THE POTENTIAL BENEFITS AND CHALLENGES OF USING LAYER 3 IPV6 CONFIGURATION COMMANDS IN INDUSTRIAL COMMUNICATION ROUTERS AND MULTILAYER SWITCHES

by

Benjamin Chalikosa

Submitted in partial fulfilment of the requirements for the degree
Master of Engineering (Computer Engineering)

in the

Department of Electrical, Electronic and Computer Engineering
Faculty of Engineering, Built Environment and Information Technology

UNIVERSITY OF PRETORIA

April 2016

SUMMARY

THE POTENTIAL BENEFITS AND CHALLENGES OF USING LAYER 3 IPV6 CONFIGURATION COMMANDS IN INDUSTRIAL COMMUNICATION ROUTERS AND MULTILAYER SWITCHES

by

Benjamin Chalikosa

Supervisor:	Prof G.P. Hancke
Department:	Electrical, Electronic and Computer Engineering
University:	University of Pretoria
Degree:	Master of Engineering (Computer Engineering)

Keywords: Benefits, challenges, configuration commands, EIGRPv6, GNS3, hierarchical topology, HSRPv2, industrial communication, IPv6, multilayer switches, OSPFv3, ping, routers, redundancy, RIPng, ring topology, round trip time, static unicast IPv6 addresses, traceroute, transition techniques

This study investigates the potential benefits and challenges of using layer 3 Internet Protocol version 6 (IPv6) configuration commands. Although any other type of layers 3 devices could have been used in this study, only Cisco routers and multilayer switches are considered. The study is conducted using a simulator called Graphical Network Simulator-3 (GNS3). Even though real Cisco Internetwork Operating System (IOS) software is reliably used in this simulator, an avoidable limitation of this method involves not using this software on real routers and multilayer switches. However, it has been found that contrary to Cisco documentation, using the outgoing local interface as next hop address causes IPv6 static routing not to work; it only works when the neighbouring global unicast address is used as the next hop address. Other findings show that when static addresses are configured with Routing Information Protocol Next Generation (RIPng), Enhanced Interior Gateway Routing Protocol version 6 (EIGRPv6) or Open Shortest Path First version 3 (OSPFv3), RIPng has the best round-trip time (RTT), while OSPFv3 gives the best traceroute results. Likewise, 64-bit Extended Unique Identifier (EUI-64) addresses produce better RTT and traceroute results with RIPng than with EIGRPv6 and OSPFv3. Nonetheless, one challenge for RIPng involves failure to start the RIPng process by misconfiguring the ipv6 router rip

name and ipv6 rip name enable commands. The benefit of EIGRPv6 is that its RTT is faster than that of OSPFv3 and even if the router identifiers (router-ids) are configured the same on all the routers, the EIGRPv6 process still works well. However, configuring different autonomous system numbers and failing to configure the "no shutdown" or router-id commands results in routing challenges. On the other hand, configuring the same router-id on different layer 3 devices causes OSPFv3 not to work. In spite of this challenge, when OSPFv3 is used with Hot Standby Router Protocol version 2 (HSRPv2), it generates faster RTT than EIGRPv6 and RIPng. However, the success rate of OSPFv3 for failover time of the active router to the standby router is 4% lower than EIGRPv6. In comparison to Internet Protocol version 4 (IPv4), configuring of static and EUI-64 address commands is a very challenging task, because of the hexadecimal nature of IPv6 addresses. Despite this challenge, one benefit of these commands is the ability to use slash notation such as /64 for the prefix length. When used on dual stack commands, static addresses give better native router processing performance with no encapsulation overheads. However, configuring these addresses on dual stack commands in large networks is a challenge. With regard to manual IPv6 tunnelling, configuring the tunnel interface addresses in the same network and failure to configure the tunnel mode ipv6ip command, prevents this technique from working. Although IPv6 static Network Address Translation-Protocol Translation (NAT-PT) commands are easy to configure and to troubleshoot, the NAT-PT router raises the challenge of being a single point of failure in the network. On the whole, given these benefits and challenges, implementing IPv6 in industrial networks should not be scary. The results of this study are useful guidelines on how to efficiently design and configure IPv6 networks in a smooth way.

OPSOMMING

DIE POTENSIËLE VOORDELE EN UITDAGINGS VAN DIE GEBRUIK VAN LAAG-IPV6-KONFIGURASIE-OPDRAGTE IN INDUSTRIËLE KOMMUNIKASIEROETEERDERS EN MULTILAAGSKAKELAARS

deur

Benjamin Chalikosa

Studieleier:	Prof G.P. Hancke
Departement:	Elektriese, Elektroniese en Rekenaaringenieurswese
Universiteit:	Universiteit van Pretoria
Graad:	Magister in Ingenieurswese (Rekenaaringenieurswese)
Sleutelwoorde:	Voordele, uitdagings, konfigurasie-opdragte, EIGRPv6, GNS3, hiërargiese topologie, HSRPv2, industriële kommunikasie, IPv6, multilaagskakelaars, OSPFv3, ping, roeteerders, oortolligheid, RIPng, ringtopologie, heen-en-terugtyd, statiese enkelstapel-IPv6-adresse, traceroute, oorgangstegnieke

Hierdie studie ondersoek die potensiële voordele en uitdagings van die gebruik van laag 3-Internet Protokol weergawe 6- (IPw6) konfigurasie-opdragte. Alhoewel enige ander tipe laag3-toestelle in hierdie studie gebruik kon word, is slegs Cisko-roeteerders en multilaagskakelaars gebruik. Die studie is uitgevoer deur die gebruik van ’n simulator genaamd Grafiese Netwerksimuleerder-3. Hoewel werklike Cisko-Internetwerk Opererende Sisteem- (IOS) sagteware op betroubare wyse in hierdie simulator gebruik is, hou een vermybare beperking van hierdie metode in dat hierdie sagteware nie op werklike roeteerders en multilaagskakelaars gebruik word nie. Daar is nietemin bevind dat in teenstelling met Cisko-dokumentasie, die gebruik van die uitgaande plaaslike koppelvlak as volgende sprongadres veroorsaak dat statiese roetering nie werk nie; dit werk slegs as die naburige globale enkelstapel-adres as die volgende sprongadres gebruik word. Ander bevindinge was dat wanneer statiese adresse gekonfigureer word met Roeteer-informasieprotokol Volgende Generasie (RIPvg), Verhoogde Interne Poortroeteringprotokol weergawe 6 (VIPRPw6) of Oop Kortste Baan Eerste weergawe 3 (OKBEw3), RIPvg die

beste heen-en-terugtyd (HTT) het, terwyl OKBEw3 die beste spoorroeteresultate lewer. Insgelyks lewer 64-bis Uigebreide Unieke Identifiseerder-adresse (EUI-64) die beste HTT en spoorroeteresultate met RIPvt eerder as VIPRPw6 of OKBE3. ’n Uitdaging vir RIPvg is egter onvermoë om die RIPvg-proses te inisieer deur die IPw6-roeteerderripnaam en IPw6-ripnaam se ontsper-opdragte verkeerd te konfigureer. Die voordeel van VIPRPw6 is dat die HTT daarvan vinniger is as OKBEw3, en selfs as die roeteerder-ids eenders gekonfigureer word op al die roeteerders, werk die VIRRPw6-proses nog goed. As verskillende autonome sisteemgetalle egter gekonfigureer word en nagelaat word on die “geen-afskakeling-” of roeteerder-id-opdragte te konfigureer, veroorsaak dit roeteerderprobleme. Aan die ander kant versoorsaak konfigurasie van dieselfde roeteerder-id op verskillende laag3-toestelle dat OKBEw3 nie werk nie. Nieteeenstaande hierdie uitdaging genereer OKBEwv3 vinniger HTT as VIPRPw6 and RIPvg wanneer dit saam met Warm Bystandroeteerderprotokol weergawe 2 gebruik word. Nogtans is die suksessyfer van OKBEw3 vir terugvaltyd van die aktiewe roeteerder tot die bystandroeteerder 4% laer as EIGRPv6. In vergelyking met Internetprotokol weergawe 4 (IPv4), is die konfigurasie van statiese en EUI-64-adres-opdragte ’n baie uitdagende taak weens die heksadesimale aard van IPw6-adresse. Nieteenstaande hierdie uitdaging is een voordeel van hierdie opdragte die vermoë om skuisnsstreepnotasie soos /64 te gebruik vir die voorvoegsellengte. Wanneer hulle in dubbelstapel-opdragte gebruik word, lewer statiese adresse beter moederroeteerderprosesseringwerkverrigting met geen enkapsuleringbokoste nie.. Om hierdie adresse in groot netwerke met dubbelstapel-opdragte te konfigureer, is nietemin ’n uitdaging. Wat handtonnel-l IPv6 betref, verhoed konfigurasie van die tonnel-koppelvlakadresse in dieselfde netwerk en nalating om die tonnelmodus-IPw6ip-opdrag te konfigureer hierdie tegniek om te werk. Hoewel IPw6 statiese Netwerk-adres-Vertaalprotokol-vertaling-opdragte (NAV-VO) maklik is om te konfigureer en foute op te spoor, bied die NAV-VO-roeteerder die uitdaging dat dit ’n enkele punt is waar die netwerk kan faal. In die lig van hierdie voordele en uitdagings, behoort die implementering van IPw6 in industriële netwerke oor die algemeen nie intimiderend te wees nie. Die resultate van hierdie studie is nuttige riglyne oor hoe om IPw6-netwerke effektief te ontwerp en konfigureer sonder probleme.

LIST OF ABBREVIATIONS

3DES-SHA	Triple data encryption standard - secure hash algorithm
4RD	IPv4 residual deployment
4RD-NAT	IPv4 residual deployment - Network address translation
6LoWPAN	IPv6 over low power wireless personal area networks
ADSTM	Advanced dual stack transition mechanism
AFRINIC	African Network Information Centre
AH	Authentication header
APNIC	Asia Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
ARP	Address resolution protocol
ASN	Autonomous system numbers
CAN	Content aware network
CERNET	China Education and Research Network
CGA	Cryptographically generated address
CPU	Central processing unit
DAD	Duplicate address detection
DES-MD5	Data encryption standard- message-digest algorithm 5
DHCP	Dynamic host configuration protocol
DHCPv6	Dynamic host configuration protocol for IPv6
DNS	Domain name system
DNS-ALG	Domain name system application-level gateway
DSCP	Differentiated services code point
DS-LITE	Dual-stack lite
DSTM	Dual stack transition mechanism
ELW4OVER6	Enhancement of lightweight 4over6
EPC	European patent convention

ESP	Encapsulating security payload
FAN	Flow aware networks
FMIPv6	Fast handover for mobile IPv6
FPMIPv6	Fast proxy mobile IPv6
FTP	File transfer protocol
GNS3	Graphical network simulator-3
GRE	Generic route encapsulation
IANA	Internet Assigned Numbers Authority
ICMP	Internet control message protocol
ICT	Information and communications technology
IDS	Intrusion detection system
IDSMIPv6	Intrusion detection system model for IPv6
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IID	Interface identifier
IMS	IP multimedia subsystem
IOS	Internetwork operating system
IOT	Internet of things
IP	Internet protocol
IPS	Intrusion prevention systems
IPSEC	Internet protocol security
IPTV	Internet protocol television
IPv4	Internet protocol version 4
IPv6	Internet protocol version 6
ISATAP	Intra-site automatic tunnel addressing protocol
I-SERP	IPv6 security risk prototype

ISO TC 204	International Organisation for Standardization Technical Committee 204
ISP	Internet service provider
IVI	IPv4 to IPv6
LACNIC	Latin America and Caribbean Network Information Centre
LAN	Local area network
LW4OVER6	Lightweight 4over6
MIPv6	Mobile IPv6
MTU	Maximum transmission unit
NAT	Network address translation
NAT64	Network address translation for IPv6 to IPv4
NAT-PT	Network address translation/Protocol translation
NDP	Neighbour discovery protocol
NID	Network intrusion detection
OS	Operating system
P2P	Point to point
PET	Prefixing, encapsulation and translation
PMIPv6	Proxy mobile IPv6
PQ	Priority queuing
RFID	Radio frequency identification
RIPE-NCC	Reseaux IP Europeens Network Coordination Centre
RIR	Regional Internet Registry
RPL	Remote program load
RTT	Round-trip time
SBIIT	Socket identifier based IPv4/IPv6 (SBIIT) translator
SDN	Software defined networking

SMS	Short message service
SMTP	Simple mail transfer protocol
SNMP	Simple network management protocol
SSAS	Simple secure addressing scheme
SSL	Secure sockets layer
SYN	Synchronise
TCP	Transmission control protocol
TTL	Time to live
UDP	User datagram protocol
UN	United Nations
V2OIP	Voice and video over internet protocol
VOIP	Voice over internet protocol
VPN	Virtual private network
WFQ	Weight fair queuing
WIFI	Wireless fidelity
WIMAX	Worldwide interoperability for microwave access
WSAN	Wireless sensor and actuator networks
WSNs	Wireless sensor networks

ACKNOWLEDGEMENT

Without the advice, suggestions and guidance of my supervisor, Prof G.P. Hancke, the writing of this dissertation would not have been successful. Therefore, sincere gratitude and much appreciation are registered to him.

Further appreciation is extended to all the lecturers in the Computer Engineering Department, for equipping me with the much needed honours degree knowledge in Computer Engineering. This knowledge contributed much to success in writing this dissertation.

Special thanks also to Almighty God, for being the creator of the knowledge in the dissertation and for his constant love, protection and care during the period of research. The support, patience and encouragement of my family are also highly appreciated.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1 INTRODUCTION

1.1 PROBLEM STATEMENT

1.1.1 Context of the problem

In order to have more functionalities for modern industrial network devices and because of the imminent depletion of IPv4 addresses, a new version of IP called IPv6 can now be deployed in industrial communication networks. This new protocol is an upgrade of the current IPv4 protocol and is the next generation internet protocol for many industrial applications and services. In comparison to its predecessor, IPv6 offers a number of improved features and functions such as large address space of 128 bits, efficiency in packet forwarding, authentication and encryption of end to end network communication, and ability of nodes to determine their own addresses. More importantly, it is able to offer quality of service markings of flow labels and packets for identification of priority traffic, and has simpler ways of handling roaming or mobile nodes. In addition to these important features, IPv6 also has global unicast addresses, link-local addresses and unique local addresses as its three main types of unicast addresses which are useful for designing efficient industrial LAN and WAN networks. In like manner, RIPng, OSPFv3 and EIGRPv6 are its well enhanced interior routing protocols for the dynamic discovery of IP routes. However, unlike IPv4 addresses which are written in an easy to understand decimal format, IPv6 addresses are written in complex hexadecimal form and make use of a colon to separate each field of 16 bits. Nevertheless, this hexadecimal format is likely to bring about new network designs and applications for industrial communication systems [4].

Although this new protocol comes with the above and many other advantages, there is a problem of lack of knowledge of how IPv6 layer 3 configuration commands impact the performance of industrial routers and multilayer switches. Given the novelty and complex hexadecimal nature of IPv6 addresses, the effects of configuring these addresses on interior routing protocols are still not known by many network engineers. Not knowing the impact of these configurations on routers and multilayer switches can lead to poor design, implementation, monitoring and management of IPv6 industrial communication networks.

This is because these two layer 3 devices are key elements in the design, operation and management of networks. When they are misconfigured, industrial networks becomes difficult to manage and to operate efficiently. Even though there has been some studies on the usage and implementation of IPv6 configuration commands in enterprise (office) networks, many of these studies focuses on IPv4 to IPv6 transition techniques [50-78] and on resolving security issues [99-142]. Moreover, their centre of attention is on enterprise networks whose network topology design differ from industrial networks.

Thus, a study which investigates potential benefits and challenges of using layer 3 IPv6 configuration commands in industrial communication networks can remedy the above problem. As a result, many network engineers who have no experience on using IPv6 can know beforehand the challenges and benefits involved in the configuration process of layer 3 commands before they transition their networks to this new protocol. Knowing the benefits of using these commands can motivate them to expeditiously implement IPv6 in their networks, whereas knowing the challenges can help them to effectively design, monitor and troubleshoot the networks.

1.1.2 Research gap

Despite many technological discussions on the benefits and challenges of integrating IPv6 in different types of communication systems, there are still many unanswered questions on how this new protocol affects industrial communication networks. An important area missing in most of these discussions and research is the potential benefits and challenges of using IPv6 layer 3 configuration commands in industrial routers and multilayer switches. Hence, according to the purpose of this study, this research gap is investigated and filled.

1.2 RESEARCH OBJECTIVE AND QUESTIONS

This study covers the research objectives and questions described below.

1.2.1 Research objectives

- To determine the benefits and challenges of using static and EUI-64 address configuration commands on routers and multilayer switches in industrial networks.

- To determine the benefits and challenges of using static routing, RIPng, EIGRPv6 and OSPFv3 configuration commands on routers and multilayer switches in industrial communication networks.
- To determine which transition technique gives the best round trip time (RTT) and traceroute time when dual stack, manual IPv6, ISATAP and GRE transition techniques are configured with RIPng, EIGRPv6 or OSPFv3 in a ring topology of industrial communication routers and multilayer switches.
- To determine which interior routing protocol gives the best RTT and traceroute time when static routing, RIPng, EIGRPv6 or OSPFv3 are configured on static addresses in a ring or hierarchical industrial communication networks.
- To determine the differences and similarities in the usage of IPv4 and IPv6 layer 3 configuration commands.

1.2.2 Research questions

- What are the benefits and challenges of using static and EUI-64 address configuration commands on routers and multilayer switches in industrial communication networks?
- What are the benefits and challenges of using static routing, RIPng, EIGRPv6 and OSPFv3 configuration commands on routers and multilayer switches in industrial communication networks?
- Which transition technique gives the best RTT and traceroute time when dual stack, manual IPv6, ISATAP and GRE transition techniques are configured with RIPng, EIGRPv6 or OSPFv3 in a ring topology of industrial communication routers and multilayer switches?
- Which interior routing protocol gives the best RTT and traceroute time when RIPng, EIGRPv6 or OSPFv3 are configured on HSRPv2 redundancy protocol in hierarchical industrial communication networks?
- What are the differences and similarities in the usage of IPv4 and IPv6 layer 3 configuration commands?

1.3 APPROACH AND HYPOTHESIS

The following approach and hypothesis guided the direction and writing of this research:

1.3.1 Approach

A quantitative approach is used in this study because it is more exploratory and quantifies the data being analysed. Another reason for using this approach is that in the majority of cases involving this approach, the results are well defined and consist of absolute values. On the other hand, a qualitative approach is more inclined to use words rather than figures when collecting and analysing data and is not appropriate for this study. The quantitative approach also gave the researcher the ability to perceive the benefits and challenges of using IPv6 layer 3 configuration commands in greater detail and helped to refine the hypothesis and research questions further. In addition, this approach enabled the researcher to learn and understand the research problem fully and to predict the outcome correctly. Therefore, because of using a quantitative approach in this study, this research successfully explored the potential benefits and challenges of using layer 3 IPv6 configuration commands in industrial communication routers and multilayer switches.

1.3.2 Hypothesis

If IPv6 layer 3 configuration commands are configured on routers and multilayer switches then there will be potential challenges and benefits in the operation of industrial communication networks because of the new format of IP addresses and interior routing protocols.

1.4 RESEARCH GOALS

In the light of using IPv6 layer 3 configuration commands, the following are the research goals of this study:

- To provide information to IT service providers and industrial communication companies on the challenges and benefits of using IPv6 layer 3 configuration commands for industrial multilayer switches and routers.
- To help network engineers to efficiently design, configure, operate and manage IPv6

layer 3 industrial communications networks.

- To promote the usage of IPv6 in industrial communications networks.

1.5 RESEARCH CONTRIBUTION

The following are the contributions of this study to the field of computer engineering:

1.5.1 Network engineers

This study adds to the knowledge of network engineers by providing IPv6 layer 3 information on how to design, configure and troubleshoot routers and multilayer switches in industrial communication networks.

1.5.2 Experimental research tool

Oftentimes, researchers at universities use network simulators that cannot be installed with real IOS images to simulate the operation of switches and routers. Thus, with the usage of GNS3 network simulator in this study, another useful experimental research tool of networking is contributed to the area of computer engineering. GNS3 enables researchers to emulate many and different types of systems, such as Linux virtual machines, Juniper routers, windows virtual machines, Cisco routers and switches. Researchers can even connect the GNS3 simulated networks to real-world networks and be able to analyse and capture packets using wireshark.

1.5.3 IPv6 reference guide

Students and researchers studying the impact of IPv6 on routers and multilayer switches can use this study as a reference guide. Although Cisco commands are used on all the configurations, most of the concepts can still be applied to other brands of layer 3 devices as well.

1.6 OVERVIEW OF STUDY

This dissertation presents the outcome of research on the potential benefits and challenges of using IPv6 layer 3 configuration commands on routers and multilayer switches in industrial communication networks. Chapter 1 gives an explanation of the problem statement, research objectives and questions, hypothesis and approach, research goals and contributions.

The material in Chapter 2 is about literature study on the depletion of IPv4 addresses, benefits of integrating IPv6 in different types of communication systems and IPv6 transition techniques. Furthermore, this chapter reviews some challenging features of IPv6 and analyses potential applications and services of this new protocol. Vulnerabilities and security risks of IPv6 and the reasons for using a GNS3 simulator in this research are presented in this chapter as well. The chapter also reviews types of IPv6 addresses, routing protocols, tools for testing network connectivity, operation of routers and multilayer switches.

Chapter 3 presents the designed ring and hierarchical network diagrams for industrial communication networks and the methods used to configure IPv6 layer 3 configuration commands. These commands explain how to configure transition techniques, HSRPv2, static unicast and dynamic addresses, RIPng, EIGRPv6, OSPFv3 and static routing.

Configuration results are shown in Chapter 4 and discussed in Chapter 5. In the latter chapter the following are discussed: benefits and challenges of using IPv6 layer 3 configuration commands, traceroute time of RIPng, EIGRPv6 and OSPFv3 on static unicast and EUI-64 addresses. Similarly, the RTT of RIPng, EIGRPv6 and OSPFv3 on the HSRPv2 protocol, transition techniques, static unicast and EUI-64 addresses is also discussed. This chapter further examines the differences and similarities in the usage of IPv4 and IPv6 layer 3 configuration commands. The chapter ends with a discussion on the maturity level of IPv6 Cisco IOS software and the potential benefits and challenges of using ring and hierarchical network designs for industrial communication networks.

Finally, chapter six closes the work with the conclusion and recommendations for future research.

CHAPTER 2 LITERATURE STUDY

2.1 CHAPTER OBJECTIVES

The objectives of this chapter are to:

- Review whether IPv4 address exhaustion is real or not;
- Identify potential applications and services for IPv6;
- Identify and analyse IPv4-to-IPv6 transition techniques;
- Identify challenging features of IPv6;
- Review the vulnerabilities and security risks of IPv6;
- Identify the best network simulator for this research between GNS3 and Cisco packet tracer.
- Identify whether research on the potential benefits and challenges of using IPv6 layer 3 configuration commands in industrial communication routers and multilayer switches has been done before or not; and
- Review the operation of IPv6 addresses, routers, multilayer switches, routing protocols and testing tools for network connectivity at layer 3.

2.2 IPV4 ADDRESS EXHAUSTION IS REAL

Over the last 10 to 20 years, there has been a high demand for IP addresses because of new networking technologies and the growth of the internet. This development resulted in the running out of the IANA pool of IPv4 addresses on 3 February 2011. On that day, the last five blocks of IPv4 addresses were assigned to the five regional internet registries (RIRs). Within a short time the RIRs also exhausted their assigned blocks of addresses. APNIC, the RIR for the Asia-Pacific region, exhausted its block of unallocated IPv4 addresses in April 2011. RIPE-NCC, the RIR for Europe and surrounding areas, exhausted its available number of IPv4 addresses in September 2012. LACNIC, the RIR for Latin America and the Caribbean, exhausted its available number of IPv4 addresses in June 2014. ARIN, the RIR for Canada, the Caribbean and North Atlantic islands and the United States, was expected to exhaust its available block of IPv4 addresses in 2015 and by mid-2014 AFRINIC the RIR for Africa was the only RIR still giving its small supply of IPv4 addresses to ISPs for regions it was servicing [1]. Thus, there are no more available IPv4 addresses to meet the high demands of internet service providers (ISP), industrial communication and enterprise networks.

Without new IP addresses, it is extremely difficult to innovate or develop new applications and services for industrial and enterprise communication networks. Therefore, to help solve the IPv4 address shortage problem, short-term and long-term solutions have been suggested by the Internet Engineering Task Force (IETF), an organisation that is mandated to run the affairs of the internet. These short-term solutions involve the use of NAT and private IP addresses. Although these two techniques have helped to lessen the IPv4 address shortage for about a decade, the demand for more IP addresses continues. Moreover, the use of NAT with private addresses has proved to be very expensive and complicates network designs [2], [3]. This means that industrial communication and enterprise networks cannot continue to rely on using these short-term solutions for most applications and services.

Fortunately, the long-term solution of using IP version 6 (IPv6) provides a new way forward to enable industrial communication and enterprise networks to use services and applications without implementing NAT. This new protocol is also the ultimate answer to the IPv4 address shortage problem because of its abundance of IP addresses. Whereas IPv4 addresses are only 32 bits long, IPv6 addresses are 128 bits long, giving about three hundred and forty trillion trillion unique addresses. This address space is more than enough to meet the current and future needs of the internet and industrial communication systems. However, because these addresses are longer than IPv4 addresses in length, they cannot be represented in the form of IPv4 with a decimal or hexadecimal subnet mask. Instead, they use slash notations such as /64 to separate the prefix of the first half of the address from the last half, called the interface identifier. Some examples of IPv6 global addresses are 3000::1, 2002:AB:E:2:7CDF:9:0::12, 3001:A15::B231, 2001:13AA:1567:A012:B570:421C::0 and 3451:2340:0000:4000:A123:5000:2561:0010. Furthermore, note that unlike IPv4 addresses, which are written in decimal format, IPv6 addresses are written in hexadecimal form and make use of a colon to separate each field of 16 bits. This hexadecimal format is likely to bring about new network designs and applications for industrial communication systems [4].

Given the IPv4 address exhaustion facts and the abundance of IPv6 addresses, it is now imperative for RIRs to encourage service providers (ISPs) to transition their IPv4 networks to IPv6. The ISPs should also educate their customers about IPv4 address depletion not being a fallacy but a reality. Hence, both industrial communication and enterprise customers should be encouraged to start planning how to migrate their current IPv4 networks successfully to IPv6. Part of that planning requires network engineers to examine how this new protocol affects different network services and applications.

2.3 DIFFERENT TYPES OF IPV6 APPLICATIONS AND SERVICES

Not only does IPv6 solve the IPv4 address shortage problem; it also provides significant benefits when integrated in different types of communication systems. Its features of mobility support, autoconfigurations, security and abundant address space have helped to develop communication systems in telecommunications, aviation and residential networks. For ISP communication systems, IPv6 makes it possible to implement IP applications and services successfully, which cannot be sustained by the current IPv4 network infrastructure. Furthermore, with the removal of NAT in IPv6 protocol, ISP networks are now easier to design, configure and operate. This is because local IPv6 addresses do not require translation when accessing public networks. Satellite communication systems and geonetworking are other areas of communication that have benefited from IPv6 protocol as well [5]. Indeed, IPv6 has also proved to be very useful in the design of communication systems for education, medical and defense use [6]. In addition, the benefits of IPv6 are also seen in the innovation of a new generation of services and applications, such as IPv6 plug and play network devices [7], [8], management of large area lighting systems [9], IPv6 fieldbus protocols [10], software-defined networking [11], [12], smartgrids [13], [14], bittorrent and utorrent transport protocol [15], ad hoc networks [16], intelligent surveillance systems and robot software architecture [17], [18], home automantion [19], intelligent transportation [20], IPv6 workstations [21], [22], global identity [23], [24], green power plants [25], e-learning and e-health systems [26], [27], IPv6 mobolity protocols [28-32], IPv6 internet of things (IOT) technology [33-35], wireless sensor and actuators [36], auto-configuration and self-managing of devices and networks [37], [38], improving of security in wireless sensor networks [39-41], vehicular wireless access networks [42], improving of routing lookup algorithms [43], WIMAX wireless networks [44], radio frequency identification [45], voice over IP and IPv6 television [46], IPv6 smart meter technology and smart parking systems [47].

As a result of the above and many other new applications and services of IPv6 to different communications systems, the United Nations has noted that the current rate of information and communication technology (ICT) usage and development will see about fifty million devices connected to the internet by 2020. Without doubt, IPv4 will not be able to provide such a huge number of IP addresses, making the IPv6 protocol a necessity and a requirement for most applications. For this reason, enterprises and governments are required to work together and hasten the adoption of IPv6, especially in industrial communication networks. During this adoption period, careful attention should be paid to scalability, device capabilities, service provider system architecture and network management [48]. However, even as governments work together to ensure that IPv6 technology receives the attention that it deserves, it is important to know that all of the above new applications depend on the efficient design and configuration of layer 3 devices (routers and multilayer switches). These devices are the backbone of most networks and have great impact on how traffic flows in networks. Hence, it is important to study and examine their behaviour in IPv6 networks. IPv6 traffic features such as traffic volume, flow size, packet size, flow duration and distribution of the packet size should be known [49]. Understanding of these traffic features leads to innovation of new traffic management policies and network designs for IPv6 networks.

2.4 ANALYSIS OF IPV4–TO-IPV6 TRANSITION TECHNIQUES

There is no doubt that the future of IP addresses depends totally on IPv6 because of its outstanding advantages over IPv4. Despite these advantages, transitioning from IPv4 to IPv6 cannot be done within one week. These two protocols will continue to co-exist for a long time and it will take a prolonged period to transition fully from IPv4 to IPv6 networks. Therefore, it is important to examine the different transition techniques that can be used by industrial communications networks during the coexistence period. Examining these techniques helps network engineers to know the strengths and weaknesses associated with each transition technique [50].

2.4.1 Dual stack mechanism

During the initial implementation of IPv6 nodes, most organisations may use the dual stack transition mechanism (DSTM), since it supports both IPv6 and IPv4 networks. However, it is important to know that using this technique increases the chances of security threats and attacks on both IPv6 and IPv4 networks. Therefore, to help detect these threats, a lightweight penetration test tool [50] is needed to identify vulnerabilities in the networks. The idea of using test tools in dual stack networks is good because it helps to detect threats early and this prevents unnecessary network interruptions in industrial communication networks. Moreover, the test tool makes it easy for network engineers to troubleshoot faults in dual networks. Other than the security challenge, the current conversion mechanism for DSTM takes more time than expected (delay) and this has a negative effect on the overall performance of the packet transmission rate. Thus, a fast packet transmission algorithm [51] that can help reduce the time delay of data packet transmission can be used. This technique substitutes DSTM with an advanced dual stack transition mechanism (ADSTM) by making use of the IP header compression techniques. The results show that the total performance of ADSTM is 8% better than that of the ordinary DSTM.

However, despite the above challenges and issues concerning this transition mechanism, DSTM is one of the most suitable and reliable transition mechanisms for newly installed networks. It provides seamless transition from IPv4 to IPv6 and does not affect end user applications. Its ability to allow both IPv4 and IPv6 packets to be transmitted simultaneously by most prevailing software and hardware is a big advantage to both industrial communication and enterprise networks [52].

2.4.2 Tunnelling mechanism

In addition to DSTM, tunnelling is also one of the transition techniques that may be used by most ISPs. The most common types of tunnelling are manually configured and 6to4 tunnelling mechanisms. Because these two transition techniques are relatively easy to configure, they are likely to be used by most organisations, hence it is important to compare their network performance. A comparison of bandwidth utilisation, routing traffic, routing convergence and consumption of network resources [53] shows that manually configured tunnels are suitable for static networks that have bandwidth constraints and carry network applications that are not sensitive to delay. However, if the network carries applications that are delay-sensitive and require faster network convergence, then using 6to4 is better than the manually configured tunnelling mechanism. On the other hand, an evaluation report in [54] shows that 6to4 tunnelling is not a proper tool for industrial or enterprise business needs. Its network parameters of throughput, tunnelling overhead and RTT for UDP and TCP transmission protocols are not very good. Therefore, it is suitable for experiments related to research, which do not consider the load capacity of the network devices.

It is also important to know that at the early stage of developing IPv6, this transition technique may be used by intruders to inject a packet at the tunnel endpoints by spoofing the address of the packet and from where it is originating. Although a firewall may be used to prevent this security threat, there is a high possibility that because of the coexistence of IPv6 and IPv4 networks, one of the protocols may not be noticed by the firewall owing to it being encapsulated in the other protocol. One way of preventing this problem is by using IPsec to authenticate the incoming packets. However, in order to secure the tunnel endpoints thoroughly, using separate firewalls [55] to filter IPv6 and IPv4 packets ensures that no packet escapes the process of filtering. A good thing about the application of separate firewalls at the tunnel endpoints is that it has no major effect on filtering time neither does it cause delay.

2.4.2.1 The tunnelling effect on internet applications

When planning industrial and enterprise network tunnelling techniques, it is very important to compare the network performance of internet applications between IPv6-to-IPv4 networks with those of IPv6-only or IPv4-only networks. For this reason differences in delay effects and bandwidth requirements in the above three networks are investigated [56]. The findings of this experiment confirm that the size of the packets generated by the application determine the performance of the above three model networks. Applications with smaller packet sizes suffer from the encapsulation of the data through the tunnelling effect and the overhead of the larger header size of IPv6. Results furthermore show that the 6to4 tunnelling mechanism needs higher bandwidth than IPv4-only and IPv6-only networks. Other notable observations are that video streaming has the lowest bandwidth requirement compared to other applications. End-to-end delay and remote login experienced the greatest changes in delay when transmitted over tunnelling and IPv6 networks. However, video streaming, data and voice communication had similar sizes for each application.

2.4.2.2 The impact of integrated routing and addressing on 6to4 tunnelling

Among the reasons for the slow deployment of IPv6 is the total decoupling of IPv4 addressing and routing. Therefore, to help speed up this deployment, a mechanism called integrated routing and addressing is used to integrate IPv4 addressing and routing with IPv6. Integration of routing and addressing is realised by making use of a new format for addresses obtained from the use of a new type of encapsulation and format of the address obtained from IPv4. Integrated addressing and routing extends the concept of a 6to4 transition mechanism, which requires IPv6 routers to have one integrated routing table. This integration of addressing and routing greatly simplifies network management, in contrast to the approach of running a pure IPv6 network. In the integrated routing and addressing approach, there is no need to maintain two routing and addressing schemes, which means that the routing policies and topology are not duplicated. This saves time and resources on the convergence and management of the networks, subsequently making troubleshooting faster and easier [57]. This process also decreases the cost of management during the period of IPv4 and IPv6 coexistence. Although the concept of integrated routing and addressing extends the concept of a 6to4 transition mechanism, this idea works better on routing protocols than on transition techniques.

2.4.3 Comparison of ISATAP, dual stack and 6to4 tunnelling mechanisms

A comparison of ISATAP, 6to4 tunnelling and DSTMs [58] shows that the DSTM for IPv6 networks yields better performance than ISATAP and 6to4 tunnelling mechanisms. Moreover, the 6to4 tunnelling mechanism has a greater encapsulation impact on the performance of devices when used in an IPv6 network and is not easy to implement. On the other hand, a dual stack is not difficult to implement, since it enjoys greater support from the current network devices [59]. In the case of multi-protocol label switching (MPLS) networks, performance evaluation between IPv6 and IPv4 with MPLS and 6to4 tunnelling shows that the data transfer in IPv6 MPLS tunnels is better than in IPv6 and IPv4 networks. This is due to the fact that MPLS accelerates the speed of finding the next hop through avoiding the process of calculating the next hop for each and every packet [60]. MPLS technology has many benefits in IPv4 networks, therefore, it is important to see how it affects IPv6 in industrial communication networks. Hence, dedicated research on MPLS and IPv6 is needed.

2.4.4 Roaming and network performance of translation mechanism

In most of the IPv4-to-IPv6 translation mechanisms, the IPv4 addressing scheme only permits IPv4 nodes to roam in IPv4 foreign networks or IPv4 home networks. However, this scheme does not permit roaming in IPv6 networks. Realising the need of an IPv4 addressing system to roam in IPv6 networks, a new addressing mechanism [61] that uses an IPv4 care of address in IPv6 networks is suggested. This mechanism ensures that IPv4 node addresses roam in IPv6 networks and prevents the generation of duplicate addresses. Even though this mechanism solves the IPv4 and IPv6 roaming problems, translation techniques cannot properly convert between the IPv4 and IPv6 protocols in IPv6 networks. This is due to misunderstanding of DNS-ALG, information loss and disruption of application protocols embedded in IP addresses. One way of resolving these issues is by choosing an appropriate translation spot and framework for IPv4-to-IPv6 coexistence using a system called PET [62]. PET integrates translation and tunnelling in order to support IPv4-to-IPv6 interconnection and traversing, making it possible to have better communication models of IPv4-to-IPv6 interoperation and coexistence for different network scenarios.

Another challenge of roaming and translation is the lack of feasible support for a stateful IPv4-to-IPv6 translation mechanism. Given the current low understanding of roaming and translation, this mechanism poses many challenges, which demand a lot of new research ideas. Some of the issues that need to be resolved include application layer translation, scalability and heterogeneous addressing. When the solutions to these challenges are found, a translation mechanism can be applied in IPv4 and IPv6 networks without encountering network complications. Other issues that need research attention are performance reduction issues. These are brought about by reassembling and frequent fragmentation back-up schemes for security and redundancy of different translation techniques. The impact of this transition technique on end devices should also be investigated [63].

2.4.5 DNS64/NAT64 translation

This translation technique allows IPv6 clients to communicate with IPv4 internet sites in a transparent manner. Using the DNS64/NAT64 translation technique for IPv4 to IPv6 transition is not expensive or complicated. Internet service providers with fewer IPv4 addresses to offer their clients can still give the IPv6 addresses and be able to provide the same services. For locations that have no IPv6 addresses, DNS64 generates IPv6 addresses from IPv4 addresses and this process has no significant impact on the CPU load of the DNS server. The network address translation from IPv6 client addresses and IPv4 NAT64 outside port and address is done by NAT64. However, in comparison with direct requests to IPv6 locations, requests to IPv4 locations that pass through the DNS64/NAT64 mechanism have a negligible increase in RTT of about 2% for IPv6 clients [64]. The impact of this transition mechanism should be examined further using industrial routers and multilayer switches.

2.4.5.1 Socket identifier based on IPv4 to IPv6 translator

Another way to enable communication between IPv4 and IPv6 networks is by using a translator called a socket identifier based IPv4/IPv6 (SBIIT) translator. This translator is a modified version of NAT-PT and supports multicast translation and session-initiated protocol (SIP) based VOIP translation. With this method, translation is done in payloads and packet headers where IP addresses are embedded. The design and demonstration of this translator [65] show that the translator produces seamless interoperability between IPv4 and IPv6 hosts that operate on applications based on internet control message protocol (ICMP), SIP, TCP, multicast and UDP. One application of SBIIT is for IPv4 and IPv6 devices such as VOIP phones and videoconferencing devices, which coexist and interoperate for a long time. This translator enables smooth transition of VOIP and videoconferencing between IPv4 and IPv6 based on a modification of NAT-PT. It is also able to provide support for session announcement protocol multicast translation and SIP. Because these protocols place their IP addresses in payloads and packet headers, translation is done in both the packet headers and payloads without modifying the IPv4 and IPv6 end devices. Although the SBIIT algorithm overcomes many of the disadvantages of the traditional techniques, research on how fragmentation and file transfer protocol (FTP) can be supported by SBIIT is needed.

2.4.5.2 IPv4 to IPv6 protocol translation plan

Since the deployment of IPv6 can be done in stages, it is important to analyse how communication between IPv6-only hosts and IPv4-only hosts will happen. One possible way is to use an IPv4-to-IPv6 protocol translation plan and an application layer gateway frame. This combination results in a lightweight IPv4/IPv6 protocol translation mechanism called GATEVI. It is a viable transition technology suitable for IPv6 protocol and works well when deployed in small and medium networks. The scheme is resource-efficient, flexible and modification of client hosts is not required. It is suitable for small and medium scale deployment, because of its low requirement on resources such as IPv6 prefix length. Because the scheme is stateless, it does not need routers to maintain connection states. Some of the common applications that have been tested on this scheme are video streaming and HTTP web browsing [66]. Testing of application layer protocols such as ICMP, telnet, SSH and SNMP on this scheme is also needed, since these protocols are very useful in both enterprise and industrial network management.

2.4.6 IPv4-to-IPv6 protocol converter

One other IPv4-to-IPv6 transition mechanism is the low-cost IPv4-to-IPv6 protocol converter [67] based on static NAT technology. It uses the industry standard AT91RM9200 processor and Linux operating system. Benefits of this protocol converter include easy implementation and flexibility in the exchange of IPv6 and IPv4 information. This transition mechanism should be examined further on IPv6 networks to see how it can be used to create compatibility of fieldbus protocols in IPv6 and IPv4 networks.

2.4.7 Inter-communication and intra-communication of transition mechanisms

2.4.7.1 Elw4over6, Lw4over6, 4rd and 4over6

The performance of inter-communication and intra-communication between different transition mechanisms of elw4over6, 4rd, lw4over6 and 4over6 shows that elw4over6 performs very well in intra-communication compared to 4rd, lw4over6 and 4over6 transition mechanisms. Compared to lw4over6, the performance of elw4over6 is also better in terms of HTTP object response time, CPU utilisation and HTTP traffic loss. However, when it comes to inter-communication, lw4over6 performs better than elw4over6, because of its simple performance on the equipment of customers. In both inter-communication and intra-communication, the 4rd transition mechanism is unable to perform well because of its stateless operation, making it incapable for IP address allocation. For networks that need to focus on the quality of IPv4 connectivity and flexibility of IP address allocation, elw4over6 is the best option [68].

When it comes to mesh connectivity, it is important to know that lw4over6 does not support mesh IPv4 connectivity. Thus, an enhancement of lw4over6 that supports IPv4 mesh connectivity using DHCPv4 lease query over DHCP [69] is presented. Results show that in pure inter-communication the proposed system does not perform well when compared to 4over6 and lw4over6. However, when this system has high intra-communication, its performance is much better than that of lw4over6 and 4over6 because it communicates directly to the customer networks. Therefore, for those networks focusing on the quality of mesh IPv4 connectivity, using the system in [69] is the best transition method. The design and results of deploying the 4over6 transition system [70] show that 4over6 systems help to preserve the original investment, are easy to configure, are less costly in maintenance and have fewer modifications of the backbone network. Therefore, by opting to use the 4over6 transition mechanism, organisations can accelerate their pace of migrating from IPv4 to IPv6 in a very smooth and effective way. Smooth transition of networks is important to avoid disruption of the production of goods and services in industries [71].

2.4.7.2 Dual stack-lite, 4rd-NAT

Dual stack-lite (DS-lite), 4rd-NAT and 4over6 are among the transition techniques that are likely to be used to make IPv4 networks communicate with IPv6 networks. It is therefore important to see the performance of these transition tools in terms of reliability and delay for both intra-communication and inter-communication. The simulation results [72] show that 4rd-NAT centralisation yields high reliability and high performance and can be used for both communication types. However, flexibility of IP address allocation is lacking in this mechanism. Furthermore, if the networks are to serve many customers, using private IPv4 addresses may not work well because these addresses are not adequate. 4rd-NAT distribution also has relatively high reliability and high performance with no limit to communication types; however, just like 4rd-NAT centralisation, flexibility in IP address allocation is lacking. On the contrary, 4over6 has high flexibility in IP address allocation and relatively high reliability, with no limitations on communication types, but it has lower performance when compared to the other two transition tools. DS-lite has high flexibility in address allocation, but has high reliability and high performance for inter-communication only. It has low reliability and low performance for intra-communication because there is no direct communication to destinations in the same transition domains.

2.4.8 4over6 virtualisation

The 4over6 virtualisation architecture can also be used in IPv6 as a transition mechanism. It provides useful guidelines for DS- lite technique design, lightweight and public 4over6 protocols. The 4over6 virtualisation architecture depends on IPv6 serving as the virtual infrastructure. It helps to solve the IPv4 network connectivity problems in IPv6 and facilitates the implementation of IPv6. The overhead operational costs of deploying 4over6 virtualisation include routing, hardware and 4over6 addressing costs for tunnelling. However, these costs are better than those required for full dual stack networks, since they occur on small portions of the network nodes. Another advantage of 4over6 virtualisation is that it saves some IPv4 addresses better than DSTM [73].

2.4.9 IPv6 rapid deployment

Still on the subject of transition techniques, the IPv6 rapid deployment is considered. Though some ISPs [74] use this transition mechanism to prepare millions of their customers to be IPv6-ready, other ISPs cannot duplicate the same model successfully. Thus, a new approach that uses Openflow [74] to allow ISPs to provide connections to IPv6 customer networks rapidly is demonstrated. This approach is capable of providing management services such as quality of service and security services such as intrusion prevention systems (IPS). Using Openflow reduces the costs needed when ISPs plan to change network topologies or introduce new network services. Given the standard of programmable forwarding decision and control interface of Openflow, ISPs can dynamically manage the traffic flow of customers. Furthermore, as demonstrated in [74], ISPs can also provide security to their customers through an intrusion prevention system by allowing all traffic flow to and from customers to be re-routed through the IPS. Because of these security features in this design, customers need not worry or prepare for expensive security devices, but can rely on the security of their ISPs.

2.4.10 Tunnel brokers

When using this transition mechanism, interconnections between IPv4 and IPv6 networks are established through tunnel brokers. An IPv6 tunnel broker is one of the dynamic tunnelling mechanisms that provides encapsulated connection over IPv4 networks and can be activated by user request. It is the fastest and easiest IPv6 over IPv4 tunnel configuration. However, because of overhead in the IP header, it degrades network performance. This degradation is even more pronounced for smaller sizes of packets, such as ICMP, because of the payload being smaller than the header. As for FTP whose packets are sent based on maximum transmission unit (MTU), the degradation is based on the maximum packet size transmitted. Thus, for larger sizes of files with larger numbers of packets, the degradation of the network performance is more pronounced [75]. This transition technique may not be suitable for huge industrial communication networks because of the tunnel overhead in the IP header.

2.4.11 IPv4 to IPv6 mechanism

Since there are many critical servers in most ISP networks, the best way to transition these servers from IPv4 to IPv6 smoothly is through a transition mechanism called IPv4 to IPv6 (IVI). IVI is a stateless address and prefix-specific mapping mechanism for an IPv4 internet to an IPv6 network and from an IPv6 network to an IPv4 internet. The basic requirements and best implementation of IVI for ISP servers proves that IVI is an ideal and easy way for ISPs to transition their IPv4 networks to IPv6 networks. However, one of the shortcomings that need to be addressed in IVI is its dependence on DNS, which leads to embedded IPv6 or IPv4 addresses in URL not being translated properly. Another shortcoming of this transition technique is that certain protocol packets such as ICMP have to be rewritten each time they pass through the translator [76]. Solutions to these challenges should be investigated.

2.4.12 Roaming

Analysis of most IPv4-to-IPv6 transition mechanisms and their respective architectures reveals that none of the transition architectures considers a situation where IPv4 nodes can roam in IPv6 networks. This lack of communication among the IPv4 and IPv6 nodes, irrespective of the IP version networks, should be investigated. The IPv6 mobile users should be able to roam either into IPv6 or IPv4 based networks or vice versa in several ways, getting all the services they need and being able to connect to the internet [77]. One way of allowing an IPv6 node to roam into an IPv4 network without changing its IPv6 node address is using a process called IPv6 cryptographically generated address (CGA) [78]. This process allows an IPv6 device while roaming into an IPv4 network to configure an IPv6 address without modifying its hardware and with minimum modifications in the format of its IPv6 site local address. The advantage of this process is that it prevents the generation of duplicate addresses and protects the devices from malicious attacks. The CGA mechanism is very good; however further investigation on how an IPv4 device can roam in an IPv6 network using an IPv4 router of the IPv4 network visited is required.

2.4.13 IPv6 migration guides and knowledge builders

Although the implementation of IPv6 protocol is now a necessity, migration to this new protocol is slower than expected. Thus in order to hasten the pace of IPv6 deployment and migration, two applications that support the migration and deployment processes have been developed [79]. These applications are referred to as IPv6 knowledge builders and migration guides. The primary purpose of these two applications is to help inexperienced network engineers and administrators to coordinate the migration process well. These guides will significantly help network administrators and engineers during the initial IPv6 deployment. Given this knowledge in the migration guides and knowledge builders, IPv6 should not be seen as a topic for IT professions only. Decision and policy makers in government, who may be aware of the depletion of IPv4 addresses and the importance of migrating to IPv6, should also be involved.

Actually, IPv6 is not just a technical issue; it has far-reaching influence on the social and policy matters of any country. Lack of support for IPv6 can lead to a “digital divide problem” between IPv6 and IPv4 users, resulting in unavailability of IPv6 data content via IPv4. It is also obvious from these findings [80] that decision and policy makers must not ignore the issues of support for IPv6. They should include IPv6 policies and migration strategies in their budget and agenda. As for African countries, this is a time they need to unite under the existing national ICT strategies and help support the implementation of IPv6. However, since there are budget constraints and technical difficulties in various organisations, it is important that different organisations prioritise the upgrade or transition to IPv6 according to the degree of difficulty and necessity. As demonstrated in [81], the upgrading of external network services of government can motivate other organisations and companies to upgrade their networks to IPv6.

Most importantly, all upgrades should use suitable and cost-effective strategies to ensure seamless and smooth transition. Moreover, even if all the IPv4 addresses have been exhausted, panic should not be the strategy. Now more than ever before, the whole internet community needs to cooperate in order to upgrade smoothly to the IPv6 protocol. Although the IPv6 transition process is expected to be smooth and steady, most of the above transition techniques have not been tried and tested on real industrial and enterprise communication networks. Two other factors contributing to the slow adoption of IPv6 are NAT and classless inter-domain routing [82]. As a result, of these short-term solutions IPv4 is still being used in most communication networks, but it is unable to efficiently support and manage the rapid growth of information systems such as IP capable mobile telephony, cloud computing, mobile and IP telephones, all of which require using IPv6.

2.4.14 Best transition techniques for industrial communication networks

Though the need to use IPv6 transition tools in most communication systems is obvious, there is a need to carry out the transition in a well-guided and gradual way. Thus, transition mechanisms such as tunnelling, dual stack and translation have been suggested by the IETF as potential transition tools [83]. Because of the importance of these three transition mechanisms, a detailed examination of the possible weaknesses and strengths of these techniques is given in Table 2.1. Network engineers can use the information in Table 2.1 to design transitional networks that meet their budget and level of difficulty. Although these three techniques have been recommended by the IETF, organisations can still use the other transitional techniques discussed in this section. It is also important to know that the performance of these techniques depends on the type of network topology being used by a particular organisation. Another factor to consider when deploying these three techniques is the ability of the existing devices to support these techniques.

2.5 SOME CHALLENGING FEATURES OF IPV6 PROTOCOL

Despite the IETF recommendation to solve the IPv4 address exhaustion problem by transitioning to IPv6, the task of replacing the current protocol of the internet is not without challenges. This is because IPv6 has some challenging features that require much attention and analysis in most network configurations, network management and troubleshooting scenarios [84]. Thus, this section discusses and analyses some of the challenging features of

IPv6 that most network engineers may encounter as they work with this new protocol.

2.5.1 IPv6 command line structure

Although much research has been done on the configuration commands of IPv4, the few studies done on IPv6 configurations reveal that the configuration of IPv4 command lines is less complicated than those of IPv6 because of the complex nature of IPv6 addresses. However, IPv4 command lines are more abundant than IPv6 ones because of the small-scale deployment of IPv6 networks [85]. Given the complex nature of IPv6 addresses, further research on how these addresses affect industrial layer 3 devices and how they can be configured using decimal numbers is needed. Research in this area of IPv6 address management and configuration can lead to better ways of managing the IPv6 configuration commands.

2.5.2 Fragmentation of IPv6 packets and time to live

Among the new changes in the processing of IPv6 packets is the method of fragmenting the packets. Using this method, fragmentation of packets is no longer done by the routers on the networks; instead the sending device is responsible for fragmentation and choosing the right size of packets to transmit. Although this criterion is good, choosing the correct size of packets and time to live (TTL) is quite a challenging task. One possible way of ensuring that the sending node chooses the correct size of packets for fragmentation is demonstrated [86]. This method shows that it is possible for the sending device to determine the size of the packet to transmit correctly, but not the TTL.

Table 2.1 Best transition techniques for industrial communication networks

Transition techniques	Weaknesses	Strengths
Tunnelling	• Requires extra CPU load to do the encapsulation and decapsulation of IP packets. • The tunnel endpoint is a single point of failure. • Exhibits inactivity and delay problems • Requires to be manually configured in some circumstances	• Easy to install. • Permits IPv6 packets to be transmitted across the IPv4 networks.
Translation	• The use of NAT in this technique poses some security threats. • Most of the huge number of configurations done on this technique slow down the flow of packets. • Administration of this technique is very complex.	• Can work well with private addresses that use NAT to access public addresses. • It is easy to configure this technique only once. • Changes can be made in the existing IPv4 infrastructure or the new IPv6 infrastructure with fewer complications.
Dual stack	• Has high cost of routing processes. • Security required to make the network secure is not easy to implement. • Calls for more resources in terms of CPU and memory of routers.	• This technique is very popular and available on most network devices. • It is easy to implement and has backward compatibility for IPv4 support. • Capable of being used in cases where DNS resolution and address selection are a priority.

2.5.3 IPv6 duplicate address detection

The inter-domain handovers require IPv6 devices to acquire new IP address at their new location. After the handover procedure, the mobile nodes begin their IPv6 configurations using either the stateful (DHCPv6 communication) or stateless (router advertisements) method. As soon as the address is acquired, it is verified to see whether it is unique, using the duplicate address detection (DAD) technique. This procedure may take more than 1000 ms, depending on the type of interface being used and the acquired address is only used when the DAD procedure has been completed. Unfortunately, this procedure causes huge delays in the network, which results in unwanted and unnecessary reconfigurations in the handover process. To help solve this delay problem, a new mechanism [84] that removes the weight of verifying the uniqueness of the address from mobile IPv6 devices to static DHCPv6 servers is illustrated. The results of this experiment show how devices acquire IPv6 addresses and other configurations in advance before the actual handover is done. The most significant revelation of this server-side DAD and remote autoconfiguration design is the reduction of the delay from 1391 ms to 320 ms, which is a reduction of about 76%. This is far above the latency handover results obtained earlier from the standard handover methods [84]. The results also verify that DHCPv6 is not designed to work with the mobility concept.

2.5.4 IPv6 quality of service

2.5.4.1 Flow label field

Quality of service is an essential network parameter that has a great impact on the performance of real-time applications such as video streaming, interactive gaming and VOIP. In the IPv6 header, the flow label field supports and controls the quality of service. However, this field still has many unexplored issues, which are very challenging. One of the issues that require further examination is how it can be used to extend the quality of service to a flow basis rather than an aggregated basis level. Another challenge that needs attention is the scalability problem. Even though the flow label has been designed natively to help alleviate the quality of service problem, in the original design of this field, scalability problems develop easily. One way of solving this problem for end-to-end quality of service in heterogeneous networks is demonstrated [87]. This method removes the problem of scalability while maintaining the flow label based quality of service treatment. Thus, modification of the flow label improves the feature of quality of service management, while keeping the native simplicity of the IP. Applying an enhanced dynamic source routing protocol to the flow label also improves the quality of service for real-time applications in wireless IPv6 ad hoc networks [88]. In order to guarantee quality of service and reliable services, the challenge of how to allocate and design flow label fields in forwarding routers should be addressed as well. It is important to note that quality of service controlling techniques based on the flow label require safety, well-designed networks and an effective implementation strategy [89]. The successful implementation and refining of quality of service in IPv6 can lead to large-scale application and development of IPv6 networks and devices [90]. Moreover, since IPv6 is expected to be the mainstream of most networks in the future, it is very important to ensure that this feature works well throughout the networks.

Although the architecture and mechanism of providing quality of service in IPv4 and IPv6 networks are implemented in the same way, it is important to note the differences between the two protocols. While IPv4 uses complicated parameters such as DSCP and IP precedence values, IPv6 quality of service classification of packets is easier for identifying traffic flows. This is because the flow label field is located just before the address fields, which helps to minimise delays in the verification of the packets. However, even though it is easy to identify traffic flows using the flow label field, unfortunately it is not yet standardised and not all quality of service features have been developed. This underdevelopment of features has a negative effect on the management of quality of service in IPv6 [91]. One way of enhancing these features is evaluating the performance of different queuing mechanisms, such as priority queuing (PQ), weight fair queuing (WFQ) and first in first out. The simulation results [92] show that WFQ and PQ are the best scheduling algorithm that can provide better quality of service in IPv6 environments. Other notable findings from these results are that IPv6 has an easier method of traffic classification than IPv4 because of the flow label and traffic class fields. As for differentiated services or integrated services, the quality of service metrics in IPv6 and IPv4 has similar characteristics.

2.5.4.2 Intelligent internet protocol system

Other than using the flow label field for quality of service enhancement, another way of improving quality of service in IPv6 is using the intelligent internet protocol system. This system virtually divides the current IPv4 internet into three parallel internet architectures.

These three architectures, which co-exist on one physical topology, include data stream switching, IPv6 quality of service and content aware network. The primary purpose of the IPv6 quality of service parallel internet, which is implemented by using flow aware networks (FAN), is to ensure that all applications that need quality of service are supported and guaranteed to receive it. Whereas FAN specifically helps to meet IPv6 quality of service needs, other parallel internet structures ensure that this service is guaranteed for flows that are being transmitted. The use of multilayer FAN and intelligent routing has additional benefits of improving transmission in IPv6 parallel internet [93], [94]. Among the fields of research required in the area of quality of service are deployment, evaluation and development of management tools.

2.5.5 IPv6 temporary addresses

Network monitoring is an important function of any network management. The data collected through the monitoring of network devices shows the real picture of the network's data volume, host's frequently used applications and cause of network failures. A deeper analysis of the data collected shows misuse of network services and attacks as well. However, because of tunnelling and temporary addresses, it is difficult to monitor IPv6 devices in networks. Whereas in IPv4 networks addresses are used for host identification, IPv6 temporary addresses cannot be used to uniquely identify network devices because they are randomly generated and keep changing all the time. A solution to this challenge based on Netflow data and SNMP [95] helps to monitor IPv6 devices and to identify network users uniquely. Although the outcome of this experiment shows that this method is a viable approach for monitoring large networks, there are still many open challenges that need to be addressed in IPv6 monitoring. One of them is ensuring reliability of monitored data since SNMP and Netflow both use UDP and not the reliable TCP.

2.5.6 IEEE 802.15.4 and IPv6 domains

6LowPAN has the potential to be used in low-power operations, making it suitable to connect WSNs. The advantage of using this protocol is that it helps to meet the higher memory and bandwidth required in low-power wireless connections and microcontrollers

[96]. In addition, because 6lowPAN is suitable for IPv6 packets, it can be used for those applications that require lower data rates for transmission over IEEE 802.15.4 networks. However, when two different domains of IEEE 802.15.4 and IPv6 are involved, communication and management of addresses among the devices become complicated. Thus routing between the two domains is a big challenge. To help solve these challenges, a translation mechanism [97] that requires a device in the IEEE 802.15.4 to communicate to other devices in the IPv6 domain is presented. In this mechanism nodes obtain their destination and source ID for the destination and source IP address respectively from the IP translation gateway. The nodes then transmit the packets using the IDs from the gateway and thereafter the gateway translates them to ordinary IPv6 packets. Results show that using this mechanism improves the efficiency of the network and subsequently leads to higher packet transmission in a short period. The results in [97] are good; however, one important factor that is not considered in this experiment is delay and the effect of redundancy protocols, essential elements in both enterprise and industrial communication networks.

2.5.7 Point-to-point communication

One type of network communication on the internet is point-to-point (P2P) communication. P2P communication mechanism is used to exchange resources among peer devices on the internet. It is a very useful technology for programs such as distributed computing, file sharing and instant messaging. One major challenge with P2P is that IPv6 peers are unable to communicate with IPv4 peers and this weakens the growth and development of IPv6 user activities. Since the current peer-to-peer communication is based on the single IP of IPv4, there is no decisive method to effect communication between IPv6 peers and IPv4 peers in IPv6 and IPv4 coexistence networks. One possible way of achieving this peer-to-peer communication is to use request forwarding [98]. The results of this simulation show that the use of request forwarding keeps the whole peer-to-peer communication system stable. This stability covers various stages of the IPv6 evolution without any changes to the existing network devices. The ideas in this experiment are very good, but it is necessary to test them in real IPv6 networks. Furthermore, the concepts need to be extended to point-to-multipoint communications in multicast IPv6 networks, which is still a challenge and requires more investigation.

2.6 VULNERABILITIES AND SECURITY RISKS OF IPV6

Powerful features with new capabilities have emerged as a result of improving IPv6 in relation to IPv4 protocol. Although these improvements are beneficial to most networks, they also result in security threats and vulnerabilities. Thus, if IPv6 is to reach the current security operation level of IPv4, these threats need to be resolved [99]. This section examines some of these threats and shows how they can be mitigated.

2.6.1 IPv6 internet protocol security inadequate

Though IPv6 offers a lasting solution to the problem of IPv4 address shortage, many organisations have slowed down their migration to this new protocol because of inadequate security features. In fact, the more popular the IPv6 protocol becomes, the greater the number of security threats. A demonstration of the weakness of IPsec [99] shows that the approach of IPv6 to security threats is only slightly better than that of IPv4. Therefore, before organisations deploy IPv6, the following aspects of security for network traffic should be considered:

- All prevention systems such as proxies, firewalls and intrusion detection should be added to the networks.
- The traffic exchange between the local network and the internet should be protected and controlled.
- All hosts should be protected from external and internal attacks and scamming.
- The IPv6 packets should also be protected.
- Careful consideration should be taken when authorising automatically generated addresses and configurations.
- All rogue IPv6 routers should be prevented.

Another important thing to note is that IPsec does not secure everything automatically. The security level offered by IPsec is as good and secure as that of the computers’ operating system and the applications on which it is running or working. Other equally significant findings on the security of IPv6 [100] also argue that the use of IPsec on security threats of distributed denial of service attacks does not offer absolute security in IPv6 networks. For this reason designs for campus networks need a combination of flow detection, TTL/secure sockets layer (SSL) and other security network technologies. This combination works well to defend against threats and attacks such as application layer attacks, sniffer attacks, denial of service attacks and flood attacks. Another way of addressing threats in IPv6 involves providing network nodes with extra security devices for intrusion management and packet filtering. However, as noted in [101], packet filtering and intrusion management devices are also inadequate. Therefore, what is needed is a new security model that includes policy-based security management, host-based security management, end-to-end addressability, trust zones and perimeter based security. The good thing is that most of these security measures can be achieved using the current security technologies.

Furthermore, although IPsec is a resilient mechanism for securing communication through the internet, the bandwidth decreases when it is implemented in both IPv6 and IPv4 on wireless networks and the Fedora 15 operating system [102]. Other results for wireless networks and the Fedora 15 operating system [103] also show that 3DES-SHA encrypted systems have the lowest TCP throughput while DES-MD5 exhibits the highest TCP throughput. However, since these studies are done on the Fedora 15 operating system, it is necessary to extend this research to other operating systems, such as Windows 8, Linux and Solaris, in order to justify the findings in [102] and [103]. The performance of IPsec on virtual private network (VPN) technologies such as point-to-point tunnelling protocol, layer 2 tunnelling protocol and SSL also requires investigation.

2.6.2 IP spoofing

IP spoofing is a serious problem in the internet today and no single technique offers a solution to this problem. For IPv6 tunnels a new technique to safeguard IP spoofing problems [104], which uses the optional fields on the IPsec’s encapsulating security payload, is illustrated. In the padding area of this frame, an IPv6 source address is tagged and encapsulated into the IPv4 packet. When the receiving device gets the packet, it matches the

IPv6 source address after decapsulation and only forwards the packet to its destination when the address matches. In as much as the suggested solution works well, there is a need to test this technique in real IPv6 enterprise and industrial communication networks.

2.6.3 IPv6 application layer protocol not secure

Though IPv6 has good security architecture at the internet layer, its application layer has many loopholes and weaknesses. Because of this vulnerability to threats and attacks on the upper layers, a very good intrusion detection system model based on protocol analysis is necessary and important. Such a system should be capable of detecting threats on the upper semantic layers as well. One intrusion detection system model [105] is fast to detect attacks on the application layer and is capable of capturing IPv6 packets with a higher degree of efficiency compared to the traditional pattern-matching mode. Another design [106] also shows that it is possible to capture IPv6 packets efficiently and fulfil the intended security targets using the IPv6 intrusion detection system model based on protocol analysis. However, since most of these security mechanisms at the application layer involve IPsec, it is worth noting that at the network layer, IPsec only provides network security of the network layer and the next layer. It is unable to provide security to the application layer for applications such as FTP, HTTP and email. Hence IPv6 networks still need loophole scan, anti-virus, firewalls, IDS, VPN and other network security solutions [107]. It is, however, important to note that such security algorithms lead to slow transmission of data when using IPsec.

2.6.4 Common IPv6 local area network attacks

Because most proprietary and open-source security audit tools offer no support to IPv6, it is important to evaluate security threats in LANs. Three types of attacks are common to most IPv6 LANs; these are reconnaissance, denial of service and man in the middle attacks. Based on these attacks, solutions that help to develop integrated security audit tools [108], [109] are illustrated. Together with the encryption mechanism via key management, which is an essential security component in IPv6 multicast networks, these solutions are adequate to handle these threats. A competent and reliable scheme for key management helps to secure communications in multicast networks. What happens is that each time a network device joins or leaves the network, a new key is produced and distributed to all the devices in the multicast group. Unfortunately, this method leads to an increase in the number of keys being transmitted, which results in communication costs of key management. Although a number of algorithms have been suggested to resolve this issue, most of them do not address the communication costs. However, a lightweight key management scheme called the multicast-unicast key management method [110] is able to reduce both computation and communication costs effectively compared to other existing schemes. The use of security policies for securing IPv6 deployment and the distributed firewall technique also minimises these threats. Similarly, the application of a firewall for access control is very important for securing IPv6 LANs [111].

2.6.5 IPv4 malware threats in IPv6 networks

Most computer networks nowadays are being attacked constantly by malware threats, which results in huge financial losses. Since most network users are planning to migrate to the new environment of IPv6, malware attacks are likely to increase. To show the effects of this malware in an IPv6 network environment, a real Nimda worm [112] is injected into an IPv6-controlled network. Results show that IPv4 malware is able to infect even IPv6 networks without being modified and behave differently when injected in different operating systems. These malware products are also capable of degrading the network performance by flooding it with a lot of packets, leading to the depletion of the bandwidth. A study on how this malware behaves in transition mechanisms such as dual stack and tunnelling techniques needs to be undertaken and new detection mechanisms that prevent and fight these threats should be found.

2.6.6 Neighbour and router discovery protocols

2.6.6.1 Neighbour discovery protocol security threats

Neighbour discovery protocol (NDP) is an essential feature in IPv6. It helps to discover link layer addresses of neighbours on the same networks and is also useful for verifying the reachability of neighbouring devices. Though this protocol is necessary in IPv6, there are some security threats associated with it. Some of these threats include denial of service attacks, redirection attacks, fake prefix address attacks, address resolution protocol (ARP) cheating and synchronised flood attacks. Given the vicious nature of these threats, an effective NDP security strategy [113] that uses IPsec authentication techniques is demonstrated. This strategy combines IPsec AH validation and the mac-address and requires security certification for both the mac-address and IP address, making it an effective and strong defence on NDP security attacks. The only concern about this defence mechanism is that it may not overcome all the weaknesses of IPsec mentioned in [99] and [100].

2.6.6.2 Router discovery security threats

Router discovery and redirect are two important components of neighbour discovery protocol. IPv6 hosts use router discovery to detect the presence of routers and to configure network parameters such as hop limit, address prefixes, MTU and default gateway. Though router discovery is such a useful IPv6 feature, the original standard for router discovery does not state security mechanisms for it, thus it is unprotected against many exploitations. However, one way of improving security in router discovery is employing decentralised trust management that uses trust solicitation options for advertisement messages [114]. This new security mechanism prevents many attacks on neighbour discovery protocol and its traffic overhead is very low compared to secure neighbour discovery protocol.

2.6.7 Privacy extension and cryptographically generated addresses

Extension and organisationally unique identifiers are default methods for generating IPv6 addresses and the hardware manufacturer and IEEE standards association respectively assign these methods. In order to prevent nodes from having the same interface identifier (IID) each time they connect to the network, the node’s IP address should change frequently by generating a random IID each time it generates a new IP address. Two available methods for randomising the IID are privacy extension (PE) and CGA. These two mechanisms do not use unique values or mac-addresses for randomising the IID; therefore, they are prone to many address attacks. The problem with CGA is the computational costs needed to generate the IID, while PE lacks the essential security mechanisms. Actually, PE only provides limited protection against privacy attacks. One approach that helps solve this security problem involves the use of a method called simple secure addressing scheme for IPv6 autoconfiguration [115]. This approach is very secure for a wide range of applications. It uses the dynamic host configuration protocol for an IPv6 (DCHPv6) server to provide network configuration parameters dynamically to IPv6 client hosts. However, this method presents address security issues to the network. To help solve these threats, a security solution that uses CGA with the help of DCHCPv6 is presented [116]. In this design the use of a public key in CGA results in better, enhanced security features for IP address validation, while ensuring that all the necessary functions of DHCPv6 authentication are maintained. It can be seen from this solution that further research on how to enhance DHCPv6 security is needed, especially for IPv6 devices that cannot deploy the CGA method. Furthermore, since dynamic host configuration protocol (DHCP) servers are a source of network failure in most enterprise and industrial communication networks, this method may not work very well.

2.6.8 Domain name system

One of the primary elements of the internet that helps hosts to change their domain names dynamically is the DNS. Though this dynamic feature is important, it exposes the IPv6 domain name servers to security threats. With IPv4, these security vulnerabilities are resolved by using authentication between the DNS server and the network devices. However, the DNS security protocols used in IPv4 are difficult to implement in IPv6, because they do not support DNS authentication and secure DNS updating options are missing. Thus, security is still an issue for DNS update in DHCPv6 servers. To help improve this security, an extension to secure neighbour discovery is suggested [117]. This feature permits the update of the DNS resource records as the devices configure their IP addresses.

2.6.9 Anycast communications attacks

Although anycast communications are vulnerable to many security threats, providing security solutions to anycast communications with IPsec is difficult to accomplish. Nevertheless, one possible solution to provide secure communication over IPsec between servers and a client using the same anycast address [118] is demonstrated. This method helps overcome the security problem that makes it impossible to establish and exchange the needed secret keys securely between two ends of the connections. Though this solution works well in inter and intra-autonomous systems, it is still necessary to test the solution in real and complex IPv6 network scenarios. Further research is also needed on anycast type of routing, since at the moment there are no standard protocols that address this routing.

2.6.10 IPv6 extension headers

One of the good features of IPv6 is the simplified header and its ability to add additional functionality in the form of extension headers. Unfortunately, extension headers carry some threats, which destroy networks. Possible threats that result from misusing and manipulating fields of the extension headers are tiny fragmentation attacks, overlapping fragmentation attacks and flooding attacks due to unknown destination options. Because of the vicious nature of these threats, most operating systems and network devices are not mature enough to handle them. This is because most of the operating systems and network devices are not yet fully RFC complaint. Because most network administrators and engineers have less experience with the IPv6 protocol, the possibility of them preventing and fighting these threats is very low [119]. Thus, extension headers are a danger to the smooth operation of IPv6 networks. To help minimise some of these threats, strict adherence to security polices and using fully RFC compliant devices is recommended [120]. However, although these polices may help to fight these threats, further investigations into the exact security measures are needed to fight and prevent network attacks adequately, before IPv6 is deployed globally.

2.6.11 IPv6 autoconfiguration

2.6.11.1 Stateless address autoconfiguration

Stateless address autoconfiguration is a powerful and good application feature of IPv6. It enables network-capable devices to connect automatically and constantly to other devices of office networks, colleagues, family members and homes in an easy way. Though this increase in communication has many advantages, unfortunately it makes it easy for uninvited people to connect to LANs as well. This is because in its current state, stateless address autoconfiguration allows third party devices to monitor other networks easily. Apart from illegal monitoring of networks, this feature has devastating effects on other IPv6 applications. An illustration of how auto-configured addresses are used for good and bad purposes [121] reveals that the benefits of employing auto-configured addresses are far less when security implications are considered. In as much as this feature helps network devices to generate and configure their own addresses, it weakens the security of IPv6 devices and is an obstacle to the smooth management of IPv6 networks.

At the moment a tentative way of blocking external communication from malicious devices through autoconfiguration uses the feature of RA messages in ICMPv6 [122]. Although this experiment demonstrates a successful way of blocking external communication from the malicious devices by modifying the RA messages, more research is required. Thus, before IPv6 can be deployed globally, a solution that stops individual tracking and monitoring of IPv6-enabled devices should be found.

2.6.11.2 Node autoconfiguration attacks

Another possible attack against an IPv6 protocol is node autoconfiguration attack. In this attack, a malicious node transmits an incorrect response to the request of the address of a new node wanting to connect to the network. The solution [123] to this attack requires the new device that joins the network to confirm whether the network advertisement response messages that it receives when it sends the network solicitation requests are genuine. Although this method may work to secure industrial communication networks against node autoconfiguration attacks, the best security measure is using static IPv6 addresses on all the nodes.

2.6.12 Bad ack-reset and packet fragmentation attacks

Bad ack-reset and packet fragmentation attacks are also among the IPv6 security threats. Attackers use packet fragmentation attacks to control the packet fragmentation process and services, while bad ack-reset attacks are used to reset a newly established connection through network exploitation. A test of these attacks using scapy 2.0.1 and GNS3 [124-126] shows that there is a need to manage the host firewall properly as a security measure against these attacks. Although this solution of using the firewall works well, this security mechanism is not adequate; hence, it is necessary to examine further how IPsec can prevent such attacks.

2.6.13 Spam challenges

Since the beginning of internet, spam attacks have been a serious problem to SMTP and IP networks. Spammers misuse huge amounts of internet resources to meet their criminal objectives and to promote their products. To help mitigate this problem, different approaches such as DNS-based, signature-based and Bayesian-based methods have been tried and tested in IPv4 networks. Although these techniques may work well in IPv4 networks, the possibility of them being used in IPv6 is highly questionable, especially the DNS-based technique. This is because the use of temporary addresses and the large address space in IPv6 networks makes the problem of spam more complicated and difficult to solve. For this reason, IPv6 poses unique and serious security threats to ISPs. As a result, it is not easy for them to differentiate between IP addresses that originate spam messages and good IP addresses. Although a combination of gray listing, whitelisting and blacklisting algorithms may work to solve the problem of spam in IPv6 networks, it is still necessaary to explore and find better solutions to the spam challenge in IPv6 protocol [127-134].

2.6.14 Routing header attacks

One other vulnerability of the IPv6 protocol is found in the routing header. Attackers can use this header to bypass the router and firewall of a network without having the packet filtering rules broken. However, by using the prevention mechanism shown in [135-138] together with the packet filtering system, this threat can be avoided. One reason why this method works well is that it is able to check the destination address of the next hop or intermediate nodes. Moreover, the algorithm is easy to configure and requires fewer modifications to the existing packet filtering system. This is a very difficult attack to handle if enterprise or industrial communication networks are not well designed. Therefore, if the solution in [139] is to work effectively in industrial communication networks, network engineers must design their networks properly.

2.6.15 IPv6 security risk prototype system

The coexistence of IPv6 and IPv4 protocol subjects many enterprise and industrial communication networks to IPv6 and IPv4 threats. To help identify most of these threats, a threat model [140] that identifies possible security risks is illustrated. The model measures the potential security risks of a network in an enterprise by making use of an IPv6 security risk prototype (I-SERP) system. With the I-SERP system, network administrators can easily identify security risks and know which security approach is appropriate for the threats. This model also uses an equation suitable for calculating the risk value. This value can be used to identify the most at risk network devices that need to be protected and the appropriate security mechanism.

When these threats are identified, they are examined and mitigated using an integrated security system. Such a system allows vendors to use security devices that have additional capabilities for intrusion management and packet filtering. In addition, proper and well-designed networks capable of supporting IPv6 security systems are implemented. Furthermore, as illustrated in the security model shown in [141], such a system has five main components, namely policy based management, end-to-end addressability, perimeter based security, trust zones and host based security. Without these five components, attackers can evade network intrusion detection (NID) systems by exploiting transparent node mobility. A description of strategies that attackers can use to evade network intrusion systems in networks that support mobile IPv6 protocol is given in [142]. These evasion techniques are not a result of NIDs’ flaw implementation. They are a direct result of transparent node mobility and certain characteristics of mobile IPv6, such as route optimisation. In order to overcome these evasion techniques, a new defense mechanism based on the exchange of state information [142] among network intrusion detection systems can be used. However, this system is more complex than the traditional ones.

2.7 NETWORK SIMULATORS

2.7.1 Graphical network simulator 3

The Graphical Network Simulator 3 (GNS3) is a free open-source network simulator that operates by making use of real Cisco IOS images. The program that makes it possible to emulate switches and routers using these images is called Dynamips. The following are the advantages and disadvantages of using this simulator [143].

2.7.1.1 Advantages

- Users are able to design complex and high-quality network topologies.
- Users can analyse and capture packets using wireshark.
- Users are able to emulate many and different types of systems such as Linux virtual machines, Juniper routers, windows virtual machines, Cisco routers and switches.
- Users can connect the simulated networks to real world networks.
- It is easy to simulate simple ATM, frame relay and ethernet switches.
- Users are able to experiment with IPv6 configurations on the real IOS images for routers and switches.

2.7.1.2 Disadvantages

- It does not support all Cisco IOS images.
- It cannot emulate all layer 2 functions for switches.

2.7.2 Cisco packet tracer

The Cisco packet tracer [144] is another well-built network simulator program developed by Cisco Networking Academy that enables users to experiment with the behaviour of routers and switches. It has the following advantages and disadvantages:

2.7.2.1 Advantages

- It supports many networking technologies and protocols.
- It allows animation, exploration, virtualisation and experimentation with networks.
- It gives a good visual demonstration of configurations and complex technologies.

2.7.2.2 Disadvantages

- It does not use real IOS images.

- Simulated networks cannot be connected to real-world networks.
- It does not emulate other systems such as Linux virtual machines and Juniper switches and routers.

2.8 NEXT GENERATION INTERNET PROTOCOL TECHNOLOGY

Given the many shortcomings exhibited by the current IPv4 protocol, the time has come for its replacement. Thus, the next generation internet protocol for enterprise and industrial communication networks is IPv6. Most of today's industrial and enterprise networks have requirements that calls for the implementation of this new protocol especially at the network layer (layer 3). The primary function of layer 3 is addressing and routing of packets from one network to another using routers and multilayer switches. But in order to support this routing function, routers and multilayer switches must be used together with different IPv6 addresses and routing protocols. Thus, the migration to IPv6 involves and impacts more protocols than just the IP. Even though this impact affects both layer 2 and layer 3 network protocols, this study only focuses on layer 3 protocols. Although most of these network protocols are the same as IPv4, the major difference lies in their implementation. This section briefly explains some of the IPv6 addresses and protocols required in the operation of layer 3 functions [145].

2.8.1 Types of IP addresses

Three different types of addresses are needed for layer 3 applications and functions in IPv6. These are: unicast, anycast and multicast addresses.

2.8.1.1 Unicast addresses

Unicast addresses are used to send packets to only one interface of particular devices. There are many types of unicast addresses, however, the most important one for this study are global addresses, unique local and link local addresses. Unicast global addresses are public routable addresses and they start with a prefix of 2000:: /3. Link-local addresses start with the prefix of FE80:: /10 and are used as private and temporary LAN addresses, thus, they cannot be routed globally. Unique local addresses are just like link-local, however the former can be routed within a company or organisation networks while the latter cannot [145].

2.8.1.2 Multicast addresses

These addresses route packets to a subset of selected devices or multiple interfaces that are registered under a specific multicast address. They always start with FF00:: /8. Multicast addresses have replaced all broadcast addresses in IPv6. Their main function is to distribute identical services or information to some defined multicast groups (group of interfaces). Some of the link-local multicast addresses include: FF02::1 for all node communication on a link, FF02::2 for all router communication, FF02::5 and FF02::6 for OSPFv3 communication, FF02::9 for RIPng and FF02::A for EIGRPv6 communication [145].

2.8.1.3 Anycast addresses

Routers use anycast addresses to delivers packets to the nearest device it finds in terms of its routing distance. These addresses are also referred to as one-to-the nearest addresses and are only configured on routers and not hosts. In addition, they are never used as the source address of IPv6 packets. Configuring a unicast address on more than one interfaces of routers creates an anycast address for that particular unicast address [145].

2.8.2 Routers and routing

Routers are devices that connects networks together and forwards IP packets (traffic) between different interconnected networks. This process of forwarding packets from one interconnected network to another is called routing and occurs at layer 3 or network layer of the OSI model. The primary function of IPv6 is to route (forward) packets between interconnected network segments. For this process to happen, end user nodes should have IPv6 addresses on their interfaces to enable them create and send packets out to other devices. Additionally, the end user devices should also be configured with addresses of their respective default routers. This enables routers to forward packets to other networks or subnetworks. To avoid the loss or looping of packets, each header in the IPv6 packet has the destination address of the receiving device and the source address of the sending device. When an IPv6 packet arrives at the router, the router checks in its local routing table and determines whether it should reject the packet or forward it within the same network or to another network. This process of discarding or forwarding packets requires some analysis by the router. For this reason, upon receiving the frame, the router examines the frame check sequence to see whether some errors occurred. If there are any errors that happened during transmission, the router discards the frame and makes no effort of recovering the lost packet. However, if there are no errors that took place, the router inspects the Ethernet type field and extracts the type of packet contained there. After extracting the packet, the data link trailer and header are discarded [145].

If an IP packet is contained in the Ethernet type field, the router inspects its IP routing table to check for the most specific prefix that matches the destination address of the packet. A routing table is a data table in routers and multilayer switches that is used to store route information for particular networks and their respective metrics (distances). The IPv6 routing table has four different types of entries that are used to forward packets: directly attached networks routes, remote network routes, host routes and default routes. Each prefix (network) in the routing table has an outgoing interface and the next-hop router. If the packet is destined for the local interface (local link) on the router, the destination address in the packet header is used. However, if the destination address is on another network (remote link), the next-hop address is used. Before forwarding the packet to the next-hop address, the router builds a new frame for encapsulating the packet, decrements the time-to-live field by 1, and calculates a new checksum value. Soon after this process, the router encapsulates the packet in this new frame, adds a new destination address and checksum value; and sends the frame to the next-hop router [145].

2.8.3 Multilayer switches

Routers work at layer 3 of the OSI model while traditional network switches work at layer 2. A multilayer switch (also called layer 3 switch) is a specialized hardware switch that works at layer 2 and layer 3. Since packets do not have to pass through the router when routing, multilayer switches experience less network latency. However, because they are designed to operate within intranets, they do not possess features for wide area networks and WAN ports.

Multilayer switching (MLS) is a process that requires multilayer switches operating at layer 2 to use protocols and logic from the upper layers to forward packets. Although the routing process works just like in a router, the interfaces of multilayer switches slightly differ from those of routers. Multilayer switches uses VLAN interfaces, port channel interfaces and routed interfaces for routing. However, for routing to take place between VLANs, a multilayer switch also requires a virtual interface and an IP address to be configured for each VLAN. Furthermore, similar to routers, the routes in the routing table of multilayer switches also have outgoing interfaces and routing metrics [145].

2.8.4 Routing protocols

IPv6 uses interior routing protocols and exterior routing protocols for selecting the best paths (routes) among the different routes available to a particular destination. Exterior routing protocols discover and share routing information between two different organisations or autonomous systems. An example of exterior routing protocol is the border gateway protocol. Interior routing protocols are used within an organisation or autonomous system to distribute routes (paths) among the routers inside the organization boundary. Examples of interior routing protocols include: RIPng, OSPFv3 and EIGRPv6. This study only considers interior routing protocols since they relate more to the study than exterior routing protocols [145].

2.8.4.1 RIPng

This interior routing protocol is a distance vector protocol with a maximum hop count of 15. A hop count of 16 is taken as an infinite distance and regarded as unreachable. Distance vector protocols use hop count as the routing metric for determining the best routes. For preventing multicast addresses and loops on the network, poison reverse, split horizon, route poisoning, and hold-down techniques are used by this protocol. For keeping track of the next-hop addresses, RIPng use link-local addresses and not global addresses [145].

2.8.4.2 OSPFv3

OSPFv3 uses areas to separate networks into autonomous systems. It is a link state routing protocol which uses Dijkstra’s shortest path first algorithm for calculating the best route to the required destination based on cost as its metric factor [145].

2.8.4.3 EIGRPv6

Though it has some link state features, EIGRPv6 is mostly an advanced vector routing protocol. It uses diffused update algorithm for determining the shortest route to the intended destination on a network. In terms of routing metrics EIGRPv6 uses delay, bandwidth and reliability when determining the best path [145].

2.8.5 Supportive protocols

Other than the routing protocols, IPv6 also has protocols that perform different functions on the network. These are: ICMPv6, DHCPv6 and DNS protocols. ICMPv6 is used for information messaging, statistical purposes and diagnostics functions. The ICMPv6 neighbour discovery protocol is useful for discovering routes and neighbour devices on a network, and also performs ARP functions. DHCPv6 may be used to acquire IPv6 addresses and to locate the DNS servers. However, even without it, IPv6 addresses can still be acquired through auto-configuration, whereas ICMPv6 neighbour discovery protocol can be used to find the DNS server. The DNS server is responsible for domain name to IPv6 address resolutions [145].

2.8.6 Tools for testing network connectivity

2.8.6.1 Traceroute

This is a network diagnostic tool that shows the routes that packets take across an IPv6 network. For each network total hops are shown in a sequence, and each hop displays addresses, time-to-live, round trip time and best times in milliseconds. Traceroute information is useful for identifying network problems and also for verifying how routers are connected on a network [145].

2.8.6.2 Ping

A ping is also a diagnostic networking tool for testing connectivity and reachability among devices (routers and hosts) on network. Information from ping commands shows the round trip time that packets take across networks. Other than checking for network connectivity, pings also show the speed and reliability of networks [145].

CHAPTER 3 CONFIGURATION METHODS FOR LAYER 3 IPV6 COMMANDS

3.1 INTRODUCTION

This third chapter presents the methods for configuring IPv6 addresses, IPv4-to-IPv6 transition techniques, routing and redundancy protocols in a ring and hierarchical network topology. These two network topologies consist of end devices (hosts), layer 2 switches (SW), multilayer switches (M) and routers (R). In terms of addresses, both the ring and hierarchical network designs use a global routing prefix of 2002:ACE7:2222::/48 as the source of IPv6 addresses. Although end devices and layer 2 switches are included in these network designs, they only serve the purpose of completing the LANs and have no IPv6 configurations implemented on them. The multilayer switches and routers are selected randomly from the families of c3600, c3725, c3745 and c7200 Cisco platforms. The configurations are done on these selected routers and multilayer switches using real Cisco IOS software version 12.4(24)T, in a GNS3 simulator. The main focus of these configurations is to discover the challenges and benefits of using IPv6 at layer 3 (network layer) of the TCP/IP model, in industrial communication networks.

3.2 RING NETWORK TOPOLOGY FOR INDUSTRIAL COMMUNICATION

Figure 3.1 shows one possible design of an IPv6 industrial communication network using a ring topology. The topology comprises one router (RA) and eight multilayer switches, namely MB, MC, MD, ME, MF, MG, MH and MI. The router and multilayer switches are connected using single-mode (SM) fibre cables, whereas the layer 2 switches (SW) connect to multilayer switches and end devices (hosts) using unshielded twisted pair cables.

3.2.1 Subdivided networks for the ring topology

Since the ring network topology of Figure 3.1 has 20 subdivided networks (subnets), when the global routing prefix of 2002:ACE7:2222::/48 is subnetted (subdivided into 20 smaller networks), it yields the IPv6 addresses shown in Table 3.1. Note that although the 2002:ACE7:2222:000::/64 subnet identity has been included in Table 3.1, it is not assigned to any network because it is among the reserved IPv6 addresses.

Table 3.1 First twenty subnetworks for the ring network topology

2002:ACE7:2222:0000::/64	2002:ACE7:2222:000A::/64
2002:ACE7:2222:0001::/64	2002:ACE7:2222:000B::/64
2002:ACE7:2222:0002::/64	2002:ACE7:2222:000C::/64
2002:ACE7:2222:0003::/64	2002:ACE7:2222:000D::/64
2002:ACE7:2222:0004::/64	2002:ACE7:2222:000E::/64
2002:ACE7:2222:0005::/64	2002:ACE7:2222:000F::/64
2002:ACE7:2222:0006::/64	2002:ACE7:2222:0010::/64
2002:ACE7:2222:0007::/64	2002:ACE7:2222:0011::/64
2002:ACE7:2222:0008::/64	2002:ACE7:2222:0012::/64
2002:ACE7:2222:0009::/64	2002:ACE7:2222:0013::/64

3.2.2 Results of assigning nineteen subnets to the ring network topology

The results of assigning 19 of the 20 subnets in Table 3.1 to all the networks in the ring topology of Figure 3.1 are shown in Figure 3.2. In this network topology, the interface ID of the address of each interface corresponds to the name of the router or multilayer switch. For instance, router RA fastethernet 0/0 has the address of 2002:ACE7:2222:0002::A/64 and multilayer switch MB fastethernet 0/0 has the address of 2002:ACE7:2222:0001::B/64. However, because the last letter in hexadecimal notation is F, the naming of the interface ID on multilayer switches MG, MH and MI is different. MG is taken to be 10, MH is taken to be 11 and MI is represented by 12. Therefore, the following are some of the interface addresses of these switches: MG (fastethernet 1/0) is 2002:ACE7:2222:0012::0010/64, MH (fastethernet 2/0) is 2002:ACE7:2222:0010::00011/64 and MI (fastethernet 1/0) is 2002:ACE7:2222:000E::12/64.

3.3 STATIC AND DYNAMIC ADDRESS CONFIGURATIONS

3.3.1 Static unicast addresses

Configuring of static unicast addresses on multilayer switches and router interfaces is done using the “ipv6 address address/prefix length” and the “ipv6 unicast-routing” commands. Whereas the first command configures IPv6 addresses on multilayer switches and router interfaces, the second command enables IPv6 globally on the devices. The whole process of configuring these two commands on the router and multilayers switches in the ring topology of Figure 3.2 is illustrated in appendix E.

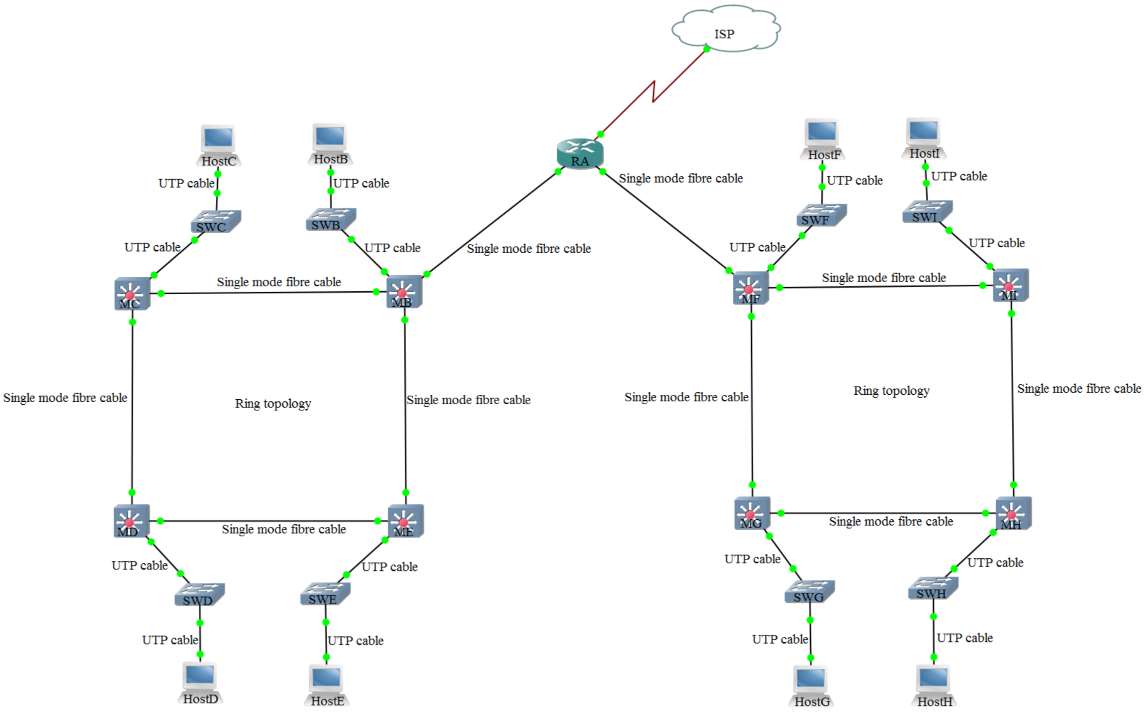

Figure 3.1. Cable connections for the ring network topology

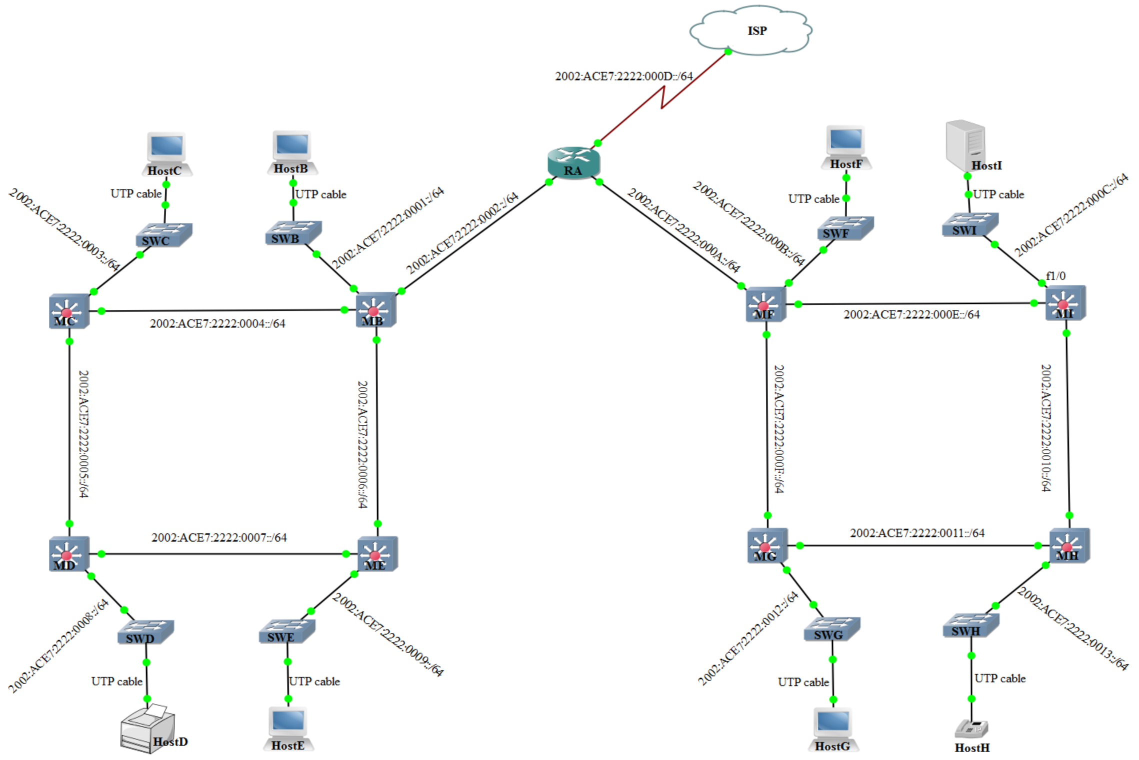

Figure 3.2. Nineteen subnetworks for the ring network topology

3.3.2 Dynamic SLAAC unicast addresses

In most industrial communication networks, network engineers configure routers and multilayers switch interfaces with static unicast addresses, as shown in Section 3.3.1. This creates network stability because addresses do not change randomly, but only when the network engineer decides to change them. Although the static way of configuring IPv6 addresses is the preferred and most stable method, multilayer switches and router interfaces can also be configured with dynamic addresses using two methods. The first method uses DHCP, while the second uses stateless address autoconfiguration (SLAAC). These two methods are suitable when connecting industrial routers to the internet through cable modems or digital subscriber line technologies. This section shows the SLAAC dynamic configuration of IPv6 addresses on the router and multilayer switches of Figure 3.2. Just like the static unicast method, the SLAAC method also uses the ipv6 address command. However, instead of assigning the actual IPv6 address to the command, a keyword of autoconfig is configured. A commandline explaination of how to configure SLAAC addresses is given in appendix F.

3.4 STATIC AND DYNAMIC ROUTING PROTOCOL CONFIGURATIONS

3.4.1 Static IPv6 routing

The "Ipv6 route prefix/length next hop address" command is used to configure static IPv6 routing on all the layer 3 devices in the ring topology of Figure 3.2. The next hop address used is the local outgoing interface or the unicast global address of the neighbour router or multilayer switch. All the static addresses used for this routing protocol are those configured in Section 3.3.1. Appendix G shows how the configuration process is done on all multilayers switches and the router.

3.4.2 Dynamic IPv6 routing protocols

This section shows how to configure RIPng, EIGRPv6 and OSPFv3 dynamic routing protocols. These protocols are configured using the static and dynamic SLAAC IPv6 addresses of sections 3.3.1 and 3.3.2 respectively.

3.4.2.1 Configuring of routing information protocol next generation

Three commands are used to configure the routing information protocol next generation (RIPng) on all the layer 3 devices. These commands are, "ipv6 rip name enable" interface subcommand, "ipv6 unicast-routing" and "ipv6 router rip name" global commands. The first command only enables RIPng on the interfaces, while the second and third commands globally enable IPv6 routing and RIPng respectively on each layer 3 devices. One significant requirement of the first and third commands is that they need to use the same arbitrary RIPng name on each device. Although this name does not need to match on all the devices, in the ring topology of Figure 3.2, the same name of benji is used on all the multilayer switches and router. Note that this name is chosen arbitrarily and is not case-sensitive. See appendix H for the whole commandline configuration process of RIPng.

3.4.2.2 Enhanced interior gateway routing protocol for IPv6

The enhanced interior gateway routing protocol version 6 (EIGRPv6) configuration process requires the following commands: “ipv6 unicast-routing” for enabling IPv6 routing globally on the multilayer switches or routers, “ipv6 router eigrp asn” command for enabling EIGRPv6 globally on the router or multilayer switches and the “ipv6 eigrp asn” subinterface command useful for enabling EIGRPv6 on the multilayer switches or router interfaces. The asn in the second and third commands stands for autonomous system number. This number ranges from 1 to 65535 and must be the same on all neighbour routers or multilayer switches. In all the EIGRPv6 configurations of Figure 3.2, an autonomous system number of 20 is used. Furthermore, unlike RIPng, EIGRPv6 also requires “no shutdown” and “shutdown” commands to enable and disable EIGRPv6 on the interfaces. Another important parameter required for EIGRPv6 configuration is the “router-id id” command where id is a 32 bit identity of the router. An example of how the EIGRPv6 configuration process is done on all layer 3 devices is shown in appendic H.

3.4.2.3 Open shortest path first version 3 configurations for a single area

The open shortest path first version 3 (OSPFv3) configurations involve three steps. The first step is the global enabling of the ospf process and number on the router or multilayer switches using the “ipv6 router ospf process-id” command, while the second step requires configuration of the router identity (id) using the “router-id id-value” command. The third step enables the ospf process and assigns the area number to an interface, using the command of “ipv6 ospf process-id area number.” In the ring topology of Figure 3.2, all the interfaces are assigned to area 0. However, since the ospf process id does not need to match on all the devices, different process identities (id) have been configured on the multilayer switches and router. Note also that even on OSPFv3 configurations, global IPv6 routing must be enabled on the router and multilayer switches using the command “ipv6 unicast-routing.” It is important that this command be configured first before the OSPFv3 commands are configured. The whole process of configuring these commands is illustrated in appendix H using router RA and multilayer switch MB.

3.5 PROCESS OF CONFIGURING RIPNG, EIGRPV6 AND OSPFV3 ON DYNAMIC SLAAC IPV6 ADDRESSES

Configuration of RIPng, EIGRPv6 and OSPFv3 on SLAAC addresses of router RA and multilayer switches MB, MC, MD, ME, MF, MG, MH is done using the commands in sections 3.3.2, 3.4.2.1, 3.4.2.2 and 3.4.2.3 respectively.

3.6 IPV4 TO IPV6 TRANSITION TECHNIQUE CONFIGURATIONS

Table 3.1 and 3.2 shows the IPv6 and IPv4 addresses used to configure IPv6 transition techniques. Using these addresses, this section explains how to configure dual stack, manual IPv6 tunnelling, ISATAP, GRE and NAT-PT transition mechanisms in a ring topology network.

3.6.1 Dual stack technique

Dual stack configurations for the 172.16.0.0 and 2002:ACE7:2222:0000 networks are configured on the router and the multilayer switches shown in Figure 3.3. All the IPv4 addresses used for this configuration are shown in Table 3.2. Although any routing protocol could have been used in this design, the IPv4 networks use OSPF, while IPv6 networks are configured with OSPFv3. Note that the process for configuring OSPF on IPv4 networks uses the “router ospf 21” global command and the “network 172.16.0.0 0.0.255.255 area 0” sub command. The commands used to configure OSPFv3 on IPv6 networks are the same as those under Section 3.4.2.3. The whole configuration process for the dual stack is shown in appendix I.

Table 3.2 IPv4 addresses used to configure IPv6 transition techniques

Layer 3 device	Multilayer switch or router interfaces	IPv4 address
RA	Fastethernet 0/0 Fastethernet 1/0 Serial 4/1	172.16.1.2/24 172.16.10.2/24 172.16.19.2/24
MB	Fastethernet 0/0 Fastethernet 1/0 Fastethernet 2/0 Fastethernet 1/1	172.16.2.1/24 172.16.3.1/24 172.16.1.1/24 172.16.6.1/24
MC	Fastethernet 0/0 Fastethernet 1/0 Fastethernet 2/0	172.16.5.2/24 172.16.4.2/24 172.16.3.2/24
MD	Fastethernet 0/0 Fastethernet 1/0 Fastethernet 3/0	172.16.8.3/24 172.16.5.3/24 172.16.7.3/24
ME	Fastethernet 0/0 Fastethernet 0/1 Fastethernet 1/0	172.16.9.4/24 172.16.6.4/24 172.16.7.4/24
MF	Fastethernet 0/0 Fastethernet 0/1 Fastethernet 1/0 Fastethernet 2/0	172.16.14.1/24 172.16.12.1/24 172.16.10.1/24 172.16.11.1/24
MG	Fastethernet 0/0 Fastethernet 0/1 Fastethernet 1/0	172.16.16.2/24 172.16.17.2/24 172.16.14.2/24
MH	Fastethernet 0/0 Fastethernet 0/1 Fastethernet 1/0	172.16.18.3/24 172.16.16.3/24 172.16.15.3/24
MI	Fastethernet 0/0 Fastethernet 0/1 Fastethernet 1/0	172.16.12.4/24 172.16.15.4/24 172.16.13.4/24

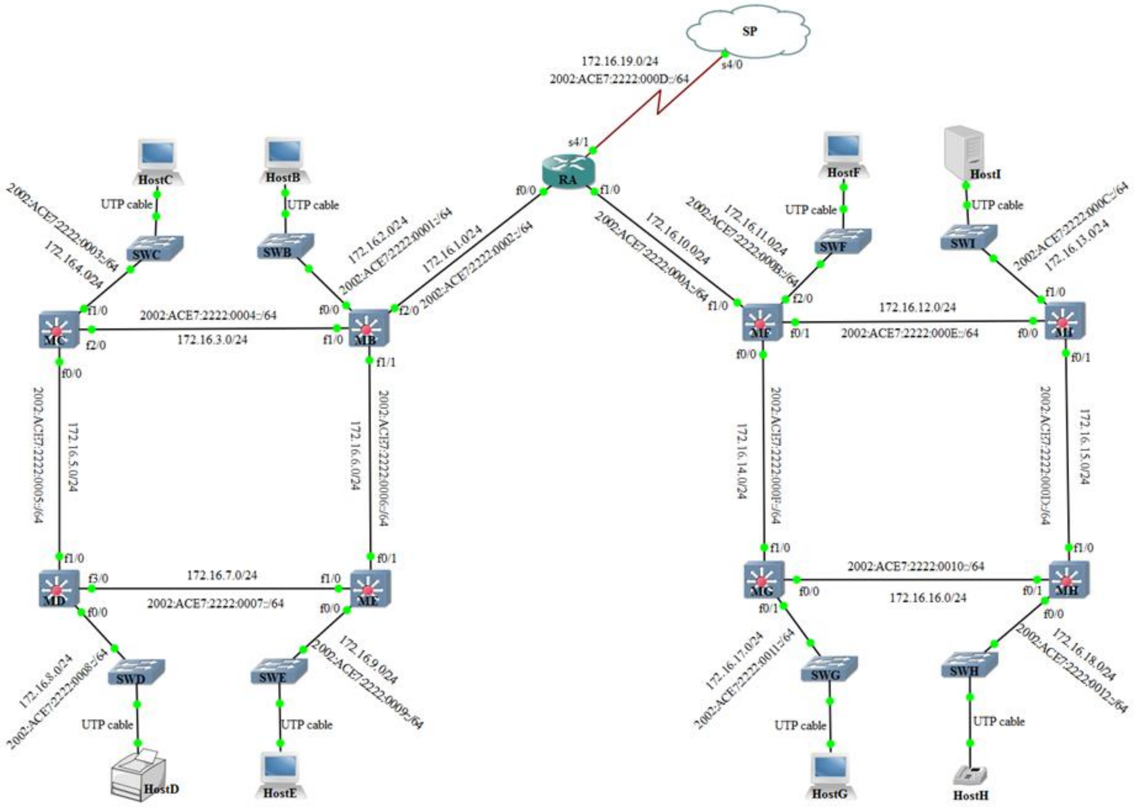

Figure 3.3. Ring network topology for dual stack configurations

3.6.2 Manual IPv6 tunnelling technique

Configurations for this transition technique are done using Figure 3.4. In this design all the multilayer switches are running on 2002:ACE7:2222::/64 networks, while routers RA and RB are on 172.16.0.0 networks. The routing protocols configured for IPv4 and IPv6 networks are RIP and RIPng respectively. The primary purpose of this technique is to demonstrate how two industrial communication IPv6 domains (MB, MC, MD, ME and MF, MG, MH, MH) can be linked through an IPv4 network (RA and RB). In other words, this technique demonstrates how an IPv4 network can serve as the transport protocol for IPv6 packets.

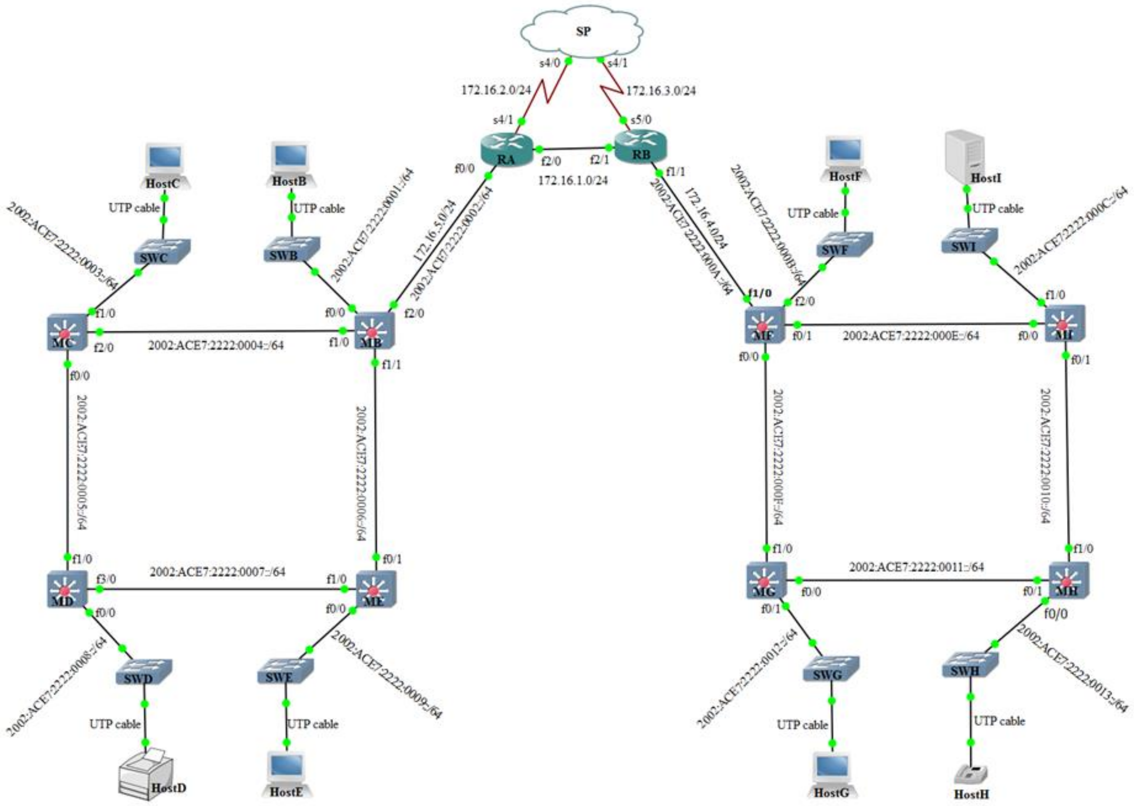

Figure 3.4. Ring network topology for manual IPv6, GRE and ISATAP configurations

One important concept introduced in this configuration is the loopback address of 172.16.6.1 and 172.16.7.1. The first address is configured on router RA and the second on RB. Unlike physical interfaces, loopback interfaces have the advantage of always being up and running, unless they are administratively shut down by the network engineer. Configuration of the manual IPv6 tunnelling technique is done on routers RA and RB as shown in appendix I. Note that the configuration process for RIP on routers RA and RB used the "router rip" global command and the "network 172.16.0.0" subcommand. The commands for RIPng configurations are the same as those used in Section 3.4.2.1.

3.6.3 Generic routing encapsulation IPv6 tunnelling technique

Using Figure 3.4, the following steps describe how GRE is configured on routers RA and RB. GRE is the default tunnelling protocol for Cisco layer 3 devices and its configuration is very similar to the manual IPv6 technique. The only difference is that under the manual IPv6 tunnel configuration, the command “tunnel mode ipv6” is used, whereas on the GRE IPv6 tunnel it is not used. One advantage of GRE is that the transport protocol can be either IPv4 or IPv6, whereas the manual IPv6 technique uses only IPv4 as its transport protocol. Appendix I show how this technique is configured on router RA and RB.

3.6.4 Intra-site automatic tunnel addressing protocol transition technique

Although the ISATAP transition technique can be used for traffic between two industrial communication network sites, it is suitable for transitioning network traffic within a site. ISATAP uses unicast addresses with a 64 bit prefix length and an EUI-64 generated interface identifier (ID). The EUI-64 ID is created using the first 32 bits of 0000:5EFE and the last 32 bits are the IPv4 address of the interface. In the configuration process of routers RA and RB of Figure 3.4, the prefixes used are 13:13::/64 and 14:14::/64 respectively. The loopback IPv4 addresses used are 172.16.8.1 for RA and 172.16.9.1 for RB. The configurations for ISATAP are done on RIPng, EIGRPv6 and OSPFv3. Appendix I show how this technique is configured on router RA and RB.

3.6.5 Static network address translation-protocol translation technique

The static NAT-PT transition technique is another powerful transition technique that can be used to communicate between IPv4-only and IPv6-only industrial communication networks. All configurations for this technique are done on router RA, the NAT-PT router of Figure 3.5. The commandline process of configuring this technique is shown in appendix I.

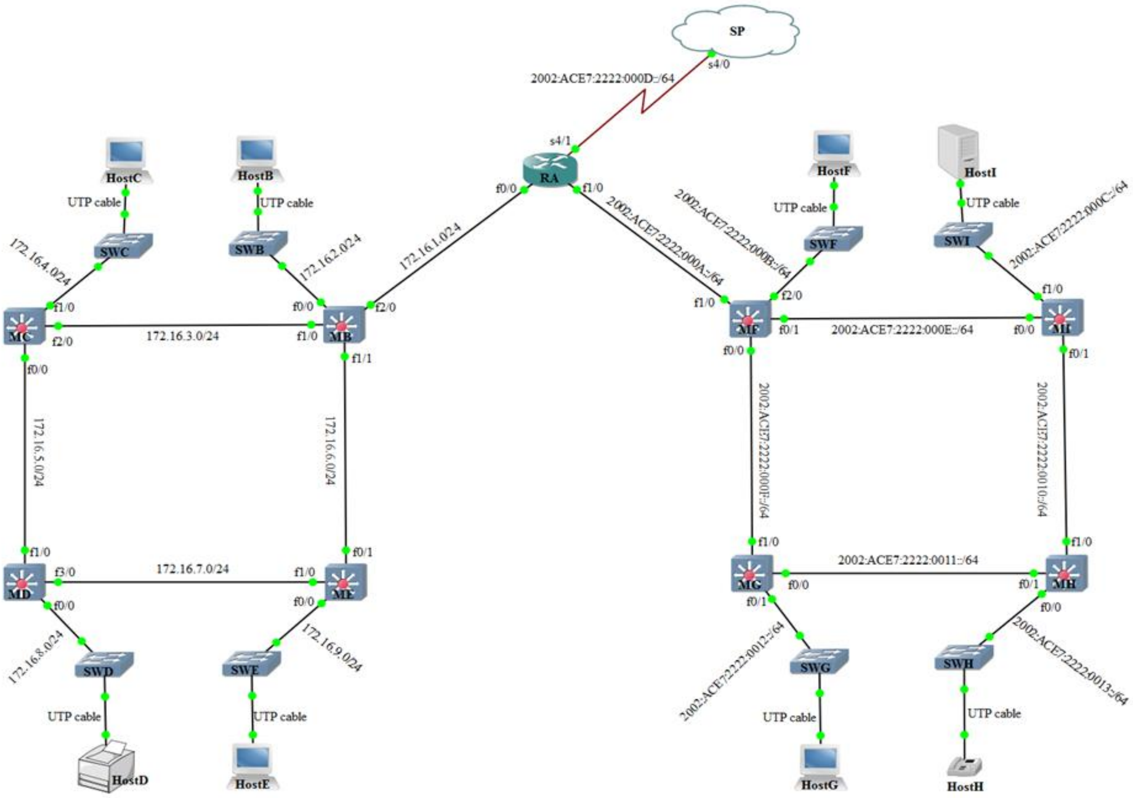

Figure 3.5. Ring network topology for static NAT-PT configurations

3.7 HIERARCHICAL NETWORK TOPOLOGY FOR IPV6 INDUSTRIAL COMMUNICATION

Figure 3.6 shows a hierarchical IPv6 industrial communication network topology comprising three levels. The first level consists of routers RG and RH, while the second level consists of multilayer switches ME and MF. The third level comprises multilayer switches MA, MB, MC, MD and layer 2 switches SA, SB, SC and SD. Connected to the layer 2 switches are end devices (hosts), named host A, host B, host C and host D. All the routers and multilayer switches are linked together using single mode fibre cables, whereas connections between multilayer switches, layer 2 switches and end devices are made using unshielded twisted pair cables. Although layer 2 switches and end devices are included in this topology, no IPv6 configurations are configured on these devices. Configurations are only done on layer 3 devices (routers and multilayer switches), while the role of layer 2 devices and end devices is only to complete the LAN connections.

Table 3.3 First 20 subnetworks for the hierarchical network topology

2002:ACE7:2222:0000::/64	2002:ACE7:2222:000A::/64
2002:ACE7:2222:0001::/64	2002:ACE7:2222:000B::/64
2002:ACE7:2222:0002::/64	2002:ACE7:2222:000C::/64
2002:ACE7:2222:0003::/64	2002:ACE7:2222:000D::/64
2002:ACE7:2222:0004::/64	2002:ACE7:2222:000E::/64
2002:ACE7:2222:0005::/64	2002:ACE7:2222:000F::/64
2002:ACE7:2222:0006::/64	2002:ACE7:2222:0010::/64
2002:ACE7:2222:0007::/64	2002:ACE7:2222:0011::/64
2002:ACE7:2222:0008::/64	2002:ACE7:2222:0012::/64
2002:ACE7:2222:0009::/64	2002:ACE7:2222:0013::/64

3.7.1 Subnetworks for the hierarchical network topology

In order to have more network prefixes for Figure 3.6, the global routing prefix of 2002:ACE7:2222::/48, has been subnetted (subdivided into 20 smaller networks), yielding the subnets shown in Table 3.3.

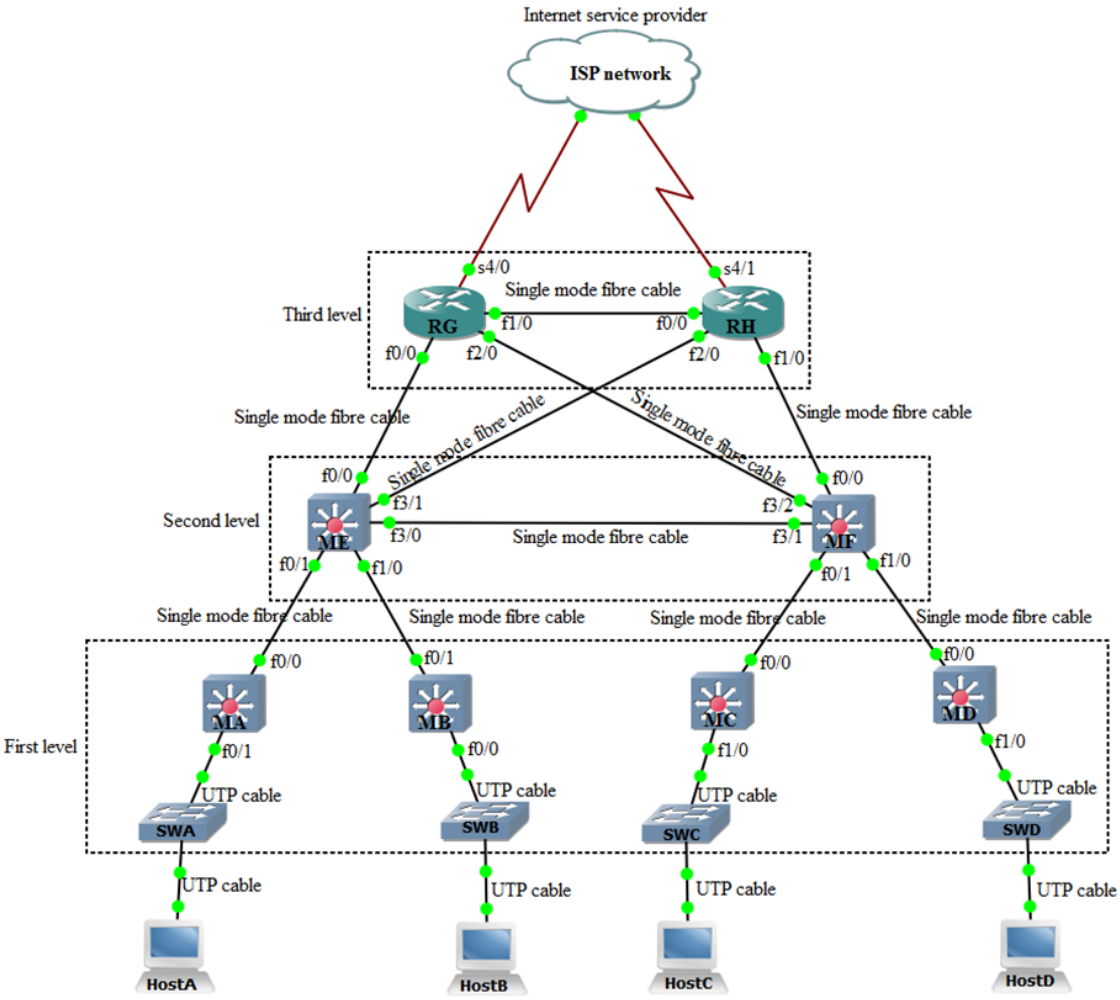

Figure 3.6. Cable connections for hierarchical network topology

3.7.2 Results of assigning sixteen subnets to the hierarchical network topology

Using the subnetworks in Table 3.3, sixteen subnets are assigned to different networks in Figure 3.6 and the results are as shown in Figure 3.7. Note that the 2002:ACE7:2222:0000::/64 subnetwork has not been assigned to any specific network because it is reserved.

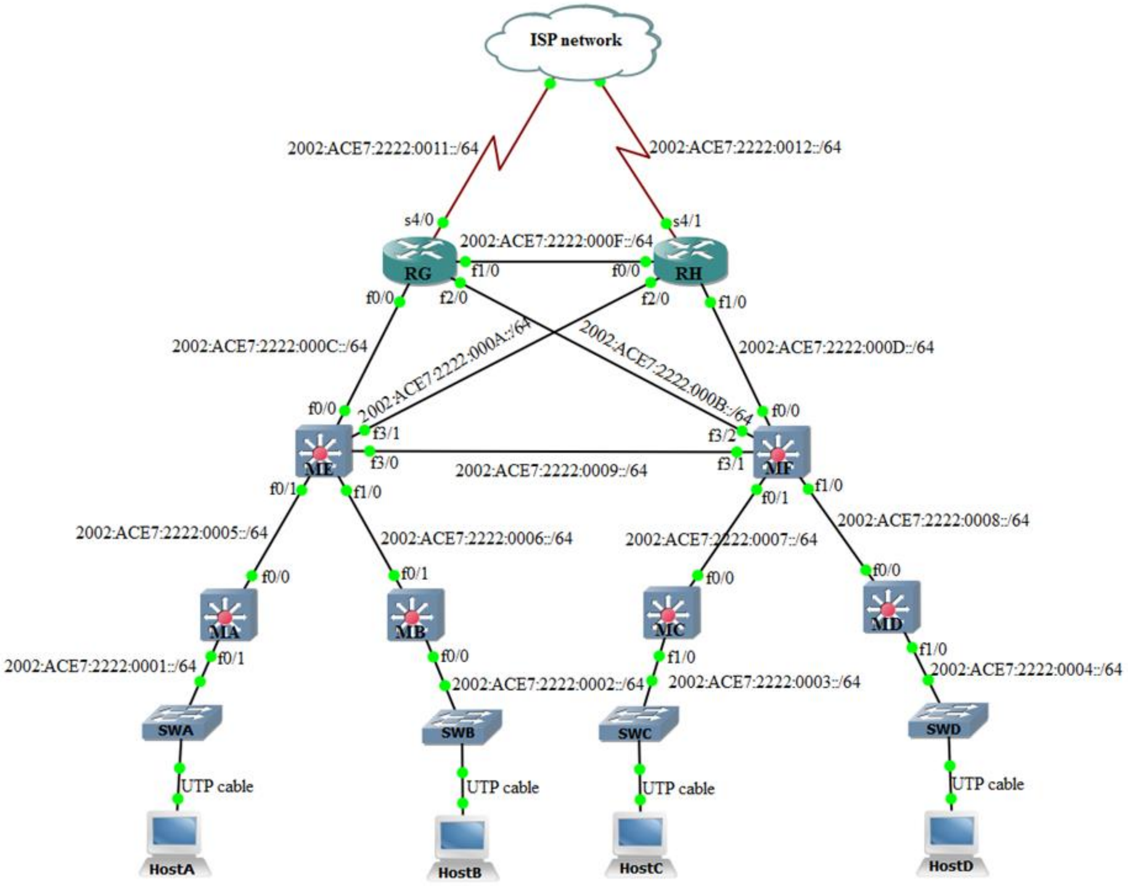

Figure 3.7. Sixteen subnetworks for hierarchical network topology

3.7.3 Static unicast IPv6 address configuration

The entire static unicast IPv6 address configuration on multilayer switches and routers in Figure 3.7 uses the same configuration commands and naming convention of interfaces as in Section 3.3.1. The configuration process is similar to the one shown in appendix E.

3.7.4 Static IPv6 routing configurations

The process of how to configure static IPv6 routing on the multilayer switches and routers in Figure 3.7 uses the same configuration commands as those shown in sections 3.4.1. The whole process is similar to the one illustrated in appendix G.

3.7.5 RIPng routing configuration process

The process of configuring RIPng in this section uses the same configuration commands as those used in Section 3.4.2.1. Appendix H shows how the whole process is done on multilayer switches and routers.

3.7.6 EIGRPv6 routing configuration process

All the eigrpv6 configurations for Figure 3.7 are done using the configuration commands of Section 3.4.2.2. See appendix H for more details on the configuration process.

3.7.7 OSPFv3 routing configuration process

Configurations in this section have been done using the same OSPFv3 commands as those in Section 3.4.2.3. More details on the configuration process are given in appendix H.

3.7.8 Extended unique identifier configuration process

The extended unique identifier (EUI-64) configuration method allows a router or multilayer switch to automatically create a unique interface ID part of the IPv6 address. It uses the "ipv6 address" command to configure only the 64 bits of the prefix of a given interface, while the rest of the address is generated with the help of EUI-64 rules. This section uses this method to configure the addresses on the routers and multilayer switches of Figure 3.7. The whole configuration process is done as illustrated on router RG in appendix I.

3.7.9 Hot standby router protocol version 2 configuration process

Three IPv6 redundancy protocols can be used in industrial communication networks to create redundancy for routers or multilayer switches. These protocols are hot standby router protocol version 2 (HSRPv2), virtual router redundancy protocol version 3 (VRRPv3) and gateway load balancing protocol (GLBP). VRRPv3 is an open standard redundancy protocol; however, at the time of writing this dissertation, it was not supported by Cisco IOS software version 12.4(24)T that is running on the GNS3 routers and multilayer switches. Both HSRPv2 and GLBP are Cisco proprietary and work in almost the same way; the only difference between them is that GLBP provides load balancing while HSRPv2 does not.

Only HSRPv2 is considered in this study, because most of its operational features cover the other redundany protocols. Thus, this section describes the configuration process of HSRPv2 on RIPng, EIGRPv6 and OSPFv3, using Figure 3.7. In these configurations, RG is the active router and RH is the standby router. Both routers provide redundancy to the ISP network. Note that all the configuration processes for RIPng, EIGRPv6 and OSPFv3 are done as shown in Section 3.4.2. The ISP router interfaces of fastethernet 0/0 and fastethernet f1/0 are configured with 2002:ACE7:2222:0011::/64 eui-64 and 2002:ACE7:2222:0012::/64 eui-64 addresses respectively. Appendix J shows how the whole process is configured on router RG and RH using RIPng, EIGRPv6 and OSPFv3 routing protocols.

3.7.10 Testing of HSRPv2 failover time

After configuring HSRPv2 on routers RG and RH for each routing protocol as described above, a ping command with a repeat count of 50 is issued on multilayer switch ME. After two seconds, the interface fastethernet 2/1 on multilayer switch ME is shut down, using the shutdown command and the failover time to the standby router RH is noted.

CHAPTER 4 RESULTS FOR LAYER 3 IPV6 CONFIGURATIONS

4.1 INTRODUCTION

This chapter shows the results of configuring IPv6 layer 3 configurations on the ring and hierarchical industrial communication networks. These layer 3 results cover static and dynamic addresses, static and dynamic routing protocols with their respective ping and traceroute results. The traceroute and ping results of configuring dual stack, manual IPv6, GRE and ISATAP on RIPng, EIGRPv6 and OSPFv3 are shown in this chapter as well. Furthermore, the ping results of configuring HSRPv2 redundancy protocol on RIPng, EIGRPv6 and OSPFv3 are also presented. Since all the layer 3 devices produced similar results for each respective configuration, the results shown are samples from randomly selected multilayer switches and routers.

4.2 STATIC AND DYNAMIC ADDRESS CONFIGURATION RESULTS

4.2.1 Results for static unicast IPv6 addresses

The results for configuring static IPv6 addresses are obtained using the “show ipv6 interface brief,” and “show ipv6 route connected updated” commands on randomly sampled routers and multilayer switches. The former command shows whether the router or multilayer switch interface is up or down, whereas the latter command helps to show the administrative distance, metric and last update of interfaces. Furthermore, the first command shows both the link-local and global unicast addresses, while the second command only shows the global unicast addresses. These two commands are very useful in troubleshooting the status of static routes in industrial communication networks. In the (up/up) interface status, the first parameter represents the physical layer and the second is the data link layer. If the interface is up and running, the line protocol of the data link layer should be up and the physical layer should also be up as well. However, if there is a problem with the line protocol the status of the interface will be shown as (up/down). When both the physical layer and the line protocol are not working the status of the interface is shown by (down/down). For brevity only interfaces configured with IPv6 addresses are shown in the results; the rest of the interfaces are omitted.

4.2.1.1 Router RA and multilayer switch ME

Table 4.1 Results of static IPv6 addresses for router RA and multilayer switch ME

RA # show ipv6 interface brief	ME # show ipv6 interface brief
FastEthernet0/0 [up/up] FE80::C801:1FFF:FE34:0 2002:ACE7:2222:2::A	FastEthernet0/0 [up/up] FE80::C004:FFF:FED0:0 2002:ACE7:2222:9::E
FastEthernet1/0 [up/up] FE80::C801:1FFF:FE34:1C 2002:ACE7:2222:A::A	FastEthernet0/1 [up/up] FE80::C004:FFF:FED0:1 2002:ACE7:2222:6::E
Serial4/1 [up/up] FE80::C801:1FFF:FE34:0 2002:ACE7:2222:D::A	FastEthernet1/0 [up/up] FE80::C004:FFF:FED0:10 2002:ACE7:2222:6::B

4.2.1.2 Multilayer switch MB

Table 4.2 Results of static IPv6 addresses for multilayer switch MB

MB # show ipv6 route connected updated
C 2002:ACE7:2222:1::/64 [0/0] via FastEthernet0/0, directly connected Last updated 11:10:05 29 November 2015
C 2002:ACE7:2222:2::/64 [0/0] via FastEthernet2/0, directly connected Last updated 11:10:06 29 November 2015
C 2002:ACE7:2222:4::/64 [0/0] via FastEthernet1/0, directly connected Last updated 11:10:06 29 November 2015
C 2002:ACE7:2222:6::/64 [0/0] via FastEthernet1/1, directly connected Last updated 11:10:06 29 November 2015

Note that the code C in the results for multilayer switch MB stands for directly connected routes.

4.2.1.3 Router MB and multilayer switch MF

Table 4.3 Results of static IPv6 addresses for router MB and multilayer switch MF

MB # show ipv6 interface brief	MF # show ipv6 interface brief
FastEthernet0/0 [up/up] FE80::C802:1CFF:FE64:0 2002:ACE7:2222:1::B	FastEthernet0/0 [up/up] FE80::C006:26FF:FE74:0 2002:ACE7:2222:F::F
FastEthernet1/0 [up/up] FE80::C802:1CFF:FE64:1C 2002:ACE7:2222:4::B	FastEthernet0/1 [up/up] FE80::C006:26FF:FE74:1 2002:ACE7:2222:E::F
FastEthernet1/1 [up/up] FE80::C802:1CFF:FE64:1D 2002:ACE7:2222:6::B	FastEthernet1/0 [up/up] FE80::C006:26FF:FE74:10 2002:ACE7:2222:A::F
FastEthernet2/0 [up/up] FE80::C802:1CFF:FE64:38 2002:ACE7:2222:2::B	FastEthernet2/0 [up/up] FE80::C006:26FF:FE74:20 2002:ACE7:2222:B::F

4.2.2 Results for stateless autoconfiguration addresses

These addresses are obtained using the “show ipv6 interface brief command” and are called link-local addresses. They are not routable but can be used for neighbour discovery, router discovery and stateless address autoconfiguration in a particular network. Notice in the results that these link-local address are created by inserting the FF:FE in the middle of the media access control (MAC) address of the router or multilayer switch. This is done in order to make the 64 bits required for an interface identifier of a router or multilayer switch. The 48 bits of the MAC address is added to the 16 bits of FFFE.

4.2.2.1 Multilayer switch MB and MF

Table 4.4 Results of stateless autoconfiguration addresses for router MB and MF

MB # show ipv6 interface brief	MF # show ipv6 interface brief
FastEthernet0/0 [up/up] FE80::C802:1CFF:FE64:0	FastEthernet0/0 [up/up] FE80::C006:26FF:FE74:0
FastEthernet1/0 [up/up] FE80::C802:1CFF:FE64:1C	FastEthernet0/1 [up/up] FE80::C006:26FF:FE74:1
FastEthernet1/1 [up/up] FE80::C802:1CFF:FE64:1D	FastEthernet1/0 [up/up] FE80::C006:26FF:FE74:10
FastEthernet2/0 [up/up] FE80::C802:1CFF:FE64:38	FastEthernet2/0 [up/up] FE80::C006:26FF:FE74:20

4.2.2.2 Multilayer switch MD and Router RA

Table 4.5 Results of stateless autoconfiguration addresses for multilayer switch MD and router RA

MD # show ipv6 interface brief	RA # show ipv6 interface brief
FastEthernet0/0 [up/up] FE80::CE05:DFF:FEE4:0	FastEthernet0/0 [up/up] FE80::C801:1FFF:FE34:0
FastEthernet1/0 [up/up] FE80::CE05:DFF:FEE4:10	FastEthernet1/0 [up/up] FE80::C801:1FFF:FE34:1C
FastEthernet3/0 [up/up] FE80::CE05:DFF:FEE4:30	Serial4/1 [up/up] FE80::C801:1FFF:FE34:0

4.3 RESULTS FOR STATIC IPV6 ROUTING PROTOCOL

4.3.1 Results of configuring static routing on global unicast addresses

The “show ipv6 route static” command is used to obtain the static routes results. Note that the code S stands for static routes.

4.3.1.1 Results for multilayer switch MB and MC

Table 4.6 Results of static routing on global unicast addresses for multilayer switch MB and MC

MB # show ipv6 route static	MC # show ipv6 route static
S 2002:ACE7:2222:3::/64 [1/0] via 2002:ACE7:2222:4::C	S 2002:ACE7:2222:1::/64 [1/0] via 2002:ACE7:2222:4::B
S 2002:ACE7:2222:5::/64 [1/0] via 2002:ACE7:2222:4::C	S 2002:ACE7:2222:2::/64 [1/0] via 2002:ACE7:2222:4::B
S 2002:ACE7:2222:7::/64 [1/0] via 2002:ACE7:2222:4::C	S 2002:ACE7:2222:6::/64 [1/0] via 2002:ACE7:2222:4::B
S 2002:ACE7:2222:8::/64 [1/0] via 2002:ACE7:2222:6::E	S 2002:ACE7:2222:7::/64 [1/0] via 2002:ACE7:2222:5::D
S 2002:ACE7:2222:9::/64 [1/0] via 2002:ACE7:2222:6::E	S 2002:ACE7:2222:8::/64 [1/0] via 2002:ACE7:2222:5::D

4.3.1.2 Results for multilayer switch MF and MI

Table 4.7 Results of static routing on global unicast addresses for multilayer switch MF and MI

MG # show ipv6 route static	MI # show ipv6 route static
S 2002:ACE7:2222:A::/64 [1/0] via ::, FastEthernet1/0	S 2002:ACE7:2222:A::/64 [1/0] via ::, FastEthernet0/0
S 2002:ACE7:2222:B::/64 [1/0] via ::, FastEthernet1/0	S 2002:ACE7:2222:B::/64 [1/0] via ::, FastEthernet0/0
S 2002:ACE7:2222:C::/64 [1/0] via ::, FastEthernet1/0	S 2002:ACE7:2222:F::/64 [1/0] via ::, FastEthernet0/0
S 2002:ACE7:2222:10::/64[1/0] via ::, FastEthernet0/0	S 2002:ACE7:2222:12::/64 [1/0] via ::, FastEthernet0/1
S 2002:ACE7:2222:13::/64 [1/0] via ::, FastEthernet0/0	S 2002:ACE7:2222:13::/64 [1/0] via ::, FastEthernet0/1

4.3.2 Ping and traceroute results when outgoing local interface is next hop address

These ping and traceroute results are obtained on routers and multilayer switches configured with static routing on unicast global addresses. The next hop address used for static routing is the outgoing local interface of the router or multilayer switch.

4.3.2.1 Traceroute results

Table 4.8 Traceroute results for multilayer switch MD using outgoing local interface

```
MD # traceroute 2002:ACE7:2222:0013::11
Type escape sequence to abort.
Tracing the route to 2002:ACE7:2222:13::11
  1  *  *  *
  2  *  *  *
  3  *  *  *
  ………..
  ………..
  ………..
 26  *  *  *
 27  *  *  *
 28  *  *  *
 29  *  *  *
 30  *  *  *
Destination not found inside max hop count diameter.
```

4.3.2.2 Ping results

Table 4.9 Ping results for multilayer switch MD using outgoing local interface

```
MD # ping 2002:ACE7:2222:0013::11
Type escape sequence to abort.
Sending 5, 100-byte ICMP echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
.....
Success rate is 0% (0/5)
```

4.3.3 Ping and traceroute results when global unicast address is next hop address

The following ping and traceroute results are obtained on routers and multilayer switches configured with static routing on static addresses and using the neighbour global unicast address as next hop address.

4.3.3.1 Ping results

Table 4.10 Ping results for multilayer switch MD using global unicast address

```
MD # ping 2002:ACE7:2222:0013::11
Type escape sequence to abort.
Sending 5, 100-byte ICMP echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 508/651/852 ms
MD # ping 2002:ACE7:2222:0013::11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 608/717/856 ms
```

4.3.3.2 Traceroute results

Table 4.11 Traceroute results for multilayer switch MD using global unicast address

```
MD # traceroute 2002:ACE7:2222:0013::11
Type escape sequence to abort.
Tracing the route to 2002:ACE7:2222:13::11
1   2002:ACE7:2222:5::C      100 msec 100 msec 100 msec
2   2002:ACE7:2222:4::B      204 msec 204 msec 268 msec
3   2002:ACE7:2222:2::A      408 msec 404 msec 304 msec
4   2002:ACE7:2222:A::F      404 msec 512 msec 404 msec
5   2002:ACE7:2222:F::10     500 msec 616 msec 608 msec
6   2002:ACE7:2222:13::11    804 msec 600 msec 600 msec
```

4.4 RESULTS FOR DYNAMIC ROUTING PROTOCOLS

4.4.1 Results of configuring RIPng on static unicast addresses

The results of configuring RIPng are obtained with the commands, “show ipv6 route rip” and “show ipv6 protocols.” The first command is useful in troubleshooting the administrative distance of the routes and their respective hops required to reach the remote networks. In addition, it is helpful in identifying the link-local addresses being used as the next-hop addresses in the networks. Although the second command does not show the IPv6 addresses configured for the RIPng process, it is very useful in determining the RIPng name and the interfaces participating in the process. Notice from the results that being a distance vector protocol, the maximum hop count of RIPng does not exceed 15. The code R stands for RIPng. Thus, these two commands can be used to effectively identify which addresses and interfaces are not participating in the process of RIPng in industrial communication networks.

4.4.1.1 RIPng results for router RA

Table 4.12 Results of configuring RIPng on router RA

```
RA # show ipv6 route rip
R   2002:ACE7:2222:1::/64 [120/2]     via  FE80::C802:1CFF:FE64:38, FastEthernet0/0
R   2002:ACE7:2222:3::/64 [120/3]     via  FE80::C802:1CFF:FE64:38, FastEthernet0/0
R   2002:ACE7:2222:4::/64 [120/2]     via  FE80::C802:1CFF:FE64:38, FastEthernet0/0
R   2002:ACE7:2222:5::/64 [120/3]     via  FE80::C802:1CFF:FE64:38, FastEthernet0/0
R   2002:ACE7:2222:6::/64 [120/2]     via  FE80::C802:1CFF:FE64:38, FastEthernet0/0
R   2002:ACE7:2222:7::/64 [120/3]     via  FE80::C802:1CFF:FE64:38, FastEthernet0/0
R   2002:ACE7:2222:8::/64 [120/4]     via  FE80::C802:1CFF:FE64:38, FastEthernet0/0
R   2002:ACE7:2222:9::/64 [120/3]     via  FE80::C802:1CFF:FE64:38, FastEthernet0/0
R   2002:ACE7:2222:C::/64 [120/3]     via  FE80::C006:26FF:FE74:10, FastEthernet1/0
R   2002:ACE7:2222:E::/64 [120/2]     via  FE80::C006:26FF:FE74:10, FastEthernet1/0
R   2002:ACE7:2222:F::/64 [120/2]     via  FE80::C006:26FF:FE74:10, FastEthernet1/0
R   2002:ACE7:2222:10::/64 [120/3]    via  FE80::C006:26FF:FE74:10, FastEthernet1/0
R   2002:ACE7:2222:11::/64 [120/3]    via  FE80::C006:26FF:FE74:10, FastEthernet1/0
R   2002:ACE7:2222:12::/64 [120/3]    via  FE80::C006:26FF:FE74:10, FastEthernet1/0
R   2002:ACE7:2222:13::/64 [120/4]    via  FE80::C006:26FF:FE74:10, FastEthernet1/0
```

4.4.1.2 RIPng results for multilayer switch MB

Table 4.13 Results of configuring RIPng on multilayer switch MB

```
MB # show ipv6 route rip
R   2002:ACE7:2222:3::/64 [120/2]     via  FE80::C603:1CFF:FEFC:20, FastEthernet1/0
R   2002:ACE7:2222:5::/64 [120/2]     via  FE80::C603:1CFF:FEFC:20, FastEthernet1/0
R   2002:ACE7:2222:7::/64 [120/2]     via  FE80::C004:FFF:FED0:1, FastEthernet1/1
R   2002:ACE7:2222:8::/64 [120/3]     via  FE80::C603:1CFF:FEFC:20, FastEthernet1/0
                                      via  FE80::C004:FFF:FED0:1, FastEthernet1/1
R   2002:ACE7:2222:9::/64 [120/2]     via  FE80::C004:FFF:FED0:1, FastEthernet1/1
R   2002:ACE7:2222:A::/64 [120/2]     via FE80::C801:1FFF:FE34:0, FastEthernet2/0
R   2002:ACE7:2222:C::/64 [120/4]     via FE80::C801:1FFF:FE34:0, FastEthernet2/0
R   2002:ACE7:2222:D::/64 [120/2]     via FE80::C801:1FFF:FE34:0, FastEthernet2/0
R   2002:ACE7:2222:E::/64 [120/3]     via FE80::C801:1FFF:FE34:0, FastEthernet2/0
R   2002:ACE7:2222:F::/64 [120/3]     via FE80::C801:1FFF:FE34:0, FastEthernet2/0
R   2002:ACE7:2222:10::/64 [120/4]    via FE80::C801:1FFF:FE34:0, FastEthernet2/0
R   2002:ACE7:2222:11::/64 [120/4]    via FE80::C801:1FFF:FE34:0, FastEthernet2/0
R   2002:ACE7:2222:12::/64 [120/4]    via FE80::C801:1FFF:FE34:0, FastEthernet2/0
R   2002:ACE7:2222:13::/64 [120/5]    via FE80::C801:1FFF:FE34:0, FastEthernet2/0
```

4.4.1.3 RIPng results for multilayer switch ME

Table 4.14 Results of configuring RIPng on multilayer switch ME

```
ME # show ipv6 route rip
R   2002:ACE7:2222:1::/64 [120/2]      via FE80::C802:1CFF:FE64:1D, FastEthernet0/1
R   2002:ACE7:2222:2::/64 [120/2]      via FE80::C802:1CFF:FE64:1D, FastEthernet0/1
R   2002:ACE7:2222:3::/64 [120/3]      via FE80::C802:1CFF:FE64:1D, FastEthernet0/1
                                       via FE80::CE05:DFF:FEE4:30,   FastEthernet1/0
R   2002:ACE7:2222:4::/64 [120/2]      via FE80::C802:1CFF:FE64:1D, FastEthernet0/1
R   2002:ACE7:2222:5::/64 [120/2]      via FE80::CE05:DFF:FEE4:30,   FastEthernet1/0
R   2002:ACE7:2222:8::/64 [120/2]      via FE80::CE05:DFF:FEE4:30,   FastEthernet1/0
R   2002:ACE7:2222:A::/64 [120/3]      via FE80::C802:1CFF:FE64:1D, FastEthernet0/1
R   2002:ACE7:2222:C::/64 [120/5]      via FE80::C802:1CFF:FE64:1D, FastEthernet0/1
R   2002:ACE7:2222:D::/64 [120/3]      via FE80::C802:1CFF:FE64:1D, FastEthernet0/1
R   2002:ACE7:2222:E::/64 [120/4]      via FE80::C802:1CFF:FE64:1D, FastEthernet0/1
R   2002:ACE7:2222:F::/64 [120/4]      via FE80::C802:1CFF:FE64:1D, FastEthernet0/1
R   2002:ACE7:2222:10::/64 [120/5]     via FE80::C802:1CFF:FE64:1D, FastEthernet0/1
R   2002:ACE7:2222:11::/64 [120/5]     via FE80::C802:1CFF:FE64:1D, FastEthernet0/1
R   2002:ACE7:2222:12::/64 [120/5]     via FE80::C802:1CFF:FE64:1D, FastEthernet0/1
R   2002:ACE7:2222:13::/64 [120/6]     via FE80::C802:1CFF:FE64:1D, FastEthernet0/1
```

4.4.1.4 RIPng results for multilayer switch MI

Table 4.15 Results of configuring RIPng on multilayer switch MI

```
MI # show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "rip benji"
Interfaces:
FastEthernet1/0
FastEthernet0/1
FastEthernet0/0
Redistribution: None
```

4.4.1.5 Ping results of RIPng on static addresses

The following are the ping results of configuring RIPng on static unicast addresses. The results are obtained on multilayer switch MD.

Table 4.16 Ping results of configuring RIPng on multilayer switch MD

```
MD # ping 2002:ACE7:2222:0013::11
Type escape sequence to abort.
Sending 5, 100-byte ICMP echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 72/84/104 ms
MD # ping 2002:ACE7:2222:0013::11
Type escape sequence to abort.
Sending 5, 100-byte ICMP echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 64/69/84 ms
```

4.4.1.6 Traceroute results of RIPng on static addresses

Table 4.17 Traceroute results of configuring RIPng on multilayer switch MA

```
MA # traceroute ipv6 2002:ACE7:2222:0004::D
Type escape sequence to abort.
Tracing the route to 2002:ACE7:2222:4::D
1    2002:ACE7:2222:5::E     64 msec 20 msec 4 msec
2    2002:ACE7:2222:9::F     36 msec 28 msec 28 msec
3    2002:ACE7:2222:8::D    48 msec 28 msec 40 msec
```

4.4.2 Results of configuring EIGRPv6 on static addresses

Obtaining the EIGRPv6 results from the sampled multilayer switches and routers is done using the commands, “show ipv6 route eigrp” and “show ipv6 route eigrp updated.” These commands lists the different routes learned with a code of D with their respective next-hop link-local addresses. Furthermore, both commands show the metrics and the administrative distances of the routes. However, the second command has the advantage of also showing the last time and date when the EIGRPv6 configuration was updated. The code D stands for eigrp routes. Notice from the results that EIGRPv6 has a lower administrative distance (AD) of 90 compared to RIPng which has an AD of 120. However, the route metrics of EIGRPv6 are higher than RIPng. Nonetheless, both of these routing protocols use link-local addresses as their next-hop addresses. Troubleshooting of industrial communication networks with these two commands would also show which interfaces and global unicast addresses are configured with EIGRPv6 protocol. Tables 4.18, 4.19, 4.20 and 4.21 shows the results of configuring EIGRPv6 on router RA and multilayer switches MB, MC and MF respectively.

4.4.2.1 Results for router RA

Table 4.18 Results of configuring EIGRPv6 on static unicast addresses on router RA

```
RA # show ipv6 route eigrp
D   2002:ACE7:2222:1::/64 [90/30720]   via FE80::C802:1CFF:FE64:38, FastEthernet0/0
D   2002:ACE7:2222:3::/64 [90/33280]   via FE80::C802:1CFF:FE64:38, FastEthernet0/0
D   2002:ACE7:2222:4::/64 [90/30720]   via FE80::C802:1CFF:FE64:38, FastEthernet0/0
D   2002:ACE7:2222:5::/64 [90/33280]   via FE80::C802:1CFF:FE64:38, FastEthernet0/0
D   2002:ACE7:2222:6::/64 [90/30720]   via FE80::C802:1CFF:FE64:38, FastEthernet0/0
D   2002:ACE7:2222:7::/64 [90/33280]   via FE80::C802:1CFF:FE64:38, FastEthernet0/0
D   2002:ACE7:2222:8::/64 [90/35840]   via FE80::C802:1CFF:FE64:38, FastEthernet0/0
D   2002:ACE7:2222:9::/64 [90/33280]   via FE80::C802:1CFF:FE64:38, FastEthernet0/0
D   2002:ACE7:2222:B::/64 [90/30720]  via FE80::C806:1CFF:FE18:1C, FastEthernet1/0
D   2002:ACE7:2222:C::/64 [90/33280]  via FE80::C806:1CFF:FE18:1C, FastEthernet1/0
D   2002:ACE7:2222:E::/64 [90/30720]  via FE80::C806:1CFF:FE18:1C, FastEthernet1/0
D   2002:ACE7:2222:F::/64 [90/30720]  via FE80::C806:1CFF:FE18:1C, FastEthernet1/0
D   2002:ACE7:2222:10::/64 [90/33280]via FE80::C806:1CFF:FE18:1C, FastEthernet1/0
D   2002:ACE7:2222:11::/64 [90/33280]via FE80::C806:1CFF:FE18:1C, FastEthernet1/0
D   2002:ACE7:2222:12::/64 [90/33280]via FE80::C806:1CFF:FE18:1C, FastEthernet1/0
D   2002:ACE7:2222:13::/64 [90/35840]via FE80::C806:1CFF:FE18:1C, FastEthernet1/0
```

4.4.2.2 Results for multilayer switch MB

Table 4.19 Results of configuring EIGRPv6 on the static unicast addresses of multilayer switch MB

```
MB # show ipv6 route eigrp
D  2002:ACE7:2222:3::/64 [90/30720]   via FE80::C80B:14FF:FEC4:38, FastEthernet1/0
D  2002:ACE7:2222:5::/64 [90/30720]   via FE80::C80B:14FF:FEC4:38, FastEthernet1/0
D   2002:ACE7:2222:7::/64 [90/30720]    via FE80::C804:12FF:FE1C:6, FastEthernet1/1
D   2002:ACE7:2222:8::/64 [90/33280]   via FE80::C804:12FF:FE1C:6, FastEthernet1/1
                                      via FE80::C80B:14FF:FEC4:38, FastEthernet1/0
D   2002:ACE7:2222:9::/64 [90/30720]    via FE80::C804:12FF:FE1C:6, FastEthernet1/1
D   2002:ACE7:2222:A::/64 [90/30720]    via FE80::C801:1FFF:FE34:0, FastEthernet2/0
D   2002:ACE7:2222:B::/64 [90/33280]    via FE80::C801:1FFF:FE34:0, FastEthernet2/0
D   2002:ACE7:2222:C::/64 [90/35840]    via FE80::C801:1FFF:FE34:0, FastEthernet2/0
D   2002:ACE7:2222:D::/64 [90/2172416]via FE80::C801:1FFF:FE34:0, FastEthernet2/0
D   2002:ACE7:2222:E::/64 [90/33280]    via FE80::C801:1FFF:FE34:0, FastEthernet2/0
D   2002:ACE7:2222:F::/64 [90/33280]    via FE80::C801:1FFF:FE34:0, FastEthernet2/0
D   2002:ACE7:2222:10::/64 [90/35840]   via FE80::C801:1FFF:FE34:0, FastEthernet2/0
D   2002:ACE7:2222:11::/64 [90/35840]   via FE80::C801:1FFF:FE34:0, FastEthernet2/0
D   2002:ACE7:2222:12::/64 [90/35840]   via FE80::C801:1FFF:FE34:0, FastEthernet2/0
D   2002:ACE7:2222:13::/64 [90/38400]   via FE80::C801:1FFF:FE34:0, FastEthernet2/0
```

4.4.2.3 Results for multilayer switch MC

Table 4.20 Results of configuring EIGRPv6 on the static unicast addresses of multilayer switch MC

```
MC # show ipv6 route eigrp
D  2002:ACE7:2222:1::/64 [90/30720]   via FE80::C802:1CFF:FE64:1C, FastEthernet2/0
D  2002:ACE7:2222:2::/64 [90/30720]   via FE80::C802:1CFF:FE64:1C, FastEthernet2/0
D  2002:ACE7:2222:6::/64 [90/30720]   via FE80::C802:1CFF:FE64:1C, FastEthernet2/0
D   2002:ACE7:2222:7::/64 [90/30720] via FE80::C803:6FF:FE2C:1C, FastEthernet0/0
D   2002:ACE7:2222:8::/64 [90/30720] via FE80::C803:6FF:FE2C:1C, FastEthernet0/0
D   2002:ACE7:2222:9::/64 [90/33280] via FE80::C803:6FF:FE2C:1C, FastEthernet0/0
                                     via FE80::C802:1CFF:FE64:1C, FastEthernet2/0
D  2002:ACE7:2222:A::/64 [90/33280] via FE80::C802:1CFF:FE64:1C, FastEthernet2/0
D  2002:ACE7:2222:B::/64 [90/35840]  via FE80::C802:1CFF:FE64:1C, FastEthernet2/0
D  2002:ACE7:2222:C::/64 [90/38400]  via FE80::C802:1CFF:FE64:1C, FastEthernet2/0
D2002:ACE7:2222:D::/64[90/2174976] viaFE80::C802:1CFF:FE64:1C, FastEthernet2/0
D2002:ACE7:2222:E::/64 [90/35840]    via FE80::C802:1CFF:FE64:1C, FastEthernet2/0
D2002:ACE7:2222:F::/64 [90/35840]    via FE80::C802:1CFF:FE64:1C, FastEthernet2/0
D2002:ACE7:2222:10::/64 [90/38400]  viaFE80::C802:1CFF:FE64:1C, FastEthernet2/0
D2002:ACE7:2222:11::/64 [90/38400]   viaFE80::C802:1CFF:FE64:1C, FastEthernet2/0
D2002:ACE7:2222:12::/64 [90/38400]   viaFE80::C802:1CFF:FE64:1C, FastEthernet2/0
D2002:ACE7:2222:13::/64 [90/40960]   viaFE80::C802:1CFF:FE64:1C, FastEthernet2/0
```

4.4.2.4 Results for multilayer switch MF

Table 4.21 Results of configuring EIGRPv6 on the static unicast addresses of multilayer switch MF

```
MF # show ipv6 route eigrp updated
D  2002:ACE7:2222:1::/64 [90/33280]  via FE80::C801:1FFF:FE34:1C, FastEthernet1/0
D  2002:ACE7:2222:2::/64 [90/30720]  via FE80::C801:1FFF:FE34:1C, FastEthernet1/0
D  2002:ACE7:2222:3::/64 [90/35840]  via FE80::C801:1FFF:FE34:1C, FastEthernet1/0
D  2002:ACE7:2222:4::/64 [90/33280]  via FE80::C801:1FFF:FE34:1C, FastEthernet1/0
D  2002:ACE7:2222:5::/64 [90/35840]  via FE80::C801:1FFF:FE34:1C, FastEthernet1/0
D  2002:ACE7:2222:6::/64 [90/33280]  via FE80::C801:1FFF:FE34:1C, FastEthernet1/0
D  2002:ACE7:2222:7::/64 [90/35840]  via FE80::C801:1FFF:FE34:1C, FastEthernet1/0
D  2002:ACE7:2222:8::/64 [90/38400]  via FE80::C801:1FFF:FE34:1C, FastEthernet1/0
D  2002:ACE7:2222:9::/64 [90/35840]  via FE80::C801:1FFF:FE34:1C, FastEthernet1/0
    The first nine interfaces were last updated 20:47:52 28 October 2015
D   2002:ACE7:2222:C::/64 [90/30720] via FE80::C807:24FF:FED4:8, FastEthernet0/1
    Last updated 21:04:18 28 October 2015
D 2002:ACE7:2222:D::/64 [90/2172416]viaFE80::C801:1FFF:FE34:1C, FastEthernet1/0
    Last updated 20:47:52 28 October 2015
D  2002:ACE7:2222:10::/64 [90/30720]  via FE80::C807:24FF:FED4:8, FastEthernet0/1
    Last updated 21:04:07 28 October 2015
D  2002:ACE7:2222:11::/64 [90/30720] via FE80::C805:13FF:FEF4:1C, FastEthernet0/0
    Last updated 20:52:33 28 October 2015
D  2002:ACE7:2222:12::/64 [90/30720] via FE80::C805:13FF:FEF4:1C, FastEthernet0/0
    Last updated 20:52:33 28 October 2015
D  2002:ACE7:2222:13::/64 [90/33280] via FE80::C805:13FF:FEF4:1C, FastEthernet0/0
    via FE80::C807:24FF:FED4:8, FastEthernet0/1
    Last updated 21:04:09 28 October 2015
```

4.4.2.5 Ping results of EIGRPv6 on static addresses

Table 4.22 Ping results of EIGRPv6 on the static unicast addresses of multilayer switch MD

```
MD # ping 2002:ACE7:2222:0013::11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 64/104/160 ms
MD # ping 2002:ACE7:2222:0013::11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 64/80/96 ms
```

4.4.2.6 Traceroute results of EIGRPv6 on static addresses

Table 4.23 Traceroute results of EIGRPv6 on the static unicast addresses of multilayer switch MA

```
MA # traceroute ipv6 2002:ACE7:2222:0004::D
Type escape sequence to abort.
Tracing the route to 2002:ACE7:2222:4::D
1    2002:ACE7:2222:5::E    56 msec 16 msec 28 msec
2    2002:ACE7:2222:9::F    32 msec 24 msec 20 msec
3    2002:ACE7:2222:8::D    84 msec 48 msec 76 msec
```

4.4.3 Results of configuring OSPFv3 for a single area on static addresses

One router and two randomly selected multilayer switches are used to obtain the OSPFv3 results. The results are obtained using the commands, “show ipv6 route ospf updated” and “show ipv6 route ospf.” The code O stands for OSPFv3 intra-routes.

4.4.3.1 OSPFv3 results for router RA

Table 4.24 Results of configuring OSPFv3 on router RA

```
RA # show ipv6 route ospf updated
O   2002:ACE7:2222:1::/64 [110/2]      via FE80::C802:1CFF:FE64:38, FastEthernet0/0
O   2002:ACE7:2222:3::/64 [110/3]      via FE80::C802:1CFF:FE64:38, FastEthernet0/0
O   2002:ACE7:2222:4::/64 [110/2]      via FE80::C802:1CFF:FE64:38, FastEthernet0/0
O   2002:ACE7:2222:5::/64 [110/4]      via FE80::C802:1CFF:FE64:38, FastEthernet0/0
O   2002:ACE7:2222:6::/64 [110/2]      via FE80::C802:1CFF:FE64:38, FastEthernet0/0
O   2002:ACE7:2222:7::/64 [110/3]      via FE80::C802:1CFF:FE64:38, FastEthernet0/0
O   2002:ACE7:2222:8::/64 [110/4]      via FE80::C802:1CFF:FE64:38, FastEthernet0/0
O   2002:ACE7:2222:9::/64 [110/12]     via FE80::C802:1CFF:FE64:38, FastEthernet0/0
O   2002:ACE7:2222:C::/64 [110/3]      via FE80::C006:26FF:FE74:10, FastEthernet1/0
O   2002:ACE7:2222:E::/64 [110/2]      via FE80::C006:26FF:FE74:10, FastEthernet1/0
O   2002:ACE7:2222:F::/64 [110/2]      via FE80::C006:26FF:FE74:10, FastEthernet1/0
O   2002:ACE7:2222:10::/64 [110/3]     via FE80::C006:26FF:FE74:10, FastEthernet1/0
    The first twelve interfaces were last updated 20:50:15 29 October 2015
O   2002:ACE7:2222:11::/64 [110/12]   via FE80::C006:26FF:FE74:10, FastEthernet1/0
    Last updated 20:41:21 29 October 2015
O   2002:ACE7:2222:12::/64 [110/12]   via FE80::C006:26FF:FE74:10, FastEthernet1/0
    Last updated 20:41:21 29 October 2015
O   2002:ACE7:2222:13::/64 [110/13]   via FE80::C006:26FF:FE74:10, FastEthernet1/0
    Last updated 20:50:15 29 October 2015
```

4.4.3.2 OSPFv3 results for router MB

Table 4.25 Results of configuring OSPFv3 on multilayer switch MB

```
MB # show ipv6 route ospf
O   2002:ACE7:2222:3::/64 [110/2]     via FE80::C603:1CFF:FEFC:20, FastEthernet1/0
O   2002:ACE7:2222:5::/64 [110/3]     via FE80::C004:FFF:FED0:1, FastEthernet1/1
O   2002:ACE7:2222:7::/64 [110/2]     via FE80::C004:FFF:FED0:1, FastEthernet1/1
O   2002:ACE7:2222:8::/64 [110/3]     via FE80::C004:FFF:FED0:1, FastEthernet1/1
O   2002:ACE7:2222:9::/64 [110/11]    via FE80::C004:FFF:FED0:1, FastEthernet1/1
O   2002:ACE7:2222:A::/64 [110/2]     via FE80::C801:1FFF:FE34:0, FastEthernet2/0
O   2002:ACE7:2222:C::/64 [110/4]     via FE80::C801:1FFF:FE34:0, FastEthernet2/0
O   2002:ACE7:2222:D::/64 [110/65]    via FE80::C801:1FFF:FE34:0, FastEthernet2/0
O   2002:ACE7:2222:E::/64 [110/3]     via FE80::C801:1FFF:FE34:0, FastEthernet2/0
O   2002:ACE7:2222:F::/64 [110/3]     via FE80::C801:1FFF:FE34:0, FastEthernet2/0
O   2002:ACE7:2222:10::/64 [110/4]    via FE80::C801:1FFF:FE34:0, FastEthernet2/0
O   2002:ACE7:2222:11::/64 [110/13]   via FE80::C801:1FFF:FE34:0, FastEthernet2/0
O   2002:ACE7:2222:12::/64 [110/13]   via FE80::C801:1FFF:FE34:0, FastEthernet2/0
O   2002:ACE7:2222:13::/64 [110/14]   via FE80::C801:1FFF:FE34:0, FastEthernet2/0
```

4.4.3.3 OSPFv3 results for router MG

Table 4.26 Results of configuring OSPFv3 on multilayer switch MG

```
MG # show ipv6 route ospf
O   2002:ACE7:2222:1::/64 [110/4]      via FE80::C006:26FF:FE74:0, FastEthernet1/0
O   2002:ACE7:2222:2::/64 [110/3]      via FE80::C006:26FF:FE74:0, FastEthernet1/0
O   2002:ACE7:2222:3::/64 [110/5]      via FE80::C006:26FF:FE74:0, FastEthernet1/0
O   2002:ACE7:2222:4::/64 [110/4]      via FE80::C006:26FF:FE74:0, FastEthernet1/0
O   2002:ACE7:2222:5::/64 [110/6]      via FE80::C006:26FF:FE74:0, FastEthernet1/0
O   2002:ACE7:2222:6::/64 [110/4]      via FE80::C006:26FF:FE74:0, FastEthernet1/0
O   2002:ACE7:2222:7::/64 [110/5]      via FE80::C006:26FF:FE74:0, FastEthernet1/0
O   2002:ACE7:2222:8::/64 [110/6]      via FE80::C006:26FF:FE74:0, FastEthernet1/0
O   2002:ACE7:2222:9::/64 [110/14]     via FE80::C006:26FF:FE74:0, FastEthernet1/0
O   2002:ACE7:2222:A::/64 [110/2]      via FE80::C006:26FF:FE74:0, FastEthernet1/0
O   2002:ACE7:2222:C::/64 [110/3]      via FE80::C006:26FF:FE74:0, FastEthernet1/0
O   2002:ACE7:2222:D::/64 [110/66]     via FE80::C006:26FF:FE74:0, FastEthernet1/0
O   2002:ACE7:2222:E::/64 [110/2]      via FE80::C006:26FF:FE74:0, FastEthernet1/0
O   2002:ACE7:2222:10::/64 [110/3]     via FE80::C006:26FF:FE74:0, FastEthernet1/0
O   2002:ACE7:2222:13::/64 [110/13]    via FE80::C006:26FF:FE74:0, FastEthernet1/0
```

4.4.3.4 Ping results of OSPFv3 on static IPv6 addresses

Table 4.27 Ping results of OSPFv3 on static IPv6 addresses

```
MD # ping 2002:ACE7:2222:0013::11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 80/95/104 ms
MD # ping 2002:ACE7:2222:0013::11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 88/96/108 ms
```

4.4.3.5 Traceroute results of OSPFv3 on static IPv6 addresses

Table 4.28 Traceroute results of OSPFv3 on static IPv6 addresses

```
MA # traceroute ipv6 2002:ACE7:2222:0004::D
Type escape sequence to abort.
Tracing the route to 2002:ACE7:2222:4::D
1    2002:ACE7:2222:5::E    12 msec 4 msec 28 msec
2    2002:ACE7:2222:9::F    36 msec 24 msec 52 msec
3    2002:ACE7:2222:8::D    68 msec 52 msec 48 msec
```

4.4.4 Results of RIPng, EIGRPv6 and OSPFv3 on SLAAC IPv6 addresses

When the show ipv6 route, show ipv6 route rip, show ipv6 route eigrp and show ipv6 route ospf commands are executed on all the multilayer switches and the router, no IPv6 results (routes) of RIPng, EIGRPv6 and OSPFv3 are obtained for SLAAC addresses.

4.5 RESULTS OF RIPNG, EIGRPV6 AND OSPFV3 ON EUI-64 ADDRESSES

The following results are obtained on multilayer switch MD using the traceroute and ping commands.

4.5.1 Ping results

4.5.1.1 RIPng ping results on EUI-64 addresses

Table 4.29 Ping results for RIPng on EUI-64 addresses

```
MA # ping 2002:ACE7:2222:4:C807:7FF:FEC8:1C
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:ACE7:2222:4:C807:7FF:FEC8:1C, timeout is
2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 28/53/64 ms
MA # ping 2002:ACE7:2222:4:C807:7FF:FEC8:1C
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:ACE7:2222:4:C807:7FF:FEC8:1C, timeout is
2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 44/60/84 ms
```

4.5.1.2 EIGRPv6 ping results on EUI-64 addresses

Table 4.30 Ping results of EIGRPv6 on EUI-64 addresses

```
MA # ping 2002:ACE7:2222:4:C807:7FF:FEC8:1C
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:ACE7:2222:4:C807:7FF:FEC8:1C, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 32/92/216 ms
MA # ping 2002:ACE7:2222:4:C807:7FF:FEC8:1C
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:ACE7:2222:4:C807:7FF:FEC8:1C, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 36/57/88 ms
```

4.5.1.3 OSPFv3 ping results on EUI-64 addresses

Table 4.31 Ping results of OSPFv3 on EUI-64 addresses

```
MA # ping 2002:ACE7:2222:4:C807:7FF:FEC8:1C
Sending 5, 100-byte ICMP echos to 2002:ACE7:2222:4:C807:7FF:FEC8:1C, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 56/92/212 ms
MA # ping 2002:ACE7:2222:4:C807:7FF:FEC8:1C
Sending 5, 100-byte ICMP echos to 2002:ACE7:2222:4:C807:7FF:FEC8:1C, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 36/69/128 ms
```

4.5.2 Traceroute results

4.5.2.1 RIPng traceroute results on EUI-64 addresses

Table 4.32 Traceroute results of RIPng on EUI-64 addresses

```
MA # traceroute ipv6 2002:ACE7:2222:4:C807:7FF:FEC8:1C

Type escape sequence to abort.

Tracing the route to 2002:ACE7:2222:4:C807:7FF:FEC8:1C

1    2002:ACE7:2222:5:C803:25FF:FE68:6     40 msec 12 msec 28 msec

2    2002:ACE7:2222:9:C804:CFF:FE70:39    40 msec 32 msec 16 msec

3    2002:ACE7:2222:8:C807:7FF:FEC8:0      52 msec 44 msec 44 msec
```

4.5.2.2 EIGRPv6 traceroute results on EUI-64 addresses

Table 4.33 Traceroute results of EIGRPv6 on EUI-64 addresses

```
MA # traceroute ipv6 2002:ACE7:2222:4:C807:7FF:FEC8:1C

Type escape sequence to abort.

Tracing the route to 2002:ACE7:2222:4:C807:7FF:FEC8:1C

1    2002:ACE7:2222:5:C803:25FF:FE68:6     52 msec 0 msec 0 msec

2    2002:ACE7:2222:9:C804:CFF:FE70:39    76 msec 44 msec 20 msec

3    2002:ACE7:2222:8:C807:7FF:FEC8:8      44 msec 40 msec 40 msec
```

4.5.2.3 OSPFv3 traceroute results on EUI-64 addresses

Table 4.34 Traceroute results of OSPFv3 on EUI-64 addresses

```
MA # traceroute ipv6 2002:ACE7:2222:4:C807:7FF:FEC8:1C

Type escape sequence to abort.

Tracing the route to 2002:ACE7:2222:4:C807:7FF:FEC8:1C

1    2002:ACE7:2222:5:C803:25FF:FE68:6      44 msec 48 msec 20 msec

2    2002:ACE7:2222:A:C802:26FF:FEA4:38     68 msec 8 msec 52 msec

3    2002:ACE7:2222:D:C804:CFF:FE70:8       64 msec 48 msec 60 msec

4    2002:ACE7:2222:8:C807:7FF:FEC8:8       88 msec 88 msec 68 msec
```

4.6 RESULTS OF CONFIGURING IPV6 TRANSITION TECHNIQUES ON DYNAMIC ROUTING PROTOCOLS

This section shows the results of configuring dual stack on RIP, RIPng, EIGRP, EIGRPv6, OSPF and OSPFv3 routing protocols. It also shows the results of configuring manual IPv6, ISATAP and GRE tunnelling transition techniques on OSPFv3, EIGRPv6 and RIPng routing protocols. All the results in this section are obtained from an IPv6 industrial communication ring network topology. The IPv4 ping and traceroute results of dual stack on RIP, EIGRP and OSPF are shown first. This is followed by the IPv6 traceroute and ping results of dual stack on OSPFv3, RIPng and EIGRPv6. Furthermore, the ping and traceroute results of manual IPv6 tunnelling on RIPng, OSPFv3 and EIGRPv6 are shown next. The last results shown in this section are the traceroute and ping results of GRE and ISATAP tunnelling on RIPng, EIGRPv6 and OSPv3. All the IPv6 and IPv4 ping results are obtained in the same duration timeout of 2 seconds. The most important thing to note in these results are the success rate and round-trip time of the ping and traceroute commands.

4.6.1 Ping and traceroute results for dual stack

4.6.1.1 IPv4 ping results of dual stack on OSPF

Table 4.35 IPv4 ping results of dual stack on OSPF

```
ME # ping 172.16.18.3 timeout 2
Type escape sequence to abort.
Sending 5, 100-byte ICMP echos to 172.16.18.3, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 80/102/140 ms
ME # ping 172.16.18.3 timeout 2
Type escape sequence to abort.
Sending 5, 100-byte ICMP echos to 172.16.18.3, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 68/88/116 ms
```

4.6.1.2 IPv4 ping results of dual stack on RIP

Table 4.36 IPv4 ping results of dual stack on RIP

```
ME # ping 172.16.18.3 timeout 2
Type escape sequence to abort.
Sending 5, 100-byte ICMP echos to 172.16.18.3, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 84/94/116 ms
ME # ping 172.16.18.3 timeout 2
Sending 5, 100-byte ICMP echos to 172.16.18.3, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 76/97/124 ms
```

4.6.1.2 IPv4 ping results of dual stack on EIGRP

Table 4.37 IPv4 ping results of dual stack on EIGRP

```
MD # ping 172.16.18.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP echos to 172.16.18.3, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 72/114/212 ms
MD # ping 172.16.18.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP echos to 172.16.18.3, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 60/107/208 ms
```

4.6.1.3 IPv4 traceroute results of dual stack on OSPF

Table 4.38 IPv4 traceroute results of dual stack on OSPF

```
MD # traceroute 172.16.18.3
Type escape sequence to abort.
Tracing the route to 172.16.18.3
1   172.16.5.2    32 msec 20 msec 20 msec
2   172.16.3.1    36 msec 28 msec 36 msec
3   172.16.1.2    52 msec 60 msec 48 msec
4   172.16.10.1   68 msec 64 msec 52 msec
5   172.16.12.4   72 msec 80 msec 84 msec
6   172.16.15.3   108 msec *  80 msec
```

4.6.1.4 IPv4 traceroute results of dual stack on RIP

Table 4.39 IPv4 traceroute results of dual stack on RIP

```
MD # traceroute 172.16.18.3

Type escape sequence to abort.

Tracing the route to 172.16.18.3

1   172.16.7.4    20 msec

    172.16.5.2    40 msec

    172.16.7.4    12 msec

2   172.16.3.1    108 msec

    172.16.6.1    48 msec

    172.16.3.1    56 msec

3   172.16.1.2    84 msec 24 msec 56 msec

4   172.16.10.1   72 msec 52 msec 52 msec

5   172.16.12.4   60 msec 60 msec 76 msec

6   172.16.1.2    84 msec 24 msec 56 msec

7   172.16.10.1   72 msec 52 msec 52 msec

8   172.16.12.4   60 msec 60 msec 76 msec

9   172.16.15.3   128 msec *  76 msec
```

4.6.1.5 IPv4 traceroute results of dual stack on EIGRP

Table 4.40 IPv4 traceroute results of dual stack on EIGRP

```
MD # traceroute 172.16.18.3

Type escape sequence to abort.

Tracing the route to 172.16.18.3

1   172.16.5.3    84 msec

    172.16.7.4    72 msec

    172.16.5.3    48 msec

2   172.16.6.1    84 msec

    172.16.3.1    76 msec

    172.16.6.1    124 msec

3   172.16.1.2    96 msec 188 msec 252 msec

4   172.16.10.1   232 msec 204 msec 260 msec

5   172.16.12.6   356 msec 332 msec 340 msec

6   172.16.15.3   328 msec 376 msec *
```

4.6.1.6 IPv6 ping results of dual stack on OSPFv3

Table 4.41 IPv6 ping results of dual stack on OSPFv3

```
MD # ping 2002:ACE7:2222:0013::11

Sending 5, 100-byte ICMP echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:

!!!!!

Success rate is 100% (5/5), round-trip min/avg/max = 232/280/368 ms

MD # ping 2002:ACE7:2222:0013::11

Sending 5, 100-byte ICMP echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:

!!!!!

Success rate is 100% (5/5), round-trip min/avg/max = 264/292/368 ms
```

4.6.1.7 IPv6 ping results of dual stack on RIPng

Table 4.42 IPv6 ping results of dual stack on RIPng

```
MD # ping 2002:ACE7:2222:0013::11

Type escape sequence to abort.

Sending 5, 100-byte ICMP echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:

!!!!!

Success rate is 100% (5/5), round-trip min/avg/max = 68/88/148 ms

MD # ping 2002:ACE7:2222:0013::11

Type escape sequence to abort.

Sending 5, 100-byte ICMP echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:

!!!!!

Success rate is 100% (5/5), round-trip min/avg/max = 68/87/100 ms
```

4.6.1.8 IPv6 ping results of dual stack on EIGRPv6

Table 4.43 IPv6 ping results of dual stack on EIGRPv6

```
MD # ping 2002:ace7:2222:0011::11

Type escape sequence to abort.

Sending 5, 100-byte ICMP 3chos to 2002:ACE7:2222:13::11, timeout is 2 seconds:

!!!!!

Success rate is 100% (5/5), round-trip min/avg/max = 352/538/712 ms

MD # ping 2002:ace7:2222:0011::11

Type escape sequence to abort.

Sending 5, 100-byte ICMP echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:

!!!!!

Success rate is 100% (5/5), round-trip min/avg/max = 448/519/604 ms
```

4.6.1.9 IPv6 traceroute results of dual stack on OSPFv3

Table 4.44 IPv6 traceroute results of dual stack on OSPFv3

```
MD # traceroute 2002:ACE7:2222:0013::11

Tracing the route to 2002:ACE7:2222:13::11

1    2002:ACE7:2222:5::C      136 msec 68 msec 68 msec

2    2002:ACE7:2222:4::B      140 msec 104 msec 132 msec

3    2002:ACE7:2222:2::A      172 msec 140 msec 168 msec

4    2002:ACE7:2222:A::F      240 msec 236 msec 140 msec

5    2002:ACE7:2222:E::12     264 msec 316 msec 276 msec

6    2002:ACE7:2222:13::11   308 msec 272 msec 276 msec
```

4.6.1.10 IPv6 traceroute results of dual stack on RIPng

Table 4.45 IPv6 traceroute results of dual stack on RIPng

```
MD # traceroute 2002:ACE7:2222:0013::11

Tracing the route to 2002:ACE7:2222:13::11

1    2002:ACE7:2222:7::E     12 msec

     2002:ACE7:2222:5::C     16 msec

     2002:ACE7:2222:7::E     20 msec

2    2002:ACE7:2222:4::B     20 msec

     2002:ACE7:2222:6::B     40 msec

3    2002:ACE7:2222:2::A     56 msec 44 msec 56 msec

4    2002:ACE7:2222:A::F     68 msec 36 msec 52 msec

5    2002:ACE7:2222:F::10    76 msec

     2002:ACE7:2222:E::12    68 msec

     2002:ACE7:2222:F::10    68 msec

6    2002:ACE7:2222:13::11  64 msec 92 msec 52 msec
```

4.6.1.11 IPv6 traceroute results of dual stack on EIGRPv6

Table 4.46 IPv6 traceroute results of dual stack on EIGRPv6

```
MH # traceroute 2002:ACE7:2222:0013::11
Tracing the route to 2002:ACE7:2222:7::D
1   2002:ACE7:2222:11::10    16 msec
    2002:ACE7:2222:10::12    160 msec
    2002:ACE7:2222:11::10    56 msec
2   2002:ACE7:2222:E::F      160 msec
    2002:ACE7:2222:F::F      140 msec
    2002:ACE7:2222:E::F      184 msec
3   2002:ACE7:2222:A::A      276 msec 228 msec 164 msec
4   2002:ACE7:2222:2::B      312 msec 296 msec 244 msec
5   2002:ACE7:2222:6::E      460 msec 204 msec 416 msec
6   2002:ACE7:2222:7::D      552 msec 448 msec 544 msec
```

4.6.2 Ping and traceroute results for manual IPv6 tunnelling

4.6.2.1 Ping results of manual IPv6 on RIPng

Table 4.47 Ping results of manual IPv6 on RIPng

```
MD # ping 2002:ACE7:2222:0013::11
Sending 5, 100-byte ICMP echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 644/812/992 ms
MD # ping 2002:ACE7:2222:0013::11
Sending 5, 100-byte ICMP echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 744/879/1056 ms
```

4.6.2.2 Ping results of manual IPv6 on OSPFv3

Table 4.48 Ping results of manual IPv6 on OSPFv3

```
MD # ping 2002:ACE7:2222:0013::11
Type escape sequence to abort.
Sending 5, 100-byte ICMP echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 676/746/808 ms
MD # ping 2002:ACE7:2222:0013::11
Type escape sequence to abort.
Sending 5, 100-byte ICMP echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 468/603/672 ms
```

4.6.2.3 Ping results of manual IPv6 on EIGRPv6

Table 4.49 Ping results of manual IPv6 on EIGRPv6

```
MD # ping 2002:ACE7:2222:13::11
Type escape sequence to abort.
Sending 5, 100-byte ICMP echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 812/1104/1800 ms
MD # ping 2002:ace7:2222:13::11
Type escape sequence to abort.
Sending 5, 100-byte ICMP echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 864/1013/1468 ms
```

4.6.2.4 Traceroute results of manual IPv6 on RIPng

Table 4.50 Traceroute results of manual IPv6 on RIPng

```
MD # traceroute ipv6 2002:ACE7:2222:0013::11

Type escape sequence to abort.

Tracing the route to 2002:ACE7:2222:13::11

1    2002:ACE7:2222:5::C      84 msec

     2002:ACE7:2222:7::E      132 msec

     2002:ACE7:2222:5::C      80 msec

2    2002:ACE7:2222:6::B      216 msec

     2002:ACE7:2222:4::B      212 msec

     2002:ACE7:2222:6::B      212 msec

3    2002:ACE7:2222:2::A      360 msec 304 msec 448 msec

4    2002:ACE7:2222:14::2     356 msec 500 msec 356 msec

5    2002:ACE7:2222:A::F      644 msec 720 msec 640 msec

6    2002:ACE7:2222:F::10     572 msec

     2002:ACE7:2222:E::12    644 msec

     2002:ACE7:2222:F::10    792 msec

7    2002:ACE7:2222:13::11   1016 msec 732 msec 712 msec
```

4.6.2.5 Traceroute results of manual IPv6 on OSPFv3

Table 4.51 Traceroute results of manual IPv6 on OSPFv3

```
 MD # traceroute 2002:ACE7:2222:0013::11

Tracing the route to 2002:ACE7:2222:13::11

1        2002:ACE7:2222:5::C      292 msec 200 msec 204 msec

2        2002:ACE7:2222:4::B      308 msec 296 msec 204 msec

3        2002:ACE7:2222:2::A      412 msec 196 msec 308 msec

4        2002:ACE7:2222:14::2     404 msec 540 msec 652 msec

5        2002:ACE7:2222:A::F      536 msec 668 msec 508 msec

6        2002:ACE7:2222:E::12     804 msec 812 msec 500 msec

7        2002:ACE7:2222:13::11   604 msec 604 msec 720 msec
```

4.6.2.6 Traceroute results of manual IPv6 on EIGRPv6

Table 4.52 Traceroute results of manual IPv6 on EIGRPv6

```
MD # traceroute 2002:ACE7:2222:0013::11

Tracing the route to 2002:ACE7:2222:13::11

1    2002:ACE7:2222:7::E      1260 msec

     2002:ACE7:2222:5::C      168 msec

     2002:ACE7:2222:7::E      208 msec

2    2002:ACE7:2222:4::B      312 msec

     2002:ACE7:2222:4::B      284 msec

3    2002:ACE7:2222:2::A      320 msec 480 msec 440 msec

4    2002:ACE7:2222:14::2     600 msec 504 msec 584 msec

5    2002:ACE7:2222:A::F      540 msec 620 msec 520 msec

6    2002:ACE7:2222:E::12     732 msec 792 msec 816 msec

7    2002:ACE7:2222:10::11   740 msec 892 msec 828 msec
```

4.6.3 Ping and traceroute results for GRE tunnelling

Ping and traceroute results for the GRE tunnelling technique are obtained on multilayer switch MD.

4.6.3.1 Ping results of GRE tunnelling on RIPng

Table 4.53 Ping results of GRE tunnelling on RIPng

```
MD # ping 2002:ACE7:2222:0013::11 timeout 2
Type escape sequence to abort.
Sending 5, 100-byte ICMP echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 672/822/964 ms
MD # ping 2002:ACE7:2222:0013::11 timeout 2
Type escape sequence to abort.
Sending 5, 100-byte ICMP echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 788/900/988 ms
```

4.6.3.2 Ping results of GRE tunnelling on OSPFv3

Table 4.54 Ping results of GRE tunnelling on OSPFv3

```
MD # ping 2002:ACE7:2222:0013::11
Sending 5, 100-byte ICMP Echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 792/922/1052 ms
MD # ping 2002:ACE7:2222:0013::11
Sending 5, 100-byte ICMP Echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 784/912/988 ms
```

4.6.3.3 Ping results of GRE tunnelling on EIGRPv6

Table 4.55 Ping results of GRE tunnelling on EIGRPv6

```
MD # ping 2002:ACE7:2222:0013::11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 344/456/576 ms
MD # ping 2002:ACE7:2222:0013::11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5), round-trip min/avg/max = 252/399/484 ms
```

4.6.3.4 Traceroute results of GRE tunnelling on EIGRPv6

Table 4.56 Traceroute results of GRE tunnelling on EIGRPv6

```
MD # traceroute 2002:ACE7:2222:0013::11
Tracing the route to 2002:ACE7:2222:13::11
1     2002:ACE7:2222:7::E      68 msec
      2002:ACE7:2222:5::C      112 msec
      2002:ACE7:2222:7::E      36 msec
2     2002:ACE7:2222:4::B      192 msec
      2002:ACE7:2222:6::B      120 msec
3     2002:ACE7:2222:2::A      76 msec 192 msec 160 msec
4     2002:ACE7:2222:14::2     156 msec 152 msec 112 msec
5     2002:ACE7:2222:A::F      156 msec 148 msec 248 msec
6     2002:ACE7:2222:F::10     160 msec 244 msec 188 msec
7     2002:ACE7:2222:11::11    156 msec 312 msec 156 msec
```

4.6.3.5 Traceroute results of GRE tunnelling on RIPng

Table 4.57 Traceroute results of GRE tunnelling on RIPng

```
MD # traceroute ipv6 2002:ACE7:2222:0013::11

Tracing the route to 2002:ACE7:2222:13::11

1        2002:ACE7:2222:7::E       80 msec

         2002:ACE7:2222:5::C       192 msec

         2002:ACE7:2222:7::E       196 msec

2        2002:ACE7:2222:4::B       388 msec

         2002:ACE7:2222:6::B       292 msec

        2002:ACE7:2222:4::B        292 msec

3       2002:ACE7:2222:2::A        392 msec 488 msec 328 msec

4       2002:ACE7:2222:14::2       648 msec 604 msec 580 msec

5       2002:ACE7:2222:A::F        672 msec 676 msec 576 msec

6       2002:ACE7:2222:E::12       772 msec

        2002:ACE7:2222:F::10       680 msec

        2002:ACE7:2222:E::12       868 msec

7       2002:ACE7:2222:13::11      944 msec 808 msec 868 msec
```

4.6.4 Ping and traceroute results for ISATAP tunnelling

4.6.4.1 Ping results of ISATAP on RIPng, EIGRP and OSPFv3

Table 4.58 Ping results of ISATAP on RIPng, EIGRP and OSPFv3

```
MD # ping 2002:ACE7:2222:0013::11

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2002:ACE7:2222:13::11, timeout is 2 seconds:

.....

Success rate is 0% (0/5)
```

4.6.4.2 Traceroute results of ISATAP on OSPFv3 EIGRPv6 and OSPFv3

Table 4.59 Traceroute results of ISATAP on OSPFv3, EIGRPv6 and OSPFv3

```
MD # traceroute ipv6 2002:ACE7:2222:0013::11
Type escape sequence to abort.
Tracing the route to 2002:ACE7:2222:13::11
  1  *  *  *
  2  *  *  *
  3  *  *  *
  4 *   *   *
  5 *  *   *
  ………..
  ………..
  ………..
  ………..
  ………..
  ………..
  ………..
28  *  *  *
29  *  *  *
30  *  *  *
Destination not found inside max hop count diameter.
```

4.6.4.3 Traceroute and ping results of NAT-PT on RIPng, EIGRPv6 and OSPFv3

Just like ISATAP, the ping and traceroute results of NAT-PT on RIPng, EIGRPv6 and OSPFv3 are not successful.

4.7 PING RESULTS OF HSRPV2 ON RIPNG, EIGRPV6 AND OSPFV3

The following HSRPv2 results are obtained using the ping command for IPv6 with a repeat count of 50.

4.7.1 HSRPv2 ping results on OSPFv3

Table 4.60 HSRPv2 ping results on OSPFv3

```
ME # ping 2002:ACE7:2222:11:C809:14FF:FE18:0 repeat 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2002:ACE7:2222:11:C809:14FF:FE18:0, timeout
is 2 seconds:
!!!!!!!!!!!!...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 94% (47/50), round-trip min/avg/max = 64/198/308 ms
```

4.7.2 HSRPv2 ping results on EIGRPv6

Table 4.61 HSRPv2 ping results on EIGRPv6

```
ME # ping 2002:ACE7:2222:11:C809:14FF:FE18:0 repeat 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2002:ACE7:2222:11:C809:14FF:FE18:0, timeout
is 2 seconds:
!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 98% (49/50), round-trip min/avg/max = 72/203/380 ms
```

4.7.3 HSRPv2 ping results on RIPng

Table 4.62 HSRPv2 ping results on RIPng

```
ME # ping 2002:ACE7:2222:11:C809:14FF:FE18:0 repeat 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2002:ACE7:2222:11:C809:14FF:FE18:0, timeout is  2 seconds:
!!!!!!!!!!!!.UUUUUUUUUUUUU
% No valid route for destination
Success rate is 44% (12/27), round-trip min/avg/max = 164/269/664 ms
```

CHAPTER 5 DISCUSSION ON THE IPV6 LAYER 3 CONFIGURATION RESULTS

5.1 INTRODUCTION

This chapter discusses the results of configuring IPv6 layer 3 commands on industrial communication routers and multilayer switches. The discussion covers the benefits and challenges of using layer 3 configuration commands for IPv6 addresses, HSRPv2, RIPng, EIGRPv6 and OSPFv3. In addition, benefits and challenges of using dual stack, manual IPv6, GRE and ISATAP commands are discussed as well. Since network topologies affect the operation of routers and multilayer switches, this chapter also looks at the benefits and challenges of using a ring and hierarchical network topology in industrial communication networks. Other elements discussed include the RTT and traceroute results for static routing, RIPng, EIGRPv6, OSPFv3, HSRPv2 and IPv6 transition techniques. The results shown for the RTT and traceroute are for the first ping and traceroute commands done on multilayer switch MD. These results are obtained after the networks have fully converged, that is, when best routes have already been determined by routers and multilayer switches. In the context of Figure 3.2, the RTT is the time it takes for a packet to travel from one end of the network to the other, that is, from multilayer switch MD to MH and back again. Most industrial communication networks require a shorter RTT for efficient processing, control and supervision of products and network services.

5.2 COMMANDS FOR CONFIGURING IPV6 ADDRESSES

This section discusses the challenges and benefits of using configuration commands for static unicast and dynamic addresses on routers and multilayer switches. Both the manual method of configuring the entire 128 bit address and the autoconfiguration method of using the EUI-64 format are discussed. Whereas the 128 bit method enables network engineers to configure the whole IPv6 address manually, the EUI-64 method enables them to configure only the first 64 bits of the address and allows the router or multilayer switch to create the remaining 64 bits of the address automatically.

5.2.1 Static unicast IPv6 address configuration command

As can be seen in Section 3.3.1, the process of configuring static unicast IPv6 addresses on multilayer switches or routers such as router RA requires the static address command of ipv6 address 2002:ACE7:2222:0002::A/64. This command is more complicated than the IPv4 address command of ip address 172.16.1.1/24. This is because of the hexadecimal complex nature of IPv6 addresses. This complexity makes the static configuration of IPv6 addresses a very challenging task to network engineers in large industrial networks. Manual configuration of many interfaces results in network errors. Furthermore, when these interfaces are configured with wrong IPv6 addresses, they still accept the addresses, but position them in wrong networks. Thus, with static unicast address configuration commands, the chances of misconfiguring IPv6 addresses are very high, which may lead to routing and troubleshooting challenges in industrial communication networks. Another notable challenge of configuring static addresses involves the possibility of forgetting to configure the ipv6 unicast routing command. Unlike IPv4 routing, IPv6 routing is not enabled by default in Cisco routers and multilayer switches. One of the challenges experienced in the configuration process of multilayer switch MB, ME and MH shows that when the routing command is not enabled, these switches act just like ordinary IPv6 hosts. Consenquently, the configured IPv6 addresses are unable to route the IPv6 packets. Therefore, in all IPv6 layer 3 configurations, network engineers should remember to configure the ipv6 unicast routing command in the networks and should also ensure that correct static unicast addresses are configured on the interfaces.

Despite the above challenges, one of the outstanding benefits of the static unicast ipv6 address command is the ability to use slash notation such as /64 or /48 for the prefix length. This is not possible with IPv4 address commands, which requires the subnet mask (prefix length) to be typed in dotted decimal format, such as 255.255.255.0 or 255.255.240.0. With the usage of slash notation, it is not easy to mistype the prefix length of the address and most industrial communication engineers should find this feature very helpful and easy to use when configuring and troubleshooting IPv6 networks.

5.2.2 EUI-64 IPv6 address configuration command

The extended unique identifier-64 (EUI-64) is a useful feature of industrial communication routers and multilayers switches. As can be observed from Section 3.7.8.1, the command ipv6 address 2002:ACE7:2222:000B::/64 eui-64, allowed router RG to configure its own 64 bits of the IPv6 address. This is a huge benefit because it removes the need for the manual configuration of the last 64 bits (interface ID) of addresses for routers, multilayer switches and DHCP servers in industrial communication networks. DHCP servers are among the primary sources of network failure in most of the networks. When these servers are down, all the devices that dynamically get their IP addresses from them are affected; subsequently leading to failure of the entire network. Therefore, one benefit of the EUI-64 address configuration command is the ability of servers to autoconfigure their own interface ID. This feature greatly minimises the human errors associated with the manual configuration of interface identifiers on DCHPv6 servers. As a result of this address autoconfiguration, routers, servers and switches have longer up time and are more stable.

In spite of the above benefit, the EUI-64 method has some challenges as well. As experienced under Section 3.7.8, this method accepts any prefix length configured on the interfaces. Consequently, if a wrong prefix length is configured, the router or multilayer switch uses it to configure its interface ID. This positions the interface in a wrong subnetwork and results in routing challenges. On the other hand, if the network engineer forgets to type the phrase EUI-64 at the end of the configured IPv6 address command, the routers and multilayer switches simply configure it as a static address, adding zeroes to the interface ID component. Ultimately this misconfiguration also results in routing challenges because packets are not routed to the intended interfaces or destinations. Furthermore, as can be observed in Section 4.4, EUI-64 configured addresses are not easy to retype either. These addresses are long and complicated, just like the 128 bit static unicast addresses. Hence when reconfiguring them on other router interfaces, the best network engineers can do is simply to copy and paste rather than retype them. This significantly reduces typing errors and misconfiguration challenges.

5.3 COMMANDS FOR CONFIGURING RIPNG, EIGRPV6 AND OSPFV3 ROUTING PROTOCOLS

This section examines the challenges and benefits of using IPv6 interior routing protocol commands for RIPng, EIGRPv6 and OSPFv3. These three interior routing protocols play a very important role in the routing of packets in industrial communication networks. Without them, routers and multilayers switches cannot dynamically learn IPv6 routes.

5.3.1 RIPng configuration commands

As can be observed in Section 3.4.2.1, configuring of RIPng on router RA and all multilayer switches requires three commands. On all these devices, the ipv6 unicast routing, ipv6 router rip benji and ipv6 rip benji enable commands are used to configure RIPng successfully. Unlike IPv4 routing, which is enabled by default on all routers and multilayer switches, the experience of configuring RIPng shows that IPv6 routing is not enabled by default on these devices. Thus one of the challenges network engineers may face as they transition RIP networks to RIPng is not enabling IPv6 routing through the ipv6 unicast routing command. Without configuring this command, no RIPng routing takes place on routers and multilayer switches. This leads to a breakdown in communication among different devices in different subnetworks or VLANs of industrial communication networks.

The other challenge for RIPng involves configuring different rip names on different routers and multilayer switches. While it is true that different names can still be used, they make it difficult to troubleshoot RIPng routing problems in very large networks. It is for this reason that the same name of benji is used in all RIPng configurations of Chapter 3. This name, which is formally called a tag, is very useful in the RIPng process of each router or multilayer switch. Although this tag has no effect on the exchange of routing information, configuring the ipv6 router rip name and ipv6 rip name enable commands with different names prevents RIPng from starting. However, if the network engineer forgets to configure the ipv6 router rip name global command, the ipv6 rip name enable subinterface command automatically configures it as well. This is benefial because it makes the configuration process of RIPng faster and easier by using just one command. The above challenges are good troubleshooting points when RIPng is not working properly in industrial communication networks. For instance, if RIPng routes have not been discovered on the networks, checking whether the same name is configured on both ipv6 router rip name and ipv6 rip name enable commands is very beneficial.

In contrast to RIP, another benefit of RIPng is that it does not require the network command and wildcard masks to configure interfaces that need to participate in the RIPng process. Instead RIPng is enabled on each interface by only using the ipv6 rip name enable subcommand. This makes it easy to include and exclude interfaces in the RIPng process. Undoubtedly, enabling of RIPng on router interfaces using this command rather than the complicated network command and the difficult-to-calculate wildcard masks makes the configuration of RIPng much easier.

5.3.2 EIGRPv6 configuration commands

In order to configure EIGRPv6 successfully, four configuration commands are needed. As illustrated in Section 3.4.2.2, these commands include ipv6 unicast routing, ipv6 router eigrp asn, ipv6 eigrp asn and the no shutdown command. The configuration experience of using these commands reveals the following challenges: Just like RIPng and OSPFv3, failure to configure the ipv6 unicast routing command on routers and multilayer switches prevents EIGRPv6 routing from working. This is because in the absence of this command, layer 3 devices behave like ordinary IPv6 hosts, totally stripped of any routing capabilities. It is therefore important not to forget to configure this command on routers and multilayer switches when transitioning EIGRP networks to EIGRPv6. The other configuration challenge for EIGRPv6 commands involves the misconfiguration of autonomous system numbers (ASN). Configuring different ASN on routers and multilayer switches prevents the formation of EIGRPv6 neighbour relationships and results in routing challenges.

In contrast to EIGRP, which does not require the “no shutdown” command for its operation, failure to configure this command on EIGRPv6 prevents the process from starting. As a consenquence, no neighbour relationships and exchange of routing updates take place among routers or multilayer switches. Similar to the challenge of not configuring the “no shutdown” command is the router id challenge. In IPv4 industrial communication networks, if the router id command is not explicitly configured, the router or multilayer switch automatically picks the highest IPv4 address on loopback or non-loopback interfaces as its router id. As for IPv6 industrial communication networks with no IPv4 addresses, forgetting to configure the router id command prevents the EIGRPv6 process from starting. Thus, at all times in the configuration process of EIGRPv6, the 32 bit router ID must be explicitly configured as shown in Section 3.4.2.2.

Despite the above challenges, EIGRPv6 commands have very good features as well. Most of these are very beneficial to the design of IPv6 industrial communication networks. One of these features is that routers or multilayer switches do not require to be in the same IPv6 subnet as a prerequisite to forming neighbour relationships. As a result the process of exchanging route updates is fast, and the routes converge even faster after changes in network topology. The other benefit is that even if the router IDs are configured the same on all routers and multilayer switches, the EIGRPv6 process still works well, which is not the case for OSPFv3. Furthermore, the use of a 32 bit address instead of a 128 bit address for the router-id has the benefit of simplifying the process of exchanging EIGRPv6 updates. Using a 128 bit address complicates the route exchange process and makes the reading and interpretation of EIGRPv6 topology tables difficult.

5.3.3 OSPFv3 configuration commands

As explained in Section 3.4.2.3, the process of configuring OSPFv3 requires three commands. The first one is ipv6 router ospf process-id, while the second is router-id id-value and the third is ipv6 ospf process-id area number. Just like RIPng and EIGRPv6, the ipv6 unicast routing global command must be configured as well. In the configuration process of Figure 3.2, it is observed that when the router-id command is not configured, the OSPFv3 process fails to establish neighbour relationships among routers and multilayer switches. As a result of this misconfiguration, communication among devices in different networks is broken. Given the importance of this command in OSPFv3 networks, most operational challenges emanate from not configuring it. For this reason, soon after enabling OSPFv3 globally on the routers, the next step should be the configuration of the router-id command.

Another challenge for OSPFv3 involves configuring the same router-id on different routers and multilayer switches. This has the effect of preventing the OSPFv3 process from starting and results in routing challenges. Thus, in order to have different unique router IDs, the ospf process-id of each router or multilayer switch should match the router-IDs. For instance, router RA has the ospfv3 process-id 10; therefore its router-ID is 10.10.10.10. This practice makes it easier to configure different router-IDs and is of great benefit when troubleshooting many OSPFv3 areas. An additional and very useful benefit of OSPFv3 is the use of a 32 bit address in the router-id command. Instead of using a 128 bit address, a 32 bit address makes the process of configuring the router-id less complex, as shown on multilayer switch MG, whose router-id is 16.16.16.16. Typing and configuring a decimal router-id is far easier than a hexadecimal address such as 2002:ACE7:2333:44DC:A107:ABEF:123B:A2B9. Using the 32 bit address as the router-id makes the process of configuring OSPFv3 easier for industrial communication engineers. Furthermore, unlike OSPF, configuring the OSPFv3 process on selected interfaces using an interface subcommand is a huge benefit. This is because this method avoids the usage of cumbersome wildcard masks to exclude and include interfaces in the OSPFv3 process.

5.4 VERIFICATION AND TROUBLESHOOTING COMMANDS FOR IPV6 ADDRESSES, RIPNG, EIGRPV6 AND OSPFV3

This section discusses the commands shown in sections 4.2, 4.3 and 4.4. These commands are very useful in verifying and troubleshooting configurations in routers and multilayer switches. Although there are many IPv6 layer 3 verification commands, the most useful and notable ones include: show ipv6 interface brief, show ipv6 route connected updated, show ipv6 route static, show ipv6 route rip, show ipv6 route eigrp, show ipv6 route eigrp updated, show ipv6 route ospf updated, show ipv6 route ospf and show ipv6 protocol. Because these commands are often used in the management of industrial communication networks, it is important to know the benefits and challenges of using them.

5.4.1 Benefits of using the verification and troubleshooting commands

- These commands helps to show which interfaces on the industrial communications networks are configured with ipv6 addresses and whether these interfaces are up and running. The show ipv6 interface brief is the most suitable command for this purpose.

- Another area where these commands are beneficial is in checking which routing protocols are configured on industrial communication networks and whether routes are being added to the routing tables or not. The commands used most often for this task include: show ipv6 route connected updated, show ipv6 route static, show ipv6 route rip, show ipv6 route eigrp, show ipv6 route eigrp updated, show ipv6 route ospf updated, show ipv6 route ospf and show ipv6 protocol.
- If industrial network engineers master how to use these commandline commands correctly, they are much faster to interface with the router or multilayer switch operating system than graphical user interface.
- These commands use far less CPU processing time and random access memory compared to the graphical user interface of accessing routers and multilayer switches.
- They also have many optional subcommands, which are very useful for verifying and troubleshooting IPv6 addresses and routing configurations.

5.4.2 Challenges of using the verification and troubleshooting commands

- No single command can be used to view all layer 3 configurations running on routers and multilayer switches. Hence, in order to have a full view of all the configurations, a combination of two or three commands is required.
- For industrial communication network engineers who are not used to the Cisco commandline way of interfacing with routers and multilayer switches, these commands are very confusing and difficult to use.
- These commands require industrial communication engineers to type them exactly and correctly; any spelling errors prevent them from working.
- Furthermore, if the commands are mistyped they have to be retyped from the beginning and this may be very frustrating for first-time users.
- If the engineer forgets the whole command, it is difficult to guess or remember how the commands can be executed.

- It is also difficult to use these commands without a keyboard and a console cable; hence they cannot be used on devices such as tablets or mobile phones.

5.5 RESULTS FOR STATIC ROUTING ON STATIC IPV6 ADDRESSES

Static routing is configured on routers and multilayer switches using either the outgoing local interface or the neighbour global unicast address, or both, as the next hop address. This section examines the results of configuring static routing on static unicast addresses using either the outgoing local interface or the neighbour global unicast address as the next hop address.

5.5.1 Ping and traceroute results when using outgoing local interface address

As shown in sections 4.3.2.1 and 4.3.2.2, the ping and traceroute results for routers and multilayer switches configured with the outgoing local interface as next hop address are not successful. This is contrary to Cisco documentation, which explains that when configuring static routing, the next hop address of a router can either be the outgoing local interface or the next hop global unicast address. Although this concept works well in IPv4 protocol, this study has shown that using the outgoing local interface as the next hop address causes IPv6 static routing not to work. This is a challenge that industrial communication engineers should be aware of as they use the Cisco IOS software version 12.4(24)T. Though there is a need to test this challenge on real routers and multilayer switches, chances are that the results may still be the same as those obtained on the GNS3 simulator. Therefore, Cisco needs to be informed about this problem so that it can be corrected in this software and other subsequent IOS software versions.

5.5.2 Ping and traceroute results when using next hop global unicast address

When all the routers and multilayer switches in Section 3.4.1 are reconfigured with only the next hop global unicast address, IPv6 static routing works. When network connectivity is tested using ping and traceroute commands, the result are successful as shown by ping and traceroute RTT in Table 5.1 and Table 5.2 respectively. Although next hop global unicast addresses work with IPv6 static routing, they are not easy to configure in very large industrial communication networks.

Table 5.1 Ping results of static routing on global unicast next hop addresses

Ping results of static routing on static IPv6 addresses	Round trip time in milliseconds		
	Minimum	Average	Maximum
First ping	508	651	852
Second ping	608	717	856

5.5.2.1 Round trip time of static routing on static IPv6 addresses

Compared to the results of configuring RIPng, EIGRPv6 and OSPFv3 on static IPv6 addresses as shown in Table 5.8, 5.9 and 5.10, the RTT of static routing on static IPv6 addresses is very slow and not good for most industrial applications.

Table 5.2 Traceroute results of static routing on global unicast next hop addresses

Traceroute results in milliseconds (msec)		
1	2002:ACE7:2222:5::C	100 msec 100 msec 100 msec
2	2002:ACE7:2222:4::B	204 msec 204 msec 268 msec
3	2002:ACE7:2222:2::A	408 msec 404 msec 304 msec
4	2002:ACE7:2222:A::F	404 msec 512 msec 404 msec
5	2002:ACE7:2222:F::10	500 msec 616 msec 608 msec
6	2002:ACE7:2222:13::11	804 msec 600 msec 600 msec

5.6 PING RESULTS OF RIPNG, EIGRPV6 AND OSPFV3 ON STATIC IPV6 ADDRESSES

For dynamic discovery of IPv6 routes, industrial communication networks need dynamic routing protocols such as RIPng, EIGRPv6 and OSPFv3. Because these routing protocols are easy to configure in industrial communication networks, it is important to know their RTT when designing networks. Thus, Table 5.3 compares the RTT of these routing protocols in milliseconds. Knowing the dynamic routing protocol that gives the best RTT helps in the design of good networks.

Table 5.3 Round trip time of RIPng, EIGRPv6 and OSPFv3 on static addresses

IPv6 interior routing protocols on static IPv6 addresses	Round trip time in milliseconds		
	Minimum	Average	Maximum
RIPng	72	84	104
EIGRPv6	64	104	150
OSPFv3	80	95	104

5.6.1 Round trip time of RIPng on static IPv6 addresses

For industrial communication networks with fewer than 16 routers or multilayer switches, RIPng is the best option to use with static IPv6 addresses. It has the best (fastest) minimum RTT of 72 and a maximum of 104 milliseconds, as shown in Table 5.3. However, because RIPng is a distance vector protocol with a maximum hop count of 15 hops and 16 as infinity (unreachable), it is not the best option for industrial communication networks using more than 15 routers or multilayer switches.

5.6.2 Round trip time of EIGRPv6 on static IPv6 addresses

EIGRPv6 is the best routing protocol to deploy in industrial communication networks with more than 15 routers and multilayer switches when configured with static IPv6 addresses. It has a minimum round trip of 64 and maximum of 150 milliseconds and has no limit of a 16 hop count like RIPng. By default, EIGRPv6 determines the best routes using cumulative delay and bandwidth and has the option of also using maximum transmission unit MTU, reliability and load. These metrics make EIGRPv6 a better option than RIPng for very large networks with more than 15 routers or multilayer switches. The main challenge of this routing protocol is that it is Cisco proprietary and may not be compatible with some of the industrial communication networks using open standard routing protocols such as RIPng and OSPFv3.

5.6.3 Round trip time of OSPFv3 on static IPv6 addresses

With a minimum of 80 and maximum of 104 milliseconds RTT in only one area, OSPFv3 is not the best option for industrial communication networks using fewer than 16 multilayer switches or routers. However, with good planning of network areas and careful configurations, it is a better option for very large industrial communication networks using open standard routing protocols.

5.7 PING RESULTS OF RIPNG, EIGRPV6 AND OSPFV3 ON EUI-64 ADDRESSES

The results shown in Table 5.4 compare the RTT of RIPng, EIGRPv6 and OSPFv3 configured on EUI-64 addresses. These addresses are generated using a 48 bit mac-address of a particular router or multilayer switch and the “FFFE” expression.

5.7.1 Round trip time of RIPng on EUI-64 addresses

Compared to EIGRPv6 and OSPFv3, the RTT of RIPng is still the best even on EUI-64 addresses, as shown in Table 5.4. It has a faster RTT than EIGRPv6 and OSPFv3. Thus, for industrial communication networks with fewer than 16 routers and multilayer switches; planning to use the EUI-64 method of configuring IPv6 addresses, configuring RIPng is beneficial. However, even with EUI-64 addresses, RIPng is still limited to 15 maximum hop count and is not suitable for industrial communication networks with more than 15 routers or multilayer switches.

Table 5.4 Round trip time of RIPng, EIGRPv6 and OSPFv3 on EUI-64 addresses

Interior routing protocols on EUI-64 addresses	Round trip time in milliseconds		
	Minimum	Average	Maximum
RIPng	28	53	64
EIGRPv6	32	92	216
OSPFv3	56	92	212

5.7.2 Round trip time of EIGRPv6 on EUI-64 addresses

EIGRPv6 is still the best option for industrial communication networks for which it is planned to use EUI-64 addresses on more than 15 routers or multilayer switches. It has a better minimum RTT and convergence time than OSPFv3. However, even on these addresses, the main challenge of EIGRPv6 is that it is not suitable for industrial communication networks using other brands of routers and multilayer switches than Cisco.

5.7.3 Round trip time of OSPFv3 on EUI-64 addresses

The second best option for industrial communication networks with more than 15 routers or multilayer switches is OSPFv3. Although the difference in the minimum and maximum RTT between EIGRPv6 and OSPFv3 is not much, EIGRPv6 has an added benefit of being easier to configure than OSPFv3. The main challenge of OSPFv3 is that in very large industrial communication networks, designing OSPFv3 areas is not easy. However, in comparison to RIPng, it is the best option for industrial networks using open standard routing protocols with a hop count of more than 16.

5.7.4 Results of configuring RIPng, EIGRPv6 and OSPFv3 protocols on stateless autoconfigured addresses

The results of configuring RIPng, EIGRPv6 and OSPFv3 on stateless autoconfigured addresses show that these addresses cannot be routed by routers or multilayer switches. They are only used to reach nodes that are directly connected on the same networks. Therefore, they cannot be used to reach other devices in other networks through routing. Stateless autoconfigured addresses are called link local addresses.

5.8 TRACEROUTE RESULTS FOR RIPNG, EIGRPV6 AND OSPFV3 ON STATIC IPV6 ADDRESSES

Traceroute is a very useful troubleshooting tool in most industrial communication networks. It uses echo packets for ICMP to determine a route to a specified destination. With the help of traceroute, network engineers can easily diagnose network response delays, routing loops, packets dropped or stopped in a particular destination of networks. This tool also helps to determine slow network links in routers or multilayer switches. Therefore, because of its importance, network engineers should know which routing protocol gives fast traceroute results. Table 5.5 and 5.6 compares the traceroute results of configuring RIPng, EIGRPv6 and OSPFv3 on static and EUI-64 IPv6 addresses.

5.8.1 Best traceroute results of RIPng, EIGRPv6 and OSPFv3 on static addresses

When static IPv6 addresses are configured with RIPng, EIGRPv6 or OSPFv3, results from Table 5.5 show that OSPFv3 gives faster traceroute results than RIPng and EIGRPv6. Thus in industrial communication networks running on static addresses and OSPFv3, traceroute network management and troubleshooting commands are fast to execute and to get response.

5.8.2 Best traceroute results of RIPng, EIGRPv6 and OSPFv3 on EUI-64 addresses

As for EUI-64 IPv6 addresses running on RIPng, EIGRPv6 or OSPFv3 industrial communication networks, Table 5.6 shows that the best results for fast traceroute commands are obtained when EUI-64 IPv6 addresses are configured with RIPng.

Table 5.5 Traceroute results of RIPng, EIGRPv6 and OSPFv3 on static addresses

IPv6 routing protocols on static unicast addresses	Traceroute results in milliseconds (msec)
RIPng	1 2002:ACE7:2222:5::E 64 msec 20 msec 4 msec 2 2002:ACE7:2222:9::F 36 msec 28 msec 28 msec 3 2002:ACE7:2222:8::D 48 msec 28 msec 40 msec
EIGRPv6	1 2002:ACE7:2222:5::E 56 msec 16 msec 28 msec 2 2002:ACE7:2222:9::F 32 msec 24 msec 20 msec 3 2002:ACE7:2222:8::D 84 msec 48 msec 76 msec
OSPFv3	1 2002:ACE7:2222:5::E 12 msec 4 msec 28 msec 2 2002:ACE7:2222:9::F 36 msec 24 msec 52 msec 3 2002:ACE7:2222:8::D 68 msec 52 msec 48 msec

Table 5.6 Traceroute results of RIPng, EIGRPv6 and OSPFv3 on EUI-64 addresses

IPv6 routing protocols on EUI-64 addresses	Traceroute results in milliseconds (msec)
RIPng	1 2002:ACE7:2222:5:C803:25FF:FE68:6 40 msec 12msec 28msec 2 2002:ACE7:2222:9:C804:CFF:FE70:39 40msec 32 msec 16msec 3 2002:ACE7:2222:8:C807:7FF:FEC8:0 52 msec 44msec 44msec
EIGRPv6	1 2002:ACE7:2222:5:C803:25FF:FE68:6 52 msec 0 msec 0 msec 2 2002:ACE7:2222:9:C804:CFF:FE70:39 76 msec 44 msec 20 msec 3 2002:ACE7:2222:8:C807:7FF:FEC8:8 44 msec 40 msec 40 msec
OSPFv3	1 2002:ACE7:2222:5:C803:25FF:FE68:6 44 msec 48 msec 20 msec 2 2002:ACE7:2222:A:C802:26FF:FEA4:38 68 msec 8 msec 52 msec 3 2002:ACE7:2222:D:C804:CFF:FE70:8 64 msec 48 msec 60 msec

5.9 COMPARISON OF IPV4 AND IPV6 LAYER 3 CONFIGURATION COMMANDS

Table 5.7 compares the IPv4 and IPv6 layer 3 configuration commands. These are the most common commands used in configuring industrial communication routers and multilayer switches. Based on this comparison, this section analyses the differences and similarities between IPv4 and IPv6 address commands and also their respective routing protocol commands.

5.9.1 Address configuration commands

In terms of usage and application, the address configuration commands for IPv4 and IPv6 are very similar. Thus, industrial network engineers who have mastered and used IPv4 address commands before may find IPv6 address commands easy to use. However, one thing that makes IPv6 address commands different from IPv4 is the long hexadecimal nature of the IPv6 addresses. An additional significant difference is that IPv4 address commands use subnet masks, while IPv6 address commands use prefix length in the form of slash notations. The benefit of slash notations is that they are much easier to configure than subnet masks. Furthermore, the use of the address autoconfig command is not in the IPv4 protocol. This command makes the configuration of IPv6 addresses less complex and easy. However, it raises security challenges for most applications in industrial communication networks.

5.9.2 Interior gateway routing protocol configuration commands

The main difference in IPv4 and IPv6 routing protocol commands is the way in which interfaces participate in the routing process. IPv4 commands use the network command and wildcard masks to include or exclude interfaces in the routing process, while IPv6 commands use subinterface commands. The removal of the network command and wildcard mask in the configuration of IPv6 routing protocols is a huge benefit. It makes the configuration of EIGRPv6, RIPng and OSPFv3 relatively easy compared to EIGRP, RIP and OSPF. Another factor that has made the configuration of IPv6 routing protocol easy is the use of slash notation for prefix length. However, other than these differences, most of the interior gateway routing protocol commands for IPv4 and IPv6 are very similar in the way they are configured and managed. In fact, most of the IPv4 routing protocol commands have just been upgraded to accommodate IPv6.

5.10 CONFIGURATION COMMANDS FOR IPV6 TRANSITION TECHNIQUES

This section examines the configuration commands for dual stack, manual IPv6, GRE, ISATAP and NAT-PT transition techniques. These techniques are potential IPv4-to-IPv6 transition methods that most industrial communication networks can use. Knowing the configuration challenges and benefits of using these techniques helps in designing appropriate and cost-effective transitional industrial communication networks.

5.10.1 Commands for dual stack technique

When configuring the dual stack transition technique, all that is needed is to configure both IPv4 and IPv6 addresses on router or multilayer switch interfaces using the configuration commands shown in sections 3.3.1 and 3.6.1. These commands are easy to configure and are a cheap method of transitioning to IPv6. Another benefit of dual stack commands is that they do not require tunnelling within the industrial communication networks. Instead the two IPs run parallel to each other and do not depend on each other to function, except for sharing of the network resources. Their routing, security measures, quality of service and redundancy protocols are all independent of each other. Moreover, because packets are not encapsulated through tunnelling, the dual stack technique has better native router processing performance with no encapsulation overheads. In view of these facts, dual stack commands present good configuration benefits for industrial communication networks that are just beginning to implement IPv6.

However, as can be observed in the configuration process of router RA and multilayer switches MA, MB, MC, MD, ME, MF, MG, MH and MI, the main challenge of dual stack commands is the configuration of static unicast addresses. These long and complicated hexadecimal addresses present typing and configuration challenges in very large industrial communication networks. Because of this, the probability of typing and configuring wrong

IPv6 addresses is very high, which may lead to routing problems in the networks. To avoid these challenges, it is important for industrial communication network engineers to plan for adequate configuration time when using the dual stack technique. A “one-day transition period” is not enough and may lead to serious routing challenges in networks. In addition to the configuration challenge, this transition method is expensive for large industrial communication networks with routers and multilayer switches that do not support IPv6, because new IPv6 capable routers and multilayers switches have to be acquired.

5.10.2 Commands for GRE tunnelling technique

According to the configuration process of Section 3.6.3, the commands for configuring GRE are similar to those of manual IPv6 tunnel configuration. Consequently, most of the problems with manual IPv6 tunnel commands also affect GRE tunnel configurations. However, in comparison to manual IPv6 tunnel configurations, GRE is far easier to configure and to troubleshoot. The other benefits of this technique include encapsulating different network layer protocols over one reliable protocol and connecting discontinuous OSPFv3 areas in industrial communication networks. GRE also has the benefit of creating secure and stable regular connections between routers or multilayer switches over distant and big networks. Therefore, it is a good transition technique for industrial communication networks in different geographical regions.

5.10.3 Commands for ISATAP tunnelling technique

Although industrial network engineers may encounter the same problems in dealing with ISATAP commands as in manual IPv6 and GRE tunnelling, ISATAP’s main challenge involves the configuration of dynamic routing protocols. As per the ping results of Section 4.6.6.2, configuring ISATAP with RIPng, EIGRPv6 and OSPFv3 fails to yield the intended results of linking all the networks of Figure 3.3 together. Consequently, this challenge excludes ISATAP from being a suitable transition technique for large industrial communication networks. However, given that most commands for ISATAP are easy to configure and to manage, this routing challenge deserves to be investigated further.

Table 5.7 Differences and similarities between IPv4 and IPv6 layer 3 commands

IPv4 configuration commands	IPv6 configuration commands
IP address subnet mask	IPv6 address/prefix length
IP routing	IPv6 unicast routing
IP route destination destination prefix mask	IPv6 route prefix/prefix length next hop address
Router rip Network network number	IPv6 router rip name IPv6 rip name enable
Router eigrp asn Network network number No equivalent	IPv6 router eigrp asn IPv6 eigrp asn No shutdown
Router ospf process-id Network wildcard bits	IPv6 ospf process-id Router id IPv6 ospf process id area number
No equivalent	IPv6 address autoconfig
Show ip interface brief	Show ipv6 interface brief
Show ip route connected	Show ipv6 route connected
Show ip route rip	Show ipv6 route rip
Ping IPv4 address	Ping IPv6 address
Show ip route eigrp No equivalent	Show ipv6 route eigrp Show ipv6 route eigrp updated

5.10.4 Commands for manual IPv6 tunnelling technique

The main challenge related to the manual IPv6 tunnel technique is the configuration of the tunnel source and destination IP addresses. Configuring these addresses on physical interfaces of routers or multilayer switches makes this tunnelling technique unstable. The reason for this is that each time these devices are rebooted; the interfaces go down and then up again. Ultimately, this behaviour negatively affects the convergence time of routing protocols and makes the network unstable. In view of this fact, it is important to configure the source and destination IP addresses on loopback interfaces. These interfaces have the benefit of stabilising networks because they are always in the up state, unless they are shut down administratively. The other challenge with this technique involves the interface subcommand of tunnel mode ipv6ip; leaving out this command in the configuration process results in the manual IPv6 technique not functioning. Another subtle challenge that prevents this technique from working involves configuring the source and destination IP addresses in the same network. Because the tunnel interface is a point-to-point connection, configuring its source and destination IP addresses in the same network may seem like the right thing to do. However, doing so causes the tunnel not to work and causes routing challenges. It is therefore important that the source and destination IP addresses are configured in different networks, with routing protocols configured to link the networks. Furthermore, failure to configure the no ip address subcommand under the tunnel interface also prevents the tunnel from functioning and creates routing challenges for IPv6 networks.

Other than the above challenges, this technique is easy to configure and to troubleshoot. All the configuration commands are easy to remember and to configure, since IPv4 addresses are used in the source and destination IP addresses of the tunnel interface. In comparison to the other tunnelling transition techniques, manual IPv6 is one of the good options that industrial communication networks can use if the current IPv4 networks do not support dual stack configuration commands.

5.10.5 Commands for IPv6 static NAT-PT tunnelling technique

Similar to GRE, the configurations for this technique are also relatively easy to configure and to troubleshoot. However, since all the configurations are done on a single router (the NAT-PT router), this router raises the challenge of being a single point of failure for industrial communication networks. As can be seen from Figure 3.5, if router RA goes down, all the devices in IPv4 and IPv6 networks cannot communicate with one another. Because of this challenge, static NAT-PT may not be suitable for industrial communication networks with no router redundancy. The usage of only the /96 prefix length on this technique is also a challenge; it can easily cause overlapping of addresses in some networks. For this reason, this technique may not be suitable for some industrial communication networks using /96 as one of the prefix lengths.

An additional challenge for this technique covers large industrial communication networks. In such networks the manual or static mapping of IPv4 to IPv6 and vice versa is very challenging, because of the many networks and subnetworks involved. This challenge is even more pronounced in industrial communication networks routing among VLANs. The usage of VLANs requires addresses for virtual interfaces and this adds to the challenge of mapping IPv4 to IPv6 addresses. In view of this fact, the IPv6 static NAT-PT transition technique may not be a suitable transition technique for large industrial communication networks.

5.11 PING RESULTS OF DUAL STACK, MANUAL IPV6, GRE AND ISATAP ON OSPFV3, RIPNG AND EIGRPV6

This section discusses and compares the RTT of the ping results of dual stack, manual IPv6, GRE and ISATAP configured on OSPFv3, RIPng and EIGRPv6.

5.11.1 Ping results on OSPFv3

5.11.1.1 Dual stack technique on OSPFv3

According to the results of Table 5.8, IPv4 packets have better RTT than IPv6 packets when the dual stack technique is configured with OSPF and OSPFv3 respectively. These results also show that IPv4 addresses and OSPF can successfully coexist with IPv6 addresses and OSPFv3 without experiencing any interference between the two type of addresses and routing protocols. In addition, these results prove that using the same OSPF process ID and router ID for OSPF and OSPv3 has no influence on the operation of both routing protocols. Furthermore, compared to manual IPv6 and GRE tunnelling techniques, the dual stack technique has fast RTT on OSPFv3. Thus, for industrial communication networks planning to run both IPv4 and IPv6 networks, using OSPF and OSPFv3 are the best transition options. However, the main challenge of the dual stack technique even on OSPF and OSPFv3 lies in the manual configuration of static unicast IPv6 addresses.

5.11.1.2 Manual IPv6 and GRE tunnelling techniques on OSPFv3

For industrial communication companies planning to use tunnelling transition techniques and OSPFv3, using manual IPv6 tunnelling is a better option than GRE. It has faster RTT than GRE, as shown in Table 5.8 and is easy to configure and manage. However, compared to the dual stack results, this RTT is not very good.

5.11.1.3 ISATAP tunnelling technique on OSPFv3

The results of Table 5.8 show that configuring OSPFv3 with ISATAP does not work. All the ping results done on this configuration had a success rate of 0%. This means that the ISATAP technique and OSPFv3 are not good transitions tools for industrial communication networks using the OSPF routing protocol.

5.11.2 Ping results on RIPng

5.11.2.1 Dual stack technique and RIPng

Table 5.9 shows that when the dual stack technique is configured with RIP and RIPng, IPv4 packets have faster RTT than IPv6 packets. These results are similar to those obtained in Table 5.8. Thus, the dual stack technique is still the best option to use when transitioning RIP industrial communication networks to the RIPng protocol. However, it is important to note that both RIP and RIPng are distance vector protocols with a minimum hop count of 15. For this reason, they may not be suitable for large industrial communication networks. On the other hand, these results also confirm that RIP and RIPng can coexist without interference.

Table 5.8 RTT of OSPFv3 on dual stack, manual IPv6, GRE and ISATAP

IPv6 transition techniques running on OSPFv3	Round trip time in milliseconds		
	Minimum	Average	Maximum
Dual stack • IPv4 packets • IPv6 packets	 80 92	 102 105	 104 128
Manual IPv6 tunnelling	676	746	808
Generic routing encapsulation	792	922	1052
Intrasite automatic tunnel addressing protocol	0 Success rate is 0	0 Success rate is 0	0 Success rate is 0

5.11.2.2 Manual IPv6 and GRE tunnelling techniques on RIPng

Even on RIPng, manual IPv6 proves to have faster RTT than GRE tunnelling, as shown in Table 5.9. Therefore, for industrial communication networks currently using RIP in their networks and for which it is planned to use tunnelling techniques and RIPng as their transition tools, manual IPv6 tunnelling is a better option than GRE tunnelling technique.

5.11.2.3 ISATAP tunnelling technique on RIPng

Just like OSPFv3, the ping results for ISATAP and RIPng had a success rate of 0%. This shows that the ISATAP transition technique does not work well even with RIPng. Hence, it is not a suitable transition tool for industrial communication networks running RIP as the routing protocol.

5.11.3 Ping results on EIGRPv6

5.11.3.1 Dual stack technique on EIGRPv6

Table 5.10 shows that even on EIGRPv6 and EIGRP dual stack configurations, IPv4 packets have faster RTT than IPv6 packets. So far on all the three routing protocols, the dual stack technique has yielded similar results. Therefore, this technique is suitable to be used as a transition tool for networks running RIP, OSPF or EIGRP protocols.

5.11.3.2 GRE technique on EIGRPv6

When configured with EIGRPv6, Table 5.10 shows that the GRE technique has the best (fastest) RTT compared to the manual IPv6 and dual stack transition techniques. Thus for networks using Cisco routers and multilayer switches and running EIGRP, using this technique is more beneficial than manual IPv6 and dual stack techniques.

5.11.4 Best transition technique for static unicast addresses

The pattern of results from tables 5.8, 5.9 and 5.10 shows that the dual stack technique has the best (fastest) RTT on static unicast addresses when configured on RIPng, EIGRPv6 or OSPFv3 routing protocols. However, the RTT of these addresses on manual IPv6 and GRE for RIPng, EIGRPv6 or OSPFv3 networks is not very good.

5.12 FAILOVER TIME RESULTS OF HSRPV2 ON RIPNG, EIGRPV6 AND OSPFV3

Based on the ping results of Table 5.11, this section compares the failover time of the active and standby router when HSRPv2 is configured on RIPng, EIGPRv6 and OSPFv3. The ping command is done on multilayer switch MA and sends ICMP echo packets to ME. In order to ensure that all packets reach their destination, the ping command is executed after the routing protocols have fully converged. HSRPv2 is one of the IPv6 redundancy protocols that ensure the availability of network routes when one interface of the router or multilayer switch fails. It uses the concept of virtual IPv6 address and mac-addresses to provide gateway redundancy to devices under a particular network. This concept works better in hierarchical network topology than in ring networks. Although HSRPv2 is suitable for these networks, future studies should consider how it can provide redundancy even to ring networks. With router redundancy in industrial communication networks, there is less down time for production of goods and services.

Table 5.9 RTT of RIPng on dual stack, manual IPv6, GRE and ISATAP

IPv6 transition techniques running on RIPng protocol	Round trip time in milliseconds		
	Minimum	Average	Maximum
Dual stack • IPv4 packets • IPv6 packets	 84 88	 94 123	 116 168
Manual IPv6 tunnelling	644	812	992
Generic routing encapsulation	672	822	964
Intrasite automatic tunnel addressing protocol	0 Success rate is 0	0 Success rate is 0	0 Success rate is 0

Table 5.10 RTT of EIGRPv6 on dual stack, manual IPv6, GRE and ISATAP

IPv6 transition techniques running on EIGRPv6 protocol	Round trip time in milliseconds		
	Minimum	Average	Maximum
Dual stack • IPv4 packets • IPv6 packets	 72 352	 114 538	 212 712
Manual IPv6 tunnelling	812	1104	1800
Generic routing encapsulation	344	456	576
Intrasite automatic tunnel addressing protocol	0 Success rate is 0	0 Success rate is 0	0 Success rate is 0

5.12.1 Failover time of HSRPv2 on OSPFv3

For industrial communication networks that require fast RTT for the smooth operation of services and products, using HSRPv2 on networks running OSPFv3 is the best option than EIGRPv6 and RIPng. This combination gives the best (fastest) RTT of 64 milliseconds (ms), which is very good for most industrial communication applications. However, the success rate of switch-over time between the standby router and active router is 4% lower than EIGRPv6.

5.12.2 Failover time of HSRPv2 on EIGRPv6

As for industrial communication applications that need fast switch-over time from the active to the standby router, using HSRPv2 and EIGRPv6 is the best option. This combination offers a very good failover time of 98% (49/50), showing that within 1 ms of interface failure, the standby router takes over as active router. Although this fast failover time is good for some applications, it may not be good for applications that require less than 72 ms of RTT.

5.12.3 Failover time of HSRPv2 on RIPng

RIPng is not suitable to be configured with HSRPv2 in industrial communication networks that require router or multilayer switch redundancy. The switch-over time from the active router to the standby router is not very good; it has a success rate of 44% (12/27). Furthermore, the RTT of 164 ms is not very good for most industrial communication applications.

Table 5.11 HSRPv2 failover time on RIPng, EIGRPv6 and OSPFv3 networks

HSRPv2 Redundancy protocol	Failover time of round trip time in miliseconds (ms)			Success rate of failover time
	Minimum	Average	Maximum	
HSRPv2 running on OSPFv3	64	198	308	94% (47/50)
HSRPv2 running on EIGRPv6	72	203	380	98% (49/50)
HSRPv2 running on RIPng	164	269	664	44% (12/27)

5.13 BENEFITS AND CHALLENGES OF CONFIGURING ROUTERS AND MULTILAYER SWITCHES IN A RING OR HIERARCHICAL NETWORK TOPOLOGY

5.13.1 Benefits of a ring network topology

- It is easy to add or remove multilayer switches or routers to the network.
- The addition of new routers or multilayer switches to the network has less impact on the bandwidth.
- It is easy to recognise network faults in this topology.
- Since the data traffic is unidirectional, transmission of packets is fairly simple and without experiencing any bottleneck.

5.13.2 Challenges of a ring network topology

- In comparison to a hierarchical network topology, transmission of data packets in a ring network topology is slower because packets go through every router and multilayer switch between the sending and receiving device.
- Failure of a link or cable on one multilayer switch or router breaks the ring network and makes the whole network go down.
- Since all routers and multilayer switches are connected, the addition of new devices requires a temporary shutdown of the network and this may disrupt production of goods and services.
- It is not easy to troubleshoot multilayer switches and routers in a ring network topology.

5.13.3 Benefits of a hierarchical network topology

- It is easier to implement a router redundancy mechanism such as HSRPv2 in a hierarchical network topology than in a ring topology.
- Because of alternative links (routes) for transmission of data, failure of a link or cable on one router or multilayer switch does not make the whole network go down.

- Given the dedicated links between any two routers or multilayer switches, hierarchical networks are able to manage large data traffic.
- Identification of network faults in hierarchical networks is easy because of point-to-point connections between every pair of multilayer switches or routers.

5.13.4 Challenges of hierarchical network topology

- The costs involved in the configuration and maintenance of this type of topology are high because of many cables, routers and multilayer switches required.
- Network administration and maintenance of hierarchical topology are not easy because of the complex nature of the networks.
- Some redundant links, routers and multilayer switches have no major functions and simply complicate the network design.
- Designing hierarchical network topology with different brands of routers and multilayer switches from different vendors may be difficult.
- In small and medium industrial communication networks, hierarchical network topologies are overkill because of the large number of routers, cables and multilayer switches required.

5.14 POTENTIAL APPLICATION AREAS FOR ROUTERS AND MULTILAYER SWITCHES

From the above discussions and analysis, it is obvious that the benefits and challenges of IPv6 layer 3 configuration commands can lead to many technological innovations. One such innovation is new areas of applications for routers and multilayer switches. Thus, this section examines some of these areas and how they affect routers and multilayer switches.

5.14.1 New network services and management protocols

In all the configurations done above, there is no need for using NAT protocol because there are many IPv6 addresses available for use in networks. The removal of NAT in industrial communication networks can lead to new management protocols and services for routers and multilayer switches. Among the router applications that are likely to benefit from the removal of NAT are VOIP, quality of service, network remote monitoring, 3G mobile data services, easy access to broadband internet and military and industrial sensors applications.

5.14.2 Efficient processing and routing of packets

As can be observed in all the configurations of Chapter 3, no broadcast IPv6 addresses are configured or enabled. The removal of all broadcast addresses in IPv6 protocol has made the processing of packets in routers and multilayer switches faster and efficient. This is because routing protocols such as RIPng, EIGRPv6 and OSPFv3 all use multicast addresses instead of broadcast addresses. Because of this, the way in which routers and multilayer switches query and reply to requests from end devices is efficient. Admittedly, the use of multicast addresses also contributes to the design of efficient industrial communication networks with fewer network loops. Given this development, new routers and multilayer switches with much higher processing speeds can be innovated.

5.14.3 Industrial automation and control

In most of today’s large industrial communication networks, network engineers are burdened with configuring IPv4 addresses to new and old multilayer switches. However, with the autoconfiguration feature, a new device can obtain its IPv6 address immediately it is connected to the network. As a result of this feature, networking, automating and control of applications and end devices in large industrial communications networks can be done easily using routers and multilayer switches. The autoconfiguration feature can also bring about new interaction protocols for neighbouring routers and multilayer switches similar to the NDP. NDP has replaced the ARP in IPv4 protocol.

5.15 MATURITY LEVEL OF THE CISCO IPV6 IOS SOFTWARE

Although this study used real Cisco IOS images in a GNS3 simulator, results in Chapter 4 show that the IPv6 software for routers and multilayer switches is matured and ready to be used in industrial communication networks. Most of the commands produced the expected results and did not show any programming errors or execution problems. However, for static routing, results show that using the outgoing local interface as the next hop address for routers or multilayer switches causes this routing protocol not to work. In this study, IPv6 static routing only works when the global unicast address of the neighbour router or multilayer switch is used as next hop address. Until this concept is tested and tried on real Cisco routers and multilayer switches, this research reveals this development as an error in the Cisco IOS software version 12.4(24)T. Thus, Cisco needs to be informed about this error so that it can be corrected before the software is deployed in real industrial communication routers and multilayer switches.

CHAPTER 6 CONCLUSION

Just like any other new technology, the use of IPv6 layer 3 commands on industrial communication routers and multilayer switches comes with benefits and challenges. The static unicast and EUI-64 address commands are more complicated than IPv4 address commands because of the complex hexadecimal nature of IPv6 addresses. This complexity makes the task of configuring static and EUI-64 address commands very challenging to network engineers. In spite of this challenge, one outstanding benefit of these two commands is the ability to use slash notation for the prefix length. Unlike IPv4 subnet masks, the use of slash notation makes the configuration of prefix lengths much easier. One other benefit of the EUI-64 address configuration commands is the ability to minimise the human errors associated with the manual configuration of IPv6 addresses.

With regard to dynamic routing protocols, RIPng is the best option to use for industrial communication networks with fewer than 16 layer 3 devices. It has better (faster) RTT for static and EUI-64 addresses than EIGRPv6 and OSPFv3. Similarly, the best results for fast traceroute commands are obtained when EUI-64 addresses are configured with RIPng. The other benefit of RIPng is the subinterface ipv6 rip name enable command. Unlike the RIP network wildcard masks, this command makes it easy to configure RIPng on selected interfaces of multilayer switches or routers. EIGRPv6 has faster RTT than OSPFv3 and no limit of a 16 hop count like RIPng. In addition, it does not require routers or multilayer switches to be in the same IPv6 subnet as a prerequisite to forming neighbour relationships, making the process of exchanging route updates faster. The other benefit is that unlike OSPFv3, the EIGRPv6 process still works well even if the router identifiers are configured the same on all routers and multilayer switches. Besides these benefits, EIGRPv6 has challenges as well. Configuring multilayer switches and routers with different ASN prevents the formation of EIGRPv6 neighbour relationships and results in routing challenges. In contrast to EIGRP, which does not require the “no shutdown” command in order to start its process, failure to configure the “no shutdown” and router id commands on EIGRPv6 causes the process not to start. OSPFv3 gives faster traceroute command results than RIPng and EIGRPv6 when configured on static unicast addresses. Thus, it is the best substitute for

RIPng in very large industrial communication networks using open standard routing protocols. A very interesting benefit of OSPFv3 commands is the use of a 32 bit address as the router-id. Unlike using a 128 bit address, a 32 bit address router-id is very beneficial to IPv6 because it makes the process of configuring the router-id and OSPFv3 simpler. However, with a minimum of 80 ms and maximum of 104 ms of RTT in only one area, it is not the best option for industrial communication networks using fewer than 15 multilayer switches or routers. Another challenge involves configuring the same router-id on different routers or multilayer switches. This misconfiguration has the effect of causing the OSPFv3 process not to start and makes neighbour relationships fail.

Although the RTT for static routing is not as fast as EIGRPv6, RIPng or OSPFv3, static routes are beneficial when connecting industrial communication networks to the internet. According to Cisco documentation, static routing can use either the outgoing local interface or the neighbour global unicast address of the router or both as next hop address. However, this study has shown that the use of the outgoing local interface as the next hop address causes static routing not to work. Successful ping results are obtained only when the neighbour global unicast address is used as the next hop address. Dual stack commands are easier to configure and have better native router processing performance with no encapsulation overheads. However, because of the complex nature of IPv6 addresses, configuring these commands is a challenge. As for the manual IPv6 tunnelling technique, its main configuration challenge is the configuration of the tunnel source and destination IP addresses. Configuring these addresses on physical interfaces of routers or multilayer switches makes this technique unstable. This is because each time routers or multilayer switches are restarted, interfaces go down and then up again. Consequently, there is no stability on networks and this affects the routing convergence time of RIPng, EIGRPv6 and OSPFv3. For this reason, the best option to deal with this challenge is to configure the tunnel source and destination IP addresses on loopback interfaces. Other than this challenge, commands for this technique are easy to configure and to troubleshoot, since IPv4 addresses are used on the source and destination ip addresses of the tunnel interface.

Configuring ISATAP with RIPng, EIGRPv6 or OSPFv3 failed to yield the results of linking networks. As for static NAT-PT commands, they are easy to configure and to troubleshoot because they are done on a single router. However, this router poses the risk of being a single point of failure in the network. The other challenge to this technique is that only the /96 prefix length can be configured as the prefix length of the NAT-PT router. All the other prefix lengths prevent this technique from working. Thus, this technique may not be suitable for some industrial networks using the /96 prefix length as one of the network prefixes. For industrial communication applications that need faster failover time from the active to the standby router, HSRPv2 and EIGRPv6 are the best options. Although a GNS3 network simulator is used in all layer 3 configurations, this study is very useful in designing good transitional IPv6 networks. It is also helpful in configuring and troubleshooting layer 3 networks. Furthermore, this study proves that most of the configuration commands in Cisco IPv6 software are mature and ready to be used in industrial communication networks. However, many of the challenges for IPv6 layer 3 commands arise from misconfiguration of the commands and the hexadecimal complex nature of IPv6 addresses. The following areas of IPv6 protocol, which are not addressed in this study, are recommended as topics for future research.

- Research on the benefits and challenges of using IPv6 layer 2 configuration commands and protocols in industrial communication switches and end devices is needed.
- A study on the benefits and challenges of using virtual router redundancy protocol version 3 (VRRPv3) on industrial communication routers and switches is required.
- Although Cisco documents that either the outgoing local interface or neighbour global unicast address or both may be used as next hop addresses of routers or multilayers switches in static routing, this study has shown that only the next hop global unicast address makes IPv6 static routing work. The use of outgoing local interface as next hop address makes IPv6 static routing not work. This concept needs to be investigated further on real Cisco routers and multilayer switches. If the results should happen to be the same as those obtained in this study on a GNS3 simulator, Cisco must be informed about this error in the IOS software version 12.4(24) T.

REFERENCES

[1] F. Li, J. Yang, J. Wu, Z. Zheng, H. Zhang and X. Wang, “Configuration analysis and recommendation: Case studies in IPv6 networks,” in *Proc. IEEE Trans. Commun.*, Beijing, 2014, pp. 37-51.

[2] W. Odom, “IP version 6 Addressing,” in *Cisco Certified Network Professional Route 642-902,* 3rd ed., Indianna, USA: Cisco Press, 2010, pp. 529-562.

[3] R. Healy, N. Mehta and W. Odom, “IP version 6,” in *CCIE Routing and Switching Exam Certification Guide,* 4th ed., Indianna, USA: Cisco Press, 2010, pp. 883-943.

[4] W. Odom, “IP version 6,” in *CCNA ICND2 640-816 Official Certification Guide,* 4th ed., Indianna, USA: Cisco Press, 2012, pp. 620-652.

[5] R. Mafievici, G. Sebestyen and A. Pop-Bidain, “Industrial control and communication framework on IPv6 infrastructure”, in *Proc. Int. Multi-Conf. Computing Global Inform. Technology*, Bucharest, 2006, pp. 7.

[6] T. Y Chen, H.W. Wei, Y. J Chen and W. K. Shih, “An emergency medical service in IPv6 network environment”, in *Proc. IEEE J. Trans. Eng. Health Med.*, Tapei, 2011, pp. 10-15.

[7] A. M. Hassaballa, A. E. EIHussen and A. A. Goup, “Industrial ethernet protocol IPv6 enabling approach”, in Proc. *Gezira J. Eng. Appl. Sci.*, Gezira, 2011, pp. 1-13.

[8] R. Yasionvsky, A. L. Wijesinha and R. Karne, “Impact of IPsec and 6to4 on VOIP quality over IPv6”, in *Proc. 10th Int. Conf. Telecommun.,* Zagreb, 2009, pp. 235 – 242.

[9] D. G. Genkov, “An algorithm and software for finding proper packet size in an IPv6 network using double connection,” in *Proc. 19th Telecommun. Forum,* Belgrade, 2011, pp. 1523 – 1526.

[10] M. Wadhwa and M. Khari, “Prevention algorithm against the vulnerability of type 0 routing header in IPv6,” in *Proc. Int. Conf. Computational Intell. and Commun. Networks,* Gwalior, 2011, pp. 616 – 620.

[11] T. Joto, T. Nakamura and W. Uemura, “A proposal for an IPv6 information sharing system for disaster scenes,” in *Proc. 11th Int. Conf. Control, Automation and Syst.*,

Gyeonggi-do, 2011, pp. 137 – 139.

[12] H. M. El-Hennawy, H. H. Gomaa and A. S. Amin, "The effectiveness of transmitting voice traffic over IPv6 convergence sublayer of WiMAX mesh networks," in *Proc. IEEE 17th Int. Conf. Telecommun.*, Doha, 2010, pp. 293 – 298.

[13] X. Li, L. Ji, Y. Li, L. Zhang and S. Wang, "Improvement of the mobile e-health wireless networks based on the IPv6 protocol," in *Proc. Int. Conf. E-Health Networking, Digital Ecosystems and Technologies*, Shenzhen, 2010, pp. 73 – 76.

[14] J. G Jayanthi and S. A. Rabara, "IPv6 addressing architecture in IPv4 network," in *Proc. ICCSN '10 2nd Int. Conf. Commun. Software and Networks*, Singapore, 2010, pp. 461 – 465.

[15] C. Alexandru, S. Andreea and R. Rughini, "Practical analysis of IPv6 security auditing methods," in *Proc. 9th Roedunet Int. Conf.*, Sibiu, ROU, 2010, pp. 36 – 41.

[16] H. Miyata and M. Endo, "Design and evaluation of a fieldbus protocol over IPv6," in *Proc. 8th IEEE Int. Conf. Ind. Informatics*, Osaka, 2010, pp. 136 – 141.

[17] Y. Xia, B. S. Lee, C. K. Yeo and V.L. Seng, "An IPv6 translation scheme for small and medium scale deployment," in *Proc. 2nd Int. Conf. Advances Future Internet*, Venice, 2010, pp. 108 – 112.

[18] Z. Zeng, "Intrusion detection system of IPv6 based on protocol analysis," in *Proc. Int. Conf. Multimedia Technology*, Ningbo, 29-31 2010, pp. 1 – 4.

[19] P. Guo and D. Fu, "The discussions on implementing QoS for IPv6," in *Proc. Int. Conf. Multimedia Technology*, Ningbo, 2010, pp. 1 – 4.

[20] C. Jun and C. Xiaowei, "Intrusion detection system research based on data mining for IPv6," in *Proc. Int. Forum Inform. Technology and Applicat.*, Kunming, 2010, pp. 384 – 388.

[21] S. H. Liu and L. Z. Shen, "A kind of routing mechanism based on IPv6 and differentiated services," in *Proc. Int. Conf. Inform. Networking and Automation*, Kunming, 2010, pp. 227 – 230.

[22] A. R. Choudhary and A. Sekelsky, "Securing IPv6 network infrastructure: A new security model," in *Proc. IEEE Int. Conf. Technologies Homeland Security*, Waltham, MA, 2010, pp. 500 – 506.

[23] T. Mrugalski, J. Wozniak and K. Nowicki, “Remote stateful autoconfiguration for mobile IPv6 nodes with server side duplicate address detection,” in *Proc. Australasian Telecommun. Networks and Applicat. Conf.*, Auckland, 2010, pp. 141 – 146.

[24] F. Beck, O. Festor, I. Chrisment and R. Droms, “Automated and secure IPv6 configuration in enterprise networks,” in *Proc. Int. Conf. Network and Service Manage.*, Niagara Falls, ON, 2010, pp. 64 – 71.

[25] P. Wu, Y. Cui, M. Xu, J. Wu, X. Li, C. Metz and S. Wang, “PET: Prefixing, encapsulation and translation for IPv4-IPv6 coexistence,” in *Proc. IEEE Global Telecommun. Conf.*, Miami, FL, 2010, pp. 1 – 5.

[26] J. Granjal, E. Monteiro and J. S. Silva, “Enabling network-layer security on IPv6 wireless sensor networks,” *in Proc. IEEE Global Telecommun. Conf.*, Miami, FL, 2010, pp. 1 – 6.

[27] E. Baccelli, T. Clausen and R. Wakikawa, “IPv6 operation for WAVE-Wireless access in vehicular environments,” in *Proc. IEEE Veh. Networking Conf.*, Jersey City, NJ, 2010, pp. 160 – 165.

[28] R. Chaparadza, S. Papavassiliou, S. Papavassiliou, S. Soulhi and J. Ding, “The self-managing future internet powered by the current IPv6 and extensions to IPv6 towards “IPv6++”- A viable roadmap scenario for the internet evolution path,” in *Proc. IEEE Globecom Workshops*, Miami, FL, 2010, pp. 551 – 556.

[29] Z. Wang, Q. Sun, X. Huang and Y. Ma, “IPv6 end-to-end QoS provision for heterogeneous networks using flow label,” in *Proc. 3rd IEEE Int. Conf. Broadband Network and Multimedia Technology*, Beijing, 2010, pp. 130 – 137.

[30] R. K. Murugesan and S. Ramadass, “IPv6 address distribution: An alternative approach,” in *Proc. 3rd IEEE Int. Conf. Broadband Network and Multimedia Technology*, Beijing, 2010, pp. 252 – 257.

[31] D. I. Choi, J. Park, S. Kim and H. K. Kahng, “IPv6 global connectivity for 6LoWPAN using short ID,” in *Proc. Int. Conf. Inform. Networking*, Barcelona, 2011, pp. 384 – 387.

[32] A. K. Davis, K. Vasudevan, J. Kuri and H. Dagale, “IPv4-IPv6 translator for VoIP

and videoconferencing," in *Proc. Int. Conf. Commun. and Signal Process.*, Kerala, 2011, pp. 367 – 369.

[33] J. Jeong, J. Kim and P. Mah, "Design and implementation of low power wireless IPv6 routing for NanoQplus," in *Proc. 13th Int. Conf. Advanced Commun. Technology,* Seoul, 2011, pp. 966 – 971.

[34] M. Dunlop, S. Groat, R. Marchany and J. Tron," The good, the bad, the IPv6," in *Proc. 9th Annu. Commun. Networks and Services Research Conf.,* Ottawa, ON, 2011, pp. 77 – 84.

[35] A. M. Taib and R. Budiarto, "Securing tunnel endpoints for IPv6 transition in enterprise networks," in *Proc. Int. Conf. Sci. and Social Research,* Kuala Lumpur, Malaysia, 2010, pp. 1114 – 1119.

[36] A. Amin, W. Anjum, M. S. Malik, S. N. Ali, A. Naseer and A. Waseem, "Performance evaluation of IPv4 and IPv6 networks in absence of link layer protection," in *Proc. Saudi Int. Electron., Commun. and Photonics Conf.*, Riyadh, 2011, pp. 1 – 5.

[37] L. M. Oliveira, J. J. Bruno, M. Maçao, P. A. Nicolau, L. R. Wang and L. Shu, "End-to-end connectivity IPv6 over wireless sensor networks," in *Proc. 3rd Int. Conf. Ubiquitous and Future Networks,* Dalian, 2011, pp. 1 – 6.

[38] C. Jun and C. Xiaowei, "Intrusion detection system research based on data mining for IPv6," in *Proc. Int. Forum Inform. Technology and Applicat.*, Kunming, 2010, pp. 384 – 388.

[39] Y. Zou, T. Wang, H. Wei, M. Liu, C. Li and X. Lu, "Robot software architecture based on IPv6," in *Proc. 6th IEEE Conf. Ind. Electron. and Applicat.*, Beijing, 2011, pp. 1666 – 1671.

[40] S. Shen, X. Lee, Z. Sun and S. Jiang, "Enhance IPv6 dynamic host configuration with cryptographically generated addresses," in *Proc. 5th Int. Innovative Mobile and Internet Services Ubiquitous Computing,* Seoul, 2011, pp. 487 – 490.

[41] W. N. Ali, A. H. Taib, N. M. Hussin, R. Budiarto and J. Othman, "Distributed security policy for IPv6 deployment," in *Proc. 3rd Int. Symp. and Exhibition Sustainable Energy and Environment,* Melaka, 2011, pp. 120 – 124.

[42] M. Colajanni, L. D. Zotto, M. Marchetti and M. Messori, “Defeating NIDS evasion in mobile IPv6 networks,” in *Proc. IEEE Int. Symp. World Wireless, Mobile and Multimedia Networks*, Lucca, 2011, pp. 1 – 9.

[43] M. Gregr, P. Matousek, M. Sveda and T. Podermanski, “Practical IPv6 monitoring-challenges and techniques,” in *Proc. IFIP/IEEE Int. Symp. Integrated Network Manage.*, Dublin, 2011, , pp. 650 – 653.

[44] Z. Lin, W. Hao and Z. Shibing, “A measurement study on bittorrent traffic behaviors over IPv6,” in *Proc. IEEE Int. Conf. Comput. Sci. and Automation Eng.*, Zhangjiajie, 2012, vol. 3, pp. 354 – 357.

[45] K. Nowicki, M. Stankiewicz, A. Mrugalska, J. Wozniak and T. Mrugalski, “Extension management of a knowledge base migration process to IPv6,” in *Proc. IEEE/IPSJ 11th Int. Symp. Applicat.and Internet*, Munich, Bavaria, 2011, pp. 497 – 501.

[46] H. Wei, S. You-ye, L. Jiang and L. Kaining, “DDoS/DoS attacks and safety analysis of IPv6 campus network: Security research under IPv6 campus network,” in *Proc. Int. Conf. Internet Technology and Applicat.,* Wuhan, 2011, pp. 1 – 4.

[47] C. Min, “Research on network security based on IPv6 architecture,” in *Proc. Int. Conf. Electron. and Optoelectronics*, Dalian, 2011, vol. 1, pp. 415 – 417.

[48] D. Yu and J. Liu, “IPv6-based smart metering networks for monitoring building and electricity”, in IEEE *J. Advances Mech. Eng.,* Jun. 2013.

[49] V. Srivastara, C. Wargo and S. Lai, “Aviation application over IPv6: Performance issues”, in *Proc. of IEEE Aerospace Conf.*, Springfield, VA, 2004, vol. 3, pp. 1-9.

[50] J. G. Jayanthi and S. A. Rabara, “Transition and mobility management in the integrated IPv4 and IPv6 network,” in *Proc. Int. Conf. Electron. and Inform. Eng.*, Kyoto, 2010, pp. 162 – 166.

[51] D. Yang, Q. Guo, Q. Xu and L. La, “Research and application of IPv6 and WSNs based on CUTE testbed,” in *Proc. 3rd IEEE Int. Conf. Comput. Sci. and Inform. Technology,* Chengdu, 2010, pp. 758 – 761.

[52] R. K. Murugesan and S. Ramadass, “A multipurpose global passport solution using IPv6,” in *Proc. 3rd IEEE Int. Conf. Comput. Sci. and Inform. Technology,* Chengdu,

2010, pp. 405 – 407.

[53] M. Aazam, I. Khan, M. Alam and A. Qayyum, “Comparison of IPv6 tunneled traffic of teredo and ISATAP over test-bed setup,” in *Proc. Int.Conf. Inform. and Emerging Technologies,* Karachi, 2010, pp. 1 – 4.

[54] Z. Zeng, “Intrusion detection system of IPv6 based on protocol analysis,” in *Proc. Int.Conf. Multimedia Technology*, Ningbo, 2010, pp. 1 – 4.

[55] P. Guo and D. Fu, “Discussions on implementing QoS for IPv6,” in *Proc. Int. Conf. Multimedia Technology*, Ningbo, 2010, pp. 1 – 4.

[56] A. K. Davis, K. Vasudevan, J. Kuri and H. Dagale, “IPv4-IPv6 translator for VoIP and videoconferencing,” in *Proc. Int. Conf. Commun. and Signal Process.*, Kerala, 2011, pp. 367 – 369.

[57] M. R. Kumar and S. Ramadass, “IPv6 address space allocation schemes: Issues and challenges, a survey,” in *Proc. 2nd Int. Conf. Network Applicat., Protocols and Services*, Kedah, 2010, pp. 170 – 175.

[58] S. Liu and L. Shen, “A kind of routing mechanism based on IPv6 and differentiated services,” in *Proc. Int. Conf. Inform. Networking and Automation*, Kunming, 2010, pp. 227 – 230.

[59] A. R. Choudhary and A. Sekelsky, “Securing IPv6 network infrastructure: A new security model,” in *Proc. IEEE Int. Conf. Technologies Homeland Security*, Waltham, MA, 2010, pp. 500 – 506.

[60] V. Visoottiviseth and P. Ngamtura, “On the performance of MIPv6 and FMIPv6 based on real IPv6 applications over IEEE 802.11g testbeds,” in *Proc. Int. Symp. Commun. and Inform. Technologies*, 2010, Tokyo, Japan, pp. 1217 – 1222.

[61] S. Kalwar, N. Bohra and A. A. Memon, “A survey of transition mechanisms from IPv4 to IPv6 - simulated test bed and analysis,” in *Proc. 3rd Int. Conf. Digital Inform., Networking, and Wireless Commun.*, Moscow, 2015, pp. 30 – 34.

[62] K. Govindarajan, S. Setapa, K. Meng and H. Ong, “Interoperability issue between IPv4 and IPv6 in openflow enabled network,” in *Proc. Int. Conf. Comput., Control, Informatics and Applicat.*, Bandung, 2014, pp. 58 – 63.

[63] M. Jung, P. Raich and W. Kastner, “The relevance and impact of IPv6 multicasting

for wireless sensor and actuator networks based on 6LoWPAN and constrained restful environments*,"* in *Proc. Int. Conf. Internet Things*, Cambridge, MA, 2014, pp. 7 – 12.

[64] S. S. Tseng, C. H. Ku and A. C. Lu," Building an IPv6 upgrade model based upon cost-effective strategies," in *Proc. IEEE Region 10 Conf.*, Bangkok, 2014, pp. 1 – 5.

[65] K. C. Yang, H. T. Fang and Q. Wu, "Openflow-based IPv6 rapid deployment mechanism," in *Proc. 2014 IEEE Region 10 Conf.*, Bangkok, 2014, pp. 1 – 6.

[66] A. S. Ahmed, R. Hassan and N. E. Othman "Security threats for IPv6 transition strategies: A review," in *Proc. 4th Int. Conf. Eng. Technology and Technopreneuship*, Kuala Lumpur, 2014, pp. 83 – 88.

[67] W. Y. Lin, K. P. Hsueh, W. H. Hsu, L.G. Yie and W. C. Tai, "Design and implementation of health monitoring system for solar panel in IPv6 network*,"* in *Proc. 10th Int. Conf. Intell. Inform. Hiding and Multimedia Signal Process.*, Kitakyushu, 2014, pp. 57 – 60.

[68] G. H. Lai, "A light-weight penetration test tool for IPv6 threats*,"* in *Proc. 10th Int. Conf. Intell. Inform. Hiding and Multimedia Signal Process.*, Kitakyushu, 2014, pp. 49 – 52.

[69] N. Chuangchunsong, S. Kamolphiwong, T. Kamolphiwong and R. Elz, "An enhancement of IPv4-in-IPv6 mechanism*,"* in *Proc. 10th Int. Conf. Intell. Inform. Hiding and Multimedia Signal Process.*, Kitakyushu, 2014, pp. 45 – 48.

[70] C. W. Tseng, S. J. Chen, Y. T. Yang, L. D. Chou, C. K. Shieh and S. W. Huang, "IPv6 operations and deployment scenarios over SDN," in *Proc. 16th Asia-Pacific Network Operations and Manage. Symp.*, Hsinchu, 2014, pp. 1 – 6.

[71] H. Lamaazi, N. Benamar, A. J. Jara, L. Ladid and D. E. Ouadghiri, "Challenges of the internet of things: IPv6 and network management*,"* in *Proc. 8th Int. Conf. Innovative Mobile and Internet Services Ubiquitous Computing*, Birmingham, 2014, pp. 328 – 333.

[72] J. L. Shah and J. Parvez, "Evaluation of queuing algorithms on QoS sensitive applications in IPv6 network," in *Proc. Int. Conf. Advances Computing, Commun. and Informatics*, New Delhi, 2014, pp. 106 – 111.

[73] R. A. Rahman, I. M. Ismail and N. Mohd, “Real time interactive learning systems over SSL IPv6 for next generation network,” in *Proc. IEEE 5th Conf. Eng. Educ.*, Kuala Lumpur, 2013, pp. 72 – 77.

[74] A. Mehdizadeh and F. Hashim, “Multicast-unicast key management scheme in IPv6 networks,” *in Proc. IEEE Int. Conf. Commun. Workshops*, Sydney, NSW, 2014, pp. 349 – 354.

[75] J. Prusa,”The role of governments in IPv6 transition,” in *Proc. IST-Africa Conf.*, Le Meridien Ile Maurice, 2014, pp. 1 – 9.

[76] A. Oxley, “Issues affecting the adoption of IPv6,” in *Proc. Int. Conf. Comput. and Inform. Sci.*, Kuala Lumpur, 2012, pp. 1 – 6.

[77] T. Mrugalski, J. Wozniak and K. Nowicki, “Remote stateful autoconfiguration for mobile IPv6 nodes with server side duplicate address detection,” in *Proc. Australasian Telecommun. Networks and Applicat. Conf.*, Auckland, 2010, pp. 141 – 146.

[78] L. F. Rahman, M. B. Reaz and M. Ali, “Beyond the WiFi: Introducing RFID system using IPv6,” in *Proc. Kaleidoscope: Beyond Internet - Innovations Future Networks and Services*, Pune, 2010, pp. 1 – 4.

[79] P. Amr and N. Abdelbaki, “Convergence study of IPv6 tunneling techniques,” in *Proc. 10th Int. Conf. Commun.*, Bucharest, 2014, pp. 1 – 6.

[80] N. Chuangchunsong, T. Kamolphiwong and T. Angchuan, “Performance of intra and inter communications of IPv4-in-IPv6 tunneling mechanism*,”* in *Proc. IEEE Region 10 Conf.*, Bangkok, 2014, pp. 1 – 6,

[81] S. Ziegler, C. Crettaz and I. Thomas, “IPv6 as a global addressing scheme and integrator for the internet of things and the cloud,” in *Proc. 28th Int. Conf. Advanced Inform. Networking and Applicat. Workshops*, Victoria, BC, 2014, pp. 797 – 802.

[82] S. Son, S. Bae, S. Sun and S. Han, “An address management mechanism for blocking external communications in IPv6 networks,” in *Proc. 11th Int. Conf. Elect. Eng.Electron., Comput., Telecommun. and Inform.Technology*, Nakhon Ratchasima, 2014, pp. 1 – 4.

[83] H. Dawood and K. F. Jassim, “Mitigating IPv6 security vulnerabilities,” in *Proc. Int.*

Conf. Advanced Comput. Sc. Applicat. and Technologies, Kuching, 2013, pp. 304 – 309.

[84] S. S. Kolahi, Y. Cao and H. Che, "Evaluation of IPv6 with IPsec in IEEE 802.11n wireless LAN using Fedora 15 operating system," in *Proc. IEEE Symp. Comput. and Commun.*, Split, 2013, pp. 203 – 206.

[85] F. Xiaorong, L. Jun and J. Shizhun, "Security analysis for IPv6 neighbor discovery protocol," in *Proc. 2nd Int. Symp. Instrumentation and Measurement, Sensor Network and Automation,* Toronto, ON, 2013, pp. 303 – 307.

[86] M. Mavani and L. Ragha, "Security implication and detection of threats due to manipulating IPv6 extension headers," in *Proc. Annu. IEEE India Conf.*, Mumbai, 2013, pp. 1 – 6.

[87] R. Duvvuru and S. K. Singh, "Minimizing transmission delay in IPv4 network to IPv6 network through ADSTM," in *Proc. 15th Int. Conf. Advanced Computing Technologies*, Rajampet, 2013, pp. 1 – 5.

[88] J. Domzal, "Flow-aware networking as an architecture for the IPv6 QoS parallel internet," in *Proc. Australasian Telecommun. Networks and Applicat. Conf.*, Christchurch, 2013, pp. 30 – 35.

[89] R. K. Murugesan and A. Osman, "Security mechanism for IPv6 router discovery based on distributed trust management," in *Proc. IEEE Int. Conf. RFID-Technologies and Applicat.,* Johor Bahru, 2013, pp. 1 – 6.

[90] F. Xiaorong, L. Jun and J. Shizhun, "The research on mobile IPv6 security features," in *Proc. IEEE Symp. Wireless Technology and Applicat.*, Kuching, 2013, pp. 125 – 128.

[91] H. Rafiee and C. Meinel, "SSAS: A simple secure addressing scheme for IPv6 auto-configuration," in *Proc. 11th Annu. Int. Conf. Privacy, Security and Trust,* Tarragona, 2013, pp. 275 – 282.

[92] E. Hodzic and S. Mrdovic, "IPv4/IPv6 transition using DNS64/NAT64: deployment issues," in *Proc. 9th Int. Symp. Telecommun.*, Sarajevo, 2012, pp. 1 – 6.

[93] C. Y. Cheng, C. C. Chuang and R. I. Chang, "Lightweight spatial IP address configuration for IPv6-based wireless sensor networks in smart grid," in *Proc. IEEE*

Sensors conf., Taipei, 2012, pp. 1 – 4.

[94] C. Qi and J. Wang, “The research on network communication based on IPV6 technology,” in *Proc. Int. Conf. Comput. Sci. and Service Syst.*, Nanjing, 2012, pp. 635 – 638.

[95] S. Janikowski, J. M. Batalla and M. H. Nowicki, “On extending open source IMS platform for integrated IPTV and VoIP services over IPv6,” in *Proc. 15th Int. Telecommun. Network Strategy and Planning Symp.*, Rome, 2012, pp. 1 – 6.

[96] K. Grgic, D. Zagar and V. Krizanovic, “Security in IPv6-based wireless sensor network - Precision agriculture example,” in *Proc. 12th Int. Conf. Telecommun.*, Zagreb, 2013, pp. 79 – 86.

[97] T. Zseby, “Is IPv6 Ready for the Smart Grid?” in *Proc. Int. Conf. Cyber Security*, Washington, DC, 2012, pp. 157 – 164.

[98] H. Rafiee, M. V. Lowis and C. Meinel, “DNS update extension to IPv6 secure addressing,” in *Proc. 27th Int. Conf. Advanced Inform. Networking and Applicat. Workshops*, Barcelona, 2013, pp. 896 – 902.

[99] D. G. Chandra, M. Kathing and D. P. Kumar, “A comparative study on IPv4 and IPv6,” *in Proc. Int. Conf. Commun. Syst. and Network Technologies,* Gwalior, 2013, pp. 286 – 289.

[100] A. Rosli, W. N. Ali and A. H. Tai, “IPv6 deployment: Security risk assessment using i-SeRP system in enterprise network,” in *Proc. IEEE Student Conf. Research and Develop.*, Pulau Pinang, 2012, pp. 210 – 213.

[101] Q. Li, T. Qin, X. Guan and Q. Zheng, “Empirical analysis and comparison of IPv4-IPv6 traffic: A case study on the campus network,” in *Proc. 18th IEEE Int. Conf. Networks*, Singapore, 2012, pp. 395 – 399.

[102] A. S. Ahmed, R. Hassan and Z. M. Ali, “Eliminate spoofing threat in IPv6 tunnel,” in *Proc. 8th Int. Conf. Inform. Sci.and Digital Content Technology*, Jeju, 2012, pp. 218 – 222.

[103] W. N. Ali, A. H. Taib, N. M. Hussin and J. Othman, “IPv6 attack scenarios testbed,” in *Proc. IEEE Symp. Humanities, Sci. and Eng. Research,* Kuala Lumpur, 2012, pp. 927 – 932.

[104] L. Liu, Y. Cui, J. Sun and Q. Sun, "The research of 4over6 transition system deployment for IPv6 backbone*,"* in *Proc. 2nd Int. Conf. on Comput. Sci. and Network Technology*, Changchun, 2012, pp. 912 – 915.

[105] O. Dobrijevic, V. Svedek and M. Matijasevic, "IPv6 deployment and transition plans in Croatia: Evaluation results and analysis," in *Proc. 20th Int. Conf. Software, Telecommun. and Comput. Networks*, Split, 2012, pp. 1 – 7.

[106] J. Veiga, A. Costa and A. Santos, "Securing anycast communications in IPv6 networks by means of IPSec," in *Proc. 20th Int. Conf. Software, Telecommun. and Comput. Networks*, Split, 2012, pp. 1 – 7.

[107] J. Pieterse and R. Wolhuter, "Investigation of handover techniques in a IPv6 mobile network," in *Proc. IEEE-APS Topical Conf. Antennas and Propagation in Wireless Commun.*, Cape Town, 2012, pp. 1020 – 1023.

[108] Y. Cui, P. Wu, M. Xu, J. Wu, Y. L. Lee, A. Durand and C. Metz, "4over6: Network layer virtualization for IPv4-IPv6 coexistence," *IEEE Network*, vol. 26, no. 5, 2012, pp. 44 – 48,.

[109] H. Rafiee, M. V. Lowis and C. Meinel, "IPv6 deployment and spam challenges*,"* *IEEE Internet Computing*, vol. 16, no. 8, pp. 22 – 29, Nov. 2012.

[110] B. Soorty and N. Sarkar, "Evaluating IPv6 in peer to peer gigabit ethernet for UDP using modern operating systems," in *Proc. IEEE Symp. Comput. and Commun.*, Cappadocia, 2012, pp. 534 – 536.

[111] N. Bahaman, E. Hamid and A. S. Prabuwono, "Network performance evaluation of 6to4 tunneling," in *Proc. Int. Conf. Innovation Manage. and Technology Research*, Malacca, 2012, pp. 263 – 268.

[112] L. Zimu, P. Wei and L. Yujun, "An innovative IPv4-IPv6 transition way for internet service provider," in *Proc. IEEE Symp. Robotics and Applicat.*, Kuala Lumpur, 2012, pp. 672 – 675.

[113] L. Gao, J. Yang, H. Zhang, D. Qin and B. Zhang, "What's going on in Chinese IPv6 world,*" in Proc. IEEE Network Operations and Manage. Symp.*, Maui, HI, 2012, pp. 534 – 537.

[114] J. H. Lee, J. M. Bonnin, I. You and T. M. Chung, "Comparative handover and

performance analysis of IPv6 mobility management protocols," *IEEE Trans. Ind. Electron.,* vol. 60, no. 3, pp. 1077 – 1088, Oct. 2012.

[115] Z. Baig and S. C. Adeniye, "A trust-based mechanism for protecting IPv6 networks against stateless address auto-configuration attacks," *in Proc. 17th IEEE Int. Conf. Networks,* Singapore, 2011, pp. 171 – 176.

[116] H. M. Fahmy and S. Ghoneim, "Performance comparison of wireless networks over IPv6 and IPv4 under several operating systems," *in Proc. IEEE 20th Int. Conf. Electron., Circuits, and Syst.,* Abu Dhabi, 2013, pp. 670 – 673.

[117] N. Chuangchunsong, S. Kamolphiwong and R. Elz, P. Pongpaibool, "Performance evaluation of IPv4/IPv6 transition mechanisms: IPv4-in-IPv6 tunneling techniques," *in Proc. Int. Conf. Inform. Networking,* Phuket, 2014, pp. 238 – 243.

[118] A. K. Tripathi, R. Radhakrishanan and J. S. Lather, "Impact of wireless link delay on handover latency in Mobile IPv6 environment," *in Proc. Int. Conf. Issues and Challenges Intell. Computing Techniques*, Ghaziabad,. 2014, pp. 424 – 428.

[119] D. Plonka and P. Barford, "Assessing performance of internet services on IPv6," *in Proc. IEEE Symp. Comput. and Communi.,* Split, 2013, pp. 820 – 826.

[120] S. Sasanus and K. Kaemarungsi, "Differences in bandwidth requirements of various applications due to IPv6 migration," *in Proc. Int. Conf. Inform. Networking,* Bali, 2012, pp. 462 – 467.

[121] F. Li, C. An, J. Yang, J. Wu and Z. Chen, "Unravel the characteristics and development of current IPv6 network," *in Proc. IEEE 37th Conf. Local Comput. Networks,* Clearwater, FL, 2012, pp. 316 – 319.

[122] S. Kapetanovic and S. Ribic, "The analysis of implementing the IPv6 protocol in Bosnia and Herzegovina," *in Proc. 20th Telecommun. Forum,* Belgrade, 2012, pp. 52 – 55.

[123] Y. Wango, S. Ye and X. Li, "Understanding current IPv6 performance: A measurement study", *in Proc. 10th IEEE Symp. Comput. and Commun.,* Beijing, 2005, pp. 71 – 76.

[124] A. Changqing, J. Yang, J. Wu, H. Zhang and F. Li, "A study of traffic from the perspective of a large pure IPv6 ISP," in *Proc. Comput. Commun.*, 2013, pp. 40 – 52.

[125] S. L. Levin and S. Schmidt, “IPv4 to IPv6: Challenges, solutions, and lessons,” in Proc. *Telecommun. Policy*, 2014, pp. 1059 – 1068.

[126] W. Y. Tai, C. E. Tan and S. P. Lau, “Improving IPv6 wireless ad-hoc networks QoS via enhanced flow label with stability based Dynamic Source Routing scheme,” in *Proc. 17th Asia-Pacific Conf. Commun.*, Sabah, 2011, pp. 643 – 648.

[127] P. Wu, Y. Cui, J. Wu, J. Liu and C. Metz, “Transition from IPv4 to IPv6: A State of the art survey*,” in Proc. IEEE Commun. Surveys and Tutorials,* 2013, pp. 1407 – 1424.

[128] A. P. Castellani, G. Ministeri, M. Rotoloni, L. Vangelista and M. Zorzi, “Interoperable and globally interconnected Smart Grid using IPv6 and 6LoWPAN,” in *Proc. IEEE Int. Conf. Commun.*, Ottawa, ON, 2012, pp. 6473 – 6478.

[129] H. Jiang, Q. Yu and X. Yu, “An improved IPv6 routing lookup algorithm of WSN,” in *Proc. 8th Int. Conf. Fuzzy Syst. and Knowledge Discovery,* Shanghai, 2011, pp. 2234 – 2238.

[130] Y. Wu and X. Zhou, “Research on the IPv6 performance analysis based on dual-protocol stack and tunnel transition,” in *Proc. 6th Int. Conf. Comput. Sci. and Educ.* SuperStar Virgo, Singapore, 2011, pp. 1091 – 1093.

[131] H. Miyata and M. Endo, “Design and evaluation of IPv4/IPv6 Translator for IP based industrial network protocols” *in Proc. 8th IEEE Int. Conf. Ind. Informatics,* 13-1 Osaka, 2010, pp. 142 – 147.

[132] T. Kyantaja, D. Mischler, T. Pfeifer and J. Parkka, “Wireless residential networks based on IPv6”, in *Proc. IEEE J. Commun.*, 2002, pp. 596-600.

[133] S. Papagiannidis, J. Berry and F. Li, “Well beyond streaming video: IPv6 and the next generation television”, in *Proc. Technological Forecasting and Social Change,* 2005, pp. 510–523.

[134] A. Ksentini, “IPv6 over IEEE 802.16 (WIMAX) networks facts and challenges”, in *Proc. J. Commun.*, 2008, pp. 1-9,

[135] J. Wu, J. H. Wang and J. Yang, “Cngi-certnet 2: An IPv6 deployment in China”, in *Proc. ACM Sigcomm Comput. Commun. review,* 2011, pp. 48 – 52.

[136] C. Shengyang and S. Yanlei, “P2P Communication mechanism based on request

forwarding in IPv4 and IPv6 coexistence network," in *Proc. Inte. Conf. e-Educ., e-bus.s, e-Manage. and e-Learning*, vol. 45, no. 1109, 2010, pp. 121 – 125..

[137] B. M. Dorge and T. Scheffler, "Using IPv6 and 6LoWPAN for home automation networks," in *Proc. IEEE Int. Conf. Consumer Electron.*, Berlin, 2011, pp. 44 – 47.

[138] O. J. Parra, A. P. Rios and G. L. Rubio, "Quality of service over IPV6 and IPV4," in *Proc. 7th Int. Conf. Wireless Commun., Networking and Mobile Computing*, Wuhan, 2011, pp. 1 – 4.

[139] G. X. Cao, D. L. Jiang and X. Wang, "The design of embedded IPV4 IPV6 protocol converter based on ARM9," in *Proc. 2nd Int. Conf. Digital Manufacturing and Automation*, Zhangjiajie, Hunan, 2011, pp. 1256 – 1260.

[140] T. Toukabri, M. Tsukada, T. Ernst and L. Bettaieb, "Experimental evaluation of an open source implementation of IPv6 GeoNetworking in VANETs," in *Proc. ITS Telecommun.* Petersburg, 2011, pp. 237 – 245.

[141] M. Zulkiflee, S. A. Azirah, N. Haniza, A. Zakiah and S. Shahrin, "Behavioral analysis on IPv4 malware on different platforms in IPv6 network environment," in *Proc. IEEE Conf. Open Syst.*, Langkawi, 2011, pp. 74 – 79.

[142] A. C. Risdianto and R. Rumani, "IPv6 tunnel broker implementation and analysis for IPv6 and IPv4 interconnection," in *Proc. 6th Int. Conf. Telecommun. Syst., Services, and Applicat.*, Bali, 2011, pp. 139 – 144.

[143] R. C. Welsh. (2013, October 25). *GNS3 Network Simulation Guide.* (1st ed.) [online]. Available: https://ebooks-it.org/1782160809-ebook.htm.

[144] A. Jesin. (2014, January 17). *Packet Tracer Network Simulator*. (1st ed.) [online]. Available: https://reader.bookshout.com.

[145] T. Lammle, "Internet protocol version 6," in *Cisco Certified Network Associate Study Guide*, 6th ed., Indianna, USA: Cisco Press, 2007, pp. 741-755.

ADDENDUM A EIGHT ADDRESS FIELDS OF AN IPV6 PACKET

Version: A field that shows the current IPv6 protocol version.
Class: Contains 8 bits used to determine explicit congestion notification and type of service
Flow label: One of the fields used by the sending device for labelling packets that belong to the same flow. It contains 20 bits.
Payload length: A field of 16 bits that routers use to determine the amount of data in the payload of a packet.
Next header: An 8 bit field that shows the protocol data unit or extension header in the packet.
Hop limit: Field with 8 bits that prevents packets network loops.
Source address: A 128 bit address of the sending device.
Destination address: A 128 bit address of the receiving device.

ADDENDUM B DIFFERENT CLASSES OF IPV6 ADDRESSES

Link local: An interface address configured using the interface identifiers and the prefix FE80::/10. These addresses are used for router communication and other network protocols.
Global unicast: These are public addresses that can be used on the internet. These addresses must be registered with the relevant authority.
Multicast: IPv6 addresses used to send packets to a subset of network hosts at the same time.
Unique local: Addresss synomous with the IPv4 private addresses, these addresses may be used by any organisation without registering them to the relevant authority.
Unicast: IPv6 addresses sent to one host and processed only by that host.
Anycast: These addresses are used to to route packets to the nearest interface of a device.
Loopback address: This is an IPv6 address used to test the protocol stack of a host.
Unspecified address: An IPv6 source address used by a host that does not have the address and is in the process of acquiring one.

ADDENDUM C EXAMPLE OF NEIGHBOUR TABLE FOR EIGRPV6, OSPFV3 AND RIPNG

EIGRPV6 neighbour table

```
MB # show ipv6 eigrp neighbours

IPv6-EIGRP neighbours for process 25

H   Address               Interface      Hold Uptime   SRTT   RTO  Q  Seq

                                    (sec)         (ms)       Cnt Num

2   Link-local address:     Fa2/0             5 00:00:21  152   912  0  53

    FE80::C801:1FFF:FE34:0

1   Link-local address:     Fa1/0            13 00:03:19  189  1134  0  84

    FE80::C803:19FF:FE64:38

0   Link-local address:     Fa1/1            14 00:03:24  196  1176  0  78

    FE80::C804:23FF:FE40:1C
```

OSPFv3 neighbour table

```
MF # show ipv6 ospf neighbour

Neighbour ID    Pri   State          Dead Time   Interface ID    Interface

10.10.10.10      1   FULL/BDR       00:00:35    5            FastEthernet1/0

18.18.18.18      1   FULL/DR        00:00:34    4            FastEthernet0/1

16.16.16.16      1   FULL/DR        00:00:34    9            FastEthernet0/0
```

RIPng database

```
MD # show ipv6 rip database
RIP process "benji", local RIB
 2002:ACE7:2222:1::/64, metric 3, installed
          FastEthernet1/0/FE80::C603:1CFF:FEFC:0, expires in 160 secs
          FastEthernet3/0/FE80::C004:FFF:FED0:10, expires in 158 secs
 2002:ACE7:2222:2::/64, metric 3, installed
          FastEthernet1/0/FE80::C603:1CFF:FEFC:0, expires in 160 secs
          FastEthernet3/0/FE80::C004:FFF:FED0:10, expires in 158 secs
```

ADDENDUM D ROUTER RA FULL RUNNING CONFIGURATION FILE

```
RA # show running-config
Building configuration...
Current configuration : 2600 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RA
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
memory-size iomem 0
archive

log config
hidekeys
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
ip address 172.16.1.2 255.255.255.0
duplex half
ipv6 enable
ipv6 nat
!
interface FastEthernet1/0
no ip address
duplex full
ipv6 address 2002:ACE7:2222:A::A/64
ipv6 nat
ipv6 ospf 15 area 0
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
```

```
speed auto
!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet3/0
no ip address
shutdown
negotiation auto
!
interface Serial4/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial4/1
no ip address
ipv6 address 2002:ACE7:2222:D::A/64
ipv6 ospf 10 area 0
serial restart-delay 0
!
interface Serial4/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial4/3
no ip address
shutdown
serial restart-delay 0
!
interface Serial4/4
no ip address
shutdown
serial restart-delay 0
!
interface Serial4/5
no ip address
shutdown
serial restart-delay 0
!
interface Serial4/6
no ip address
shutdown
serial restart-delay 0
!
interface Serial4/7
no ip address
shutdown
serial restart-delay 0
!
interface Ethernet5/0
no ip address
shutdown
duplex half
!
interface Ethernet5/1
```

```
no ip address
shutdown
duplex half
!
interface Ethernet5/2
 no ip address
 shutdown
 duplex half
!
interface Ethernet5/3
no ip address
shutdown
duplex half
!
!
router ospf 20
log-adjacency-changes
network 172.16.0.0 0.0.255.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
ipv6 nat v4v6 source 172.16.1.1
2002:ACE7:2222:15::20
ipv6 nat v6v4 source
2002:ACE7:2222:A::F 172.16.1.50
ipv6 nat prefix 2002:ACE7:2222::/96
ipv6 router ospf 15
router-id 20.20.20.20
log-adjacency-changes
redistribute connected metric 3
!
ipv6 router ospf 10
router-id 10.10.10.10
log-adjacency-changes
!
control-plane
!
mgcp fax t38 ecm
!
gatekeeper
 shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
end
```

```
!
RA#
!
!
```

ADDENDUM E COMMANDS REQUIRED TO CONFIGURE STATIC IPV6 ADDRESSES

Router RA

```
RA > enable
RA # configure terminal
RA (config) # ipv6 unicast-routing
RA (config) # interface fastethernet 0/0
RA (config-if) # ipv6 address 2002:ACE7:2222:0002::A/64
RA (config-if) # no shutdown
RA (config) # interface fastethernet 1/0
RA (config-if) # ipv6 address 2002:ACE7:2222:000A::A/64
RA (config-if) # no shutdown
RA (config) # interface serial 4/1
RA (config-if) # ipv6 address 2002:ACE7:2222:000D::A/64
RA (config-if) # no shutdown
RA (config-if) # end
RA # copy running-config startup-config
```

Multilayer switch MB

```
MB > enable
MB # configure terminal
MB (config) # ipv6 unicast-routing
MB (config) # interface fastethernet 0/0
MB (config-if) # ipv6 address 2002:ACE7:2222:0001::B/64
MB (config-if) # no shutdown
MB (config-if) # interface fastethernet 2/0
MB (config-if) # ipv6 address 2002:ACE7:2222:0002::B/64
MB (config-if) # no shutdown
MB (config-if) # interface fastethernet 1/0
MB (config-if) # ipv6 address 2002:ACE7:2222:0004::B/64
MB (config-if) # no shutdown
MB (config-if) # interface fastethernet 1/1
MB (config-if) # ipv6 address 2002:ACE7:2222:0006::B/64
MB (config-if) # no shutdown
MB (config-if) # end
MB # copy running-config startup-config
```

ADDENDUM F COMMANDS REQUIRED TO AUTOCONFIGURE IPV6 ADDRESSES

Process of configuring SLAAC addresses

```
RA > enable
RA # configure terminal
RA (config) # ipv6 unicast-routing
RA (config) # interface fastethernet 0/0
RA (config-if) # ipv6 address autoconfig
RA (config-if) # no shutdown
RA (config) # interface fastethernet 1/0
RA (config-if) # ipv6 address autoconfig
RA (config-if) # no shutdown
RA (config) # interface serial 4/1
RA (config-if) # ipv6 address autoconfig
RA (config-if) # no shutdown
RA (config-if) # end
RA # copy running-config startup-config
MB > enable
MB # configure terminal
MB (config) # ipv6 unicast-routing
MB (config) # interface fastethernet 0/0
MB (config-if) # ipv6 address autoconfig
MB (config-if) # no shutdown
MB (config-if) # interface fastethernet 2/0
MB (config-if) # ipv6 address autoconfig
MB (config-if) # no shutdown
MB (config-if) # interface fastethernet 1/0
MB (config-if) # ipv6 address autoconfig
MB (config-if) # no shutdown
MB (config-if) # interface fastethernet 1/1
MB (config-if) # ipv6 address autoconfig
MB (config-if) # no shutdown
MB (config-if) # end
MB # copy running-config startup-config
```

Extended unique identifier configuration process

```
RG > enable
RG # configure terminal
RG (config) # ipv6 unicast-routing
RG (config) # interface fastethernet 2/0
RG (config-if) # ipv6 address 2002:ACE7:2222:000B::/64 eui-64
RG (config) # interface fastethernet 0/0
RG (config-if) # ipv6 address 2002:ACE7:2222:000C::/64 eui-64
RG (config) # interface fastethernet 1/0
RG (config-if) # ipv6 address 2002:ACE7:2222:000F::/64 eui-64
RG (config) # interface serial 4/1
RG (config-if) # ipv6 address 2002:ACE7:2222:0011::/64 eui-64
RG (config-if) # end
RG # copy running-config startup-config
```

ADDENDUM G COMMANDS REQUIRED TO CONFIGURE STATIC IPV6 ROUTING

Configurations for router RA

```
RA > enable
RA # configure terminal
RA (config) # ipv6 route 2002:ACE7:2222:0001::/64 2002:ACE7:2222:0002::B
RA (config) # ipv6 route 2002:ACE7:2222:0004::/64 2002:ACE7:2222:0002::B
RA (config) # ipv6 route 2002:ACE7:2222:0006::/64 2002:ACE7:2222:0002::B
RA (config) # ipv6 route 2002:ACE7:2222:0007::/64 2002:ACE7:2222:0002::B
RA (config) # ipv6 route 2002:ACE7:2222:000B::/64 fastethernet 1/0
RA (config) # ipv6 route 2002:ACE7:2222:000C::/64 fastethernet 1/0
RA (config) # ipv6 route 2002:ACE7:2222:000E::/64 fastethernet 1/0
RA (config) # ipv6 route 2002:ACE7:2222:000F::/64 fastethernet 1/0
RA (config) # ipv6 route 2002:ACE7:2222:0003::/64 fastethernet 0/0
RA (config) # ipv6 route 2002:ACE7:2222:0005::/64 fastethernet 0/0
RA (config) # ipv6 route 2002:ACE7:2222:0008::/64 fastethernet 0/0
RA (config) # ipv6 route 2002:ACE7:2222:0009::/64 fastethernet 0/0
RA (config) # ipv6 route 2002:ACE7:2222:0010::/64 fastethernet 1/0
RA (config) # ipv6 route 2002:ACE7:2222:0011::/64 fastethernet 1/0
RA (config) # ipv6 route 2002:ACE7:2222:0012::/64 fastethernet 1/0
RA (config) # ipv6 route 2002:ACE7:2222:0013::/64 fastethernet 1/0
RA (config) # end
RA # copy running-config startup-config
```

ADDENDUM H COMMANDS REQUIRED TO CONFIGURE RIPng, EIGRPv6 AND OSPFv3

RIPng configurations for router RA and multilayer switch MB

```
RA > enable                                    MB > enable
RA # configure terminal                        MB # configure terminal
RA (config) # ipv6 unicast-routing             MB (config) # ipv6 unicast-routing
RA (config) # ipv6 router rip benji            MB (config) # ipv6 router rip benji
RA (config) # interface fastethernet 0/0       MB (config) # interface fastethernet 0/0
RA (config-if) # ipv6 rip benji enable         MB (config-if) # ipv6 rip benji enable
RA (config-if) # interface fastethernet 1/0    MB (config-if) # interface fastethernet 1/0
RA (config-if) # ipv6 rip benji enable         MB (config-if) # ipv6 rip benji enable
RA (config-if) # interface serial 4/1          MB (config-if) # interface fastethernet 2/0
RA (config-if) # ipv6 rip benji enable         MB (config-if) # interface fastethernet 1/1
RA (config-if) # end                           MB (config-if) # ipv6 rip benji enable
RA # copy running-config startup-config        MB (config-if) # end
RA #                                           MB # copy running-config startup-config
```

EIGRPv6 configurations for router RA and multilayer switch MB

```
RA > enable                                    MB > enable
RA # configure terminal                        MB # configure terminal
RA (config) # ipv6 unicast-routing             MB (config) # ipv6 unicast-routing
RA (config) # ipv6 router eigrp 20             MB (config) # ipv6 router eigrp 20
RA (config) # router-id 11.11.11.11            MB (config) # router-id 12.12.12.12
RA (config) # no shutdown                      MB (config) # no shutdown
RA (config) # interface fastethernet 0/0       MB (config) # interface fastethernet 0/0
RA (config-if) # ipv6 eigrp 20                 MB (config-if) # ipv6 eigrp 20
RA (config-if) # interface fastethernet 1/0    MB (config-if) # interface fastethernet 1/0
RA (config-if) # ipv6 eigrp 20                 MB (config-if) # ipv6 eigrp 20
RA (config-if) # interface serial 4/1        MB (config-if) # interface fastethernet 2/0
RA (config-if) # ipv6 eigrp 20               MB (config-if) # ipv6 eigrp 20
RA (config-if) # end                         MB (config-if) # interface fastethernet 1/1
RA # copy running-config startup-config      MB (config-if) # ipv6 eigrp 20
RA #                                         MB # copy running-config startup-config
```

OSPFv3 configurations for router RA and multilayer switch MB

```
RA > enable                                  MB > enable
RA # configure terminal                      MB # configure terminal
RA (config) # ipv6 unicast-routing           MB (config) # ipv6 unicast-routing
RA (config) # ipv6 router ospf 10            MB (config) # ipv6 router ospf 11
RA (config-rtr) # router-id 10.10.10.10      MB (config-rtr) # router-id 11.11.11.11
RA (config-rtr) # exit                       MB (config-rtr) # exit
RA (config) # interface fastethernet 0/0     MB (config) # interface fastethernet 0/0
RA (config-if) # ipv6 ospf 10 area 0         MB (config-if) # ipv6 ospf 11 area 0
RA (config-if) # interface fastethernet 1/0  MB (config-if) # interface fastethernet 1/0
RA (config-if) # ipv6 ospf 10 area 0         MB (config-if) # ipv6 ospf 11 area 0
RA (config-if) # interface serial 4/1        MB (config-if) # interface fastethernet 1/1
RA (config-if) # ipv6 ospf 10 area 0         MB (config-if) # ipv6 ospf 11 area 0
RA (config-if) # end                         MB (config-if) # interface fastethernet 2/0
RA # copy running-config startup-config      MB (config-if) # ipv6 ospf 11 area 0
RA #                                         MB # copy running-config startup-config
```

ADDENDUM I COMMANDS REQUIRED TO CONFIGURE IPv6 TRANSITION TECHNIQUES

Dual stack

```
RA > enable
RA # configure terminal
RA (config) # interface fastethernet 0/0
RA (config-if) # ip address 172.16.1.2 255.255.255.0
RA (config-if) # ipv6 address 2002:ACE7:2222:0002::A/64
RA (config-if) # interface fastethernet 1/0
RA (config-if) # ip address 172.16.10.2 255.255.255.0
RA (config-if) # ipv6 address 2002:ACE7:2222:000A::A/64
RA (config-if) # interface serial 4/1
RA (config-if) # ip address 172.16.19.2 255.255.255.0
RA (config-if) # ipv6 address 2002:ACE7:2222:000D::A/64
RA (config) # router ospf 21
RA (config-router) # network 172.16.0.0 0.0.255.255 area 0
RA (config-router) # end
RA # copy running-config startup-config
```

Manual IPv6 tunnelling technique

```
RA > enable
RA # configure terminal
RA (config) # interface tunnel 12
RA (config-if) # no ip address
RA (config-if) # ipv6 address 2002:ACE7:2222:0014::1/64
RA (config-if) # tunnel source 172.16.6.1
RA (config-if) # tunnel destination 172.16.7.1
RA (config-if) # tunnel mode ipv6ip
RA (config-if) # end
RA (config) # router rip
RA (config-router) # network 172.16.0.0
RA # copy running-config startup-config
```

```
RB > enable
RB # configure terminal
RB (config) # interface tunnel 12
RB (config-if) # no ip address
RB (config-if) # ipv6 address 2002:ACE7:2222:0014::2/64
RB (config-if) # tunnel source 172.16.7.1
RB (config-if) # tunnel destination 172.16.6.1
RB (config-if) # tunnel mode ipv6ip
RB (config-if) # end
RB (config) # router rip
RB (config-router) # network 172.16.0.0
RB # copy running-config startup-config
```

Generic routing encapsulation IPv6 tunnelling technique

```
RA > enable
RA # configure terminal
RA (config) # interface tunnel 12
RA (config-if) # no ip address
RA (config-if) # ipv6 address 2002:ACE7:2222:0014::1/64
RA (config-if) # tunnel source 172.16.6.1
RA (config-if) # tunnel destination 172.16.7.1
RA (config-if) # end
RA (config) # router rip
RA (config-router) # network 172.16.0.0
RA # copy running-config startup-config
RB > enable
RB # configure terminal
RB (config) # interface tunnel 12
RB (config-if) # no ip address
RB (config-if) # ipv6 address 2002:ACE7:2222:0014::2/64
RB (config-if) # tunnel source 172.16.7.1
RB (config-if) # tunnel destination 172.16.6.1
RB (config-if) # end
RB (config) # router rip
RB (config-router) # network 172.16.0.0
RB # copy running-config startup-config
```

Intra-site automatic tunnel addressing protocol transition technique

```
RA > enable
RA # configure terminal
RA (config) # interface tunnel RA-RB
RA (config-if) # ipv6 address 13:13::/64 eui-64
RA (config-if) # tunnel source 172.16.8.1
RA (config-if) # tunnel mode ipv6ip isatap
RA (config-if) # end
RA # copy running-config startup-config

RB > enable
RB # configure terminal
RB (config) # interface tunnel RA-RB
RB (config) # ipv6 address 14:14::/64 eui-64
RB (config-if) # tunnel source 172.16.9.1
RB (config-if) # tunnel mode ipv6ip isatap
RB (config-if) # end
RB # copy running-config startup-config
```

Static network address translation-protocol translation technique

```
RA > enable
RA # configure terminal
RA (config) # interface fasethernet 0/0
RA (config) # ipv6 nat
RA (config) # interface fasethernet 1/0
RA (config) # ipv6 nat
RA (config) # ipv6 nat v4v6 source 172.16.1.1 2003::20
RA (config) # ipv6 nat v6v4 source 2002:ACE7:2222:A::F 172.16.1.20
RA (config) # ipv6 nat prefix 2003::/96
RA (config) # ipv6 router ospf 10
RA (config-rtr) # redistribute connected metric 3
RA (config) #end
RA # copy running-config startup-config
```

ADDENDUM J COMMANDS REQUIRED TO CONFIGURE HOT STANDBY ROUTER PROTOCOL VERSION 2

```
Router RG
RG > enable
RG # configure terminal
RG (config) # interface fastethernet 2/1
RG (config-if) # ipv6 address 2002:ACE7:2222:0011::/64 eui-64
RG (config-if) # no shutdown
RG (config-if) # standby version 2
RG (config-if) # standby 10 ipv6 autoconfig
RG (config-if) # standby 10 priority 155
RG (config-if) # standby 10 preempt delay minimum 20
RG (config-if) #end
RG # copy running-config startup-config
```

```
Router RH
RH > enable
RH # configure terminal
RH (config) # interface fastethernet 3/0
RH (config-if) # ipv6 address 2002:ACE7:2222:0012::/64 eui-64
RH (config-if) # no shutdown
RH (config-if) # standby version 2
RH (config-if) # standby 10 ipv6 autoconfig
RH (config-if) # standby 10 priority 130
RH (config-if) # standby 10 preempt delay minimum 20
RH (config-if) #end
RH # copy running-config startup-config
```