CHAPTER-2

BASIC CONCEPTS AND RESEARCH DESIGN

The transition from IPv4 to IPv6 is a major event that touches all aspects of a corporation’s information systems. As such, there has been much literature written identifying the best methodologies to transition systems to the new routing protocol. Additionally, much literature has also been written outlining issues that corporations will inevitably face in making the transition. The literature reviewed for this research provides the necessary background information, key concepts, and issues surrounding the transitioning from IPv4 to IPv6 to Mobile IPv6 and various techniques to the solution up to now. There are several underlying concepts that can be found in the majority of literature reviewed for this thesis. These concepts include, but are not limited to, Internet protocols, Mobile IPv6 benefits and transition methodologies.

2.1. Internet Protocol (IP)

The Internet Protocol is the method of transporting data across the Internet. It specifies an addressing scheme as well as the format of data packets. This combined with the Transmission Control Protocol (TCP) provides a connectionless virtual connection between a source and destination.

2.2. Internet Protocol Version 4.0

IPv4 is the current most widely used specification of the Internet Protocol used on the Internet today. It was developed by the Defense Advanced Research Projects Agency (DARPA) in 1981 under the Internet Engineering Task Force (IETF) Request for Comments (RFC) 791 (University of Southern California, 1981) [41]. The specification provides a 32-bit address format, which uniquely identifies 4.3 billion addresses. With the increasing popularity of the Internet and the increasing number of new networks, there is a concern that all IPv4 addresses will be allocated by 2010 (Geesey, 2005) [42]. The IPv4 specification provides for a 32-bit IP address to identify network components. This 32-bit address results in a total of 4.3 billion unique addresses. In other words, there are only 4.3 billion network
components that can be uniquely identified throughout the world. In 1981, this number of addresses seemed more than adequate for a network standard. Since the release of the IPv4 standard, the Internet has grown exponentially and spans across the globe. It is not uncommon to find more than one computer in the average household. As the Internet continues to grow, IPv4 addresses continue to be allocated and used up. It is believed that the pool of IPv4 address space will be exhausted in the next few years.

2.3. Internet Protocol Version 6.0

IPv6 is the next generation of the Internet Protocol specification based upon the IETF RFC 2460 [43]. The specification provides a 128-bit address format, which uniquely identifies $3.4 \times 10^{38}$ addresses. RFC 1719 set guidelines for choosing the replacement protocol to IPv4. These guidelines took into consideration address space exhaustion, networking trends, advanced feature sets, and the timeline required to develop, field and integrate the next generation IP (IPng) [44]. The answer to this RFC is contained in RFC 2460, which contains the IPv6 technical specifications. These specifications provide for increased address space, a simplified header, improved support for extensions and options, flow labeling, and authentication and privacy capabilities (Deering and Hinden, 1998b) [45]. Although the address space is in fact limited, it can be reasonably assumed that the IPv6 address space pool will not near exhaustion like that of IPv4. This increase in address space supports the growth of future Internet technologies by allowing the networking of devices other than computers. For example, smart home appliances, such as sprinkler systems, can be turned on or off remotely via the Internet. Corporations are already beginning to develop home appliance controllers to perform these functions (NTT Communications, 2001) [46]. The increased address space is only one of several features. Geesey and Fullerton (2006) [47] explain that IPv6 is "an evolutionary step from the current Internet protocol IPv4". In fact, the IPv6 specification accounts for several features that are not available in IPv4. These features include (a) a simplified header, (b) improved routing, (c) enhanced mobility features, (d) easier configuration capabilities, (e) improved quality of service, and (f) integrated Internet protocol security (USGAO, 2005) [48]. All of these features make IPv6 more dynamic than IPv4 and allow for technology growth.
Header

At forty bytes, the IPv6 header is double the size of the IPv4 one. Despite the size, the header is actually much simpler than the IPv4 one. The number of fields in the IPv4 header was reduced in the IPv6 header without losing any functionality of IPv4. Instead, a second set of headers, known as extension headers, was introduced. The benefit of the second set of headers is that the fields are intended for the end network and not the intermediate network (Geesey and Fullerton, 2006) [47]. Thus, the fields can be ignored in the routing process simplifying the routing of the packet and increasing routing performance.

IPv6 Routing

In addition to the routing improvements seen as a result of the new header, other routing improvements were incorporated into IPv6. The protocol itself provides the possibility of a policy-based routing capability in which the application layer of the OSI model can designate required priority and service of originating packets based upon service level agreements established between a user and its Internet service provider (ISP) (Geesey and Fullerton, 2006).

Mobility Support

The IPv6 protocol also provides a capability to support mobile devices. This feature allows for a device to have one unique IP address that permanently belongs to it regardless of location. As the mobile devices moves from network to network a new IPv6 address is created by incorporating the devices unique IP address and the network’s designation number.

IPv6 Auto Configuration

Another larger feature contained in the protocol is the IPv6 auto configuration capability. Unlike IPv4, IPv6 allows for a stateless auto configuration capability in which end devices are capable of generating their own IP address based upon information that they are already receiving from the network. This is a true advantage in that manual configuration of devices and servers aiding in
configuration will no longer be required. In essence, a true plug-and-play capability exists with IPv6.

**Quality of Service**

One of the greatest challenges of transmitting near real-time voice and video over the Internet is that the transmission is a best effort and there are no guarantees as to the timing and arrival of the packets. IPv6’s quality of service (QoS) extension header provides a capability to address this problem. Voice and video type packets can be marked by the applications in order to identify how the network should handle the packet. Based upon this field, the network can be enabled to prioritize packets based upon this marking.

**IPv6 Security**

Finally, IPv6 provides for increased security of network traffic. In IPv4, virtual private networks (VPNs) provide a level of security by encrypting data sent over networks. On the contrary, IPv6’s security mechanism is built into the protocol by providing an authentication and encapsulation security payload (ESP) headers (Deering and Hinden, 1998b) [45]. The authentication header provides authentication of the origin of the packet while the ESP header protects the data as it is transported across networks. Together these headers essentially provide the same functionality of a VPN without the necessity to deploy and configure more network devices.

**Overcoming IPv4 Limitations**

Over the years, corporations have implemented a series of workarounds to overcome the most critical limitations of the IPv4 protocol address space and network security. These workarounds have proven to be successful in dealing with the shortfalls of IPv4 and are commonplace on most networks today (Garretson, 2005) [49].

**IPv4 Address Space Limitations**

The shortage of IPv4 addresses has by no means stopped or slowed the deployment of networks. Many corporations that have faced the address space barrier have solved the problem by implementing network address translation (NAT)
technology (USGAO, 2005) [48]. NAT works by assigning all the network devices a private non-routable IP address. These devices are located behind a NAT router, which has a public routable IP address space. All workstations behind the NAT router appear to have the same IP address as the NAT router. Thus, when data is sent across the Internet to a specific workstation, it is actually sent to the NAT router, which is responsible for determining which workstation to send the data to. By implementing address translation, corporations can essentially add as many devices as they would like without worrying about address space limitations. Although NAT is a suitable work around for the address space limitation, it significantly hinders efficient network management. The configuration of the network increases in that NAT must be deployed, configured, and maintained in addition to the other network components. In addition to adding complexity to the network configuration, NAT also adds complexity to network troubleshooting. One of the common difficulties that occur in the troubleshooting of networks running NAT is that it is difficult to perform end-to-end troubleshooting. Instead, each segment of the communications must be troubleshooted independently. An example of this troubleshooting difficulty occurs when two workstations, on different NAT enabled networks, are experiencing difficulties communicating. From each workstation’s perspective, it is communicating with the NAT router rather than the workstation. This results in a three-step troubleshooting scenario. First, the communications from the first workstation to the first NAT router are troubleshooted. Next, the communications from the first NAT router to the second NAT router are troubleshooted. Finally, troubleshooting commences from the second NAT router to the second workstation. If the networks were not running NAT, troubleshooting could occur across the network from workstation to workstation.

2.4. Mobile Internet Protocol Version 6.0

The Internet Protocol version 6 (IPv6) [4], developed by the Internet Engineering Task Force (IETF) IP Version 6 working group (IPv6) in 1998, itself does not provide a node the feasibility to stay reachable while roaming around in different IPv6 networks. Due to the lack of mobility support, packets intended to such a moving Mobile Node (MN) would never reach the mobile node while it is away from the home network. The mobile node could change its IP address each time it moves to a new point-of-attachment. However, in this case the mobile node
would not be able to maintain already established transport-layer connections. Mobile IPv6 (MIPv6) [13, 15], developed by the IETF Mobility for IPv6 working group [MIP6], is a protocol developed in 2004 as an extension of IPv6 [4] to support node mobility. Mobile IPv6 is an update of Mobile IP [12], which was designed for IPv4 node mobility, and adds roaming capabilities of mobile nodes into IPv6 networks. The major benefit of this standard is to keep alive any communication between a Correspondent Node (CN) and a mobile node while the mobile node moves from one to another IPv6 network and thus changing its point-of-attachment. This is feasible as the mobile node is always addressable via its Home Address (HoA), an IP address assigned to the mobile node within its home network. The mobile node is always reachable at its home address, independent from its current point-of-attachment in the IPv6 Internet. If the mobile node is at home, packets addressed to this home address are normally routed to the mobile node. While the mobile node is away from its home network and attached to a foreign network, it maintains at least one Care-of Address (CoA). The care-of address is an IP address with the subnet prefix of the foreign network and addresses the mobile node in the foreign network. This care-of address can for example be derived through IPv6 auto-configuration. While the mobile node is staying in the foreign network, packets addressed to the care-of address will be routed to the mobile node. Figure 2.1 depicts how Mobile IPv6 works. To be able to forward packets to the mobile node while it is not in the home network, a so called Binding between the mobile node's home address and the care-of address is created. While the mobile node is away from home, for example, if the mobile node moves to a foreign network (black line in Figure 2.1), a node on its home link is taking care of packets address to the mobile node's home address. This node is called Home Agent (HA). When the mobile node receives a new care-of address, it associates the care-of address with its home address by performing a binding registration with the home agent. This is done by sending a Binding Update (BU) message to the home agent. The home agent replies to the mobile node with a Binding Acknowledgement (BA) message, which finishes the binding registration. The home agent now intercepts packets addressed to the mobile node's home address and forwards them using an Internet Protocol Security (IPsec) [8] Encapsulation Security Protocol (ESP) [50] tunnel to the mobile node's care-of address [15]. The mobile node could also send a Binding Update to a potential correspondent node to update the correspondent nodes binding cache.
Therefore, it first has to complete the Return Routability Procedure. Goal of the return routability procedure is to ensure that the mobile node is addressable at its home address and its claimed care-of address. A correspondent node only accepts Binding Updates from the mobile node which successfully performs the return routability procedure to ensure that the data traffic is directed or received from the mobile node using the care-of address. Therefore, Mobile IPv6 performs tests whether packets addressed to the home address and care-of address are routed to the mobile node. The mobile node can pass the test only if it is able to supply proof that it received certain data (the 'keygen tokens') which the correspondent node sends to those addresses. These data are combined by the mobile node into a binding management key." [13] The message flow for the return routability procedure is also shown in Figure 2.1. The mobile node sends two messages: the Home Test Init (HoTI) and Care-of Test Init (CoTI) messages at the same time. The HoTI message is sent to the correspondent node via the home agent, whereas the CoTI message is sent directly, not via the home agent. The correspondent node responds to HoTI message with the Home Test (HoT) message, which is again sent via home agent. The Care-of Test (CoT) message is sent by the correspondent node in response to the CoTI message. This message is again sent directly to the mobile node. These four messages implement the return routability procedure. The procedure requires some processing at the involved nodes to calculate some tokens and cookies. More details are described in [13]. Nevertheless, the HoT and CoT messages can be returned quickly. After having successfully completed the return routability procedure, the mobile node is able to update its binding cache at the correspondent node.

Two communication modes between a mobile node and a correspondent node are possible. The first mode, the so called Bi-directional Tunneling, does not require the correspondent node to support Mobile IPv6. In this mode, packets from the correspondent node to the mobile node are routed to the home agent who tunnels them to the mobile node by performing IPv6 encapsulation [16]. Packets from the mobile node to the correspondent node are tunneled to the home agent, so called Reverse Tunnelled, and than routed to the correspondent node.
The lines in Figure 2.1 represent the packets being sent in this mode. The second mode, called Route Optimization, requires the correspondent node to support Mobile IPv6. Here, the mobile node registers its current binding also to the correspondent node, thus the correspondent node is able to address packets directly to the mobile node's care-of address. This direct communication between the mobile node and correspondent node allows using the shortest path and rapidly decreases the traffic at the home agent.

2.5. Internet Society Documents

Significant Resources

Although several sources of literature were reviewed for this report, certain works are significant in that they are continuously referenced throughout the majority of other literature reviewed.
Internet Society Documents

The Internet Society (ISOC) is comprised of several global organizations and members and provides guidance for the Internet’s future. It is the premier source for information about the Internet. All standards are documented in requests for change (RFCs).

I. IP Version 6 Addressing Architecture (Deering and Hinden, 1998a) [43]. This document, known as RFC 2373, defines the IPv6 addressing model. It explains, in great detail, the components of the 128-bit IPv6 address and how to reference the textual representation of the address. In addition it specifies how IPv4 addresses are encapsulated into an IPv6 address when the tunneling transition methodology is used.

II. Internet Protocol DARPA Internet Program Protocol Specification (University of Southern California, 1981) [41]. This document is formally known as RFC 791 and is the official specification of IPv4. It provides all the technical details of the IPv4 packet and the header field definitions.

III. Internet Protocol, Version 6 (IPv6) Specificafion (Deering and Hinden, 1998b) [45]. This document is often referred to as RFC 2460 and contains the formal specification of the IPv6 protocol. It provides all the technical details of an IPv6 packet. In addition, it defines all the fields of the IPv6 header as well as their possible values and meanings.

IV. Connection of IPv6 Domains via IPv4 Clouds (Carpenter and Moore, 2001) [51]. This document, known as RFC 3056, outlines the tunneling approach to the transition Methodology. It provides several network scenarios and guidance on how IPv6 packets can be tunneled across an IPv4 network. Carpenter and Moore (2001) make it clear that the approach is “intended as a start-up transition tool used during the period of co-existence of IPv4 and IPv6” (p. 1) and is no means a permanent solution.

V. DHCP: IPv4 and IPv6 Dual-Stack Issues (Chown, Venaas and Strauf, 2005) [52]. This document is considered work in progress in that it is an Internet draft waiting on formal approval as a RFC. It outlines issues with the dual stack transition approach and the use of the dynamic host configuration
protocol (DHCP), which is used to automatically configure a device for the protocol environment. It outlines the DHCP issues and provides their potential solutions.

**Government Document**

A United States Department of Defense (DOD) directive requiring that all government agencies are transitioned to IPv6 by 2008. Based upon this directive, several studies regarding the best approach for the DOD transition have been conducted.

I. Internet Protocol Version 6 – Federal Agencies Need to Plan for Transition and Manage Security Risks (USGao, 2005) [48]. This document is a congressional report outlining the necessity for government agencies to begin to plan for the transition to IPv6. It outlines all the steps required for a successful transition. It also outlines the potential for security risks to occur during transition and recommends planning to ensure that security is not compromised during the transition.

II. IPv6 Economic Assessment (National Institute of Standards and Technology [NIST], 2005) [53]. This report is based upon research conducted by RTI International for the United States Department of Commerce. It is intended to provide cost and benefit estimates for the transition to IPv6 over the next 25 years. It is only an estimate and the NIST (2005)[53] report makes note that it could be considered conservative since the results “do not reflect future, next generation applications that may be enabled by IPv6”.

III. GSA and IPv6 White Paper (Williams, 2004) [54]. This white paper addresses the need for IPv6 from the government’s standpoint. It outlines the benefits and costs associated with the transition. Furthermore, it suggests the need for the federal government to begin planning for the transition by developing transition plans and establishing policy requiring the modification of contracts to include IPv6 capabilities.

**Miscellaneous Documents**

I. Guide to Federal Agencies Transitioning to IPv6, IPv6 Best Practices World Report (Geesey, 2006) [42]. This guide was developed by Juniper networks
and is intended to provide the government of an overview of the best industry practices for transitioning to IPv6. It is based upon research of industry wide IPv6 transitioned approaches and is tailored specifically for the United States government.

II. Guide to Federal Agencies Transitioning to IPv6, IPv6 Capable – A Guide for Federal Agencies (Geesey and Fullerton, 2006) [47]. This guide is intended as a follow on to the IPv6 Best Practices World Report. It describes IPv6 in more detail and what it means to be IPv6 capable. Additionally, it describes the three primary transition mechanisms.

III. Final Report on IPv6 Deployment Issues (Information Society Technologies, 2005) [55]. This report outlines issues that need to be resolved before full deployment of IPv6 on the 6NET project. The 6NET project is an IPv6-only network connecting various research and educational networks. The report covers topics ranging from vendor support to network management on a dual stack network configuration.

2.1.6 Transition Methodologies

The transition to IPv6 is a complex process that affects all the components of a corporation’s information system. It is essential that the transition take place with the least amount of impact to the corporation’s operations. The three current popular transition approaches are (a) translation, (b) tunneling, and (c) dual stack configuration. All three approaches minimize the impact to a corporation’s information system by allowing IPv4 devices to communicate with IPv6 ones. This enables a corporation to transition its network over a course of time that can be controlled by its resources.

2.6.1 Translation

The translation methodology consists of translating IPv4 packets to IPv6 ones. This form of mapping provides the capability of preparing a packet from an IPv4 network for a destined IPv6 network. An example of this can be found in the situation when an IPv6 network communicates with an IPv4 network. The originating IPv6 packet must be converted to an IPv4 one as it arrives at the IPv4 network. Translation provides the mechanism for dissimilar networks to
communicate. This translation occurs in the hardware connecting the dissimilar networks.

**Transition Requirements**

In transitioning from IPv4 to IPv6, all corporations will choose one of the three approaches that best meets their business needs. To facilitate a smooth and successful transition; the corporation must understand all transition requirements and plan accordingly. Regardless of the chosen approach, the corporation must plan for hardware, software, and all associated costs.

**Hardware Requirements**

The first step in becoming IPv6 ready is insuring that all hardware supports IPv6. There are two primary types of hardware requirements that need to be addressed in transition planning – networking hardware and systems support hardware. It is important to note that regardless of the transition approach chosen, IPv6 and IPv4 equipment can co-exist on a network (Rubens, 2004). Furthermore, this co-existence may last decades as the NIST study estimates that the IPv6 transition will take approximately twenty-five years (NIST, 2005). If the need to transition is not eminent, a corporation can upgrade its network infrastructure according to its normal equipment life cycle management policies.

**Networking Hardware**

The main networking components required for transitioning consist of IPv6 capable switches and routers. The level of required equipment is dependent upon the transition approach selected. Regardless of the transition method chosen, the network must include IPv6 capable equipment. All three transitioning approaches require IPv6 capable equipment where IPv6 and IPv4 networks connect. In addition, the tunneling and translation approach may require more IPv6 capable equipment if the corporation’s strategic plan is to convert the corporate network to IPv6 and tunnel it across an IPv4 network. In order to convert the corporate network, all equipment on the network must support IPv6. Since the dual stack configuration operates with both protocols running simultaneously, equipment can be upgraded to IPv6 over time providing the corporation the flexibility in scheduling the transition over a few years. Currently, all major router manufacturers; Cisco, Juniper, Foundry
Networks, and Extreme Networks now support IPv6 with their new products (Marsan, 2003) [69]. Since these manufacturers have been supporting IPv6 for some (NIST, 2005), corporations will more than likely have already deployed a significant amount of network equipment that is IPv6 capable. In order to assess the amount of IPv6 equipment that a corporation possesses, it is important that corporations incorporate a one hundred percent inventory of all network equipment when planning for the IPv6 transition.

**Systems Support Hardware**

In addition to networking hardware, corporations must also account for systems support hardware when planning for transition. Systems support hardware consists of all equipment that supports the network. This equipment includes intrusion detection devices, firewalls, performance monitoring equipment, and servers used to support the network. In particular, the number of servers required to support a transition could be numerous. Servers provide several network management functions such as: DHCP configuration, domain name service (DNS), configuration management, and performance management. In the case of the IPv4 and IPv6 protocols co-existing on the same network, separate servers are required for different support systems. For example, in the case of a DHCP server two servers are required to run DHCP – one for IPv4 and one for IPv6 (Chown et al, 2005). It is estimated that IPv6 running alone on a network requires approximately ten percent more server resources (Rubens, 2006). Thus, in planning for transition, it is important that the corporation plan to upgrade their support systems to support the transition.

**Software Requirements**

In addition to understanding the hardware requirements for transition, IPv6 software requirements must be understood. The software requirements for transition can be categorized into two systems - operating systems, and business applications.

**Operating Systems**

The key to any networked device is its underlying operating system. In order for a device to be considered IPv6 capable the operating system must be IPv6 capable. The operating system is a key component in any IPv6 transition as the
transport, session, presentation, and application layers of the OSI model all rely upon it. Currently, there are several operating systems that support IPv6 as shown below.

**Operating Systems with IPv6 Support (Vulovic, 2005) [67]**

Operating System Version: - Windows XP (SP1 and higher) Microsoft Windows Windows 2003

Linux Kernel 2.2, BSD Open BSD 2.7, MacOS, MacOS X 10.2

Solaris Solaris 7 and higher, AIX AIX 4.3

HP-UX HP-UX 11i (TOUR2 upgrade)

Vendors are also beginning to enhance the IPv6 capabilities of the existing operating systems listed. For example, Microsoft recently released a beta version of Microsoft Vista (formerly known as Leghorn), the replacement for Windows 2003 Server, which has an integrated built-in suite of IPv6 capabilities that increases the IPv6 toolset found in Microsoft Windows 2003 (Kearns, 2006) [68].

**Business Applications**

The majority of corporations rely heavily on enterprise resource planning (ERP) and customer relationship management (CRM) software provided by vendors such as Oracle, PeopleSoft and SAP. These vendors have been slow to release software that is IPv6 capable (Marsan, 2003) [69]. It was not until recently that Oracle started incorporating IPv6 support in its 10g Application Server (Goel, 2005) [70]. As IPv6 networks emerge, the market for IPv6 enable business applications will increase and we should see an increased amount of IPv6 business applications being developed.

**Transition Costs**

Determining the costs to transition from an IPv4 network to one that is IPv6 capable is not an easy task. Garretson (2005) [49] explains that the reason “IPv6 upgrade costs are so hard to quantify is that, outside of government projects and test implementations at a handful of companies, few in this country use the 10-year-old protocol.” Information from a few of the test implementations is now available and
the results are contrary to the popular opinion that the IPv6 transition will be extremely expensive. Verio, a subsidiary of NTT Communications, deployed the first IPv6 commercial network in the United States and found that the deployment costs were not as extensive as previously thought (Marsan, 2003) [69]. Other research agrees with these findings. In 2005, RTI International researched the costs of transition for the National Institute of Standards and Technology’s IPv6 Economic Assessment report (NIST, 2005) [53]. This research estimates that IPv6 will cost the United States 25.4 billion dollars over the next twenty five years. This equates to approximately a 1 billion dollar per year expenditure on IPv6. RTI International’s research also estimates that for every dollar spent on IPv6, only 8 cents will be spent on infrastructure upgrades. The remaining 92 cents will be spent integrating IPv6 into existing business practices (Patterson, n.d.) [71]. Since the infrastructure needs to be in place before a corporation can take advantage of the protocol, the initial costs will be incurred upgrading networks to the new protocol.

Despite some of the limitations in quantifying the costs, an understanding of the transition requirements and the tasks involved provides guidance to corporations in developing a transition budget. The transition costs can easily be broken down into two distinct areas: technology and human factors (Williams, 2004) [54]. Technology costs consist of those costs associated with planning, deploying, and operating an IPv6 enabled network whereas the human factor costs are related to changing business practices based upon new technology.

**Planning Costs**

The initial planning for the transition is one of the largest technological tasks that a corporation will face. For a successful transition, corporations must determine how IPv6 will be used within the corporation. In terms of the transition, the greatest amount of labor resources will be consumed during the planning phase. These labor resources consist of developing a transition strategy, conducting a one hundred percent inventory of all information technology equipment, and training the information technology staff on IPv6 technologies.
Deploying Costs

The costs associated with deploying the network can be considered the most predictable transition costs. Based upon network inventories, the corporation can easily assess which hardware is currently IPv6 capable and which needs upgrading. Thus, the costs associated with deploying the network are restricted to new equipment and the labor costs required installing it.

Operating Costs

Corporations will find that their biggest expenditure is on operating the IPv6 network. These costs coincide with the 92 cent integration costs that were previously discussed. The operating costs consist of the upgrading and addition of network servers, deploying new security suites and the development of new performance management systems. Another cost that must be accounted for is the cost required to maintain a network in which both IPv4 and IPv6 coexist. It was previously mentioned that more systems support hardware would be required to maintain both networks. Thus, for every server required supporting IPv4 a similar server would be required for IPv6. These costs do not only include the hardware but also the increased staffing levels required to maintain both sets of equipment.

Human Factor Costs

The largest questionable costs are considered human factor costs. These unknown costs are those associated with changing the way a corporation does business based upon a new capability (Williams, 2004). Although, the costs are difficult to ascertain, it can be assumed that the costs will be greater with aggressive transition timelines.

2.6.2. Tunneling

The tunneling methodology consists of tunneling IPv4 packets over IPv6 networks and vice versa. In tunneling, an IPv4 packet is encapsulated into an IPv6 packet to be sent across an IPv6 network. An example of tunneling occurs when two networks have been transitioned to IPv6 but still rely on an IPv4 network to communicate. As the originating IPv6 packet arrives at the IPv4 network, it is encapsulated into IPv4 packets for communication over the IPv4 network. Once the
IPv4 packets arrive at the destined IPv6 network, the IPv4 headers are removed providing the original IPv6 packet. Similar to translation, tunneling occurs in the hardware connecting the dissimilar networks.

2.6.3. Dual Stack Configuration

The dual stack configuration occurs when a network has partially been transitioned to IPv6 and consists of both IPv4 only and IPv6 only devices. This hybrid type of network requires the capability to allow both protocols to exist simultaneously. To support the dual stack configuration, both protocols are enabled on the network routing devices allowing them to communicate with devices that are only running one type of protocol.

2.7. Network Address Translation

2.7.1 Definition

Network Address Translation (NAT) was initially designed in order to overcome the shortage of available IP addresses [56]. It operates by translating an address space used within an internal network into another address space used on the external public network. If a host on the internal network tries to communicate with a host on the public network, the NAT gateway translates the internal private-space address of this host to an address usable on the public network. On the internal network of a NAT gateway, usually private space IP addresses [57] are used. Originally, Network Address Translation (NAT) [2] were designed to overcome the shortage of IP address space in the Internet. NATs allow the translation of local IP addresses into one globally unique IP address. This is done by mapping a few real IP addresses which are required for Internet communication to the many local IP addresses, whereas the local IP address can be shared over the Internet. This process is called Network Address Translation or Network Masquerading. As traffic passes from the local network to the Internet, the source address in each packet on the y can be translated by a NAT device from the private addresses to the public address (es). When a reply returns to the NAT, it uses the connection tracking data it stored during the outbound phase to determine where on the internal network to forward the reply. The TCP or UDP client port numbers are used to demultiplex the packets if the NAT has only one public IP address. Both IP address and port numbers are
translated when multiple public addresses are available on packet return. To a system on the Internet, the NAT device itself appears to be the source or destination for this traffic. How the addresses and port numbers are converted is defined by the rules of the NAT. If the address and port are converted for a packet, the same conversion must be also done for all other packets of the same data stream. Subsequently, an entire subnet can be mapped into one IP address. Nodes can be addressed over the NAT only if the rules define an appropriate address conversion. The main disadvantage of network address translation is that it breaks the end-to-end connectivity and does not allow a true end-to-end connectivity which is required by some applications, e.g., real-time application like VoIP. Such applications require the use of for example a proxy to successfully traverse the NAT. However, this complicates and slows down the communication process, especially the communication initialization.

2.7.2. Task of NAT

A firewall that only uses a NAT component can fulfill the following tasks:

1. **Access control**: the NAT can verify the identity of the communication endpoints on the base of their port numbers and their IP addresses.

2. **Filtering and modification**: the NAT decides whether the data are forwarded or not and whether an address conversion for a certain communication connection is accomplished or not. A modification of the data is necessary before forwarding in order to change the used IP addresses and port numbers.

3. **Hiding**: the network structure is completely hidden by the NAT.

4. **Logging**: if data are dropped or modified by the NAT, this is noted accordingly.

RFC 2663 [58] lists the following characteristics which are common among most of the current NAT implementations:

1. **Transparent address assignment**

   NAT assigns IP addresses or port numbers temporarily to hosts on the internal network if they try to communicate with hosts on the external
network. Depending on the implementation, this assignment can be either static or dynamic.

2. Transparent routing through address translation

The NAT gateway connects the internal private network to the external public network. Therefore it is responsible for rewriting the IP addresses and port numbers in the IP packets. As modifications of the headers of an IP packet invalidate the old checksum of the packet, the gateway needs to recalculate the checksum.

3. ICMP error packet payload translation

Not only the actual TCP/UDP packets must be rewritten, but also ICMP packets must be inspected. The NAT gateway also needs to rewrite the payload of ICMP packets which contain a related IP packet.

2.7.3. Type of NAT’s and Mode of Operation

NAT devices can be divided into different classes. While all NAT devices solve the same problem, there are subtle differences in the heuristic which decide if a packet should be forwarded to the internal network. RFC 3489 [20] describes the following flavors which have been identified among UDP NAT implementations and The study on the STUN protocol [20], use terms such as Full Cone, Restricted Cone, Port Restricted Cone and Symmetric to describe the different types of NATs. These NATs are discussed with reference to UDP only.

Full Cone

Once a binding ((X, x), (Y, y)) has been created for an internal host (X, x), the same external address (Y, y) is also used if packets are sent to a different location than the one for which the binding was originally created. All external hosts can send a packet to (Y, y) which then gets forwarded to (X, x) even if (X, x) did not send any packet to the particular host first. A full cone NAT is also known as a one-to-one NAT. Once an internal IP address and port are mapped to some external IP address and port respectively, all the packets with the internal IP address and port will be translated to the fixed external IP address and port. Furthermore, any external
host can send a packet to the internal host by sending a packet to the mapped external address.

**Restricted Cone**

Basically, this is the same as Full Cone, but with an additional restriction: If an external host \((Z, z)\) wants to send a packet to the \((Y, y)\) mapping, the internal host \((X, x)\) must first have sent a packet to the IP address \(Z\). In the restricted cone NAT, all requests from an internal IP address and port are mapped to a fixed external IP address and port. It is similar to the full cone NAT except that unlike the full cone NAT, an external host \(s2\) (with IP address \(x\)) can send a packet to an internal host only if the internal host has previously sent a packet to the IP address \(x\) through the restricted cone NAT.

**Port Restricted Cone**

Together with the restriction introduced in the Restricted Cone variant, the packet, which the external host requires from the internal host prior to transmission, must also match the port number \(z\). This means, that \((X, x)\) needs to send a packet to \((Z, z)\) before \((Z, z)\) is able to use the \((Y, y)\) binding to contact \((X, x)\). The port restricted cone NAT is similar to the restricted cone NAT. However, the port restricted cone NAT also takes the port numbers into account along with the IP addresses. An external host can send a packet with source IP address \(x\) and source port \(p\) to an internal host only if the internal host has previously sent a packet to the IP address \(x\) and port \(p\).

**Symmetric**

A Symmetric NAT uses a binding \((Yn, yn)\) for each packet which is sent from a source \((X, x)\) to a destination \((Zn, Zn)\). This means that for each new external (IP, port) pair, a new mapping is created. Unlike the other classes, symmetric NATs usually pose a problem to NAT traversal techniques. If two hosts want to communicate with each other, but each one is behind a symmetric NAT, they have no possibility to find out the values used in the \((Yn, yn)\) tuple [12]. Therefore, they cannot directly communicate with each other, but need to use a third party relay. In a symmetric NAT, any request from an internal IP address and a port number to some destination IP address and port number is mapped to a unique external IP...
address and a unique port number. If the same host sends a packet from the same source address and the same port number but to a different destination, a different mapping is used. Only the external host that receives a packet from an internal host can send a UDP packet back to the internal host.

2.8. Related Works

Zao and Condell [81] discuss the use of IPSec over Mobile IP for HA-MN, HA-FA, CN-HA, CN-FA, and MN-CN connections (HA: home agent, FA: foreign agent, CN: correspondent node, MN: mobile node). IPSec is used to replace IP-IP-tunneling. Adaptations to Mobile IP messages are proposed for coping with IPSec tunnel establishment. Special IPSec tunnel extensions are added to advertisements and registration messages.

Binkley and Richardson [82] describe how a secure firewall protected area may tolerate Mobile IP or mobile systems using DHCP only and remain secure. They propose to use bi-directional IPSec tunnels between the home agent as a classic bastion host and the mobile node [83]. A secure mobile networking concept has been proposed that is based on ad-hoc networking and secure bi-directional IPSec tunnels. The standard Mobile IP scenario is treated as a special ad-hoc routing case where home agent and mobile node build a secure ad-hoc network. Considering the IP mobility problem as a special case of the general ad-hoc networking problem is a nice idea, but may be too complex for the goal to secure a Mobile IP environment only.

Gupta and Montenegro [84] describe enhancements enabling Mobile IP operation in a network, which is protected by a combination of source-filtering routers, sophisticated firewalls, and private address space. These enhancements should allow a mobile user in the public Internet to maintain a secure virtual presence within his firewall-protected office network. The authors propose to use SKIP [85] for key management, authentication and encryption. The reason why they chose SKIP instead of ISAKMP/Oakley [86], is SKIP’s ability to look up the sender’s public key based on alternate names, while this is done with source addresses in the case of ISAKMP/Oakley. The concept of a secured Mobile IP seems to be an easy and efficient way to solve Mobile IP security problems, but it requires introducing new protocols.
Pahlke et al. [87] propose the deployment of special gateways that include any security (e.g., firewall) and foreign agent functionality in the same node. IPSec tunnels are established among those nodes in order to achieve security. The approach allows leaving mobile nodes unchanged but requires the presence of those nodes in any visited network. In addition, securing a wireless link requires link-level mechanisms leading to possibly duplication of encryption.

Supporting dual stack mobility by addressing IPv4 and IPv6 mobility separately could result in an inefficient mobility management as explained in [59]. For example, operating both Mobile IPv4 [12] and Mobile IPv6 [13] on a single node would require that both IPv6 and IPv4 are operated in each of the visited network while the Mobile Node (being a host or a router) is moving in the Internet. For example, a node connecting to an IPv6-only network would not be able to operate Mobile IPv4 anymore, thus disrupting all of its IPv4 applications. Furthermore, managing two different protocols creates operational overhead both on the Mobile Node (MN) and the network as it mandates to operate the necessary software and infrastructure on the MN and at the operator level.

A first solution [88] combines IPv6-in-IPv4 tunneling with NAT-PT [28] to manage handovers of a MN operating Mobile IPv6 in IPv4-only networks. Tunnelling provides IPv6 connectivity to the node in the IPv4 network, while NAT-PT takes care of translating the IPv6 packets into IPv4 (and conversely) when the node communicates with an IPv4-only correspondent. One major operational overhead of this proposal is that all tunneled packets are extracted to be translated by a NAT-PT device that must be located on the path between the communicating peers. Furthermore, this solution addresses IPv6 mobility in IPv4 networks, but not IPv4 mobility at all. How to handle NAT in the visited IPv4 networks is also not considered.

Another proposal [89] defines a small extension to Mobile IPv4 that enables the registration of an IPv6 address to the HA while the MN is in an IPv4 network. IPv6 packets originated from or destined to the MN are encapsulated in an IPv4 header between the MN and it’s HA. This solution is only designed to provide IPv6 connectivity in IPv4 networks at the cost of an extra IP encapsulation, and does not address the possibility to roam in pure IPv6 networks. This work served as a base to define Dual Stack Mobile IPv4 (DSMIPv4 [90]) which also allows a node to
use IPv4 and IPv6 HoAs. However, this solution relies on the Mobile IPv4 signaling, thus preventing the node from roaming in IPv6-only networks.

The work presented in [91] explains how Mobile IPv6 and Mobile IPv4 can be operated at the same time to achieve seamless IPv6 handovers in IPv4 networks. When roaming in IPv4 networks, the Mobile IPv4 HoA is translated to a 6to4 address used as a CoA to register to the HA. All the IPv6 traffic originated from or destined to the MN then transits through the tunnel operated by Mobile IPv4. This solution results in a large header overhead due to the three encapsulations needed to transport the IPv6 packets from the node to the Mobile IPv6 HA. Furthermore, this solution does not consider the continuity of the IPv4 service when roaming in IPv6 networks.

None of the solutions described so far considers the continuity of both IPv6 and IPv4 sessions whatever the IP version in the network where the MN roams in is operated. The Mobile IPv6 support for dual stack Hosts and Routers specification (DSMIPv6 [3]) presented in the next section is currently discussed at the IETF as a single protocol that ensures a very flexible management of both IPv4 and IPv6 mobility in either IPv4-only or IPv6-only or dual stack networks.