Configuration commands and provides scenarios to show common configuration mistakes that occur.

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fiprrp_r/1rfeigrp.htm *Date of access: 18/11/2005 23:23*

  The above URL provides the link to the chapter titled "EIGRP Commands" which is a part of the Cisco "Command Reference". The website and its contents are maintained by CISCO Sys.

  Summary: This page provides all the EIGRP command available with examples. This can be a very useful resource, which can be used when performing EIGRP configuration

- EIGRP – White paper available at
  http://www.ssuet.edu.pk/~amkhan/cisco/EIGRP_white_paper.pdf

  Date of access: 18/11/2005 23:31

  The white paper is also available from authenticated CISCO sites.

  Summary: The white paper provides detailed explanation on most EIGRP related topics. It gives details of EIGRP theory of operation, Split Horizon and Poison Reverse issues, Troubleshooting SIA, Redistribution, Route Summarization, Query Process and Range, Bandwidth configuration, Load Balancing, Metric configuration, using Administrative Tags and detailed usage of show IP EIGRP Topology.

- http://www.rhyshaden.com/eigrp.htm *date of access: 18/11/2005 21:53.*

Summary: This webpage gives brief information on EIGRP routing metrics but provides a comprehensive reference to EIGRP packets, Neighbour discovery and adjacencies, the DUAL Finite State Machine and Diffusing Computation.

- http://www.unix.org.ua/cisco/CCNP-CCDP/CID-Sybex/ewtoc.html *date of access: 19/11/2005 19:23.*

  The above URL provides a link to the CCDP: Cisco Internetwork Design Study Guide.
  Summary: Chapter 4 of this guide is concerned with designing networks for IP routing protocols. It has a subsection that is concerned with the network design for network using EIGRP. Although the guide doesn't provide much information about the protocol it highlights some design issues that need to be considered when designing networks for EIGRP. It gives an overview of the DUAL mechanism and provides an explanation with diagram about the convergence of EIGRP. It discusses other factors such as RTP, SIA, Load balancing and bandwidth usage.

- http://www.cisco.com/warp/public/105/46.html *date of access: 19/11/2005 20:17.*

  The above URL provides a link to the document titled "How does Load Balancing work?" with the document id 5212 on the Cisco website.
  Summary: The document provides a simple overview of the idea behind load balancing in networks. It also explains how the Cisco IOS on routers support load balancing by default. It then provides links to IGRP metrics and Explanations. It also provides another link to a document that details the method by which the metric of EIGRP can be manipulated to set preferred routes.

- http://www.cisco.com/warp/public/103/19.html *date of access: 19/11/2005 21:48*

  The above URL provides a link to the document titled "How does Unequal cost path load balancing (Variance) work in IGRP and EIGRP?" with the document id 13677 authored by *Syed Faraz Shamim* on the Cisco website.
  Summary: The document provides detailed information on how to perform load balancing on unequal cost path on a network. The document also provides significant explanation and diagrams of test networks that may be used during the course of the project. The document also outlines some of the required commands that are needed to perform load balancing with unequal cost paths.

- http://www.cisco.com/warp/public/103/18.html *date of access: 19/11/2005 22:24.*

  The above URL provides a link to the document titled "What does EIGRP DUAL-3-SIA Error message mean?" with the document id 13676 on the Cisco website.
  Summary: This document provides complete information about the EIGRP Stuck in Active issue. This is one of the major issues of EIGRP that a network administrator needs to have complete knowledge of in order to be able to reduce downtime. It give complete background information to the problem, the reasons for which the problem may occur and also the solutions to this problem.

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt2/1cdeigrp.htm *date of access: 19/11/2005 23:12.*

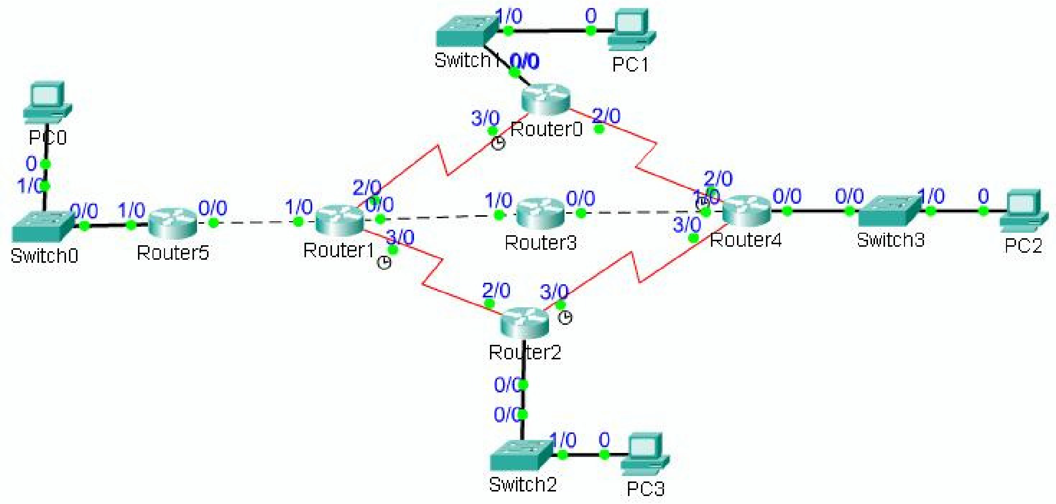
  Summary: This document provides information about Cisco EIGRP implementation. If provides the configuration commands that are needed for the deployment of EIGRP. This document also explains some configuration setting in details with the aid of diagrams and different scenarios. The configuration provided in this document mainly concerns transition to EIGRP from IGRP, adjusting EIGRP metric, disabling router summarization, manual route summarization, authentication, changing hold time , changing hello packet intervals, disabling split horizon and stub networks. It contains various examples of configuration to provide a better understanding of the related issues.

Preliminary Work Done

Preliminary research was carried out by studying material on routed protocols and routing protocols. Further research was carried out on EIGRP routing protocol that allowed enough understanding of the protocol to decide upon the aim and objectives of the project.

Remote Lab access available at the institution was used in order to test and verify methods that have been outlined in the methodology to perform the experiments on the small test network. The remote lab sessions were successful and showed that the same technique can be used during the experiment phase to perform analysis of EIGRP routing protocol. This confirms that the methodology that has been outlined in this project proposal can be followed. It further shows that the objectives and the aim of the project can be achieved by following the approach outlined in this proposal. Details of the remote lab experiment including the initial experiment network diagram (Figure A-1), configuration used and the outputs obtained can be found in *Initial Practical Work* section of this proposal.

The research carried out on EIGRP also allowed for enough insight into the protocol and its key capabilities, to start the designing of the actual test network. A proposed design for the test network (Figure 4) has been drawn up which may be used to perform the experiments that need to be carried for analysis. The design of the test network has not been finalized and may require changes depending on the information that is obtained when further research is carried out during the course of the project.



Proposed Test Network Design (Figure 4)

The proposed network has taken into account all the possible test scenarios that need to be simulated. The test network will be used to conduct experiments on the following areas:

- Convergence times and issues.
- DUAL and its functionality
- Establishment of neighbour relationship
- Neighbour relationship maintenance and recovery.
- Tables used and their contents during different scenarios
- Selection process of Successor
- Selection process of Feasible Successor
- Convergence after link failure when Feasible Successor is available: Local computing.
- Convergence after link failure when Feasible Successor is not available: Diffusing Algorithm.
- Load Balancing over equal cost paths.
- Load Balancing over unequal cost paths.
- Usage of network bandwidth during and after convergence.
- Redistribution with other routing protocols
- Support for VLSM and Route summarization.
- Issues of Hub and Spoke design
- SIA and other troubleshooting issues.

Table of Contents for Final Report (Proposed)

1.8 Project organization
2. Literature Review
2.1 Overview of Router Protocols
2.2 Description of Router Protocols
2.3 Overview of Routing Protocols
2.4 Brief description of common routing protocols
2.5 Background of EIGRP
2.6 Description of EIGRP
2.6.1 EIGRP overview
2.6.2 EIGRP Key Technologies
2.6.2.1 Neighbour relationship
2.6.2.1.1 Forming relationship
2.6.2.1.2 Hello Packets and Usage
2.6.2.1.3 Maintaining Neighbour relationships
2.6.2.1.4 Information exchanged with neighbours
2.6.2.2 DUAL
2.6.2.2.1 FSM
2.6.2.2.2 Successor
2.6.2.2.3 Feasible Successor
2.6.2.2.4 Advantages
2.6.2.2.5 Disadvantages
2.6.2.2.6 Route Selection
2.6.2.2.6.1 Tables Used
2.6.2.2.6.1.1 Neighbour Table
2.6.2.2.6.1.2 Topology Table
2.6.2.2.6.1.3 Routing Table
2.6.2.2.6.2 Route selection
2.6.2.3 RTP
2.6.2.3.1 Functionality
2.6.2.3.2 Advantages
2.6.2.4 Protocol dependent Modules
2.6.2.4.1 Functionality Advantages.
2.6.3 EIGRP Advanced Feature
2.6.3.1 Load Balancing
2.6.3.1.1 Equal cost path load balancing
2.6.3.1.2 Unequal cost path load balancing
2.6.3.2 Support for VLSM
2.6.3.3 Router Summarisation
2.6.3.3.1 Automatic Route Summarization
2.6.3.3.1.1 Description
2.6.3.3.1.2 Advantages and disadvantages.
2.6.3.3.2 Manual Route Summarization
2.6.3.4 Redistribution with other networks
2.6.3.4.1 IGRP
2.6.3.4.2 RIP
2.6.3.4.3 OSPF
2.6.4 Issues with EIGRP
2.6.4.1 SIA
2.6.4.2 Convergence issues
2.6.4.3 Hub and Spoke Network Issues

2.6.4.4 Stub Network Issues
2.6.5 EIGRP Implementation
2.6.5.1 EIGRP implementation issues
2.6.5.2 Configuration
2.6.5.2.1 Basic configuration
2.6.5.2.2 Advanced Configuration
2.6.6 Troubleshooting EIGRP
3. Design of Experiment
3.1 Design of Test Scenarios
3.1.1 Neighbour discovery and relationship
3.1.2 Usage of hello packets and BW consumed
3.1.3 Neighbour recovery
3.1.4 Initial convergence times
3.1.5 Dual Mechanism
3.1.5.1 Successor
3.1.5.2 Feasible Successor
3.1.5.3 Route Selection
3.1.5.4 Table Status
3.1.5.4.1 Topology
3.1.5.4.2 Neighbour
3.1.5.4.3 Routing
3.1.6 Convergence times due to link failure
3.1.7 Load Balancing
3.1.7.1 Equal Cost paths
3.1.7.2 Unequal Cost paths
3.1.8 SIA issues
3.1.9 Router Summarization
3.1.9.1 Manual
3.1.9.2 Automatic
3.1.10 Redistribution with other protocols
3.1.10.1 Route Tagging
3.1.10.2 Metrics
3.1.10.3 Administrative distances
4. Method and Execution
4.1 Methodology
4.1.1 Research
4.1.2 Design
4.1.3 Experiment
4.1.4 Report writing
5. Analysis of Results
5.1 Neighbour relationship
5.2 Convergence times and issues
5.3 Dual Mechanism
5.4 Route Selection
5.5 Recovery from failure
5.6 SIA issues
5.7 Produced a balanced conclusion from the results
6. Critical Evaluation
6.1 Evaluation of Research carried out
6.2 Evaluation of Experiments carried out

6.3 Evaluation of achievement of objectives
6.4 Evaluation of achievement of final aim
6.5 Overall evaluation of the project
7. Conclusion
7.1 Conclusion from Research
7.2 Conclusion from Experiments
7.3 Balanced overall Conclusion.
References and Bibliography
Glossary
Index
Appendix –A – Project Plans
Appendix B – Network Design
Appendix C – Test Plans
Appendix D – Detailed Test Results
Appendix E – EIGRP configuration commands

Conclusion

The project proposal has been created after initial investigation and research on the subject area, which provided a good understanding of the theme area of the project. The objectives and the aim of the project have been set to allow through research of the subject area and in-depth analysis of EIGRP routing protocol. The scope of the project and the justification for carrying out the project has been defined along with the major milestones and deliverables. The approach or methodology that will be used to achieve aim and objectives of the project has also been outlined. The approach that is used for this project uses a modular design to break the project down into research, design and experiment phases that makes management of the project easier. Project management skills have been applied to draw out a project plan to carry out the necessary work and complete the project successfully on time. Related project management tools such as WBS, Gantt chart and Pert chart for the project has also been included in this proposal. All the project tasks and deliverables have been allocated a time frame using Gantt chart so that progress during the project can be closely monitored. Literature and materials that were reviewed have been detailed and referenced in the proposal. Furthermore to prove that the methodology that is being proposed can be followed and it can also be used to achieve the objectives and the aim of the project, initial experiments were conducted. The result of the initial experiment has been attached to *Initial work Done* section of this proposal.

The proposed project has been well researched and planned. The objectives and the aim of the project are attainable if the outlined methodology and schedule are followed.

References and Bibliography

- **Kirkman, J. (1999)** *Full Marks: Advice on Punctuation for Scientific and Technical Writing* 3rd ed, Ramsbury Books.

- **Kirkman, J (1992)** *Good Style – Writing for Science and Technology, Spon.*
- **Van Emden, J (2001)** *Effective Communication for Science and Technology,* Palgrave.
- **Gowers, E. (1997)** *The complete Plain Words,* Pelican. revised 1997
- **Fraser, J (1995)** *Professional Proposal Writing,* Gower, 1995
- **Technical Report writing Notes** by Dr. Saeed R Taghizadeh
  URL:
  http://homepages.unl.ac.uk/~taghizas/Digital%20Systems/Microprocessors/EE203/EE203.html
  Date of access: 7th December 2005
- **Report writing and Project Management Notes by** Dr. N. Ioannides
  URL:
  http://homepages.unl.ac.uk/~ioannidn/EE249.htm
  Date of access: 1st January 2006

- **Cisco Systems, Inc. (2003)** *CCNA 3 and4 – Companion Guide,* Cisco Press, 3rd ed. ISBN 1587131137.
- **Malhotra, R. (2002)** *IP Routing,* O'Reilly, 1st ed. ISBN 0596002750.
- **Pepelnjak, I. (1999)** *EIGRP Network Design Solution,* Cisco Press, ed. 1st ISBN 1578701651
- **Aziz, Z. & Liu, J. (2002)** *Troubleshooting IP Routing Protocols (CCIE Professional Development Series),* Cisco Press, ed. 1st ISBN 1587050196.
- http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2017.htm *Date of access: 18/11/2005 22:29 Integrating Enhanced IGRP into Existing Networks*
- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/en_igrp.htm#xtocid0
  Date of access: 18/11/2005 22:49 Enhanced IGRP
- http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/np1_c/1cprt1/1ceigrp.htm *Date of access: 18/11/2005 23:09 Configuring EIGRP*
- http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fiprrp_r/1rfeigrp.htm *Date of access: 18/11/2005 23:23 EIGRP Commands*
- *EIGRP – White paper* http://www.ssuet.edu.pk/~amkhan/cisco/EIGRP_white_paper.pdf
- http://www.rhyshaden.com/eigrp.htm *date of access: 18/11/2005 21:53.*
- http://www.unix.org.ua/cisco/CCNP-CCDP/CID-Sybex/ewtoc.html *date of access: 19/11/2005 19:23. CCDP: Cisco Internetwork Design Study Guide.*
- http://www.cisco.com/warp/public/105/46.html *date of access: 19/11/2005 20:17.How does Load Balancing work?*

Initial Practical Work

The remote lab access available from the university was used to perform a preliminary experiment. The topology used during the experiment is given below:

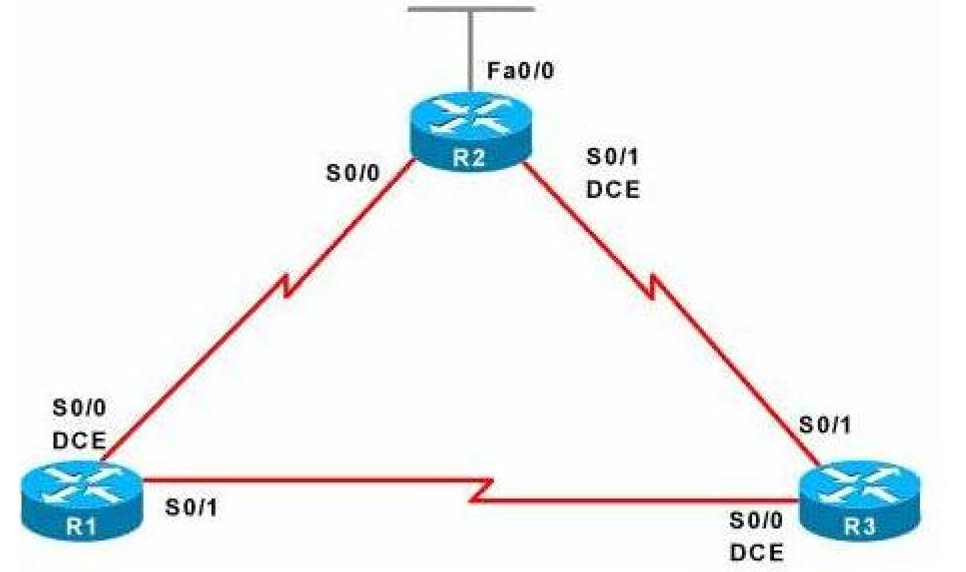


Figure A-1

Topology for network used for initial Experiment.

All the three routers were configured with EIGRP routing protocol using sub-netted network addresses. After initial convergence of the network link failure was simulated by administratively shutting down the serial link between Router R2 and Router R3. The scenario was used to perform some simple tests of the protocol.

The initial tests were carried out on the following areas:

- Contents of Routing Table before failure of link
- Contents of Topology Table before failure of link
- Use of Hello Packets in maintaining neighbour relationship.
- The effect of link failure on:
  - Topology Table
  - Routing Table
- Diffusing computing after failure of link as no feasible successor was available.
- Local computing when the link was reactivated.
- DUAL mechanism of updating neighbours with new routing information.

The configuration settings for the routers are given below:

Configuration for Router R1

```
interface Serial0/0
 ip address 192.168.64.1 255.255.255.252
 clockrate 64000
!
interface Serial0/1
 ip address 192.168.1.1 255.255.255.0
!
```

```
router eigrp 100
 network 192.168.1.0
 network 192.168.64.0
!
End
```

Configuration for Router R2

```
interface FastEthernet0/0
 ip address 192.168.72.1 255.255.255.0
!
interface Serial0/0
 ip address 192.168.64.2 255.255.255.252
!
interface Serial0/1
 ip address 192.168.64.6 255.255.255.252
 clockrate 64000
!
router eigrp 100
 network 192.168.64.0
 network 192.168.72.0
!
End
```

Configuration for Router R3

```
hostname SanJose2
!
interface Serial0/0
 ip address 192.168.1.2 255.255.255.0
 clockrate 64000
 no shutdown
!
interface Serial0/1
 ip address 192.168.64.5 255.255.255.252
 no shutdown
!
router eigrp 100
 network 192.168.1.0
 network 192.168.64.0
!
End
```

The content of the following Tables was extracted from Router R3 showing the topology Table after initial convergence.

Initial Topology Table of Router R3

```
IP-EIGRP Topology Table for AS(100)/ID(192.168.64.5)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.72.0/24, 1 successors, FD is 20514560, serno 7
         via 192.168.64.6 (20514560/28160), Serial0/1
         via 192.168.1.1 (21026560/20514560), Serial0/0
P 192.168.64.0/30, 1 successors, FD is 21024000, serno 8
         via 192.168.64.6 (21024000/20512000), Serial0/1
P 192.168.64.0/24, 1 successors, FD is 20512000, serno 5
         via Summary (20512000/0), Null0
         via 192.168.1.1 (21024000/20512000), Serial0/0
P 192.168.64.4/30, 1 successors, FD is 20512000, serno 4
```

```
         via Connected, Serial0/1
P 192.168.1.0/24, 1 successors, FD is 20512000, serno 1
         Via Connected, Serial0/0
```

The content of the following Tables was extracted from Router R3 showing the Routing Table after initial convergence. The Table shows the protocols ability to support VLSM.

Initial Routing Table of Router R3

```
D    192.168.72.0/24 [90/20514560] via 192.168.64.6, 00:01:13, Serial0/1
     192.168.64.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.64.0/30 [90/21024000] via 192.168.64.6, 00:01:13, Serial0/1
D       192.168.64.0/24 is a summary, 00:01:14, Null0
C       192.168.64.4/30 is directly connected, Serial0/1
C    192.168.1.0/24 is directly connected, Serial0/0
```

The following Table shows extracts of debugging output of Router R3. The output shows sending and receiving of hello packets on each link during normal operation of EIGRP. It can be seen that the interval of packets received or sent on any link is 5 seconds, which is default for high bandwidth networks.

Exchange of Hello Packets

```
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK)
SanJose2#
00:05:48: EIGRP: Sending HELLO on Serial0/1
00:05:48: EIGRP: Received HELLO on Serial0/0 nbr 192.168.1.1
00:05:50: EIGRP: Sending HELLO on Serial0/0
00:05:51: EIGRP: Received HELLO on Serial0/1 nbr 192.168.64.6
00:05:53: EIGRP: Sending HELLO on Serial0/1
00:05:53: EIGRP: Received HELLO on Serial0/0 nbr 192.168.1.1
00:05:55: EIGRP: Sending HELLO on Serial0/0
00:05:55: EIGRP: Received HELLO on Serial0/1 nbr 192.168.64.6
```

The following Table shows extracts of debugging output of the router showing diffusing computing taking place after the simulated link failure. The output shows DUAL trying to find and use feasible successor to reach network whose connection has been lost due to the link failure. When feasible successor to the destination network cannot be located the routes become active. After new route information is received from other neighbours, DUAL flushes old route information and installs the new routes. To complete the process it updates all its neighbours with the changes in its routing Table.

Diffusing Computing after simulated link failure

```
00:08:29: DUAL: Find FS for dest 192.168.64.4/30. FD is 20512000, RD is
20512000
```

```
00:08:29: DUAL: Dest 192.168.64.4/30 entering active state.
00:08:29: DUAL: Find FS for dest 192.168.72.0/24. FD is 20514560, RD is
20514560
00:08:29: DUAL: Dest 192.168.72.0/24 entering active state.
00:08:29: DUAL: Find FS for dest 192.168.64.4/30. FD is 4294967295, RD is
4294967295
found
00:08:29: DUAL: Removing dest 192.168.64.4/30, nexthop 192.168.1.1
00:08:29: DUAL: No routes.  Flushing dest 192.168.64.4/30
00:08:29: DUAL: dual_rcvreply(): 192.168.72.0/24 via 192.168.1.1 metric
21026560/20514560
00:08:29: DUAL: Find FS for dest 192.168.72.0/24. FD is 4294967295, RD is
4294967295
found
00:08:29: DUAL: Removing dest 192.168.72.0/24, nexthop 192.168.64.6
00:08:29: DUAL: RT installed 192.168.72.0/24 via 192.168.1.1
00:08:29: DUAL: Send update about 192.168.72.0/24.  Reason: metric chg
00:08:29: DUAL: Send update about 192.168.72.0/24.  Reason: new if
Output omitted . . . .
```

The following Tables show extracts from router output showing the Routing Table and the topology Table respectively after the simulated link failure and completion of DUAL calculations.

Updated Routing Table

```
D    192.168.72.0/24 [90/21026560] via 192.168.1.1, 00:00:23, Serial0/0
D    192.168.64.0/24 [90/21024000] via 192.168.1.1, 00:06:55, Serial0/0
C    192.168.1.0/24 is directly connected, Serial0/0
```

Updated Topology Table

```
IP-EIGRP Topology Table for AS(100)/ID(192.168.1.2)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.72.0/24, 1 successors, FD is 21026560, serno 11
         via 192.168.1.1 (21026560/20514560), Serial0/0
P 192.168.64.0/24, 1 successors, FD is 21024000, serno 3
         via 192.168.1.1 (21024000/20512000), Serial0/0
P 192.168.1.0/24, 1 successors, FD is 20512000, serno 2
         via Connected, Serial0/0
```

The following Table shows extracts from the router output showing DUAL calculations taking place after the link between Router R2 and R3 is re-activated. This shows DUAL local computing feature. As soon as Router R3 receives information of better routes to the destination networks it installs the new routes and updates all its neighbours with the changes to its routing Table.

Local Computing: DUAL (Reactivated failed link)

```
00:09:31: DUAL: dest(192.168.72.0/24) not active
00:09:31: DUAL: dual_rcvupdate(): 192.168.72.0/24 via 192.168.64.6 metric
20514560/28160
00:09:31: DUAL: Find FS for dest 192.168.72.0/24. FD is 21026560, RD is
21026560
00:09:31: DUAL:         192.168.1.1 metric 21026560/20514560
00:09:31: DUAL:         192.168.64.6 metric 20514560/28160 found Dmin is
20514560
00:09:31: DUAL: RT installed 192.168.72.0/24 via 192.168.1.1
00:09:31: DUAL: RT installed 192.168.72.0/24 via 192.168.64.6
00:09:31: DUAL: Send update about 192.168.72.0/24.  Reason: metric chg
00:09:31: DUAL: Send update about 192.168.72.0/24.  Reason: new if
```