Maryam Tavakoli Momtaz
Michael Swanson

IPv4 to IPv6 Transition and Security

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Thesis

11 November 2015

Author(s) Title Number of Pages Date	Maryam Tavakoli Momtaz Michael Swanson IPv4 to IPv6 Transition and Security 89 pages + 7 appendices 11 November 2015
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Networking
Instructor(s)	Sami Sainio, Supervisor Erik Pätynen, Senior Lecturer

This document is intended for the use of network administrators and people with a knowledge of networking. It aims to provide guidelines for people intending to migrate to IPv6. The practical implementation can be used in a production environment.

The goal of the project was to implement and transition from IPv4 to IPv6 in a small to medium size network using the best current practices and security. Due to the exhaustion of IPv4 addresses, migration to IPv6 has become a necessity. A native IPv6 network will be time-consuming and expensive to implement, due to the expertise required and the necessity of IPv6 compatible devices.

Security is a vital aspect of the migration process. Due to the unique structure of the IPv6 protocol, new attacks and security concerns arise and some IPv4 attacks still exist. This project evaluated and provided security considerations for the secure deployment of an IPv6 network including extension header threats, first-hop security concerns and IPsec.

Transition mechanisms allow enterprises to adapt to IPv6 while maintaining an existing IPv4 network. This gradual migration minimises the network disruption, as well as offers considerable benefits, such as cost and time-efficiency, scalability and simpler deployment. During this project, two of the most commonly used methods, dual-stacking and tunnelling, were implemented and tested in a laboratory environment. This project was carried out using Cisco routers and switches, and for the end terminals, Windows desktop computers were used.

The project resulted in the creation of two redundant networks, with two completely different transition mechanisms, dual-stack and tunnelling. For each mechanism, various tests and experiments were conducted in order to study the networks performance and to gain a deeper knowledge of the technologies in use.

Keywords	IPv4, IPv6, transition mechanisms, dual-stack, tunnel, security, migration

Acknowledgements

We would like to express our appreciation to the following people for their contribution and significant help in writing this thesis.

To Sami Sainio, Erik Pätynen and Heikki Rahkonen for their intellectual contribution as well as support, insight and advice.

In addition to Sami Sainio and Erik Pätynen for their supervision, reading and correction of this thesis.

A special thanks to Taru Sotavalta for proofreading and her constructive criticism of this thesis.

Finally to the Helsinki Metropolia University of Applied Sciences for providing us with the opportunity of studying as well as affording us the facilities.

Abbreviations

ACL	Access Control List
AFRINIC	African Internet Numbers Registry
AH	Authentication Header
ARIN	American Registry for Internet Numbers
AS	Autonomous System
BCP	Best Current Practice
BGP	Border Gate Protocol
CW	Company West
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
EH	Extension Header
ESP	Encapsulation Security Payload
EUI	Extended Unique Identity
FHS	First Hop Security
Gi	Gigabit Ethernet Interface
GRE	Generic Routing Encapsulation
HbH	Hop-by-Hop
HQ	Headquarters
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocols
IKE	Internet Key Exchange
IOS	Internetwork Operating System
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6

ISAKMP	Internet Security Association Management Protocol
ISP	Internet Service Provider
Lab	Laboratory
Lo	Loopback
LSA	Link-State Advertisement
MAC	Media Access Control
MH	Main Header
MI	Malicious Intruder
MITM	Man In The Middle
NAT	Network Address Translation
NAT-PT	Network Address Translation - Protocol Translation
ND	Neighbor Discovery
NDP	Neighbor Discovery Protocol
NS	Neighbor Solicitation
OSPF	Open Shortest Path First
PC	Personal Computer
QoS	Quality of Service
RA	Router Advertisement
RFC	Request for Comments
RH	Routing Header
RIR	Regional Internet Registry
RS	Router Solicitation
RSA	Rivest, Shamir, and Adelman
SA	Security Association
SLAAC	Stateless Address Autoconfiguration
SPF	Shortest Path First
TLV	Type Length Value
ULA	Unique Local Address
Unicast RPF	Unicast Reverse Path Forwarding
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

Contents

Appendices

1 Introduction

The Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol. It provides an identification and location system for computers on networks and is used to route traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) as replacement for Internet Protocol version 4 (IPv4). This deals with the long-anticipated problem of address exhaustion and the finite number of Autonomous System (AS) numbers. Based on RFC 6996, the majority of private use AS numbers have already been deployed.

The choice of this project is due to the fact that the transitioning between IPv4 and IPv6 is currently high on the agenda for many organisations and governments. In comparison to IPv4, IPv6 is evolving and therefore there is limited experience of IPv6 networks. At present, the transition between protocols is an ongoing process and therefore realistic scenarios were chosen for this project.

The client, Company West (CW), is a fictitious company existing only in the laboratory (Lab) environment. The company, although limited in network size, encompasses many of the characteristics of a real organisation and the problems faced are identical. The aim of this project is to implement two common transition scenarios when transitioning to IPv6 while maintaining parts of the enterprise network as IPv4.

During the implementation, dual-stack mechanisms, where the Internet Service Provider (ISP) will be dual-stacked to provide connectivity to the IPv6 network, and IPv6 tunnelling, which allows IPv6 domains to connect over an IPv4 ISP, will be implemented. Some security aspects of the IPv6 protocol will be implemented and evaluated as well. [1.]

2 Theoretical Background

The number of individual users on the Internet is expanding at a significant rate. Comparing the total number of individual Internet users in 2005 (2048 million) to 2014 (5846 million), shows a growth of 3799 million new individual Internet users. This shows an increase of close to 4 billion new users in ten years as illustrated in figure 1.

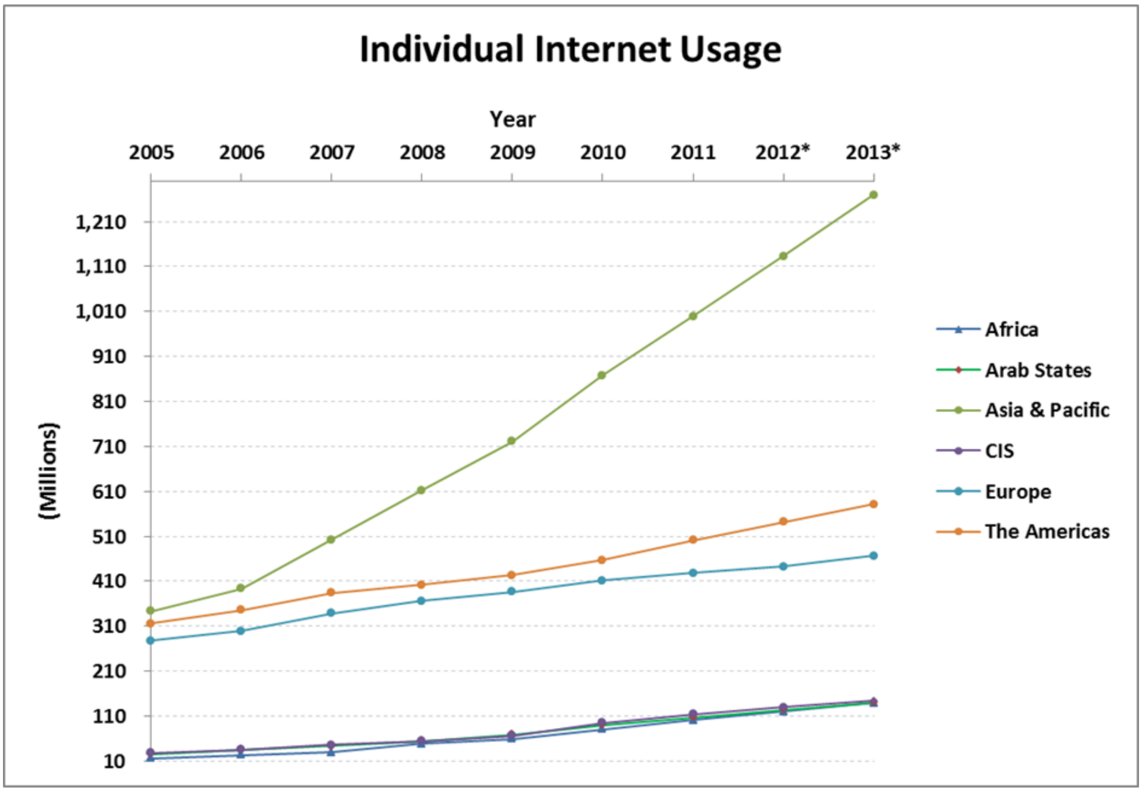


Figure 1. Individual Internet Usage (* Estimated) [2].

The Internet growth has been especially significant in the developing countries as can be seen in figure 1. As approximately two thirds of today's Internet users live in developing countries, a higher growth rate is expected with the expanding mobile-broadband access. [2]

On 3rd February 2011, the Internet Assigned Numbers Authority (IANA), the body responsible for the global coordination of the Domain Name System (DNS) Root, IP addressing and other Internet protocol resources, allocated the last of the /8 address blocks to each of the Regional Internet Registries (RIR). Of the five RIR's, only the American Registry of Internet Numbers (ARIN) and the African Internet Numbers Registry (AfriNIC) have any addresses left, with ARIN expecting to run out of addresses in May 2015 and AfriNIC expecting to run out in the next few years. [3]

On 20th May 2014, the Internet Corporation for Assigned Names and Numbers (ICANN), began the process of allocating the remaining blocks of IPv4 addresses to the five RIR's. These are from the IANA IPv4 Recovered Address Space registry. Due to the existing IPv4 addressing scheme exhaustion and in order to accommodate the significant increase in usage, the need to move to IPv6 has become essential.

The IPv4 and IPv6 protocols are designed for Internet communication and share many similarities, there are however some differences between these two protocols which are discussed in more detail in section 2.1. [4]

2.1 An Overview of IPv6

2.1.1 The IPv6 Address Structure and Header

IPv6 uses a 128-bit address, illustrated in figure 2 and provides a large address space of approximately 7.9×10^{28} times as many as IPv4. IPv4 as illustrated in figure 3, uses a 32-bit address and provides approximately 4.3 billion addresses.

2001:0db8:0000:0000:0000:0000:0000:0001

Figure 2. IPv6 128 Bit Address

Comparisons between the 128 bit address format that is required for the IPv6 protocol and a typical 32 bit address format of an IPv4 address are demonstrated in figure 2 and figure 3.

192.168.100.125

Figure 3. IPv4 32 Bit Address

The IPv6 header consists of two parts, the main header (MH) and the extension header (EH). The MH is same as the IPv4 header but with some improvements to enhance performance. The similarities and differences between these two protocol headers is illustrated in figure 4.

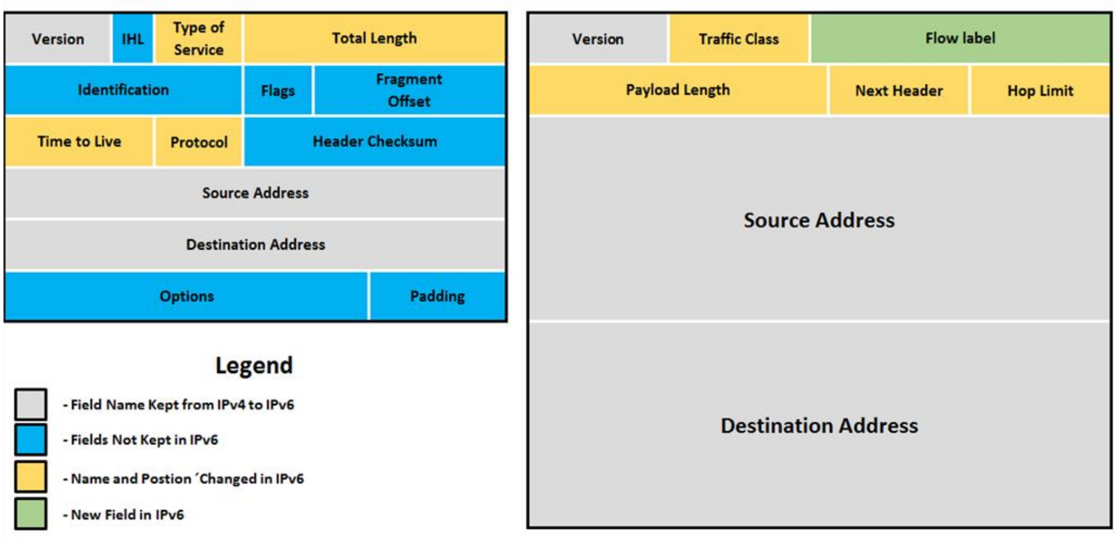


Figure 4. Differences between IPv4 and IPv6 Headers

As shown in figure 4, it is clear that the IPv6 header is more streamlined. The separate IPv6 EH is between the IPv6 Header and the Upper Layer Header and can travel completely unchecked along a route, until the packet reaches the destination. The Hop-by-Hop header, an EH, is the one exception to this. [1.]

2.1.2 IPv6 Enhanced Features

The IPv4 address depletion was not the only reason for the design of IPv6, but it was also to overcome other issues associated with IPv4. The Public-to-Private Network Address Translation (NAT) was developed as a solution for the limited number of IPv4 addresses. IPv6 eliminates the need for NAT due to the much larger address pool. Unlike IPv4, IPv6 does not have broadcast addresses. Instead it has unicast, multicast and anycast addresses.

IPv6 improves router efficiency by using a simplified header that includes

- Routing efficiency for performance and forwarding-rate scalability
- No requirement for processing checksums
- Simpler and more efficient EH mechanisms
- Flow labels for per-flow processing
- No need to examine transport layer information to identify the various traffic flows.

Another significant advantage of IPv6 over IPv4 is mobility and security. The mobile IP is an IETF standard that enables users to move around in a network without a break in connectivity. The mobile IP is available for both IPv4 and IPv6. However IPv4 requires additional configuration as it is not configured automatically. In IPv6, mobility is a built-in feature which makes it more efficient for end-users. [5,693.]

The IPv6 address has some unique features that add to its flexibility, including the following:

- Stateless Address Autoconfiguration (SLAAC), which includes the device’s data link layer address to IPv6 address.
- Prefix renumbering, where the router advertises the new prefix and the other devices in the network can begin to use it. This mechanism simplifies address and prefix renumbering.
- Multi address per interface of various types that they run simultaneously.
- Link local address will automatically be created on each interface. One of the uses is in the Interior Gateway Protocol (IGP) as the next hop address when exchanging routing updates.

Provider-dependent or provider-independent addressing that allows enterprises to choose to use addresses from the ISP or their own provider-independent addressing space. [5,694.]

2.1.3 IPv6 Address Types

There are three types of IPv6 addresses, unicast, anycast and multicast and each of these individual types is identified by the first bits in the left hand side of the address. Important to note is the 0:0:0:0:0:0:0:0 address, the unspecified address, which may never be assigned to any node and signifies the absence of an address.

- Unicast is used for a single interface, similar to an IPv4 address. A packet sent to a unicast address is delivered to the interface with the specified address. It encompasses the entire IPv6 address range, with the exception of the FF00::/8 range, which is used for multicast addresses. There are multiple types of unicast addresses including, global unicast, link-local and unique local. The following figure 5 demonstrates the scope of different unicast addresses.

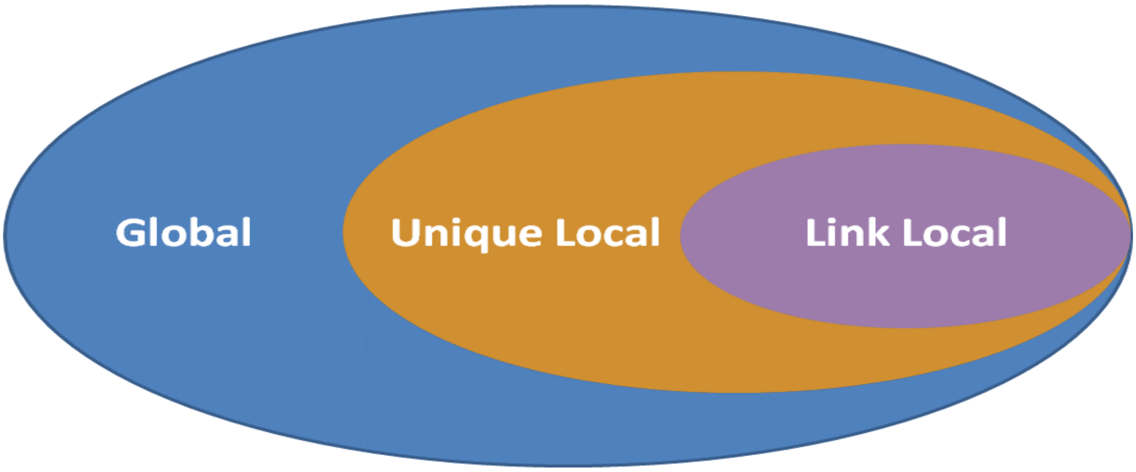


Figure 5. Scope of Different Unicast Addresses

As demonstrated in figure 5 above, global unicast addresses are globally routable on the public Internet. Unique local addresses (ULA) are for communication within a site and routable to multiple local networks, but they are not globally routable. Link local addresses are private addresses that are not globally routable.

- Multicast identifies a group of different device interfaces. Packets to multicast are delivered to the interface group using a multicast address for identification.
- Anycast identifies a group of different device interfaces. Packets to anycast are delivered to the closest interface using a anycast address for identification and therefore the interface group provides a uniform service. [5,704-705;6.]

2.1.4 IPv6 Routing Protocols

Prior to configuring any IPv6 routing protocol, IPv6 routing needs to be enabled using the Cisco Internetwork Operating System (IOS) IPv6 unicast-routing command, in global configuration mode.

Static routes in IPv6 are configured and used in the same way as in IPv4. An example of where static routes can be used, is in connecting the headquarters (HQ) to a Branch Office to avoid unnecessary routing overhead.

The IGP is used for routing within an AS. One of the most commonly used IGP’s in IP networking is Open Shortest Path First (OSPF). OSPFv3 is the new protocol implementation for IPv6. Most of the algorithms in OSPFv2 and OSPFv3 are similar, but changes were made in OSPFv3 to handle the larger address space of IPv6. Although the general mechanism is the same in both versions, the internals of the protocol are different in OSPFv3. OSPFv2 and OSPFv3 run independently of each other, that is, if they are both configured on the same router, they each run a separate shortest path first (SPF) instance. Some of the IPv6 specific features of OSPFv3 include:

- Using a link local address as the source address
- Allowing multiple addresses and OSPF instances per interface
- Supporting authentication
- Running over a link rather than a subnet
- Removing every OSPFv2 IPv4-specific semantic

When configuring OSPFv3 for an internal network, it is important to understand how it differs from OSPFv2 and the differences in the configuration. As OSPFv2 was designed to support the IPv4 address family and OSPFv3 can support both or either, there are differences when configuring OSPF on a Cisco IOS router for IPv4 as opposed to IPv6. For example, OSPFv3 has fewer commands under the routing protocol but there are more configurations that are configured under the interface, such as the type of the interface and the area.

Other notable changes, are that for IPv6, all the show commands with the keyword IP in them, are replaced with IPv6 and the OSPF keyword with OSPFv3. The biggest change in configuration is in the address-family structure, both the IPv4 and IPv6 address-families are configured under router OSPFv3. However only the IPv4 address family is configured under OSPFv3, after all of the interfaces are configured with IPv4, they should only then, be IPv6-enabled. This feature allows an interface to have multiple router processes, but only one process per address family. [5,747-772;7;8;9.]

2.2 Transitioning To IPv6

2.2.1 Preliminary Transition Considerations

Due to the complexity and the cost involved in fully transitioning an existing IPv4 network to IPv6, various methods have been developed in order to minimize the disruption and cost. The costs involved in deploying IPv6 depends upon various factors including the number of products, applications and deployment strategy. Fixed costs include training and personnel while variable costs can be dependent on expertise, network devices and IPv6-compatible applications.

Multiple factors need to be taken into consideration prior to transition a network to IPv6. Once the preliminary preparation for transition has been completed, a decision needs to be made as to which mechanisms will be utilised to achieve the desired goal. The Best current practice (BCP) recommends that the way forward is to use dual-stack mechanisms when the ISP is able to provide IPv6 addresses and connectivity. However in the case of the ISP being unable to provide IPv6, tunnelling needs to be used. Where companies have an existing IPv4 network that works perfectly, investing in a completely new IPv6 network would cause major disruption as well as significant costs incurred in the investment of new devices. Using a transition mechanism, enables retaining the existing structure to utilise IPv6. In effect, this means that as components need to be replaced, they can be upgraded to IPv6 compliancy.

It is the companies' responsibility to contact their ISP and discover what their current and planned support for IPv6 is. It is important to have a list of the required services and items when negotiating with ISPs. There are many considerations to take into account, such as

- support for Border Gate Protocol (BGP) peering over IPv6
- maximum accepted prefix by ISP
- support for dual-stack
- any additional costs for IPv6 services
- performance and support for IPv6. [11]

This is a brief list of items that need to be considered when transitioning. Some of the ISPs do not yet have native IPv6 and they are only able to provide the necessary support by providing a separate circuit or a tunnel interface. After contacting the ISP and obtaining the IPv6 addresses, the next step is to evaluate the current network devices. It is important to do a thorough audit of the platforms and associated software and to check their support for IPv6. After ensuring the ISP is able to offer dual-stack support and that all the necessary software and hardware supports IPv6, with the necessary expertise and time, dual-stack is the best approach and the most practised method. In situations where the ISP is not able to give the needed support for IPv6, there are alternative methods to explore such as tunnelling. [10;11.]

2.2.2 Dual-Stack Mechanism

Dual-stack is one of the primary and most often used methods that makes transition to IPv6 possible. In dual-stack, the stacks can be on either multiple interfaces or the same interface and each node has both IPv4 and IPv6 connectivity. The node decides where the packet is destined for, dependent upon the destination address of the packet.

Dual-stack is one of the most commonly used methods because it allows the existing IPv4 application to continue running as before, while IPv6 will be added without causing any disruption to the existing network. As soon as IPv4 and IPv6 configurations are completed on an interface, the interface is dual-stacked and starts forwarding both IPv4 and IPv6 traffic.

A drawback of dual-stack, is the resources that each device requires for each protocol. The device processes each protocol independently and must keep a record of dual routing protocols, routing protocol topology tables. There is also increased administrative complexity such as troubleshooting and monitoring.

2.2.3 Tunnelling Mechanism

Tunnels are often used to overcome the incompatibility of the underlying network to support the required services. For IPv6, tunnelling is one of the migration methods, allowing for IPv6 network connectivity without the need to convert the intermediary network to IPv6. This is ideal in the situation where the ISP is not IPv6-enabled. This concept is more clearly demonstrated in figure 6.

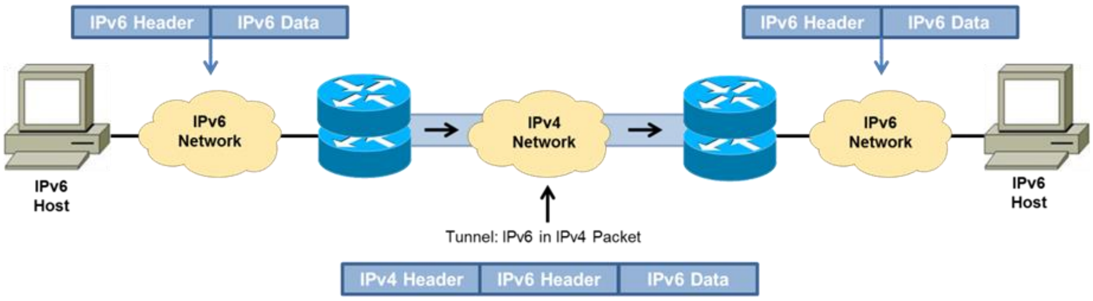


Figure 6. IPv6 Packets Inside IPv4 Packets

As shown in figure 6, an IPv4 network is the intermediary network between two IPv6 sites. In order to have connectivity between the sites, a tunnel is configured. The connection is achieved by allowing IPv6 packets to be encapsulated inside IPv4 packets.

The GRE protocol is a tunnelling protocol developed by Cisco Systems, and is the default tunnelling protocol on Cisco routers. The GRE protocol allows for several different network layer protocols. Packets are sent through a virtual point-to-point tunnel link. The tunnel interfaces for the IPv6 configuration, are manually created and each interface is configured with an IPv6 address manually and do not have an IPv4 address. The tunnel uses a physical interface to route the traffic and this physical interface has an IPv4 address. The BCP is to use a loopback interface for the tunnel source and destination, as it only goes down if the router goes down. This increases the stability of the tunnel as a real physical interface can go down for various reasons, such as physical failure or data link layer problems. The loopback with an IPv4 address should be reachable from any point within the network. Figure 7 illustrates the concept of a tunnel interface running over a physical interface.

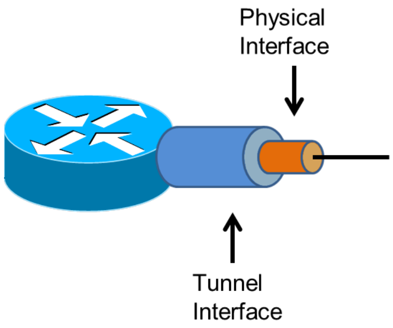


Figure 7. Tunnel Interface Running Over a Physical Interface

Using figure 7 as an example, the concept remains the same when using the loopback interface for the tunnel instead of the physical interface.

It is important to note that, the GRE protocol tunnel does not encrypt the data, and the data travels through the tunnel in clear text. To assure the confidentiality and integrity of data, a security mechanism such as Internet Protocol Security (IPsec) needs to be implemented. The GRE protocol over an IPsec tunnel supports multicast IPv6 traffic and encrypts the data. [5,826-845.]

3 Materials and Methods

3.1 Existing Operational Environment

CW represents an enterprise transitioning to IPv6. The company network is being implemented in a controlled lab environment and is currently running IPv4. The company HQ is connected to the Finance branch over the Internet. For the purposes of redundancy and to increase the reliability of the Internet connection, HQ is connected to the Internet using two different ISPs. This is called multihomed ISP connectivity, with redundancy built into the design, and is therefore resistant to a single ISP failure. The route to ISP1 is selected as the primary route with a metric of 210 and the route to ISP2 as a back-up route with a metric of 220. In the event of the failure of the link to ISP1, the network traffic will automatically be routed via ISP2.

The internal network of the company runs the OSPFv2 protocol. HQ is connected to the OSPF area 0 backbone and the site Finance to OSPF area 1. The network has been logically segmented into Virtual Local Area Networks (VLAN's), with VLAN 10 for users at HQ and VLAN 20 for users of the Finance site. Each access layer switch has a separate VLAN 99 configured for management and is assigned an IP address. Certain network security measures were implemented as a baseline on all devices. Password protection was enabled on all telnet and console connections. Switches are protected against Media Access Control (MAC) flooding or a spoofing attack, port security is configured on the VLAN 10 and VLAN 20 access ports.

Most of the users in HQ use desktop workstations and the MAC addresses do not change very often. Therefore VLAN 10 is configured with sticky learning. Each port on this VLAN allows for a maximum of two MAC addresses to be dynamically learned. In VLAN 20, the users have more mobile devices such as laptops and therefore only port security is enabled to allow mobility in the network. In order to secure Dynamic Host Configuration Protocol (DHCP) against denial of service (DoS) and man-in-the-middle (MITM) attacks, DHCP snooping is enabled on access layer switches and the DHCP request rate per second is limited to 20 on the user's access ports. Route filtering is configured on both R1 and R2 to avoid transit traffic through the company network. All the unused device ports are set as administratively down and in order to minimize the propagation of flapping routes across the internetwork, BGP route dampening is enabled on routers. There is now full connectivity and reachability across the existing network and the connections to ISPs are learned through BGP, as shown in figure 8. [12;13.]

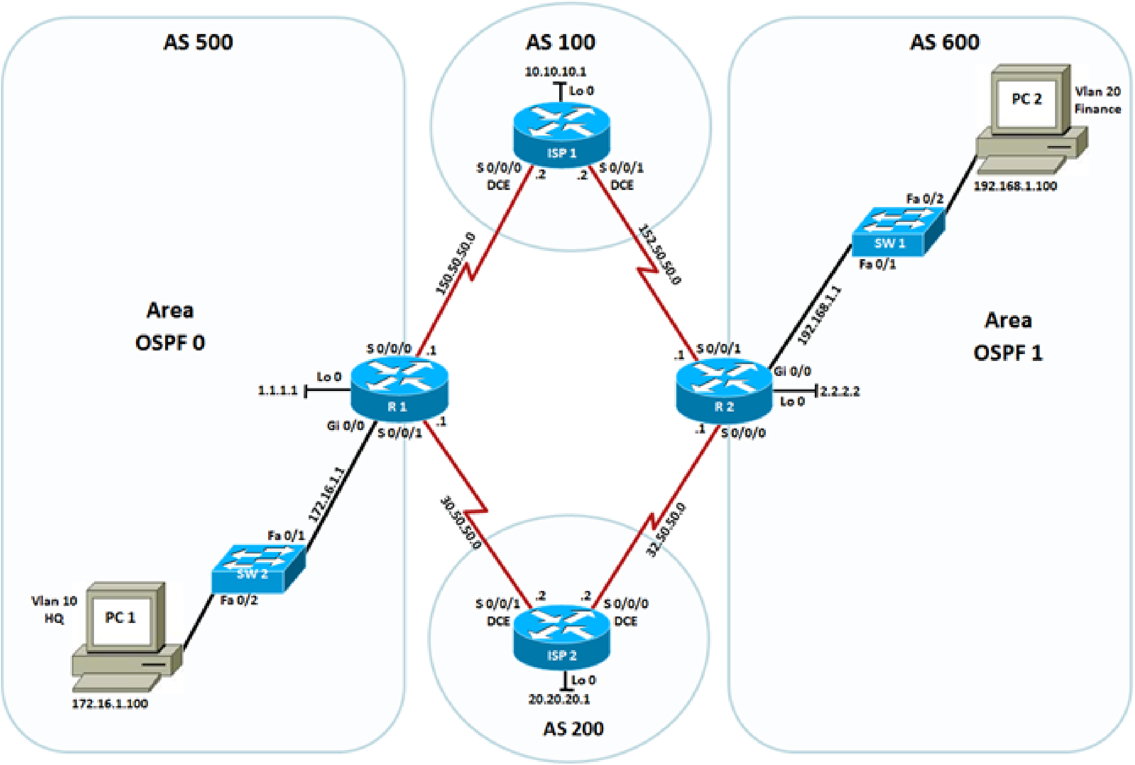
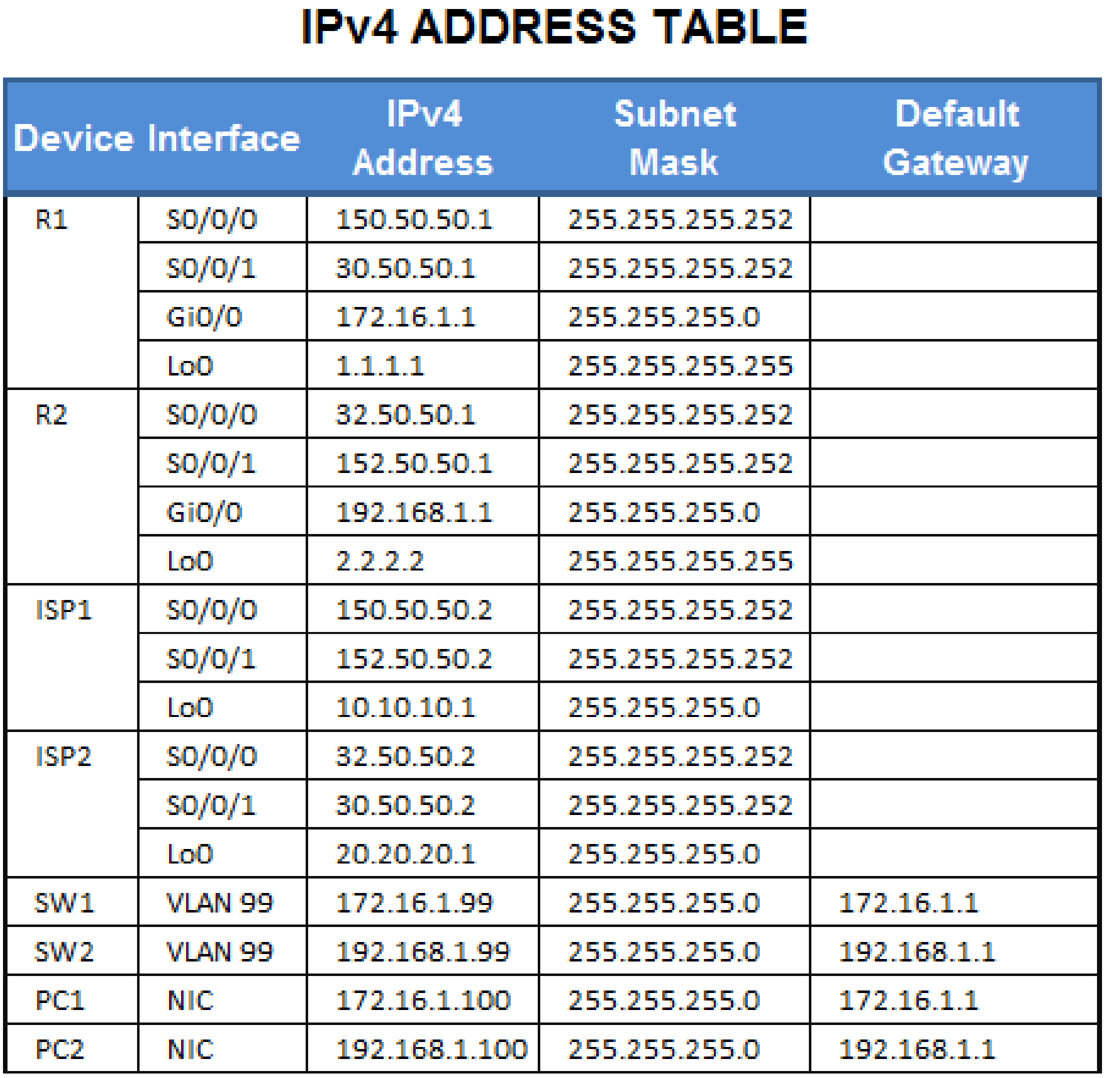


Figure 8. Company West Current IPv4 Network Topology

The addressing scheme of the current topology of the company is illustrated in table 1.

Table 1. Company West IPv4 Network Addressing Scheme

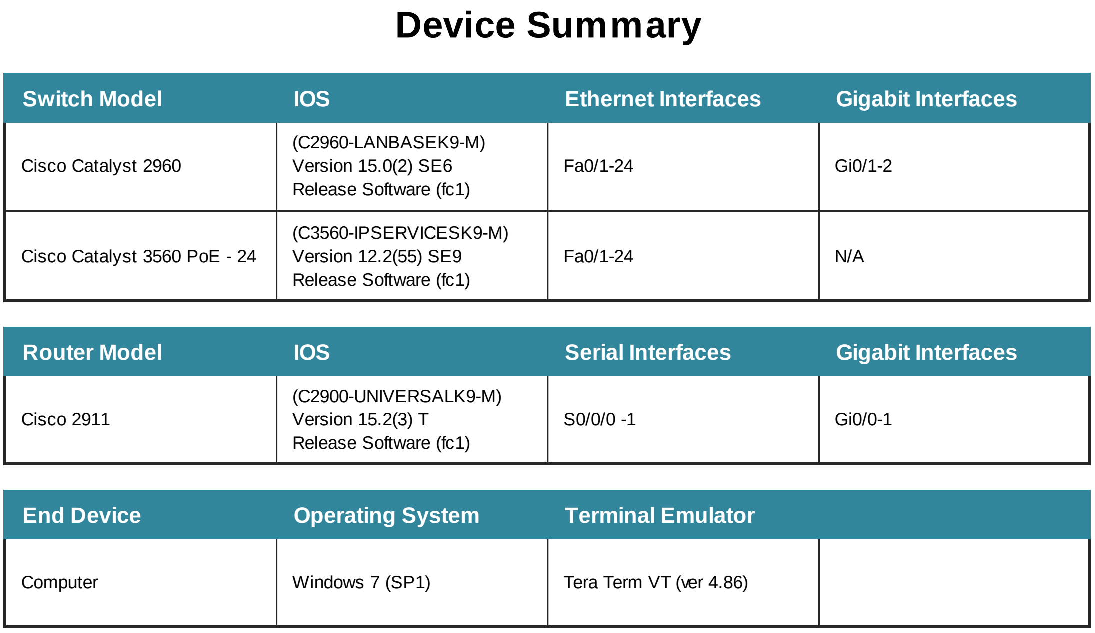


IPv4 ADDRESS TABLE

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	S0/0/0	150.50.50.1	255.255.255.252	
	S0/0/1	30.50.50.1	255.255.255.252	
	Gi0/0	172.16.1.1	255.255.255.0	
	Lo0	1.1.1.1	255.255.255.255	
R2	S0/0/0	32.50.50.1	255.255.255.252	
	S0/0/1	152.50.50.1	255.255.255.252	
	Gi0/0	192.168.1.1	255.255.255.0	
	Lo0	2.2.2.2	255.255.255.255	
ISP1	S0/0/0	150.50.50.2	255.255.255.252	
	S0/0/1	152.50.50.2	255.255.255.252	
	Lo0	10.10.10.1	255.255.255.0	
ISP2	S0/0/0	32.50.50.2	255.255.255.252	
	S0/0/1	30.50.50.2	255.255.255.252	
	Lo0	20.20.20.1	255.255.255.0	
SW1	VLAN 99	172.16.1.99	255.255.255.0	172.16.1.1
SW2	VLAN 99	192.168.1.99	255.255.255.0	192.168.1.1
PC1	NIC	172.16.1.100	255.255.255.0	172.16.1.1
PC2	NIC	192.168.1.100	255.255.255.0	192.168.1.1

To implement this lab the following network devices were used and the following table 2 shows the list and detail of the devices.

Table 2. Company West Network Device Summary.



Device Summary

Switch Model	IOS	Ethernet Interfaces	Gigabit Interfaces
Cisco Catalyst 2960	(C2960-LANBASEK9-M) Version 15.0(2) SE6 Release Software (fc1)	Fa0/1-24	Gi0/1-2
Cisco Catalyst 3560 PoE - 24	(C3560-IPSERVICESK9-M) Version 12.2(55) SE9 Release Software (fc1)	Fa0/1-24	N/A

Router Model	IOS	Serial Interfaces	Gigabit Interfaces
Cisco 2911	(C2900-UNIVERSALK9-M) Version 15.2(3) T Release Software (fc1)	S0/0/0 -1	Gi0/0-1

End Device	Operating System	Terminal Emulator	
Computer	Windows 7 (SP1)	Tera Term VT (ver 4.86)	

To accommodate the company’s growth, it was decided the site Finance currently running IPv4 needed to expand and a new site Research and Engineering needed to be added to the existing network.

To facilitate future expansion, access to limitless IP addresses and mobility, the company decided to run IPv6. The branch office Finance will run both IPv4 and IPv6 as new sites, Research and Engineering will be native IPv6, while the HQ will remain IPv4. CW will use transition mechanisms to migrate to IPv6 and gradually implement IPv6 throughout the entire network.

There will be two scenarios for CW transition. In scenario one, the ISP1 is able to provide IPv6 services to the company and the routers will be configured as dual-stack. In the second scenario, the ISP is unable to provide IPv6 and therefore the connection to the sites will be accomplished by using a tunnelling mechanism. The topology in both scenarios is the same except where the ISP1 will be disconnected from the network to demonstrate the second scenario. All the new devices such as switches will be configured in accordance with the existing network requirements.

3.2 Dual-Stack Scenario

In accordance with the Request for Comments (RFC) 6180, for documentation purposes the 2001:db8::/32 IPv6 address range is used. In order to differentiate between the company assigned IPv6 addresses and the Internet address, Lo 1 on ISP1 has the address of 3001:db8::10/128. A successful ping to this Lo 1 means that there is connectivity to the IPv6 Internet.

The basic prefix structures for this network are:

- Site prefix --/48
- VLAN or non-Point-to-Point links --/68
- Point-to-Point links --/127.

After the request of the company for an IPv6 address, ISP1 will provide the company with an address block of 2001:db8:1::/48. Figure 9 is a demonstration of the logical view of the network and how dual-stack works.

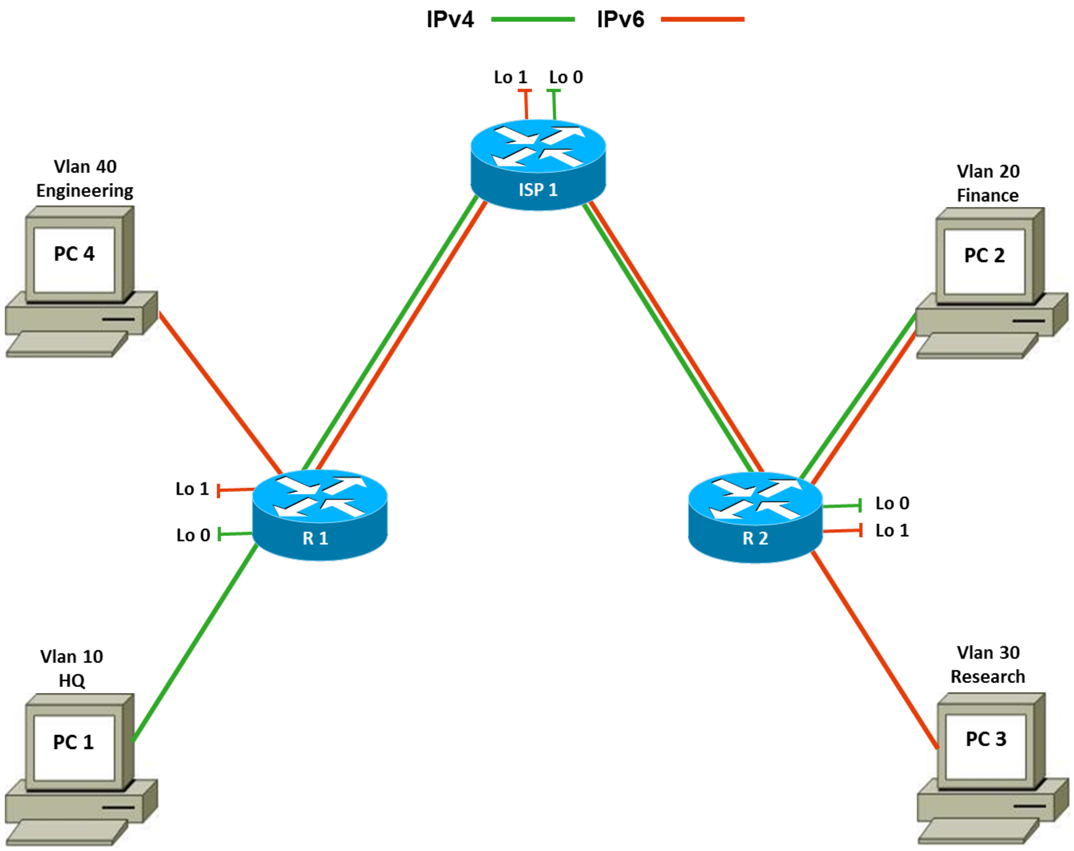


Figure 9. Dual-Stack Logical View

Figure 9 shows how each stack runs completely independently of the other and the routers forward the packets based on the destination address [10].

3.2.1 Testing IPv6 Implementation

For the purpose of testing the IPv6 implementation, a ULA of FD01:db8::/32 was configured for the Finance site. A ULA is similar to an IPv4 private address and is for use in a private network. They are not routable in the global IPv6 Internet. In order to configure the IPv6 in site Finance, IPv6 routing between R2 and Personal Computer (PC) 2, needs to be enabled. The IPv6 ULA will be assigned on interface Gigabit Ethernet Interface (Gi) 0/0 of R2 using the SLAAC feature. The SLAAC mechanism allows the generation of its own addresses by the host as well as autoconfiguration of the hosts.

The IPv6 SLAAC is a mechanism that allows a host to generate its own addresses using a combination of locally available information and information advertised by routers and therefore requires no manual configuration of hosts. When a host requires an IPv6 address, it will send an Internet Control Message Protocol (ICMPv6) Router Solicitation (RS) requesting the link information. The router responds with an ICMPv6 router advertisement that provides the IPv6 prefix and the host checks for its availability using duplicate address detection (DAD) and then starts using the address.

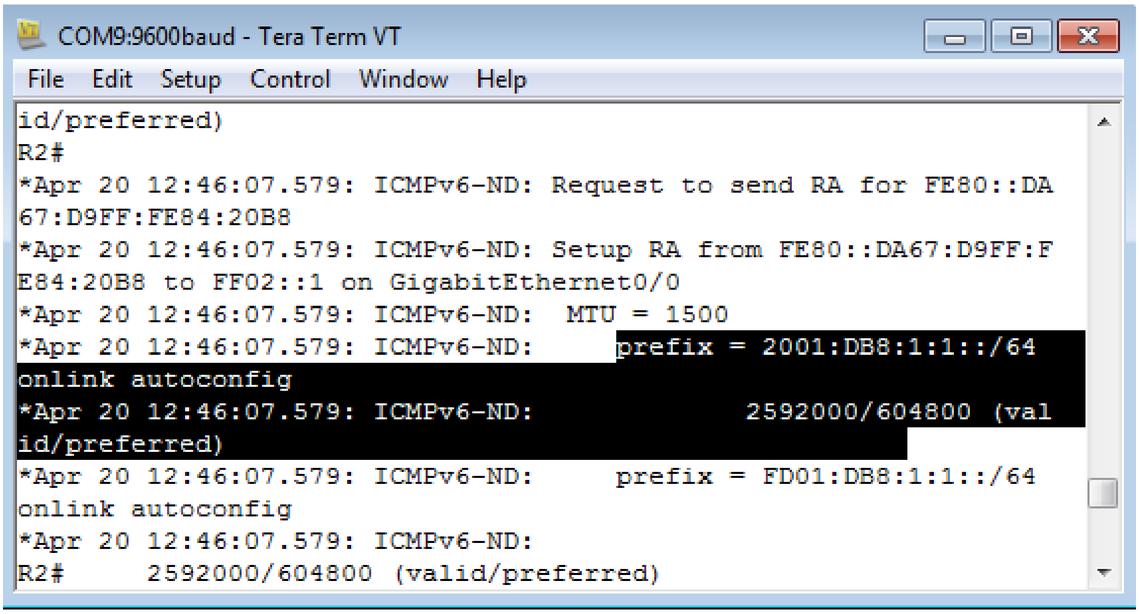
After configuration, hosts on this site can automatically configure themselves by adding their IPv6 interface identifier to the local link 64-bit prefix. This method demonstrates how Extended Unique Identity (EUI-64) works. [5,720;14;15.]

The following commands were entered on R2:

```
R2(config)# ipv6 unicast-routing
R2(config)# int gi0/0
R2(config-if)# ipv6 address fd01:db8:1:1::/64 eui-64
```

Listing 1. Autoconfiguration using EUI-64 method

After entering the configuration in listing 1, the debug command for Neighbor Discovery (ND) was enabled on R2 to observe how it works. Figure 10 demonstrates the result.


COM9:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
id/preferred)
R2#
*Apr 20 12:46:07.579: ICMPv6-ND: Request to send RA for FE80::DA
67:D9FF:FE84:20B8
*Apr 20 12:46:07.579: ICMPv6-ND: Setup RA from FE80::DA67:D9FF:F
E84:20B8 to FF02::1 on GigabitEthernet0/0
*Apr 20 12:46:07.579: ICMPv6-ND:  MTU = 1500
*Apr 20 12:46:07.579: ICMPv6-ND:     prefix = 2001:DB8:1:1::/64
onlink autoconfig
*Apr 20 12:46:07.579: ICMPv6-ND:             2592000/604800 (val
id/preferred)
*Apr 20 12:46:07.579: ICMPv6-ND:     prefix = FD01:DB8:1:1::/64
onlink autoconfig
*Apr 20 12:46:07.579: ICMPv6-ND:
R2#     2592000/604800 (valid/preferred)
```

Figure 10. The Debug Output for Neighbor Discovery

As the debug output in figure 10 demonstrates, the link is autoconfigured and the router includes an additional Type Length Value (TLV) to Router Advertisement (RA) messages.

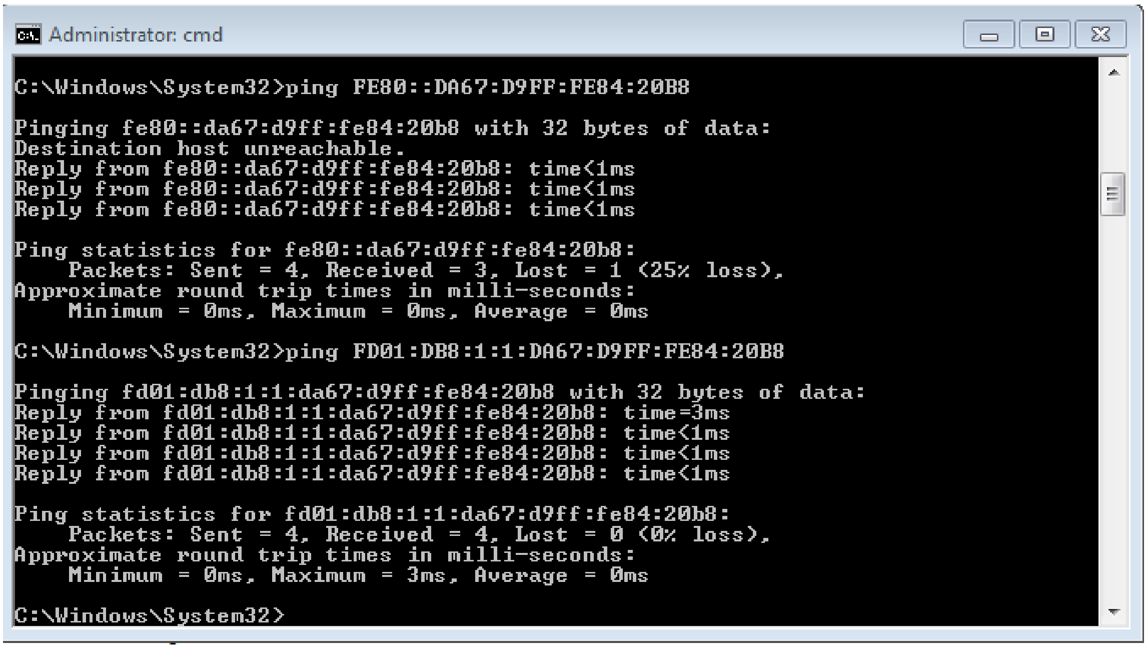
Link-local addresses are locally significant and are dynamically created on all IPv6 enabled interfaces using the specific link-local prefix of FE80::/10 and a 64-bit interface identifier. This is illustrated in in the highlighted area of listing 2, of the output of interface Gi0/0

```
R2#show ipv6 interface gi0/0
GigabitEthernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is
FE80::DA67:D9FF:FE84:20B8
No Virtual link-local address(es):
Global unicast address(es):
FD01:DB8:1:1:DA67:D9FF:FE84:20B8, subnet is
FD01:DB8:1:1::/64 [EUI]
<output omitted>
```

Listing 2. Interface Gi0/0 Output

After the configuration was completed, PC2 obtained an IPv6 address and connectivity between R2 and PC2 was successfully established.

Figure 11 shows the ping to the link-local and the IPv6 address of the interface Gi0/0 of R2.



```
C:\Windows\System32>ping FE80::DA67:D9FF:FE84:20B8

Pinging fe80::da67:d9ff:fe84:20b8 with 32 bytes of data:
Destination host unreachable.
Reply from fe80::da67:d9ff:fe84:20b8: time<1ms
Reply from fe80::da67:d9ff:fe84:20b8: time<1ms
Reply from fe80::da67:d9ff:fe84:20b8: time<1ms

Ping statistics for fe80::da67:d9ff:fe84:20b8:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\System32>ping FD01:DB8:1:1:DA67:D9FF:FE84:20B8

Pinging fd01:db8:1:1:da67:d9ff:fe84:20b8 with 32 bytes of data:
Reply from fd01:db8:1:1:da67:d9ff:fe84:20b8: time=3ms
Reply from fd01:db8:1:1:da67:d9ff:fe84:20b8: time<1ms
Reply from fd01:db8:1:1:da67:d9ff:fe84:20b8: time<1ms
Reply from fd01:db8:1:1:da67:d9ff:fe84:20b8: time<1ms

Ping statistics for fd01:db8:1:1:da67:d9ff:fe84:20b8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\Windows\System32>
```

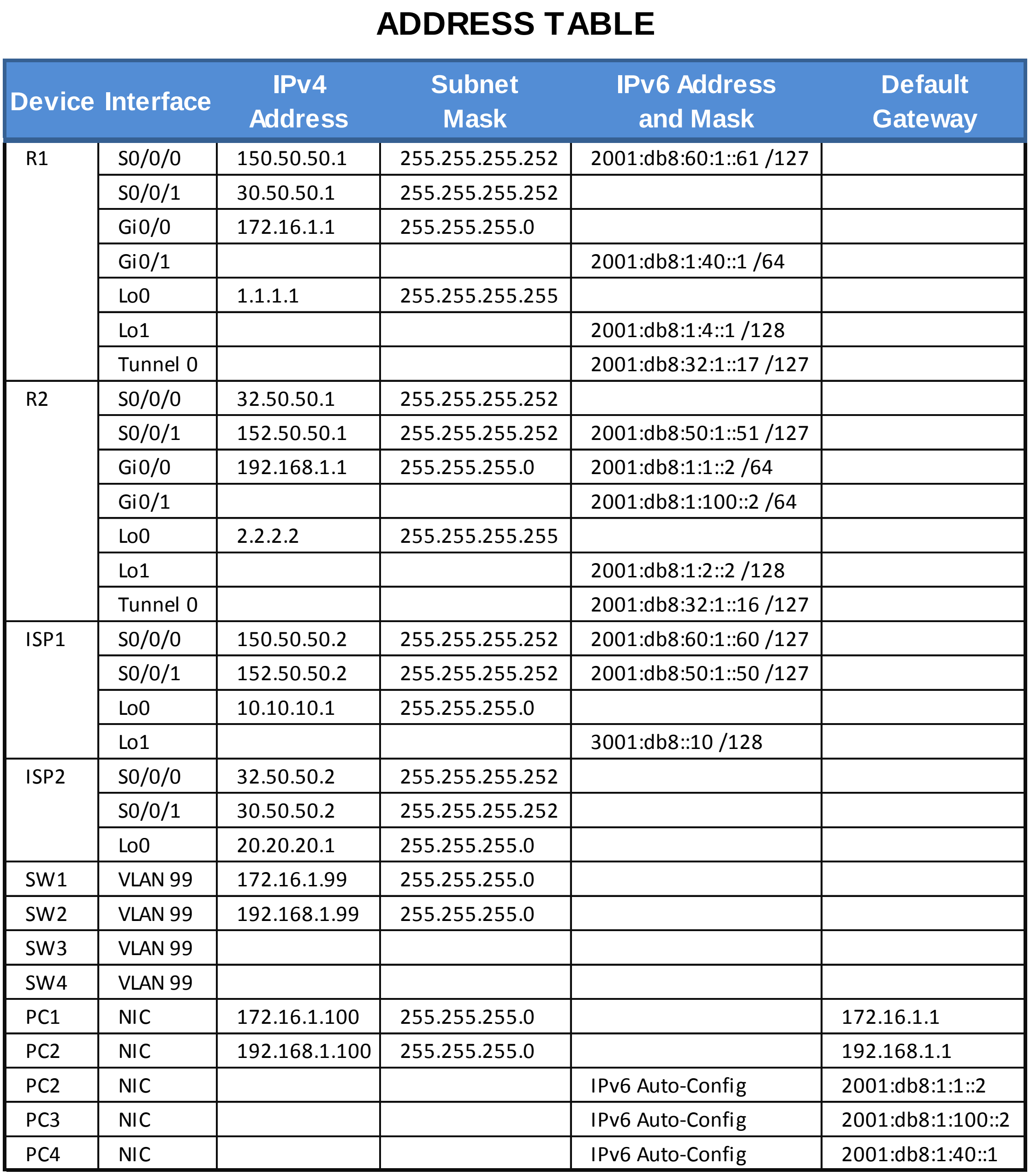
Figure 11. Pings from PC2 to R2

Based on figure 11, the pilot test was successful. After examining the behaviour of IPv6, global unicast addresses will be assigned to sites Finance, Research and Engineering. [5,707.]

3.2.2 IPv6 Address Assignment

From the IPv6 address block obtained from ISP1, IPv6 addresses will be manually assigned to sites. Table 3 shows the full addressing plan for the network.

Table 3. Addressing Plan for Company West



ADDRESS TABLE

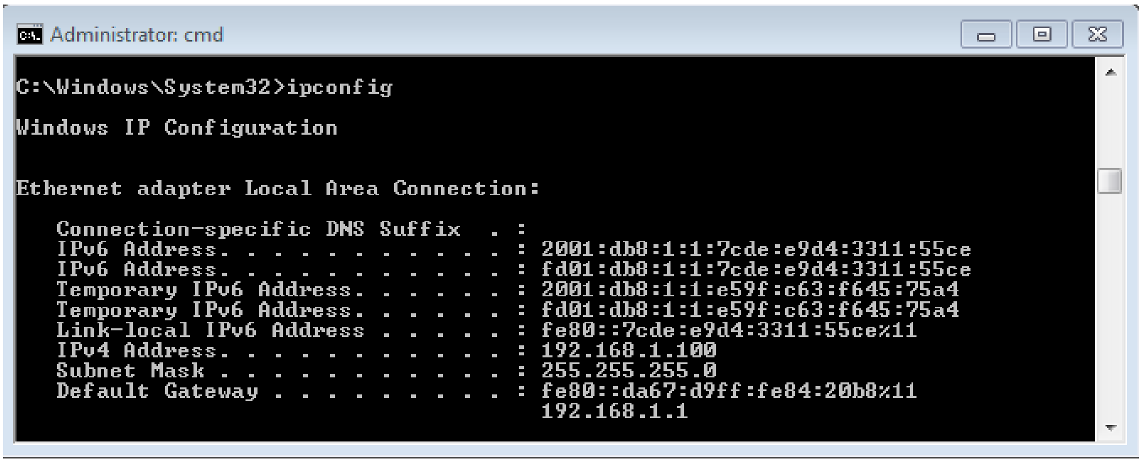
Device	Interface	IPv4 Address	Subnet Mask	IPv6 Address and Mask	Default Gateway
R1	S0/0/0	150.50.50.1	255.255.255.252	2001:db8:60:1::61 /127	
	S0/0/1	30.50.50.1	255.255.255.252		
	Gi0/0	172.16.1.1	255.255.255.0		
	Gi0/1			2001:db8:1:40::1 /64	
	Lo0	1.1.1.1	255.255.255.255		
	Lo1			2001:db8:1:4::1 /128	
	Tunnel 0			2001:db8:32:1::17 /127	
R2	S0/0/0	32.50.50.1	255.255.255.252		
	S0/0/1	152.50.50.1	255.255.255.252	2001:db8:50:1::51 /127	
	Gi0/0	192.168.1.1	255.255.255.0	2001:db8:1:1::2 /64	
	Gi0/1			2001:db8:1:100::2 /64	
	Lo0	2.2.2.2	255.255.255.255		
	Lo1			2001:db8:1:2::2 /128	
	Tunnel 0			2001:db8:32:1::16 /127	
ISP1	S0/0/0	150.50.50.2	255.255.255.252	2001:db8:60:1::60 /127	
	S0/0/1	152.50.50.2	255.255.255.252	2001:db8:50:1::50 /127	
	Lo0	10.10.10.1	255.255.255.0		
	Lo1			3001:db8::10 /128	
ISP2	S0/0/0	32.50.50.2	255.255.255.252		
	S0/0/1	30.50.50.2	255.255.255.252		
	Lo0	20.20.20.1	255.255.255.0		
SW1	VLAN 99	172.16.1.99	255.255.255.0		
SW2	VLAN 99	192.168.1.99	255.255.255.0		
SW3	VLAN 99				
SW4	VLAN 99				
PC1	NIC	172.16.1.100	255.255.255.0		172.16.1.1
PC2	NIC	192.168.1.100	255.255.255.0		192.168.1.1
PC2	NIC			IPv6 Auto-Config	2001:db8:1:1::2
PC3	NIC			IPv6 Auto-Config	2001:db8:1:100::2
PC4	NIC			IPv6 Auto-Config	2001:db8:1:40::1

The IPv6 address assignment begins with site Finance and continues with site Research. Interface Lo1 will be created and interfaces Gi0/0 and Gi0/1 will be assigned IPv6 addresses. One of the IPv6 features is that a single interface can have multiple IPv6 addresses of any type and therefore there is no need to delete the ULA.

```
R2(config)# ipv6 unicast-routing
R2(config)#interface loopback 1
R2(config-if)#ipv6 address 2001:db8:1:2::2/128
R2(config)#interface gi0/0
R2(config-if)#ipv6 address 2001:db8:1:1::2/64
R2(config)# interface gi0/1
R2(config-if)#ipv6 address 2001:db8:1:100::2/64
```

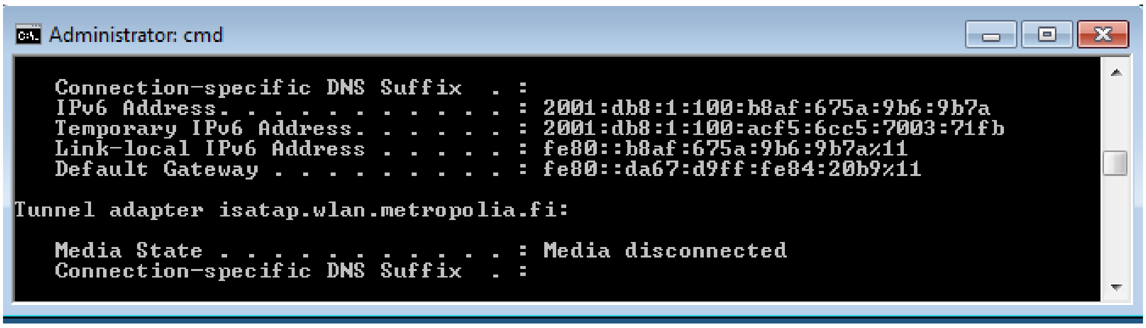
Listing 3. IPv6 Address Assignment for R2 Interfaces

Hosts on sites Finance and Research autoconfigured themselves and obtained IPv6 addresses, as illustrated in figures 12 and 13.



```
C:\Windows\System32>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:1:1:7cde:e9d4:3311:55ce
   IPv6 Address. . . . . . . . . . . : fd01:db8:1:1:7cde:e9d4:3311:55ce
   Temporary IPv6 Address. . . . . . : 2001:db8:1:1:e59f:c63:f645:75a4
   Temporary IPv6 Address. . . . . . : fd01:db8:1:1:e59f:c63:f645:75a4
   Link-local IPv6 Address . . . . . : fe80::7cde:e9d4:3311:55ce%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::da67:d9ff:fe84:20b8%11
                                       192.168.1.1
```

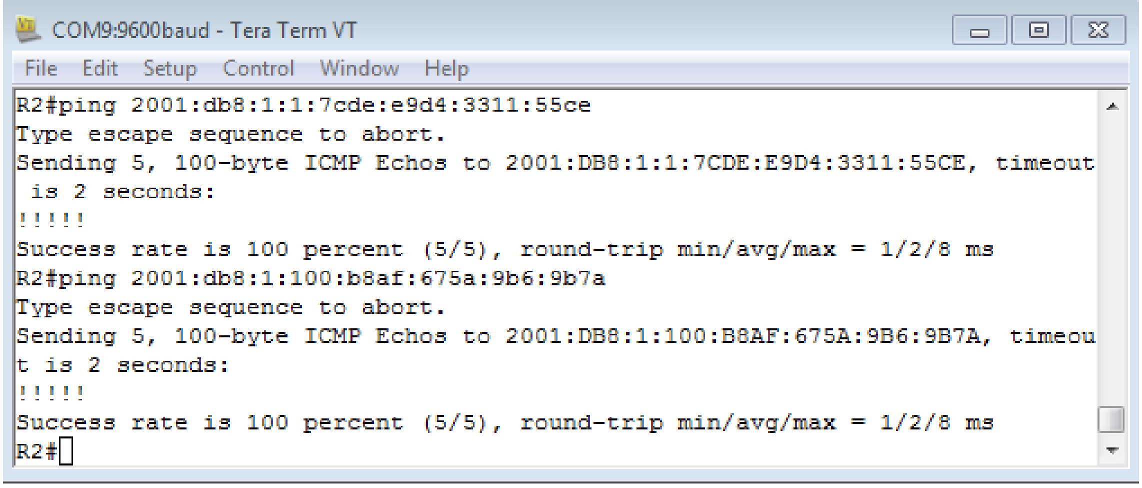
Figure 12. Autoconfiguration Output of PC2



```
   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:1:100:b8af:675a:9b6:9b7a
   Temporary IPv6 Address. . . . . . : 2001:db8:1:100:acf5:6cc5:7003:71fb
   Link-local IPv6 Address . . . . . : fe80::b8af:675a:9b6:9b7a%11
   Default Gateway . . . . . . . . . : fe80::da67:d9ff:fe84:20b9%11

Tunnel adapter isatap.wlan.metropolia.fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Figure 13. Autoconfiguration Output of PC3

Connectivity was then tested from R2 by pinging both hosts as demonstrated in figure 14.


COM9:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
R2#ping 2001:db8:1:1:7cde:e9d4:3311:55ce
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1:1:7CDE:E9D4:3311:55CE, timeout
 is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
R2#ping 2001:db8:1:100:b8af:675a:9b6:9b7a
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1:100:B8AF:675A:9B6:9B7A, timeou
t is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
R2#
```

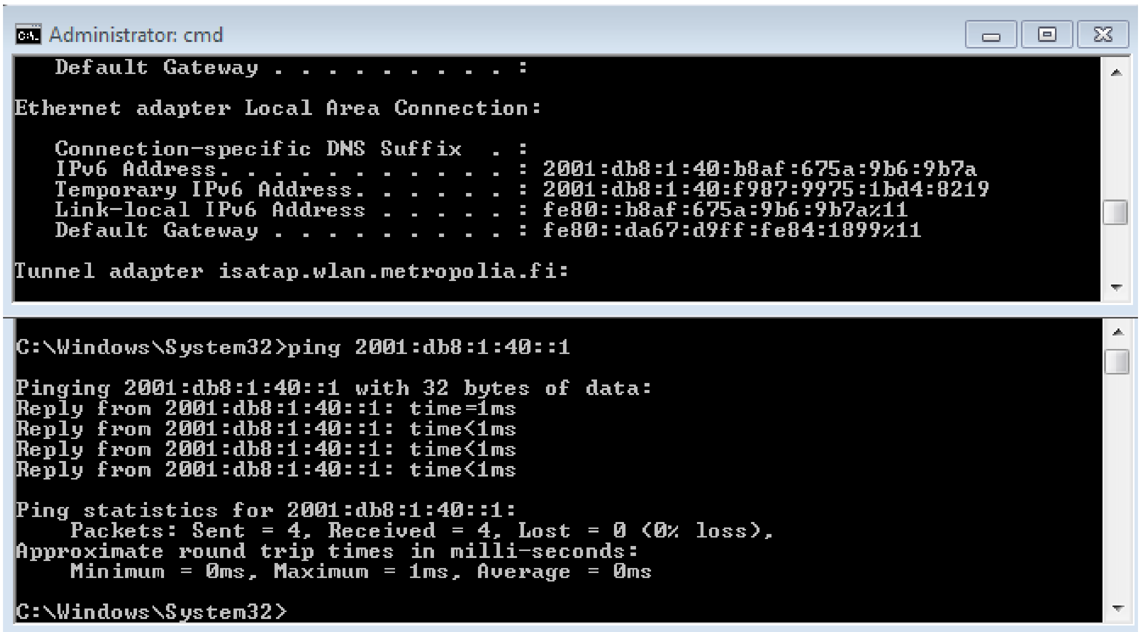
Figure 14. R2 Pings to PC2 and PC3

The next requirement is to enable the IPv6 network on the Engineering site. The following commands were entered on R1:

```
R1(config)#ipv6 unicast-routing
R1(config)#interface loopback 1
R1(config-if)#ipv6 address 2001:db8:1:4::1/128
R1(config)#interface gi0/1
R1(config-if)#ipv6 address 2001:db8:1:40::1/64
```

Listing 4. Enabling IPv6 on Engineering

The host, PC4, on the Engineering site, obtained an IPv6 address dynamically and connectivity was verified by pinging R1 from PC4 as demonstrated in figure 15.



```
   Default Gateway . . . . . . . . . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:1:40:b8af:675a:9b6:9b7a
   Temporary IPv6 Address. . . . . . : 2001:db8:1:40:f987:9975:1bd4:8219
   Link-local IPv6 Address . . . . . : fe80::b8af:675a:9b6:9b7a%11
   Default Gateway . . . . . . . . . : fe80::da67:d9ff:fe84:1899%11

Tunnel adapter isatap.wlan.metropolia.fi:
```

```
C:\Windows\System32>ping 2001:db8:1:40::1

Pinging 2001:db8:1:40::1 with 32 bytes of data:
Reply from 2001:db8:1:40::1: time=1ms
Reply from 2001:db8:1:40::1: time<1ms
Reply from 2001:db8:1:40::1: time<1ms
Reply from 2001:db8:1:40::1: time<1ms

Ping statistics for 2001:db8:1:40::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Windows\System32>
```

Figure 15. IP Configuration Output and Ping to PC4

Pings from PC4 to R1 were successful, verifying the connectivity, as shown in figure 15.

3.2.3 Interior Gateway Protocol Configuration

At this point, after assigning an IPv6 address to all of the devices, the interior routing protocol needed to be configured. As previously mentioned in section 3.1, the network was running OSPFv2 for IPv4, and therefore OSPFv3 will be configured as the IGP protocol for the network.

The site Finance is running both IPv4 and IPv6. The address family feature allows for two router processes per interface but only one OSPF process per address family, and therefore R2 must have two process ids to support site Finance. The use of different process IDs results in each address family establishing different adjacencies, having a different link state database and computing a different shortest path tree. [7;16;17.]

The configuration for R2 is shown in listing 5 below.

```
R2(config)# router ospfv3 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#auto-cost reference bandwidth 1000
R2(config-router)##igonor lsa mospf
R2(config-router)#log-adjacency-changes
R2(config-router)#address-family ipv6 unicast
R2(config-router-af)#area 1 range 2001:db8:1:1::/64
R2(config-router-af)#area 1 range 2001:db8:1:2::2/128
R2(config-router-af)#area 1 range 2001:db8:1:100::/64
R2(config-router-af)#redistribute statics
R2(config-router-af)#default-information originate always
metric 100 metric-type 2
R2(config-router-af)#exit-address-family
R2(config-router)#router ospfv3 2
R2(config-router)# address family ipv4 unicast
R2(config-router-af)#area 1 range 192.168.1.0 255.255.255.0
R2(config-router-af)#area 1 range 2.2.2.2  255.255.255.255
R2(config-router-af)#default-information originate always
metric 100 metric-type 2
R2(config-router-af)#end
```

Listing 5. OSPFv3 configuration for R2

Link-State Advertisement (LSA) type 6 multicast OSPFv3 packets are ignored, as they are not supported. After configuring OSPFv3 and the OSPFv3 area, OSPFv3 must be enabled on the interfaces. In OSPFv3 each interface must be enabled in the interface configuration mode. In OSPFv2, interfaces were indirectly enabled using the router configuration mode.

OSPFv3 can be enabled on an interface with the IPv4 or the IPv6 address family or by enabling OSPFv3 on an interface as illustrated in listing 6.

```
R2(config)# interface gi0/0
R2(config-if)#ospfv3 2 area 1 ipv4
R2(config)# interface loopback 0
R2(config-if)#ospfv3 2 area 1 ipv4
R2(config)# interface gi0/1
R2(config-if)#ospfv3 1 area 1 ipv6
R2(config)#interface loopback 1
R2(config-if)#ipv6 ospf 1 area 0.0.0.1
```

Listing 6. Enable OSPFv3 on an Interface

R1 is connected to two networks, one that is IPv4 and running OSPFv2 and the other is an IPv6 network and running OSPFv3. OSPFv3 and OSPFv2 run independently of each other and run a separate SPF instance. Neither protocol is aware of the other, and for this reason the approach is to run OSPFv3 for both address families on R1. Each address family will have its own OSPF process id and will be enabled on the correct interface.

As site HQ is running OSPFv2, in order to enable OSPFv3, IPv6 needs to be enabled on the Gi0/0 interface first, but no IPv6 address assignment is needed as listing 7 illustrates.

```
R1(config)#interface gi0/0
R1(config-if)#ipv6 enable
R1(config)#interface loopback 0
R1(config-if)#ipv6 enable
R1(config-if)#exit
R1(config)# router ospfv3 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#auto-cost reference bandwidth 1000
R1(config-router)#igonor lsa mospf
R1(config-router)#log-adjacency-changes
R1(config-router-af)#address-family ipv6 unicast
R1(config-router-af)#area 3 range 2001:db8:1:4::1/128
R1(config-router-af)#area 3 range 2001:db8:1:40::/64
R1(config-router-af)#redistribute statics
R1(config-router-af)#default-information originate always
metric 100 metric-type 2
R1(config-router-af)#exit-address-family
R1(config-router)#router ospfv3 2
R1(config-router)# address family ipv4 unicast
R1(config-router-af)#area 0 range 172.16.1.0  255.255.255.0
R1(config-router-af)#area 0 range 1.1.1.1  255.255.255.255
R1(config-router-af)#default-information originate always
metric 100 metric-type 2
R1(config-router-af)#end
```

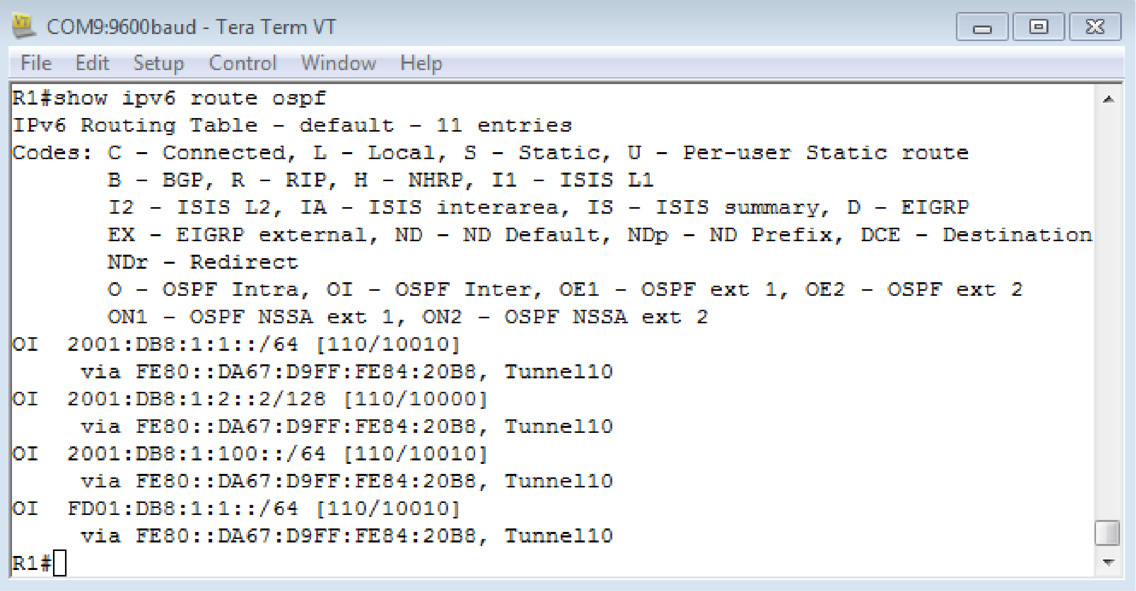
Listing 7. Configure OSPFv3 on R1

Enabling the OSPFv3 on interfaces is shown in listing 8.

```
R1(config)# interface gi0/0
R1(config-if)#ospfv3 2 area 0 ipv4
R1(config)# interface loopback 0
R1(config-if)#ospfv3 2 area 0 ipv4

R1(config)# interface gi0/1
R1(config-if)#ospfv3 1 area 3 ipv6
R1(config)# interface loopback 1
R1(config-if)#ospfv3 1 area 3 ipv6
```

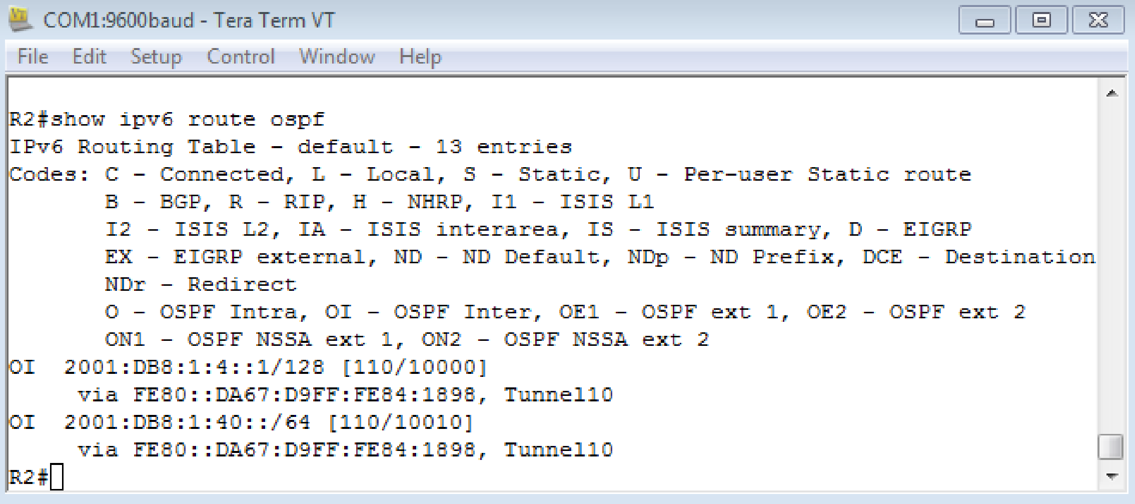
Listing 8. Enable OPSFv3 on Interfaces

After entering the configurations in listings 7 and 8, to check the routes the `show ipv6 route ospf` command was entered on both R1 and R2 as illustrated in figures 16 and 17.


COM9:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
R1#show ipv6 route ospf
IPv6 Routing Table - default - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OI  2001:DB8:1:1::/64 [110/10010]
     via FE80::DA67:D9FF:FE84:20B8, Tunnel10
OI  2001:DB8:1:2::2/128 [110/10000]
     via FE80::DA67:D9FF:FE84:20B8, Tunnel10
OI  2001:DB8:1:100::/64 [110/10010]
     via FE80::DA67:D9FF:FE84:20B8, Tunnel10
OI  FD01:DB8:1:1::/64 [110/10010]
     via FE80::DA67:D9FF:FE84:20B8, Tunnel10
R1#
```

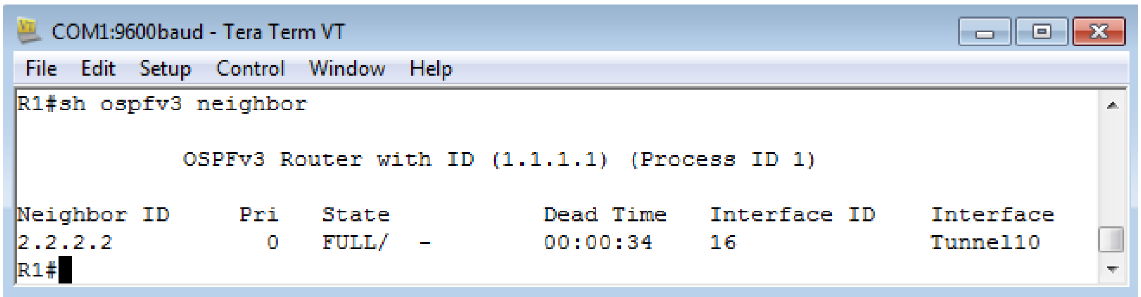
Figure 16. R1 Output for OSPFv3 Routes


COM1:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
R2#show ipv6 route ospf
IPv6 Routing Table - default - 13 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OI  2001:DB8:1:4::1/128 [110/10000]
     via FE80::DA67:D9FF:FE84:1898, Tunnel10
OI  2001:DB8:1:40::/64 [110/10010]
     via FE80::DA67:D9FF:FE84:1898, Tunnel10
R2#
```

Figure 17. R2 Output for OSPFv3 Routes

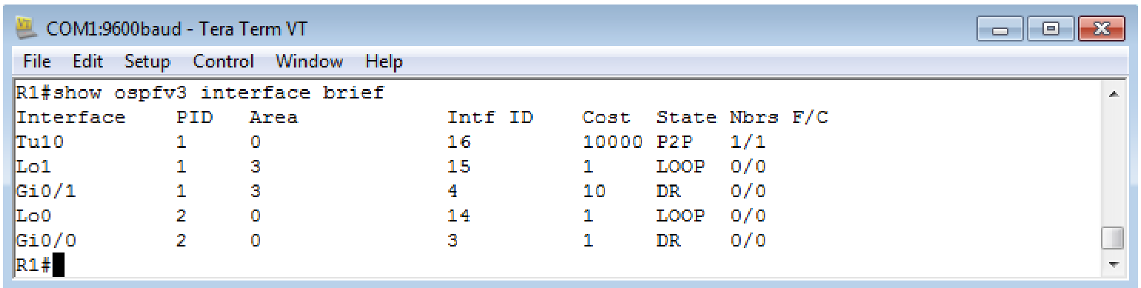
As shown in figures 16 and 17, each router learns the routes to the other router via tunnel 10. Figure 18 shows the OSPFv3 neighbours.


COM1:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
R1#sh ospfv3 neighbor

            OSPFv3 Router with ID (1.1.1.1) (Process ID 1)

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
2.2.2.2           0   FULL/  -        00:00:34    16              Tunnel10
R1#
```

Figure 18. Show OSPFv3 Neighbor Output

As shown in figure 18, the routers have formed a neighbor relationship via tunnel 10. To verify the interfaces connected to each area the `show OSPFv3 interfaces brief` command was entered on R1, as illustrated in figure 19.


COM1:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
R1#show ospfv3 interface brief
Interface    PID   Area            Intf ID    Cost  State Nbrs F/C
Tu10         1     0               16         10000 P2P   1/1
Lo1          1     3               15         1     LOOP  0/0
Gi0/1        1     3               4          10    DR    0/0
Lo0          2     0               14         1     LOOP  0/0
Gi0/0        2     0               3          1     DR    0/0
R1#
```

Figure 19. Show Command for OSPFv3 Interfaces

As shown in figure 19, this command shows interfaces in each area with the corresponding process ID as well as the state and cost.

3.2.4 IPv6 Static Routing

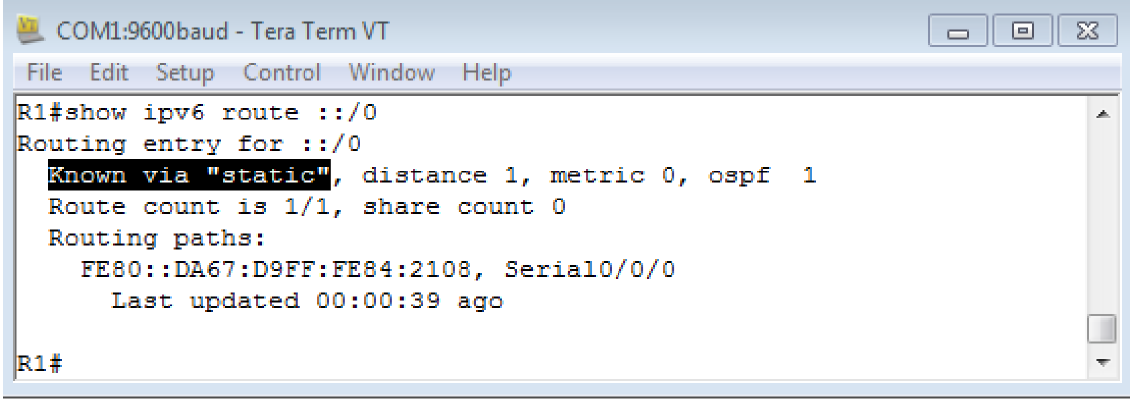
Finally the connectivity to the IPv6 Internet and between the sites needs to be configured. ISP1 has IPv6 Internet connectivity but IPv6 is not enabled internally. ISP1 can however advertise IPv6 prefixes over the IPv6 Internet by enabling static routing. ISP1 is therefore dual-stacked to support both IPv4 and IPv6. IPv6 addresses need to be assigned to serial links that are connected to ISP1. IPv6 static default routing needs to be enabled using a link local address as the next hop, pointing toward ISP1.

The network devices will then be able to ping the IPv6 Internet. Listing 9, illustrates the commands issued on ISP1, R1 and R2.

```
ISP1(config)# ipv6 unicast-routing
ISP1(config)#interface s0/0/1
ISP1(config-if)#ipv6 address 2001:db8:50:1::50/127
ISP1(config)#interface s0/0/0
ISP1(config-if)#ipv6 address 2001:db8:60:1::60/127
ISP1(config-if)#exit
ISP1(config)#ipv6 route 2001:db8:1:1::/64 2001:db8:50:1::51
ISP1(config)#ipv6 route 2001:db8:1:100::/64
2001:db8:50:1::51
ISP1(config)#ipv6 route 2001:db8:1:40::/64
2001:db8:60:1::61
ISP1(config)#ipv6 route 2001:db8:1:2::2/128
2001:db8:50:1::51
ISP1(config)#ipv6 route 2001:db8:1:4::1/128
2001:db8:60:1::61

R2(config)# interface s0/0/1
R2(config-if)#ipv6 address 2001:db8:51:1::51/127
R2(config-if)#exit
R2(config)# ipv6 route ::/0 serial 0/0/1
FE80::DA67:D9FF:FE84:2108
R1(config)#interface s0/0/0
R1(config-if)#ipv6 address 2001:db8:60:1::61/127
R1(config)#ipv6 route ::/0 serial 0/0/0
FE80::DA67:D9FF:FE84:2180
```

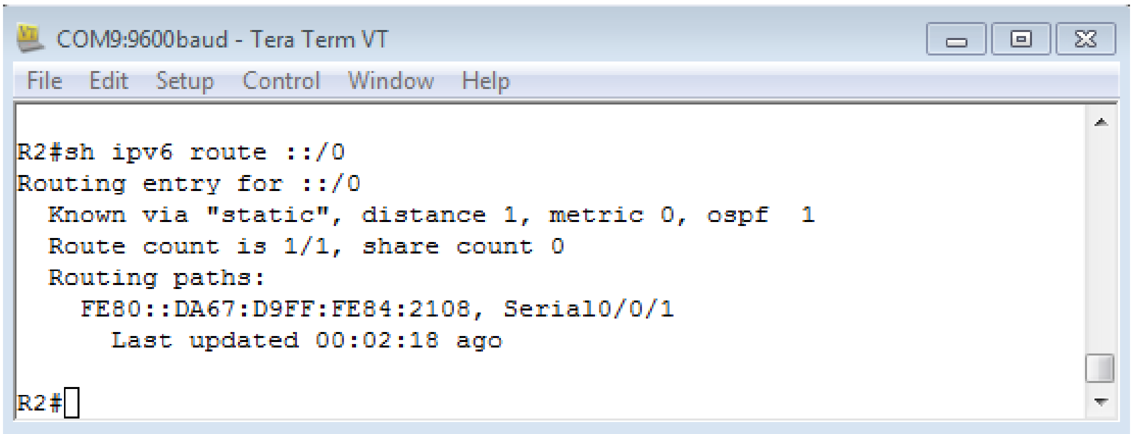
Listing 9. IPv6 Address Assignments on Links to ISP1

To verify the IPv6 static routing configurations, the `show ipv6 route ::/0` command was entered on both R1 and R2 as illustrated in figures 20 and 21.


COM1:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
R1#show ipv6 route ::/0
Routing entry for ::/0
  Known via "static", distance 1, metric 0, ospf  1
  Route count is 1/1, share count 0
  Routing paths:
    FE80::DA67:D9FF:FE84:2108, Serial0/0/0
      Last updated 00:00:39 ago

R1#
```

Figure 20. IPv6 Static Routing Verification for R1

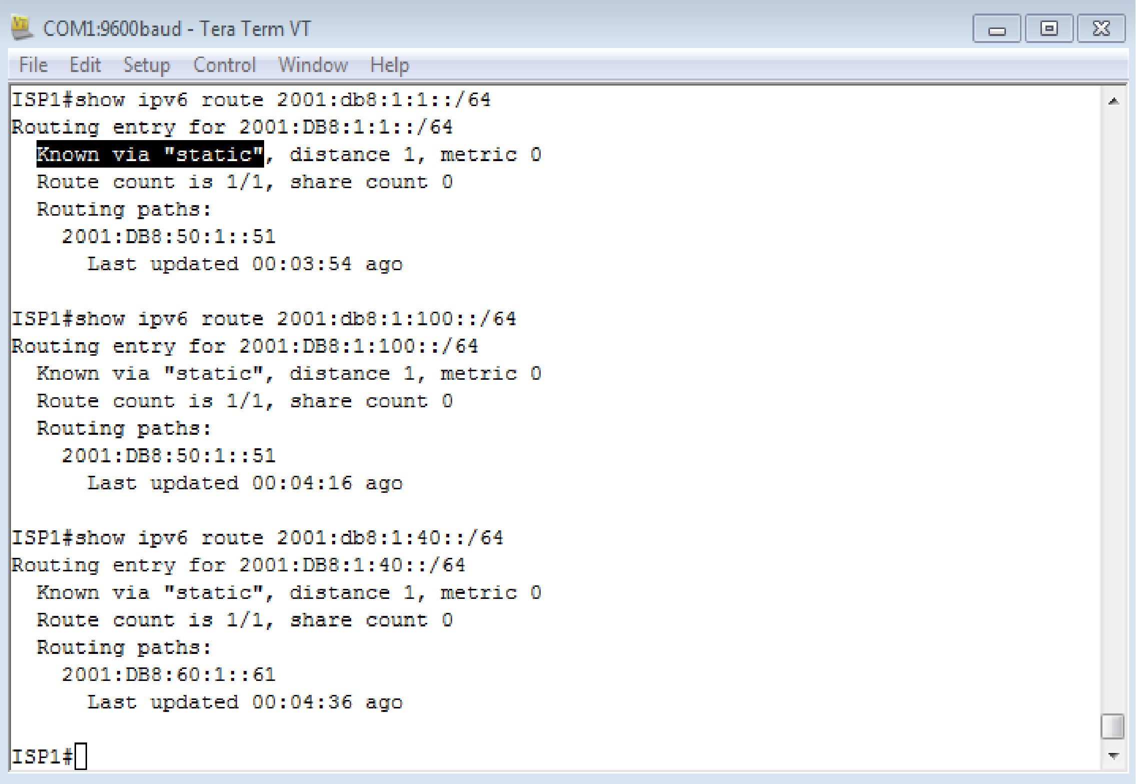

COM9:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
R2#sh ipv6 route ::/0
Routing entry for ::/0
  Known via "static", distance 1, metric 0, ospf  1
  Route count is 1/1, share count 0
  Routing paths:
    FE80::DA67:D9FF:FE84:2108, Serial0/0/1
      Last updated 00:02:18 ago

R2#
```

Figure 21. IPv6 Static Routing Verification for R2

Figures 20 and 21 show that these routes are learned statically and therefore have a default administrative distance of 1. The default static route ::/0 specifies that the destination IPv6 prefix and prefix length are all zeros.

ISP1 also needs to learn about the routes and by using the `show ipv6 route` command for the IPv6 prefix of the sites, verification of the route being added to the ISP1 routing table is obtained as illustrated in figure 22.


COM1:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
ISP1#show ipv6 route 2001:db8:1:1::/64
Routing entry for 2001:DB8:1:1::/64
  Known via "static", distance 1, metric 0
  Route count is 1/1, share count 0
  Routing paths:
    2001:DB8:50:1::51
      Last updated 00:03:54 ago

ISP1#show ipv6 route 2001:db8:1:100::/64
Routing entry for 2001:DB8:1:100::/64
  Known via "static", distance 1, metric 0
  Route count is 1/1, share count 0
  Routing paths:
    2001:DB8:50:1::51
      Last updated 00:04:16 ago

ISP1#show ipv6 route 2001:db8:1:40::/64
Routing entry for 2001:DB8:1:40::/64
  Known via "static", distance 1, metric 0
  Route count is 1/1, share count 0
  Routing paths:
    2001:DB8:60:1::61
      Last updated 00:04:36 ago

ISP1#
```

Figure 22. Routing Entries for Site Prefixes on ISP1

Figure 22 shows the path for each route and the routes are learnt statically.

The completed topology of CW after the configurations were completed as demonstrated in the following figure 23.

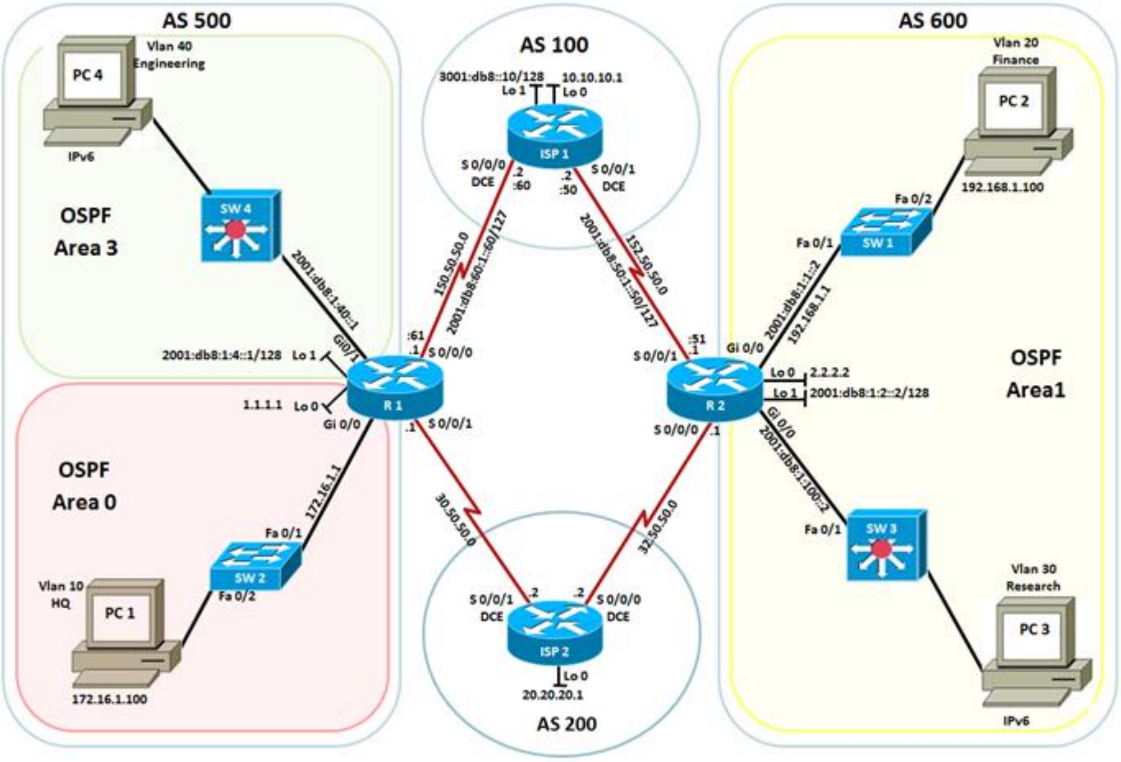
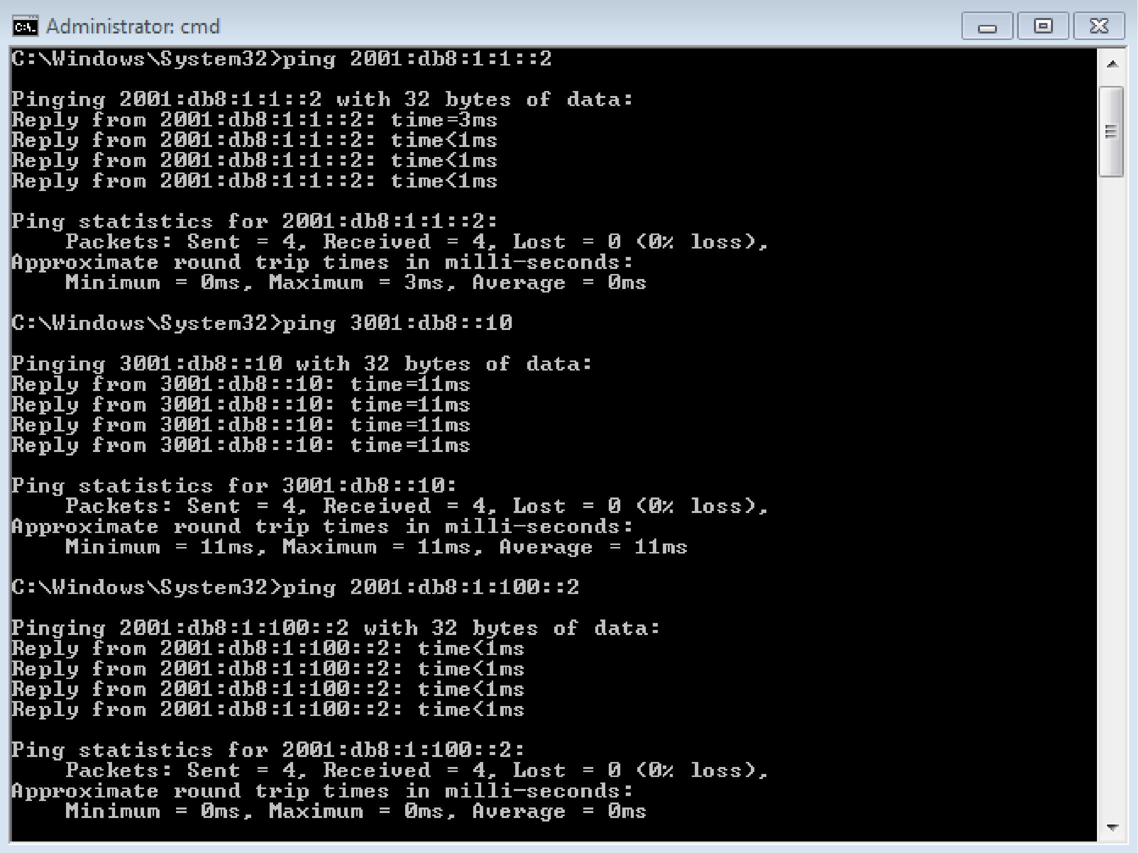


Figure 23. Company West Dual-Stack Network Topology

As shown in figure 23, each route to ISP1 is dual-stacked and has both IPv4 and IPv6 addresses, allowing connectivity between IPv6 domains.

The hosts on each site are able to ping the Internet, and figure 24 shows the pings.



```
C:\Windows\System32>ping 2001:db8:1:1::2

Pinging 2001:db8:1:1::2 with 32 bytes of data:
Reply from 2001:db8:1:1::2: time=3ms
Reply from 2001:db8:1:1::2: time<1ms
Reply from 2001:db8:1:1::2: time<1ms
Reply from 2001:db8:1:1::2: time<1ms

Ping statistics for 2001:db8:1:1::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\Windows\System32>ping 3001:db8::10

Pinging 3001:db8::10 with 32 bytes of data:
Reply from 3001:db8::10: time=11ms
Reply from 3001:db8::10: time=11ms
Reply from 3001:db8::10: time=11ms
Reply from 3001:db8::10: time=11ms

Ping statistics for 3001:db8::10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 11ms, Average = 11ms

C:\Windows\System32>ping 2001:db8:1:100::2

Pinging 2001:db8:1:100::2 with 32 bytes of data:
Reply from 2001:db8:1:100::2: time<1ms
Reply from 2001:db8:1:100::2: time<1ms
Reply from 2001:db8:1:100::2: time<1ms
Reply from 2001:db8:1:100::2: time<1ms

Ping statistics for 2001:db8:1:100::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 24. PC 2 Pings to Internet and to its Default Gateway

PC2 is able to successfully ping its own default gateway and the loopback on ISP1 which signifies IPv6 Internet connectivity.

3.3 Tunnelling Scenario

CW requests IPv6 support, the ISP is unable to provide the support. To demonstrate this scenario, ISP1 is disconnected and ISP2, only IPv4-enabled, becomes the sole ISP as illustrated in figure 25.

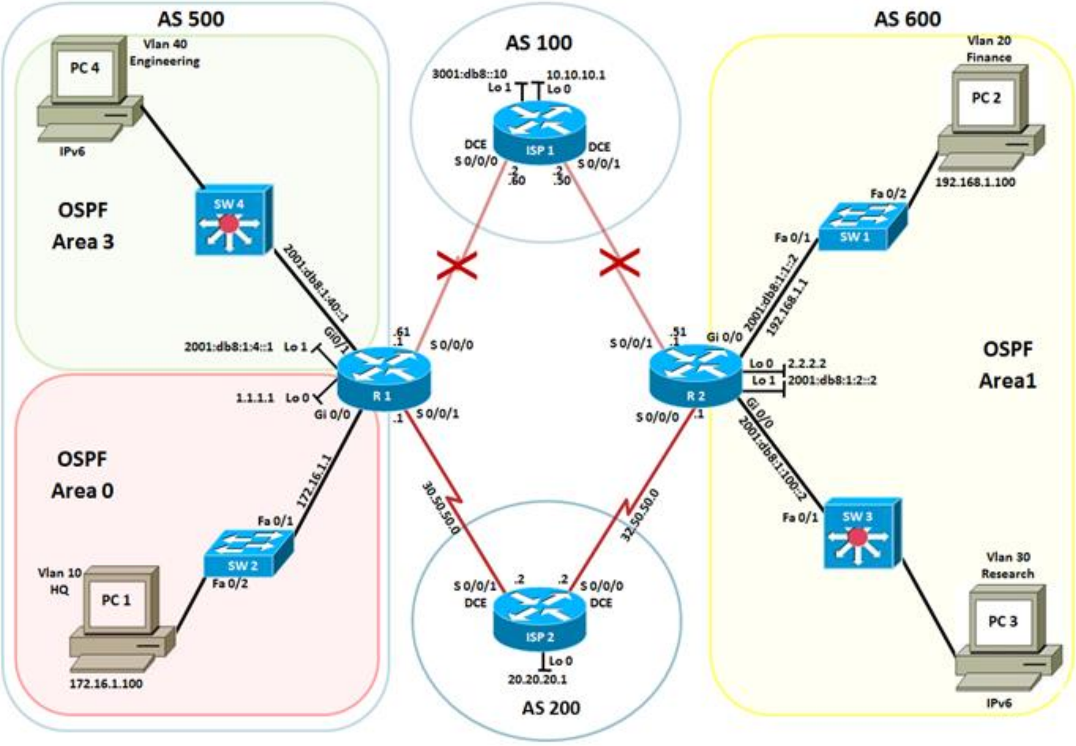
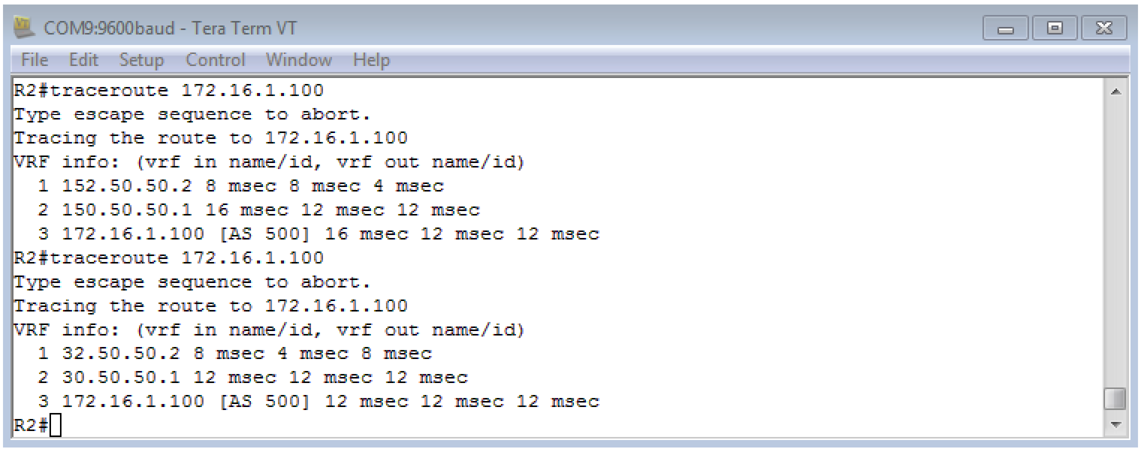


Figure 25. Company West Network Topology IPv4 ISP

CW is multihomed, and therefore when the connection to ISP1 is lost, the route to ISP2 becomes the primary route.

The following traceroute command in figure 26, demonstrates the IPv4 connectivity and the route preference before and after disconnecting the route to ISP1.


COM9:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
R2#traceroute 172.16.1.100
Type escape sequence to abort.
Tracing the route to 172.16.1.100
VRF info: (vrf in name/id, vrf out name/id)
  1 152.50.50.2 8 msec 8 msec 4 msec
  2 150.50.50.1 16 msec 12 msec 12 msec
  3 172.16.1.100 [AS 500] 16 msec 12 msec 12 msec
R2#traceroute 172.16.1.100
Type escape sequence to abort.
Tracing the route to 172.16.1.100
VRF info: (vrf in name/id, vrf out name/id)
  1 32.50.50.2 8 msec 4 msec 8 msec
  2 30.50.50.1 12 msec 12 msec 12 msec
  3 172.16.1.100 [AS 500] 12 msec 12 msec 12 msec
R2#
```

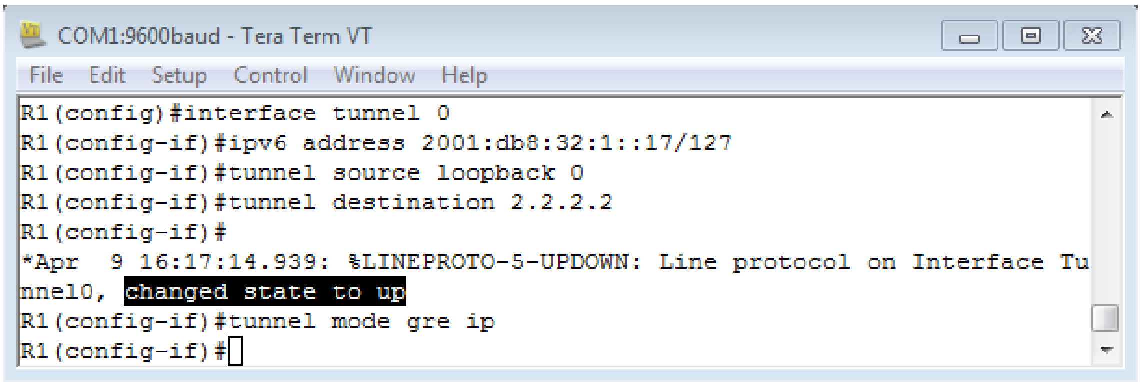
Figure 26. Primary and Backup Route Preference Verification

In order to achieve connectivity between IPv6 sites over an IPv4 network, tunnelling solutions are required. There are different tunnelling modes to choose from, but for this lab, the GRE protocol tunnel was implemented. [18.]

3.3.1 GRE Tunnel Configuration

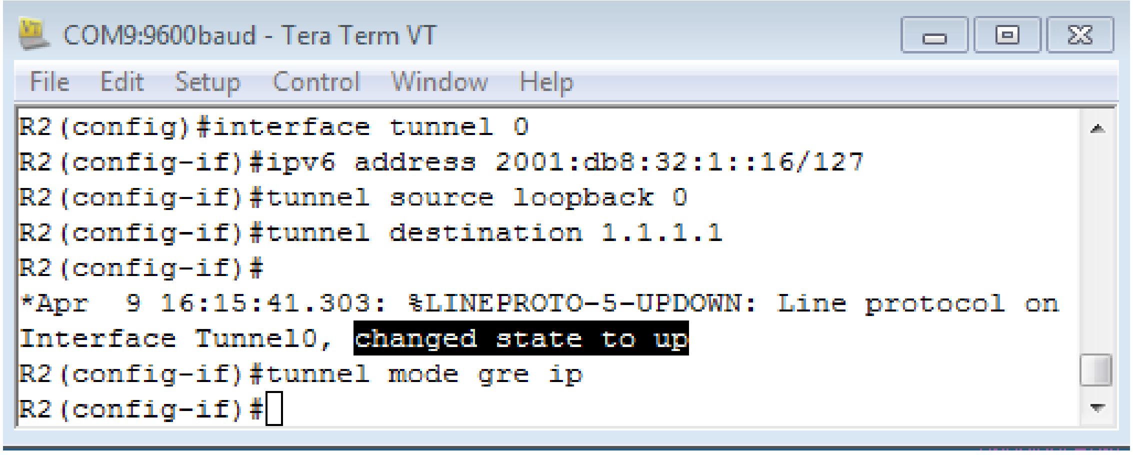
To create a GRE protocol tunnel between R1 and R2, the tunnel interfaces are first created at each end and IPv6 addresses are manually assigned on each end of the tunnel interface. For stability purposes, the tunnel uses loopback interfaces with IPv4 addresses to carry traffic. The tunnel destination is the other router’s loopback interface, and the router will associate that interface with the tunnel. Once the tunnel interface has been created, it comes up and the tunnel mode defines the encapsulation, which in this case is the GRE protocol.

Figure 27 and figure 28 illustrate the GRE protocol tunnel configuration on R1 and R2.


COM1:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
R1(config)#interface tunnel 0
R1(config-if)#ipv6 address 2001:db8:32:1::17/127
R1(config-if)#tunnel source loopback 0
R1(config-if)#tunnel destination 2.2.2.2
R1(config-if)#
*Apr  9 16:17:14.939: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tu
nnel0, changed state to up
R1(config-if)#tunnel mode gre ip
R1(config-if)#
```

Figure 27. GRE tunnel configuration for R1


COM9:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
R2(config)#interface tunnel 0
R2(config-if)#ipv6 address 2001:db8:32:1::16/127
R2(config-if)#tunnel source loopback 0
R2(config-if)#tunnel destination 1.1.1.1
R2(config-if)#
*Apr  9 16:15:41.303: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Tunnel0, changed state to up
R2(config-if)#tunnel mode gre ip
R2(config-if)#
```

Figure 28. GRE Protocol Tunnel Configuration for R2

The tunnel interfaces have IPv6 addresses and the source and the destination are IPv4 interfaces. To achieve full connectivity, OSPFv3 needs to be enabled on the tunnel interfaces. The tunnel interfaces will be participating in the routing process like any other IPv6 link. The tunnel interfaces will be connected to the OSPFv3 backbone area 0, as the loopback interfaces are in different OSPF areas. The configuration is shown in listing 10.

```
R1(config)#interface tunnel 0
R1(config-if)#ipv6 ospf 1 area 0

R2(config)#interface tunnel 0
R2(config-if)#ipv6 ospf 1 area 0
```

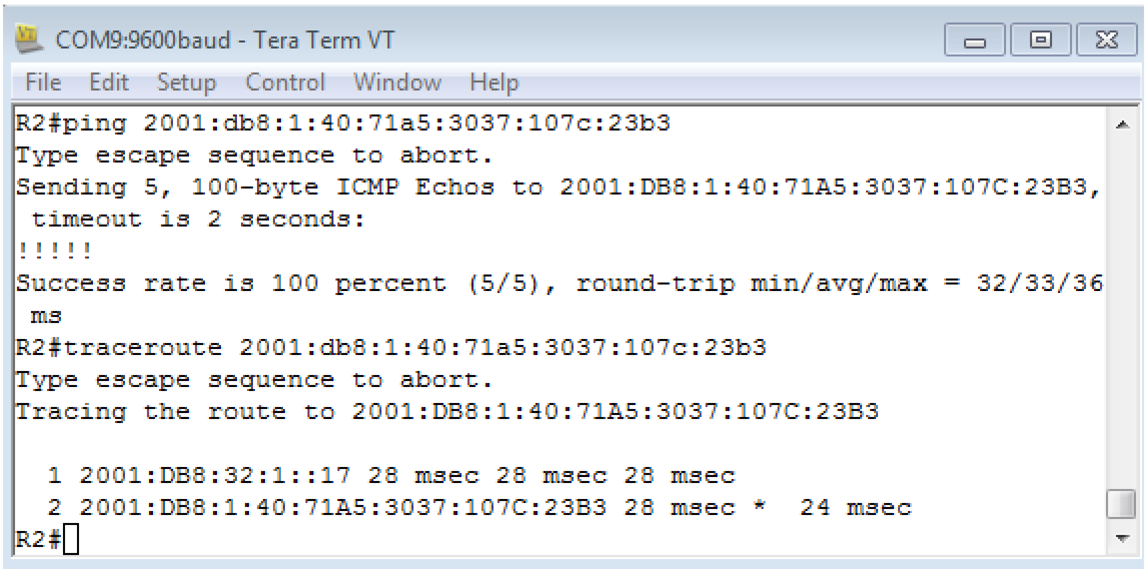
Listing 10. Connecting Tunnel Interface to OSPFv3 Area 0

In addition to the configuration in listing 10, a static route needs to be configured for all destinations pointing to the tunnel interface, as shown in listing 11.

```
R1(config)#ipv6 route ::/0 tunnel10
FE80::DA67:D9FF:FE84:20B8
R2(config)#ipv6 route ::/0 tunnel10
FE80::DA67:D9FF:FE84:1898
```

Listing 11. Static Route Pointing to Outgoing Interface of Tunnel

To verify full connectivity across the tunnel, a ping and a trace route from R2 to host PC4 was performed as shown in figure 29.


COM9:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
R2#ping 2001:db8:1:40:71a5:3037:107c:23b3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1:40:71A5:3037:107C:23B3,
 timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/33/36
 ms
R2#traceroute 2001:db8:1:40:71a5:3037:107c:23b3
Type escape sequence to abort.
Tracing the route to 2001:DB8:1:40:71A5:3037:107C:23B3

  1 2001:DB8:32:1::17 28 msec 28 msec 28 msec
  2 2001:DB8:1:40:71A5:3037:107C:23B3 28 msec *  24 msec
R2#
```

Figure 29. Ping and Traceroute from R2 to PC4

The result of the traceroute command shows that the packet enters the tunnel and leaves for its destination as shown in figure 29. It is now verified that CW has site-to-site connectivity and that the tunnel is up and running.

Figure 30 shows the CW topology after the new configuration.

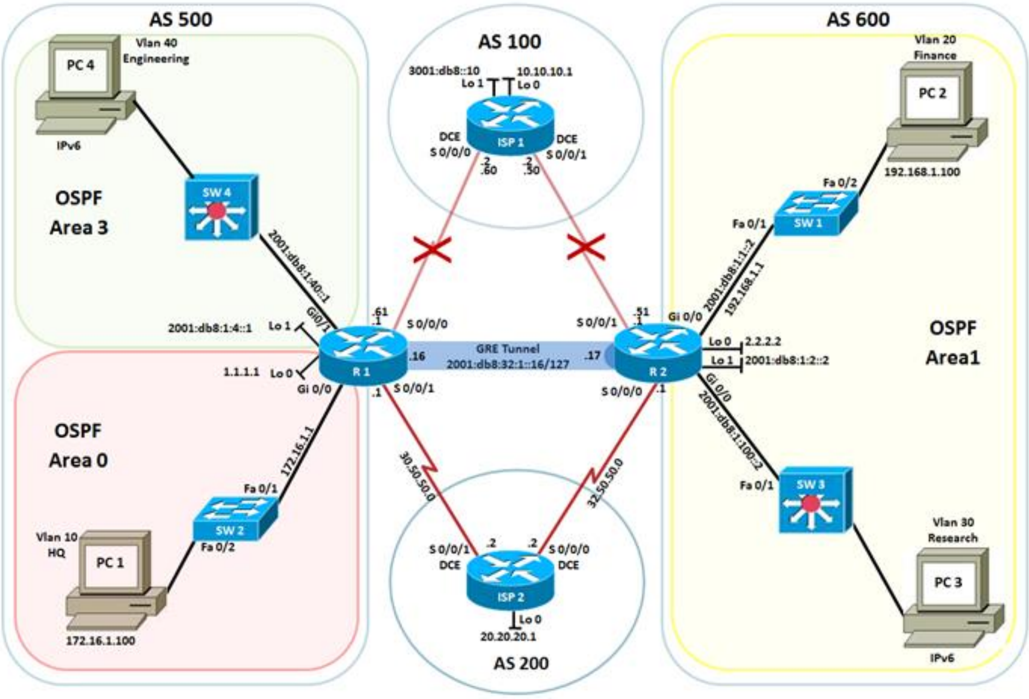


Figure 30. Company West GRE Protocol Tunnel Network Topology

The IPv4 traffic takes the path through ISP2 and the IPv6 traffic travels through the GRE tunnel.

3.3.2 IPsec over GRE Tunnel

The GRE protocol tunnel itself provides no encryption and is just an encapsulation protocol. By default all Internet traffic is in clear text. In this implementation, in order to provide confidentiality, integrity and authentication for the tunnelled IPv6 traffic, the communication will be secured with the use of IPsec as an encryption technology. This mechanism is illustrated in figure 31.

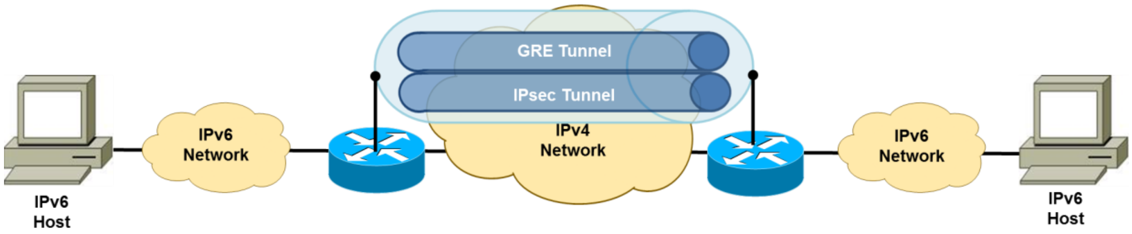


Figure 31. GRE Protocol over IPsec Tunnel Mechanism

As illustrated in figure 31, IPsec will encrypt the packets that are sent through the GRE protocol tunnel, providing security for the data traveling through the tunnel. IPsec is a protocol suite for securing IP communications by authenticating and encrypting each IP packet of a communication session. IPsec provides data authentication and anti-replay services in addition to data confidentiality services.

The point-to-point GRE protocol first encapsulates routing protocols in the GRE protocol and then the GRE protocol packets are encapsulated in IPsec and encrypted. Figure 32 shows the encapsulation process. The routing protocols will be associated with the tunnel interface, which is the IPv4 interface of the router, to send the GRE protocol traffic which should match the parameters of the crypto map and the interface and should therefore be encrypted by the IPsec.

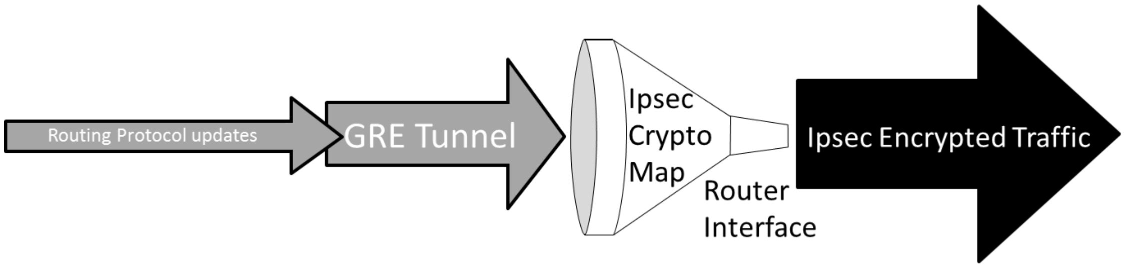


Figure 32. Tunnel Encapsulation Process

As shown in figure 32, the concept of crypto map is the same as a funnel. Crypto map is the initial and terminal point of the IPsec tunnel. The IPsec setting is grouped with the crypto map and applied to the interface. Traffic is allowed through the funnel, only if it meets the criteria and therefore policies are enforced.

Prior to configuring anything else, an Access Control List (ACL) needs to be configured to allow the GRE protocol traffic as shown in listing 12.

```
R1(config)#access-list 101 permit gre any any
R2(config)#access-list 101 permit gre any any
```

Listing 12. Configuration of GRE Protocol ACL 101

Configuration in listing 12, allows for all the GRE protocol traffic from any source to any destination.

IPsec is then configured on R1 and R2 as shown in listing 13.

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#hash md5
R1(config-isakmp)#group 2
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#exit
R1(config)#crypto isakmp key thesis-10 address 2.2.2.2
255.255.255.255
R1(config)#crypto ispsec transform-set thesis0 esp-3des
esp-md5-hmac
R1(config)#crypto map s2svpn 10 ipsec-isakmp
R1(config-crypto-map)#set peer 2.2.2.2
R1(config-crypto-map)#set transform-set thesis0
R1(config-crypto-map)#match address 101

R2(config)#crypto isakmp policy 10
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#hash md5
R2(config-isakmp)#group 2
R2(config-isakmp)#encryption 3des
R2(config-isakmp)#exit
R2(config)#crypto isakmp key thesis-10 address 1.1.1.1
255.255.255.255
R2(config)#crypto ipsec transform-set thesis0 esp-3des esp-
md5-hmac
R2(config-crypto-map)#crypto map s2svpn 10 ipsec-isakmp
R2(config-crypto-map)#set peer 1.1.1.1
R2(config-crypto-map)#set transform-set thesis0
R2(config-crypto-map)#match address 101
```

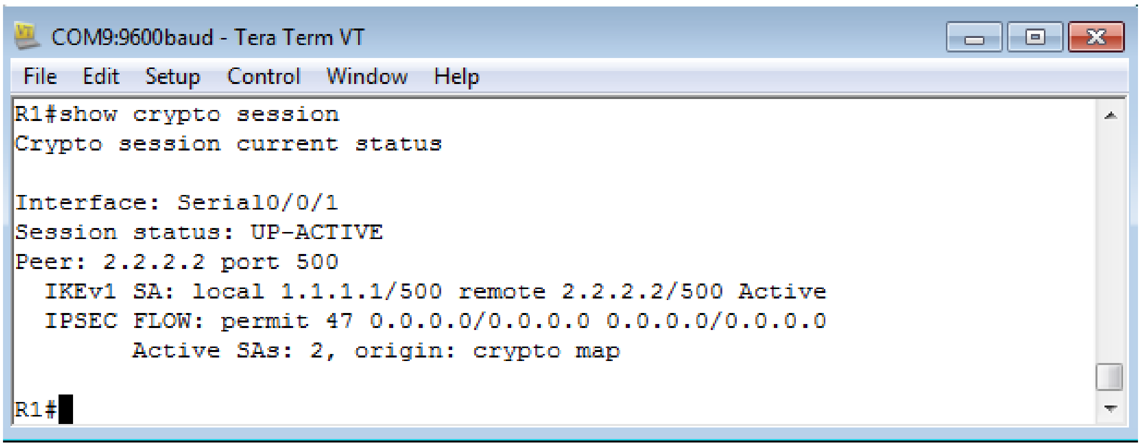
Listing 13. IPsec Configuration of R1 and R2

The next step is to enable process switching on R1 and R2 in order for IPsec to encrypt the outgoing packets as shown in listing 14.

```
R1(config)#interface serial0/0/1
R1(config-if)#crypto map s2svpn
```

Listing 14. Enabling IPsec on the Outgoing Interface

After configuring the devices, the IPsec Virtual Private Network (VPN) tunnel can then be verified as shown in figure 33:

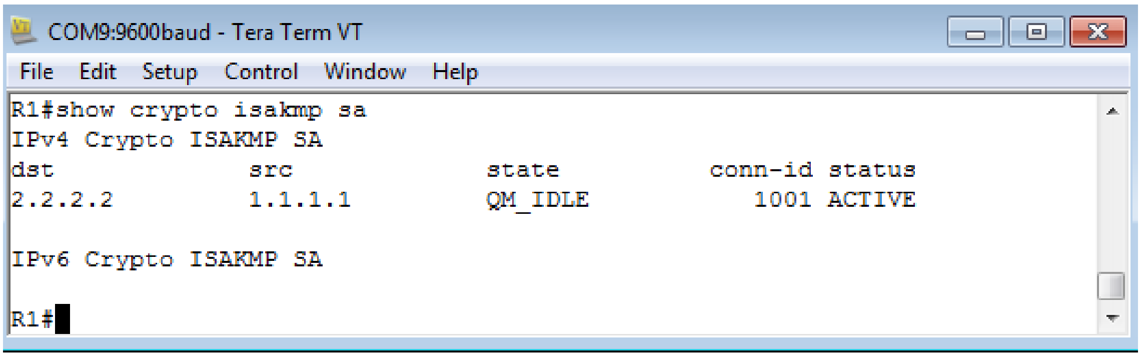

COM9:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
R1#show crypto session
Crypto session current status

Interface: Serial0/0/1
Session status: UP-ACTIVE
Peer: 2.2.2.2 port 500
  IKEv1 SA: local 1.1.1.1/500 remote 2.2.2.2/500 Active
  IPSEC FLOW: permit 47 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map

R1#
```

Figure 33. Crypto Session Verification for R1

As confirmed by figure 33, the crypto session is up and active, and the crypto map has been applied to interface Serial 0/0/1 facing towards the Internet.

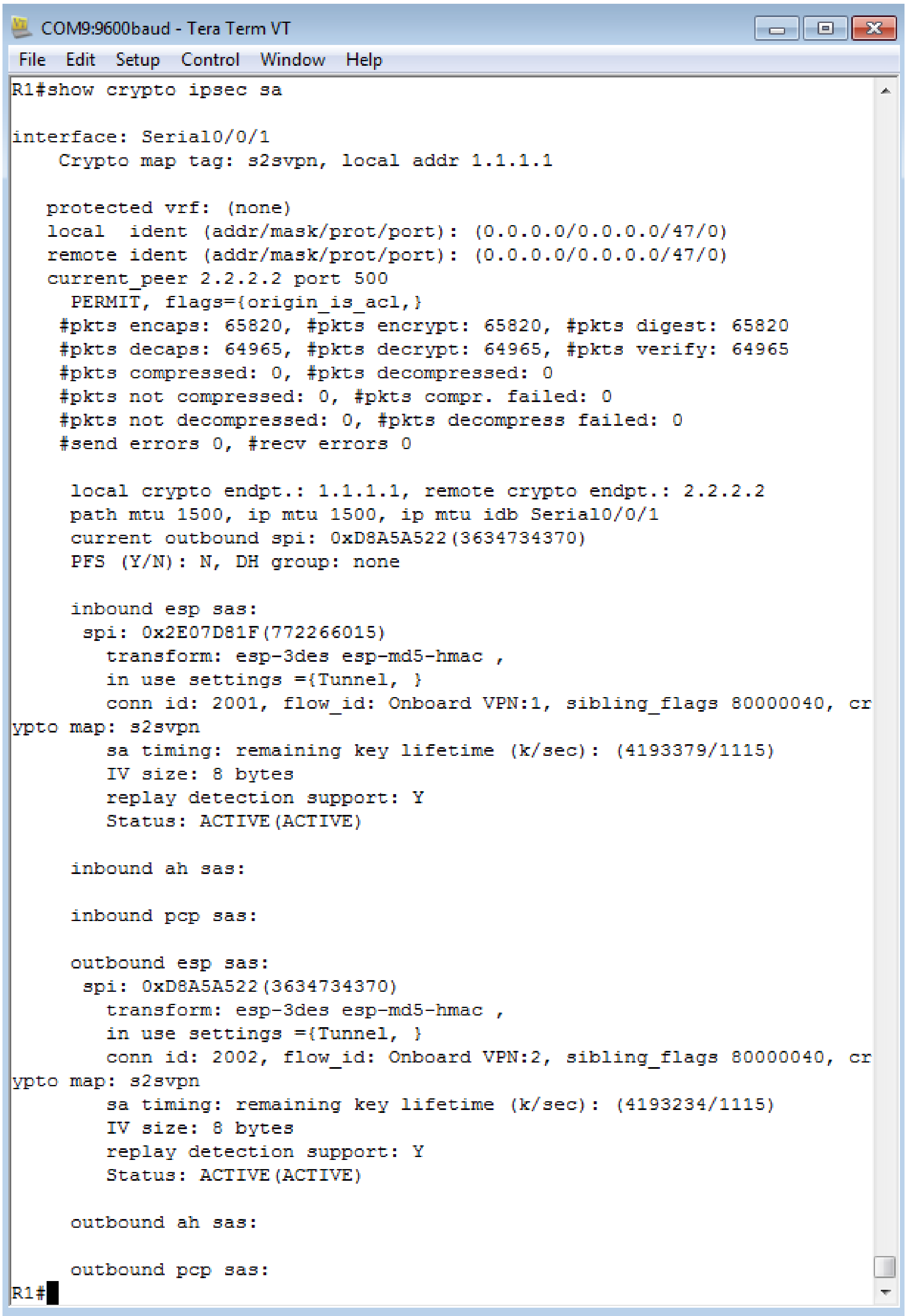
On R1 the command to check the Internet Security Association Management Protocol (ISAKMP) security associations (SAs) was entered, as is illustrated in figure 34.


COM9:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
2.2.2.2         1.1.1.1         QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA

R1#
```

Figure 34. Crypto ISAKMP SA on R1

Based on figure 34, the state QM_IDLE shows the ISAKMP SA is built between peers. Following the verification that ISAKMP was active, IPsec was then verified as up and running on R1 as shown in figure 35.

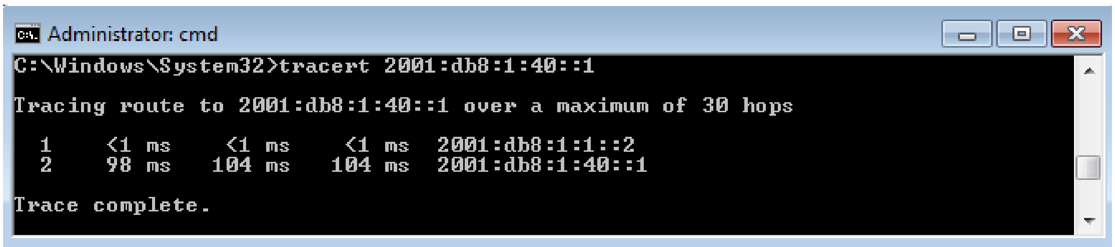

COM9:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
R1#show crypto ipsec sa

interface: Serial0/0/1
    Crypto map tag: s2svpn, local addr 1.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/47/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/47/0)
   current_peer 2.2.2.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 65820, #pkts encrypt: 65820, #pkts digest: 65820
    #pkts decaps: 64965, #pkts decrypt: 64965, #pkts verify: 64965
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 1.1.1.1, remote crypto endpt.: 2.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/1
     current outbound spi: 0xD8A5A522(3634734370)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x2E07D81F(772266015)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: Onboard VPN:1, sibling_flags 80000040, cr
ypto map: s2svpn
        sa timing: remaining key lifetime (k/sec): (4193379/1115)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xD8A5A522(3634734370)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: Onboard VPN:2, sibling_flags 80000040, cr
ypto map: s2svpn
        sa timing: remaining key lifetime (k/sec): (4193234/1115)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
R1#
```

Figure 35. Output of Crypto IPsec SA Command

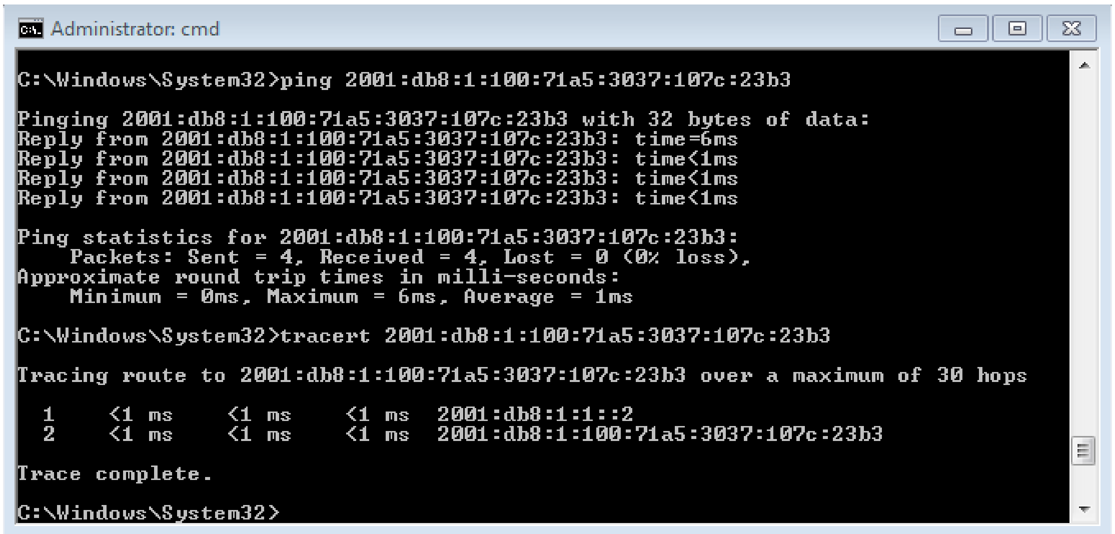
The output in figure 35 shows that IPsec SA is built between the peers. The encrypted tunnel is built between 1.1.1.1 (R1 Lo0) and 2.2.2.2 (R2 Lo0) for all the GRE protocol traffic. The two Encapsulation Security Payloads (ESP) SAs are built inbound and outbound and an Authentication Header (AH) is not used since there is no AH SAs.

The final check is to verify full connectivity across the network. In order to verify the connectivity and path preference, several ping and trace route commands were sent from PC2 to every node in the network. The result is demonstrated in figures 36, 37 and 38.



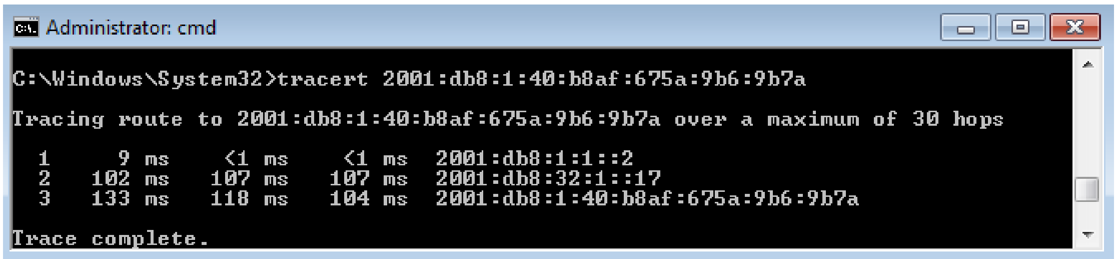
```
C:\Windows\System32>tracert 2001:db8:1:40::1

Tracing route to 2001:db8:1:40::1 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  2001:db8:1:1::2
  2    98 ms   104 ms   104 ms  2001:db8:1:40::1

Trace complete.
```

Figure 36. Trace Route Output from PC2 to R1 Lo1



```
C:\Windows\System32>ping 2001:db8:1:100:71a5:3037:107c:23b3

Pinging 2001:db8:1:100:71a5:3037:107c:23b3 with 32 bytes of data:
Reply from 2001:db8:1:100:71a5:3037:107c:23b3: time=6ms
Reply from 2001:db8:1:100:71a5:3037:107c:23b3: time<1ms
Reply from 2001:db8:1:100:71a5:3037:107c:23b3: time<1ms
Reply from 2001:db8:1:100:71a5:3037:107c:23b3: time<1ms

Ping statistics for 2001:db8:1:100:71a5:3037:107c:23b3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\Windows\System32>tracert 2001:db8:1:100:71a5:3037:107c:23b3

Tracing route to 2001:db8:1:100:71a5:3037:107c:23b3 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  2001:db8:1:1::2
  2    <1 ms    <1 ms    <1 ms  2001:db8:1:100:71a5:3037:107c:23b3

Trace complete.

C:\Windows\System32>
```

Figure 37. Ping from PC2 to PC3 Followed by Trace Route



```
C:\Windows\System32>tracert 2001:db8:1:40:b8af:675a:9b6:9b7a

Tracing route to 2001:db8:1:40:b8af:675a:9b6:9b7a over a maximum of 30 hops

  1     9 ms    <1 ms    <1 ms  2001:db8:1:1::2
  2   102 ms   107 ms   107 ms  2001:db8:32:1::17
  3   133 ms   118 ms   104 ms  2001:db8:1:40:b8af:675a:9b6:9b7a

Trace complete.
```

Figure 38. Trace Route Output from PC2 to PC4.

As figures 36, 37 and 38 demonstrate, pings were successful and there is full connectivity and the traceroute command demonstrates the path that the packets take. [5,637;19;20.]

4 Security Considerations

The deployment of IPv6 is constantly increasing within different organisations. For the successful deployment of IPv6, security and quality of service (QoS) is essential, and must be of a similar quality to that of the IPv4 infrastructure. Despite the security improvements made in the IPv6 protocol, IPv6 networks are still exposed to different types of attacks. Some types of IPv4 attacks are not necessarily eliminated in IPv6, and some attacks are associated with the IPv6 protocol operation itself. [21.]

4.1 Extension Header Threats

Based on the IETF specification, the EH and the order in which they should be chained in an IPv6 packet are as follows: IPv6 main header, Hop-by-Hop Options header, Destination Options header, Routing header, Fragment header, Authentication header, Encapsulating Security Payload header, Destination Options header and the Upper-layer header. An attacker is able to chain many EHs in order to pass through firewalls and intrusion detection systems. The attacker can also cause a DoS attack, as an intermediary device or a host might fail if they are incapable of processing many chained EHs.

The covert channel security attack allows the attacker to stealthily transfer information by using processes that are not allowed to communicate by computer security policy. Some fields in the IPv6 EH can be used to create a covert channel. The hop-by-hop options header is used to carry optional information and is the only EH that should be processed by every device in the network [1] and can contain the IPv6 Router Alert Option, which makes the router intercept and look further inside the datagram. Routers with inefficient hardware and slower software might be vulnerable to DoS attack if flooded by many router alerts.

Another EH threat is the Routing Header (RH) 0 which is a subtype of the RH. The packet construction allows multiple oscillations between two RH 0 processes or routers due to the fact that multiple intermediate addresses may be included in one RH 0 while the same address may be repeated many times. Amplification of a stream of packets on the path between two remote routers by an attacker will then be allowed which in turn could cause congestion along remote paths and in turn act as a DoS. The seriousness of this attack is due its effect on the entire path and not only on the local networks or nodes. The IPv6 RH 0 was deprecated due to these serious attacks [25]. Although header type 0 packets are deprecated, it nevertheless remains important to block potentially harmful traffic such as the RH0 or Hop-by-Hop (HbH) that may be directed toward the network. [1;22;23;24.]

4.2 First Hop Security (FHS) Concerns

FHS in IPv6 faces various local link (layer 2) security threats as the functionality in layer 2 operations in IPv6 differ from those of IPv4. Link operations, constrained by link boundaries necessitate a node communicating with its neighbours. Link operations include local network configuration, default gateway discovery and neighbor reachability tracking. The new patterns within the IPv6 link operations are very different to those of IPv4. They allow more end nodes on the link, thereby increasing the neighbor cache size on the end nodes and the default router which in turn increase the viability of DoS attacks. An additional threat in IPv6 is the protocols, Neighbor Discovery Protocol (NDP) and DHCP. Address management in IPv6 is de-centralised and could allow malicious hosts to abuse them.

4.2.1 Router Discovery Threats

Router discover, a new IPv6 process, where hosts can detect routers on an attached link, raises new FHS security issues.

Attacks against IPv6 Router Discovery

ICMPv6 messages, especially layer 2 multicast, are used by IPv6 neighbor discovery. ND is used by the hosts to locate the router on the attached link. As shown in figure 39, host A sends an ICMPv6, RS message to discover the router in its link. A legitimate router, shown as Router 1, responds with ICMPv6 router advertisement to let the hosts know it is the router on the link. Then the host A installs the default route in its routing table pointing to Router 1.

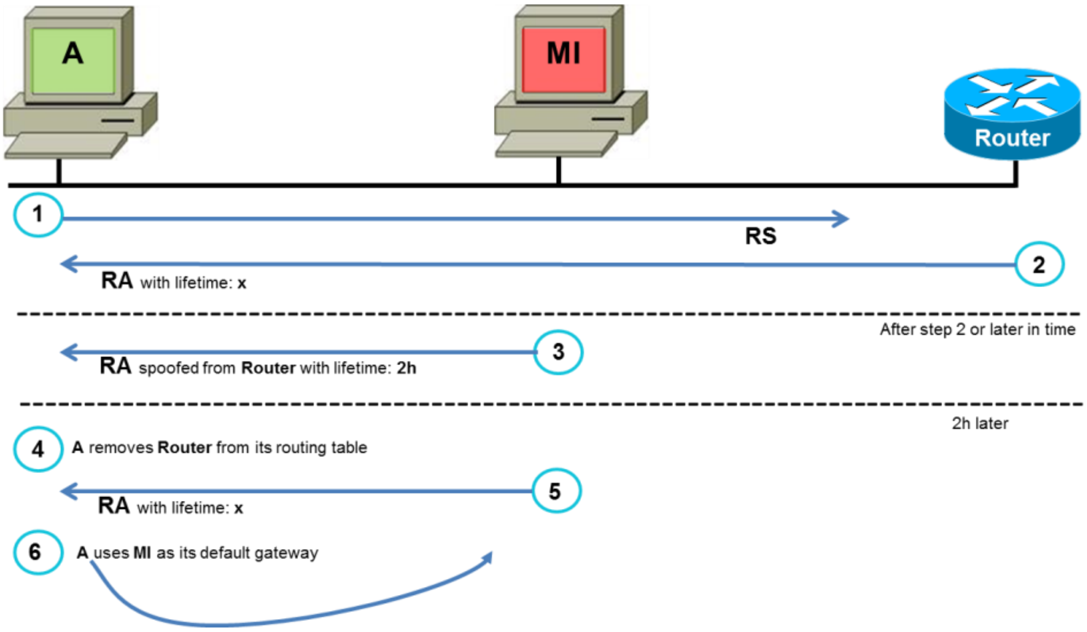

A
MI
Router
1
RS
2
RA with lifetime: x
After step 2 or later in time
3
RA spoofed from Router with lifetime: 2h
2h later
4
A removes Router from its routing table
5
RA with lifetime: x
6
A uses MI as its default gateway

Figure 39. IPv6 Router Discovery Attack

If a Malicious Intruder (MI), as shown in figure 39, is able to install itself in the link, MI could insert itself as the default router for host A, by spoofing the new router advertisement to host A from Router 1 and setting the life time to 2 hours. "If RemainingLifetime is less than or equal to 2 hours, ignore the Prefix Information option with regard to the valid lifetime, unless the Router Advertisement from which this option was obtained has been authenticated". [15]

Host A therefore removes the installed default routes to Router 1 after 2 hours. The MI is then able to send another router advertisement to insert itself as the default router. If the MI succeeds and becomes the default router, it will be able to see all the traffic from host A, and may gain additional information or deploy other types of attacks such as a MITM attack. [26.]

Stateless Address Autoconfiguration Attack

SLAAC eliminates the need for DHCP by enabling an endpoint to receive an IPv6 address automatically. This mechanism is stateless and therefore no address allocation tracking is required. It is based on the IPv6 prefix information in ICMPv6 router advertisements. Host A requests an IPv6 address and Router 1 responds with an offer and the host then checks the address availability by performing DAD, and then starts to use it, as the shown in figure 40.

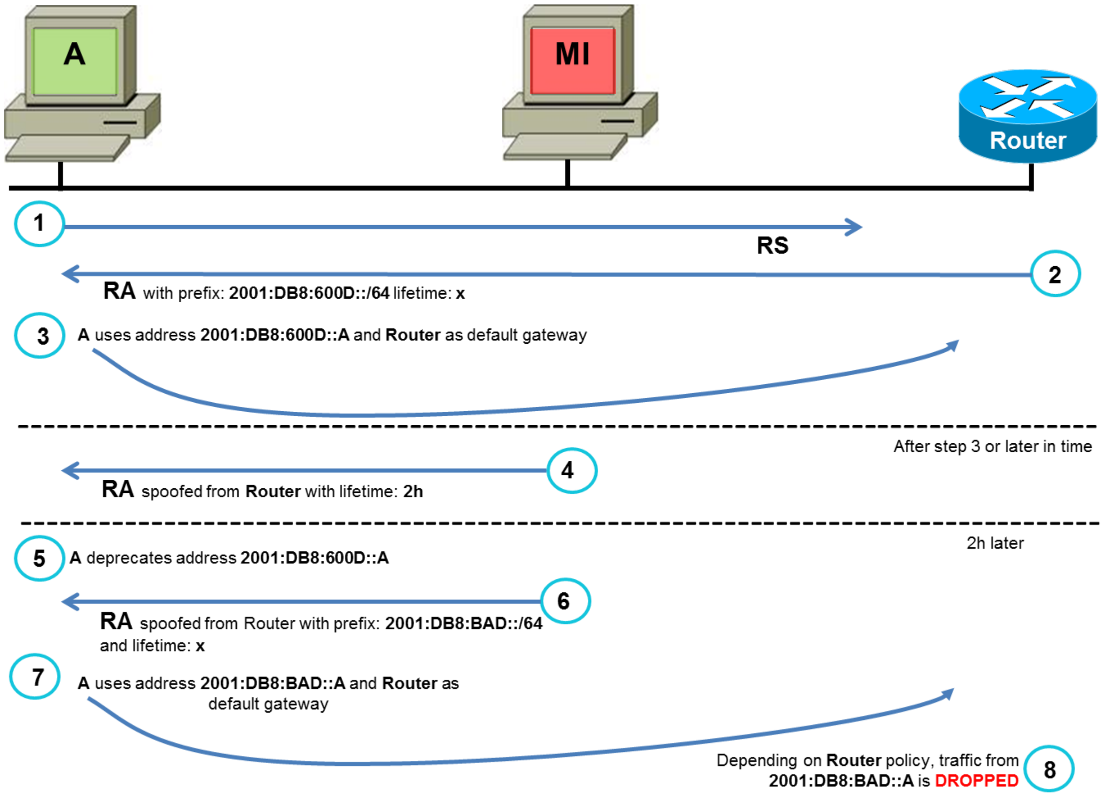

A
MI
Router
1
RS
2
RA with prefix: 2001:DB8:600D::/64 lifetime: x
3
A uses address 2001:DB8:600D::A and Router as default gateway
After step 3 or later in time
4
RA spoofed from Router with lifetime: 2h
2h later
5
A deprecates address 2001:DB8:600D::A
6
RA spoofed from Router with prefix: 2001:DB8:BAD::/64 and lifetime: x
7
A uses address 2001:DB8:BAD::A and Router as default gateway
Depending on Router policy, traffic from 2001:DB8:BAD::A is DROPPED
8

Figure 40. IPv6 Autoconfiguration Attack

As illustrated in figure 40, if a MI manages to insert itself into the link, it would be able to spoof an ICMPv6 router advertisement of Router 1 and set the life to 2 hours, using the same mechanisms as in the previous scenario. This results in the expiry of the host A address and the MI could send a new prefix through a router advertisement. Host A takes the new address and depending upon the Router 1 ACL, the new address may be denied access to the network. Without proper FHS and with IPv6 SLAAC in use, the MI, by spoofing two IPv6 router advertisements, could black hole hosts in their local link.

4.2.2 Neighbor Discovery Threats

For hosts, the ND is the same as router discovery and it performs processes such as DAD. In ND, ICMPv6 messages are responsible for network discovery in much the same way as in Router Discovery.

Address Resolution Attack

IPv4 uses ARP to discover another host's layer 2 address (MAC address), unlike IPv6 which uses ICMPv6 messages. As shown in figure 41, host A sends an ICMPv6 Neighbor Solicitation (NS) request to host B for its MAC address and host B responds with an ICMPv6 Neighbor Advertisement (NA) message. Host A learns the MAC address of host B and creates a neighbor cache entry that associates the MAC address of host B to its IPv6 address.

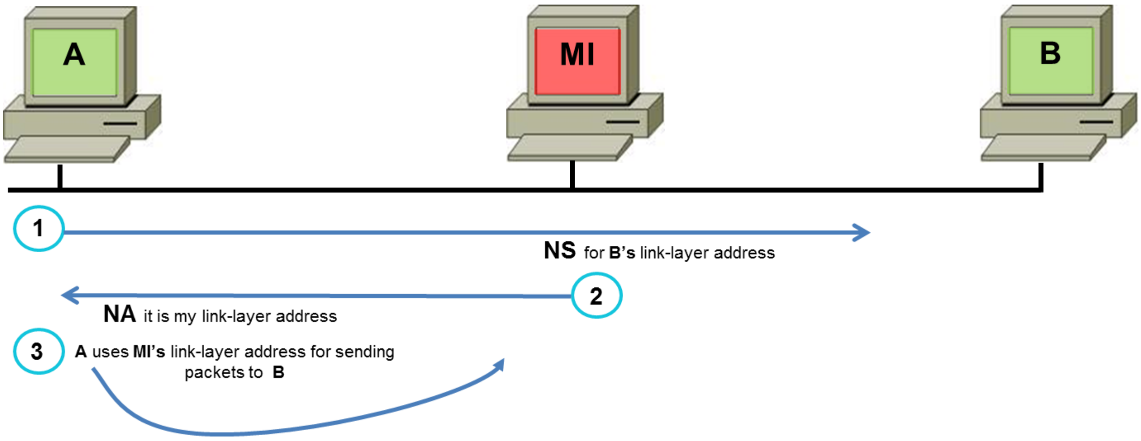

A
MI
B
1
NS for B's link-layer address
2
NA it is my link-layer address
3
A uses MI's link-layer address for sending packets to B

Figure 41. IPv6 Address Resolution Attack

If MI is able to insert itself in the link then it can impersonate host B and intercept all the traffic that was intended for host B, as is illustrated in figure 41. If FHS security is not configured properly, the MI can perform a MITM attack.

Duplicate Address Detection Attack

An endpoints uniqueness of an address is verified by the DAD protocol in IPv6. Figure 42 illustrates the steps of duplicate address attack.

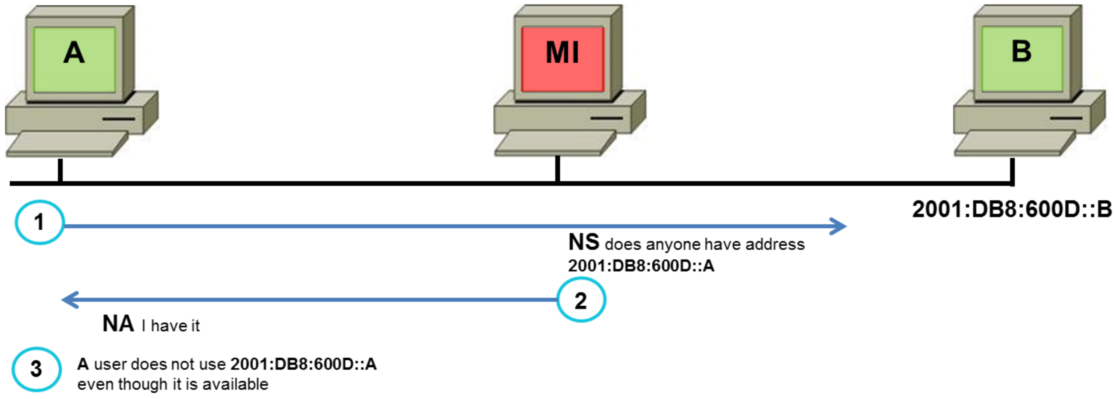

A
MI
B
2001:DB8:600D::B
1
NS does anyone have address 2001:DB8:600D::A
2
NA I have it
3
A user does not use 2001:DB8:600D::A even though it is available

Figure 42. Duplicate Address Detection Attack

When host A sends NS messages for checking by DAD, the MI can claim the address is in use as illustrated in figure 42. The MI, by claiming every address that host A tries to perform DAD on, prevents host A from getting an IPv6 address and therefore host A will not be able to communicate with the network.

Neighbor Cache Attack

A host creates a neighbor cache after resolving another host's MAC address. An interface identifier of an IPv6 address is 64 bits, resulting in the possibility of 2^{64} hosts on links and a corresponding 2^{64} neighbor cache entries. These entries in comparison to the ARP table size in IPv4 are significantly larger.

The steps in a neighbor cache attack are demonstrated in figure 43.

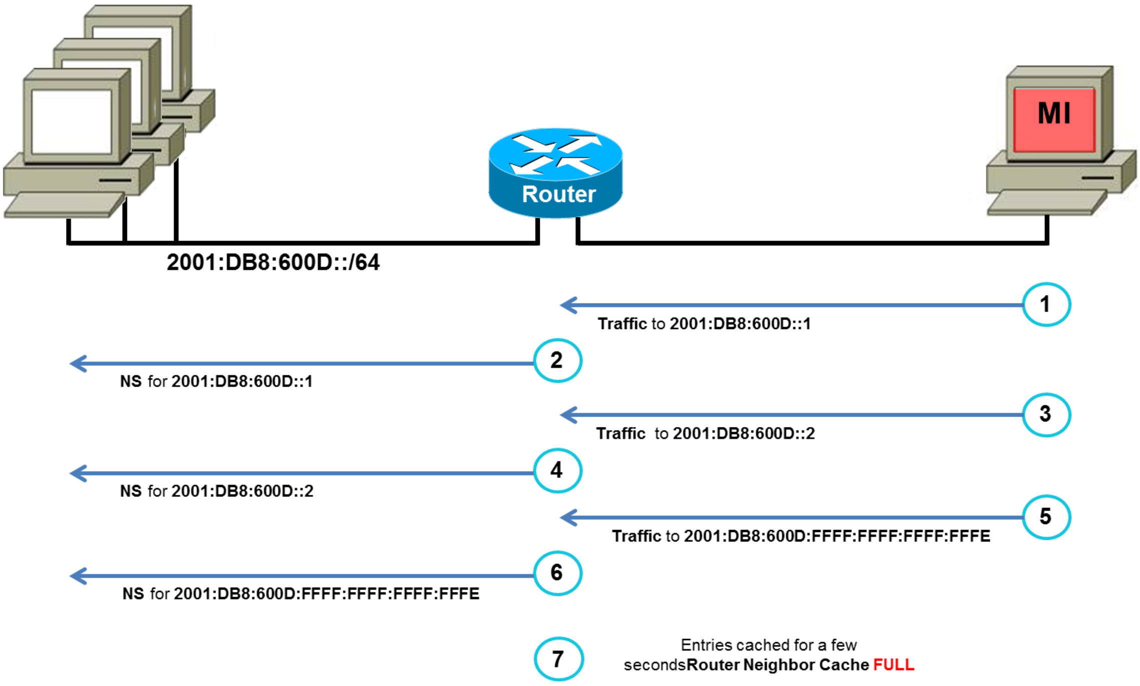

MI
Router
2001:DB8:600D::/64
1
Traffic to 2001:DB8:600D::1
2
NS for 2001:DB8:600D::1
3
Traffic to 2001:DB8:600D::2
4
NS for 2001:DB8:600D::2
5
Traffic to 2001:DB8:600D:FFFF:FFFF:FFFF:FFFE
6
NS for 2001:DB8:600D:FFFF:FFFF:FFFF:FFFE
7
Entries cached for a few secondsRouter Neighbor Cache FULL

Figure 43. Neighbor Cache Attack

The MI can cause DoS or simply fill the device cache entry by attacking the neighbor cache of the host or routing device, as illustrated in figure 43. If the MI connects to R1, and knows the network prefix that the hosts are connected to, it can scan the network by sending packets to hosts on the link. R1 tries to resolve the IPv6 address to forward the packets to their destination, irrespective of the presence of the destination host. R1’s neighbor cache will be filled with incomplete cache entries as result of absent hosts on the link until the timeout. In the event of the MI managing to scan a large portion of hosts within a few seconds, the cache entry of Router 1 could be filled and thereby cause a DoS condition.

Traditional IPv4 attacks using viruses and email worms still remain a threat in IPv6 and although network scanning in IPv6 is not easy they are possible and in addition other alternatives exist. As IPsec is not a mandatory specification of IPv6, IPv4 attacks such as sniffing and flooding remain the same. Most attacks occur on the application layer where IPsec is powerless to prevent them. [21.]

5 Security Recommendations

Security considerations are important but embedding best practice within the security policy and creating a security culture is vital. Some of the IPv6 security threats previously mentioned in section 4 and some of the best security practices follow below.

5.1 ICMPv6

ICMPv6 is essential for IPv6 functionality as it is used in establishing and maintaining communications. One method to eliminate threats associated with ICMPv6 messages, is ICMPv6 filtering. Establishing a strategy for filtering is of paramount importance as strict filtering can impact IPv6 communications. ICMPv6 messages should not be filtered by the ISP and instead should be left to the end users to create a policy on which communication elements to filter.

Due to the complexity of traffic an effective filtering strategy will be based on traffic type as not all traffic needs to be filtered. Traffic essential for network communication, establishment and maintenance, including error messages, connectivity checking messages and address configuration messages must never be dropped.

Creating a policy is strongly recommended as certain types of traffic such as redirect messages could pose a critical risk and filtering rules need to be defined. A situation based decision is needed for unallocated messages. Experimental allocation messages and informational message types that are not explicitly defined by IANA should be dropped. [27.]

5.2 Layer 3 Spoofing

Spoofing is an attack mechanism that forges source addresses. To block malicious IPv6 layer 3 traffic, Unicast Reverse Path Forwarding (unicast RPF) can be used. This protects the network by enabling routing devices to check the reachability of packet source addresses. Spoofed IP addresses are limited in the network as in packets with invalid source addresses will be discarded. [29.]

5.3 Extension Header

In order to secure the network from a possible EH attack, it is important to block such harmful traffic. R1 was configured with the following commands in order to block HbH and RH0 as demonstrated in listing 15, and the access list is applied on the incoming interface.

```
R1(config)#ipv6 access-list HBH
R1(config-ipv6-acl)#deny hbh any any
R1(config-ipv6-acl)#deny ipv6 any any routing-type 0
R1(config-ipv6-acl)#permit icmp any any
R1(config-ipv6-acl)#permit ipv6 any any

R1(config)#interface serial0/0/0
R1(config-if)#ipv6 traffic-filter HBH in
R1(config)#interface serial0/0/1
R1(config-if)#ipv6 traffic-filter HBH in
```

Listing 15. HbH Access List and the Interface Application

As shown in listing 15, the access list denies HbH and RH0 and permits ICMP and all other IPv6 traffic. IPv6 node tasks such as ND, depend on ICMPv6 functionality and in addition R1 needs to be able to send and reply to RS messages or sender nodes may experience DoS.

In order to avoid the possibility of a DoS, a router must be able to send and receive RS messages, which in addition to ND, is one of the tasks performed by the IPv6 nodes which in turn rely on ICMPv6 functionality.

5.4 Neighbor Discovery Protocol

The SEND protocol is designed to secure NDP Vulnerabilities, particularly within a wireless environment where physical link security is not guaranteed. Cryptography can be used to secure IPv6 and MAC association as well as SLAAC. The Rivest, Shamir and Adelman (RSA) signature will affect performance and port security is needed to associate the port with the MAC address. IPsec is limited to manual configuration in NDP, due to Internet Key Exchange (IKE) bootstrapping problems and is therefore not the preferred solution. [28.]

5.5 Secure Transitioning

Due to dual-stack running both IPv4 and IPv6, it is vulnerable to attacks to both protocols. Host security on a dual-stack network is of importance as it is needed to inspect and block from each stack. In a dual-stack network, if a host is running IPv4 and is protected, the IPv6 is enabled by default and the host does not run IPv6, it is prone to attacks. An attacker can send Router Advertisements and configure the host to IPv6 and perform various attacks. Best practice is to disable IPv6 on the host running IPv4 only or to configure the network with IPv6. All IPv6 tunnelling mechanisms provide a solution for the IPv6 connectivity however IPsec is the only tunnelling mechanism that provides authentication. [30.]

6 Results

The CW network represents a typical IPv4 infrastructure and is the baseline for this project. Currently IPv4 is the predominant protocol used by enterprises, however due to limited IPv4 availability for expansion, and the fact that the Internet is moving to be fully IPv6 compliant, the only solution is to migrate to IPv6. By taking these factors into account, networking practices need to adapt to IPv6. With this in mind the network was designed using two completely different implementations to reflect the real case scenarios faced by an average enterprise. These realistically represent the options and probable preferred solutions chosen for the needs of the different network environments. Choices of network design were based on factors such as timescale, cost efficiency, scalability, available expertise and infrastructure readiness.

The first scenario represents a case where the ISP was able to offer IPv6 support and therefore the best practice would be to use the dual-stack mechanism. After each phase was configured, the network connectivity was tested before proceeding further. In the case of encountering a configuration error, the network behaviour was carefully monitored in order to detect the cause of errors thereby enabling immediate remediation. Due to the complexity of the IPv6 address structure, in order to avoid human error, a logical addressing scheme was crucial. A challenge that arose was that the HQ area 0 was running OSPFv2 and was unable to communicate with the rest of network due to the fact that OSPFv2 and OSPFv3 operate separately. In order to overcome the issue area 0 was configured to run OSPFv3.

As a result of these changes, IGP routes were learned and this was verified by using various show commands on the routing devices. Connectivity between domains was successfully established and tested by using ping commands. The traceroute command output, demonstrated that, by dual-stacking, the IPv6 traffic navigated the route via ISP1.

In the second scenario, the ISP was unable to provide IPv6 services and therefore the only option was to use a tunnelling mechanism to provide IPv6 connectivity. The GRE protocol was chosen as the tunnelling protocol. The tunnel was configured between the two edge routers and the show command for the tunnel verified that the tunnel interface was up. Connectivity between IPv6 domains was verified using various extended pings on all the network devices. The IPv6 traffic travelled through the tunnel to its destination, as was confirmed by the use of the traceroute command. To overcome the absence of security in the GRE protocol tunnel, IPsec was configured to encrypt the data flow between the sites. When IPsec errors were encountered, the first troubleshooting step was to check for key mismatch as a result of spelling errors and secondly to ensure that the crypto map was applied to the correct interfaces. Operation of IPsec was confirmed with the use of `debug crypto ipsec` and `show crypto ipsec sa` commands.

The ping results confirmed successful connectivity over the IPv4 networks as well as IPv6 networks. The network performed as designed, as was validated by full connectivity and therefore the goal of the project was achieved.

7 Discussion

IPv6 is a reality and over time will replace IPv4. Fully transitioning to IPv6 is disruptive, expensive, time-intensive and requires staff training. Transitioning mechanisms provide alternative solutions by allowing gradual network migration in a cost-efficient manner. Two of the most common implementations were practiced in this project.

Dual-stack allows for both protocols to run independently of each other, to share network resources and to allow for native packet forwarding without additional encapsulation and overhead. Over time, the IPv4 protocol can be replaced by the IPv6 protocol. Disadvantages to using dual-stack are the network resources required to keep data related to both protocols, such as two routing table and two topology tables. The administrative overhead increases due to the extra staff training and the complexity of the network maintenance and troubleshooting. In a dual-stack environment, security is essential, as all the threats to both protocols still exists. Another limiting factor is that IPv6 needs to be enabled from the ISP across the entire network to the client site.

Another cost-effective approach is the tunnelling mechanism, which allows IPv6 domains to connect over an IPv4 backbone, by utilising routing based on labels. This method requires no additional core router configuration and few backbone infrastructure upgrades. The downsides of tunnelling are that the underlying infrastructure services are not available, the users of the different protocols cannot communicate without dual-stack hosts, and the administration overhead increases as the number of tunnels grow.

Security is of paramount importance in the migration process. IPsec is only a recommendation and therefore without IPsec, IPv6 is very similar to IPv4. A number of FHS concerns arise requiring appropriate protection mechanisms due to the functionality of ICMPv6. Layer 3 and above threats are almost identical to IPv4 threats, as well as application layer attacks and mitigation techniques.

When deciding to migrate to IPv6, there are various migration strategies available. The logical planning and design should be based on the existing infrastructure, future scalability, available technical knowledge and support.

8 Conclusion by Michael Swanson

The goal of this project was to transition an existing IPv4 network to IPv6 utilising the best and most practical methods available. In order to effectively demonstrate the transitional processes, two likely scenarios were used to represent real challenges faced by enterprises attempting this. The basic scenarios were very real situations that enterprises are likely to face when addressing this issue. In the case of dual-stack, the ISP is able to provide support for IPv6 and in the case of the tunnel, the ISP is unable to provide support for IPv6.

After dual-stack was implemented, the network was extensively tested and performed as designed. The tunnel implementation was also successful and the network traffic successfully negotiated the tunnel link and performed as designed.

There are advantages to using transition mechanisms instead of implementing a native IPv6 network transitioning to IPv6. Some of the most obvious include cost as well as training administrators. An additional advantage however is that once a transition mechanism is in place, the network can function on IPv4 for as long as needed without implementing IPv6 natively. Disadvantages include having to run two different protocols and a lag in network speed due to the mechanisms themselves.

Limitations were placed on the project by constraints such as the limited number of devices in the network, thereby restricting the number of different options that were able to be utilised. Though security and other mechanisms were implemented in this network, not every mechanism or protocol can be run on the limited network size and therefore the small scale of the network, in my opinion cannot truly reflect a real-life scenario. The network encompasses the most commonly used protocol, OSPF, as well as addresses security issues that these networks should be aware of.

In achieving the goal of implementing a transition to IPv6, addressing many issues associated with the implementation and documenting each stage, we have achieved our stated objective and in the process have created a useful roadmap for anyone considering the change to benchmark against their network.

9 Conclusion by Maryam Tavakoli Momtaz

The goal of the project was to build a network and implement the most practised transitioning mechanisms to the IPv6. Two separate networks were built to accommodate the two most possible scenarios in reality. The transitioning to IPv6 is an involved implementation that requires considerations and extensive evaluations of network elements and the needed services from the network. ISP’s ability to provide the necessary services and support for IPv6, determines the mechanisms that an enterprise should implement. When the ISP is IPv6-enabled or is able provide support for IPv6, the best practice is to use dual-stack mechanism, which was implemented in the first scenario in this project. Dual-stack has several benefits. It is cost and time efficient and the network can gradually remove the IPv4 and become a native IPv6 network.

Transitioning to IPv6 largely depends on the region and its need to move to IPv6, and therefore it is realistic that the ISPs are not able to provide the necessary support to route IPv6. Tunnelling was implemented in the second scenario to demonstrate this mechanism and how to connect the IPv6 domains over and the IPv4 core network. Tunnelling has several benefits and allows the underlying network to function normally as it provides the IPv6 connection. The most important consideration is security which can be provided by IPsec.

Due to limitations of implementing a larger network in the lab environment, the network was designed to reflect a real, small to average size enterprise network. However the network is scalable and the methods are applicable to a network of any size. Security is of importance when it comes to a network and with IPv6 introduction to networks and transitioning mechanisms, the network needs to be secured against attacks to both protocols. Further studies and practices can expose possible threats and provide the best security practices.

References

1. RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, S. Deering, R. Hinden (December 1998) [online].
   URL: http://tools.ietf.org/html/rfc2460. Accessed 6 October 2014

2. Data gathered from ITU World Telecommunication/ICT Indicators database (23 December 2014) [online].
   URL: http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/ITU_Key_2005-2014_ICT_data.xls. Accessed 22 January 2015.

3. Free Pool of IPv4 Address Space Depleted (3 February 2011) [online].
   URL: https://www.nro.net/news/ipv4-free-pool-depleted. Accessed 7 September 2014.

4. Remaining IPv4 Addresses to be Redistributed to Regional Internet Registries | Address Redistribution Signals that IPv4 is Nearing Total Exhaustion (20 May 2014) [online].
   URL: https://www.icann.org/news/announcement-2-2014-05-20-en. Accessed 7 September 2014.

5. Teare Diane. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide Foundation learning for the ROUTE 642-902 Exam. Cisco Press; 2010.

6. RFC 2373, IP Version 6 Addressing Architecture, S. Deering, R. Hinden (July 1998) [online].
   URL: http://www.ietf.org/rfc/rfc2373.txt. Accessed 14 January 2015.

7. RFC 5340, OSPF for IPv6, R. Coltun, D. Ferguson, J. Moy, A. Linden (July 2008) [online].
   URL: https://tools.ietf.org/html/rfc5340. Accessed 15 January 2015.

8. RFC 1371, Choosing a "Common IGP" for the IP Internet (The IESG's Recommendation to the IAB), P. Gross (October 1992) [online].
   URL: https://tools.ietf.org/html/rfc1371. Accessed 20 October 2014.

9. IP Routing: OSPF Configuration Guide, Cisco IOS Release 15SY OSPFv3 Address Families (2015) [online].
   URL: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15-sy/iro-15-sy-book/ip6-route-ospfv3-add-fam.html. Accessed 22 May 2015.

10. RFC 6180, Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment, J. Arkko, F. Baker (May 2011) [online].
    URL: https://tools.ietf.org/html/rfc6180. Accessed 11 November 2014.

11. Deploying IPv6 in the Internet Edge, Shannon McFarland (1 May 2012) [online].
    URL: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Internet_Edge/InternetEdgeIPv6.html. Accessed 26 February 2015.

12. IP Routing Sample Configuration for BGP with Two Different Service Providers (Multihoming) (17 August 2005) [online].
URL: http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/23675-27.html. Accessed 16 April 2015.

13. IP Routing Troubleshooting Flapping BGP Routes (Recursive Routing Failure) (10 August 2005) [online].
URL: http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/19167-bgp-rec-routing.html. Accessed 16 April 2015.

14. RFC 4193, Unique Local IPv6 Unicast Addresses, R. Hinden, B. Haberman (October 2005) [online].
URL: https://tools.ietf.org/html/rfc4193. Accessed 4 November 2014.

15. Quoted from RFC 4862, IPv6 Stateless Address Autoconfiguration, S. Thomson, T. Narten, T. Jinmei (September 2007) [online].
URL: https://tools.ietf.org/html/rfc4862. Accessed 17 March 2015.

16. RFC 2740, OSPF for IPv6 R. Coltun, D. Ferguson, J. Moy (December 1999) [online]. URL: https://tools.ietf.org/html/rfc2740. Accessed 25 April 2015

17. IP Routing: OSPF Configuration Guide, Cisco IOS XE Release 3S OSPFv3 Address Families (2015) [online].
URL: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-3s/iro-xe-3s-book/ip6-route-ospfv3-add-fam-xe.html. Accessed 25 April 2015.

18. RFC 3904, Evaluation of IPv6 Transition Mechanisms for Unmanaged Networks R. Austein, S. Satapati, R. van der Pol (September 2004) [online].
URL: https://www.ietf.org/rfc/rfc3904.txt. Accessed 21 October 2014.

19. RFC 2406, IP Encapsulating Security Payload (ESP) S. Kent, R. Atkinson (November 1998) [online].
URL: https://www.ietf.org/rfc/rfc2406. Accessed 21 May 2015.

20. Cisco IOS Security Configuration Guide, Release 12.2 Configuring IPSec Network Security (2001 - 2006) [online].
URL: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfipsec.html#wp1000900. Accessed 21 May 2015.

21. IPv6 First-Hop Security Concerns [online].
URL: http://www.cisco.com/web/about/security/intelligence/ipv6_first_hop.html. Accessed 3 November 2014

22. Intrusion Detection FAQ: What is covert channel and what are some examples? Aman Abdulla [online].
URL: http://www.sans.org/security-resources/idfaq/covert_chan.php. Accessed 24 April 2015.

23. RFC 6564, A Uniform Format for IPv6 Extension Headers S. Krishnan, J. Woodyatt, E. Kline, J. Hoagland, M. Bhatia (April 2012) [online].
URL: https://tools.ietf.org/html/rfc6564. Accessed 2 March 2015.

24. RFC 2711, IPv6 Router Alert Option C. Partridge, A. Jackson (October 1999) [online].
URL: https://tools.ietf.org/html/rfc2711. Accessed 1 April 2015.

25. RFC 5095, Deprecation of Type 0 Routing Headers in IPv6 J. Abley, P. Savola, G. Neville-Neil (December 2007) [online].
URL: https://tools.ietf.org/html/rfc5095. Accessed 9 April 2015.

26. RFC 4861, Neighbor Discovery for IP version 6 (IPv6) T. Narten, E. Nordmark, W. Simpson, H. Soliman (September 2007) [online].
URL: https://tools.ietf.org/html/rfc4861. Accessed 3 November 2014.

27. RFC 4890, Recommendations for Filtering ICMPv6 Messages in Firewalls E. Davies, J. Mohacsi (May 2007) [online].
URL: https://tools.ietf.org/html/rfc4890. Accessed 28 April 2015.

28. RFC 3971, SEcure Neighbor Discovery (SEND) J. Arkko, J. Kempf, B. Zill, P. Nikander (March 2005) [online].
URL: https://tools.ietf.org/html/rfc3971. Accessed 5 May 2015.

29. Understanding Unicast Reverse Path Forwarding [online].
URL: http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html. Accessed 25 February 2015.

30. IPv6 Security Best Practices E. Vyncke (2007) [online].
URL: http://www.cisco.com/web/SG/learning/ipv6_seminar/files/02Eric_Vyncke_Security_Best_Practices.pdf. Accessed 2 April 2015.

31. IPSec Negotiation IKE Protocols IPsec Troubleshooting: Understanding and Using debug Commands Document ID: 5409 (15 July 2009) [online].
URL: http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html. Accessed 7 April 2015.

Appendix 1: Router 1 Running Configuration

```
R1#show running-config
Building configuration...

Current configuration : 3984 bytes
!
! Last configuration change at 14:50:40 UTC Mon May 18 2015
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 cef
ip auth-proxy max-login-attempts 5
ip admission max-login-attempts 5
!
no ip domain lookup
ip cef
!
multilink bundle-name authenticated
!
license udi pid CISCO2911/K9 sn FCZ1627202V
!
redundancy
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key thesis-10 address 2.2.2.2
!
crypto ipsec transform-set thesis0 esp-3des esp-md5-hmac
!
crypto map s2svpn local-address Loopback0
crypto map s2svpn 10 ipsec-isakmp
 set peer 2.2.2.2
 set transform-set thesis0
 match address 101
!
interface Loopback0
 description R1 loopback
 ip address 1.1.1.1 255.255.255.255
 ipv6 enable
 ospfv3 2 area 0 ipv4
!
interface Loopback1
```

```
 description ipv6 R1 loopback
 no ip address
 ipv6 address 2001:DB8:1:4::1/128
 ospfv3 1 area 3 ipv6
!
interface Tunnel10
 no ip address
 ip mtu 1400
 ipv6 address 2001:DB8:32:1::17/127
 ospfv3 1 area 0 ipv6
 tunnel source Loopback0
 tunnel destination 2.2.2.2
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description HQ VLAN 10
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 enable
 ospfv3 2 area 0 ipv4
!
interface GigabitEthernet0/1
 description ENG VLAN 40
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:1:40::1/64
 ipv6 enable
 ospfv3 1 area 3 ipv6
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 description R1->ISP1
 ip address 150.50.50.1 255.255.255.252
 ipv6 address 2001:DB8:60:1::61/127
 ipv6 traffic-filter HBH in
!
interface Serial0/0/1
 description R1->ISP2
 ip address 30.50.50.1 255.255.255.252
 ipv6 traffic-filter HBH in
 crypto map s2svpn
!
router ospfv3 2
 !
 address-family ipv4 unicast
  default-information originate always metric 100
  area 0 range 1.1.1.1 255.255.255.255
  area 0 range 172.16.1.0 255.255.255.0
 exit-address-family
```

```
!
router ospfv3 1
 router-id 1.1.1.1
 ignore lsa mospf
 auto-cost reference-bandwidth 1000
 !
 address-family ipv6 unicast
  area 3 range 2001:DB8:1:4::1/128
  area 3 range 2001:DB8:1:40::/64
  default-information originate always metric 100
  redistribute static
 exit-address-family
!
router bgp 500
 bgp log-neighbor-changes
 bgp dampening
 network 1.1.1.1 mask 255.255.255.255
 network 172.16.1.0 mask 255.255.255.0
 neighbor 30.50.50.2 remote-as 200
 neighbor 30.50.50.2 distribute-list 1 out
 neighbor 150.50.50.2 remote-as 100
 neighbor 150.50.50.2 distribute-list 1 out
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 150.50.50.2 210
ip route 0.0.0.0 0.0.0.0 30.50.50.2 220
!
access-list 1 permit 1.1.1.1
access-list 1 permit 172.16.1.0 0.0.0.255
access-list 101 permit gre any any
ipv6 route ::/0 Tunnel10 FE80::DA67:D9FF:FE84:20B8
ipv6 route ::/0 Serial0/0/0 FE80::DA67:D9FF:FE84:2108
!
ipv6 access-list HBH
 deny hbh any any
 deny ipv6 any any routing-type 0
 permit icmp any any
 permit ipv6 any any
!
control-plane
!
banner exec ^CC!!!BEWARE!!!Unauthorised access to this device is prohibited^C
banner login ^CC!!!STOP!!!Unauthorised access to this device is prohibited^C
banner motd ^CC!!!WAIT!!!Unauthorised access to this device is prohibited^C
!
line con 0
 exec-timeout 0 0
 password 7 0958460C0A0C04
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 password 7 0958460C0A0C04
 login
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password 7 0835444B1A1016
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Appendix 2: Router 2 Running Configuration

```
R2#show running-config
Building configuration...

Current configuration : 4086 bytes
!
! Last configuration change at 14:48:41 UTC Mon May 18 2015
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 cef
ip auth-proxy max-login-attempts 5
ip admission max-login-attempts 5
!
no ip domain lookup
ip cef
!
multilink bundle-name authenticated
!
license udi pid CISCO2911/K9 sn FCZ1627202Q
!
redundancy
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key thesis-10 address 1.1.1.1
!
crypto ipsec transform-set thesis0 esp-3des esp-md5-hmac
!
crypto map s2svpn local-address Loopback0
crypto map s2svpn 10 ipsec-isakmp
 set peer 1.1.1.1
 set transform-set thesis0
 match address 101
!
interface Loopback0
 description R2 loopback
 ip address 2.2.2.2 255.255.255.255
 ipv6 enable
 ospfv3 2 area 1 ipv4
!
interface Loopback1
```

```
 description IPv6 R2 loopback
 no ip address
 ipv6 address 2001:DB8:1:2::2/128
 ospfv3 1 area 1 ipv6
!
interface Tunnel10
 no ip address
 ip mtu 1400
 ipv6 address 2001:DB8:32:1::16/127
 ospfv3 1 area 0 ipv6
 tunnel source Loopback0
 tunnel destination 1.1.1.1
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description FIN VLAN 20
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2001:DB8:1:1::2/64
 ipv6 address FD01:DB8:1:1::/64 eui-64
 ospfv3 1 area 1 ipv6
 ospfv3 2 area 1 ipv4
!
interface GigabitEthernet0/1
 description RES VLAN 30
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:1:100::2/64
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 description R2->ISP2
 ip address 32.50.50.1 255.255.255.252
 ipv6 traffic-filter HBH in
 crypto map s2svpn
!
interface Serial0/0/1
 description R2->ISP1
 ip address 152.50.50.1 255.255.255.252
 ipv6 address 2001:DB8:50:1::51/127
 ipv6 traffic-filter HBH in
!
router ospfv3 2
 !
 address-family ipv4 unicast
  default-information originate always metric 100
  area 1 range 2.2.2.2 255.255.255.255
  area 1 range 192.168.1.0 255.255.255.0
 exit-address-family
```

```
!
router ospfv3 1
 router-id 2.2.2.2
 ignore lsa mospf
 auto-cost reference-bandwidth 1000
 !
 address-family ipv6 unicast
  area 0 range 2001:DB8:32:1::16/127
  area 1 range 2001:DB8:1:1::/64
  area 1 range 2001:DB8:1:2::2/128
  area 1 range 2001:DB8:1:100::/64
  default-information originate always metric 100
  redistribute static
 exit-address-family
!
router bgp 600
 bgp log-neighbor-changes
 bgp dampening
 network 2.2.2.2 mask 255.255.255.255
 network 192.168.1.0
 neighbor 32.50.50.2 remote-as 200
 neighbor 32.50.50.2 distribute-list 1 out
 neighbor 152.50.50.2 remote-as 100
 neighbor 152.50.50.2 distribute-list 1 out
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 152.50.50.2 210
ip route 0.0.0.0 0.0.0.0 32.50.50.2 220
!
access-list 1 permit 2.2.2.2
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 101 permit gre any any
ipv6 route ::/0 Serial0/0/1 FE80::DA67:D9FF:FE84:2108
ipv6 route ::/0 Tunnel10 FE80::DA67:D9FF:FE84:1898
!
ipv6 access-list HBH
 deny hbh any any
 deny ipv6 any any routing-type 0
 permit icmp any any
 permit ipv6 any any
!
control-plane
!
banner exec ^CC!!!BEWARE!!!Unauthorised access to this device is prohibited^C
banner login ^CC!!!STOP!!!Unauthorised access to this device is prohibited^C
banner motd ^CC!!!WAIT!!!Unauthorised access to this device is prohibited^C
!
line con 0
 exec-timeout 0 0
 password 7 13111F17180517
 logging synchronous
 login
```

```
line aux 0
 exec-timeout 0 0
 password 7 13111F17180517
 login
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password 7 15060309172338
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Appendix 3: ISP1 Running Configuration

```
ISP1#show running-config
Building configuration...

Current configuration : 2589 bytes
!
! Last configuration change at 14:56:55 UTC Mon May 18 2015
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ipv6 unicast-routing
ipv6 cef
ip auth-proxy max-login-attempts 5
ip admission max-login-attempts 5
!
no ip domain lookup
ip cef
!
multilink bundle-name authenticated
!
license udi pid CISCO2911/K9 sn FCZ1627202L
!
redundancy
!
interface Loopback0
 description ISP Internet network
 ip address 10.10.10.1 255.255.255.0
!
interface Loopback1
 no ip address
 ipv6 address 3001:DB8::10/128
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
```

```
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 description ISP->R1
 ip address 150.50.50.2 255.255.255.252
 ipv6 address 2001:DB8:60:1::60/127
 clock rate 128000
!
interface Serial0/0/1
 description ISP1->R2
 ip address 152.50.50.2 255.255.255.252
 ipv6 address 2001:DB8:50:1::50/127
 clock rate 128000
!
interface Serial0/1/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
!
router bgp 100
 bgp log-neighbor-changes
 bgp dampening
 network 10.10.10.0 mask 255.255.255.0
 neighbor 150.50.50.1 remote-as 500
 neighbor 152.50.50.1 remote-as 600
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ipv6 route 2001:DB8:1:1::/64 2001:DB8:50:1::51
ipv6 route 2001:DB8:1:2::2/128 2001:DB8:50:1::51
ipv6 route 2001:DB8:1:4::1/128 2001:DB8:60:1::61
ipv6 route 2001:DB8:1:40::/64 2001:DB8:60:1::61
ipv6 route 2001:DB8:1:100::/64 2001:DB8:50:1::51
!
control-plane
!
banner exec ^CC!!!BEWARE!!!Unauthorised access to this device is prohibited^C
banner login ^CC!!!STOP!!!Unauthorised access to this device is prohibited^C
banner motd ^CC!!!WAIT!!!Unauthorised access to this device is prohibited^C
!
line con 0
 exec-timeout 0 0
 password 7 105A011C161E01
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 password 7 105A011C161E01
 login
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password 7 13111F17180517
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Appendix 4: ISP2 Running Configuration

```
ISP2#show running-config
Building configuration...

Current configuration : 2049 bytes
!
! Last configuration change at 14:38:51 UTC Mon May 18 2015
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
no ipv6 cef
ip auth-proxy max-login-attempts 5
ip admission max-login-attempts 5
!
no ip domain lookup
ip cef
!
multilink bundle-name authenticated
!
license udi pid CISCO2911/K9 sn FCZ1627202T
!
redundancy
!
interface Loopback0
 description ISP2 Internet network
 ip address 20.20.20.1 255.255.255.0
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 description ISP2->R2
 ip address 32.50.50.2 255.255.255.252
 clock rate 128000
!
interface Serial0/0/1
 description ISP2->R1
 ip address 30.50.50.2 255.255.255.252
 clock rate 128000
!
router bgp 200
 bgp log-neighbor-changes
 bgp dampening
 network 20.20.20.0 mask 255.255.255.0
 neighbor 30.50.50.1 remote-as 500
 neighbor 32.50.50.1 remote-as 600
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner exec ^CC!!!BEWARE!!!Unauthorised access to this device is prohibited^C
banner login ^CC!!!STOP!!!Unauthorised access to this device is prohibited^C
banner motd ^CC!!!WAIT!!!Unauthorised access to this device is prohibited^C
!
line con 0
 exec-timeout 0 0
 password 7 105A011C161E01
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 password 7 105A011C161E01
 login
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password 7 15060309172338
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Appendix 5: Switch 1 Running Configuration

```
SW1#show running-config
Building configuration...

Current configuration : 7293 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname SW1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
system mtu routing 1500
!
!
ip dhcp snooping vlan 10
ip dhcp snooping
no ip domain-lookup
!
!
crypto pki trustpoint TP-self-signed-112546176
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-112546176
 revocation-check none
 rsakeypair TP-self-signed-112546176
!
!
crypto pki certificate chain TP-self-signed-112546176
 certificate self-signed 01
  30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101
05050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D
43657274
  69666963 6174652D 31313235 34363137 36301E17 0D393330 33303130
30303035
  365A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403
1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3131
32353436
  31373630 819F300D 06092A86 4886F70D 01010105 0003818D 00308189
02818100
  C7FF4C1A F19F00EA 12A0EAC5 1F7F6E5D B9610DB9 C7FAA642 BE223FEF
E446D1CC
  3861757F 0CE14D5C 8DE50702 98A58C6B E532D0C4 6D8153ED 79EE1E85
F1B35929
  4AB7A172 6BF77748 362A89A1 B29CFD74 BB16544A B8D92BCF 679CDAFD
DEC7C36A
  9F172919 0EF1BBF1 B7BF2577 F9A6B4E6 63A6A0E7 ABFB6DFF B3FD788B
3E00717B
```

```
  02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F
0603551D
  23041830 16801433 48C406AE 821DC418 25BD1BB9 F77086FB 6B89B230
1D060355
  1D0E0416 04143348 C406AE82 1DC41825 BD1BB9F7 7086FB6B 89B2300D
06092A86
  4886F70D 01010505 00038181 00BA17BC 56745BFE 0842F952 4ABD8B06
F0268C7E
  B73D72D1 8367A00A C4086668 372F228C A0D04EAC 3BFAD557 2D7B76CE
0D35E579
  19C864F3 F87324FA F6A44F5F 68337D14 48B98624 CD1D52EA AF79F4DD
A6643230
  2D222C90 7E233374 5B8E72F4 92C0AE38 FD10B40E 174F4DE0 A1A8B515
9B3A2581
  38447DC8 94533E95 E00D1F3B 3A
        quit
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
!
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 ip dhcp snooping trust
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
 ip dhcp snooping trust
!
interface FastEthernet0/3
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/4
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/5
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/6
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/7
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/8
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/9
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/10
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/11
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/12
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/13
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/14
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/15
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/16
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/17
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/18
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/19
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
```

```
interface FastEthernet0/20
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/21
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/22
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/23
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/24
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
 ip dhcp snooping limit rate 20
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 ip address 172.16.1.99 255.255.255.0
!
ip default-gateway 172.16.1.1
ip http server
ip http secure-server
!
banner exec ^C!!!BEWARE!!!Unauthorised access to this device is prohibited^C
banner login ^C!!!STOP!!!Unauthorised access to this device is prohibited^C
banner motd ^CUnauthorized access to this device is prohibited!^C
!
line con 0
 exec-timeout 0 0
 password 7 105A011C161E01
 logging synchronous
 login
line vty 0 4
 exec-timeout 0 0
 password 7 105A011C161E01
 login
line vty 5 15
 login
!
end
```

Appendix 6: Switch 2 Running Configuration

```
SW2#show running-config
Building configuration...

Current configuration : 5310 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname SW2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
system mtu routing 1500
!
!
ip dhcp snooping vlan 20
ip dhcp snooping
no ip domain-lookup
!
!
crypto pki trustpoint TP-self-signed-3760990464
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3760990464
 revocation-check none
 rsakeypair TP-self-signed-3760990464
!
!
crypto pki certificate chain TP-self-signed-3760990464
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101
05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
43657274
  69666963 6174652D 33373630 39393034 3634301E 170D3933 30333031
30303030
  35365A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33
37363039
  39303436 3430819F 300D0609 2A864886 F70D0101 01050003 818D0030
81890281
  81008B5E 41F3039A D69F6A80 A884361C C0870AEB EE90DDA4 4AE3B5AF
3A725D5A
  BC965926 19955318 E0920D7C 171EC846 499FD712 6AC225F3 7F0EC239
0AEE30A3
  D2BB2DC8 3FDD71EC 585DC033 420DBC92 DBA8AA84 0DDFA677 75F1A0C0
392A4C71
  0C02CB8E 6BF3FF3E E5B1D6E8 F4B5E7F6 2BBA3386 1A573454 492908D7
76AB5E6E
```

```
  B4E70203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
301F0603
  551D2304 18301680 149FCCC8 C5CB2096 ED52E8AE 606B3F74 95272B7E
44301D06
  03551D0E 04160414 9FCCC8C5 CB2096ED 52E8AE60 6B3F7495 272B7E44
300D0609
  2A864886 F70D0101 05050003 81810002 A93FDB8C BC46D3D2 0284DC74
4436A4A2
  6951CBB9 2CBB5C8A 6FF1C8A5 AD7EE84E 3228E317 72A2A0AA F11D354D
98703D82
  3983AB99 F4637591 38F3F9EA CCC0551B 7D4A312C 30DEF567 1DE1A1CC
84F82F66
  E78A7B7C 655A8188 90E389ED 64AD2A71 119064BF 42E2C97C 55DBBE73
0A16B7A9
  FFE88D3D E1766944 1EAAD5E2 74A26F
        quit
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
!
!
interface FastEthernet0/1
 switchport access vlan 20
 switchport mode access
 ip dhcp snooping trust
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
 ip dhcp snooping trust
!
interface FastEthernet0/3
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/4
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/5
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/6
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/7
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/8
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/9
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/10
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/11
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/12
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/13
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/14
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/15
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/16
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/17
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/18
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/19
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/20
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/21
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/22
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/23
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/24
 switchport mode access
 switchport port-security
 ip dhcp snooping limit rate 20
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 ip address 192.168.1.99 255.255.255.0
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
banner exec ^C!!!BEWARE!!!Unauthorised access to this device is prohibited^C
banner login ^C!!!STOP!!!Unauthorised access to this device is prohibited^C
banner motd ^C!!!WAIT!!!Unauthorised access to this device is prohibited^C
!
line con 0
 exec-timeout 0 0
 password 7 02120C5E180F1C
 logging synchronous
 login
line vty 0 4
 exec-timeout 0 0
 password 7 02120C5E180F1C
 login
line vty 5 15
 login
!
end
```

Appendix 7: Switch 4 Running Configuration

```
SW4#show running-config
Building configuration...

Current configuration : 3715 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname SW4
!
boot-start-marker
boot-end-marker
!
!
!
!
no aaa new-model
system mtu routing 1500
no ip domain-lookup
!
!
ipv6 unicast-routing
!
!
crypto pki trustpoint TP-self-signed-2448865152
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2448865152
 revocation-check none
 rsakeypair TP-self-signed-2448865152
!
!
crypto pki certificate chain TP-self-signed-2448865152
 certificate self-signed 01
  3082023C 308201A5 A0030201 02020101 300D0609 2A864886 F70D0101
04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
43657274
  69666963 6174652D 32343438 38363531 3532301E 170D3933 30333031
30303031
  30315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32
34343838
  36353135 3230819F 300D0609 2A864886 F70D0101 01050003 818D0030
81890281
  8100CEDD F37522AA BAB9F383 EABAA2C5 9D78EC58 A1CEB74B FE94627B
9A287F4E
  CF489C98 D3D48B0C 77F24D33 BDA71292 F5C13206 C4120E55 38063C22
01762932
  0499DE08 D6BDDBDA D47410D6 DD3996BB C1BAAC8A 835DC450 0B0EC511
43F7FD0A
```

```
  7B088D35 3B3974D4 F6985966 6004EF00 609E5222 BEB16006 E876873A
E394B156
  23790203 010001A3 64306230 0F060355 1D130101 FF040530 030101FF
300F0603
  551D1104 08300682 04535734 2E301F06 03551D23 04183016 80142310
847B33F7
  20B9170E A8124405 A9699A0C 4849301D 0603551D 0E041604 14231084
7B33F720
  B9170EA8 124405A9 699A0C48 49300D06 092A8648 86F70D01 01040500
03818100
  1DA0548D EA8E1DDD 532DF640 09376C34 BBB97ACE F7DFFB61 73510EB9
53679901
  72F2D688 AB347DEE 23D26699 B0C635A0 232336AE 6A892BAD 448AD168
0DA7721A
  BF445698 73C0F44C D625E49F B67466E3 5C92FFD7 66F8A6FE C41A1F4A
7614FB05
  8C999536 6F508D91 986ED78D 81F77141 B74DD691 1AC572D1 ACD93BD5
C7A5031B
  quit
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
interface FastEthernet0/1
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 shutdown
!
interface FastEthernet0/8
 shutdown
!
interface FastEthernet0/9
 shutdown
!
```

```
interface FastEthernet0/10
 shutdown
!
interface FastEthernet0/11
 shutdown
!
interface FastEthernet0/12
 shutdown
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
 shutdown
!
interface FastEthernet0/24
 shutdown
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 no ip address
 ipv6 address 2001:DB8:1:40::99/64
!
```

```
ip classless
ip http server
ip http secure-server
!
!
ipv6 route ::/0 2001:DB8:1:40::1
!
!
!
banner exec ^C!!!BEWARE!!!Unauthorised access to this device prohibited^C
banner login ^C!!!STOP!!!Unauthorised access to this device prohibited^C
banner motd ^C!!!WAIT!!!Unauthorised access to this device prohibited^C
!
line con 0
 exec-timeout 0 0
 password 7 061207245F471A
 logging synchronous
 login
line vty 0 4
 exec-timeout 0 0
 password 7 061207245F471A
 login
line vty 5 15
 login
!
end
```