Daniel Kiregu Gitau

Implementing IPv6 in a Production Network

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Thesis

1 April 2011

Abstract

Author(s) Title Number of Pages Date	Daniel Kiregu Gitau Implementation of IPv6 in a production network 60 pages +2 appendices 27 May 2010
Degree	Bachelor of Engineering
Degree Program	Information Technology
Specialisation option	Bachelor of Engineering
Instructor(s)	Audrey Blair, Project Manager Erik Pätynen, Senior Lecturer

CompanyXYZ IT is planning on taking a more proactive role in the deployment of IPv6 in its production network in order to facilitate its IT vision of providing secure, anytime, anywhere, any device access to accurate information with a focus on simplicity, efficiency and speed to information.IPv6 implementation at CompanyXYZ production network involves a cross functional team that consists of the client services team, server team, network team, security team, application team and the business team to be able to cover all angles of the production network. The goal of this work was to create a step by step detailed procedure and mechanism how the networking team at companyXYZ deployed IPv6 to the production network.

The scope for a full integration of IPv6 to the production network is quite broad; hence a phased IPv6 deployment, starting from an IPv6 verification cycle migrating our way through the datacenter, core layer network, distribution layer network and finally the access layer network. In the different phases of the project companyXYZ migrated to IPv6 by utilizing the dual stack technology, making it possible to use both IPv6 and IPv4 protocols simultaneously but in areas where the dual stack technology could not be implemented companyXYZ used the tunneling technology as a backup solution.

This project created the procedure that was involved in setting up a dual stack environment at companyXYZ production network allowing the existing IPv4 network to work optimally but also allowing the introduction of the IPv6 network so as when the network elements are migrated and integrated to be IPv6 compatible, the current companyXYZ production network would be able to facilitate IPv6 usage in the network for them.

The results of this document will serve as the primary source of implementation input for systems engineering and product engineering in the creation of Functional Requirement and Functional Specification documents for the deployment of IPv6 protocol on a production network.

Keywords	IP ,IPv4, IPng ,IPv6

Abbreviation

AH	Authentication Header
APAC	Asia-Pacific
APNIC	Asia Pacific Network Information Centre
ARIN	American Registry for Internet Number
BGP	Border Gateway Protocol
CAR	Committed Access Rate
CatOS	Catalyst Operating System
CIDR	Classless Inter-Domain Routing
CM	Contract Manufacturing
CRTP	Compressed Real-Time Protocol
DHCP	Dynamic host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DNS	Domain Name Server
DSCP	Differentiated Service Code Point
DSCP	Differentiated Services Code Points
DUAL	Diffusing Update Algorithm
ECN	Explicit Congestion Notification
ECN	Explicit Congestion Notification
EIGRP	Enhanced Interior Gateway Routing Protocol
EMEA	Europe, the Middle East and Africa
ESP	Encapsulating Security Protocol
EU	European Union
FDDI	Fiber Distributed Data Interface
FHRP	First Hop Redundancy Protocol
GRE	Generic Routing Encapsulation
HQ	HeadQuarters
HSRP	Hot Standby Router Protocol
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IOS	Internetwork Operating System
IP	Internet Protocol
IPNG	Internet Protocol Next Generation
IPsec	Internet Protocol Security

IPT	Internet Protocol Telephony
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISP	Internet Service Provider
ISP	Internet Service Provider
IT	Information Technology
LAC	Latin America and Caribbean
LAN	Local Area Network
LLQ	Low Latency Queuing
LTE	Long Term Evolution
MAC	Media Access Control
MLS	Multi-Layer Switching
MPLS PIP	Multi-Protocol Label Switching based Private IP
MPLS	Multi-Protocol Label Switching
MTU	Maximum Transmission Unit
NA	North America
NAT	Network Address Translation
NBAR	Network-Based Application Recognition
NLRI	Network Layer Reachability Information
OS	Operating System
PA	Provider Aggregately
PI	Provider Independent
POE	Power over Ethernet
PPL	People
PPP	Point-to-Point Protocol
QoS	Quality Of service
R&D	Research and Development
RFC	Request for Comment
RFPs	Request for Proposal
RIB	Router Information Base
RIPE NCC	Réseaux IP Européens Network Coordination Centre
RIR	Regional Internet Registry
RPF	Reverse Path Forwarding
SAFI	Subsequent Address Family Identifier
SLAAC	Stateless Address Auto-Configuration

TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
ToS	Type of Service
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VOIP	Voice over Internet
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WRED	Weighted Random Early Detection
WS	Work Station

Contents

1 Introduction

IP version 6 (IPv6) is the next generation communication protocol. The deployment of IPv6 is eminent and gradually becoming a mandatory requirement for broadband and mobile infrastructure products. This is not only a result of the industry approaching the exhaustion of IP version 4 (IPv4) addresses and the consequent enablement of more service provider's infrastructures for IPv6 around the world, but also the imminent availability of IPv6 in consumer devices.

This project dealt with the practical implementation of IPv6 on CompanyXYZ production network by the networking team. IPv6 implementation at companyXYZ will help facilitate IT´s vision of Providing Secure, anytime, anywhere, any device access to accurate information with a focus on simplicity, efficiency and speed to information. The main goal of this project was to experiment in practice IPv6 integration and support of all services provided in companyXYZ production network.

This project aim was to create a step by step detailed procedure and mechanism how CompanyXYZ as a whole deployed IPv6 to its production network. The document aims to be used primarily for marketing, planning, project management, systems engineering and product engineering. It will serve as the primary source of implementation input for systems engineering and product engineering in the creation of Functional Requirement and Functional Specification documents for the deployment of IPv6 protocol on any production network

2 Overview of IPv6

As an industry, Internet Protocol (IP) has served as a basis for a rich communications infrastructure for consumers, enterprises, and providers for decades. Practically every data stream transported by service providers' networks are or soon will be a series of IP packets with some set of additional wrappers placed around them by the providers in order to support the providers' network infrastructure functions. As such, CompanyXYZ products absolutely depends directly or indirectly on supporting IP and its evolution in the industry, i.e. IPv6 – as IP is what all our customers are or soon will be almost exclusively using within their networks.[4]

For over 40 years, the world's IP networks have been utilizing IPv4 address space of 2^{32} (about 4 billion) addresses. As most know the industry is rapidly nearing the exhaustion of this space due to the increasing demand and the explosion of new IP-enabled devices, the growth of undeveloped regions and the rapid growth of other regions. Currently the unallocated pools of IPv4 addresses have a reservoir of only 10% remaining and are estimated to be depleted before the end of 2012.The industry has been aware of this eventuality for almost 20 years. IPv6 was recommended by the IPv6 Area Directors of the Internet Engineering Task Force (IETF) at the Toronto meeting on July 25, 1994, and documented in RFC 1752, "The Recommendation for the IP Next Generation Protocol" [3]. The recommendation was approved by the Internet Engineering Steering Group on November 17, 1994 and made a Proposed Standard. As such, the industry developed IPv6 also referred to as Internet Protocol Next Generation (IPng) [4] to overcome the limitation of the current standard IPv4 [5] and finally succeed IPv4 [6] via creating a new version of the protocol which serves the function of IPv4, but without the same limitations of IPv4 [4].

IPv6 was under development and testing for most of the 1990s. Since then, most vendors, i.e. Cisco, Juniper and ALU have been including support for IPv6 in most new equipment. IPv6 support is here today – it is no longer an experiment or research that needs additional proof points. Many providers have already enabled IPv6 technologies on their core infrastructures and have proven the technology to be mature and stable in very large deployments, these same providers are considering extending IPv6 deployment to the edges of their networks, an example being the mobile backhaul. It is on CompanyXYZ advantage to develop IPv6 in their products to support such deployments. [1]

Changing from IPv4 to IPv6 means changing dozens of Internet protocols and conventions, ranging from how IP addresses are stored in domain name system (DNS) and applications, to how datagram's are sent and routed over Ethernet, Point-to-Point Protocol (PPP), Token Ring, Fiber Distributed Data Interface (FDDI), and every other medium, to how programmers call network functions. [4] This document will look at how these changes will be blended into CompanyXYZ production network.

2.1 Features of IPv6

IPv6 is a powerful enhancement to the IPv4 technology, with features that better suit the current and foreseeable network demands. [5] In the early design stages of the Internet they came up with IPv4 which provided an addressing capability of about 4 billion addresses (2^{32}). This was deemed sufficient as per the time. But with the explosive growth of the Internet it became apparent that alternative methods had to be developed to conserve the exhausting IPv4 address space. They introduced Conservational mechanisms like Classless Inter-Domain Routing (CIDR), Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT) to alleviate IPv4 address exhaustion. However these conservational mechanisms complicated the advantages of peer-to-peer communication, end-to-end security and Quality of Service (QOS) [5] hence leading to the development of IPv6 in 1994 by the Internet Engineering Task Force (IETF).

IPv6 technology brought about 2^{128} (about 3.4×10^{38}) available addresses [6]. Hence increasing the number of address bits by a factor of 4 from 32 to 128 as figure 1 illustrates, allowing enough address space such that every user could have multiple unique global addresses [5] and thus improving total connectivity, reliability, and flexibility on the Internet. [4]

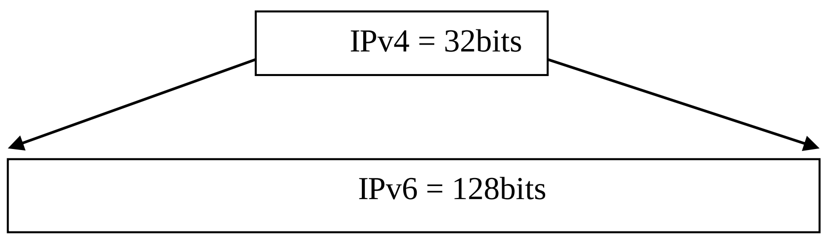

Figure1. IPv4 compared to IPv6 address bits [9]

IPv6 technology enabled a more simplified and manageable network architecture with its plug and play functionality, whereby all IPv6 host would participate in stateless auto configuration, by creating a guaranteed-unique IP address via combining its LAN

MAC address with a prefix provided by the network router [4]. This unique address paves the way to powerful secure end-to-end, peer-to-peer networks. This will enable people to access information and share resources without going through a complex maze of middle boxes that requires IT management. This can make introducing new services, such as Voice over IP (VoIP) or instant messaging, much easier [7].

IPv6 technology builds-in and mandates the new Internet Protocol Security (IPsec) security protocols, Encapsulating Security Protocol (ESP) and Authentication Header (AH) as a fundamental interoperability requirement ensuring a secure network unlike in the IPv4 where there are add-ons. These are just some of the major features that are implemented in the IPv6 technology. Others include multicasting, seamless mobility, efficient and hierarchical addressing and routing infrastructure, jumbo grams and options extensibility.

2.2 IPv6 Packet Format

IPv6 is the next generation communication protocol for hosts and routers. In order for IPv6 to be implemented and interoperable it needs to define the header format which specifies how the data is being processed. IPv6 reduced the packet-header processing hence increasing network performance by having a fixed header size and removing the rarely used IPv4 fields as figure 2 illustrates [8].

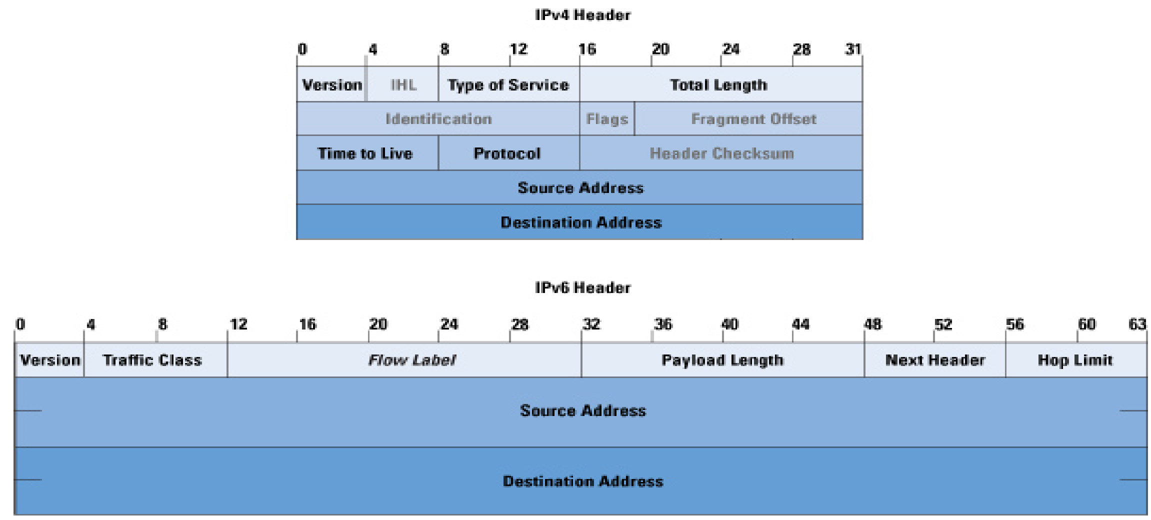

Figure 2: IPv4 and IPv6 header [9]

The version field is set to 6 to indicate the protocol version. The traffic class field actually consists of 2 subfields. The first 6 bits of this field constitute the differentiated service code point (DSCP) used to provide QOS to traffic [10]. The remaining 2 bits of the field are reserved for Explicit Congestion Notification (ECN) [11], which is used to alert the transport protocol of congestion along the path a packet takes. The flow label is used to define the sequence of packets from a source to a destination. The length of the rest of the packet following the IPv6 header is denoted by payload length. The Next Header field points to the upper-layer protocol that is carried in the packet's payload. For data this is typically TCP and UDP. However, IPv6 defines multiple extension headers which may be present e.g. packets using mobile IP may use routing header and destination option [12].

The time-to-live field in IPv4 has been renamed to hop limit field which determines how far a packet should traverse the internet. It´s value decrement by one for each node that forwards the packet when the value reaches zero the packet is dropped. The source and destination address field specify the originator and the receiver of the packet respectively. If the routing header is present the destination address does not need to specify the ultimate receiver. The extension headers appear between the IPv6 header and upper layer headers. They include IPv6 header, hop-by-hop optional header, destination options header, routing header, fragment header, authentication header and encapsulation security payload header and upper layer header [5].

2.3 IPv6 Address

Increasing the IP address pool was one of the major forces behind developing IPv6. It uses a 128-bit address, meaning that we have a maximum of 2^{128} addresses available, or 340,282,366,920,938,463,463,374,607,431,768,211,456.These newfangled IP’s require eight 16-bit hexadecimal colon-delimited blocks. So not only are they longer, they use numbers and letters e.g. 2001:0db8:3c4d:0015:0000:0000: abcd: Ef12. [13]
Under IPv4 we have the old familiar Unicast, broadcast and multicast addresses. In IPv6 we have Unicast, multicast and any cast. With IPv6 the, broadcast addresses are not used anymore, because they are replaced with multicast addressing. [13]

IPv6 Unicast address is a single address identifying a single interface and similar to the IPv4 unicast address. There are three types of unicast addresses:

Global unicast addresses, which are conventional, publicly routable address, just like conventional IPv4 publicly routable addresses.

Link-local addresses are akin to the private, non-routable addresses in IPv4 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). They are not meant to be routed, but confined to a single network segment. Link-local addresses mean you can setup a temporary LAN, such as for conferences or meetings, or set up a permanent small LAN the easy way. [13]

Unique local addresses are also meant for private addressing, with the addition of being unique, so that joining two subnets does not cause address collisions. Special addresses like loopback addresses, IPv4-address mapped spaces, and 6-to-4 addresses for crossing from an IPv4 network to an IPv6 network. [13]

IPv6 Multicast address is similar to the old IPv4 broadcast address a packet sent to a multicast address is delivered to every interface in a group. The IPv6 difference is that, instead of annoying every single host on the segment with broadcast blather. Only hosts who are members of the multicast group receive the multicast packets. IPv6 multicast is routable, and routers will not forward multicast packets unless there are members of the multicast groups to forward the packets to. Anyone who has ever suffered from broadcast storms will appreciate the multicast address. [13]

IPv6 any cast address is a single address assigned to multiple nodes. A packet sent to an any cast address is then delivered to the first available node. This is an advanced method of providing both load-balancing and automatic failover. The idea of any cast has been around for a long time; it was proposed for inclusion in IPv4 but it never happened. Several of the Domain Name Server (DNS) root servers' use a router-based any cast implementation, which is really a shared unicast addressing scheme. (While there are only thirteen authoritative root server names, the total number of actual servers is considerably larger, and they are spread all over the globe). The same IP address is assigned to multiple interfaces, and then multiple routing tables' entries are needed to move everything along.IPv6 any cast addresses contain fields that identify them as any cast, so all one has to do is configure the network interfaces appropriately. The IPv6 protocol itself takes care of getting the packets to their final destinations. [13]

There are conventional forms for representing IPv6 addresses as text strings. The preferred form is X:X:X:X:X:X:X:X , where the 'x's are the hexadecimal values of the eight 16-bit pieces of the address e.g. FEDC:BA98:7654:3210:FEDC:BA98:7654:3210. [14] Naturally network administrators want shortcuts, because IPv6 addresses are long and all those zeroes are just too much. Leading zeroes can be omitted, and contiguous blocks of zeroes can be omitted entirely, so an IPv6 address like this 1080:0:0:0:8:800:200C:417A can be simplified to 1080::8:800:200C:417A. [13] The text representation of IPv6 address prefixes is similar to the way IPv4 addresses prefixes are written in CIDR notation. An IPv6 address prefix is represented by the notation: IPv6-address/prefix-length i.e. 12AB:0:0:CD30::/60. [13]

The IPv6 address has three parts: the network identifier, the subnet, and the interface identifier as can be seen below. [13]

2001: 0db8:3c4d:0015:0000:0000: abcd: ef12
______________|____|___________________
Global prefix   subnet   Interface ID   [13]

The global routing prefix comes from a pool assigned to the company , either by direct assignment from a Regional Internet Registry(RIR) like Asia Pacific Network Information Centre (APNIC), American Registry for Internet Number (ARIN), or Réseaux IP Européens Network Coordination Centre (RIPE NCC), or more likely from the company´s Internet service provider. The subnet and interface IDs are controlled by the hardworking local network administrator. [13]

2.4 Business Justification for IPv6 Implementation

Today CompanyXYZ is seeing customer requirements to support IPv6. This is not only a result of the industry approaching the exhaustion of IPv4 addresses and the consequent enablement of more service provider's infrastructures for IPv6 around the world, but also the imminent availability of IPv6 in consumer devices. CompanyXYZ sees examples today of service providers i.e. EU Commission, P&G and China Telecom. where full IPv6 infrastructures are already underway, fortunately for CompanyXYZ, most common deployments of IPv6 today are being seen in limited scale, contained in the core areas of their networks and deployed carefully where there is co-existence of IPv4 and IPv6 addresses by means of deploying dual IP address schemes, encapsulating or translating one IP technology into another.

Consequently it is apparent that the adoption and introduction of IPv6 will not happen overnight and especially at the mobile backhaul. Regardless, the deployment of IPv6 is eminent and IPv6 is gradually becoming a mandatory requirement for broadband and mobile infrastructure products, as seen in multiple Request for Proposal (RFP) received in the last year.

It's given that Mobile Operators certainly will migrate to IPv6 as new data oriented services are rolled-out onto next-generation mobile network infrastructures such as Long Term Evolution (LTE). Furthermore most of companyXYZ competitors, as pointed above, already support IPv6. If CompanyXYZ wants to remain relevant in the mobile IP space, CompanyXYZ data products must support IPv6.AT&T is an example of an early adopter of IPv6 as an infrastructure protocol in the Mobile backhaul. [2]

3 Current CompanyXYZ Network

Before deploying IPv6 to an already existing network it is mandatory to understand the general idea of the company's network. This chapter will deal with familiarizing with CompanyXYZ network. This type of network may resemble other cooperate network and with each kind of a network a different IPv6 implementation will take place.

Hosts on the Local Area Network (LAN) will be grouped to different Virtual Local Area Network (VLAN´s) this is our method of classifying our different networks. This VLAN´s will be pointed to a DNS server and a DHCP server or router in some sales office. They will acquire an address and a hostname and can be allowed to the network as figure 3 illustrates below.

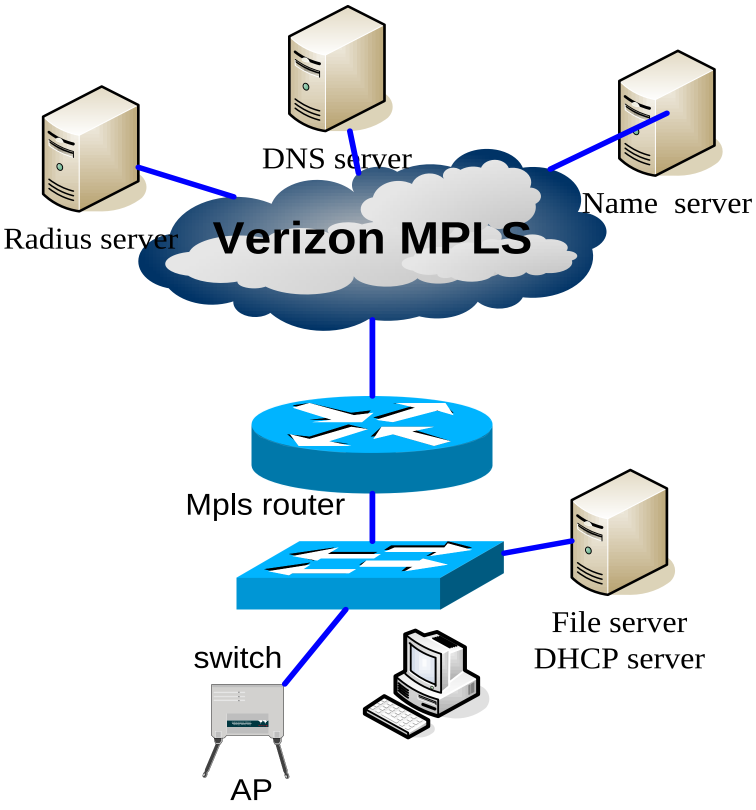

Figure 3. CompanyXYZ LAN [46]

When one host wants to communicate with a host in another VLAN the first traffic will be forwarded to a Multi-Layer Switch (MLS) which will route the initial traffic to the right VLAN and the rest of the traffic will just go directly without going via the MLS. [46]

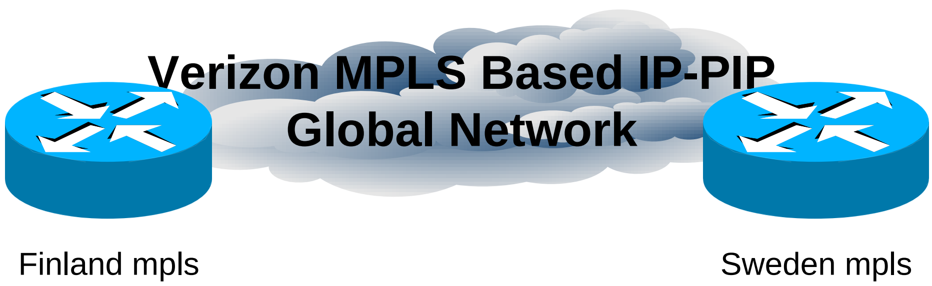

Figure 4. Verizon MPLS cloud [46]

Inter site communication is facilitated by Verizon company whereby we have Border Gateway Protocol (BGP) routes from each site to all other sites. Verizon is running an Multi-Protocol Label Switching (MPLS) network to facilitate communication over there cloud as figure 4 illustrates. For some smaller sales office we may be having Virtual Private Network (VPN) tunnels via their internet connection to the sites as figure 5 illustrates. In some cases we have VPN connection as a backup as figure 6 illustrates. This are the methods a host can use for inter-site communication.

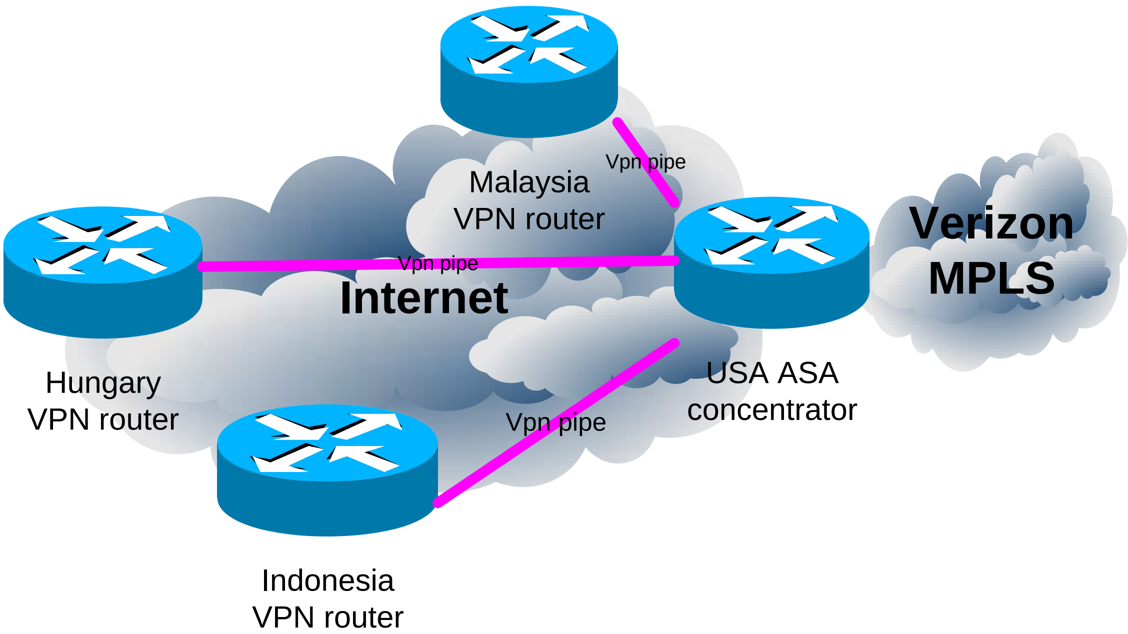

Figure 5. CompanyXYZ VPN connection [46]

Some big sites e.g. Finland, China and the United States have separate Internet circuit´s for users to access the Internet. These connections to the Internet have firewall or firewall service modules in between CompanyXYZ network and the local Internet providers to block traffic to and from the Internet as figure 7 illustrates.

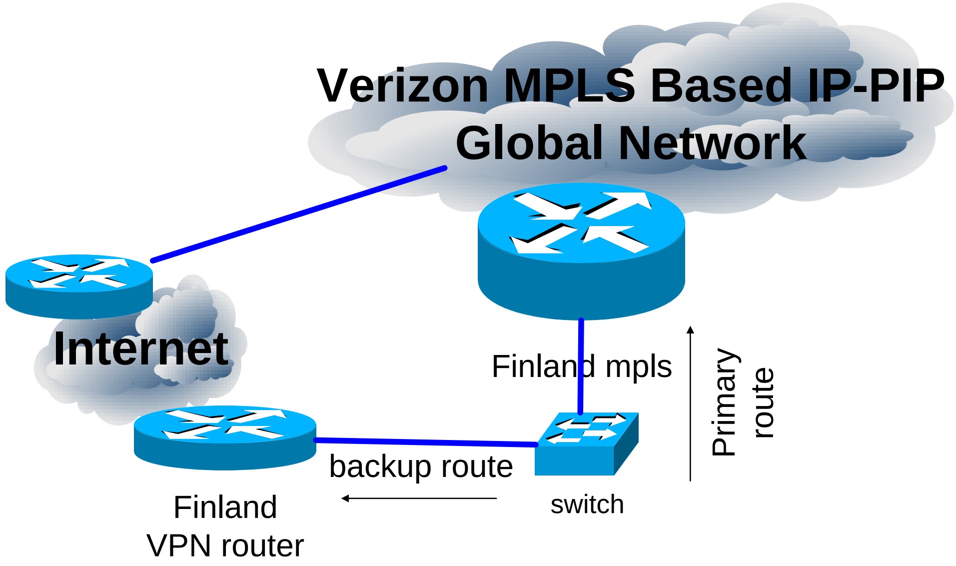

Figure 6. CompanyXYZ MPLS backup VPN connection [46]

In some cases companyXYZ has CM sites which connect either via VPN or via Verizon network (MPLS). Contract Manufactures (CM) are sites that are not fully CompanyXYZ owned but have contractors in them where some CompanyXYZ activities have been outsourced to them.

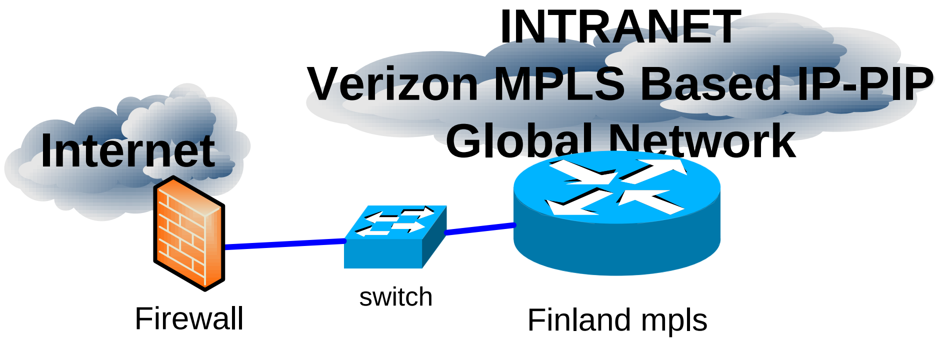

Figure 7. CompanyXYZ intranet and internet connection [46]

With this general understanding CompanyXYZ went ahead and took an inventory of its network to help understand the network.

3.1 IPv6 Readiness at CompanyXYZ

Compatibility with IPv6 networking is mainly a software or firmware issue. However, much of the older hardware that could in principle be upgraded is likely to be replaced instead. Most personal computers running recent operating system versions are IPv6-ready. Some applications with network capabilities were not ready but would be upgraded with support from the developers. [46]

Most equipment would be IPv6 capable with a software or firmware update if the device has sufficient storage and memory space for the new IPv6 stack. However, manufacturers may be reluctant to spend on software development costs for hardware they have already sold when they are poised for new sales from IPv6-ready equipment. In some cases, non-compliant equipment needs to be replaced because the manufacturer no longer exists or software updates are not possible. [46]

CompanyXYZ performed an inventory on its infrastructure and came up with the operating system (OS) currently deployed at CompanyXYZ infrastructure and those it plans to use going forward are summarized in table 1. Most of the operating systems and the network gear deployed were found to be IPv6 compatible but the ones that were not compatible would be upgraded via the regular refresh cycles to avoid additional costs.

Table 1. CompanyXYZ production network Operating Systems [46]

Device Type	Present OS	Future OS
PC and workstations	Windows XP Windows 7 Red Hat v3 Red Hat v4 Red Hat v5 Sun Solaris 8 Sun Solaris 9 Sun Solaris 10	Windows 7 Red Hat v6 Sun Solaris 10
servers	VMware ESX 3.5 VMware ESX 4.0 VMware ESX 4.1 Windows server 2000 Windows server 2003 Windows server 2008	VMware ESX 4.1 Windows server 2008
Routers and Switches	Cisco IOS,CatOS	Cisco IOS,IOS-XE and NX-OS

CompanyXYZ performed an inventory of the network elements currently deployed at CompanyXYZ infrastructure and those it plans to use going forward are summarized in table 2.

Table 2. CompanyXYZ production network elements [46]

Network functionality	Elements
MPLS	Cisco 2851 Cisco 1841
MLS switches	Cisco catalyst 6509
lab switches	Cisco WS-C2950 Cisco WS-C3500
VPN devices	Cisco 3845 Cisco 1841
ASAs	ASA 5500
Firewalls	Palo-alto Cisco 3845 Cisco 1841

Most of the operating systems and the network gear deployed were found to be IPv6 compatible but the ones that were not compatible would be upgraded via the regular refresh cycles to avoid additional costs. [46]

3.2 IPv6 Transition Mechanisms

3.2.1 Dual Stack

The successful market adoption of any new technology depends on its easy integration with the existing infrastructure without significant disruption of service. CompanyXYZ network consists of number of IPv4 networks and thousands of IPv4 nodes. The challenge for IPv6 lies in making the integration of IPv4 and IPv6 nodes and the transition to IPv6 as transparent as possible to the end users. The transitioning from IPv4 to IPv6 does not require upgrades on all nodes at the same time; IPv4 and IPv6 will coexist for some time. CompanyXYZ will use dual stack mechanism the most common techniques to transition from IPv4 to IPv6. [15]

IPv4 addresses will officially be in use for the next decade, although for most practical purposes one can consider the pool of IPv4 addresses to be depleted already. Hence during the transition period IPv6 world will co-exist with the IPv4 world as figure 8 illustrates. For this reason CompanyXYZ saw that dual stacking is by far the preferable solution in most scenarios. The dual stacked device can speak equally to IPv4 devices, IPv6 devices, and other dual-stacked devices (with the two devices agreeing on which IP version to speak). The entire transition can be driven by DNS: If a dual-stacked device queries the name of a destination and DNS gives it an IPv4 address (a DNS A Record), it sends IPv4 packets. If DNS responds with an IPv6 address (a DNS AAAA Record), it sends IPv6 packets. [16]

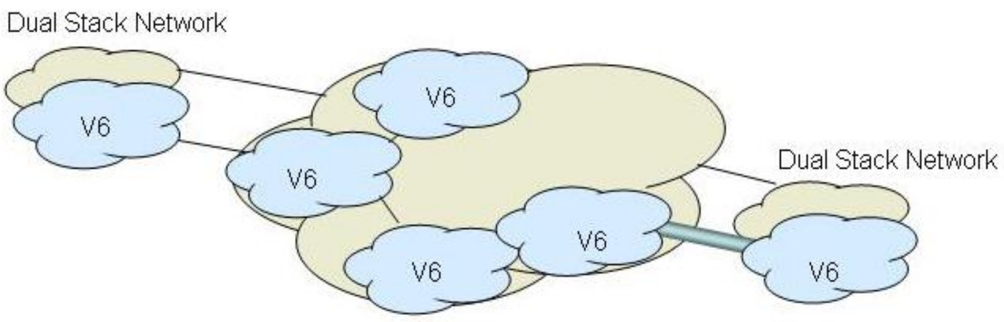

Figure 8. Dual stack network [47]

CompanyXYZ dual-stack migration strategy is to make the transition from the core to the edge. This involves enabling two TCP/IP protocol stacks on the WAN core routers, then perimeter routers and firewalls, then the server-farm routers and finally the desktop access routers. After the network supports IPv6 and IPv4 protocols, the process will enable dual protocol stacks on the servers and then the edge computer systems. [16]

3.2.2 Tunneling

Another secondary approach for CompanyXYZ is to use tunnels to carry one protocol inside another. These tunnels take IPv6 packets and encapsulate them in IPv4 packets to be sent across portions of the network that haven't yet been upgraded to IPv6. Tunnels can be created where there are IPv6 islands separated by an IPv4 ocean, which will be the norm during the early stages of the transition to IPv6 as figure 9 illustrates. Later there will be IPv4 islands that will need to be bridged across an IPv6 ocean. [17]

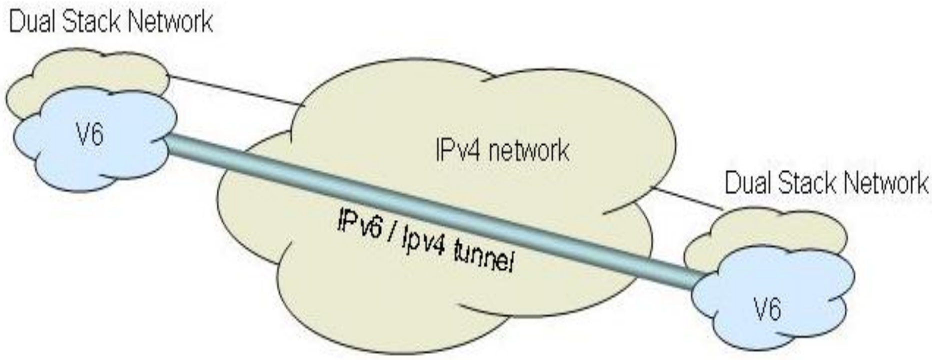

Figure 9. IPv6 tunneling [48]

The general idea of how IPv6 tunneling works is the entry node of the tunnel (the encapsulator) creates an encapsulating IPv4 header and transmits the encapsulated packet. The exit node of the tunnel (the decapsulator) receives the encapsulated packet, reassembles the packet if needed, removes the IPv4 header, and processes the received IPv6 packet. The encapsulator may need to maintain soft-state information for each tunnel recording such parameters as the MTU of the tunnel in order to process IPv6 packets forwarded into the tunnel. [16]

4 Addressing Architecture

The current IPv4 addressing plan at CompanyXYZ was done independently for each site in a hierarchical scheme [18]. This was due to the fact that each site had to acquire the address space from the local service provider; hence they could easily create a hierarchy on their local site but not on the global perspective of CompanyXYZ. In IPv6 companyXYZ opted to do a hierarchical addressing from the company level all the way down to the subnet level as figure 10 illustrates. This would help keep the routing table small and backbone routing efficient [19].

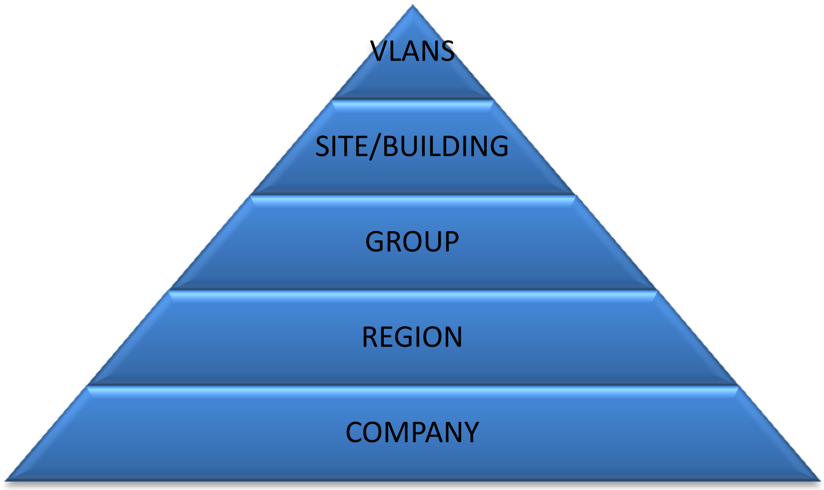

Figure 10. Hierarchical addressing [46]

CompanyXYZ hierarchical architecture is such that the company is split up to the different regions in the world that is Europe, the Middle East and Africa (EMEA), Asia-Pacific (APAC), North America (NA) and Latin America and Caribbean (LAC). In these regions we have different sites with different roles i.e. sales sites, contract manufacturing (CM) sites, headquarters (HQ) sites and research and development (R&D) sites as can be illustrated in figure 11

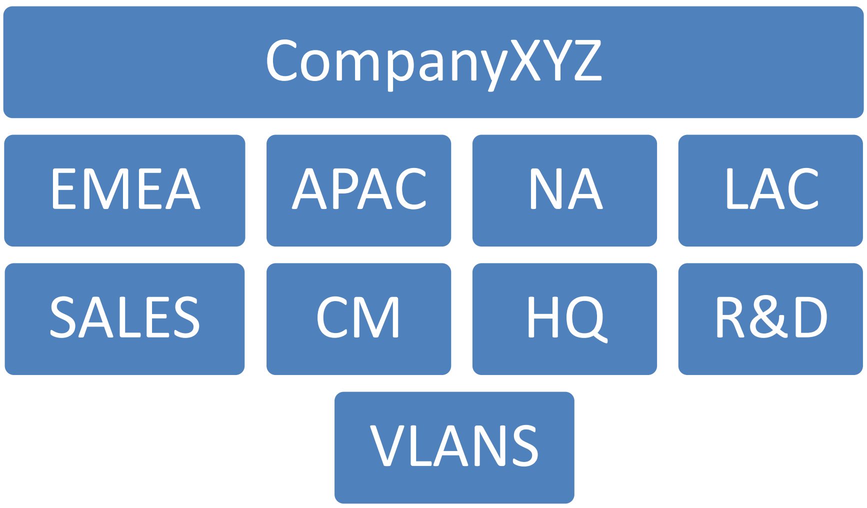

Figure 11. CompanyXYZ hierarchical architecture [46]

The addressing mechanism used at each hierarchical level will be discussed in details in chapter 4.1.

4.1 Company Level Addressing Scheme

CompanyXYZ enterprise network is comprised of four big regions that include

- Asia Pacific and Japan (APAC)
- Europe, the Middle East and Africa (EMEA)
- North America (NA)
- Latin America and Caribbean (LAC)

These regions compose CompanyXYZ sites/offices, located in different countries. All these CompanyXYZ sites are connected into a private extranet Multi-Protocol Label Switching based Private IP (MPLS PIP) network provided by Verizon business as figure 12 illustrates, which by its design emulates the functioning of the Internet.

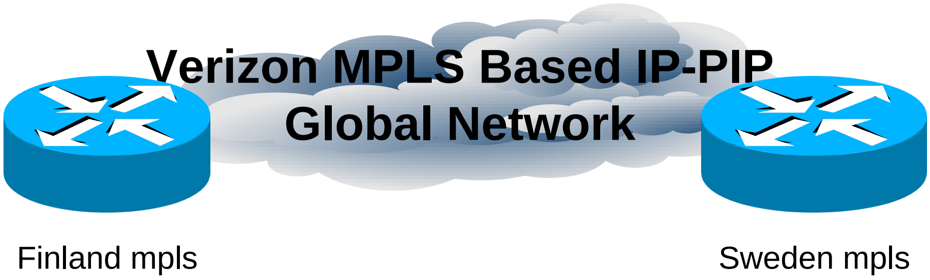

Figure 12. CompanyXYZ MPLS network [46]

The Internet connection for CompanyXYZ is done per region with centralized exit points at particular internet service provider (ISP) as described below.

- APAC region internet termination is at Singapore office ISP
- EMEA region internet termination is at Finland office ISP
- AMERICA region internet termination is at Naperville office ISP. [46]

These ISP's are in different Regional Internet Registry (RIR) as illustrated in Appendix 1. Hence we had to contact the different RIR's for each region for an IPv6 address space.

From all this three RIR's companyXYZ was issued with Provider Independent (PI) address space because companyXYZ WAN network is multi-homed between multiple service providers using BGP. Other alternative methods presented to companyXYZ were

- Ordering a Provider Aggregately (PA) space from your ISP.
- Ordering a 6to4 tunnel from a company like Hurricane Electric (HE). But then the company would be using Hurricane Electric IPv6 address space since you likely won't qualify for a block direct from a RIR

The PI address space issued to CompanyXYZ from the RIR's are illustrated in figure 13. N/B due to company policy I will be using the address space reserved by IPv6 for documentation and that is 2001:db8:: /32 and not the actual address space reserved for CompanyXYZ.

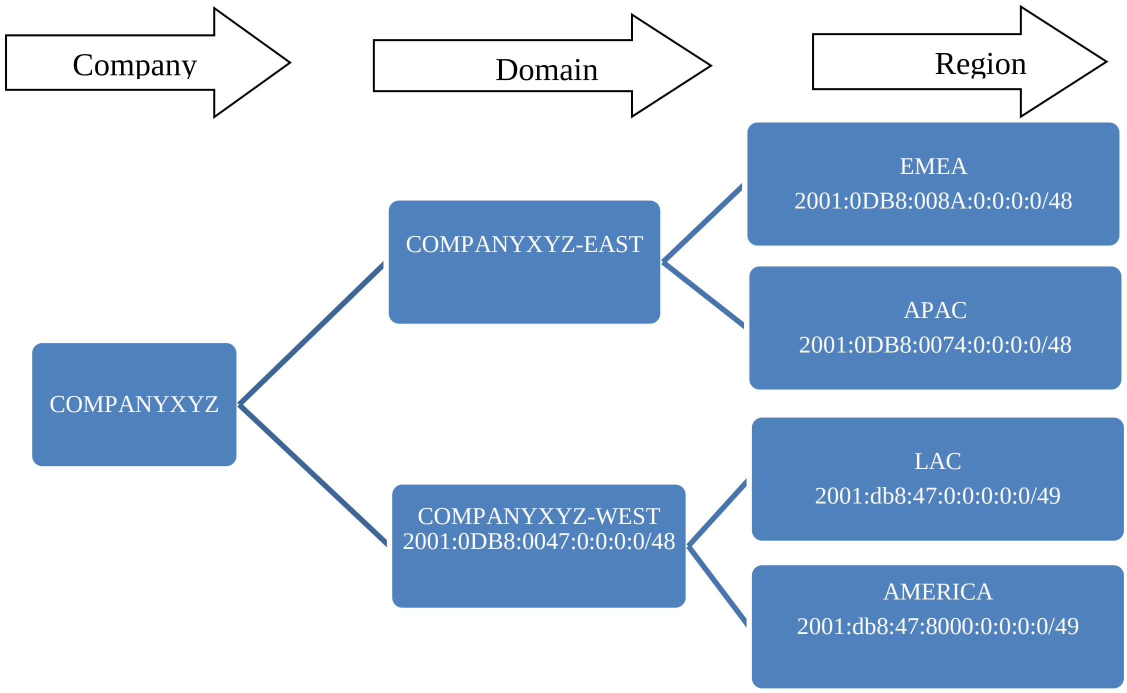

Figure 13. CompanyXYZ PI address pool [18]

The /48 is the common network prefixes being issued by most RIR or ISP to subscribers' sites, yielding 65536 subnets (2^{16}) from it. [20]

4.2 Regional Level Addressing Scheme

The CompanyXYZ region contain different sites in different countries. These sites have different business functionality e.g. sales offices, research and development (R&D)

offices or contract manufacturing (CM) offices. Hence for the region level companyXYZ grouped the sites as figure 14 illustrates.

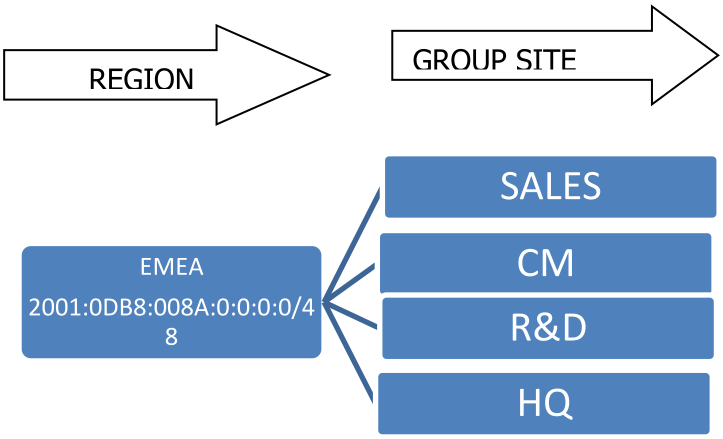

Figure 14. EMEA region group sites [46]

The different sites in companyXYZ region were assigned to a particular group if the site possesses the basic characteristics of that particular group as summarized in table 3

Table 3. CompanyXYZ group site characteristics [46]

	STAFF	WAN	WLAN	LAN	E.G
Sales Site	6-10 PPL	MPLS circuit VPN tunnel	CompanyXYZ wireless	CompanyXYZ LAN	South-Africa Spain
R&D Site	6-50 PPL	MPLS circuit	CompanyXYZ wireless	CompanyXYZ LAN VOIP Server network Lab network	Finland Oulu, Denmark
HQ site	6-500 PPL	MPLS circuit	CompanyXYZ wireless CompanyXYZ guest	CompanyXYZ LAN VOIP Video Server network Lab network VPN	Finland, Naperville
CM site	non-CompanyXYZ employees			CompanyXYZ LAN	Hungary

Once the site were grouped per region companyXYZ went ahead and followed the below general IPv6 addressing scheme for each region. The first /64 address space from each region`s address pool will be reserves for the loopback addresses i.e.2001:DB8: 008a:0000:0000:0000:0000:0000/64 with each loopback address being a /128 bit host. The second /52 address space from each region`s address pool will be reserved for the HQ office end-node addresses i.e. 2001:DB8: 008a:1000:0000:0000:0000:0000/52. To subnet the HQ office we use the first 4 bits for the site and left the other 12 bits for the VLAN´s as shown below.

```
|    N bits (48)            | s (4)    | v (12)   |   128-b-s bits (64)   |
+------------------+------+-------+----------------+
| Global routing prefix   | site     | VLAN     |     interface ID       |
+------------------+--------------+----------------+
```

Hence the HQ site summary address will be 2001:DB8: 008a:S000:0000:0000:0000:0000/52 and the HQ site VLAN summary address is 2001:DB8: 008a: SSVV: 0000:0000:0000:0000/64. Thus VLAN 3 in Finland Espoo would be 2001:DB8: 008a:1003: : /64.

In some regions companyXYZ has the HQ site having multiple buildings. In this case companyXYZ can break the site down into the different buildings by using the first 4 bits for the group site the second 4 bits for the building and the remaining 8 bits for the VLAN`s as shown below.

```
|        N bits (48)       | s (4)  | b (4)   | v (8)  | 128-b-s bits (64)   |
+------------------------+-------+--------+-------+---------------------+
| Global routing prefix  | site    | BLDG  | vlan  |  interface ID        |
+------------------------+------------------------+---------------------+
```

Hence the HQ site summary address will be 2001:DB8: 008a:S000:0000:0000:0000:0000/52 and the HQ site building summary address is 2001:DB8: 008a: SB00: 0000:0000:0000:0000/64 and the HQ site VLAN summary address is 2001:DB8: 008a: SBVV: 0000:0000:0000:0000/64. Thus VLAN 3 in building 7 in Finland Espoo would be 2001:DB8: 008a:1703:: /64.

The third /52 address space from each region`s address pool will be reserved for the R&D office end-node addresses i.e. 2001:DB8: 008a:2000:0000:0000:0000:0000/52. To subnet the R&D offices companyXYZ used the first 4 bits to identify the group the site is in , the second 4 bits to identify the site and leave the other 8 bits for the VLAN`s as shown below.

```
|        N bits (48)          | g (4)  | s (4)  | v (8)    | 128-b-s bits (64)    |
+-----------------------------+--------+-------+---------+----------------------+
 | Global routing prefix    | GRP   | site    | VLAN   |  interface ID         |
+---------------------------+----------------------------+---------------------+
```

Hence the group R&D summary address will be 2001:DB8: 008a:G000:0000:0000:0000:0000/52 and the R&D site summary address will be 2001:DB8: 008a: GS00: 0000:0000:0000:0000/64 and the R&D site VLAN summary address is 2001:DB8: 008a: GSVV: 0000:0000:0000:0000/64. Thus VLAN 3 in Denmark R&D site would be 2001:DB8: 008a:2103:: /64.

The fourth /52 address space from each region`s address pool will be reserved for the sales office end-node addresses i.e. 2001:DB8: 008a:3000:0000:0000:0000:0000/52.While the fifth /52 address space from each region`s address pool will be reserves for the CM office end-node addresses i.e. 2001:DB8: 008a:4000:0000:0000:0000:0000/52. To subnet the CM and sales offices companyXYZ used the first 4 bits to identify the group the next 8 bits to identify the site and leave the last 4 bits for the VLAN`s as shown below.

```
|        N bits (48)          | g (4)  | s (8)     | v (4) | 128-b-s bits (64)    |
+---------------------------+--------+---------+-------+----------------------+
 | Global routing prefix    | GRP   | site      | VLAN  |  interface ID         |
```

Hence the group Sales summary address will be 2001:DB8: 008a:S000:0000:0000:0000:0000/52 and the Sales site summary address will be 2001:DB8: 008a: GSS0: 0000:0000:0000:0000/60 and the sales site VLAN summary address is 2001:DB8: 008a: GSSV: 0000:0000:0000:0000/64. Thus VLAN 3 in France sales site will be 2001:DB8: 008a:3223:: /64.

4.3 Site Level Addressing

Each of CompanyXYZ site´s contains multiple networks, each of this site networks were issued with one of the reserved /64 address space for that particular site. The hosts in the site network will use both stateless and state full auto configuration for IPv6 address acquisition. This is due to the fact that current end user devices do not support DHCPv6 because IPv6 has automated the IP address configuration process. CompanyXYZ can obtain the address from stateless auto configuration and the DNS server address from state-full auto-configuration (DHCPv6). [15]

5 Test Network

The CompanyXYZ environment as figure 15 illustrates was set up to evaluate the integration of the IPv6 technology with the current CompanyXYZ production network.

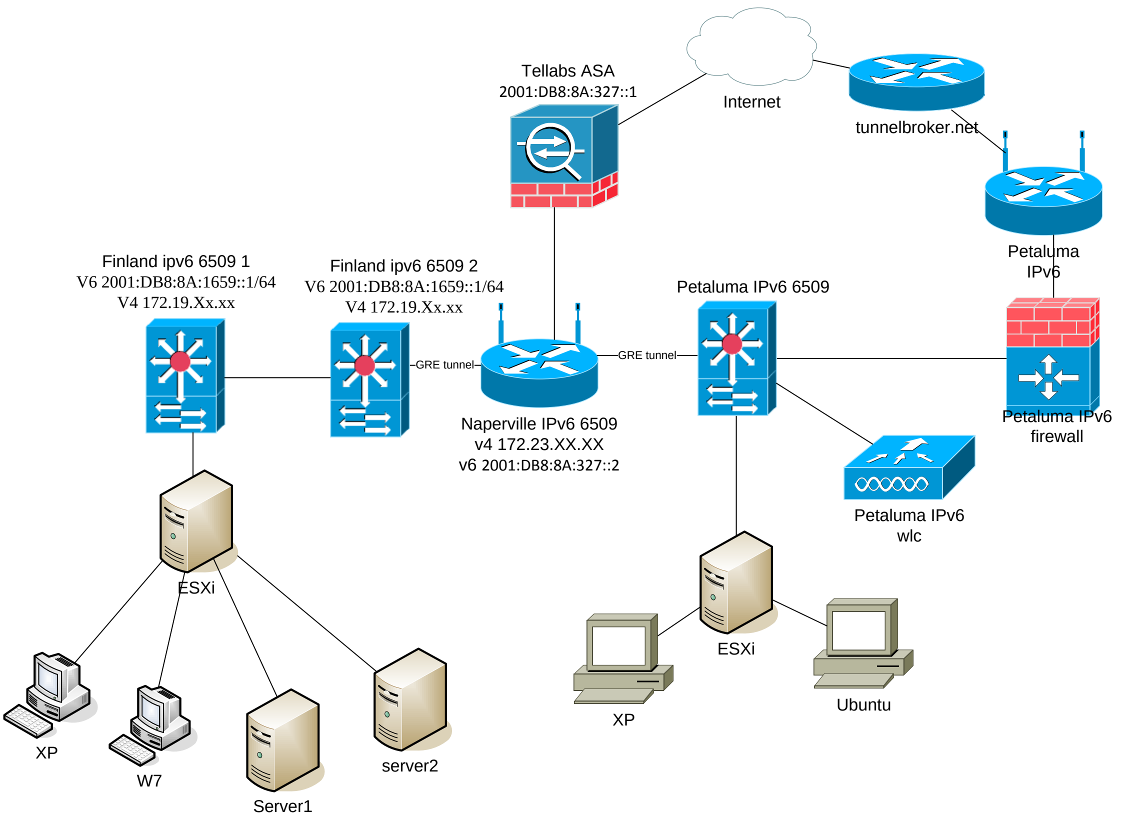

Figure 15: IPv6 Test Bed Environment [46]

CompanyXYZ provisioned the appropriate equipment as described below and build the test network as figure 15 illustrates.

Routers

- Three Cisco 6509 router i.e. fiesp-ipv6-6509-1,fiesp-6509-2 and uspet-ipv6-6509 as figure 15 illustrates with 256 MB of memory and 512 Kb of flash, integrated 10/100/1000 Mbps Ethernet interfaces, loaded with Cisco 12.2(2) T
- Two Cisco c870 router i.e. usnap-ipv6-sky as figure 15 illustrates with 256 MB of memory and 512 Kb of flash, integrated 10/100/1000 Mbps Ethernet interfaces, loaded with Cisco 12.4(22)T
- One Palo alto PA-4020 firewall i.e.uspet-ipv6-fw as figure 15 illustrates with 2 Gbps firewall throughput, 2 Gbps threat prevention throughput,1 Gbps IPsec VPN throughput,2,000 IPsec VPN tunnels and tunnel interfaces,60,000 new sessions per second, 500,000 max sessions, (16) 10/100/1000 + (8) SFP optical gigabit interfaces,(2) Dedicated high availability interfaces (10/100/1000), (1) Dedicated out of band management interface (10/100/1000), (1) DB9 interface , loaded with version 3.1.5
- One Cisco ASA 5520 i.e. companyXYZ ASA as figure 15 illustrates with 150 Mbps Firewall Throughput ,100 Mbps VPN Throughput,10,000 Concurrent Sessions,10 IPsec VPN Peers,25 Premium Any Connect VPN Peer License Levels and ,8-port Fast Ethernet switch with dynamic port grouping (including 2 POE ports)
- One Cisco 4400 Series WLAN Controller i.e. uspet-ipv6-wlc as figure 15 illustrates with four Gigabit Ethernet ports supports up to 100 lightweight access points and provides two expansion slots that can be used to add enhanced functionality, such as VPN termination and other capabilities

Hosts

- IPv6 enabled laptops running Microsoft windows XP sp3, Windows 7 and Ubuntu workstations and servers

Servers

- power edge 2850 dell ESX server with 2CPU * 2.793 GHz , Intel(R) xen-on(TM) CPU, 2.80 GHz processor , 3 NICs interfaces, 681.75 GB data store loaded with VMware evaluation mode license.
- Windows 2008 32 bit R2 server

Table 4. IPv6 test bed addressing scheme [46]

VLAN	IPv6 address	Description
VLAN 660	2001:DB8:008a:1660::/64	Finland IPv6-mgmt
VLAN 661	2001:DB8: 008a:1661::/64	Finland IPv6 LAN 1
VLAN 662	2001:DB8: 008a:1662::/64	Finland lab 1
VLAN 663	2001:DB8: 008a:1663::/64	Finland server
VLAN 250	N/A	
VLAN 283	2001: DB8: 008a:283::/64	Petaluma IPv6 Clients
VLAN 383	2001: DB8: 008a:383::/64	Petaluma IPv6 Servers
VLAN 305	2001: DB8: 008a:305::0/64	Petaluma IPv6 Mgmt
Tunnel10	2001: DB8: 008a:350::/64	tunnel10 pet-to-nap
VLAN 400	2001: DB8: 008a:400::/64	871 and 6509
	2001: DB8: 008a:327::/64	Naperville to sky walker
	2001: DB8: 008a:454::/64	sky walker

CompanyXYZ also designed an IP addressing scheme for the test bed environment as summarized in table 4.

6 CompanyXYZ Proof of Concept

6.1 Implementing Hosts and Servers for IPv6

CompanyXYZ underwent IPv6 proof of concept to demonstrate IPv6 feasibility in CompanyXYZ production network. This phase will help demonstrate IPv6 in principle, with a purpose to test and verify IPv6 integration in CompanyXYZ network and its usefulness at CompanyXYZ.

Support for (IPv6), a new suite of standard protocols for the Network layer of the Internet, is built into the latest versions of Microsoft Windows, which include Windows 7, Windows Server 2008 R2, Windows Vista, Windows Server 2008, Windows Server 2003, and Windows CE.NET. IPv6 is also built in to all Unix and Linux machines.

IPv6 is not enabled by default in Windows XP with Service Pack 3, Windows XP with Service Pack 2, Windows XP SP1 and Windows XP Embedded SP1 it has to be explicitly installed and enabled. One can do it by going to

```
Start>run>CMD>ipconfig>netsh>interface>ipv6>install.
```

6.2 Implementing DHCP for IPv6

CompanyXYZ enterprise network has been obtaining it´s addresses for the IPv4 network via state full auto configuration (DHCPv4 server). During this dual stack deployment companyXYZ will use both stateless and state full auto configuration for IPv6 address acquisition. This is due to the fact that some of our current end user devices i.e. Windows XP work stations do not support DHCPv6 and also that stateless auto configuration does not provide the many common options that DHCPv4 or DHCPv6 provides, such as DNS/NTP servers or a domain/host name to be used by the client [22]. The work stations can obtain the address from stateless auto configuration and the other network service options e.g. DNS from state full auto-configuration (DHCPv4/ DHCPv6).

CompanyXYZ also noted that purely IPv6 state full auto configuration for the IPv6 world will only be supported by Cisco IOS software V12.4 that is to be released in Q4/11.Stateless DHCPv6 is a combination of stateless Address Auto configuration and Dynamic Host Configuration Protocol for IPv6. When using stateless-DHCPv6, a device will use Stateless Address Auto-Configuration (SLAAC) to assign one or more IPv6 addresses to an interface, while it utilizes DHCPv6 to receive additional parameters which may not be available through SLAAC (5) such as DNS or NTP server addresses and are provided in a stateless manner by DHCPv6.

Stateless Auto Configuration has automated the IP address configuration of individual network devices. It simplifies the process of IP address allocation by allowing a more streamlined assignment of network addresses thereby facilitating unique identification of network devices over the Internet and intranet.

The first task in stateless auto configuration is for the host to create a unique interface identifier to be used for any link-local or global addresses. This interface identifier called EUI-64 is 64 bits that is adapted from the device's layer two address typically MAC-48 in LAN´s. The IEEE dictates that the conversion from MAC-48 to EUI-64 is carried out by inserting a value of 0xfffe after the first 24 bits of the MAC address. Assuming 0xX (the company ID) and 0xY are hexadecimal values of the original MAC-48 address, the EUI-64 identifier would be computed as XX-XX-XX-FF-FE-YY-YY-YY. Most systems would then insert a binary one at bit seven (counting from the right) to indicate a global scope. The following example illustrates this. The interface identifier is then appended to the prefix fe80::/10, which is reserved for link-local addresses [22].

MAC-48: 00:01:03:69:8B:CF

EUI-64: 0201:03ff:fe69:8bcf

As a point to note, stateless Auto Configuration will not work with layer 2 addresses larger than 118 bits. [22]

The second task in stateless auto configuration is Link-Local Address Uniqueness Test. Where the host performs duplicate address detection (DAD) to ensure the address is unique to the link. The host then joins the all-nodes and solicited-node multicast addresses using the tentative address. With neighbor solicitation and advertisement messages, the host can determine if the address is unique to the link. [22]

Once the uniqueness test is cleared, the IP interface is assigned the link local address, the host then uses the link-local address to send a router solicitation to ff02::2, the all-routers multicast address. The router sends a router advertisement to the all-nodes multicast address with a network prefix, preferred and valid lifetimes, and a MTU for the link. The prefix is appended to the interface identifier and a globally routable IPv6 address is added to the interface. [22]

Once a unique IPv6 address is assigned using stateless auto configuration or static configuration the work stations will use DHCPv6 only to obtain network configuration parameters other than the IPv6 address e.g. DNS and NTP. [22]

The client will send via the link-local address a Unicast or multicast message with its DHCPv6 unique identifier (DUID) to All_DHCP_Relay_Agents_and_Servers and gets a reply with the DHCPv6 options such as DNS and NTP server's parameters. [23]

All client and server messages use the same format i.e. an 8-bit message type with a 24-bit transaction ID and a variable length of options. The transaction ID is used to synchronize server responses to client messages, and must be fairly unique to minimize security issues. [23]To achieve the above DHCPv6 stateless auto configuration we issued the below configuration on the ipv6-core box.

```
IPv6 unicast-routing
IPv6 dhcp pool dhcp-pool
          Dns-server 2001:DB8:8A:1663::2
          Domain-name ipv6test.companyXYZ.com
Interface Vlan661
          Description ipv6 LAN 1
          Ip address 172.19.231.1 255.255.255.240
          Ip helper-address 172.19.231.34
          Ipv6 address 2001:DB8:8A:1661::/64 eui-64
          Ipv6 enable
          Ipv6 nd other-config-flag
          Ipv6 eigrp 220
           Ipv6 dhcp server dhcp-pool
```

The Windows 7 workstation followed the DHCPv6 stateless auto configuration process and was able to acquire the IPv6 address from stateless auto configuration and other network parameters e.g. DNS from state full auto configuration (DHCPv6) as figure 16 illustrates.

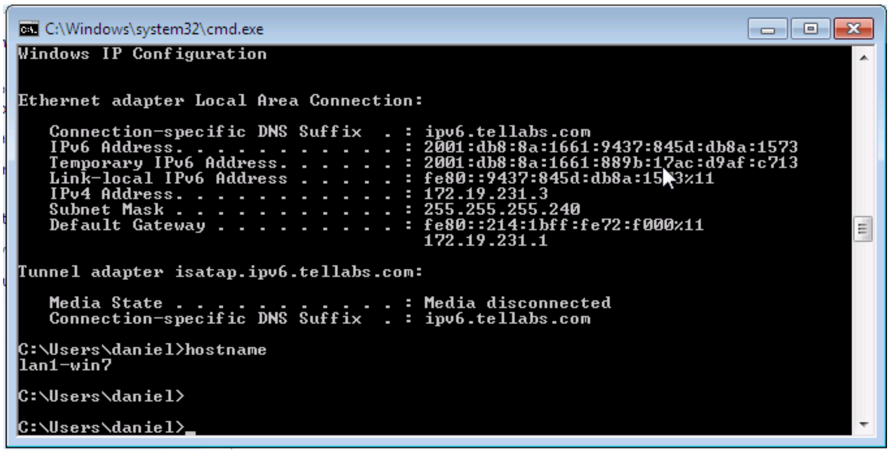

Figure 16. Windows 7 CMD prompt after issued with IPv6 address

Due to the fact that Windows XP workstation don't support DHCPV6 it picked the IPv6 address from stateless auto configuration and used the IP helper-address option to get other network parameters e.g. DNS and NTP as figure 17 illustrates.

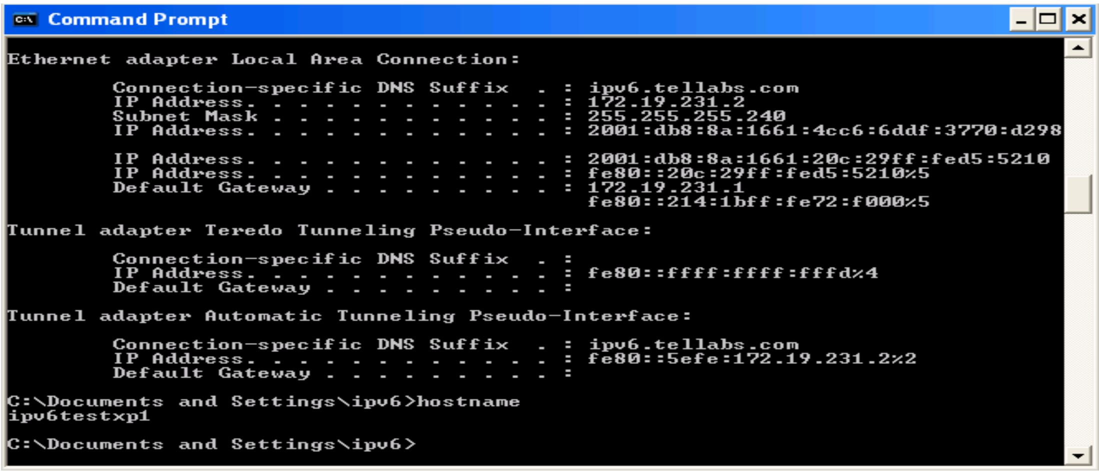

Figure 17. Windows XP CMD prompt after issued with IPv6 address

CompanyXYZ has 60% of the employees still using the Windows XP machine but the workstation´s will be migrated to Windows 7 during normal refresh cycles after end of life of the workstation

6.3 IPv6 Interior Routing

6.3.1 Implementing Static Routes for IPv6

Interior routing protocols or interior gateway protocols (IGP) are protocols which manage routing within an autonomous system (AS). An "autonomous system" in routing terms is a collection of networks that is administered as a whole by a single specific administrator, or in less vague terms, a collection of networks (and/or hosts) that are all connected to each other and which can communicate with each other without resorting to routing outside the autonomous system [24]. CompanyXYZ is currently using static routes and EIGRP routing to route traffic between the different networks in a particular site.

CompanyXYZ uses static routes for sections of a network that have only one path to an outside network and mostly to backup dynamic routes learned through EIGRP. The benefit of using static routes includes security and resource efficiency. Static routes use less bandwidth than dynamic routing protocols and no CPU cycles are used to calculate and communicate routes. The main disadvantage to using static routes is the lack of automatic reconfiguration if the network topology changes.

Before configuring the router with a static IPv6 route, enable the forwarding of IPv6 packets using the ipv6 unicast-routing global configuration command, enable IPv6 on at least one interface, and configure an IPv6 address on that interface.

```
IPv6 unicast-routing
Interface Vlan661
          Ipv6 enable
```

In directly attached static routes, only the output interface is specified. The destination is assumed to be directly attached to this interface, so the packet destination is used as the next-hop address. This example shows such a definition [24]

```
Ipv6 route 2001:db8:8a:1661::/64 vlan 661
```

In a recursive static route, only the next hop is specified. The output interface is derived from the next hop. This example shows such a definition:

```
Ipv6 route 2001:db8:8a:1663:: /64 2001:db8:8a:1663:: 1
Ipv6 route ::/0 2001:470:8229:400::1
```

In a fully specified static route, both the output interface and the next hop are specified. This form of static route is used when the output interface is a multi-access one and it is necessary to explicitly identify the next hop. The next hop must be directly attached to the specified output interface. The following example shows a definition of a fully specified static route:

```
Ipv6 route 2001:db8:8a:1661::/64 gi3/1 2001:db8:8a:1661::1
```

Floating static routes are static routes that are used to back up dynamic routes learned through configured routing protocols. A floating static route is configured with a higher administrative distance than the dynamic routing protocol it is backing up. As a result, the dynamic route learned through the routing protocol is always used in preference to the floating static route. If the dynamic route learned through the routing protocol is lost, the floating static route will be used in its place. The following example defines a floating static route:

```
Ipv6 route 2001:db8:8a:1661::/64 gi3/2 2001:db8:8a:1661::1 210
```

6.3.2 Implementing EIGRP for IPv6

CompanyXYZ is currently using Cisco EIGRP as the internal routing protocol. CompanyXYZ choose EIGRP because it uses an algorithm called the diffusing update algorithm (DUAL) allowing faster network convergence properties and operating efficiency [25]. This algorithm guarantees loop-free operation at every instant throughout a route computation and allows all devices involved in a topology change to synchronize at the same time. Routers that are not affected by topology changes are not involved in recompilations. [25]

EIGRP for IPv6 was directly configured on the interfaces over which it runs i.e. VLAN 661, VLAN 662 and VLAN 663, which allows EIGRP for IPv6 to be configured without the use of a global IPv6 address.

```
Interface Vlan661
     Ipv6 eigrp 220
     No shutdown
```

An admin can also use IPv6 EIGRP passive-interface configuration instead of configuring on the interface that is made passive.

```
Ipv6 router eigrp 220
        Passive-interface default
        No passive-interface Vlan661
        No passive-interface Vlan663
        No passive-interface Vlan662
        No passive-interface Tunnel20
```

To display info about interfaces configured for IPv6 EIGRP

```
Fiesp-ipv6-65091#show ipv6 eigrp 220 topology
EIGRP-IPv6 Topology Table for
AS(220)/ID(172.19.231.245)
Codes: P - Passive, A - Active, U - Update, Q - Query,
R - Reply,
       r - reply Status, s - sia Status
P 2001:DB8:8A:1662::/64, 1 successors, FD is 2816
        via Connected, Vlan662
P 2001:470:8229:327::/64, 1 successors, FD is 26882560
        via FE80::AC17:E5FA (26882560/28160), Tunnel20
P 2001:470:8229:383::/64, 1 successors, FD is 28160256
        via FE80::AC17:E5FA (28160256/26880256), Tun-
nel20
P 2001:470:8229:283::/64, 1 successors, FD is 28160256
        via FE80::AC17:E5FA (28160256/26880256), Tun-
nel20
P 2001:470:8A:1660::/64, 1 successors, FD is 26880000
        via Connected, Tunnel20
P 2001:DB8:8A:1661::/64, 1 successors, FD is 2816
        via Connected, Vlan661
P 2001:470:8229:305::/64, 1 successors, FD is 28160256
        via FE80::AC17:E5FA (28160256/26880256), Tun-
nel20
P 2001:DB8:8A:1663::/64, 1 successors, FD is 2816
        via Connected, Vlan663
P 2001:470:8229:454::/64, 1 successors, FD is 28162560
        via FE80::AC17:E5FA (28162560/26882560), Tun-
nel20
P 2001:470:8229:350::/64, 1 successors, FD is 28160000
        via FE80::AC17:E5FA (28160000/26880000), Tun-
nel20
```

Below are a list of ways in which EIGRP for IPv6 differs from EIGRP IPv4 and also a list of IPv6 for EIGRP restrictions: [25]

- EIGRP for IPv6 is directly configured on the interfaces over which it runs. This feature allows EIGRP for IPv6 to be configured without the use of a global IPv6 address. There is no network statement in EIGRP for IPv6.
- In per-interface configuration at system startup, if EIGRP has been configured on an interface, then the EIGRP protocol may start running before any EIGRP router mode commands have been executed.
- An EIGRP for IPv6 protocol instance requires a router ID before it can start running.
- EIGRP for IPv6 has a shutdown feature. The routing process should be in "no shut" mode in order to start running.

- When a user uses a passive-interface configuration, EIGRP for IPv6 need not be configured on the interface that is made passive.
- EIGRP for IPv6 provides route filtering using the distribute-list prefix-list command. Use of the route-map command is not supported for route filtering with a distribute list. [25]

6.4 IPv6 Exterior Routing

6.4.1 Implementing Multiprotocol BGP for IPv6

Exterior routing protocols or Exterior Gateway Protocols (EGP) are protocols which manage routing outside an Autonomous System and get you from your current network, through your service provider network and onto any other network. An autonomous system in routing terms is a collection of networks that is administered as a whole by a single specific administrator [24]. CompanyXYZ is currently using BGP routing to route traffic between the different Autonomous Systems.

CompanyXYZ uses BGP on the WAN as an EGP mainly to connect separate routing domains that contain independent routing policies (autonomous systems). CompanyXYZ autonomous systems communication is facilitated by Verizon Company. Verizon is running an MPLS network to facilitate communication over there cloud. Currently our WAN provider; Verizon business does not currently support BGP for IPv6. They project that they will start to support IPv6 BGP in the beginning of Q3/11. Verizon business currently supports only IPv6 on the internet side [26] [27]. CompanyXYZ tested multiprotocol BGP for IPv6 in its test bed but not in the production network.

Multiprotocol BGP is the supported EGP for IPv6. Multiprotocol BGP extensions for IPv6 support the same features and functionality as IPv4 BGP. IPv6 enhancements to multiprotocol BGP include support for an IPv6 address family and Network Layer Reachability Information (NLRI) and next hop (the next router in the path to the destination) attributes that use IPv6 addresses. [28]

IPv6 enhancements to multicast BGP include support for an IPv6 multicast address family, NLRI and next hop attributes that use IPv6 addresses. Users must use multiprotocol BGP for IPv6 multicast when using IPv6 multicast with BGP because the unicast

BGP learned routes will not be used for IPv6 multicast. Multicast BGP functionality is provided through a separate address family context. A Subsequent Address Family Identifier (SAFI) provides information about the type of the network layer reachability information that is carried in the attribute. Multiprotocol BGP unicast uses SAFI 1 messages, and multiprotocol BGP multicast uses SAFI 2 messages. SAFI 1 messages indicate that the routes are only usable for IP unicast, but not IP multicast. Because of this functionality, BGP routes in the IPv6 unicast RIB must be ignored in the IPv6 multicast RPF lookup. [28]

The graceful restart capability is supported for IPv6 BGP unicast, multicast, and VPNv6 address families, enabling Cisco Nonstop Forwarding (NSF) functionality for BGP IPv6. The BGP graceful restart capability allows the BGP routing table to be recovered from peers without keeping the TCP state. [28]

NSF continues forwarding packets while routing protocols converge, therefore avoiding a route flap on switchover. Forwarding is maintained by synchronizing the FIB between the active and standby RP. On switchover, forwarding is maintained using the FIB. The RIB is not kept synchronized; therefore, the RIB is empty on switchover. The RIB is repopulated by the routing protocols and subsequently informs FIB about RIB convergence by using the NSF_RIB_CONVERGED registry call. The FIB tables are updated from the RIB, removing any stale entries. The RIB starts a failsafe timer during RP switchover, in case the routing protocols fail to notify the RIB of convergence. [28]

For CompanyXYZ to support multiprotocol BGP extensions for IPv6 it first created the BGP routing process then configured the peering relationships, and finally customize the BGP to suite CompanyXYZ production network.

BGP uses a router ID to identify BGP-speaking peers. The BGP router ID is 32-bit value that is often represented by an IPv4 address. By default, the Cisco IOS software sets the router ID to the IPv4 address of a loopback interface on the router or the highest IPv4 address configured to a physical interface on the router. When configuring BGP on a router that is enabled only for IPv6 (the router does not have an IPv4 address), you must manually configure the BGP router ID for the router.[28]

```
Router bgp 65000
         No bgp default ipv4-unicast
         Bgp router-id 172.19.XX.XX
```

The neighbor remote-as command in router configuration mode exchange only IPv4 unicast address prefixes To exchange other address prefix types, such as IPv6 prefixes, neighbors must also be activated using the neighbor activate command in address family configuration mode for the other prefix types, as shown for IPv6 prefixes

```
Router bgp 65000
Neighbor 2001: DB8: 008a:1668::101 remote-as 66000
Address-family ipv6
Neighbor 2001: DB8: 008a:1668::101 activate
```

To inject a network into another database, such as the IPv6 BGP database, you must define the network using the network command in address family configuration mode for the other database, as shown for the IPv6 BGP database.

```
Router bgp 65000
Address-family ipv6 unicast
Network 2001: DB8: 8a:1669::/64
```

IPv6 Multiprotocol BGP Redistribution is the process of redistributing, or injecting, prefixes from one routing protocol into IPv6 multiprotocol BGP.

```
Router bgp 65000
Address-family ipv6
Redistribute bgp 64500 metric 5 metric-type external
```

It is possible to use IPv6 to advertise the IPv4 routes. Configure the peering using the IPv6 addresses within the IPv4 address family. Set the next hop with a static route or with an inbound route map because the advertised next hop will usually be unreachable. Advertising IPv6 routes between two IPv4 peers is also possible using the same model.

```
Router bgp 65000
Neighbor 2001:DB8:8A:1668::101 remote-as 66000
Address-family ipv4
 Neighbor 2001:DB8:8A:1668::101 remote-as 66000
```

To view the IPv6 BGP routing table, use the show BGP IPv6 unicast command. Below is the result

```
BGP table version is 45, local router ID is 172.19.231.81
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP,? - Incomplete

   Network                          Next Hop              Metric
       LocPrf     Weight              Path
*>2001: DB8: 008a:1668::101                            0
3748          4697                                  i
*>2001: DB8: 008a:1669::/64       2001:   DB8:   008a:1667::100
0      3748          4697          i
*>2001: DB8: 008a:1670::/64       2001:   DB8:   008a:1668::100
0      3748          4697          i
```

To view the status of all IPv6 BGP connections use the show bgp IPv6 unicast summary command. Below is the output.

```
BGP router identifier 172.19.xx.xx, local AS number 6500
BGP table version is 45, main routing table version 45

Neighbor                                                    V    AS
MsgRcvd MsgSent   TblVer  InQ  OutQ  Up/Down   State/PfxRcd
2001:470:8A:1668::101
4    6600    639        629         45              0       0
   2w2d       Active
```

6.4.2 Implementing Tunneling for IPv6

In some circumstance the IPv4 infrastructure was not upgraded to accommodate IPv6 hence we used tunneling to communicate with isolated IPv6 networks. The tunnels allowed stable secure connections between two dual-stack edge routers. We used the below tunneling mechanism.

```
Router Finland IPv6 6509 1
     Interface Tunnel20
           Ipv6 address 2001:DB8:8A:1660:: 2/64
           Ipv6 enable
           Tunnel source Vlan660
           Tunnel destination 172.23.XX.XX
           Tunnel mode ipv6ip
```

```
Router Naperville IPv6
    Interface Tunnel20
             Ipv6 address 2001:470:8A:1660::1/64
             Ipv6 enable
             Tunnel source Vlan1
             Tunnel destination 172.19.XX.XX
             Tunnel mode ipv6ip
```

With the Manually configured tunnels an IPv6 address was configured on a tunnel interface and a manually configured IPv4 addresses were assigned to the tunnel source and the tunnel destination both routers at each end of the configured tunnel supported both the IPv4 and IPv6 protocol stacks. [29] This method was used to interconnect the different IPv6 test beds in CompanyXYZ production network when the CompanyXYZ network was not IPv6 ready.

```
Router Finland IPv6 6509 1
    Interface Tunnel20
           Ipv6 address 2001:DB8:8A:1660:: 2/64
           Ipv6 enable
          Tunnel source Vlan660
           Tunnel destination 172.23.XX.XX
          Tunnel mode gre ipv6

Router Usnap-ipv6-sky
    Interface Tunnel20
             Ipv6 address 2001:470:8A:1660::1/64
             Ipv6 enable
             Tunnel source Vlan1
             Tunnel destination 172.19.231.245
             Tunnel mode gre ipv6
```

To verify the configuration

```
Finland IPv6 6509 1#show ipv6 int tunnel 20
         Tunnel20 is up, line protocol is up
           IPv6 is enabled, link-local address is
         FE80::AC13:E7F5
           No Virtual link-local address (es):
           Global unicast address (es):
             2001:DB8:8A:1660::2, subnet is
         2001:DB8:8A:1660::/64
           Joined group address (es):
             FF02::1
             FF02::2
             FF02::A
             FF02::1:FF00:2
             FF02::1:FF13:E7F5
           MTU is 1480 bytes
```

```
  ICMP error messages limited to one every
100 milliseconds
  ICMP redirects are disabled
  ICMP unreachables are disabled
  Output features: HW Shortcut Installation
  ND DAD is enabled, number of DAD attempts:
1
  ND reachable time is 30000 milliseconds
  Hosts use stateless autoconfig for ad-
dresses.
```

With GRE/IPv4 tunnels, IPv6 traffic is carried over standard IPv4 GRE tunnels. The GRE tunnel carries IPv6 as the passenger protocol with the GRE as the carrier protocol and IPv4 or IPv6 as the transport protocol. With GRE IPv6 tunnels, IPv6 addresses are assigned to the tunnel source and the tunnel destination. The tunnel interface can have either IPv4 or IPv6 addresses assigned. The router at each end of a configured tunnel must support dual stack mode. [29]

6.4.3 Implementing Tunnel brokers for IPv6

As early adopters CompanyXYZ used tunnel brokers to hook up to an existing IPv6 network and to get stable, permanent IPv6 addresses and DNS names to reach the IPv6 Internet by tunneling over existing IPv4 connections from your IPv6 enabled host or router to one of the tunnel brokers IPv6 router. A dual stack router will be needed to use this service. [30]

CompanyXYZ followed the below steps to get a free tunnel broker service to the test network

- go to http://tunnelbroker.net/
- click register and fill in the form.
- after registering a password will be sent to your email
- return to the site to activate tunnel. Upon tunnel activation configuration commands for a variety of platforms will be automatically generated. Once you configure your side you will be able to reach the IPv6 Internet

In the Petaluma dual stack IPv6 test environment. CompanyXYZ connected to the IPv4 internet.

```
Interface Tunnel100
      Description tunnelbroker.net
      IP unnumbered Loopback0
      Tunnel source Loopback0
      Tunnel destination 72.52.XX.XX
```

CompanyXYZ then created a tunnel to the tunnel broker as can be seen in the configuration above in order to establish a secure connection with the tunnel broker. After this configuration were issued with an IPv6 address space of 2001:470:8229::/48.

7 IPv6 advanced Features

7.1 Implementing HSRP for IPv6

The Hot Standby Router Protocol (HSRP) is a First Hop Redundancy Protocol (FHRP) designed to allow for transparent failover of the first-hop IP router. HSRP provides high network availability by providing first-hop routing redundancy for IP hosts on Ethernet configured with a default gateway IP address. HSRP is used in a group of routers for selecting an active router and a standby router. In a group of router interfaces, the active router is the router of choice for routing packets; the standby router is the router that takes over when the active router fails or when preset conditions are met. HSRP is designed to provide only a virtual first hop for IPv6 hosts. [31]

An HSRP IPv6 group has a virtual MAC address that is derived from the HSRP group number, and a virtual IPv6 link-local address that is, by default, derived from the HSRP virtual MAC address. HSRP IPv6 uses a different virtual MAC address block than does HSRP for IP: 0005.73A0.0000 through 0005.73A0.0FFF (4096 addresses). [31]

HSRP uses a priority mechanism to determine which HSRP configured router is to be the default active router. To configure a router as the active router, assign it a priority that is higher than the priority of all the other HSRP-configured routers. The default priority is 100, so if one router is configured to have a higher priority, that router will be the default active router.

HSRP version 2 must be enabled on an interface before HSRP IPv6 can be configured. [31]

```
Finland IPv6 6509 1
         Interface Vlan661
          Standby version 2
          Standby 1 ipv6 2001:DB8:8A:1661::1
          Standby 1 preempt
          Standby 1 priority 110
         Standby 1 timers 2 5

Finland IPv6 6509 2
         Interface Vlan661
          Standby version 2
          Standby 1 ipv6 2001:DB8:8A:1661::1
          Standby 1 preempt
          Standby 1 timers 2 5
```

Router solicitation messages, which have a value of 133 in the Type field of the Internet Control Message Protocol (ICMP) packet header, are sent by hosts at system startup so that the hosts can immediately auto configure without needing to wait for the next scheduled RA message. [31]

```
Finland IPv6 6509 1#show standby
     Vlan661 - Group 1 (version 2)
       State is Active
         2 state changes, last state change 1d00h
       Link-Local Virtual IPv6 address is
     FE80::5:73FF:FEA0:1 (impl auto EUI64)
         Virtual IPv6 address 2001:DB8:8A:1661::1/64
       Active virtual MAC address is 0005.73a0.0001
         Local virtual MAC address is 0005.73a0.0001 (v2
     IPv6 default)
       Standby router is FE80::214:1BFF:FE9B:4C00, priori-
     ty 100 (exp in 3.728 sec)
       Priority 110 (configured 110)
       Group name is "hsrp-Vl661-1" (default)
     Finland IPv6 6509 2#show standby
    Vlan661 - Group 1 (version 2)
      State is Standby
        1 state change, last state change 00:00:00
      Link-Local Virtual IPv6 address is
    FE80::5:73FF:FEA0:1 (impl auto EUI64)
        Virtual IPv6 address 2001:DB8:8A:1661::1/64
      Active virtual MAC address is 0005.73a0.0001
        Local virtual MAC address is 0005.73a0.0001 (v2
    IPv6 default)
      Preemption enabled
      Active router is FE80::214:1BFF:FE72:F000, priority
    110 (expires in 3.584 sec)
         Standby router is local
```

```
Priority 100 (default 100)
Group name is "hsrp-Vl661-1" (default)
```

7.2 QoS for IPv6

CompanyXYZ had hoped for good improvement in the next generation of the IP protocol. The reality is that neither evolutionary nor revolutionary changes were introduced in the IPv6 QoS. QoS improvements in IPv6 are but a myth at this point. The same concepts and the same architecture apply to the new protocol with a few small differences and implementation consideration that are worth mentioning [32].

The IPv6 header was redesigned to minimize header overhead and reduce the header process for the majority of the packet as illustrated in picture 3. [33] Currently IPv6 provides support for QoS marking via a field in the IPv6 header. Similar to the type of service (ToS) field in the IPv4 header, the traffic class field (8 bits) is available for use by originating nodes and/or forwarding routers to identify and distinguish between different classes or priorities of IPv6. [34]

The traffic class field may be used to set specific precedence or differentiated services code point (DSCP) values. These values are used in the exact same way as in IPv4.

IPv6 also has a 20-bit field known as the flow label field [35]. The flow label enables per-flow processing for differentiation at the IP layer. It can be used for special sender requests and is set by the source node. The flow label must not be modified by an intermediate node. The key advantage with the flow label is that the transit routers do not have to open the inner packet to identify the flow, which aids with identification of the flow when using encryption and other scenarios.

Current Cisco IOS® Software support for IPv6 QoS includes:

- Packet classification
- Queuing (includes LLQ; excludes legacy PQ/CQ)
- Traffic shaping
- WRED

Planned Cisco IOS Software support for IPv6 QoS includes:

- Compressed Real-Time Protocol (CRTP)
- Network-based application recognition (NBAR)
- Committed access rate (CAR).[35]

IPV6 uses a more sophisticated approach to handle data from applications requiring priority handling. the originating device will query the destination in order to determine the maximum size of the payload that can be handled across the complete route. then it adjusts its own parameters and will not load the originating packet with more data that the smallest frames or cell the network can handle. This approach reduces fragmentation and latency but can also result in inefficient utilization. The tradeoff is that shorter payloads, it achieve a higher bandwidth with prompt arrival. [36]

7.3 Implementing NetFlow for IPv6

CompanyXYZ uses NetFlow to collect traffic flow statistics for our network elements and be able to analyze traffic patterns for our production network. [37] For CompanyXYZ to support NetFlow for the IPv6 world we had to use NetFlow Version 9. [37] NetFlow version 9 export format is the newest NetFlow export format. The distinguishing feature of the NetFlow version 9 export formats is that it is template based. Templates make the record format extensible. NetFlow version 9 export format allows future enhancements to NetFlow without requiring concurrent changes to the basic flow-record format. [38]

The NetFlow version 9 export record format is different from the traditional NetFlow fixed format export record. In NetFlow version 9, a template describes the NetFlow data, and the flow set contains the actual data. This arrangement allows for flexible export. [38]

NetFlow version 9 export format provided CompanyXYZ some key benefits that include: [38]

- CompanyXYZ could be able to export almost any information from a router or switch, including Layer 2 through 7 information, routing information, IP version 6 (IPv6), IP version 4 (IPv4), multicast, and Multiprotocol Label Switching (MPLS) information. This new information allows new applications for export data and new views of network behavior.

- The NETQOS tool did not have to recompile the applications each time a new NetFlow export field is added. Instead it used an external data file that documents the known template formats.
- CompanyXYZ was able to add new features to NetFlow more quickly, without breaking current implementations. The NetFlow version 9 export packet header format is shown in Table 5

Table 5. NetFlow Version 9 Export Packet Header Field Names and Descriptions [38]

Bytes	Field Name	Description
0-1	Version	The version of NetFlow records exported in this packet; for version 9, this value is 0x0009.
2-3	Count	Number of Flow Set records (both template and data) contained within this packet.
4-7	System Uptime	Time in milliseconds since this device was first booted.
8-11	Unix Seconds	Seconds since 0000 Coordinated Universal Time (UTC) 1970.
12-15	Sequence Number	Incremental sequence counter of all export packets sent by this export device; this value is cumulative, and it can be used to find out whether any export packets have been missed. This is a change from the NetFlow version 5 and version 8 headers, where this number represented "total flows."
16-19	Source ID	The Source ID field is a 32-bit value that is used to guarantee uniqueness for each flow exported from a particular device. (The Source ID field is the equivalent of the engine type and engine ID fields found in the NetFlow version 5 and version 8 headers.) The format of this field is vendor specific. In Cisco's implementation, the first two bytes are reserved for future expansion and are always zero. Byte 3 provides uniqueness with respect to the routing engine on the exporting device. Byte 4 provides uniqueness with respect to the particular line card or Versatile Interface Processor on the exporting device. Collector devices should use the combination of the source IP address and the Source ID field to associate an incoming NetFlow export packet with a unique instance of NetFlow on a particular device.

CompanyXYZ implemented the below configuration to enable IPv6 NetFlow on it production network

```
Ipv6 unicast-routing
Mls flow ipv6 interface-full
Mls nde sender
Ipv6 flow-export version 9
Ipv6 flow-export source loopback 100
Ipv6 flow-export destination 10.0.101.254 9991
Ipv6 flow-top-talkers
 Top 10
 Sort-by packets
Interface FastEthernet6/3
Ipv6 flow ingress
```

With NetFlow enabled CompanyXYZ could monitor the IPv6 network.

8 Conclusions

In most of the current networks, the transition to IPv6 is yet to be accomplished on many fronts. Not only technical issues such as ISO/OSI layers or application-development perspective need to be refined but also administrative procedures for transition and business cases for IPv6 will have to be developed. The goal of this work was to create a step by step detailed procedure and mechanism how CompanyXYZ as a whole deployed IPv6 to its production network.

In the first chapter I introduced the company and presented the business justification for CompanyXYZ to deploy and transition to IPv6 in its production network. In the second chapter I gave an overview of IPv6 and also covered the basic concepts of IPv6 protocol in this chapter. The third chapter dealt with assessing and taking an inventory of CompanyXYZ production network to help us evaluate IPv6 readiness in CompanyXYZ production network, in this chapter I also went ahead and described the several transition strategies, targeted to the distinct types of CompanyXYZ networks. Each of these strategies was described in terms of addressing scheme, layer 2 technologies and network protocols. Also, a transition roadmap for each particular strategy was given. The fifth chapter looked at the test environment that CompanyXYZ built to evaluate the integration of IPv6 technology with CompanyXYZ production network finally chapter 6 and 7 discussed IPv6 proof of concept to demonstrate IPv6 feasibility in CompanyXYZ production network.

The overall IPv6 deployment experience has been very positive for CompanyXYZ. CompanyXYZ has deployed IPv6 on all the existing IPv4 network links, enabling both unicast and multicast IPv6 traffic. CompanyXYZ has enabled many network and application services dual stack including our external facing web server and DNS services. The dual-stack approach to deployment worked well for CompanyXYZ.

IPv6 is robust in operation and has overcomes many of the limitations of IPv4 while introducing new features and functionality. Where IPv6 is significantly different from IPv4, the changes are meant to enhance the administration experience. Where the similarities to IPv4 remain, the IPv6 protocol feels familiar. CompanyXYZ has not observed any degrading of long established IPv4 services. There have been occasional issues that have risen, but these have been addresses quite quickly and none were significant.

The main challenge in running dual stack enterprise lies in monitoring and managing both protocol and to ensure consistent operation between the protocols. The main tasks CompanyXYZ has still to complete are to establish a DHCPv6 services for our client system, to enable IPv6 support in the remaining applications. By integrating IPv6 services in the intranet, CompanyXYZ is well positioned to take advantage of the potential offered by these developments. It can quickly evolve in step with them and it can therefore maintain leadership in its market.

CompanyXYZ noted that IPv6 is still an open issue and there are a lot of challenges to work on. The biggest challenge is in making people aware of the importance of returning to a simple Internet that can support innovation and exciting new ideas. Towards this end CompanyXYZ must assure that there is a focus on IPv6 at the edges. As users we should demand it of the vendors and as implementers we should make use of IPv6 and, when possible, provide our own implementations.

I hope this work will be found useful by both network operators and designers, and will be used to design strategies for transition to IPv6 protocol based on the presented strategies, or at least as a reference.

References

1 About CompanyXYZ [online].
URL: http://www.companyXYZ.com/about/. Accessed 16 August 2010

2 AT&T and IPv6 [online].
URL: http://www.corp.att.com/gov/solution/network_services/data_nw/ipv6/. Accessed 16 August 2010

3 RFC 1752. The Recommendation for the IP Next Generation Protocol [online].
URL: http://tools.ietf.org/html/rfc1752. Accessed 17 August 2010

4 What is IPv6? [Online].
URL: http://www.opus1.com/ipv6/whatisipv6.html. Accessed 11 August 2010

5 Building scalable Cisco internetworks. 3rd edition (BSCI). Diane Teare, Catherine Paquet, Paul boger, Cisco press 800 east 96th street Indianapolis, IN 46240 USA. Page 649-650

6 IPv6 Wikipedia [online].
URL: http://en.wikipedia.org/wiki/IPv6. Accessed 11 August 2010

7 RFC 4862. IPv6 Stateless Address Auto configuration [online].
URL: http://www.rfc-editor.org/rfc/rfc4862.txt. Accessed 11 August 2010

8 IPv6 security issues [online].
URL: http://www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf. Accessed 11 June 2010

9 IPv4 header and IPv6 header [online].
URL:http://shivasoft.in/tutorialImages/113/IPV6IPv4.jpg.
Accessed 13 August 2010

10 S.Blake, etal. An Architecture for differentiated services. RFC2475, internet Engineering task force December 1998

11 k.Ramakrishnan, S.Floyd and D.Black."The addition of explicit congestion Notification (ECN) to IP,"RFC3168, internet engineering task force, September 2001

12 IPv6 advanced protocols implementation Qing li, tatuya jinmei, keiichi shima. Morgan Kaufmann publishers 500 sansome street suite 400, San Francisco. Printed by Elsevier Inc

13 Enterprise networking planet. Understand IPv6 Addresses [Online] URL:http://www.enterprisenetworkingplanet.com/netsp/article.php/1095336332111/Understand-IPv6-Addresses.htm. Accessed 14 August 2010

14 RFC 2373. IP Version 6 Addressing Architecture [online]. URL: http://www.ietf.org/rfc/rfc2373.txt. Accessed 13 August 2010

15 Building scalable Cisco internetworks, 3rd edition, Diane Teare, Catherine Paquet, pg. 688-689

16 RFC4213.Basic transition mechanisms for IPv6 hosts and routers [online]. URL: http://tools.ietf.org/html/rfc4213. Accessed 13 August 2010

17 Network world.IPv6: dual stack where you can; tunnel where you must [online]. URL: http://www.networkworld.com/news/tech/2007/090507-tech-uodate.html. Accessed 13 August 2010

18 CompanyXYZ IPv4 Address management. TNIC [online]. URL:https://sharepoint.companyXYZ.com/sites/IT/Networking/Pages/Secured.aspx?RootFolder=%2fsites%2fIT%2fNetworking%2fSecured%2fNetwork%20Documents%2fTNIC&FolderCTID=&View={7204BF8C-2218-4F56-A156-690732DC90DD}.Accessed 1 September 2010

19 IBM. Hierarchical Addressing and Routing Infrastructure [online] URL:http://publib.boulder.ibm.com/infocenter/zvm/v5r4/index.jsp?topic=/com.ibm.zvm.v54.kijl0/hcsk7b3012.htm.Accessed 1 July 2010

20 ARIN IPv6 address planning Wikipedia [online] URL: http://www.getipv6.info/index.php/IPv6_Addressing_Plans. Accessed 1 august 2011

21 Address supporting organization [online]. URL: http://aso.icann.org/. Accessed 1 august 2011

22 Stateless auto configuration [online]. URL: http://www.prolixium.com/ipv6_autocfg/node7.html. Accessed October 25 2010

23 Stateless auto configuration (DHCPv6). [Online]. URL: http://www.prolixium.com/ipv6_autocfg/node8.html\. Accessed October 26 2010

24 Existing routing protocol and IPv6 [online].
URL: http://www.tuxick.net/linux/ip6routing.html. Accessed 28 February 2011

25 Cisco. Implementing EIGRP for IPv6 [online].
URL:http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-eigrp.html.Acessed 28 February 2011

26 Verizon business whitepaper. Border gateway protocol best practice [online].
URL: http://onesc.net/communities/as701/bordergateproto.pdf.
Accessed February 4 2011

27 Verizon business. Verizon begins testing IPv6 on FIOS services [online].
URL: http://newscenter.verizon.com/press-releases/verizon/2010/verizon-begins-testing-ipv6.html. Accessed February 4 2011

28 Cisco. Implementing multiprotocol BGP for IPv6 [online].
URL:http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-mptcl_bgp_ps6922_TSD_Products_Configuration_Guide_Chapter.html.
Accessed February 5 2011

29 Cisco. Implementing Tunneling for IPv6. [Online].
URL:http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6 tunnel.html. Accessed February 6 2011

30 RFC 3053. IPv6 tunnel broker [online].
URL:http://www.faqs.org/rfcs/rfc3053.html. Accessed February 6 2011

31 Cisco. Configuring first hop redundancy protocols I IPv6. [Online].
URL: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-fhrp.html. Accessed February 16 2011

32 Deploying IPv6 networks. Ciprian popoviciu, Eric levy-abegnoli, Patrick Grossetete. Cisco press 800 East 96th street, Indianapolis, IN 46240 USA.

33 IPv6DISSemination and exploitation. QoS support in IPv6 environment [online].
URL: http://www.6diss.org/workshops/see-1/qos.pdf.Accessed February 17 2011

34 Cisco. IPv6 QoS at a glance [online].
URL: http://www.cu.ipv6tf.org/cookbook/ipv6qos.pdf.
Accessed February 18 2011

35 RFC 3697.IPv6 flow label specification [online].
URL: http://www.faqs.org/rfcs/rfc3697.html. Accessed February 18 2011

36 Secureit-net. Quality of service in IPv6 [online].
URL:http://www.netdummy.net/qos.html. Accessed February 18 2011

37 Cisco. Implementing NetFlow for IPv6 [online].

URL:http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-netflow.html. Accessed February 18 2011

38 Cisco. NetFlow v9 for IPv6 [online].
URL:http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ ip6-netlow_v9_ps6441_TSD_Products_Configuration_Guide_Chapter.html. Accessed February 18 2011

39 Wikipedia. Regional internet registry. [Online].
URL:http://en.wikipedia.org/wiki/Regional_Internet_registry.
Accessed January 8 2011

40 African Network Information Centre (AfriNIC) [Online].
URL: http://www.afrinic.net/. Accessed January 8 2011

41 American Registry for Internet Numbers (ARIN) [Online].
URL: https://www.arin.net/. Accessed January 8 2011

42 Asia-Pacific Network Information Centre (APNIC) [Online].
URL: http://www.apnic.net/. Accessed January 8 2011

43 Latin America and Caribbean Network Information Centre (LACNIC) [Online].
URL: http://www.lacnic.net/en/index.html. Accessed January 8 2011

44 Réseaux IP Européens Network Coordination Centre (RIPE NCC) [Online].
URL: http://www.ripe.net/. Accessed January 8 2011

45 Number Resource Organization (NRO) [Online].
URL: http://www.nro.net/. Accessed January 8 2011

46 CompanyXYZ networking documents [Online].
Url:https://sharepoint.companyxyz.com/sites/IT/Networking/.
Accessed 14 August 2010

47 Dual stack network [Online].
URL: http://www.potaroo.net/ispcol/2009-09/fig2.jpg. Accessed 13 August 2010

48 IPv6 tunneled network [Online].
URL: http://www.potaroo.net/ispcol/2009-09/fig1.jpg. Accessed 13 August 2010

Appendix 1: Regional Internet registry

A regional Internet registry (RIR) is an organization that manages the allocation and registration of Internet number resources within a particular region of the world. Internet number resources include IP addresses and autonomous system (AS) numbers. [39]

There are five RIRs as can be seen in figure below:

- African Network Information Centre (AfriNIC) for Africa [40]
- American Registry for Internet Numbers (ARIN) for the United States, Canada, and several parts of the Caribbean region.[41]
- Asia-Pacific Network Information Centre (APNIC) for Asia, Australia, New Zealand, and neighboring countries.[42]
- Latin America and Caribbean Network Information Centre (LACNIC) for Latin America and parts of the Caribbean region [43]
- RIPE NCC for Europe, the Middle East, and Central Asia [44]

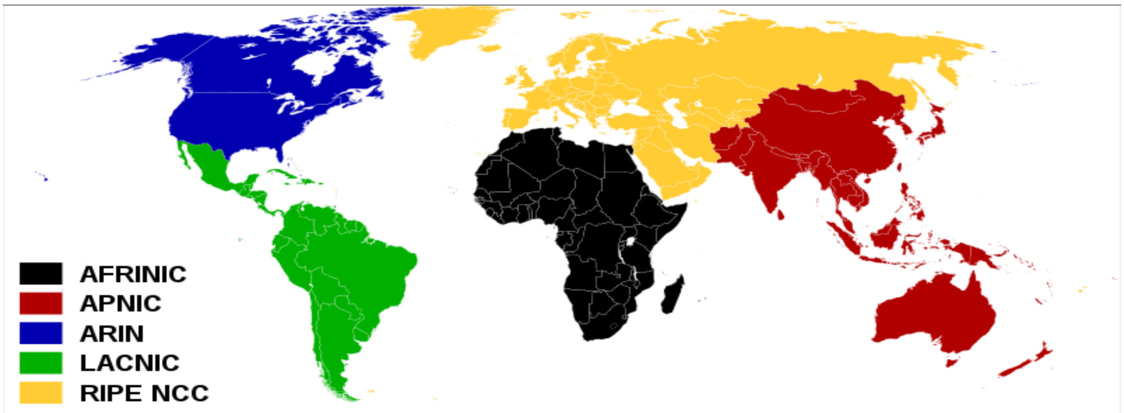

Fig 18: Regional Internet Registries world map [13]

The Internet Assigned Numbers Authority (IANA) delegates Internet resources to the RIRs who, in turn, follow their regional policies to delegate resources to their customers, which include Internet service providers and end-user organizations. Collectively, the RIRs participate in the Number Resource Organization (NRO), [45] formed as a body to represent their collective interests, undertake joint activities, and coordinate their activities globally. The NRO has entered into an agreement with ICANN for the establishment of the Address Supporting Organization (ASO), [21] which undertakes coordination of global IP addressing policies within the ICANN framework. [39]

Appendix 2: Introduction to CompanyXYZ