IPv6 is More Than Addresses

John W. McClain

ICTN 6885

Spring 2014

Abstract

Version 6 of the internet protocol (IPv6) is the designated successor for internet protocol version 4 (IPv4). The need for this new protocol version was driven by the depletion of IPv4 addresses. At this time there are no more IPv4 addresses available. The explosive growth of internet activity and mobile devices like smartphones created the perfect conditions to deplete the available IPv4 addresses. So, anyone designing a network must consider IPv6 during the discussion phase of the project. The explosive growth of internet activity and mobile devices created security issues for users and providers of computing services. The purpose of this paper is to discuss the reasons why IPv6's security features are just as important as more addresses. This paper will go through a three phased approach to discussing IPv6 security. The first section of this paper will go through the planning process for implementing IPv6 on a network. It should be noted that most devices have IPv6 capabilities built into the devices now. The latest Windows systems have IPv6 capabilities. The second section of this paper will discuss the differences between IPv4 and IPv6. At some point during an upgrade IPv4 and IPv6 will need to exist together so knowing the differences is important. The last section of the paper will look at ways to exploit IPv6's vulnerabilities. The hackers aren't going let better security features stop their assault plans. Overall, IPv6 is more than additional addresses, the security features are extremely important.

The advances of information technology are actually making an internet of things possible. The term internet of things is based upon the ability to connect various devices using information technology. In Japan one of the main drivers for more internet protocol addresses is the desire to have more devices that are managed using internet protocol addresses. All of these devices need a designation for communication and access to other devices in order to communicate. The best way to locate and communicate these devices is using an internet protocol address. These numbers are similar to a person's home address. This individual home identifier allows the movement of mail to the right location. Internet protocol address performs the same function for technology devices. Recently most of these addresses were internet protocol version 4 addresses but the huge expansion of internet activity depleted the available ipv4 addresses. In order to addresses this issue the internet protocol version 6 was invented to alleviate this problem. IPv6 has enough addresses to account for any addresses needs for now and in the future. The address problem is solved but the security side of thing is a major problem. IPv4 wasn't designed with security in mind. This can't be considered a failure on the designers of this protocol. No one could have forecasted the explosive growth in devices and gadgets that have made the lives of a lot of people better and increased the level of communication and the speed of communication (Hogg, 2013)[12]. When IPv4 was started the need was communication in an office environment with a defined network perimeter and remote access was using a slow modem connection for dialup. Now, 6 out of 10 employees use personal devices at work (ISACA)[16]. According to some sources there will be 24 billion connected devices by 2020 (ISACA)[16]. A great example of what's happening is a typical home network. In a home network today, an array of devices using wired and wireless connections. These devices include in some cases servers, personal computers, wireless modems, routers and various devices for play like XBOX with all of them having a unique address for setup. This connectivity is typically used for the local exchange of information between devices with the home network for the exchange of documents between two or more computers. Another area of importance is for the exchange of information between devices and the internet. The data exchange is where a protocol like IPv6 could be used to help protect the data that's in transit. IPv6 is a major enabler for the deployment of internet protocol services for wireless phones. Operating systems like Windows 7, Vista, Linux, Mac OS support IPv6 (Horley, 2014)[13]. Japan directed that IPv6 capability be part of the technology deployments in 2005. China, France and Korea are deploying IPv6 networks. The US government mandated that all government agencies support IPv6 by 2008 (Internet Society)[2]. IPv6 is clearly part of the landscape and growing. The IPv6 website put the following information regarding IPv6 on its website (World IPv6 Launch)[1].

- Google reports the number of visitor to its sites using IPv6 has more than doubled in the past year.
- The number of networks that have deployed IPv6 continues to grow with significant IPv6 traffic worldwide.
- Austrailian ISP Internode reports that 10 percent of its customers now use IPv6 to access the internet.
- Akami reports that it is currently delivering approximately 10 billion requests per day over IPv6, which represents a 250 percent growth rate since June of last year.

Obviously, IPv6 is fully operational in a lot of locations. The upgrade to IPv6 requires some planning for users that decide to deploy this new protocol or in some cases like the U.S. government agencies face a mandated call to upgrade to this protocol (Marsan, 2012)[19]. The reason mandates like the one mentioned previously is most entities aren't looking to change something if it's not broken. These headaches and issues related to upgrades are conducive to slow changes. The next section of this paper looks at the planning required to get an IPv6 network installed.

The huge number of potential addresses available for IPv6 drives a lot of the discussion for going forward with an IPv6 install or upgrade of an information technology network.   The discussion concerning an upgrade to IPv6 must include making a business case and analysis for IPv6. The business case is designed to make sure the upgrade is occurring for the right reasons (Robertson, 2004)[25].   Making the business case will prevent vague reasons for the upgrade and potentially keep the cost low. As a project driver this will allow you justify the effort in time and costs for conducting the upgrade. In order to be effective the business case should address the following areas (Svendblad, 2013)[28]:

- The investment's goals
- The amount of time and money required to make the investment work
- The expected benefits or desired benefits from the project
- The scope of the project
- The stakeholders who are the source of the requirements
- The conversion/rollout plan for the project
- Project risk analysis

Once the business case is documented it's important to analyze the business case. This process is going to take time but it's important for the stakeholders involved to look at this document. The upgrade is mainly a technical process. But, this creates a bit of problem because technically it can be done but the cost and time required must be within guidelines. The guidelines are the business case followed by an analysis of the case to see if something is missed. Even with mandates like the one required of United States government agencies to implement IPv6 the planning process must occur. It’s important because cost overruns and security breaches are extremely good for newspapers. The following list contains some of the areas that should be looked at during the business case analysis (Robertson, 2004)[25]:

- Look over the business case to see if it’s complete. Also, the appropriate management team will need to sign off on the document.
- Make sure the financial and planning forecasts are included for the project.
- A project leader needs to be identified for the project. This person’s job is to make the project run smoothly.
- Make sure a communication plan is in place so that progress and problems are clearly communicated in a timely manner.
- Determine if action plans are available for remedial action and cost overruns.
- Make sure the teams working on the project understand IPv6 technology. If necessary, find a vendor that understands some of the issues that can occur when deploying IPv6 technology. Also, training needs to be available so that more than a couple of technical specialists understand IPv6.
- Have the plan available for review prior to starting the upgrade to IPv6.

Cost considerations for the project will need some detail because the cost of hardware and technicians will consume a lot of money but other costs will need to be detailed.

The following list is some of the cost’s that need to be considered (Svendblad, IPv6 Cost Considerations)[29]:

- IPv6 address space best practices and training: You'll want to quickly secure a block of IPv6 address space for your enterprise. Given the larger number of host IP addresses available for IPv6, IP address space design best practices have shifted from preserving IP address spaces to optimizing IP address aggregation. IP aggregation is also known as supernetting, and is used as a means to optimize router performance. You will need to re-train your staff to understand how to aggregate your network and avoid common IPv6 security pitfalls.

- Network hardware and software costs: Not all network equipment is IPv6 ready, and some routers that do support IPv6 do so using general purpose processors instead of dedicated hardware (like ASICs or network processors); this means that these routers process IPv6 packets with slower forwarding rates, resulting in reduced network performance.
- Enterprise system management tools: Most organizations with large heterogeneous environments have a complex patchwork of both commercial off-the-shelf (COTS) and custom or homegrown network and system management tools. You'll need to inventory these tools, validate their IPv6 compliance and remediate or upgrade them.
- SIP-based applications: Most applications don't care about the IP protocol of the underlying network. But some do, such as real-time services using the Session Initiation Protocol (SIP). SIP's creators made a crucial error by including IP address information within SIP message headers. Vendors and developers of SIP-based applications must reconfigure their apps to support IPv6 information in the SIP header. You'll need to make sure any of your SIP-based applications are ready for IPv6.
- Provider services: Support for IPv6 is still not comprehensive, especially for services such as MPLS and residential Internet. Many residential routers don't yet include IPv6 support. Some top Internet service providers -- including Verizon, Comcast, NTT and

Hurricane Electric -- are already well into their v6 deployments. Most carriers are adopting a dual-stack architecture; carrying both IPv4 and IPv6 while using "Carrier-Grade NAT" as a v4 to v6 gateway. But carrier grade NAT can introduce additional transit delay in the carrier's network. And many Internet architects worry that carrier grade NAT breaks the end-to-end Internet model; meaning that carriers can restrict unwanted services by not allowing them to transverse their NATs. Regardless, just make sure you know what each of your providers can support when it comes to IPv6.

- Non-traditional IP devices: IP networks today consist of a lot more than routers, switches and PCs. Security and building management systems, sensors and M2M devices all will require that you analyze them for their ability to support IPv6. It's important that you plot either an upgrade or gateway strategy to ensure that legacy applications and devices can co-exist in a mixed IPv4/v6 network.

Once the cost of going to IPv6 is established, the benefits of going to IPv6 are put on the table. The following list is some of the benefits of going to IPv6 (Svendblad, IPv6 benefits: Making the IPv6 business case, 2013)[28]:

- Mobility and collaboration: The explosion of IP enabled mobile devices over the past few years is often cited when discussing the need for more addresses. But for most enterprises these mobile devices can use private IPv4 addresses and leverage network address translation (NAT) ortunneling to gain access to services. However, a growing number of applications like peer-to-peervideoconferencing assume and can benefit from a globally unique, directly reachable IP address, which is made possible by IPv6.
- M2M communications: Like mobile devices, non-traditional IP devices are consuming an increasing number of IP addresses. Forty-four percent of enterprises expect these devices

to continue to grow within them. In some cases these devices need to communicate peer-to-peer with other devices or systems (e.g., smart grids or sensor networks).

- Network simplicity: While many can and will get away with using NAT for their IPv4 networks for many years to come, the growth of mobile and non-traditional IP devices, along with growth in peer-to-peer applications, will make these NATd networks increasingly complex and less secure and will result in increased operational costs and decreased business agility.

One way to maximize the benefits going to forward with IPv6 is making sure a test plan is in place. For example, when new software is being designed, one of the first actions is to define a testing plan to make sure the software meets the needs and is designed to specifications (Conklin & Shoemaker, 2014)[6]. This can be a four step process for simplicity sake. The first action is to define the high level requirements. The second action is to design the algorithms. The third step is to start software development. The fourth step is to conduct active and passive testing. This last phase of testing is designed to make sure the functions specifications defined are actually working and executing code in a proper manner. On the other hand, internet protocol network deployment is tested to the level that software is tested. In order to make sure proper planning is occurring, a number of planning considerations like the following should be considered (Five steps for overcoming IPv6 planning pitfalls, 2011)[8]:

- IPv6 planning pitfall #1: Hardware or software?
- Most routers and switches have IPv6 support, but how these network devices forward IPv6 packets varies. High-capacity core routers typically process packets in dedicated hardware (i.e., ASICs or network processors) to speed IPv4 forwarding. But hardware

architectures often don’t support IPv6; this means routers process IPv6 packets in general purpose processors, with the result being slower forwarding rates and lower capacity.

- IPv6 planning pitfall #2: Applications
- Most applications don’t care about the Internet Protocol (IP) of the underlying network. But some do, such as real-time services using the Session Initiation Protocol (SIP). SIP’s creators made a crucial error by including IP address information within SIP message headers. Vendors and developers of SIP-based applications must reconfigure their apps to support IPv6 information in the SIP header.
- IPv6 planning pitfall #3: Carriers
- Support for IPv6 is still very limited, especially for services such as MPLS and residential Internet. For example, Verizon’s FiOS lacks IPv6 support, so home/teleworkers on FiOS can’t access v6 services without some form of tunneling. Many residential routers don’t yet include IPv6 support. Meanwhile, other providers including Comcast, NTT and Hurricane Electric are already well into their IPv6 deployments. Most carriers are adopting a dual-stack architecture; they are carrying both IPv4 and IPv6 while using carrier grade NAT as a v4 to v6 gateway. But carrier grade NAT can introduce additional transit delay in the carrier’s network. And many Internet architects worry that carrier grade NAT breaks the end-to-end Internet model; this means that carriers can restrict unwanted services by not allowing them to transverse their NATs. Regardless, carrier grade NAT is perhaps the only currently viable solution to overcome not only the need for IPv4 to IPv6 interworking, but also the need to minimize IPv4 and IPv6 route propagation to reduce carrier border router
- IPv6 planning pitfall #4: Multihoming and private addressing

- Multihoming is standard practice for most enterprises, but the IPv6 addressing scheme was designed as a hierarchy to summarize routes into aggregates to simplify route lookup tables. IPv6 designers didn't anticipate the need for private IP addressing or multihoming, but enterprises demand both for security and resiliency. Creating a multihoming or v6 NAT strategy requires close coordination with your service providers and possibly obtaining your own IPv6 address space.
- IPv6 planning pitfall #5: Everything else
- Once you've solved the first four planning pitfalls, the last one may be the biggest. IP networks today consist of a lot more than routers, switches and PCs. Wide area network (WAN) optimizationand management platforms, provisioning and change management applications, sensors and M2M devices, and management tools all require analysis from IT shops. IT engineers must analyze them for their ability to support IPv6, and plot either an upgrade or gateway strategy to ensure that legacy applications and devices can coexist in a mixed IPv4-IPv6 network.

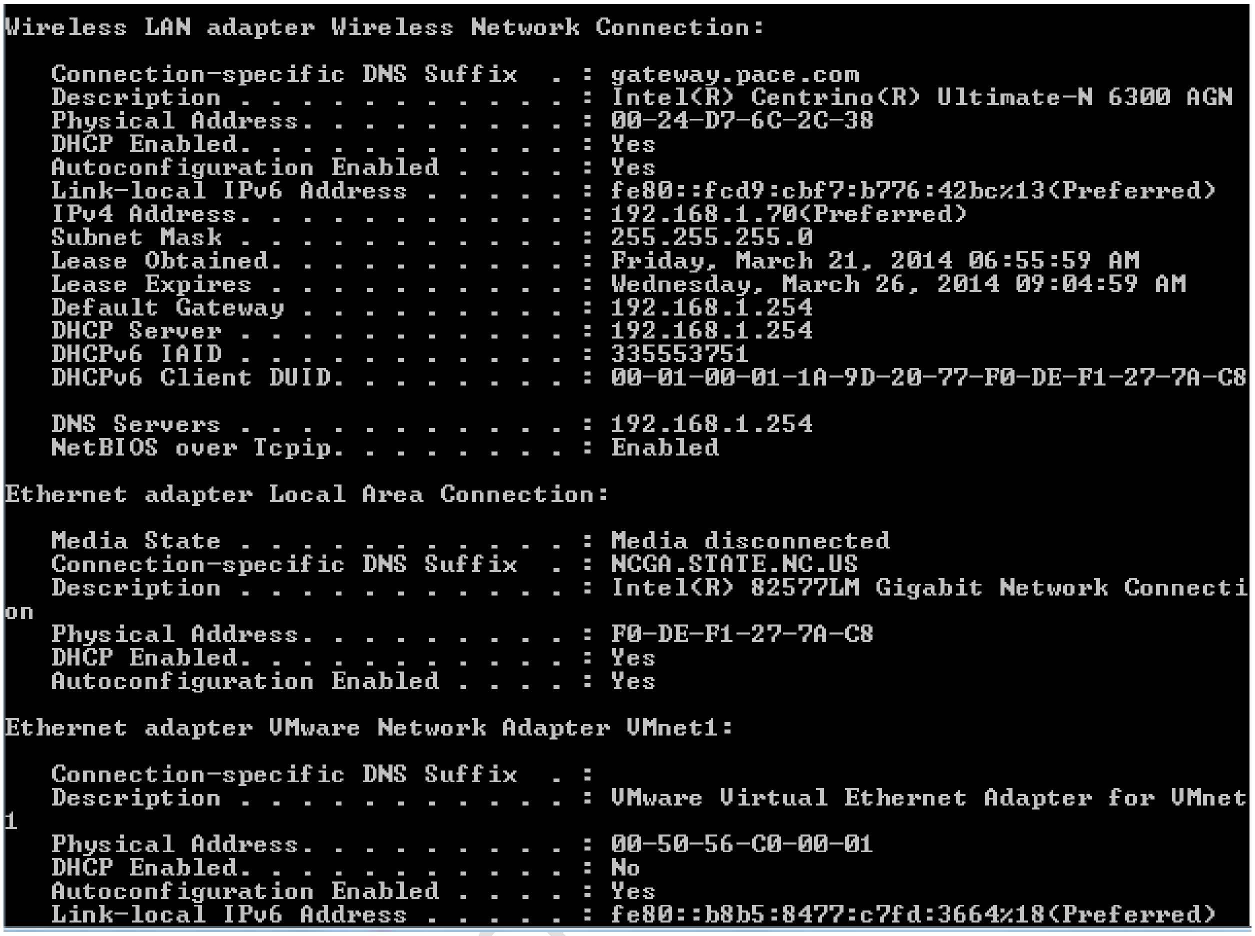
A detailed look at planning issues and potential pains are designed to create the best conditions for making the plan work and discover potential areas that might cause a failure. Because IPv6 gets a lot of press as a great security tool some of the expectation must be tempered with the reality of today's hyper connected world. A failure to properly plan for this upgrade will have the following impact and risk to the long term health of any entity making the transition (ISACA, IPv6 Security Audit/Assurance Program, 2012)[17]:

- Disclosure of privileged information
- Loss of physical assets
- Loss of intellectual property or other digital assets

- Loss of competitive advantage
- Loss of customer confidence
- Violation of regulatory requirements
- Infection of computer systems with viruses and other malware, which disrupt processing and require costly disinfection
- Use of the network as a launching pad for malicious activity against other enterprises (and the potential to be held liable for their damages)
- Inability to meet contractual service level agreements (SLAs) with third parties, resulting in legal liability

These risk areas need to be in the back of everyone's mind that working on the project.

The next section of the paper will compare IPv4 and IPv6. This is one of those planning areas that addresses the fact that unless the implementation is new. The vast majority of any upgrades will occur with both protocols operating on the network. As mentioned earlier in the paper, the major hardware and software vendors support IPv6. The following screenshot is from a Lenovo laptop connected to a home network. The ipconfig /all command ran from a command prompt presented the following results:



```
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : gateway.pace.com
   Description . . . . . . . . . . . : Intel(R) Centrino(R) Ultimate-N 6300 AGN
   Physical Address. . . . . . . . . : 00-24-D7-6C-2C-38
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::fcd9:cbf7:b776:42bc%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.70(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, March 21, 2014 06:55:59 AM
   Lease Expires . . . . . . . . . . : Wednesday, March 26, 2014 09:04:59 AM
   Default Gateway . . . . . . . . . : 192.168.1.254
   DHCP Server . . . . . . . . . . . : 192.168.1.254
   DHCPv6 IAID . . . . . . . . . . . : 335553751
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1A-9D-20-77-F0-DE-F1-27-7A-C8

   DNS Servers . . . . . . . . . . . : 192.168.1.254
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : NCGA.STATE.NC.US
   Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connecti
on
   Physical Address. . . . . . . . . : F0-DE-F1-27-7A-C8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet
1
   Physical Address. . . . . . . . . : 00-50-56-C0-00-01
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::b8b5:8477:c7fd:3664%18(Preferred)
```

The operating system on this device is windows 7, one of the previously mentioned systems that have support for IPv6. This is one of those simple things that are overlooked because this protocol is working and could be a potential attack avenue.   Another example of something simple that could create problems area that could create problems on an IPv6 network is the universal naming convention. UNC names identify network resources using a specific notation. UNC names consist of three parts - a server name, a share name, and an optional file path. These three elements are combined using backslashes as follows (Posey, 2010)[24]:

\\server\share\file_path

This creates in issue for IPv6 addresses because if Windows sees a colon, the operating system assumes you’re trying to reference a drive letter. Microsoft established a special domain to get around this issue. If an IPv6 address is used for a UNC path then colons need to be replaced with dashes and append Ipv6.literal.net to the end of the address. This address 2001:0db8:85a3:08d3:1319:8a2e:0370:7348 would be written as 2001-db8-85a3-8d3-1319-8a2e-370-7348.ipv6-literal.net (Posey, 2010)[24].   Another area that will require a bit more attention is access control list. The biggest difference between IPv4 and IPv6 is the addressing scheme which in IPv6 is hexadecimal. The IPv6 access list is comparable to the extended named ACL in IPv4 (Graziani, 2012)[11]. IPv4 uses standard and extended ACL's. IPv6 doesn't have numbered ACL's this protocol uses name ACL's. I Access control lists do the following (Monaco, Living with Access Lists, 2008)[21]:

- Provide and audit trail for your security organization.
- Enhance the security and availability of your network by reducing or eliminating mistakes.

Here's an example of a IPv6 access list that denies FTP access (Graziani, 2012)[11].

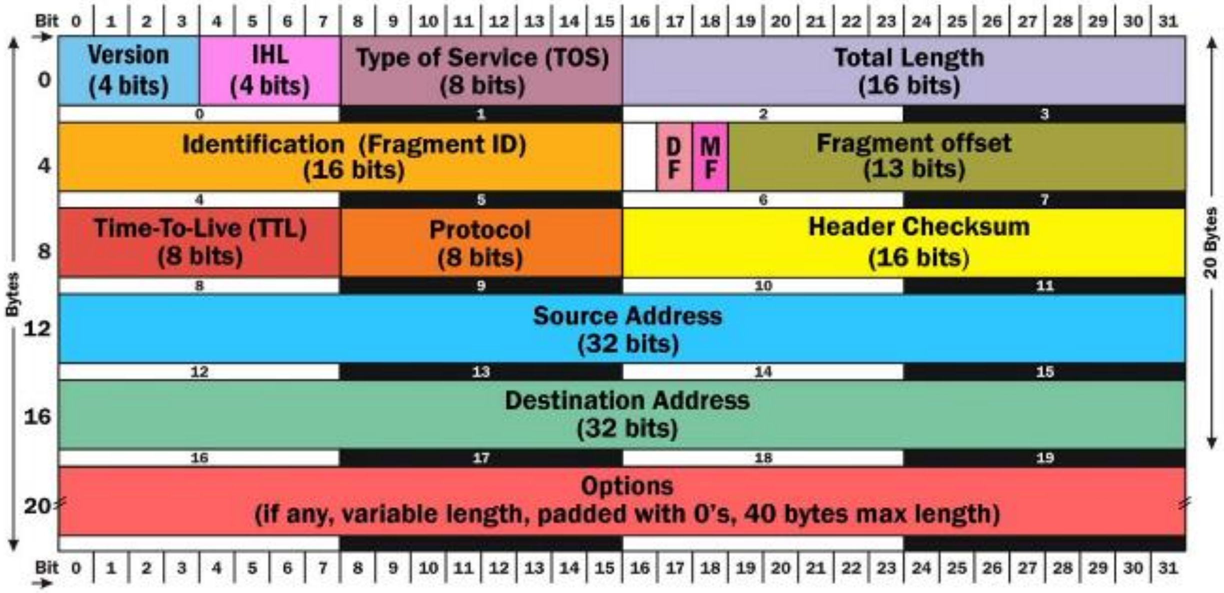
```
ipv6 access-list acl_out deny tcp any host 3001:1::203:A0FF:FED6:162D eq
ftp.
```

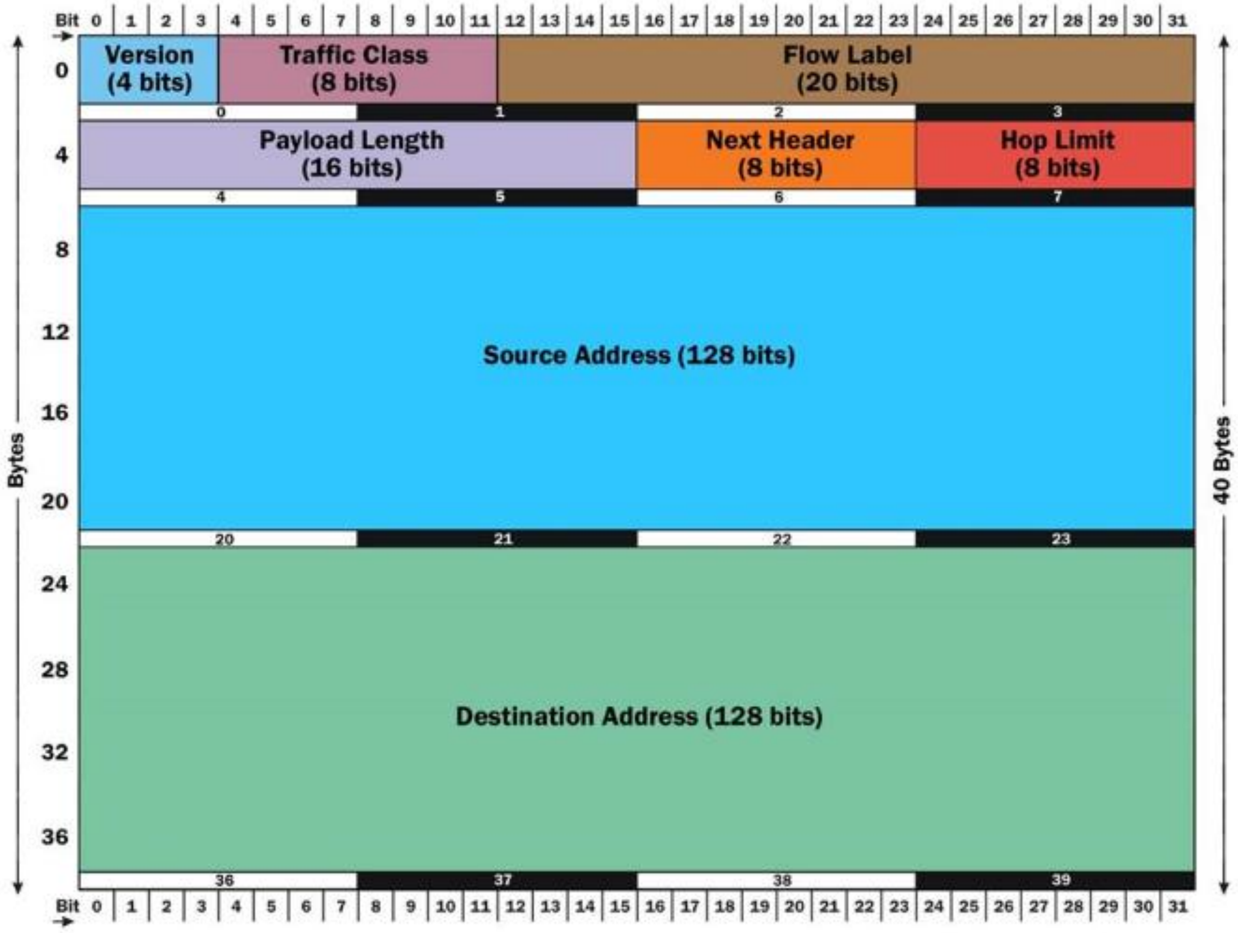
The previously mentioned areas of access control list and UNC pathing aren't the only areas that crop up when making the transition but they are simple everyday activities that could be problematic. When first looking at IPv4 compared to IPv6 the visual differences stand. IPv6 is built around six major areas (Graziani, 2012)[11]:

- Larger addressing space (128 bits)
- Stateless Automatic configuration
- Simplified Packet Routing
- Simplified Header

- Improved Security features (IPSec Support)
- Real-time support and media services

The following figures show the IPv4 and IPv6 headers (IPv4 and IPv6 headers)[14].


Bit 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Bytes
0
Version (4 bits)
IHL (4 bits)
Type of Service (TOS) (8 bits)
Total Length (16 bits)
0 1 2 3
4
Identification (Fragment ID) (16 bits)
D F
M F
Fragment offset (13 bits)
4 5 6 7
8
Time-To-Live (TTL) (8 bits)
Protocol (8 bits)
Header Checksum (16 bits)
8 9 10 11
12
Source Address (32 bits)
12 13 14 15
16
Destination Address (32 bits)
16 17 18 19
20
Options (if any, variable length, padded with 0's, 40 bytes max length)
20 Bytes



There are four main differences between the IPv6 and IPv4 headers (Horley, 2014)[13].

- The length of the header has been changed from 20 to 40 bytes.
- IPv4 has 4 bytes for addresses (32 bits) but IPv6 has 16 bytes (128 bits).
- The fields in the header has been reduced from 12 (IPv4) to 8 (IPv6).
- There is no options field in IPv6 header however it uses extensions headers that support greater functionality.

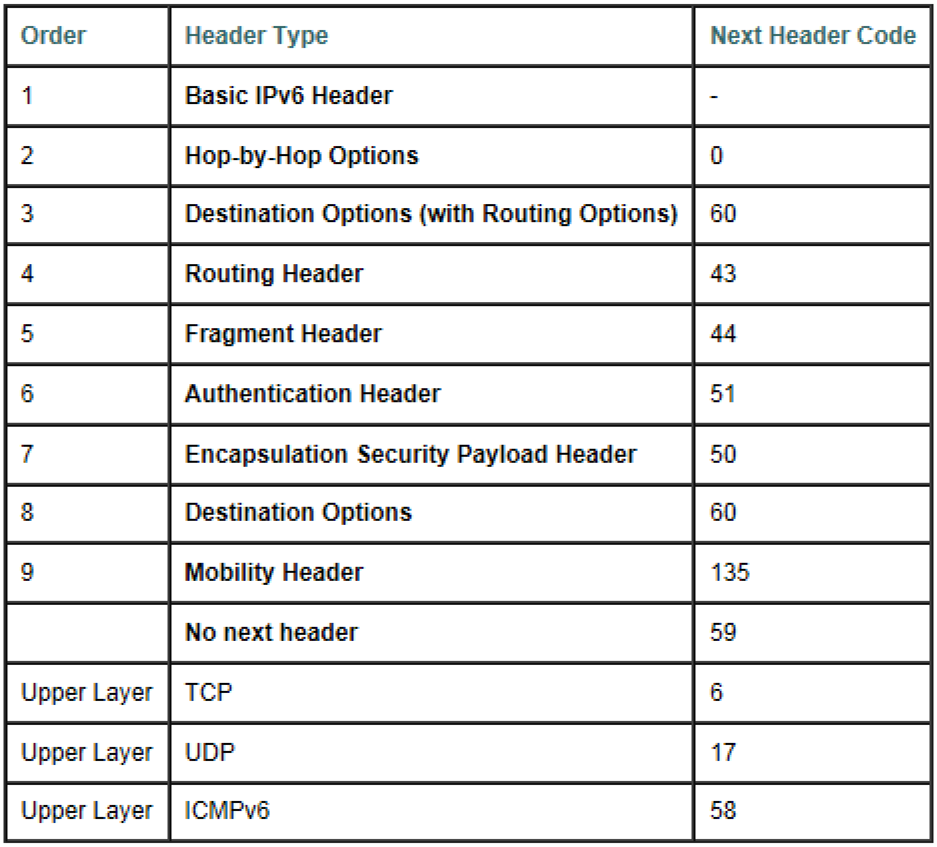
The changes from IPv4 Packet Header to IPv6 Packet Header are as follows (Graziani, 2012)[11]:

- IPv4 Version field - same size (4 bits), same name, same function, in IPv6 Packet Header.

- IPv4 IHL (Internet Header Length) field - discarded since IPv6 Packet Header is fixed length (40 bytes).
- IPv4 Type of Service field - same size (8 bits), new name (Traffic Class), same function in IPv6 Packet Header.
- IPv4 Total Length field - same size (16 bits), new name (Payload Length), now does not include length of the Packet Header, so new Payload Length = old Total Length - 40.
- IPv4 Identification (Fragment ID) field - twice as big (32 bits), same name, same function, moved to Fragmentation Extension Header.
- IPv4 DF flag - discarded, effectively always 1 (set) in IPv6.
- IPv4 MF flag -same size (1 bit), same name, same function, moved to Fragmentation Extension Header.
- IPv4 Fragment Offset field - same size (13 bits), same name, same function, moved to Fragmentation Extension Header.
- IPv4 Time-To-Live (TTL) field - same size (8 bits), new name (Hop Limit), same function in IPv6 Packet Header.
- IPv4 Protocol field - same size (8 bits), new name (Next Header), same function, in IPv6 Packet Header. There is a new set of possible values (some are the same as in the Protocol field in the IPv4 Packet Header, such as values for TCP, UDP and SCTP).
- IPv4 Header Checksum field - discarded, considered to be superfluous.
- IPv4 Source Address field - new size (128 bits instead of 32), same name, same function, in IPv6 Packet Header.
- IPv4 Destination Address field - new size (128 bits instead of 32), same name, same function, in IPv6 Packet Header.

- IPv4 Options field - discarded (virtually never used in IPv4 Packet Header) - now Packet Header is fixed length (40 bytes) instead of 20 bytes + length of options field.

The following figures show the extension headers and their recommend order in a packet (Cisco, 2012)[5]:



Order	Header Type	Next Header Code
1	Basic IPv6 Header	-
2	Hop-by-Hop Options	0
3	Destination Options (with Routing Options)	60
4	Routing Header	43
5	Fragment Header	44
6	Authentication Header	51
7	Encapsulation Security Payload Header	50
8	Destination Options	60
9	Mobility Header	135
	No next header	59
Upper Layer	TCP	6
Upper Layer	UDP	17
Upper Layer	ICMPv6	58

The options field in IPv4 performed an important role in internet protocol operations. Because of this role, the feature was keep when IPv6 was developed. In IPv6 the options field is a series of extension headers. The extension headers don't have size restrictions. This feature allows the extension headers to contract or expand depending upon need. According to information on the IPv6.com website the header structure for IPv6 make moving packets easier due to less fragmentation and processing at the intermediate router level. The following list shows the headers and functions associated with the headers (Graziani, 2012) (Cisco, 2012) (Wu, Cui, Wu, Liu, & Metz, 2013)[11,5,30]:

- Hop-by-Hop EH is used for the support of Jumbo-grams or, with the Router Alert option, it is an integral part in the operation of MLD. Router Alert [3] is an integral part in the operations of IPv6 Multicast through Multicast Listener Discovery (MLD) and RSVP for IPv6.
- Destination EH is used in IPv6 Mobility as well as support of certain applications.
- Routing EH is used in IPv6 Mobility and in Source Routing. It may be necessary to disable "IPv6 source routing" on routers to protect against DDoS.
- Fragmentation EH is critical in support of communication using fragmented packets (in IPv6, the traffic source must do fragmentation-routers do not perform fragmentation of the packets they forward)
- Mobility EH is used in support of Mobile IPv6 service
- Authentication EH is similar in format and use to the IPv4 authentication header defined in RFC2402.
- Encapsulating Security Payload EH is similar in format and use to the IPv4 ESP header defined in RFC2406. All information following the Encapsulating Security Header (ESH) is encrypted and for that reason, it is inaccessible to intermediary network devices. The ESH can be followed by an additional Destination Options EH and the upper layer datagram.
- Destination Option EH is used when the source passes the information to the intended destination only. The routers in between are not permitted to access the information.

Understanding the differences between the packet structures of IPv6 and IPv4 is fairly simple. Unless, a simple way of transitioning networks from IPv4 to IPv6 is invented communication will need to occur within networks and outside of the network perimeter. API's that are designed for IPv4 will not work the same way for IPv6 applications. QoS, security and other features that are native to IPv6 aren't native to IPv4 (Miller & Convery, 2004)[7]. So, modifications need to be accounted for and modified when working with IPv6 devices. The API changes will mean more than modifications to a graphical user interface. Security monitoring devices like firewalls, IDS and IPS will need to analyze IPv6 traffic. IDS/IPS devices for the most part use a library of signatures to prevent attacks but a lot of these signatures are designed for IPv4 packets. There are newer device types that use heuristic algorithms but these devices will need to be checked for compatibility. If this isn't done properly or the devices configured properly it's likely that the number of false positives, bad analysis or unidentified threats. Overall, this is not a good scenario for security and product delivery. Another area of extreme importance in the transition arena for both protocols is communicating between entities. One company that spent a lot to effort on the networking stack is Microsoft because they needed to make sure their operating systems could work in different environments. Microsoft focused on helping IPv4 hosts reach IPv6 host by using transition technologies like 6to4, ISATAP and Teredo (Horley, 2014)[13]. These technologies are tunneling technologies that are designed to provide a way to use an existing IPv4 routing infrastructure to carry IPv6 traffic. IPv6 has three main transition technologies (Horley, 2014)[13].

1. Dual-Stack Network

   Dual stack is a transition technology in which IPv4 and IPv6 operate in tandem over shared or dedicated links. In a dual-stack network, both IPv4 and IPv6 are fully deployed across the infrastructure, so that configuration and routing protocols handle both IPv4 and IPv6 addressing and adjacencies

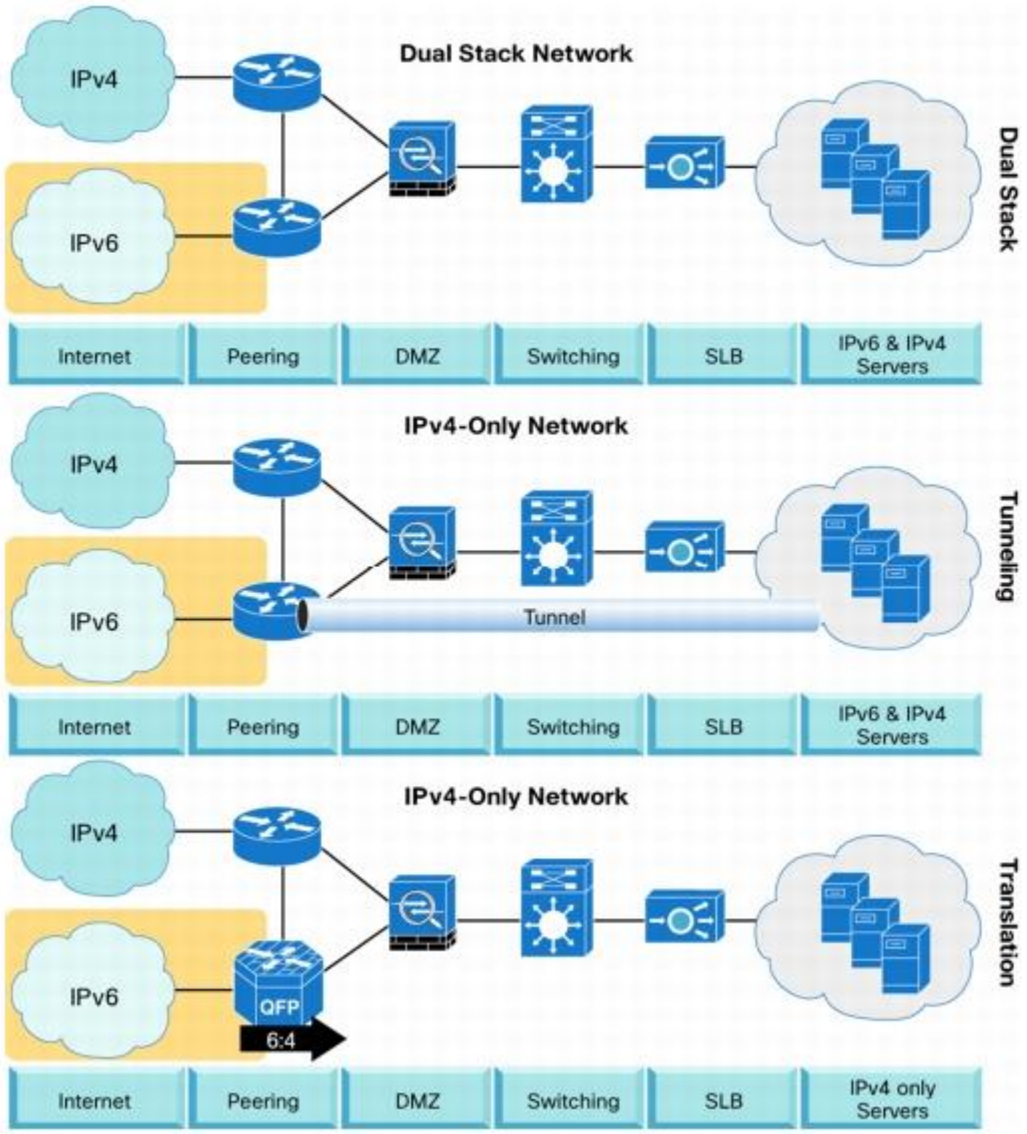
2. Tunneling

   Using the tunneling option, organizations build an overlay network that tunnels one protocol over the other by encapsulating IPv6 packets within IPv4 packets and IPv4 packets within IPv6 packets.

3. Translation

   Address Family Translation (AFT), or simply translation, facilitates communication between IPv6-only and IPv4-only hosts and networks (whether in a transit, an access, or an edge network) by performing IP header and address translation between the two address families.

Each of these technologies has advantages and disadvantages but the issue is looking at those areas and deciding the best route forward. The following figure shows examples for each (Cisco, 2012)[5]:



The next section of this paper looks at security.

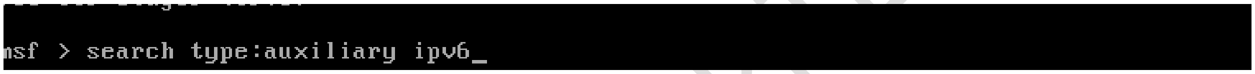
IPv6 main selling point is the endless supply of ip addresses. This fact is a great selling point for users of devices and gadgets. Another very important selling point for IPv6 is the security features. IPsec is an open standard that defines policies for securing communications in a network. VPN is normally associated with the use of IPsec but IPv6 has support for IPsec natively. IPv4 doesn't support IPsec natively but can be implemented. IPsec supports the following areas (Irvin & Ha, 2011)[15]:

- Data Encryption Standard (DES) 56-bit and Triple DES (3DES) 168-bit symmetric key encryption algorithms in IPSec client software.
- Certificate authorities and Internet Key Exchange (IKE) negotiation. IKE is defined in RFC 2409.
- Encryption that can be deployed in standalone environments between clients, routers, and firewalls.
- Environments where it's used in conjunction with L2TP tunneling.

Ipsec is supported on various operating system platforms, supports data confidentiality and it's an open standard so it's not tied to a specific device. The reason IPsec is an important tool is the ability to use the protocol to protect various kinds of transactions. This protocol can be used to secure branch connective over the internet, it can be used to secure remote access on the internet in the form of vpn clients, it can be used to protect electronic commerce and can be used for extranet and internet connectivity between partners (Stallings & Brown, 2012)[27]. The last factor is important because of mergers and partnerships between companies. They need to have confidence that communication between locations is secure. IPsec supports tunneling and transport mode, in transport mode IPsec provides protection for the upper layer protocols but in tunneling mode the entire IP packet is encrypted with optional authentication (Stallings & Brown, 2012)[27]. Kenneth Geers discusses IPv6 in a report concerning cyber security. The report titled "Strategic Cyber Security" points out various ways that an IPv6 implementation could help reduce internet user's vulnerability to spoofing, sniffing and man in the middle attacks but recent looks at the IPv6 mentions that some of these claims my not be totally true (Geers, 2011) (Gont, 2011)[9,10]. In this report the issue of privacy is raised due to the nature of IPv6 addressing. Instead of using Network addressing technologies to conserve addresses, IPv6 has enough addresses for anyone or anything to have a specific address (Geers, 2011)[9]. NAT allows networks to hidden behind a public address. This allowed users to have a bit of privacy. If IPv6 is used user to user communication isn't hidden or obscured so this will give hackers or anyone in general a chance to monitor point to point communications. One way to address this is to use privacy extensions. Privacy extensions in theory are designed to allow users to surf the web without fear of having their privacy compromised because the user is able to obtain a random but temporary address to use. The extensions inhibit device and user tracking. Privacy extensions are supported in Windows and MacOS. In order to better understand the security issues that are part of IPv6 consider attacks that are similar in both protocols. Here's a list of issues that can affect both protocols (Miller & Convery, 2004)[20]:

- Sniffing: IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4
- Application layer attacks: The majority of vulnerabilities on the internet today are at the application layer, IPsec cannot prevent these attacks.
- Rogue devices: Rogue devices will be easy to insert into an IPv6 network as in IPv4. Physical security isn't helped or hurt by IPv6.
- Flooding: Flooding attacks are identical between IPv4 and IPv6.
- Man-in-the-Middle Attacks (MITM): Without strong mutual authentication, any attacks utilizing MITM will have the same likelihood in IPv6 as in IPv4.

The reason MITM attacks are possible with IPv6 is the router discovery operation in IPv6. IPv6 uses a router discovery mechanism that uses IPv6 messages to discover routers in IPv6. The routers respond to solicitations with advertisement messages. An attacker could send fake advertisement messages to solicitations and act like a legitimate router. IPv6's packet structure has routing headers. These headers can be exploited if an attacker uses specific packets to generate headers to reach targeted hosts. If these headers are accepted then the some nodes will send malicious traffic. Mobile IPv6 needs the routing headers so any way to protect the headers must account for this factor. A lot of networks have IPv6 traffic traversing the network but don't know because they are comfortable that IPv6 isn't deployed but IPv6 is on by default in many networks. If IPv6 traffic isn't being monitored then it can be used as an attack avenue into a network (Miller & Convery, 2004)[20]. Hackin9 magazine in an article in their September 2012 edition discussed ways to use the penetration tool Metasploit to explore the attack surface of IPv6. The search command can be used at the Metasploit console to find IPv6 modules. Here's an example of this command (Sheward, 2012)[26]:



```
msf > search type:auxiliary ipv6_
```

This command will reveal the modules that are available for scanning IPv6 networks. A couple of the best commands for scanning IPv6 networks are the following (Sheward, 2012)[26]:

- auxiliary/scanner/discovery/ipv6_multicast_ping
- auxiliary/scanner/discovery/ipv6_neighbor
- auxiliary/scanner/discovery/ipv6_neighbor_router_advertisement

The ipv6_neighbor module is designed to take advantage of the Neighbor Discovery Protocol (NDP). The NDP process uses ICMP messages to determine the link-layer address of devices on the same network to verify the device is reachable this creates the possibility of a denial of service attack if the attacker can create device in use messages. The first stage of an attack is reconnaissance (Sheward, 2012). The use of tools like metasploit gives hackers tools that are easily usable and easily accessible.

IPv6 is a new protocol that alleviates any concerns about IP address depletion. This protocol has IPsec natively installed which is a big help due to traffic on the internet is using layer 3. So, IPsec is a tremendous help as a security feature in that regard. The real importance of IPv6 addresses and security won't do anything for entities that are going to IPv6 or working in a parallel configuration with both IPv4 and IPv6 if proper planning isn't done properly. Because IPv6 is available it's important that time and effort be spent learning this protocol. The attackers are basing their attack plans on the reluctance or inability of the defenders to understand this protocol and how to defend loose networks against their attacks. Tools like metasploit that are easy to use and easy to obtain is in the hands of the good guys as well as the bad guys. If proper planning and scoping isn't done this protocols security features and unlimited supply of addresses mean nothing. In the case of addresses, this means the hackers have more targets to exploit.

Bibliography

1. (n.d.). Retrieved from World IPv6 Launch: http://www.worldipv6launch.org/press/one-year-after-world-ipv6-launch/

2. (n.d.). Retrieved from Internet Society: http://www.internetsociety.org/deploy360/blog/2012/09/with-september-30-deadline-looming-us-government-enables-ipv6-for-hundreds-of-websites/

3. Bedell, C. (n.d.). *IPv6 migration guide: Essential Knowledge for a smooth transition*. Retrieved from Computer Weekly: http://www.computerweekly.com/tutorial/IPv6-migration-guide-Essential-knowledge-for-a-smooth-transition

4. Choudhary, A. R., & Selesky, A. (2010). Securing IPv6 Network Infrastructure: A New Security Model. *IEEE*, 500-506.

5. Cisco. (2012, April). *NAT64 Technology: Connecting IPv6 and IPv4 Networks*. Retrieved from Cisco: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html

6. Conklin, A. W., & Shoemaker, D. (2014). *CSSLP*. New York: McGraw Hill.

7. Convery, S., & Miller, D. (2004). *IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation.* Indianapolis: CiscoPress.

8. *Five steps for overcoming IPv6 planning pitfalls*. (2011, Feburary 18). Retrieved from Search Enterprise Wan: http://searchenterprisewan.techtarget.com/tip/Five-steps-for-overcoming-IPv6-planning-pitfalls

9. Geers, K. (2011). *Strategic Cyber Security.* Tallin: NATO.

10. Gont, F. (2011). *Hacking IPv6 Networks.* Vienna: DEEPSEC.

11. Graziani, R. (2012). *IPv6 Fundamentals : A Straightforward Approach to Understanding IPv6.* Indianapolis: Cisco Press.

12. Hogg, S. (2013, June 24). Mobile Devices and BYOD are Driving IPv6 Adoption. *Network World*, pp. 1-5.

13. Horley, E. (2014). *Practical IPv6 fro Windows Administrators.* New York: Apress.

14. *IPv4 and IPv6 headers.* (n.d.). Retrieved from https://www.google.com/search?q=IPv4+and+IPv6+headers&biw=1366&bih=599&tbm=isch&imgil=98cVWGshNDa8iM%253A%253Bhttps%253A%252F%252Fencrypted-tbn1.gstatic.com%252Fimages%253Fq%253Dtbn%253AANd9GcQUDQm5Wmj7TW1Yk4d5Q6NhQuwF9eRBk-59l2wAY8FLmgHBRJiL%253B573%253B

15. Irvin, E., & Ha, J. (2011, June). IPv6 Is Here. Are You Ready? *ISSA Journal*, pp. 28-30.

16. ISACA. (n.d.). Retrieved from http://www.isaca.org/cobit/pages/default.aspx

17. ISACA. (2012). *IPv6 Security Audit/Assurance Program.* Rolling Meadows: ISACA.

18. Link, J. (2009). *IPv6 - Migration Planning.* Berlin: LinuxTag.

19. Marsan, C. (2012, April 18). *Network World*. Retrieved from The sorry state of federal IPv6 support: http://www.networkworld.com/news/2012/041812-federal-ipv6-258436.html

20. Miller, D., & Convery, S. (2004). *IPv6 and IPv4 Threat Comparison and Best Practice Evaluation.* San Jose: CiscoPress.

21. Monaco, J. (2008). Living with Access Lists. *ISSA Journal*, 34-37.

22. Monaco, J. (2008, June). Living with Access Lists. *ISSA Journal*, pp. 34-40.

23. Parvez, J., & Shah, J. L. (2014). Migration from IPv4 to IPv6: Security Issues and Deployment Challenges. *International Journal of Advanced Research in Computer Science and Software Engineering*, 373-376.

24. Posey, B. (2010, October 22). *10 things you should know about IPv6 addressing.* Retrieved from TechRepublic: http://www.techrepublic.com/blog/10-things/10-things-you-should-know-about-ipv6-addressing/

25. Robertson, S. (2004, September). Requirements and the Business Case. *IEEE Computer Society*, pp. 93-95.

26. Sheward, M. (2012, September). How to Explore: the IPv6 Attack Surface with Metasploit. *Hackin9*, pp. 22-27.

27. Stallings, W., & Brown, L. (2012). *Computer Security: Principles and Practice.* Boston : Pearson.

28. Svendblad, H. (2013, June 1). *IPv6 benefits: Making the IPv6 business case*. Retrieved from Search Enterprise Wan: http://searchenterprisewan.techtarget.com/tip/IPv6-benefits-Making-the-IPv6-business-case

29. Svendblad, H. (n.d.). *IPv6 Cost Considerations*. Retrieved from http://searchenterprisewan.techtarget.com/tip/IPv6-cost-considerations

30. Wu, P., Cui, Y., Wu, J., Liu, J., & Metz, C. (2013). Transition from IPv4 to IPv6: A State-of-the-Art Survey. *IEEE*, 1407-1424.