March 8, 2004

Arden L. Bement, Jr., Director
National Institute of Standards and Technology

Michael D. Gallagher
Acting Assistant Secretary for Communications and Information
National Telecommunications and Information Administration

Dear Dr. Bement and Assistant Secretary Gallagher:

Cisco Systems, Inc. is pleased to respond to the Department of Commerce’s Request for Comments dated January 14, 2004. It is evident by the depth of questions in the RFC that the Department’s Internet Protocol version 6 (IPv6) Transition Task Force spent considerable time studying the issue of transition to IPv6. Cisco applauds this effort, and we pledge to make technical resources available to answer any further questions the Department or the task force may have.

Weighing the costs and benefits of transitioning to a new protocol, the most important consideration is to promote US economic competitiveness in the global market. The RFC asked the question succinctly: “…will late entry into global IPv6 markets by U.S. firms have a significant long-term negative effect on market shares and economic performance?” Japan, China, and to a limited extent, Europe, already see the lethargy in the U.S. as an opportunity to seize economic leadership. The applications being developed there will not only be cheaper than the IPv4/NAT-based ones in the U.S., they will have more creative freedom as developers are free to focus core products and services, or those for which people will pay, instead of being forced to spend time on context, designing workarounds in the limited IPv4/NAT environment. Concentrating on core vs. context is key to improving productivity. Once leadership in Internet services and applications is lost, it will be difficult for US application developers to compete globally.

Cisco, as a global market vendor, has supported IPv6 development, standards, implementation, and operations since its inception. Cisco employees have had leading roles in the definition and implementation of the IPv6 architecture within the Internet Engineering Task Force (IETF), serving as co-chairs for multiple IETF IPv6 Working Groups for several years, and leading IPv6-standards-related IETF Request for Comment (RFC) development. Cisco is a founding and principal member of the IPv6 Forum and has been an active participant in world-wide IPv6 promotion. Cisco IOS Technology Preview code, available since 1996, helped to build the experimental IPv6 Internet “6Bone”. In Europe, we are a founding partner of 6Net, a 16-country native IPv6-based network. We also support Moonv6, a collaborative effort between the North American IPv6 Task Force (NAv6TF), the University of New Hampshire – Interoperability Lab, the Joint Interoperability Test Command, other DoD Agencies, and Internet2. Cisco’s IPv6 education initiative includes “ABCs of IPv6,” a Cisco Press Book, and various white papers and presentations. All Cisco IOS Software release trains, supporting 24 platforms, support IPv6.
Applying our extensive experience with IPv6 to this RFC, four key findings emerge. We suggest that the Department of Commerce consider these as guiding principles as it formulates US national policy:

**IPv6 will replace IPv4 over time** – but questions remain concerning the rate at which this replacement will occur, where this change will happen first, and the key drivers forcing this change to occur.

**Applications must be protocol agnostic** – To enable IPv6 deployment, it is important that new or updated applications be written so that their functions are independent of the Internet protocol used.

**The difficulty and cost of transitioning to IPv6 will depend on the type of equipment in each network and the migration objectives** – a decision to replace rather than work with large numbers of NAT devices or middle boxes, for example, can increase costs and add to difficulty.

**IPv6 deployment in the US, government and businesses, lags that in some foreign governments and businesses** – especially in emerging economies in Asia where relatively small IPv4 investments have been made and governments have taken a leading IPv6 deployment position with clear economic and competitive goals.

**The role that the US government should play in transitioning to IPv6 should consider political as well as technological factors** – a motivator for taking action is to avoid losing leadership in innovation, but a factor for businesses to delay is the lack of an incentive for building IPv6 into products.

Cisco has provided detailed comments in the appendix attached to this letter, organized around the four major topic areas presented in the RFC:

**Potential Benefits and Uses of IPv6** – including a discussion of the impacts of an increased address space, the potential for improved security, end user applications, and network evolution.

**Cost of IPv6 Deployment and the Transition from IPv4 to IPv6** – including a description of expected hardware, software, and deployment costs as well as special transition costs involved in migrating, such as security costs and other added costs.

**Current Status of Domestic and International Deployment** – including a discussion of useful metrics used to measure deployment along with an assessment of US and international commercial and governmental efforts underway.

**Government's Role in IPv6 Deployment** – including an assessment of the need for and nature of government involvement and the exposures to the government and the business community if action is delayed.

We hope our comments are helpful to the Department in developing a national IPv6 transition policy. Please feel free to call on me or my staff as you work through these issues. I will ensure that appropriate Cisco resources are made available to assist you in this important undertaking.

Regards,

Joel P. Bion
SVP, Internet Technology Division
Cisco Systems, Inc.
Appendix

1. Potential Benefits and Uses of IPv6

A. Increased Address Space

How many IPv4 addresses have been allocated?
As of 2/10/04, the ARIN report to NANOG showed the IANA registry central pool with 89 remaining reserved /8 blocks, or 34.7% of the total. (/8 is the typical allocation unit to the regional registries. [1] [2] [3]

How long will the remaining IPv4 addresses be sufficient to meet US and International needs?
Projections of address IPv4 space exhaustion vary in time frame from 2022 to 2045. In all cases, assignment policies are assumed to be held constant. Depending on which model one uses [1], there are a number of reasons why we would not see a constant rate of consumption:

- Increased utilization of “always-on” home networking. By some estimates 20% of homes in the United States use a broadband service such as DSL or cable. Introduction of neighborhood wireless in some cities may allow for additional and more rapid broadband penetration.

- Development of additional home networking technologies, such as smart personal data recorders and power management systems may further accelerate address rate consumption.

- The developing world has not yet fully embraced broadband largely for economic factors. Should those economies accelerate their growth, we should expect to see a commensurate acceleration of address space.

- Personal computing devices such as mobile phones and digital assistants are becoming prevalent. Their need for addresses places may accelerate the overall rate of consumption.

Taken together in their worst case these factors could have a multiplicative impact. However, mitigating advances in technology may extend the lifetime of IPv4, as will be discussed in detail later. Not all applications will require globally unique address spaces.

How will the limitation on IPv4 addresses affect different geographic regions?
Eventually, the existing pool of IPv4 addresses will be insufficient to support the goal of 20% market saturation on a global scale. Only 36 of the 208 UN recognized entities (17.3%) have reached at least 20% of their IPv4 target markets. If the top 15 countries assigned a single address to 20% of their population, over 300% of the remaining IPv4 pool would be consumed. [4]

Because of strong market penetration & large historical allocations, the United States, Western Europe, and Australia are least likely to be impacted by such address space concerns for quite some time, whereas populous nations and emerging economies such as China and India are likely to be impacted more heavily. Again, the point at which anyone is impacted depends very much on the rate of consumption. [5]

What new products, services, features, applications and other uses are likely to result from addresses offered by IPv6?
Because of its larger address space, IPv6 enables globally unique addressing which facilitates ‘always-on’ applications, peer-to-peer applications as well as applications based upon IP connectivity originating from within the network to subscribers.
Such ubiquitous networks are both broadband and mobile in the sense that they can be accessed from anywhere. They are multi-modal networks, that is, users can freely cross the boundaries between fixed and mobile networks, wired and wireless, communication and broadcasting, and between terrestrial and satellite transmission. [6]

The information equipment used in ubiquitous networks includes not only personal computers and cellular phones but also terminal equipment already in the market but currently not capable of accessing the Internet.

Ubiquitous networks make it possible for all devices to access the Internet using Internet protocols, preferably IPv6. These include PDAs, videogame consoles, and popular audio-visual equipment, including home servers, set-top boxes digital TV sets, networked home appliances, (commonly called information appliances), car navigation systems and intelligent transport systems (ITSs) and servers in trains, ships and airplanes. All can be connected via IPv6.

The effectiveness of ubiquitous networks as the basis of a new social system will be enhanced further by linking radio frequency IDs (RFIDs), sensors, webcams and other devices which enable machine-to-machine (MtoM) communication via the Internet protocols. This new environment will be also enhanced by establishing "always-on" connection with equipment that is connected to IP, in addition to connecting the information equipment that works as a medium for human communication.

IPv6 also offers a new opportunity for mobile computing. Previously, it was necessary to make the architectural assumption that correspondent nodes were unaware of whether or not a device was mobile. Because mobility is a part of the base standard, it is now possible for mobile nodes to communicate location changes to their correspondents, allowing for optimal routing.

**Has NAT/CIDR slowed the consumption of IPv4 addresses?**

NAT, along with CIDR and DHCP, slowed the consumption of address space with techniques such as address reuse with translation and temporary-use allocations. [7]

Always-on environments (such as residential Internet through broadband, cable modem, or Ethernet-to-the-Home) are not always compatible with IP address conversion, pooling, and temporary allocation techniques. The "plug and play" required by consumer Internet appliances further increases the address requirements. IPv6 reintroduces end-to-end Security and Quality-of-Service (QoS) that are not always readily available throughout a NAT-based network.

While there have been many reasons why consumption of IPv4 addresses have slowed, there can be no doubt that NAT has been a major factor. A trip to the local electronics store will demonstrate how successful NAT has been. Many products now provide a combination of wired and wireless connectivity along with firewall and NAT services. Their success indicates that the family is able to connect through a single Internet connection, using a single IPv4 address that has been assigned by DHCP.

The result of single allocations per household has slowed address consumption as compared to the number of simultaneously active devices.

The evolution of routing Internet registries (RIRs) and their policies along with the advent of CIDR has also slowed the growth of consumption. A reasonable question one may ask is whether they have slowed the growth of consumption too much. Even more relevant will be allocation policies for IPv6. Because of its increased address space the opportunity for less restrictive policies exists.

**Would a NAT device represent a single point of failure?**

Currently yes, and there are two general cases. In the case of a single homed site such as a consumer home, the link and the router components are as much or more likely to be of concern. In multi-homed environments, the state kept by one NAT must be shared with others, and they must represent to the public Internet the same addresses allocations and ports, if transport...
connections are to be maintained. Such appearance can be impractical for backup servers that are topologically diverse. However networking products are now emerging that support stateful NAT (the ability to redundantly deploy address translational gateways that allow for real-time failover should an outage occur and for example in remote access applications, where NAT is pervasively used, a redundant deployment of stateful NAT devices can preserve connectivity and IP sessions seamlessly during a failure.

B. Purported Security Improvements
Cisco recently completed a threat comparison and best practices evaluation for IPv4 and IPv6. This paper, attached to this response, provides additional information. [8]

**Does IPv6 enhance network security?**
Because the operational models of IPv4 and IPv6 are substantially the same, use of IPv6 will not substantially enhance network security.

Although there are no substantial differences, minor differences exist, for example: IPv6 subnet sizes will increase from $O(1)$ to $O(264)$. It will therefore take substantially longer for a hacker to perform an exhaustive address and port sweep (280,772 years for just the address space at 40Gbps).

While it remains to be seen how service providers in the U.S. deploy IPv6 to the home, if they follow existing practice of early deployments in Japan of static allocation it is possible that the global address space will improve traceability. It is anticipated, however, that logging will continue to be a requirement to understand who is using a particular address at a particular time.

**Can IPv6 degrade network security?**
Fundamentally the security architectures of IPv4 and IPv6 are similar. Hence IPv6 in and of itself does not degrade network security.

Because IPv4 is substantially more mature than IPv6, it is reasonable to assume in the short term that implementation errors will be found, leading to some number of vulnerabilities.

Furthermore, in as much as multiple firewall rule sets are necessary during transition, it is likely that administrators will suffer periodic policy inconsistencies.

**Will IPsec be easier to use with IPv6?**
From a pure protocol standpoint, IPsec may be easier to use in IPv6 since its inclusion is mandatory as part of the protocol, as stated in the standard. However, the fundamental IPv4 and IPv6 management and trust issues remain the same. Also, in cases where IPv6 stacks have implemented IPv6 without IPsec, IPv6 will not bring any additional benefits. These issues will prevent the widespread use of IPsec for a long time to come. Basic Internet traffic from organizations or consumers on the Internet to servers will still be in the clear.

**Will IPsec become more useful if NAT devices are no longer used?**
NAT traversal mechanisms are now emerging for IPv4, so removing NAT is not a significant advantage to IPv6 IPsec. The key management and trust issues are a far bigger impediment and are present in both versions of IP.

**Are there critical IPsec implementation issues unrelated to the IP version?**
Yes, Public Key Infrastructure (PKI). This is really a non-technical problem of trust relationships. Even if limited communities can deploy a PKI, there will still be a need to tie the communities together and so far this has largely not happened in the IP Security markets.

**How dependent is IPsec upon workable trust models?**
PKI has been, and will continue to be the major stumbling block. Organizations like the U.S. DoD that already have a managed PKI will be able to ‘take advantage of IPsec, but in the short term the average consumer will not. Even for example if the financial services industry figure out how to build a PKI for their customers, there will continue to be a need for a high-level trust entity to tie disparate key infrastructures together.
What IPsec issues will impact the growth of IPv6?
IPsec is only one component of an overall security model. The end-to-end confidentiality provided by IPsec is a security value to the end users, but to the data-inspection-oriented network manager, it is a detriment. While the confidentiality afforded via IPsec may be a driver in some environments, the limitations and costs associated with making applications work in the face of increasing complexity of IPv4/NAT will be a stronger driver for IPv6 deployment.

Will IPsec deter “spoofing” attacks and allow tracing of messages?
Spoofing of content can be avoided through the use of ESP with NULL encryption. Spoofing of the address can be avoided through AH. A more effective approach to avoid spoofing is implementation and deployment of reverse path forwarding (RPF) checks, as recommended in RFC 2827.

An IPv6 packet can be forged much the same as an IPv4 packet.

Would IPv6 further national security and law enforcement interests over and above IPv4?
No. The net change in security from IPv4 to IPv6 is minimal unless IPsec can be more consistently deployed.

Would IPv6 improve ability to identify the source of malicious or illegal activity?
While there is sufficient space for ISPs to allocate static IPv6 prefix values to their customers, because of existing operational models it is not clear how static allocations will actually be. A reason for keeping the existing models is that topological changes demand prefix changes that must be propagated to customers. Thus predictions in this area would be premature.

There is a capability in IPv6 called ‘Privacy addressing’ that is intended to deter malicious or marketing web sites from tracking mobile appliances as they move around the network. Privacy addressing schemes will make some aspects of law enforcement effort more difficult when it comes to tracing the actual end system once the subnet has been determined. Addresses are traceable to the ISP/customer demarcation point, but beyond that traceability requires access to the local routers. Even with access to the routers, addresses change frequently, creating the same architectural characteristic as the IPv4/NAT combination and making it difficult to determine which of 2 hosts on the same subnet originated an attack. As a result it may be challenging for law enforcement to be able to trace a specific node as it moves between attachment points, or over extended periods of time.

C. End User Applications

How would IPv6 reduce management burdens, simplify mobile access, and improve Quality-of-Service (QoS)?
IPv6 simplifies the process of subnet address management. One of the hidden costs within corporate networks is the time and effort needed to change the address space allocated to subnets. Growth or shifts in function among locations can cause a mismatch between the number of active nodes and the amount of address space allocated to a specific office. This problem goes away with IPv6 because every subnet will have substantially more address space allocated than the number of nodes that can be physically attached (~ 10^16 greater than current technology supports).

What value does IPv6’s improved capabilities provide?
Reduction of the number of architectural functions in the network will reduce the number of components that can fail, increase network resilience, reduce management complexity, and thus reduce both deployment and ongoing support costs.

What are examples of how IPv6’s improved capabilities would benefit users?
Examples are very often specific to a specific market segment or application area, but consideration should be given to the following examples:-
Auto-configuration of addresses is one feature that can ease the deployment of low-cost appliances, broadband access routers and enable ad-hoc networking.

In some cases, optimized routing of Mobile IP will improve traffic flow and performance. Mandatory support for multiple addresses may also provide innovative overlay topologies.

**Would IPv6 allow the Internet to return to its original open scheme?**
Yes, as the original Internet model was open in a way that application developers did not need to know the underlying infrastructure to run peer-to-peer applications reliably. This scheme is restored by IPv6.

No. Because firewalls have become a required featured in today’s network in order to enforce security policies that were not necessary in the early Internet days.

**Are there additional NAT- or middle-box-related issues that impact the growth of IPv6?**
NAT and middle boxes have extended the life of IPv4, providing IPv6 implementers valuable time to mature their products. In the end, some middle boxes may no longer be necessary. However, even within the context of IPv6 the use of private or Locally Unique addresses may create a market for NAT. The reasons for this pressure are primarily enterprise needs for stable addressing in the face of mergers and changes of providers. This is an ongoing area of research.

**Will NAT preclude the use of peer-to-peer devices and applications?**
There exist mechanisms such as STUN and ICE that enable limited peer to peer communications. These mechanisms have shown themselves to be acceptable in the consumer market, but less so in the large enterprise or service provider environment. The reasons are that they involve probing of static points in a network. Should the path of the actual communication diverge from that which was tested, either due to multiple Internet connections or due to a routing change, the information learned by the probe may be invalidated.

A small number of NATs exist that are not compatible with such workarounds. In addition, there are environments where using a third party to establish communication may be unacceptable from either a security or reliability perspective.

**Will middle boxes affect the availability and function of peer-to-peer devices and applications?**
Certainly some middle boxes (like firewalls) are inserted into the network with the explicit intent of inhibiting particular applications. The issue boils down to where the middle box is placed relative to its function, and how closely its policy matches any affected users. For example, a firewall placed at the edge of an enterprise network will most likely implement the policy of that enterprise, while that same firewall placed in the middle of a carrier network would affect other customers who might have a different policy.

**Can “work arounds” for particular applications be developed to prevent NATs or middle boxes from interfering with peer-to-peer interactions?**
As stated above, such workarounds can be developed, but they will not be applicable to every situation. Thus a key argument for IPv6 is generality, so that application developers only have to support a single mechanism. Some U.S. service providers have raised this very concern in the context of voice and remote access to home services.

**To what extent will workarounds affect application performance?**
The level of impact will depend on the environment, the application and the mechanism. Periodic in-band mechanisms that retrieve NAT bindings are likely to not have a substantial performance impact.

**Will those workarounds scale well?**
In the current consumer market these mechanisms appear to scale sufficiently for gaming applications and some voice applications but we are unable as yet to measure the impact of large scale deployment of Internet appliances for this market. Because the enterprise and service
provider environments are far more complex it is unlikely that workarounds will scale well. This is due to multiple Internet connections, security policies that intentionally limit connectivity, and multiple concentric security domains and address spaces.

*What additional cost might firms incur in developing workarounds for NATs and middle boxes?*

The additional cost will vary based on mechanism. In the short term we can expect additional development costs related to these mechanisms, as well as additional ongoing support costs.

In the longer term, if the advances of these workarounds follow the same pattern of other technology, and it seems reasonable to make this assumption, the various mechanisms are likely to consolidate over time. We can additionally anticipate that as they do, standard libraries will become available, reducing development cost. The support costs are likely to remain for as long as the workaround is needed.

For example, in order to implement early versions of the Mosaic web browser with SOCKS proxy support, approximately two lines of code were changed. However, the SOCKS server became a substantial support burden. These same issues apply to any application gateway or other workaround that would be necessary to ameliorate NAT problems.

**D. Network Evolution**

*Is increased address space the only compelling reason for adopting IPv6?*

No. It is a compelling reason but the ability to develop interactive applications that take advantage of increased addressing is another reason. IP convergence is a huge business driver for IPv6.

*Can IPv6 features be implemented over IPv4 networks and will they perform effectively?*

Many features are available for both IPv6 and IPv4. The most common examples are IPsec and Mobile IP. A major difference is the topological span of deployment. In the case of Mobile IP, a large scale deployment of the technology by the Mobile Wireless phone industry will be more easily done through Mobile IPv6 and its feature set.

*What are the added costs of implementing IPv6 features on IPv4 networks?*

The set of features that was straight-forward to integrate into IPv4 has already been done.

*What are the clear feature advantages of IPv6 over IPv4?*

In addition to a larger address space, IPv6 includes improvements that simplify network administration, such as:

- Improved main header processing
- Simplified network administration in general due to a fixed subnet length.
- Embedded support for Mobile IP and mobile computing devices
- Enhanced multicast support with increased addresses and efficient mechanisms
- Potential for improved support of Anycast addresses

*Will the increased size of the IPv6 header have an impact on latency sensitive applications such as VoIP?*

Impact on latency-sensitive applications will depend more on the capacity of the path being used. As bandwidth increases delay approaches a constant. IPv6 increases the main header portion of a packet by twenty bytes. Low bandwidth links require commensurately small amounts of CPU to apply compression techniques.

*Will IPv6 header compression schemes result in improved performance without requiring more processing?*

The IPv6 header compresses better than the IPv4 header because its options and other variable values were moved out of the base header. Although the IPv6 header is larger, when compressed it is actually smaller, assuming it makes sense to perform compression over low capacity links.
**Does IPv6 require new routing technologies that present system design and operational challenges?**

No. The underlying capabilities and challenges remain the same because the routing philosophy in IPv6 is the same of IPv4. Were IPv6 deployed instantaneously without any transition, the routing table in the default-free-zone would shrink from currently around 150,000 entries to about 20,000 entries. However, because it is likely that both networks would run simultaneously on the same physical infrastructure, the default-free-zone would temporarily increase through the transition, and then temporarily decrease as IPv4 routes that are not well aggregated get withdrawn. As enterprises continue to multi-home, however, and as service providers improve their connectivity, the size of the IPv6 routing table will continue to grow. Scaling of the routing system is an ongoing development activity.

**Does IPv6 have inherent design limitations?**

Every system has design limitations. When the IETF promulgated the standard, design tradeoffs were made. The chief tradeoff made in IPv6 was use of a fixed-length address in order to reduce processing complexity, rather than a variable length address that was smaller.

Other technical limitations that have been identified to date are (1) the lack of a simple solution to the complex problem of sites connecting to multiple providers, and (2) the operational difference between the multiple addresses per host method vs. current IPv4 practice. Ongoing work to deal with the multiple connection problem has focused on an alternative architecture. In any case, IPv6 offers the same technique for the multiple-connection issue as IPv4, plus a new approach that may work in some environments.

**Are IPv6 hardware and software technologies mature and practical?**

Software implementations of IPv6 have existed for quite some time. All major computer operating systems offer IPv6. However, support tools such as network management applications lag in development. Hardware-based forwarding implementations are now available. In particular, any hardware or software that has been built with a 32-bit IPv4 address assumption will need to be updated to support IPv6 at a similar performance level.

**Does IPv6 depend on modifications to existing transmission systems?**

No, the point of either version of IP is to isolate the end-to-end packet layer from the morass of transmission technologies that are used by various providers. In particular, IPv6 can run over IPv4, and in doing so treat the entire IPv4 Internet as a transport link.

**Will IPv6 allow greater use of existing transport and transmission networks and applications?**

IP (either version) is generally unaware of the underlying transmission. The transport protocol that rides over IP usually does what it can to take full advantage of any available resource below IP. IPv6 has changed the default expectation of the minimum maximum-transmission-unit (MTU) of any link. If the average packet size ends up being higher as a result, any link that is underutilized due to limitations in the ability to process packet headers will see an improvement, while any that are limited by external factors will see a decrease due to the loss of header bytes from the extra packets. Since packet header processing is rarely a long-term problem in current systems, IPv6 is not likely to make any difference to typical transmission utilization.

**Will spectrum management issues arise in IPv6-based wireless and hybrid networks?**

Wireless communication is just another media which IP ties together to create the overall Internet. However, the ultimate driver will be the number of devices that contend for access to a particular frequency in a particular area, and the amount of bandwidth their applications require. Because IPv6 holds out the promise for a globally accessible device, the nature of wireless connectivity could substantially change. Also, as video and audio capabilities improve, the demand for bandwidth will increase. Since voice is merely an application run atop an IP network, there is room for a new wireless Internet service provider in the market place who can allow end users to select and use those services they wish to use.
By technical necessity, today’s U.S. cellular carriers can only provide a limited form of Internet connectivity, where address translation must occur. Without that need, enterprising individuals will be able to develop their own services that will drive spectrum usage by mobile users of those servers.

**Will IPv6 require transport layer modifications?**
The necessary transport (as the Internet community uses that term) protocol changes were documented in the base IPv6 protocol document, IETF RFC 1883 (December 1995), and its updates. Any part of a system of interacting applications that accesses IP addresses directly will need to be fixed or replaced. In particular, applications that try to ‘do a better job than the OS stack at flow management’ or have a fixed allocation of 32 bits for a DNS response will need to be updated to allow for 128-bit addresses. Application developers should investigate alternative transport layer technologies such as SCTP.

There are no changes necessary for transport (as the telephony community uses that term) due to the layer independence (see discussion about transmission above).

**Will IPv6 require transport layer modifications to improve performance?**
In the general case we do not expect IPv6 implementations to require transport improvements.

**E. Other Benefits and Uses**

**What new service possibilities will IPv6 create?**
It is difficult to predict the future. However, unfettered peer-to-peer access without the need for middle boxes will allow for more rapid prototyping and development of services. Prototyping is at the heart of technical innovation. An example of innovative new services that are being investigated is remote diagnostics of consumer appliances.

**What are potential economic impacts of other IPv6 developments?**
Again, while it is difficult to predict the future, the constraining influence of a small address space will eventually preclude development of innovative services that require end-to-end connectivity. The opportunity cost, therefore, is as difficult to predict as the initial Internet boom was.

**How could VoIP drive IPv6 implementation?**
The primary driver for VoIP over IPv6 may well be the wireless market, as we discussed above. 3rd Generation wireless standards bodies, 3GPP and 3GPP2 defined new domain, IP Multimedia System (IMS), is being added to the mobile core network. The introduction of IMS system is driven by the demand to offer more and enhanced services to end users. At the heart of IMS is an IP based transport mechanism for both real-time and non-real-time services, plus the introduction of multimedia call control. 3GPP has selected Session Initiation Protocol (SIP) as the only call control protocol between terminals (or mobile devices) and the network. 3GPP also mandated the use of IPv6 [9] as the only IP version protocol for the IMS components. IPv6 provides the end-to-end addressing required by the new multimedia environments for mobile phones and residential Voice over IP (VoIP) gateways. IPv6 provides the services, such as integrated auto-configuration, QoS, security, and direct-path mobile IP, also required by IMS system environments.

As mentioned above, standards bodies for the wireless data services and 3G wireless Multimedia Subsystem are preparing for the future, and IPv6 provides the end-to-end addressing required by these new environments for mobile phones and residential Voice over IP (VoIP) gateways. IPv6 provides the necessary addressing space to enable peer-to-peer, always-on services. It can also improve services required by these environments, for example, integrated auto-configuration, QoS, security, and direct-path mobile IP.

The addition of powerful multimedia capabilities to next generation mobile phones with the introduction of new “IPv6 only IP Multimedia System” (IMS)” within mobile core networks
enable the need for smooth integration and coexistence between IPv6 based mobile networks and legacy network.

Apart from next generation wireless networks, it would otherwise be speculative to predict that VoIP will drive IPv6 implementation. Enterprise use of VoIP is unlikely to change significantly, as firewalls integrate functionality necessary to support connections. Certain aspects of VoIP may, however, change over time. The opportunity to create ad-hoc conferences without third party servers with public addresses will present itself.

**Will IPv6 improve VoIP performance?**
IPv6 makes VoIP scalability possible to address a new set of markets such as Residential VoIP or public Wi-Fi VoIP services. IPv4 lacks the numbers of available addresses it would require. The elimination of middle box functions will improve reliability of the service, thus potentially further commending VoIP as a replacement for legacy voice service.

**Are there other applications that could benefit from IPv6?**
In general, IPv6 allows the application developer to focus on solving the user problem, rather than the complexity of the network. Distributed computing – or Peer-to-Peer – and Distributed services – where servers are located on the end-user’s networks – may be achieved on a large scale, opening the door for innovative applications and services.

**Could other applications thrive with only a partial IPv6 implementation?**
Unless those other applications make use of IPv6 functionality or direct connectivity, they can make use of either IPv4 or IPv6. Some applications that make use of IPv6 functionality exist today with a partial deployment. Because IPv6 was designed with a long transition in mind, the expectation was that in IPv6 nodes would be able to benefit from old legacy applications that are unaware of IPv6 as well as new applications that take advantage of the global address space.
2. Cost of IPv6 Deployment and the Transition from IPv4 to IPv6

A. Cost of Deploying IPv6

1. Hardware Costs

What are typical IPv6 deployment costs and time frames?
In the short term, deployment may require replacement of forwarding devices that are either unable to understand IPv6 or are unable perform sufficiently. In the longer term, as IPv6 becomes more prevalent in implementations, customers will be able to transition based on their need to do so without excessive regard to hardware costs. We anticipate that it will be a very long time in most complex environments before the last IPv4 device is turned off.

What are IPv6 deployment costs for hardware changes?
Today, the cost to the consumer and small business can be approximated to the cost of a software upgrade and any associated configuration and training costs. Offering dual stack (IPv4 and IPv6) solutions need higher memory and processing speeds. Hardware devices such as high end routers, switches, fire walls are already started offering dual stack (IPv4 and IPv6) implementations using advanced memory and processor technologies. Software based forwarding devices generally already provide IPv6 support, and therefore do not require replacement. As previously mentioned, end host equipment is largely capable of supporting IPv6 today without additional expenditure as long as they can support a recent operating system release.

What is the cost of replacing/modify premises equipment (DSL and Cable Modems)?
This is technology-dependent. Those devices operating at Layer 2 will not need to be changed. Any device that looks at the IP layer will need to understand IPv6 as well as IPv4. Cost will depend on how much is software based vs. ‘hardware based.

What is the useful life of premises equipment (DSL and cable modems)?
Consumers expect equipment to last from 5-10 years, while enterprises and service providers often work on a 3-5 year amortization/replacement cycle. The Y2K issue caused a significant skew in the normal diversity between organizations, and synchronized a substantial percentage of the market. This timing synchronization will eventually dissipate, but the amortization periods are often tied to tax code.

Will differences in technical and economic life expectancies of equipment affect the decision to move from IPv4 to IPv6?
Economic life expectancies of devices are based on several factors:

- equipment amortization;
- anticipated opportunity cost of new services that could be deployed; balancing work-around overlay costs vs. newer equipment;
- cost of maintaining the existing service on old equipment; and
- ability to scale to larger environments or the necessity and cost to maintain more capacity during times of contraction.

Are the costs of IPv6 and IPv4 equipment similar?
For physical equipment this will likely happen by default because most vendors are already including IPv6 as a base feature. Some software vendors may wish to charge a functionality fee in-line with their software pricing. Others may choose to bundle support for IPv6 into an upgrade. Some software upgrades will take a substantial amount of resources. For instance, upgrading versions of a database may take several years of planning, development, and execution in a complex environment at a single enterprise.
Will added operating and administrative costs of purchasing IPv6 equipment cause customers to stay with IPv4?
Since IPv6 functionality is now integrated with many IPv4 products, the administrative costs of purchasing IPv6-capable products would in most cases be addressed through the normal product upgrade cycle. Therefore going forward, acquiring IPv6 products should not represent a significant purchasing delta over the overall costs associated with the IP infrastructure.

Will manufacturers continue producing equipment and applications that can handle only IPv4 packets?
Several network equipment vendors have already started offering dual stack based equipment in market place. Application developers have begun to develop applications on top of IPv6. Although Japanese consumer market is producing IPv6 based electronic appliances, but consumer markets in USA is lagging behind, in short term a trip to the local electronics store will confirm that this is the case. Those manufacturers that export products are likely to ship devices with IPv6 enabled to markets such as Japan and China, where there is demand. However, just because IPv6 is delivered to one market does not necessarily mean that it will be delivered to the U.S. market. Memory footprint and dual stack considerations will factor into production costs, particularly in the very price-sensitive consumer market.

What market conditions would persuade manufacturers to cease producing IPv4 equipment?
Manufacturers will stop producing IPv4 equipment when customers stop ordering it. There is a vast difference between IPv4 capable & IPv4-only capable equipment. The successful suppliers will offer simultaneous IPv6/IPv4 capability until customers are no longer willing to pay the costs for supporting IPv4. Given the independent nature of deployment decisions, IPv4 support in equipment will be required for years to come.

2. Software costs
To what extent will the modifications to routers, hosts, servers, and terminal equipment mentioned above involve only software changes?
Hosts and servers will generally only require software changes. General purpose routers and terminal equipment can usually get by with only software changes. High-end enterprise and service provider switches and routers that use hardware forwarding today may require software upgrades. Networked applications such as databases, file servers, network operations tools, complex web servers, and Internet PBX systems may require substantial modification.

What is the likely magnitude of those costs?
If the market is allowed to gracefully transition, the costs of development can be amortized over the rest of a development cycle. For IPv6 there will be a one-time development & training cost.

Will applications and Internet services (e.g., search engines, content delivery networks, DNS) have to be modified to make them compatible with IPv6 transmission?
Yes.

What are the estimated costs of those changes?
The extent of changes will depend on how much the application or service interacts with the IP layer. In some cases, the software changes are likely to be relatively minor. In some cases, the software changes may already be in place, and simply need to be deployed or turned on. For instance, the Bind name server today supports IP version 6.

In other cases, the changes will be more substantial. Content delivery networks that attempt to optimize routing at the Internet layer will need to develop an analogous IPv6 capability. However, because IPv6 offers an explicit Anycast scoping, they may at the same time be able to improve their underlying service offering.

Many network management applications and tools lag behind in development of IPv6 capabilities. However, it is worth noting that some components of network management may not
need to support IPv6 for quite some time. For instance, while it will be important to understand IPv6 addresses within control streams such as SNMP, because the transition model calls for a long transition, IPv6 capable networks will be manageable through protocols that run atop IPv4. Thus, a market driven transition would require MIBs to be completed prior to protocol changes. It is worth noting that requirements from certain government funded research programs may eliminate this logical prioritization.

**Will the necessary modifications to software and applications require extensive changes in the underlying coding and, if so, at what cost?**

In general, applications will not require substantial changes. However, software that is written with a significant number of implicit assumptions about 32-bit address values will require significant changes at an equally significant cost to find them all. Because the library interfaces of IPv4 and IPv6 are substantially similar, only in those cases where IPv6 offers additional functionality will there be extensive changes. Because those enhancements are generally below the application layer, only specialized applications that deal with functions such as mobility and network management would require substantial change along the lines previously discussed.

**How much will it cost to train an organization’s personnel to install, operate, maintain, and service IPv6 hardware and software?**

This will depend on the size and the expertise of the current staff. While many of the concepts are similar, some are just different enough that they may prove challenging to current staff. For the day-to-day enterprise and carrier operations staff that only worries about router configurations, most of the costs will be related to understanding colon-delimited hex rather than dotted decimal addresses. For host administrators, the costs will be that plus dealing with potential differences in how addresses are configured on each system, as well as how many addresses are assigned to any one interface.

**How do training costs compare as a percentage of the cost of IPv6 hardware and software and will this cost influence an organization’s decision to adopt IPv6?**

Training is just one of the overall cost factors in the decision and is a one-time event. Some organizations may look at IPv6 training as a career advancement opportunity and bury the explicit cost in an overall staff development program. Others may look at it as a significant identifiable hurdle to be avoided because they never bother to add up the complexity-induced costs over multiple years. Still others may receive free training as part of an existing training program.

**What are the opportunity costs of waiting to deploy IPv6 and will these costs vary by market segment (e.g., small and medium enterprises, large enterprises, academia, civilian government, military, individual users, and any other relevant segments)?**

A shift to IPv6 over a short period of time will be more expensive than doing it as part of the normal life-cycle update. Transition technologies were specifically designed to enable a prolonged overlap, and to minimize deployment and operational interdependencies. Rather than forcing a short-term shift, a reasonable deployment plan would focus on replacing as much IPv4-only hardware and software as possible through normal life-cycle updates. Over any period of acquisition, turning on IPv6 for routine use should only occur after a critical mass of IPv6-enabled replacement technology and training is in hand.

Opportunity costs vary more by perceived goals than by segment. For example, some parts of the military segment (with a substantial IPv4 address pool) may want to continue their current tasks at reduced cost, so IPv4 may present a better opportunity cost. Other parts of the military segment may look at future scenarios and the number of independently addressable devices necessary to accomplish their task, and may recognize that IPv6 is their only path. In these cases, opportunity cost with respect to a non-existent IPv4 alternative doesn’t make sense. For retail establishments looking to track millions of inventory items on a global scale, the opportunity cost is based on the trade-off between continuing with manual efforts vs. moving to automated always-on technologies (like RFID). Waiting simply means more delays, errors, and salary for manual
counting, vs. the one-time cost of an automated system which can provide current, error-free accounting without the substantial staff salary & benefit costs.

**How will the transition path of the U.S., relative to the rest of the world, influence costs and prices of IPv6 equipment, services, and applications?**

In as much as the products and services in the Asian market are applicable to the U.S. market, those vendors offering services will have absorbed some of the initial development costs. Those savings may be passed on to customers as they themselves build services in the United States. In as much as Asian market products do NOT translate to the U.S. market, the loss of economic scale may not be acceptable.

**Will costs and prices decrease over time as a function of the worldwide IPv6 installed base?**

With any new technology, costs will decrease per instance as the development costs get spread over more instances. As deployments in the United States mature, the cost to the consumer will drop.

**Could waiting for international development and deployment of IPv6 lead to reduced R&D costs and fewer security problems for U.S. adopters?**

As products mature, fewer vulnerabilities are found. Indeed the U.S. has already benefited some from the experience of others. Although it is difficult to say when it will happen, there will, however, come a point of diminishing returns. The foreign market has already driven some amount of domestic development in this area.

**Will late entry into global IPv6 markets by U.S. firms have a significant long-term negative effect on market shares and economic performance?**

R&D costs incurred by IPv6 implementation, like any other advanced technologies, can be borne by early adopters. Excessive delay by U.S developers may not allow them to charge such premiums if there are already mature competing products in the market place. However, such costs are not likely to be a dominant factor for most application services.

However, one cost that cannot be quantified is any paradigm shift that might occur due to innovations made possible by an IPv6 deployment.

**What is the impact of slow IPv6 deployment on the development of native IPv6 applications?**

If native means IPv6-only, the answer is virtually zero. It doesn’t make business sense to build IPv6-only applications at this time, unless the target environment is self-contained and doesn’t need to interact with any existing IPv4-only node. At the same time, the cost for supporting both IPv4 & IPv6 is negligible. The strategy of an extended overlap period will allow individuals to move at their own pace, without impacting existing operations. During this period, any new applications (like 3degrees.com) that can run self-contained, will find that it is simply cheaper to leave IPv4 out altogether.

The only negative impact of slow development & deployment of IPv6-only applications is on mind-set. People can be myopic and want to see ‘the world is going IPv6-only’ before they bother to worry about making a change. Unfortunately by the time they wake up, the world will have long since left them behind.
B. Transition Costs and Considerations

1. Migration from IPv4 to IPv6 and the Coexistence of Dual Protocols

What are the costs, burdens, and potential problems of ensuring interoperability between IPv6 and IPv4 networks?

Interoperability between IPv6-only & IPv4-only does add a degree of complexity. With respect to end-systems, simultaneous support for both IPv4 & IPv6 will avoid any interoperability problem. The only time IPv6-only makes any sense is for a green-field application, where there is absolutely no need to access any IPv4-only application or data.

There are technologies defined for the cases where IPv6-only to IPv4-only does become a requirement. For example, an aging database server is nearing the end of its life-cycle to be retired soon & is IPv4-only, but the rest of an environment is being built with new IPv6-only mobile appliances. It is expected that when the amortization on the database server ends it will be replaced with an IPv6-capable server. In a scenario like this, it would be appropriate to use a NAT Protocol Translation device in front of the aging database server to get the new application off the ground without the delay that would be incurred until the server is replaced.

What are the incremental costs resulting from operating IPv6 and IPv4 concurrently?

This situation is similar to the incremental costs of running IPv4 alongside its predecessors in the past. One of Cisco’s key success factors in the marketplace has been enabling of migration of applications from legacy protocols such as X.25 to IPv4. For a time there will be concurrent security costs in firewalls, as rules based on IPv4 addresses are replicated for IPv6. Similarly, management of both address spaces will come at some cost.

To what extent will various interoperability solutions continue to function efficiently and effectively as traffic increases?

Some of the transition tools are clearly intended for end-game scenarios (either early or late), but the basics of dual-stack & 6to4 tunneling will scale well. Since IPv6 does not limit one to an either/or scenario, it makes more sense to leave both native and tunneling up and minimize the demand on tunnel-terminating relay routers. Following the preference rules in IETF RFC 3484 will lead to use of native service when available.

Does the operation of dual IPv4/IPv6 equipment impose significant costs relative to IPv4 or IPv6-only equipment?

No. Almost all equipment is capable of more than IPv4-only already, so one more protocol is insignificant. Handset manufacturers complained early on about the memory impact of both protocol stacks, but quickly realized the ~ 10% overhead was easily offset by the operational complexity of trying to manage translation servers.
To what extent do measures to ensure interoperability reduce the performance of network routers, increase routing tables, or have other adverse effects?

In as much as devices must maintain state for both IPv4 and IPv6 networks it is possible that we will see a short term increase the size of the routing table, as discussed above.

What are the costs and benefits of transition mechanisms that allow interoperability among IPv4 and IPv6 hosts and networks, including dual stack, tunneling IPv6 over IPv4 networks, and IPv6-only to IPv4-only translation?

This question requires a lengthy answer and considerable research. Different technologies address different deployment scenarios, including tunneling techniques for both public & private network deployments, as well as one that works in the presence of address translation. Stateful & stateless translators exist that work at each layer in the stack to mask what is happening below them. These technologies should be looked at in the following order to see if they address the need:

(1) Dual Stack – The benefit of dual stack is that it allows IPv4-only apps to continue working (at least as well as they currently do), during the introduction of IPv6 into the environment. By preferring IPv6 (IETF RFC 3484), updated applications will transition at their own pace of deployment. Once IPv4 is no longer used, it can be removed from the environment. The cost of doing this is maintaining and managing both protocols during the overlap. There is a minimal amount of additional DNS overhead necessary to communicate both IPv4 and IPv6 addresses. In as much as multiple queries are made, some amount of latency may be introduced. As previously noted, because multiple mechanisms will be enabled on individual hosts and portions of the network, policies must be kept consistent between IPv4 and IPv6.

(2) Tunneling – If part of the IP infrastructure can’t be moved in the same timeframe as the edges, or other routers, tunneling makes sense. There are tunneling approaches varying between manual configuration and full automation, with higher operating costs on the manual end, and lower costs on the automated end. The tunnel-broker approach sits in between with the Service Provider end automated, while the customer end needs manual establishment. In any case, these approaches present the appearance of an IPv6 network upward, while treating the IPv4 network as a global non-broadcast substrate (much the way IPv4 runs over frame-relay or ATM networks today). The costs for tunnels vary by how much automation there is, and how much impact the extra 20 bytes impacts overall capacity or latency. A configured tunnel presents what looks like a managed circuit between the tunnel ends, so for all operational purposes it can be treated as a circuit. Tunnel broker services automate the ISP end and delegate prefixes based on the authenticated user. The tunnel state is usually more dynamic than a configured tunnel, but may be based on static assignment of a prefix to any individual customer. Automated tunnels like 6to4, ISATAP, and Teredo embed the IPv4 address of the tunnel endpoints into the IPv6 address. This is a simple technique, but has restrictions. 6to4 requires access to public IPv4 addresses on each end, so it won’t work through a NAT. ISATAP allows private IPv4 addresses, but is restricted to use within a private network. Teredo works across the public network, when there are NATs in the path, but is restricted to use from an endpoint rather than a router.

(3) Translation – NAT-PT is like IPv4 NAT in that it translates addresses, but it also translates protocol versions on the fly. It has a limitation in that certain applications may be problematic, as well the inability to de-multiplex multiple devices behind a single transport layer port number.

Is there a “best” or accepted approach that will provide for interoperability between islands of IPv4 and/or IPv6 and the Internet at large?

The best approach in the general case is likely to be dual stack because each node may continue to use IPv4.

What factors may determine whether and where alternative transition mechanisms will be available and applicable?

An overriding concern for consistent policy enforcement may drive use of otherwise suboptimal methods.
Can alternative transmission mechanisms co-exist while still providing end-to-end interoperation among IPv6 and IPv4 networks?

In some cases, yes. It is possible, for instance, for a dual stack node to communicate through a tunnel to another dual stack node. Indeed this will likely happen in as much as tunnels are deployed. However, additional study is needed to understand the limits of interoperability between hosts running separate stacks.

Does the embedded base of IPv4 equipment and applications function as a barrier that could isolate the U.S. from the benefits of foreign IPv6 deployments and/or test beds?

Potentially, the answer to this question is “yes”. Forwarding thinking entrepreneurs might not be able to develop new services based on IPv6 or simply participate to the new economies emerging in other IPv6 geographies. However, U.S. manufacturers have limited resources, if they prematurely deploy IPv6 and realize no gain, the opportunity cost could be too high.

Will domestic and international market forces alone produce a level of network interoperability that maximizes overall social welfare, or will government intervention be needed to produce such an outcome?

Although much of the technology continues to be developed due to external forces, such as foreign markets and government requirements, service providers see little need today to provide IPv6 as a commercial service. Clearly they do not perceive significant demand for end users. In addition, as the Internet industry is still relatively young in historic terms, service providers have yet very immature provisioning systems for IPv4 that must yet be improved in order to drive efficiencies. In large part this is where there minds are today, and not on transition to IPv6. Refer to Part 4 for a more complete discussion.

If government intervention is needed, what form should it take?

As previously discussed, provision of a frequency for IPv6-based mobile networks might further spur development of services geared toward the mobile user. Tax incentives for service providers and enterprises would only provide incentive in as much as they offset additional operating costs of a transition. Put into effect prematurely, the costs of such transitions would be substantial. Should such tax incentives be offered, a mechanism should be provided to ensure that offerings are in fact delivered to the consumer and the enterprise. Another potential tax incentive would be a credit for Enterprises who incur transition costs from IPv4 to IPv6.

What problems, if any, may arise when existing IPv4 networks convert hardware, appliances and middleware to IPv6?

The main operational problem that is anticipated is the need to find all the locations where IPv4 addresses are stored and used. Simply identifying them will require substantial effort, as applications may store addresses reasons unknown to all but the developer.

Will applications that use IP services migrate easily?

Those applications that require a basic interface to the Internet layer will require very minimal changes. Those applications that need to more substantially interact with the Internet layer may require additional changes. In both cases, because the operating models of IPv4 and IPv6 are largely the same, the software necessary to implement IPv6 support will largely mirror that needed to implement IPv4.

Are there estimates of the cost associated with converting existing IPv4 network hardware, appliances and middleware to IPv6?

As previously discussed, if a graceful transition is allowed to occur, the costs of conversion will be minimal; however, if one wishes to migrate to IPv6 now, the costs will vary based on size and scale. Because of the W2K synchronization effect, it is reasonable to assume that a high percentage of hardware-based products will need to be replaced. On the other hand, this upgrade is beginning now as the 3-5 year amortization cycle is ending. Software-based devices may already contain support.
How would the technical requirements for MPLS, ATM, frame relay, Ethernet, and wireless protocol layers and dependencies of protocol layers supported by IPv4 (e.g., UDP and TCP) be impacted by the use of IPv6?

The point of the IP layer (independent of version) is to isolate the upper layers from the morass of technologies below. IPv6 does this just as well as IPv4. In turn, the never-ending list of new lower layer protocols led to a unified address resolution process in IPv6. Whereas IPv4 has a unique address resolution protocol for each lower layer technology, IPv6 has one.

Is the current set of IETF standards for IPv6 technically complete enough to enable widespread commercial deployment of interoperable IPv6 (and IPv4/IPv6 transition mechanisms) networks, equipment and applications?

Since commercial deployments have already started in other parts of the world, the empirical answer would be yes. If there are inadequacies in the ability to deliver something specific to the U.S. market, those will only surface when the U.S. market actually deploys IPv6 in quantity for production use.

Although commercial deployment has already started, management of a native IPv6 network is still a challenge because the working group still has not updated all the components, including MIBs, and billing or provisioning statistics.

Would it be helpful for the IETF standards-track RFCs to define “mandatory” services (e.g., protocol capabilities) and “optional” services?

IETF standards already specify such functions in order to provide for interoperability. It should be noted that the Japanese government is currently sponsoring the IPv6 Ready Logo program that is presently driving IPv6 compliance schemes in Japan. [10]

What problems, if any, may arise in implementing IPv6, as embodied by the IETF standard set, in various types of equipment and software?

Since most operating system vendors already have implemented the IETF set, and demonstrated interoperability at periodic events, there aren’t any obvious ones. IPsec is lacking in some products at this point in time, but that has more to do with historical U.S. government regulations regarding export control on encryption technologies than it does with its ability to make the IPsec technology work over IPv6.

Will the standards create undue hardship on equipment and software providers?

If those standards take the form of procurement requirements or if they are premature, they will harm the U.S. market.

Are additional industry or government specifications required to successfully realize the potential benefits of IPv6?

While additional development of support functions might be necessary over time, at this time the standards necessary to implement IPv6 are mature, for the most part.

2. Security in Transition

To what extent would the simultaneous operation of IPv4 and IPv6 networks and applications, potentially interconnected by a set of diverse transition mechanisms, compromise efforts to safeguard the integrity and security of communications traffic, or limit government’s ability to protect legitimate security and law enforcement interests?

Impacts would be limited to the degree that enforcement infrastructure would need to understand, and endpoints would need to protect, both protocols equally. The fact that one protocol could be carried within the other is not limited to transition, because either protocol could be carried within another header of the same version. Since the enforcement infrastructure needs to be capable of dealing with tunneling in the normal case, the tunneling transition mechanisms don’t introduce any new security concerns. Translation mechanisms could be used to obscure the origin or destination of traffic.
3. Other Transition Concerns

**Does the deployment of IPv6 create address allocation issues for any market segment?**

It simplifies the process for acquiring large blocks to meet a growing demand. Current allocation policies of the Regional Internet Registries (RIRs) restrict direct allocations to ISPs, with the expectation that other market segments will acquire allocations from their ISP.

**How will allocations to end users and end-user devices be affected by IPv6 deployment?**

Because there is no scarcity of IPv6 addresses, the ability of end users to acquire IPv6 addresses will be based on service provider policies. Experience in the U.S. market has shown substantial variance in this area. Some service providers provide a value-added service that includes static IP address allocations, whereas some service providers provide IP addresses gratis. Because a change in mindset is necessary due to the lessening scarcity, it remains to be seen how service providers will support varying IP address allocations.

**Will small and mid-sized ISPs and IT firms have equitable access to the addresses they need?**

The simple technical answer is yes, but local policy and business practice could have an impact. Current allocation policies practices on the IPv4 Internet are that allocations are made by the RIRs to the Internet Service Providers, with ISPs making further assignments to their customers, but any ISP that has a plan to assign addresses to at least 200 customers has the same rights to the minimum /32 allocation as any other. That same RIR policy measures the management efficiency of each ISP in terms of how many /48s they have allocated to customers. Since there is no benefit to the ISP in being more efficient than the /48 metric, it is expected that all IT organizations will be able to get at least that much space. In practical terms, many global corporations would find /48 constraining, but if those organizations ask for more they should be able to get it.

**Are the existing national and international registries technically capable of handling administrative tasks required for IPv6 numbering and addressing?**

Yes for the current policy. Current allocations are: RIPE 293; APNIC 133; ARIN 95; LACNIC 6.

**If not, identify the tasks and the costs for registries to be made capable of handling IPv6 related administrative tasks.**

If the policy were changed to allow direct allocation to non-ISPs, verifying whatever qualifications are in a new policy might require scaling up the staff.
3. Current Status of Domestic and International Deployment

A. Appropriate Metrics to Measure Deployment

What are the most appropriate metrics to gauge IPv6 deployment?

In the short term, the most important factor will likely be application and hardware development, and not deployment.

In the medium term, service providers and RIRs will be able to report the number of customers they have assigned IPv6 address space.

Over the long term, traffic comparisons may prove more appropriate to determine activity of both the IPv6 and IPv4 deployments. In as much as data inspection is available, TCP/UDP/SCTP port information may provide hints as to lagging functionality.

What is sufficient to properly define the IPv6 market – the quantity of equipment purchased, the number of routers acquired, the number of addresses assigned, the number of hosts with IPv6 operating systems, the number of available applications that are IPv6 or IPv6/IPv4 compatible, or the amount of IPv6 traffic?

See above. It will be difficult to measure the IPv6 market based on equipment purchase, because IPv6 and IPv4 are likely to be bundled together by many manufacturers for the foreseeable future.

Are there other metrics or some combination of metrics best suited to characterize the domestic and international penetration of IPv6?

Defining a market requires an unstated context. For vendors or consumers focused on particular segments of the overall market, any of the previously listed metrics might or might not be sufficient. How do they measure the IPv4 market? Some might measure the volume of email that has been carried over IPv6 (email is one example of applications that will be later to market as they do not adhere to clean layering and have overly complex direct interaction with the IP layer). If the goal is to relate the use of IPv6 to the use of IPv4, then traffic volume might provide a simple metric. Other measures might be appropriate as well.

What is the known current volume of deployed native IPv6 and IPv4 network equipment (e.g., hosts, routers, switches)?

Since this is proprietary information, a precise count can’t be known.

To what extent does the pace and extent of IPv6 deployment vary from country to country or region to region (e.g., North America vs. Europe vs. Asia)?

China, Japan & South-Korea are putting emphasis on IPv6 deployments as a catalyst to spur economic growth. As a whole, Asia has the most pressing need, as they have the smallest part of the IPv4 resource pool (which is even more exaggerated by disparity with the population distribution). Thus it is no surprise to see the initial commercial services emerging in that region. It is also no surprise to see the strong emphasis on application development. 11]. The rest of the world currently lags these three countries.

How is that equipment deployed by market segment?

In terms of network/routers deployments, Asia has a lead. In terms of end hosts, there is no clear lead as Windows XP & 2003server, Mac OS-X, as well as recent Linux, and the various flavors of BSD-derived Unix all include IPv6. In the U.S. the routers that are deployed and enabled are primarily in the R&E, and FedNet backbones. The majority of the campus networks attached to those have not enabled IPv6. There is a small number of IPv6-enabled routers in ISP environments.

What is the approximate domestic and global value of all deployed IPv4 and IPv6 equipment?

We refer you to market research firms on total Internet penetration.
What is the percentage (and proportion as compared to IPv4) of known IPv6 deployments by market segment?
We refer you to market research firms on total Internet penetration.

B. Private Sector and Government Deployment Efforts

1. Overall Domestic Efforts

Are technology suppliers producing the necessary hardware, software, applications, training, and any other products and services in sufficient quantity to meet the demand for IPv6 in the United States?
As there is currently very little demand in the United States, the answer to this question is “mostly yes”. There are specific market segments where demand may not be met.

What are the relevant product and service categories and what is the breadth and depth of offerings in those categories. For example, is the market for IPv6 routers characterized by multiple suppliers offering a variety of products, or does only a single supplier produce only a limited number of products?
Routers are, and have been available from multiple suppliers for several years. New operating systems shipped since early 2001 have all had IPv6 available in some form. A few suppliers are still limiting distribution, but this might have more to do with applications and packaging than anything else. The applications segment is clearly lagging and stands to lose its lead to Japan where applications are a major focus. As previously mentioned, service providers currently lack sufficient demand to deliver IPv6 as a service.

For any products and services that are not available or are in limited supply, what is their projected availability in the future, including analysts' estimates and suppliers' business plans?
Business plan-related information is confidential.

How many enterprise network routers are currently IPv6-capable?
The number of enterprise routers capable of routing IPv6 traffic is fairly high. However, once v6 traffic picks up, their legacy devices may require a hardware upgrade. Enterprises that forecast a transition may not want to begin with their existing hardware but just wait for their next round of investment.

How many public or backbone network routers are IPv6-capable?
 Virtually all of them are capable of moving IPv6 packets. Customers that insist on IPv6 service from their ISPs are able to acquire it from multiple providers. If all customers started demanding IPv6 at once, a portion of the backbone routers might need hardware or software updates to align their efficiency of IPv6 traffic handling with the demand.

How does U.S. router deployment compare with other countries?
Router deployments will follow application availability.

How many ISPs are currently capable of handling IPv6 traffic?
In the U.S. only Verio has announced* commercial availability, but there have been private reports that others will provide it if the requestor presses. (*NTT -parent of Verio- announced over 500 global customers in the same press release.) [11] [12] ARIN IPv6 Prefix allocation database as well as the U.S. based IPv6 Internet Exchange Point (IPv6 IX) offers an overview of the U.S. ISP involvement.[13]

What percentage of Internet access customers receive IPv6 capable services?
A very small percentage for native IPv6 services.

What proportion of end-user equipment (e.g., computers, wired and wireless end-user devices, cable modems, DSL modems, printers and other peripheral equipment, and other devices) is capable of handling IPv6 packets?
Approximately 1/3 of the deployed desktop systems are ‘capable’. At this point, virtually all of the rest of the listed equipment is IPv4-only due to lack of U.S. customer demand.
To the extent that such capability is only provisioned in such devices, how easy/costly will it be for users to activate that capability?
For network routers, the network administrators need to configure the protocol. For Windows XP, an IPv6-enabled app can turn on the capability. For Linux, etc. the system administrators need to add documented lines to configuration files. Appliances that are not capable of being upgraded will need to be replaced. The perceived costs for the upgrade will depend on if the upgrade is part of a life-cycle replacement, or explicitly needed to enable a new application. Only the new application path will be counted as a cost for IPv6, and even then it may be written off as the cost for the new application.

How many of the critical functions within an enterprise are IPv6 enabled (e.g., DNS, wireless firewalls)?
As previously mentioned, DNS has been IPv6 capable for some time. However, wireless and firewall functions are far less mature, and generally have not been procured by enterprise yet. Indeed wireless deployment may become a gating factor as many enterprises have just completed capital purchase rounds of this technology.

To the extent possible, what is projected growth for specific products and services, as well as projections among customer segments?
We refer you to market research firms for this information.

2. Domestic Government Efforts

What is the cost of IPv6 research efforts and test beds, including IPv6 deployments in federal research networks (Fednets), the Abilene backbone network, and any other similar efforts, and the expected effects these activities may have on the deployment of IPv6 within the United States?
The 6net project is a European predecessor to the North American test beds, and with 18M € funding over 3 years it has a substantial lead in documenting real-world issues. [14]

What is the current state of IPv6 deployment by other federal, state, and local government agencies?
The normal leading R&D parts of the federal government are operating or testing IPv6, but as usual the rest of the government is waiting for commercial availability (if they are even aware). While this path makes sense for the majority of evolutionary services, IPv6 represents enough of a step that concerted advanced planning by government agencies may be required.
Outside of some interest by the state of Oregon (driven by local Universities), state and local governments are at zero. One specific issue that could be of use to local government agencies is the addressing model. It has been suggested by active community leaders that http://www.ietf.org/internet-drafts/draft-hain-ipv6-pi-addr-06.txt could be used as a basis for replacing street addresses when dealing with government agencies. Another specific value to state & local agencies is the ability to quickly set up ad-hoc event-scene networks to coordinate between agencies.

How do factors like geographic location, population density and/or available expertise impact the costs/benefits for state and local municipalities that are considering IPv6 deployments?
Available expertise is or will be a major factor. A document repository like the one from 6net will be one of the most valuable results from the Moonv6 project.

How will the recent DoD requirement that all Global Information Grid assets be IPv6-capable by 2008 affect the procurement plans and decisions of other federal agencies?
Because they are not removing the capability of IPv4, there is no immediate impact on other agencies. Longer-term impact will be directly related to the degree of interaction between the DoD & each agency.
**What is the current state of IPv6 deployment by state and local government agencies?**

Only the states of Oregon and Florida have even started asking questions. The following institutions are deploying IPv6: FLR (Florida Lambda Rail) NCNI/NCREN (North Carolina Research and Education Network), Boston University. Others will be deploying soon: MAX (Mid-Atlantic Cross Connect), (OARnet) Ohio Academic and Research Network and National Lambda Rail (NLR).

**How do factors like geographic location, population density and/or available expertise impact the costs/benefits for state and local municipalities that are considering IPv6 deployments?**

Rural deployments will rely on expertise from nearby universities, as they do for other technologies. Without a widely distributed research funding model, universities will lack the expertise to provide that assistance.

3. **International Efforts**

**What are current and projected levels of IPv6 deployment across the globe, on both a regional basis (e.g., Europe, Asia, and South America) and on a country specific basis, where available?**

The government of China recently allocated new licenses to build the “China Next Generation Internet (CNGI)” infrastructure. $170 Million has been assigned to 6 providers (5 ISPs + NRN) with a repartition of the cities and IPv6 IX among them. The goal is to be fully operational toward end of CY05. It is clear the carriers are feeling political pressure to showcase China as a technology leader in a new frontier. It was reported that 50% of the CNGI project should go to local vendors.

The European Commission is calling for IPv6 deployment as part of the e-Europe 2005 document.

The Republic of Korea is one of the Asian countries that is now putting emphasis on IPv6.

In Japan, some recently announced service-provider dual-stack service offerings include:

- NTT Com to offer its dual stack service nationwide – 03/13/2003

- NTT Unveils Next-Generation Services Based on New IP Networking Infrastructure
  "the investment will not exceed 500 billion yen in the coming five years," Wada”, NTT President added.

- New strategy of NTT Communications includes IPv6 – 03/18/2003

- Nifty begins ADSL dual stack service – 03/17/2003

- KDDI IPv6 trial includes mobile dual stack service – 03/17/2003

- IPv6 Emerges as Key Part of NTT Com's Global Strategy, Company Exec. VP Says– Oct. 2002

**How have particular initiatives or programs by foreign governments or foreign suppliers helped (or hindered) IPv6 deployment? For example, have government commitments to reach a specific level of IPv6 deployment by a date certain helped spur deployment?**

Outside of Japan this is hard to measure. The tax incentive program in Japan clearly spurred a faster deployment than might otherwise have happened. Now current initiatives in China with
CNGI, and Korea with their e-Korea initiative, they are expected to follow Japan to create the similar demand.

**Are governments devoting significant funding for IPv6 deployment efforts?**
In terms of their GNP, no, but as compared with the U.S., yes. Targeted expenditures at key hurdles appear to be the typical strategy. By comparison, $50M directed to application research in the U.S. would directly offset some of the EC funding.
4. Government's Role in IPv6 Deployment

A. Need for Government Involvement in IPv6 Deployment

1. Reliance on Market Forces

*Given commenters’ views on the current and predicted rates of IPv6 deployment, do commenters believe those rates demonstrate a sufficient uptake of IPv6 in the United States and can they cite specific reasons?*

“Sufficient” presumes a need for uptake. At this time given the linear growth of IPv4 address consumption, the only need for uptake would be due to competitive issues relating to application development or substantial pain in the enterprise market due to NATs. Enterprises are very capable of articulating their pain to us in this regard, if and when it presents itself.

Also maintain leadership position in IT by driving innovation to create applications based on IPv6 and be competitive with the rest of the world, especially over Japan, China and Korea.

2. Potential Market Impediments

a) Technological Interdependencies and the “Chicken and Egg” Problem

*Does a “chicken and egg” relationship exists between IPv6 applications and supporting infrastructure, and if so, how is that relationship manifesting itself in the market for IPv6 products and services?*

Transition mechanisms were specifically designed to avoid this chicken and egg problem, from a technical sense. It remains an open question as to whether and when service providers will offer native IPv6 in America. The two drivers will be consumer or enterprise applications that require IPv6 or are impractical to implement on IPv4 or more basically the additional cost of some of the ameliorations discussed above. If applications are to drive the transition, whether they are be developed elsewhere or in islands of IPv6 connectivity domestically, they can be developed independent of the U.S. market for IPv6 so long as the feature is saleable somewhere in the global market.

Americans have a service that is today sufficient to their actual needs, and they are not going to be willing to pay for development of a service that does not provide a service improvement that is meaningful to their lives. Even were hardware and software completely available and free, service providers will have no incentive to offer a service until Americans see that meaningful improvement.

Since the “chicken and egg” problem is most acute when interrelated products are costly to develop and are highly interdependent (i.e., the end product is a complex and capital intensive system), are those characteristics present for IPv6 infrastructure and applications?

In general it would be true that IPv6 applications and ISP routing services would be interdependent, but the transition technologies were specifically developed to break that dependence. That said, lack of progress by the U.S. application development community hints that the fear of interdependence is still there and as a result developers are reluctant to take the leap of faith.

How does the expected degree of interoperability between IPv6 and IPv4 networks affect this potential chicken and egg problem?

Because the networks can run side by side with each other for quite some time and applications and hosts can avail themselves of either, the chicken and egg problem is minimized.

Will the interoperability between IPv6 and IPv4 reduce potential impediments to the synchronized deployment of IPv6 infrastructure and applications, or will that interoperability merely serve to delay decisions to upgrade infrastructure and applications to IPv6?
This is a scenario-dependent question, and only comes into consideration if someone insists on moving to an IPv6-only network that needs access to IPv4-only systems. Networks that deploy IPv6 alongside IPv4 will find opportunity for new applications. Those that insist on IPv6-only will find the pain of scaling the translation services, and that the applications will be limited to those that work over IPv4/NAT.

**How does the deployment of IPv6 compare to other standards-based technology transitions and does IPv6 present the same or similar concerns that warrant government action?**

IP networking has undergone transitions in the past, albeit smaller in scope. The industry has transitioned from a number of networking protocols to IP. These include AppleTalk, SNA, DECNET, and IPX. So long as the transition begins in a reasonable period of time and can conclude prior to RIRs having to tighten IPv4 allocation policies, government intervention should be limited to training and research opportunities.

**b) Monopoly Power**

**Does any firm or firms have monopoly power for IPv6 products and services, and how would the exercise of such monopoly power affect IPv6 deployment in the United States?**

IPv6 is an open industry standard developed under the auspices of the Internet Assigned Numbers Authority (IANA). Anyone may use the IPv6 standard, including all makers of networking equipment and software. Therefore, we believe it is unlikely that any one company would come to have monopoly power over the implementation of the IPv6 standard or networking products that implement that standard.

**Do IPv4 and IPv6 qualify as direct substitutes making it unlikely that providers of IPv6 equipment, applications, and services will be able to charge excessive prices for their products?**

IPv4 and IPv6 are substitutes. As noted on page {15} above, IPv6 is backward compatible with IPv4. Therefore, any company implementing IPv6 would need to compete with both the huge installed base of IPv4 products, new IPv4 products, and other IPv6 products. Given the existence of this competition, we believe it is unlikely that providers of IPv6 equipment, applications, and services would be able to exploit market power or otherwise charge excessive prices for their products.

**Does IPv6 build on IPv4, allowing an early entrant into the market to establish sufficient market power to impede adequate competition?**

As noted in the response to the two questions immediately preceding this one, both because IPv6 is an industry standard available to anyone, and because networking devices implementing IPv6 will be backward compatible with devices that support only IPv4, it is unlikely that an early adopter of IPv6 would be able to establish market power over IPv6 or any related market for devices that implement IPv6.

**c) Network Externalities**

**What is the magnitude of network externalities that could impede efficient deployment of IPv6?**

The transition technologies defined by the IETF specifically mitigate many of the externalities that would impede deployment. By decoupling the decision points, the value can be realized when both ends are ready, without concern about upgrading devices in between that are outside of local control.

**Will IPv6-based networks will be interoperable to a considerable degree with embedded IPv4 networks and, therefore, allow IPv6 users to communicate with IPv4 users in many instances?**

The recommended strategy is to deploy IPv6 in parallel with IPv4, such that interaction between the protocols is minimized. Technologies do exist that allow such direct communication between
the protocols, so ease of use is a matter of demand, and operator deployment. To the extent that new end devices continue to support IPv4 for interaction with older devices, interoperability problems should be kept to a minimum.

To what extent does that affect the size or scope and timing of any network externalities associated with deployment of IPv6?

Disruptive technology advances that rely on IPv6 capabilities will have an accelerating effect on any transition.

Do network externalities arise, if at all, from all IPv6-based services and applications, or are they limited to specific offerings (e.g., gaming services whose value to individual users likely depends on the number of potential opponents)?

Since IPv6 is plumbing, and most people never look at the plumbing, the decision is really at the application developer and making something new work, or lowering their development cost. Since there is nothing limiting about IPv6, its value would apply to all applications.

Given the early state of IPv6 deployment, is it premature to predicate a case for government intervention at this time on the possible existence of network externalities?

Because we believe the impact of network externalities to be minimal, the government should not intervene on this basis.

How important are network externalities in the U.S. market for domestic firms who want to compete in global markets?

Because IPv6 is intended to be a global standard, there is unlikely to be a US-specific market for IPv6 enabled devices. Any differentiation between products implementing IPv6 that are available in the US and products available elsewhere will likely be based not on the presence or absence of IPv6, but on differences in local consumer demand (for example, the early adoption of 3G mobile in Japan relative to the United States) or of other technology standards which are different between the US and elsewhere (for example, the use of the SONET optical networking standard in the United States versus the use of SDH outside the US).

How important is it to coordinate IPv6 migration to achieve efficient market penetration?

The defined transition tools minimize the need to coordinate deployments. Overall efficiency of the network is achieved over time as independent decisions result in wider deployment of native IPv6 services.

d) Other Impediments

Are there other potential market impediments that may hinder IPv6 deployment in the United States?

Other than the DOD, the U.S. agencies are currently not demanding IPv6 capability in the products and services they buy. Since the government represents the single largest consumer of services in the U.S. market, the lack of demand sets a tone which impedes application development, and in turn, deployment.

3. Public Goods

a) Security

Can the security benefits from IPv6 further the delivery of public goods (important national security, national defense, and law enforcement interests)?

In the general case, we expect that IPv6 to offer the same substrate capabilities as IPv4. However, as previously mentioned IPv6 offers opportunities for exploration in the use of ad-hoc networking for emergency services. Ad-hoc networking capabilities of IPv6 offer emergency services room for exploration in this area.

Would IPv6 features (e.g., expanded address space, auto-configuration) further security-related interests (military command and control and national emergency first responders) requiring government action to speed the deployment of IPv6 in the United States?
Defense department requirements of ad hoc networking will demand specialized support applications to take advantage of IPv6 capabilities. For instance, while it is possible to back four trucks up and create a network, that network still requires name service and management tools that will be specific to this application. In such cases, DoD or other agencies with unique requirements such as those who are tasked as first responders should directly fund development efforts.

*If the private sector fails to sufficiently implement IPsec or other security mechanisms, would government action to accelerate the deployment of IPv6 aid private sector security efforts?*

Key management will be the major hindrance to IPsec deployment that will continue even with IPv6 deployment. The issue of establishing trust relationships has been a stumbling block.

**b) National Competitiveness**

*Given other nations’ announced commitments to IPv6, is U.S. government action to support domestic IPv6 warranted and appropriate in order to preserve the competitiveness of U.S. businesses internationally?*

Through insightful questions in this RFC, the authors have adequately demonstrated the complexity in answering this question. If the government acts hastily and with great force it could hamper development of other necessary technologies, reduce corporate profits, and ultimately put industry at a competitive disadvantage. At the same time, the Internet is a global marketplace built on standards that are available both inside and outside the US, most importantly the TCP/IP protocol. Government support for key areas of Internet research, such as new avenues and markets opened by the larger globally unique address space, would enhance American competitiveness. If, on the other hand, the industry fails to offer IPv6 over the next several years, we may find ourselves with limited ability to communicate to key regions.

*Would the competitiveness of U.S. equipment firms, application developers, and service providers be adversely affected by slower deployment of IPv6 domestically?*

Although Internet equipment manufacturers will likely see little impact as many already respond to international needs, other sectors may feel some impact as their products and services become “Internet enabled”. As previously mentioned, U.S. firms may be adversely impacted by slow deployment of IPv6 if they miss a paradigm shift. The problem with paradigm shifts is that they are not easily predicted or understood. We encourage the department to concern itself in this area.

What is the nature and magnitude of the cost advantages that use of IPv6 (as opposed to IPv4) may confer on a company in a global market context?

Given current corporate applications, we do not expect firms to realize significant cost advantages simply by upgrading to IPv6. However, the government should be mindful of paradigm shifts, as previously discussed.

In as much as IPv6 does afford lowered operational costs, this will reflect itself in national productivity numbers.

**B. Nature of Government Action**

1. **No Government Action**

*What would be the potential costs to the U.S. economy if government inaction results in a domestic implementation of IPv6 that lags other industrialized nations?*

This question has an implied time component to it. If the government chose not to act for two to three years, the impact to American industry would be little to none. Beyond that period, the product life cycle would begin to work against the economy, as companies begin to upgrade their equipment and services outside their normal lifecycle due to impending address space exhaustion.
2. Options for Government Action

a) Government as Information Resource

What would be the costs, benefits and essential elements of an effective clearinghouse program?

One of the things the government did during the early deployment of IPv4 was to act as an information resource. This underappreciated function of documenting and charting an unfamiliar path is still critical for every new effort. Government participation and leadership in industry groups such as the IETF and NANOG could facilitate development of Best Current Practices for agencies and American companies alike.

The Department of Commerce is can also be an excellent vehicle for statistics collection on the nature of IP deployment

b) Government as Consumer

Should the government use its position as a large consumer of information technology products to help spur IPv6 deployment? And could this have any unintended, adverse effects on the market for IPv6 products and services?

The government’s primary consideration as consumer should be on the functions necessary to support government networking and application needs. Government deployment of IPv6 should pace domestic deployment of IPv6, so that agencies and departments can efficiently interact with constituents and transition from IPv4 is not prolonged. Premature use of government buying power may cause suppliers to hurry products to market, causing government to shoulder early adopter expenses or causing suppliers to burden those same costs.

Should procurement policies apply to all government entities, or are there specific classes of agencies that should adopt these policies before others?

A coordinated transition plan will minimize management and support costs by avoiding excessively lengthy transitions.

How should government fund any additional costs (if any) associated with the adoption of IPv6 procurement policies?

Individual departments will need to budget for operational transition costs of support both versions of IP for some period of time. There will be a one time cost for training, planning, and integration of the new version of IP. Once integration of the new stack is complete, ongoing operational costs should return to approximately current levels. The magnitude of any additional funds would depend on the time period of adoption with respect to both routine life-cycle replacement plans, and wide availability of IPv6 capable products.

Are current research and development efforts sufficient?

There remain open areas of research in networking that deserve substantial consideration, which are not currently addressed by either version of IP. For example, the Internet is currently bound by routing limitations where the cost of a multi-homed site is not well borne by that site, but by the network as a whole.

Overall, the existing Fednets & Abilene IPv6 deployments have not driven the community to develop its expertise as that happened with early deployments of IPv4. Today, this has neither resulted in a sharing of expertise, nor development of applications that can leverage the deployed infrastructure.

One specific area of application research might be in efficient K-12 remote learning experiences. Specific areas of research would be in integrating a ‘kid-friendly’ user interface with the complex tools currently used for remote collaboration, and study of curriculum options to effectively present distant information or concepts in the K-12 environment.
Does the government possess research and development tools or resources for IPv6 that are not readily available to the private sector?

Yes. As previously mentioned, RF spectrum is a public resource that could provide a useful research vehicle for new markets.

If the government does provide research and development assistance, what form should it take (e.g., use of government facilities, tax incentives, matching grants, direct funding)?

Matching grants or direct funding of application research requiring the direct peer capabilities of IPv6 is something the government could accomplish. The open market will face explicit training costs until academia starts turning out graduates trained in IPv6. History shows that it doesn’t happen until there is someone doing local research that is available to educate the educators. In addition to expanding the educated base, funded application research will lead to new products and services in the open market.

Should the federal government attempt to spur the growth of IPv6 networks, applications, and services through direct funding of IPv6-related activities, how should these programs be structured and how much would they cost?

Research grants through the University system would simultaneously spur innovative applications, and broaden the base of knowledgeable professors. This has a trickle-down impact on local expertise that will prove valuable in order to begin even planning deployment. Typical grants for application and services research have been around $250,000 per year.

Could existing policies and programs be used to provide such funding, or would new legislative authorization be required?

Research funding is frequently provided through NSF, ARPA/DARPA, NASA, NIST, DoE, and other existing bodies. Focusing the topic of research should be all that is required.

c) Government Funding of IPv6 Deployment

Should the federal government attempt to spur the growth of IPv6 networks, applications, and services through direct funding of IPv6-related activities, how should these programs be structured and how much would they cost?

As previously mentioned, any targeted funding should be timed so that their beneficiaries will be able to accomplish a specific task. As one of those tasks will be making public information accessible, the timing of that task might have the side effect of spurring services. The timing relationship with respect to normal life-cycle replacement will determine the magnitude of any costs.

Could existing policies and programs be used to provide such funding, or would new legislative authorization be required?

We believe that no new funding is required to provide access to information over IPv6.

Should the federal government require state and local agencies to purchase IPv6-capable emergency communication equipment?

Until such time as there are products in the market place it would be premature to make such demands of state and local agencies. However, we recommend that the department work with research bodies to investigate use of ad-hoc networking capabilities in IPv6 to assist first responders.

d) Government IPv6 Mandates

Comment on the authority, the timeline and the benefits for imposing an IPv6 mandate

While it is possible for the government to decide to procure IPv6 service for government use, it is by no means required for the general market.
References:
[8] IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0) [attached]
[9] www.ipv6tf.org
 fuseaction=press&id=571071003304
# IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0)

*Sean Convery (sean@cisco.com)*

*Darrin Miller (dmiller@cisco.com)*

## Table of Contents

1. Introduction ............................................................................................................. 2
   1.1 Caveats .................................................................................................................. 3
2. Overview of IPv4 Topology and Best-Practice Security Rules .............................. 3
3. Threat Analysis ........................................................................................................ 4
   3.1 Attacks with New Considerations in IPv6 ......................................................... 4
      3.1.1 Reconnaissance .............................................................................................. 4
      3.1.2 Unauthorized Access .................................................................................... 7
      3.1.3 Header Manipulation and Fragmentation ...................................................... 11
      3.1.4 Layer 3-Layer 4 Spoofing ............................................................................. 13
      3.1.5 ARP and DHCP Attacks ............................................................................. 15
      3.1.6 Broadcast Amplification Attacks (smurf) ...................................................... 16
      3.1.7 Routing Attacks ............................................................................................ 17
      3.1.8 Viruses and Worms ..................................................................................... 18
      3.1.9 Translation, Transition, and Tunneling Mechanisms .................................... 19
   3.2 Attacks with Strong IPv4 and IPv6 Similarities ................................................ 20
      3.2.1 Sniffing ......................................................................................................... 20
      3.2.2 Application Layer Attacks .......................................................................... 21
      3.2.3 Rogue Devices ............................................................................................. 21
      3.2.4 Man-in-the-Middle Attacks ........................................................................... 21
      3.2.5 Flooding ....................................................................................................... 21
3. Overview of IPv6 Topology and Best-Practice Security Rules .............................. 22
4. Summary .................................................................................................................. 25
5. Acknowledgments .................................................................................................... 25
6. Change Log .............................................................................................................. 26
7. References ................................................................................................................ 26

Appendix A: Current and Future Directions for Research ........................................... 28

Appendix B: Configurations from the Lab ................................................................. 29
1 Introduction

IPv6 [1] security is in many ways the same as IPv4 [2] security. The basic mechanisms for transporting packets across the network stay mostly unchanged, and the upper-layer protocols that transport the actual application data are mostly unaffected. However, because IPv6 mandates the inclusion of IP Security (IPsec) [3], it has often been stated that IPv6 is more secure than IPv4. Although this may be true in an ideal environment with well-coded applications, a robust identity infrastructure, and efficient key management, in reality the same problems that plague IPv4 IPsec deployment will affect IPv6 IPsec deployment. Therefore, IPv6 is usually deployed without cryptographic protections of any kind. Additionally, because most security breaches occur at the application level, even the successful deployment of IPsec with IPv6 does not guarantee any additional security for those attacks beyond the valuable ability to determine the source of the attack.

Some significant differences, however, exist between IPv4 and IPv6 beyond the mandate of IPsec. These differences change the types of attacks IPv6 networks are likely to see. It is also unlikely that the average organization will migrate completely to IPv6 in a short timeframe; rather it will likely maintain IPv4 connectivity throughout the multiyear migration to IPv6. To date, however, there has not been a thorough treatment of the threats such networks will face and the design modifications needed to address these threats.

This paper outlines many of the common known threats against IPv4 and then compares and contrasts how these threats, or similar ones, might affect an IPv6 network. Some new threats specific to IPv6 are also considered. The current capabilities of available products are evaluated, as is how any inherent protocol characteristics of IPv6 affect the nature of the threat. This is prefaced by a brief overview of current best practices around the design of an IPv4 Internet edge network and then followed by a review of how that IPv4 edge network needs to evolve in order to secure the addition of IPv6.

The appendixes of this document highlight the configurations used in the test lab in support of this paper and point to areas of future research. For several points in this paper, reasonable hypotheses are identified but no actual testing has yet been performed. Over time it is the hope of the authors that the community can contribute to the testing of these areas and their results integrated into this document.

This document is meant to benefit the following groups of individuals:

- Network and security architects—This large body of individuals has been responsible for building the Internet today and has remained, with the exception of certain countries, largely disengaged from the IPv6 protocol and its modifications. By reviewing this document, these architects should be able to apply the concepts discussed here to their own areas of the Internet to ensure that as IPv6 is deployed it is done in a secure manner from the outset rather than slowly migrating toward security, as happened with IPv4.

- Security researchers—Reading this document should stimulate further ideas for research in IPv6 security; some ideas are defined in Appendix A.

- IETF members—The IETF [4], the group responsible for the development of the IP protocol, should benefit from a comparative study of the threats in IPv4 as compared to IPv6.

- Government policy makers—The U.S. Department of Defense has stated that it plans a full migration to IPv6 by 2008 [5], spurred in part by its goal for security. Although this goal is admirable, IPv6 is not a panacea for all security problems. Additionally, a substantial investment in the development of new training materials for government employees will be required to meet the 2008 deadline. Furthermore, other groups inside the government have focused on IPv6 as a means to improve Internet security. This document should help such groups identify areas that need attention.

2
1.1 Caveats
IPv6 security is a large and complex subject. It is also one that has seen little examination, except by the group who designed the protocol themselves. Therefore, some topics are not addressed in this document. For example, this document does not address Mobile IP Version 6 (MIPv6) [6], which is still in the draft stage in the IETF. Some of the implications regarding the support of the routing header (a key element in MIPv6) are discussed, but only as the routing header impacts a static IPv6 network.

Additionally, this document focuses on the security requirements of medium to large edge networks on the Internet. These networks typically house some element of public services (Domain Name System [DNS], HTTP, Simple Mail Transfer Protocol [SMTP]) and a filtering router or firewall protecting their internal resources. The document does not address the implications of the threats to service providers (or other core network entities).

Finally, because of the ubiquity of their deployment, Cisco routers are the principal network entity tested in this research. The threats and mitigation techniques described in this document should apply to a network built with any vendor’s equipment, however, and the configurations provided should be easily modified as necessary.

2 Overview of IPv4 Topology and Best-Practice Security Rules

Figure 1 shows a typical IPv4 Internet edge network.

![Diagram of a typical IPv4 Internet edge network]

**Figure 1  Typical IPv4 Internet Edge Network**

In this network, two principal points of network security enforcement are inline: the firewall and the edge router. These devices can be combined into a single device in some cases, or they can have additional security technologies applied to them directly or to companion devices not shown in the figure. These include intrusion detection systems (IDSs), application proxies, and so on. Additionally, each of the public servers can have host security controls such as antivirus software, host intrusion detection, file system integrity checkers, host firewalls, and so on.

This basic design and its countless variations are in use today in thousands of networks around the world. The mechanisms to provide security to networks designed this way are well-understood, as are the limitations of this approach. In support of this paper, a network was built in the lab emulating this design and configurations; and diagrams are provided in Appendix B. The specific techniques used to secure this network for IPv4 threats are summarized in section 3 as each threat is explored.
It should be noted that for larger organizations it is becoming increasingly difficult to identify perimeters within a network. The introduction of IPv6 (or any new core technology) could make things even more perilous without an adequate understanding of the threats identified in section 3.

3 Threat Analysis

This section evaluates and compares threats in IPv4 and in IPv6. It is divided into two main sections, the first of which outlines attacks that significantly change as a result of IPv6, and the second summarizes attacks that do not fundamentally change.

3.1 Attacks with New Considerations in IPv6

The following nine attacks have substantial differences when moved to an IPv6 world. In some cases the attacks are easier, in some cases more difficult, and in others only the method changes.

- Reconnaissance
- Unauthorized access
- Header manipulation and fragmentation
- Layer 3 and Layer 4 spoofing
- Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) attacks
- Broadcast amplification attacks (smurf)
- Routing attacks
- Viruses and worms
- Transition, translation, and tunneling mechanisms

3.1.1 Reconnaissance

The first category of attack is reconnaissance, which also is generally the first attack executed by an adversary. In this attack the adversary attempts to learn as much as possible about the victim network. This includes both active network methods such as scanning as well as more passive data mining such as through search engines or public documents. The active network methods have the goal of giving the adversary specific information about the hosts and network devices used in the victim network, their interconnections with one another, and any avenues of attack that can be theorized based on the evaluation of this data.

3.1.1.1 IPv4 Considerations

In IPv4 the adversary has several well-established methods of collecting this information:

- Ping sweeps—By determining the IPv4 addresses in use at an organization (through active probes, whois lookups, and educated guesses), an adversary can systematically sweep a network with ICMP or Layer 4 “ping” messages that solicit a reply, assuming both query and response are not filtered at the network border. Following this scan, the adversary uses the data to formulate some hypothesis regarding the layout of the victim network. Tools such as traceroute and firewalk can provide further data to aid the adversary.

- Port scans—After identifying reachable systems, the adversary can systematically probe these systems on any number of Layer 4 ports to find services both active and reachable. By discovering hosts with active services, the adversary can then move to the next phase.
• Application and vulnerability scans—The adversary can then probe these active ports by various means to determine the operating system and the version numbers of applications running on the hosts, and even test for the presence of certain well-known vulnerabilities.

Some tools such as Nmap [7] can perform elements of all these scan types at the same time. Attack mitigation techniques for these reconnaissance techniques are generally limited to filtering certain types of messages used by an adversary to identify the resources of the victim network and trying to detect the reconnaissance activity that must be permitted. Reconnaissance activity cannot be stopped completely because the very act of permitting communications with your devices permits some form of reconnaissance.

3.1.1.2 IPv6 Considerations

This section outlines the differences in the reconnaissance attack when moved to IPv6. Because port and application vulnerability scans are identical after a valid address is identified, this section focuses on identifying valid addresses. The first subsection highlights technology differences independent of currently available technology, and the latter outlines current capabilities in this area for the adversary and the defender.

3.1.1.2.1 Technology and Threat Differences

With regard to technology, IPv6 reconnaissance is different from IPv4 reconnaissance in two major ways. The first is that the ping sweep or port scan, when used to enumerate the hosts on a subnet, are much more difficult to complete in an IPv6 network. The second is that new multicast addresses in IPv6 enable an adversary to find a certain set of key systems (routers, Network Time Protocol [NTP] servers, and so on) more easily. Beyond these two differences, reconnaissance techniques in IPv6 are the same as in IPv4. Additionally, IPv6 networks are even more dependent on ICMPv6 to function properly. Aggressive filtering of ICMPv6 can have negative effects on network functions. ICMPv6 filtering alternatives are reviewed in section 3.1.2.

3.1.1.2.1.1 IPv6 Subnet Size Differences

The default subnet size of an IPv6 subnet is 64 bits, or $2^{64}$, versus the most common subnet size in IPv4 of 8 bits, or $2^8$. This increases the scan size to check each host on a subnet by $2^{64} - 2^8$ (approximately 18 quintillion). Additionally, the 64-bit address is derived based on the EUI-64 version of a host MAC address, or in the case of IPv6 privacy extensions [8] (which are enabled by default in Windows XP and available on numerous other platforms), the number is pseudorandom and changes regularly. So a network that ordinarily required only the sending of 256 probes now requires sending more than 18 quintillion probes to cover an entire subnet. Even if we assume that sound network design principles are discounted and that the same 64-bit subnet now contains 10,000 hosts, that still means only one in every 1.8 quadrillion addresses is actually occupied (assuming a uniform random distribution). And even at a scan rate of 1 million probes per second (more than 400 Mbps of traffic), it would take more than 28 years of constant scanning to find the first active host, assuming the first success occurs after iterating through 50 percent of the first 1.8 quadrillion addresses. If we assume a more typical subnet with 100 active hosts, that number jumps to more than 28 centuries of constant 1-million-packet-per-second scanning to find that first host on that first subnet of the victim network.

Now it should be noted that many variables can make this scanning easier for the adversary. First, public services on the Internet edge need to be reachable with DNS, giving the adversary at least a small number of critical hosts within the victim network to attack. Second, the large nature of IPv6 addresses and the lack of a strict requirement for Network Address Translation (NAT) will cause more networks to adopt dynamic DNS or other mechanisms to ensure that even hosts have a valid DNS name (typing FE80:CA01:0:56::ABCD:EF12:3456 to talk to your friend’s PC is no fun). This means that a compromise
of a DNS server within the organization under attack could yield large caches of hosts. Third, administrators may opt for easy-to-remember host addresses for key systems (::10, ::20, ::F00D, and so on) that could be entered into a database used by the scanning tool. These easy-to-remember names could include simply mapping the decimal v4 last octet to the hex v6 last octet, because dual stack will be the norm for years to come (this was done in the lab detailed in Appendix B for convenience). Fourth, by focusing on popular IEEE OUI designations for NIC vendors, an adversary could significantly reduce the number space of $2^{64}$. And finally, by exploiting poorly secured routers or other gateway devices, an adversary could view the IPv6 neighbor-discovery cache data (the functional equivalent of an ARP cache) to find available hosts, or could simply turn on a packet-capture capability such as tcpdump to find addresses available to scan.

Also, like in IPv4 networks, the internal hosts should be protected by a firewall that limits or completely prevents uninitiated conversations from reaching these systems.

The implications of these larger subnets are significant. Today’s network management systems often use ping sweeps as a method of enumerating a network for an administrator. New techniques need to be adopted for this purpose (perhaps neighbor cache checks on routers). Based on initial testing, the neighbor cache is populated on a router only when the device is communicated with by the router (such as sending off-net traffic).

Additionally, this has potentially far-reaching implications for the way Internet worms are propagated, whether they are random address-based or use some form of hierarchical address designations. The basic assumption is that worms will have a much more difficult time propagating in the same manner as they have in IPv4. This is an area that requires further research; some ideas are highlighted in Appendix A.

### 3.1.1.2.1.2 New Multicast Addresses

IPv6 supports new multicast addresses that can enable an adversary to identify key resources on a network and then attack them. These addresses have a node, link, or site-specific domain of use as defined in RFC 2375 [9]. For example, all routers (FF05::2) and all DHCP servers (FF05::3) have a site-specific address. Although this setup clearly has a legitimate use, it is in effect handing the adversary an official list of systems to further attack with simple flooding attacks or something more sophisticated designed to subvert the device. Therefore, it becomes critical that these internal-use addresses are filtered at the border and not reachable from the outside.

### 3.1.1.2.2 Current Technology Capabilities

Today there is no known ping sweep tool for IPv6. Nmap, which supports ping sweeping in v4, elected not to support it in IPv6, most likely for the reasons outlined in section 3.1.1.2.1.1. On the detection side, some IDS systems today (host or network) do not support IPv6, making detection of the scanning activity difficult. This will improve as more vendors ship IPv6 inspection capabilities. Current versions of most popular network firewalls do support IPv6, meaning that filtering various messages to complicate the reconnaissance efforts of the adversary is possible.

On the network management side, very few—if any—network management tools have been developed to deal with the host identification problem outlined in this section.

### 3.1.1.3 Candidate Best Practices

Based on the changes in reconnaissance attacks in IPv6, the following candidate best practices are suggested:

- Implement privacy extensions carefully—Although privacy extensions are a benefit from an obscurity standpoint regarding scanning attacks, they can also make it difficult to trace problems and troubleshoot issues on a network. If a network has a misbehaving host and that host’s address changes regularly, it could be quite difficult to trace the exact host or to determine if the problems are
from one host or many. Better options are to use static addresses for internal communication that are MAC address-based and pseudorandom addresses for traffic destined for the Internet. In addition, this makes current audit capabilities to track worms more challenging because when we track an infection back to a particular subnet, the privacy extensions rotation of the addresses or a machine reboot could make it difficult to identify the infected end host.

- **Filter internal-use IPv6 addresses at the enterprise border routers**—Administrators can define site-local addresses for their organization, including specific multicast addresses such as the all-routers address FF05::2. These site-local addresses can potentially lead to new avenues of attack, so administrators must filter these addresses at the enterprise border routers.

- **Use standard, but nonobvious static addresses for critical systems**—Instead of standardizing on host addresses such as ::10 or ::20, try something that is more difficult for adversaries to guess, such as ::DEF1 for default gateways. This is certainly a “security through obscurity” technique, but because it involves little additional effort on the administrator’s part, its use has no drawbacks. The goal here is to make it difficult for the adversary to guess the global addresses of key systems. Standardizing on a short, fixed pattern for interfaces that should not be directly accessed from the outside allows for a short filter list at the border routers.

- **Filter unneeded services at the firewall**—Like in IPv4, your public and internal systems should not be reachable on services that they do not need to be reached on. Though some are hoping that tools such as IPsec will eliminate the need for firewalls, they will be around for years to come as Layer 3 and 4 filtering is well understood. Until some nontechnical issues (such as the international politics of who controls any trust roots) are resolved, wide-scale deployment of IPsec will be impractical for both IPv4 and IPv6.

- **Selectively filter ICMP**—Because neighbor discovery uses ICMP and fragmentation is done only on end stations (which requires path maximum-transmission-unit discovery [PMTUD]), it is imperative that some ICMP messages be permitted in IPv6. That said, nonessential ICMP messages can be filtered at a firewall, as can ICMP echo and echo-reply messages, if that aspect of manageability can be sacrificed. The author’s recommend that, particularly for IPv6, ICMP echo be enabled in all directions for all hosts, except that inbound ICMP echoes from the Internet to the internal network should be denied. Additionally, IPv6 requires ICMPv6 neighbor discovery-neighbor solicitation (ND-NS) and neighbor discovery-neighbor advertisement (ND-NA) messages to function (described in section 3.1.2), as well as router-solicitation (RS) and router-advertisement (RA) messages if autoconfiguration is used and RA messages are sent from the router for prefix lifetime advertisements. Finally, as in IPv4, packet-too-big messages should be broadly permitted to ensure proper functioning of PMTUD. Section 3.1.2.2.1.3 describes the ICMP messages required in more detail.

- **Maintain host and application security**—Although timely patching and host lockdown are critical elements in IPv4, they are even more critical during the early stages of IPv6 because many host protections (firewalls, IDSs, and so on) do not yet broadly support IPv6. Additionally, it is highly likely (though testing is necessary; refer to Appendix A) that the initial introduction of IPv6 into networks will result in some hosts not being properly secured. It is necessary to focus on maintaining host security to ensure that hosts that are compromised will not become stepping stones to compromise other end hosts.

### 3.1.2 Unauthorized Access

Unauthorized access refers to the class of attacks where the adversary is trying to exploit the open transport policy inherent in the IPv4 protocol. Nothing in the IP protocol stack limits the set of hosts that can establish connectivity to another host on an IP network. Attackers rely upon this fact to establish connectivity to upper-layer protocols and applications on internetworking devices and end hosts.
3.1.2.1 IPv4 Considerations
IPv4 networks have concentrated on limiting unauthorized access by deploying access control technologies within the end systems and on gateway devices in between the IPv4 endpoints. These controls can occur at both Layer 3 and Layer 4. The access control methods in IPv4 get more complex as you move up the protocol stack. At the IP layer, the defender uses basic access control lists (ACLs) to allow only approved hosts to send packets to a device. The ACLs are intended to limit access to or through a device based on security policy and by doing so, limit the available avenues of attack to specific services available on the network. In IPv4 networks, these access controls are implemented in networking devices (firewalls) and on end devices themselves (host firewalls). Although firewalls can implement security policy based on information in the IPv4 headers only, they are best used when combined with upper-layer inspection of TCP/UDP and application layer information.

3.1.2.2 IPv6 Considerations
The need for access control technologies is the same in IPv6 as in IPv4, though eventually the requirement for IPsec may enable easier host access control. The defender wants to limit the ability of the adversary to gain avenues of attack against services on an end host. The ability to do access control based in IPv6 changes not only the information that can be filtered in the Layer 3 header, but also the way the addressing and routing systems of IPv6 are architected. The addressing system of IPv6 changes from that for IPv4 because it includes the ability for one adapter in an IPv6-enabled node to have multiple IPv6 addresses. These multiple IPv6 addresses have significance for communicating on the local subnet (link local - FE80::/10), within an organization (site local – FC00::/16 or FD00::/16 pending working group decision), or on the Internet at large (global unicast addresses – aggregates of prefix binary 001). When the use of these address ranges is combined with the routing system, the network designer can limit access to IPv6 end nodes through IPv6 addressing and routing.

For instance, with IPv6 the network designer can assign global unicast addresses only to devices that need to communicate with the global Internet while assigning site-local addresses to devices that need to communicate only within the organization. Likewise, if a device needs to communicate only within a particular subnet, only the link-local address is needed. Additionally, the use of IPv6 privacy extensions, as mentioned earlier, can limit the time any single IPv6 address is accessible and exposed to a security threat. Beyond the previously stated differences in IPv6, the following sections outline the differences in the unauthorized access attack avenues when the network moves to IPv6. The first subsection highlights the technology differences in the IPv4 and IPv6 header that are independent of currently available technology, and the latter outlines current capabilities in this area for the adversary and the defender.

3.1.2.2.1 Technology and Threat Differences
In IPv6 the basic function of mitigating access to other IP devices based on policy is still implemented with firewalls and ACLs on end hosts and internetworking devices. However, numerous significant differences between the IPv6 and IPv4 headers may change how an administrator deploys these technologies. The following paragraphs discuss some of the areas of difference.

3.1.2.2.1.1 IPsec
When implemented with IPv4 or IPv6, IPsec has similar impacts on the administrator’s ability to enforce security policy with IP header information. The following discussion points apply to both IPv4 and IPv6. If IPsec encryption is implemented from end to end, current firewalls are effective only in applying policy based on Layer 3 information because of the cryptographic protections. If IPv6 uses only the authentication header, it is conceivable that IPv6-capable firewalls could inspect the upper-layer protocols within the authentication-header (AH) encapsulation and permit or deny access to the packet based on that information.
3.1.2.2.1.2 Extension Headers

IP options in IPv4 are replaced with extension headers in IPv6. With this replacement, extension headers may be used in an attempt to circumvent security policy. For example, all IPv6 endpoints are required to accept IPv6 packets with a routing header. It is possible that in addition to accepting IPv6 packets with routing headers, end hosts also process routing headers and forward the packet. With this possibility, routing headers can be used to circumvent security policy implemented on filtering devices such as firewalls [10]. To avoid this possibility, the network manager should designate the specific set of nodes that are to act as MIPv6 home agents (typically the default router for the subnet). The network designer should also validate that the operating systems within their organization do not forward packets that include the routing header. If operating systems that do forward packets that include the routing header are on the network, then the network designer must configure the network to filter the routing header on access control devices. If MIPv6 is not needed, packets with the routing header can be easily dropped at access control devices without relying on the end host to not forward the packets. Although it is easy to start with a “no MIPv6” policy, the emerging applications on handheld devices with WiFi access will make that stance challenging to maintain. For this reason it is best to make sure the end system policy is correctly implemented as “no-forwarding.”

3.1.2.2.1.3 ICMP

ICMPv6 is an integral part of IPv6 operations, even more so than in IPv4. Current best practice for IPv4 firewalling of ICMP is sometimes debated, but it is generally accepted that stringent ICMP filtering is a best practice. In some extreme cases all ICMP messages should be filtered. This blanket prohibitive filtering is simply not possible in IPv6. For the purposes of this document, comparing and contrasting how a generic ICMPv4 policy would translate to ICMPv6 is critical. The following ICMPv4 messages are permitted through the firewall, and all others are denied. The general rules are to permit these messages inbound ICMP from the Internet to a DMZ on a firewall and deny ICMP to the firewall device. These rules may be more or less stringent than a given administrator’s ICMP policy, but are included here only for the sake of demonstration.

- ICMPv4 Type 0 - echo reply
- ICMPv4 Type 3 Code 0 - Destination unreachable net unreachable
- ICMPv4 Type 3 Code 4 – Fragmentation needed but don’t-fragment (DF) bit set
- ICMPv4 Type 8 - Echo request
- ICMPv4 Type 11 - Time exceeded

In contrast, an ICMPv6 firewall policy needs to support additional messages not only through the device but also to and from the firewall device.

ICMPv6 messages required to support equivalent functions to the firewall policy stated previously are as follows:

- ICMPv6 Type 1 Code 0 – No route to destination
- ICMPv6 Type 3 - Time exceeded
- ICMPv6 Type 128 and Type 129 - Echo request and echo reply

New IPv6 messages potentially required to be supported through the firewall device follow:

- ICMPv6 Type 2 - Packet too big—This is required for PMTUD to function correctly because intermediate nodes on an IPv6 network are not allowed to fragment packets. Though allowing PMTUD to function in IPv4 is useful, in IPv6 intermediary devices cannot fragment, so this message becomes more critical to proper network operations.
• ICMPv6 Type 4 - Parameter problem—This is required as an informational message if an IPv6 node cannot complete the processing of a packet because it has a problem identifying a field in the IPv6 header or in an extension header. Further research into the potential abuse of this message type is needed.

ICMPv6 messages potentially required to be supported to and from the firewall device are as follows:
• ICMPv6 Type 2 – Packet too big—The firewall device must be able to generate these messages for proper MTU discovery to take place, because the firewall device cannot fragment IPv6 packets.
• ICMP Type 130-132 - Multicast listener messages—In IPv4, IGMP would need to be permitted for multicast to function properly. In IPv6 a routing device must accept these messages to participate in multicast routing.
• ICMPv6 Type 133/134 – Router solicitation and router advertisement—These are necessary for a variety of reasons, most notably IPv6 end-node autoconfiguration.
• ICMPv6 Type 135/136 – Neighbor solicitation and neighbor advertisement—These messages are used for duplicate address detection and Layer 2 (Ethernet MAC)-to-IPv6 address resolution.
• ICMPv6 Type 4 – Parameter problem—Refer to the previous explanation; this message may be required, but further research is warranted.

3.1.2.2.1.4 Multicast Inspection
Currently most IPv4 firewalls do minimal multicast inspection and filtering. Local-use multicast is integral to the functioning of IPv6. Firewall devices, at a minimum, need to allow the link-local multicast addresses to the firewall in order to provide neighbor discovery. Firewalls in Layer 3 mode should never forward link-layer multicasts. Devices acting as firewalls should inspect all source IPv6 addresses and filter any packets with a multicast source address.

3.1.2.2.1.5 Anycast Inspection
Additionally, although anycast as per RFC 2373 [11] is restricted to routers at this time, operating systems have started to add anycast support to their kernels. This could make anycast usage for services such as DNS or NTP [12] more prevalent in the short term. If this happens, any stateful device (firewall, network IDS [NIDS], server load balancing [SLB]) needs to make feature enhancements to its code to be able to designate an anycast address for inspection and origin servers that listen and respond to the anycast address. If this is done, then when a server that is serving an anycast service answers with its real address the stateful device can map the return traffic to the inbound-initiated traffic with the anycast address. Finally, as has been noted in [13], using IPsec and Internet Key Exchange (IKE) to secure anycast communications has limitations. Work within the IETF is ongoing, but this requirement can potentially be addressed with the use of Group Domain of Interpretation (GDOI) [14].

3.1.2.2.1.6 Transparent Firewalls
Several “Layer 2” or “transparent” firewalls on the market act as bridges while enforcing Layer 3 to Layer 7 policy. In current IPv4 networks, these devices have to be specially programmed to deal with a variety of IP and data link layer interactions such as ARP inspection and DHCPv4. In IPv6 these types of firewalls need to enhance their inspection capabilities to inspect the appropriate IPv6 ICMP and multicast messages. As discussed earlier, ICMPv6 is integral to the proper functioning of an IPv6 network, and a transparent firewall must be able to track the ICMPv6 messages that deal with neighbor discovery, duplicate address detections, autoconfiguration, and multicast management, just to name a few. These capabilities would offer a way to mitigate against attacks that spoof IP-to-MAC address bindings or spoofed DHCP messages. Refer to section 3.1.5 for more discussion on this topic. Additionally, security policy needs to be explicitly defined for the extensive use of multicast addresses in IPv6. For instance, a
bridge must forward all FF02:1 multicast in IPv6. An IPv6 transparent firewall must be able to define filters to forward the link local all multicast nodes (FF02:1) address that is used in IPv6 functions such as autoconfiguration.

3.1.2.2 Current Technology Capabilities
Though many IPv6-capable firewalls are available, many are implementing partial solutions for IPv6 for time-to-market reasons. For example, some IPv6 firewalls understand only a subset of the extension headers in IPv6, and they drop IPv6 traffic that includes these headers. An example is a firewall that does not have logic to process the routing header. If the firewall receives a packet with the routing header, it discards the packet. This behavior has some security benefit when the firewall is protecting hosts that might unpack and forward a packet with a routing header. However, this behavior precludes the firewall from being utilized in an environment that requires MIPv6.

3.1.2.3 Candidate Best Practices
Based on the differences in the IPv6 header and associated extension headers, the following candidate best practices are suggested:

• **Determine what extension headers will be allowed through the access control device**—Network designers should match their IPv6 policy to their IPv4 IP options policy. If any IPv4 IP options are denied on the access control device, the IPv6 access control device should implement the same policies. Additionally, administrators should understand the behavior of the end-host operating system when dealing with the extension headers and dictate security policy based on that behavior. For instance, as noted earlier, the administrator should validate that end-host operating systems do not forward packets that contain a routing header.

• **Determine which ICMPv6 messages are required**—It is recommended that administrators match their policy map closely to the equivalent ICMPv4 policy with the following additions:
  – ICMPv6 Type 2 - Packet too big
  – ICMPv6 Type 4 – Parameter problem
  – ICMPv6 Type 130-132 – Multicast listener
  – ICMPv6 Type 133/134 – Router solicitation and router advertisement
  – ICMPv6 Type 135/136 – Neighbor solicitation and neighbor advertisement

3.1.3 Header Manipulation and Fragmentation
The third category of attack is fragmentation and other header manipulation attacks. This category of attack has been primarily used for one of two purposes. The first purpose is to use fragmentation as a means to evade network security devices, such as NIDS or stateful firewalls. The second purpose of the attack is to use fragmentation or other header manipulation to attack the networking infrastructure directly.

3.1.3.1 IPv4 Considerations
In IPv4 fragmentation is a technique used to fit the IPv4 datagram into the smallest MTU on the path between end hosts. IPv4 fragmentation has been used as a technique to bypass access controls on devices such as routers and firewalls. Fragmentation also has been used to obfuscate attacks in order to bypass network security monitoring products such as NIDS. Most modern firewall and NIDS products go to great lengths to reassemble packets and match the reassembled packets to access control rules or to attack signatures. In general, large amounts of fragmented traffic have been used as an early indicator of an
intrusion attempt because most baselines of Internet traffic indicate that the percentage of fragmented traffic is low [15].

3.1.3.2 IPv6 Considerations

This section outlines the differences in the fragmentation attacks when moved to IPv6. The first subsection highlights technology differences independent of currently available technology, and the latter outlines current capabilities in this area for the adversary and the defender.

3.1.3.2.1 Technology and Threat Differences

IPv6 fragmentation by intermediary devices is prohibited per RFC 2460 (refer to sections 4.5 and 5). One of the most common fragmentation attacks uses overlapping fragments to obfuscate attacks from IPv4 security devices. In IPv6, overlapping fragments is not a proper way of handling fragmentation based on the rules outlined in RFC 2460; these fragments can possibly be viewed as an attack and dropped. Additionally, if the overlapping packets are allowed to bypass the security device, several end-host operating systems drop overlapping fragments in their IPv6 stack software. However, if the end operating system does accept overlapping fragments, there is nothing to prevent the adversary from using fragmented packets in an attempt to bypass the IPv6 security device policy for similar purposes as the IPv4 fragmentation attacks. Additionally, an adversary can still use out-of-order fragments to try to bypass string signatures of a network-based IDS.

RFC 2460 section 5 says “IPv6 minimum MTU is 1280 octets.” For this reason, administrators can allow the security device to drop fragments with less than 1280 octets unless the packet is the last packet in the flow. Administrators can perform this action if the sending operating system fragments the original packet at the MTU supplied by the PMTUD messages and continues to create this size of IPv6 fragments until the last segment of the original packet is delivered. If the host operating system does not behave in this manner, then the security device has to continue to accept and process IPv6 fragments with less than 1280 octets. This behavior would continue to allow obfuscation of attacks by sending large amounts of small fragmented packets. Baselining the fragmentation and reassembly behavior of popular operating systems is necessary to validate the potential of this filtering.

Additional fragmentation issues should be considered for devices that are not configured to do fragment reassembly (routers not running firewall), but are trying to enforce security policy based on Layer 3 and Layer 4 information. For example, in IPv4 some routers have the fragment keyword in the access control entry definition. The only packets that match this IPv4 ACL are those packets that have a fragment offset not equal to zero, that is, noninitial fragments. For IPv4 packets, we know the protocol fragments flags and offset values from the IP header, so we can easily calculate if enough of the upper-layer protocol is within the first fragment to determine the Layer 4 port number. So nonfragmented packets and first fragments go through the normal access-list process and can have the appropriate security policy applied. The combination of multiple extension headers and fragmentation in IPv6 creates the potential that the Layer 4 protocol is not included in the first packet of a fragment set, making it difficult to enforce Layer 4 policy on devices that do not do fragment reassembly. An example of this is a router running Cisco IOS Software without the firewall feature set that does fragment reassembly. With IPv6, Cisco IOS Software matches noninitial IPv6 fragments and the first fragment if the protocol cannot be determined. Cisco IOS Software also supports a new keyword “undetermined transport,” which matches any IPv6 packet where the upper-layer protocol cannot be determined.

3.1.3.2.2 Current Technology Capabilities

Similar to IPv4, current IPv6 firewalls and IDSs implement fragment reassembly and other fragmentation checks in order to mitigate fragmentation attacks. These fragmentation checks include examining out-of-sequence fragments and switching these packets into order, as well as examining the number of fragments from a single IP given a unique identifier to determine denial-of-service (DoS) attacks. IPv6 has no
known fragmentation attack tools, but that does not eliminate the threat that such tools exist or can be
created easily. Firewalls checking for these attacks will want to be matching on source subnets to catch
the case where the adversary is using RFC 3041 addressing to generate fragment streams from what
would appear to be multiple sources.

3.1.3.3 Candidate Best Practices

As stated earlier, though the handling of IPv6 fragmentation is specified to be much different than in
IPv4, the threats in bypassing security devices remain the same. The following candidate best practices
should be considered in IPv6 networks to limit the effectiveness of fragmentation attacks:

• Deny IPv6 fragments destined to an internetworking device when possible—This will limit certain
attacks against the device. However, this filtering should be tested before deployment to ensure that
it does not cause problems in your particular network environment.

• Ensure adequate IPv6 fragmentation filtering capabilities—The combination of multiple extension
headers and fragmentation in IPv6 creates the potential that the Layer 4 protocol will not be included
in the first packet of a fragment set. Security monitoring devices that expect to find the Layer 4
protocol need to account for this possibility and reassemble fragments.

• Drop all fragments with less than 1280 octets (except the last one)—RFC 2460 section 5 says “IPv6
minimum MTU is 1280 octets.” For this reason security devices may be able to drop any IPv6
fragment with less than 1280 octets unless it is the last fragment in the packet. More testing is
necessary in this area, as specified in section 3.1.3.2.1. A case that should be noted is for Layer 2
firewalls and IPv4 routers transporting a tunnel. There is no requirement that IPv6 packets be 1280
octets or more between Layer 3 interfaces, just that if the packet is fragmented, the fragments must
be reassembled at the receiving interface before forwarding. This is done specifically to allow
tunneling over IPv4 networks where the MTU might be less than 1280. In that case, IPv4 is
architecturally Layer 2.

3.1.4 Layer 3-Layer 4 Spoofing

A key element enabling numerous different types of IP attacks is the ability for an adversary to modify
their source IP address and the ports they are communicating on to appear as though traffic initiated from
another location or another application. This so-called “spoofing” attack is prevalent despite the presence
of best practices to mitigate the usefulness of the attack.

3.1.4.1 IPv4 Considerations

Today in IPv4, spoofing attacks (principally Layer 3-based) occur every day. They can make DoS, spam,
and worm or virus attacks more difficult to track down. Layer 3 spoofing attacks are not generally used in
interactive attacks as return traffic routes to the spoofed location, requiring the adversary to “guess” what
the return traffic contains (not an easy proposition for TCP-based attacks because TCP has 32-bit
sequence numbers). Layer 4 spoofing can be used in interactive attacks in order to make traffic appear to
come from a location it did not (such as injecting false Simple Network Management Protocol (SNMP)
messages or syslog entries). RFC 2827 [16] specifies methods to implement ingress filtering to prevent
spoofed Layer 3 traffic at its origin. Unfortunately such filtering is not broadly implemented, and because
it requires widespread usage to have a significant benefit, spoofed traffic is still very common. It is
important to note that RFC 2827 ensures that only the network portion of an address is not spoofed, not
the host portion. So in the 24-bit subnet 192.0.2.0/24, RFC 2827 filtering ensures that traffic originating
from 192.0.3.0 is dropped but does not stop an adversary from spoofing all the hosts within the
192.0.2.0/24 subnet assigned to a broadcast domain. RFC 2827 does allow the administrator to track
attacks to a particular organization, and tracking is one of the first steps to accountability.
In addition to stopping the spoofing of valid ranges within the IPv4 address space, a large body of addresses have not been allocated [17] in IPv4, and reserved addresses exist that will likely never be allocated [18]. These ranges can be globally blocked, and attacks that attempt to use those spoofed ranges can be identified and stopped at network choke points as implemented with a security policy.

### 3.1.4.2 IPv6 Considerations

This section outlines the differences in Layer 3 and Layer 4 spoofing attacks when moved to IPv6. The first subsection highlights technology differences independent of currently available technology, and the latter outlines current capabilities in this area for the adversary and the defender.

#### 3.1.4.2.1 Technology and Threat Differences

One of the most promising benefits of IPv6 from a Layer 3 spoofing perspective is the globally aggregated nature of IPv6 addresses. Unlike IPv4, the IPv6 allocations are set up in such a way as to easily be summarized at different points in the network. This allows RFC 2827-like filtering to be put in place by Internet service providers (ISPs) to ensure that at least their own customers are not spoofing outside their own ranges. Unfortunately this is not required standard behavior, and it requires conscious implementation on the part of operators. Layer 4 spoofing attacks are not changed in any way, because Layer 4 protocols do not change in IPv6 with regard to spoofing. Just be aware that subnets are much larger in IPv6, so even with RFC 2827-like filtering an adversary can spoof an enormous range of addresses.

From a transition standpoint, the various tunneling mechanisms offer the ability for an adversary with either IPv4 or IPv6 connectivity to send traffic to the other version of IP while masking the true source. As an example, adversaries can use 6to4 relay routers to inject traffic into an IPv6 network with very little ability to trace back to the true source [19]. It should be noted that this is no worse than the inability to trace IPv4, but simple checks at the relay, such as making sure the outer IPv4 source matches the address embedded in the IPv6 source, enhances traceback from the IPv6 destination.

#### 3.1.4.2.2 Current Technology Capabilities

Currently Layer 3 spoofing can be mitigated using the same techniques as in IPv4 with standard ACLs. Layer 4 spoofing is not changed in any way. Spoofed traffic can be detected using IPv6-capable firewalls or IDSs. Currently no techniques are available to mitigate the spoofing of the 64 bits of host address space available in IPv6. What would be useful in IPv6 networks (and IPv4 networks as well) is a method to correlate IP, MAC, and Layer 2 port pairings for traffic. This data could be stored by the switch and then polled by or sent to a management station, enabling the operator to quickly determine the physical switch port on which a given IP address is communicating.

#### 3.1.4.3 Candidate Best Practices

Based on the changes in Layer 3 and Layer 4 spoofing attacks in IPv6, the following candidate best practices are suggested:

- **Implement RFC 2827-like filtering and encourage your ISP to do the same**—At least containing spoofed traffic to the host portion of the IPv6 address provides a large benefit for at least tracing the attack back to the originating network segment.

- **Document procedures for last-hop traceback**—With the large range of spoofable addresses in a IPv6 subnet, it is critical that when an attack does occur you have mechanisms to determine the true physical source of the traffic. This generally entails some combination of Layer 2 and Layer 3 information gleaned from switches and routers.
• Use cryptographic protections where critical—If an application uses strong cryptographic protections, a successful spoof attack is meaningless without also subverting the cryptographic functions on the device.

3.1.5 ARP and DHCP Attacks

ARP and DHCP attacks attempt to subvert the host initialization process or a device that a host accesses for transit. This generally involves the subversion of host bootstrap conversations through either rogue or compromised devices or spoofed communications. These attacks try to get end hosts to communicate with an unauthorized or compromised device or to be configured with incorrect network information such as default gateway, DNS server IP addresses, and so on.

3.1.5.1 IPv4 Considerations

DHCP uses a broadcast message from the client when it initially boots up, allowing a rogue DHCP server to attempt to respond to the host before the valid DHCP server is able to. This allows the rogue server to set critical connectivity settings, including default gateway and DNS server, thus enabling man-in-the-middle attacks. Additionally, DHCP messages can be spoofed, allowing an adversary to consume all available DHCP messages on the server.

ARP attacks center around spoofing ARP information to cause the IP-MAC binding of a particular host to be changed so that the IP address remains valid but the victims communicate with the adversary’s MAC address. This is most often done to spoof the default gateway.

Technologies have been developed in IPv4 to address some of these attack types. For example, Cisco has a feature in Ethernet switches called DHCP snooping [20], which allows certain ports designated as “trusted” to participate in DHCP responses while most of the other ports are configured to allow sending only DHCP client messages. Additionally, a feature called ARP inspection [21] performs similar protections for ARP. Furthermore, some IDS systems can detect certain types of ARP misuse.

3.1.5.2 IPv6 Considerations

This section outlines the differences in ARP and DHCP attacks when moved to IPv6. The first subsection highlights technology differences independent of currently available technology, and the latter outlines current capabilities in this area for the adversary and the defender.

3.1.5.2.1 Technology and Threat Differences

In IPv6, unfortunately, no inherent security is added on to the IPv6 equivalents of DHCP or ARP. Because stateless autoconfiguration (a lightweight DHCP-like functionality provided in ICMPv6) can provide a viable alternative to DHCP in many cases, dedicated DHCP servers are not common in IPv6 and are not even broadly available in modern server operating systems. Dedicated DHCPv6 servers may appear in order to offer additional configuration parameters such as DNS servers, time servers, IP telephony servers, and so on, so a level of DHCP protection is still required. Unfortunately, stateless autoconfiguration messages can be spoofed, and spoofing can be used to deny access to devices. To mitigate this, the trusted port concept should be used in conjunction with router-advertised messages.

In IPv6, rather than continue with a unique version of ARP for every media type, ARP is replaced with elements of ICMPv6 called neighbor discovery. Neighbor discovery has the same inherent security as ARP in IPv4. Though the possibility of enabling some sort of more secure neighbor discovery using IPsec exists, this is far from standardized, and it involves unique implementation considerations because of the added security. The Securing Neighbor Discovery (SEND) [22] working group in the IETF is working on a solution to this problem. At present, both router and neighbor-solicitation and -advertisement messages can be spoofed and will overwrite existing neighbor-discovery cache information on a device, resulting in
the same issues present in IPv4 ARP. For instance, a spoofed router discovery could inject a bogus router address that hosts listen to and perhaps choose for their default gateway; the bogus router can record traffic and forward it through the proper routers without detection.

These ARP spoofing-like attacks have not been implemented in any publicly available test code, so some unique considerations may appear after such code is released and tested. Although DHCPv6 is investigating security options, the protocol is too new to be considered in this paper. At a minimum the approaches used for protecting DHCP in IPv4 networks should be implemented for IPv6.

3.1.5.2.2 Current Technology Capabilities

No security tools are available today to help detect or stop DHCPv6, autoconfiguration, or neighbor-discovery abuses in IPv6. These messages can be filtered at a router or firewall like any ICMP message, but because most of these attacks are locally significant only, this will have minimal benefit. The neighbor-discovery attacks have not been implemented in any publicly available test code for IPv6, so some unique considerations may appear after such code is released and tested. Getting the equivalent inspection capability that is now present in IPv4 would help mitigate this threat.

3.1.5.3 Candidate Best Practices

Without the ability to detect the misuse of neighbor-discovery messages or to secure their transport, best practices are limited to the following:

- *Use static neighbor entries for critical systems*—In highly sensitive environments you can specify that a system has a static entry to its default router and avoid many of the typical neighbor-discovery attacks. This is a very administratively burdensome practice and should not be undertaken lightly.

3.1.6 Broadcast Amplification Attacks (smurf)

Broadcast amplification attacks, commonly referred to as “smurf” attacks, are a DoS attack tool that takes advantage of the ability to send an echo-request message with a destination address of a subnet broadcast and a spoofed source address, using the victim’s IP. All end hosts on the subnet respond to the spoofed source address and flood the victim with echo-reply messages.

3.1.6.1 IPv4 Considerations

Documented in the late 1990s, this common attack has a simple mitigation method in IPv4 networks. If IPv4-directed broadcasts are disabled on the router, when an adversary sends an echo-request message to the broadcast address of the IP subnet they end up sending one echo-reply message to the victim, as opposed to replies from all the devices on the network. According to Best Current Practice (BCP) 34 [23], the default behavior for IP routers is to turn IP-directed broadcasts off. The command `no ip directed broadcasts` is the default for Cisco IOS Software Version 12.0 and later. This specific attack is becoming less common, but can still be used to create an effective DoS attack. A current website still monitors smurf attack-capable subnets.

3.1.6.2 IPv6 Considerations

This section outlines the differences in broadcast amplification attacks when moved to IPv6. The first subsection highlights technology differences independent of currently available technology, and the latter outlines current capabilities in this area for the adversary and the defender.
3.1.6.2.1 Technology and Threat Differences
In IPv6 the concept of an IP-directed broadcast is removed from the protocol and specific language is added to the protocol designed to mitigate these types of attacks. Specifically with regard to a smurf attack, RFC 2463 [24] states that an ICMPv6 message should not be generated as a response to a packet with an IPv6 multicast destination address, a link-layer multicast address, or a link-layer broadcast address (RFC 2463 section 2.2). If end nodes are compliant to RFC 2463, then smurf and other amplification attacks used against IPv4 are not an issue in IPv6 networks.

3.1.6.2.2 Current Technology Capabilities
Our testing has shown that several popular operating systems comply with the RFC and do not respond to an echo request directed at the link-local all nodes multicast address sourced from a spoofed address. Some ambiguity still exists in the standard about whether end nodes should respond to ICMP messages with global multicast addresses as the source address. If the end nodes do respond to these multicast addresses, then an adversary could make an amplification attack on the multicast infrastructure that may cause a DoS due to resource consumption on the internetworking devices.

3.1.6.3 Candidate Best Practices
• Implement ingress filtering of packets with IPv6 multicast source addresses—There is no valid reason for a multicast source address, so the administrator should drop any packets with a multicast source address at the border of the enterprise.

No other candidate best practices will be available until amplification attacks are discovered in IPv6. Specific testing needs to be performed on a range of operating system end nodes to determine their behavior when responding to an ICMP packet sourced with a global multicast address.

3.1.7 Routing Attacks
Routing attacks focus on disrupting or redirecting traffic flow in a network. This is accomplished in a variety of ways, ranging from flooding attacks, rapid announcement and removal of routes, and bogus announcement of routes. Particulars of the attacks vary, depending on the protocol being used.

3.1.7.1 IPv4 Considerations
In IPv4, routing protocols are commonly protected using cryptographic authentication to secure the routing announcements between peers. The most common implementation is a Message Digest Algorithm 5 (MD5) authentication with a preshared key between routing peers.

3.1.7.2 IPv6 Considerations
This section outlines the differences in several routing protocols underlying security mechanisms when moved to IPv6. The first subsection highlights technology differences independent of currently available technology, and the latter outlines current capabilities in this area for the adversary and the defender.

3.1.7.2.1 Technology and Threat Differences
Several protocols do not change their security mechanism when transitioning from IPv4 to IPv6. Multiprotocol Border Gateway Protocol (BGP) was extended to carry IPv6 interdomain routing information in RFC 2545 [25]. As such, BGP continues to rely on TCP MD5 for authentication. The Intermediate System-to-Intermediate System (IS-IS) protocol [26] was extended in a draft specification [27] to support IPv6, but the extension does not change the underlying authentication of IS-IS. Originally, IS-IS provided for the authentication of link-state packets (LSPs) through the inclusion of authentication
information as part of the LSP. However, the simple password authentication was not encrypted. RFC 3567 [28] adds a cryptographic authentication to IS-IS, and this cryptographic authentication will continue to be used to protect IS-IS for IPv6 traffic.

In Open Shortest Path First Version 3 (OSPFv3) [29], the authentication fields of the OSPF header are removed. Routing Information Protocol Next-Generation (RIPng) [30] has also removed the authentication from the protocol specification. OSPF and RIPng rely on IPsec AH and Encapsulating Security Payload (ESP) headers to provide integrity, authentication, confidentiality, and antireplay protection of routing information exchanges. Additional work is being done to secure both IPv4 and IPv6 protocols, such as the “The Generalized TTL Security Mechanism” [31]. This mechanism is also applicable to IPv6-specific protocols if the Hop-Limit field in the IPv6 header is used to protect a protocol stack.

3.1.7.2.2 Current Technology Capabilities
The security mechanisms to secure protocols that have changed with IPv6, OSPFv3, and RIPng are implemented inconsistently across internetworking vendors.

3.1.7.3 Candidate Best Practices
- Use traditional authentication mechanisms on BGP and IS-IS.
- Use IPsec to secure protocols such as OSPFv3 and RIPng—This is dependant on functioning vendor implementations.

*Use IPv6 hop limits to protect network devices*—Investigate vendor implementations of IPv6 hop limits to protect the protocol stack from attack. For instance, a basic technique is to start the time to live (TTL) of 255 for a valid peer and ensure that the resulting TTL accepted by the router is high enough to prevent acceptance of a spoofed packet that has come from a different part of the infrastructure.

3.1.8 Viruses and Worms
Viruses and worms remain one of the most significant problems in IP networking today, with almost all of the most damaging publicly disclosed attacks in recent years having a virus or worm at its nexus.

3.1.8.1 IPv4 Considerations
In IPv4, viruses and worms not only damage the hosts themselves but also can damage the transport of the network through the increased burden to routers and mail servers around the Internet. SQL slammer [32], for example, caused massive network flooding due in part to the rate with which it scanned the network (each attack packet was a single UDP message). Timely patching, host antivirus, and early detection followed by perimeter blocking have been the three techniques used in IPv4. Early detection is most easily performed with anomaly detection systems such as those available from Arbor Networks. Additionally, newer host-based IDS products can intercept certain system calls that would have caused the compromise in the system.

3.1.8.2 IPv6 Considerations
This section outlines the differences in virus and worm attacks when moved to IPv6. The first subsection highlights technology differences independent of currently available technology, and the latter outlines current capabilities in this area for the adversary and the defender.
3.1.8.2.1 Technology and Threat Differences
A traditional virus in no way changes with IPv6. E-mail based viruses or those that infect removable media remain as you would expect. However, worms or viruses and worms that use some form of Internet scanning to find vulnerable hosts may experience significant barriers to propagation in IPv6 due to the issues raised in section 3.1.1. Further research is necessary to identify how significant a change this would be or what techniques the worm writer could employ to improve its propagation efficiency. It would seem that a SQL slammer-type worm would be far less effective in an IPv6 environment because of its inability to find hosts to infect and thus its inability to bring about the flooding result.

3.1.8.2.2 Current Technology Capabilities
The three mitigation techniques currently used in IPv4 are all still available in IPv6. There is not, however, broad IPv6 support in the host IDS products currently available. Additionally, the information provided by routers to aid in anomaly detection is not as extensive in IPv6 at this time.

3.1.8.3 Candidate Best Practices
Beyond establishing techniques to make local attack traceback easier, there are no best practice changes with virus and worm attacks. All the mechanisms from IPv4 (when the products support IPv6) work properly.

3.1.9 Translation, Transition, and Tunneling Mechanisms
Much thought and attention has been paid to how IPv4 networks will be transitioned to IPv6 networks. Additionally, work has already started on evaluating the security implications of the IPv4-to-IPv6 migration techniques. This section does not attempt to analyze these mechanisms in detail, but instead summarizes the security research efforts and provides observations.

Several approaches to transitioning from IPv4 to IPv6 networks exist. These approaches fall into the following categories:

- Dual stack
- Tunneling
- Translation

The existence of so many transition technologies creates a situation in which network designers need to understand the security implications of the transition technologies and select the appropriate transition technology for their enterprise. The previous sections of this document assumed that the end hosts and networking infrastructure were dual stacked when discussing IPv6 native access. The following outlines some of the issues when the end hosts are not dual stacked and must rely on tunneling or translation technologies for IPv4 communications.

3.1.9.1 Issues and Observations
- With regard to IPv6 tunneling technologies and firewalls, if the network designer does not consider IPv6 tunneling when defining security policy, unauthorized traffic could possibly traverse the firewall in tunnels. This is similar to the issue with Instant Messaging (IM) and file sharing applications using TCP port 80 out of enterprises with IPv4.
- As noted in many of the transition studies done, automatic tunneling mechanisms are susceptible to packet forgery and DoS attacks. These risks are the same as in IPv4, but increase the number of paths of exploitation for adversaries.
Tunneling overlays are considered nonbroadcast multiaccess (NBMA) networks to IPv6 and require the network designer to consider this fact in the network security design. The network designer must consider this when deploying automatic or static tunneling.

Relay translation technologies introduce automatic tunneling with third parties and additional DoS vectors. These risks do not change from IPv4, but do provide new avenues for exploitation [33]. These avenues can be limited by restricting the routing advertisements of relays to internal or external customers.

Static IPv6 in IPv4 tunneling is preferred because explicit allows and disallows are in the policy on the edge devices.

Translation techniques outlined for IPv6 have been analyzed [34] and shown to suffer from similar spoofing and DoS issues as IPv4-only translation technologies.

IPv6-to-IPv4 translation and relay techniques can defeat active defense traceback efforts hiding the origin of an attack.

When focusing on host security on a dual-stack device, be aware that applications can be subject to attack on both IPv6 and IPv4. Therefore, any host controls (firewalls, VPN clients, IDSs, and so on) should block traffic from both IP versions when a block is necessary. For example, when split tunneling is disabled on an IPv4 VPN client, that VPN client should block IPv6 split tunneling as well, even if the VPN service does not expressly support IPv6. IPv4 to IPv6 transition attack tools are already available that can spoof, redirect, and launch DoS attacks.

### 3.1.9.2 Candidate Best Practices

General recommendations for enterprises when considering IPv6-to-IPv4 transition techniques include the following:

- **Use dual stack as your preferred IPv6 migration choice**—Use either native IPv4 or IPv6 access to services but not translation because the security issues are better understood and policy implementations can be simplified.

- **Use static tunneling rather than dynamic tunneling**—This allows the administrator to establish a trust relationship between tunnel endpoints and continue to implement inbound and outbound security policy.

- **Implement outbound filtering on firewall devices to allow only authorized tunneling endpoints**—Examples are filtering outbound IP Protocol 41 for 6to4 tunneling and UDP port 3544 for Teredo-based tunneling.

### 3.2 Attacks with Strong IPv4 and IPv6 Similarities

This section outlines attacks that are not fundamentally altered by IPv6:

- **Sniffing**
- **Application layer attacks**
- **Rogue devices**
- **Man-in-the-middle attacks**
- **Flooding**

#### 3.2.1 Sniffing

Sniffing refers to the class of attacks that involves capturing data in transit across a network. The most common example of this is Tcpdump, which is included in most UNIX-like operating systems. An
adversary executing sniffing attacks can often determine login credentials or view sensitive information in plaintext protocols. Although IPv6 provides fundamental technology to prevent sniffing with IPsec, it does not provide any simplification for the key management issues that have proved to be challenging. Until the key management issues (among others) are resolved, deployment of IPsec will be stalled and sniffing attacks will continue to be possible.

### 3.2.2 Application Layer Attacks

Application layer attacks refer to all the attacks performed at Layer 7 of the OSI model. This is the bulk of all attacks on the Internet today, and the vulnerabilities that enable these attacks represent the source of most of the insecurities in today’s networks. General attacks such as buffer overflows, Web application attacks (Common Gateway Interface [CGI] and so on), and viruses and worms all fall into this category. IPv4 and IPv6 are both, for the most part, neutral parties to application layer attacks. Certainly if the protocol had adopted more stringent authentication of IP addresses some of these attacks could be more easily traced, but the bulk of any blame in application layer attacks lies in the affected application, not the underlying transport.

Even assuming the worldwide implementation of IPsec, application layer attacks change very little with IPv6 adoption. Even though a given connection can be cryptographically protected, there is nothing to stop an application layer attack from traversing the encrypted link and causing the same damage as if it were in the clear. The only difference is that tracing back the attack may prove easier because of the authentication in cases where Layer 3 information could otherwise be spoofed.

However, if IPsec is more ubiquitously deployed from end station to end station, without some mechanism for key, all security protections will fall to the host. Because all a firewall or IDS sees is encrypted traffic, it cannot make any decisions based on such data.

### 3.2.3 Rogue Devices

Rogue devices are devices introduced into the network that are not authorized. Although this could most easily be a simple unauthorized laptop, more interesting for an adversary would be a rogue wireless access point, DHCP or DNS server, router, or switch. These attacks are fairly common in IPv4 networks and are not substantially changed in IPv6. If IPsec were ever used in a more comprehensive way in the IPv6 protocol (including device bootstrap), authentication for devices could mitigate this attack somewhat. The 802.1x standard also has the potential to help here, though an undetected rogue device could funnel 802.1x authentication sequences to a compromised node acting as a AAA server while capturing valid credentials.

### 3.2.4 Man-in-the-Middle Attacks

Because the IPv4 and IPv6 headers have no security mechanisms themselves, each protocol relies on the IPsec protocol suite for security. In this fashion IPv6 falls prey to the same security risks posed by a man in the middle attacking the IPsec protocol suite, specifically IKE. Tools that can attack an IKE aggressive mode negotiation and derive a preshared key are documented. With this in mind, we recommend using IKE main mode negotiations when requiring the use of preshared keys. IKEv2 is expected to address this issue in the future.

### 3.2.5 Flooding

Though certainly the increase in IP addresses that can be spoofed may make flooding attacks more difficult to trace, the core principles of a flooding attack remain the same in IPv6. Whether a local or a
distributed DoS attack, flooding a network device or host with more traffic than it is able to process—or more than the link can transmit—is an easy way to take a resource out of service. The same techniques used to locate and trace back DoS attacks in IPv4 can be used in IPv6, though new techniques may be available. This is an area for further research, and is highlighted in Appendix A.

4 Overview of IPv6 Topology and Best-Practice Security Rules

After migrating the typical IPv4 Internet edge network to a dual-stack IPv4 or IPv6 design, the topology itself does not change, as shown in Figure 2.

![Figure 2 Candidate Design of Dual-Stack IPv4 or IPv6 Internet Edge Network](image)

As was discussed in section 3, many threats that have different attack vectors or different levels of impact in an IPv6 network. The impact of these changes can be seen in the configurations provided in Appendix B. This section briefly highlights high-level best-practice differences in the dual-stack design vs. IPv4 only. The candidate best practices presented throughout section 3 are then included for easy reference.

Some of the main considerations for deployment of a dual-stack Internet edge are ensuring that you have good configuration change control and monitoring for your firewall and edge router. For example, the configuration of the IPv4-only firewall in the test lab was just over 200 lines long. When v6 is added, the configuration is over 300 lines long. Just like in any device, as the configuration size increases, so does the chance for error. Combine that with the fact that these hosts now have two distinct protocols on which they can be attacked as well as a lack of broad IPv6 support in current security technologies, and the chance that the adversary will find a new way into your network with IPv6 increases.

One interesting best-practice shift not already discussed in this document is how bogon filtering changes with IPv6. In IPv4, because so much of the IPv4 range has been allocated, it is generally easier to block bogons than it is to permit nonbogons. In IPv6, only three top-level aggregation identifiers (TLAs) have been allocated thus far. The Internet Assigned Numbers Authority (IANA) maintains a document [35] listing the most current list of IPv6 TLA assignments. The three currently allocated follow:

- 2001:/16 – Main IPv6 production block with sub-TLA assignments to the RIRs—Periodically tracking the /23s allocated to the regional Internet registries (RIRs) will allow even tighter protection.
- 2002:/16 – 6to4 tunneling—Hosts using 6to4 may still need to communicate with your IPv6 hosts. The IPv4 bogon list is applicable to the subsequent 32 bits.
- 3FFE:/16 – 6Bone testing—This range is deprecated and scheduled to be vacated by June 6, 2006.

Therefore, ACLs can permit these ranges (and certain multicast ranges if used) and block all other IPv6 traffic. This certainly does not prevent you from receiving spoofed traffic because the ranges that have
been allocated are immense, but it stops obviously malicious or malformed traffic using unallocated addresses.

The other main change to the filtering practices in the IPv6 portion of the dual-stack configuration is the additional ICMP types that may be necessary, as discussed in section 3.1.2.

The following lists the candidate best practices presented throughout section 3. They are listed as candidate because without more broad testing and input from the community they cannot be construed as anything more than a best guess:

- **Implement privacy extensions carefully**—Although privacy extensions are a benefit from an obscurity standpoint regarding scanning attacks, they can also make it difficult to trace problems and troubleshoot issues on a network. If a network has a misbehaving host and that host’s address changes regularly, it could be quite difficult to trace the exact host or to determine if the problems are from one host or many. Better options are to use static addresses for internal communication that are MAC address-based and pseudorandom addresses for traffic destined for the Internet. In addition, this makes current audit capabilities to track worms more challenging because when we track an infection back to a particular subnet, the privacy extensions rotation of the addresses or a machine reboot could make it difficult to identify the infected end host.

- **Filter internal-use IPv6 addresses at the enterprise border routers**—Administrators can define site-local addresses for their organization, including specific multicast addresses such as the all-routers address FF05::2. These site-local addresses can potentially lead to new avenues of attack, so administrators must filter these addresses at the enterprise border routers.

- **Use standard, but nonobvious static addresses for critical systems**—Instead of standardizing on host addresses such as ::10 or ::20, try something that is more difficult for adversaries to guess, such as ::DEF1 for default gateways. This is certainly a “security through obscurity” technique, but because it involves little additional effort on the administrator’s part, its use has no drawbacks. The goal here is to make it difficult for the adversary to guess the global addresses of key systems. Standardizing on a short, fixed pattern for interfaces that should not be directly accessed from the outside allows for a short filter list at the border routers.

- **Filter unneeded services at the firewall**—Like in IPv4, your public and internal systems should not be reachable on services that they do not need to be reached on. Though some are hoping that tools such as IPsec will eliminate the need for firewalls, they will be around for years to come as Layer 3 and 4 filtering is well understood. Until some nontechnical issues (such as the international politics of who controls any trust roots) are resolved, wide-scale deployment of IPsec will be impractical for both IPv4 and IPv6.

- **Selectively filter ICMP**—Because neighbor discovery uses ICMP and fragmentation is done only on end stations (which requires path maximum-transmission-unit discovery [PMTUD]), it is imperative that some ICMP messages be permitted in IPv6. That said, nonessential ICMP messages can be filtered at a firewall, as can ICMP echo and echo-reply messages, if that aspect of manageability can be sacrificed. The author’s recommend that, particularly for IPv6, ICMP echo be enabled in all directions for all hosts, except that inbound ICMP echoes from the Internet to the internal network should be denied. Additionally, IPv6 requires ICMPv6 neighbor discovery-neighbor solicitation (ND-NS) and neighbor discovery-neighbor advertisement (ND-NA) messages to function (described in section 3.1.2), as well as router-solicitation (RS) and router-advertisement (RA) messages if autoconfiguration is used and RA messages are sent from the router for prefix lifetime advertisements. Finally, as in IPv4, packet-too-big messages should be broadly permitted to ensure proper functioning of PMTUD. Section 3.1.2.2.1.3 describes the ICMP messages required in more detail.

- **Maintain host and application security**—Although timely patching and host lockdown are critical elements in IPv4, they are even more critical during the early stages of IPv6 because many host
protections (firewalls, IDSs, and so on) do not yet broadly support IPv6. Additionally, it is highly likely (though testing is necessary; refer to Appendix A) that the initial introduction of IPv6 into networks will result in some hosts not being properly secured. It is necessary to focus on maintaining host security to ensure that hosts that are compromised will not become stepping stones to compromise other end hosts.

• **Determine what extension headers will be allowed through the access control device**—Network designers should match their IPv6 policy to their IPv4 IP options policy. If any IPv4 IP options are denied on the access control device, the IPv6 access control device should implement the same policies. Additionally, administrators should understand the behavior of the end-host operating system when dealing with the extension headers and dictate security policy based on that behavior. For instance, as noted earlier, the administrator should validate that end-host operating systems do not forward packets that contain a routing header.

• **Determine which ICMPv6 messages are required**—It is recommended that administrators match their policy map closely to the equivalent ICMPv4 policy with the following additions:
  - ICMPv6 Type 2 - Packet too big
  - ICMPv6 Type 4 – Parameter problem
  - ICMPv6 Type 130-132 – Multicast listener
  - ICMPv6 Type 133/134 – Router solicitation and router advertisement
  - ICMPv6 Type 135/136 – Neighbor solicitation and neighbor advertisement

• **Deny IPv6 fragments destined to an internetworking device when possible**—This will limit certain attacks against the device. However, this filtering should be tested before deployment to ensure that it does not cause problems in your particular network environment.

• **Ensure adequate IPv6 fragmentation filtering capabilities**—The combination of multiple extension headers and fragmentation in IPv6 creates the potential that the Layer 4 protocol will not be included in the first packet of a fragment set. Security monitoring devices that expect to find the Layer 4 protocol need to account for this possibility and reassemble fragments.

• **Drop all fragments with less than 1280 octets (except the last one)**—RFC 2460 section 5 says “IPv6 minimum MTU is 1280 octets.” For this reason security devices may be able to drop any IPv6 fragment with less than 1280 octets unless it is the last fragment in the packet. More testing is necessary in this area, as specified in section 3.1.3.2.1. A case that should be noted is for Layer 2 firewalls and IPv4 routers transporting a tunnel. There is no requirement that IPv6 packets be 1280 octets or more between Layer 3 interfaces, just that if the packet is fragmented, the fragments must be reassembled at the receiving interface before forwarding. This is done specifically to allow tunneling over IPv4 networks where the MTU might be less than 1280. In that case, IPv4 is architecturally Layer 2.

• **Implement RFC 2827-like filtering and encourage your ISP to do the same**—At least containing spoofed traffic to the host portion of the IPv6 address provides a large benefit for at least tracing the attack back to the originating network segment.

• **Document procedures for last-hop traceback**—With the large range of spoofable addresses in a IPv6 subnet, it is critical that when an attack does occur you have mechanisms to determine the true physical source of the traffic. This generally entails some combination of Layer 2 and Layer 3 information gleaned from switches and routers.

• **Use cryptographic protections where critical**—If an application uses strong cryptographic protections, a successful spoof attack is meaningless without also subverting the cryptographic functions on the device.
• **Use static neighbor entries for critical systems**—In highly sensitive environments you can specify that a system has a static entry to its default router and avoid many of the typical neighbor-discovery attacks. This is a very administratively burdensome practice and should not be undertaken lightly.

• **Implement ingress filtering of packets with IPv6 multicast source addresses**—There is no valid reason for a multicast source address, so the administrator should drop any packets with a multicast source address at the border of the enterprise.

• **Use traditional authentication mechanisms on BGP and IS-IS.**

• **Use IPsec to secure protocols such as OSPFv3 and RIPng**—This is dependant on functioning vendor implementations.

• **Use IPv6 hop limits to protect network devices**—Investigate vendor implementations of IPv6 hop limits to protect the protocol stack from attack. For instance, a basic technique is to start the time to live (TTL) of 255 for a valid peer and ensure that the resulting TTL accepted by the router is high enough to prevent acceptance of a spoofed packet that has come from a different part of the infrastructure.

• **Use dual stack as your preferred IPv6 migration choice**—Use either native IPv4 or IPv6 access to services but not translation because the security issues are better understood and policy implementations can be simplified.

• **Use static tunneling rather than dynamic tunneling**—This allows the administrator to establish a trust relationship between tunnel endpoints and continue to implement inbound and outbound security policy.

• **Implement outbound filtering on firewall devices to allow only authorized tunneling endpoints**—Examples are filtering outbound IP Protocol 41 for 6to4 tunneling and UDP port 3544 for Teredo-based tunneling.

## 5 Summary

As shown in this paper, IPv6 has both benefits and drawbacks from a security standpoint. The opportunity to ensure secure IPv6 deployments from the outset rather than a slow migration toward security, as occurred with IPv4, should be strongly considered by the Internet community. However, the amount of attention that IPv6 security has so far received is quite low, and new considerations will certainly be uncovered. Without adequate training and attention on the part of network operators to the new considerations with IPv6 security, it will be very difficult to ensure a smooth transition (or any transition at all) to IPv6.

This paper has introduced you to the security issues and candidate best practices surrounding the introduction of IPv6 into the enterprise network, with or without IPsec. With this understanding, you should be able to identify areas that need further research in your own network, or begin to think about how a migration to dual-stack IPv6 might occur. When ready, the information in this paper will aid you in modifying your security policies to account for IPv6 and in the beginning to test the suitability of the best practices in this document as applied to your own network. Ongoing research will continue to refine the contents of this paper and provide more information on candidate best practices and technology updates.

## 6 Acknowledgments

The authors wish to thank all the reviewers of this document, including Steve Acheson, Bora Akyol, John Bashinski, Liang Gao, Craig Huegen, Franjo Majstor, Shannon McFarland, Steve Pollock, Gavin Reid, Mike Schiffman, and Andrew Wright, and a special thanks to Tony Hain for his extensive support of this document.
7 Change Log
08 MAR 2004 – Initial Version 1.0 Released

8 References


Appendix A: Current and Future Directions for Research

Numerous areas regarding IPv6 need further research. This section briefly outlines some ideas.

First is the notion of system identification within an organization. With the advent of privacy extensions and the size of the IPv6 ranges in use, identifying systems within an organization and, in particular, identifying misbehaving hosts can be quite difficult and problematic. This document explores these problems and some potential solutions, but more research is needed in this area.

Second, the increased dependence on multicast addresses in IPv6 could have some interesting implications with flooding attacks. For example, all routers, NTP servers, and so on have site-specific multicast addresses. Can these addresses be used as a form of amplification attack much like the smurf attack in IPv4?

Third, because neighbor discovery is a new addition to IPv6 and because it is an essential component of a well-run IPv6 network, it should be exhaustively tested from a security standpoint. For example, can the neighbor-discovery cache fall victim to a resource starvation attack in any of the currently deployed neighbor-discovery implementations? Can the CPU of a device be exhausted by processing neighbor-discovery information?

Fourth, with a new header configuration, new extension headers, and new ICMP message types, there may be novel ways to deal with flooding attacks. At the very least, the various extensions proposed for IPv4 to deal with flooding attacks should be examined for applicability in IPv6.

Fifth, because IPv6 is new and security information on the protocol is not widespread, it is the opinions of the authors that a large number of dual-stack hosts may be more exposed to attack with IPv6 than they currently are in IPv4. Within the limits of the law, it would be very useful to actively scan such systems to confirm or debunk this theory and get a sense of the magnitude of the issues with currently deployed IPv6 security. This same testing can include vulnerability scans of default operating system installs against IPv4 and IPv6.

Finally, though some work has been done in this area, it would be useful to examine how some of the recent Internet worms might have fared in an IPv6 environment. This should certainly examine worms such as SQL slammer and also theoretical worms that have not yet seen release. New ways that future worms might better react to with respect to the size of the IPv6 range should also be explored. Such research should consider if any differences in propagation rate occur with only our current TLAs allocated or some time in the far future with higher-speed links and a much larger percentage of addresses allocated from the 128-bit IPv6 range. The expected increase in heterogeneity of IPv6 devices as compared to IPv4 should also be considered (refrigerators, and so on being connected to the network).
Appendix B: Configurations from the Lab

Figure B1 shows the lab topology first shown just for the IPv4 component of the lab:

The enterprise represented by Figure B1 controls the configuration of router “FW” and router “ENT”. ENT is acting as the WAN router to the ISP, and FW is acting as the FW router between the Internet and the internal network. The relevant configuration components of router ENT are as follows:

**Figure B1  Lab Topology – IPv4**

The enterprise represented by Figure B1 controls the configuration of router “FW” and router “ENT”. ENT is acting as the WAN router to the ISP, and FW is acting as the FW router between the Internet and the internal network. The relevant configuration components of router ENT are as follows:
version 12.3
!
hostname ENT
!
boot-start-marker
boot system flash:c2600-ik9o3s3-mz.123-3.bin
boot-end-marker
ip cef
!
!
interface FastEthernet0/0
  ip address 172.19.93.178 255.255.255.240
  ! This is the primary inbound ACL for basic bogon filtering
  ! and anti-spoof filtering
  ip access-group 101 in
  ! Enable unicast RPF checking for anti-spoofing
  ip verify unicast reverse-path
  ! Basic best practices regarding the handling of certain ICMP
  ! types
  no ip redirects
  no ip unreachables
  no ip proxy-arp
!
interface FastEthernet0/1
  ip address 172.19.93.193 255.255.255.240
  ! This is the last point of egress filtering before traffic is sent to the ISP
  ip access-group 102 in
  ! Enable unicast RPF checking for anti-spoofing
  ip verify unicast reverse-path
  ! Basic best practices regarding the handling of certain ICMP
  ! types
  no ip redirects
  no ip unreachables
  no ip proxy-arp
!
! This entire lab was built using static routing
ip route 0.0.0.0 0.0.0.0 172.19.93.177
ip route 172.19.93.208 255.255.255.240 172.19.93.194
ip route 172.19.93.224 255.255.255.240 172.19.93.194
!
!
logging trap warnings

! Log back to the syslog daemon on dell2
logging 172.19.93.228

! ACL limiting access to NTP to the actual NTP server we are
! communicating with
access-list 96 permit 171.68.10.80
access-list 96 deny   any log

! Bogon filtering (RFC 3330) Note that RFC 1918 private
! ranges are not filtered since these are used in the test
! lab. Also RFC 2827 filtering is implemented via unicast RPF
! filtering as opposed to explicit ACL entries
access-list 101 deny   ip 0.0.0.0 0.255.255.255 any
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any
access-list 101 deny   ip 169.254.0.0 0.0.255.255 any
access-list 101 deny   ip 192.0.2.0 0.0.0.255 any
access-list 101 deny   ip 198.18.0.0 0.1.255.255 any

! Filter multicast ranges, not a good idea if you route
! multicast with your ISP
access-list 101 deny   ip 224.0.0.0 15.255.255.255 any
access-list 101 deny   ip 240.0.0.0 15.255.255.255 any

! Standard IPv4 ICMP filtering best practices, drop fragments
! and allow messages which are needed. Note, in this lab ICMP
! echo and echo-reply was broadly permitted to ease testing
! in a production network more restrictive filtering is
! probably warranted.
access-list 101 deny   icmp any any fragments
access-list 101 permit icmp any any echo
access-list 101 permit icmp any any echo-reply
access-list 101 permit icmp any any packet-too-big
access-list 101 permit icmp any any time-exceeded
access-list 101 deny   icmp any any
access-list 101 permit ip any any

! Inbound on the internal facing interface basic ICMP
! filtering is all that is present.
! RFC 2827 filtering is implemented using unicast RPF
! filtering
access-list 102 deny   icmp any any fragments
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
access-list 102 permit icmp any any packet-too-big
access-list 102 permit icmp any any time-exceeded
access-list 102 deny   icmp any any
access-list 102 permit ip any any
ntp clock-period 17179981
ntp access-group peer 96
ntp server 171.68.10.80

end

Note that not all router hardening steps are shown here nor should this be assumed a fully locked down IPv4 router config. The following is the IPv4 configuration for the FW device:

! version 12.3
!
hostname FW
!
boot-start-marker
boot system tftp c2600-bino3s-mz.ipv6_eft 172.19.93.228
boot-end-marker
!
ip cef
!

! The following commands setup the parameters for the IOS firewall, they have not been tuned in any way. The
! inspection name for the v4 firewall is “v4_fw”.
ip inspect audit-trail
ip inspect max-incomplete low 150
ip inspect max-incomplete high 250
ip inspect one-minute low 100
ip inspect one-minute high 200
ip inspect udp idle-time 20
ip inspect dns-timeout 3
ip inspect tcp idle-time 1800
ip inspect tcp finwait-time 3
ip inspect tcp synwait-time 15
ip inspect tcp max-incomplete host 40 block-time 0
ip inspect name v4_fw tcp timeout 300
ip inspect name v4_fw udp
ip inspect name v4_fw tftp
ip inspect name v4_fw http
ip inspect name v4_fw fragment maximum 256 timeout 1
!

interface FastEthernet0/0
ip address 172.19.93.194 255.255.255.240
! This is the primary inbound ACL for traffic sent from the Internet which has passed by the ENT router. As a note, with IOS FW, the return traffic does not need to be explicitly permitted. This functionality is facilitated with the "ip inspect" command.

ip access-group 101 in
! Enable unicast RPF checking for anti-spoofing
ip verify unicast reverse-path
! Basic best practices regarding the handling of certain ICMP types
no ip redirects
no ip unreachables
no ip proxy-arp
! enable IOS FW functionality on this interface
ip inspect v4_fw in
!

interface FastEthernet0/1
ip address 172.19.93.225 255.255.255.240
! This is the primary ACL for traffic originated from the internal network
ip access-group 103 in
! Enable unicast RPF checking for anti-spoofing
ip verify unicast reverse-path
! Basic best practices regarding the handling of certain ICMP types
no ip redirects
no ip unreachables
no ip proxy-arp
! enable IOS FW functionality on this interface
ip inspect v4_fw in
!

interface Ethernet1/0
ip address 172.19.93.209 255.255.255.240
! This is the primary ACL for traffic originated within the public server segment (DMZ)
ip access-group 102 in
! Enable unicast RPF checking for anti-spoofing
ip verify unicast reverse-path
! Basic best practices regarding the handling of certain ICMP types
no ip redirects
no ip unreachables
no ip proxy-arp
! enable IOS FW functionality on this interface
  ip inspect v4_fw in

! no ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 172.19.93.193
!
!
! Enable logging to the syslog daemon on dell2
logging 172.19.93.228
! ACL to control access to NTP
access-list 96 permit 171.68.10.80
access-list 96 deny any log
! Access-list 101 is the inbound ACL for outside traffic
! ICMP filtering best practices
access-list 101 deny icmp any any fragments
access-list 101 permit icmp any any echo
access-list 101 permit icmp any any echo-reply
access-list 101 permit icmp any any packet-too-big
access-list 101 permit icmp any any time-exceeded
access-list 101 deny icmp any any
! ACL entry to facilitate remote lab access (not needed in
! production)
access-list 101 permit ip any host 172.19.93.194
! ACL entry allowing SSH access to the entire DMZ network for
! testing, Not needed or desirable in production
access-list 101 permit tcp any 172.19.93.208 0.0.0.15 eq 22
! Standard ACL entries to permit access to the SMTP and DNS
! listeners at this IP address, these functions are merged on
! a single device in the test lab but in most situations will
! be on separate machines
access-list 101 permit tcp any host 172.19.93.211 eq smtp
access-list 101 permit tcp any host 172.19.93.211 eq domain
access-list 101 permit udp any host 172.19.93.211 eq domain
! Permit access to the .210 on web and ftp
access-list 101 permit tcp any host 172.19.93.210 eq www
access-list 101 permit tcp any host 172.19.93.210 eq ftp
! ACL entry to permit remote SSH access to the dell2 machine,
! not needed or desirable in a production network
access-list 101 permit tcp any host 172.19.93.228 eq 22
! ACL entries to permit syslog and TFTP access from the ENT
! router to the syslog and TFTP listeners on dell2
access-list 101 permit udp host 172.19.93.193 host 172.19.93.228 eq syslog
access-list 101 permit udp host 172.19.93.193 host 172.19.93.228 eq tftp
! deny all other traffic and log the event including the
! input source
access-list 101 deny ip any any log-input
! Standard ICMP filtering
access-list 102 deny icmp any any
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
access-list 102 permit icmp any any packet-too-big
access-list 102 permit icmp any any time-exceeded
access-list 102 deny icmp any any
! Permit both public servers to send syslog to the syslog
! listener on dell2
access-list 102 permit udp 172.19.93.210 0.0.0.1 host 172.19.93.228 eq syslog
! Permit SSH and TFTP from these servers to dell2 for testing
access-list 102 permit udp 172.19.93.210 0.0.0.1 host 172.19.93.228 eq tftp
access-list 102 permit tcp 172.19.93.210 0.0.0.1 host 172.19.93.228 eq 22
! Permit the outside SMTP server to transfer incoming mail
! via SMTP
access-list 102 permit tcp host 172.19.93.211 host 172.19.93.228 eq smtp
! Deny any other access to the internal network
access-list 102 deny ip any 172.19.93.224 0.0.0.15
! Allow the two public servers to initiate outbound requests
! for DNS, SSH, WWW Proxy, and VNC. In a production network
! this would be far more limited but these permits were
! entered for testing.
access-list 102 permit tcp 172.19.93.210 0.0.0.1 any eq domain
access-list 102 permit udp 172.19.92.210 0.0.0.1 any eq domain
access-list 102 permit tcp 172.19.93.210 0.0.0.1 any eq 22
access-list 102 permit tcp 172.19.93.210 0.0.0.1 any eq www
access-list 102 permit tcp 172.19.93.210 0.0.0.1 any eq 3128
access-list 102 permit tcp 172.19.93.210 0.0.0.1 any eq 1080
! Deny any other traffic and log the input source
access-list 102 deny ip any any log-input
! Basic ICMP filtering
access-list 103 deny icmp any any
access-list 103 permit icmp any any echo
access-list 103 permit icmp any any echo-reply
access-list 103 permit icmp any any packet-too-big
access-list 103 permit icmp any any time-exceeded
access-list 103 deny icmp any any
! Permit SSH access from the internal network to the public
! servers. In a production network this should be locked down
! to the specific hosts that need access.
access-list 103 permit tcp 172.19.93.224 0.0.0.15 172.19.93.210 0.0.0.1 eq 22
! Permit web and ftp requests of surftech
access-list 103 permit tcp 172.19.93.224 0.0.0.15 host 172.19.93.210 eq www
access-list 103 permit tcp 172.19.93.224 0.0.0.15 host 172.19.93.210 eq ftp
! Permit mail and DNS requests of pipeline, In a production
! network this would be much more locked down to the specific
! hosts required
access-list 103 permit tcp 172.19.93.224 0.0.0.15 host 172.19.93.211 eq smtp
access-list 103 permit tcp 172.19.93.224 0.0.0.15 host 172.19.93.211 eq domain
access-list 103 permit udp 172.19.93.224 0.0.0.15 host 172.19.93.211 eq domain
! Deny any other traffic to the DMZ and log
access-list 103 deny ip any 172.19.93.208 0.0.0.15 log-input
! Allow the internal network to initiate outbound requests
! for DNS, SSH, WWW Proxy, and VNC. In a production network
! this would be far more limited but these permits were
! entered for testing. In almost all cases additional
! services need to be opened up to the Internet to enable
! other applications in a production network.
access-list 103 permit tcp 172.19.93.224 0.0.0.15 any eq 22
access-list 103 permit tcp 172.19.93.224 0.0.0.15 any eq telnet
access-list 103 permit tcp 172.19.93.224 0.0.0.15 any eq www
access-list 103 permit tcp 172.19.93.224 0.0.0.15 any eq domain
access-list 103 permit udp 172.19.93.224 0.0.0.15 any eq domain
access-list 103 permit tcp 172.19.93.224 0.0.0.15 any eq 3128
access-list 103 permit tcp 172.19.93.224 0.0.0.15 any eq 1080
! Allow outbound TFTP, normally not needed but used for
! testing
access-list 103 permit udp 172.19.93.224 0.0.0.15 any eq tftp
! Allow TFTP responses from dell2 to the FW inside interface.
! This is needed because the IOS FW does not operate on
! traffic it originates itself.
access-list 103 permit udp host 172.19.93.228 eq tftp host 172.19.93.225 gt 1023
! Deny all other traffic and log
access-list 103 deny ip any any log-input
!
ntp clock-period 17208089
ntp access-group peer 96
ntp server 171.68.10.80
!
end
The lab topology now with v6 addresses added in addition to v4 is shown in figure B2:

Figure B2  Lab Topology – IPv4 and IPv6
The configuration for device “ENT” is as follows showing the IPv6 additions and not the v4 elements:

```mermaid
! version 12.3
!
hostname ENT
!
```
boot system flash:c2600-ik9o3s3-mz.123-3.bin

ipv6 unicast-routing
ipv6 cef

interface FastEthernet0/0
ipv6 address 3FFE:C15:C002:46::2/64
ipv6 traffic-filter inbound in
ipv6 rip v6 enable
ipv6 cef

interface FastEthernet0/1
ipv6 address 3FFE:C15:C002:47::1/64
ipv6 traffic-filter outbound in
ipv6 rip v6 enable
ipv6 cef

ipv6 router rip v6

ipv6 access-list inbound
! deny all traffic with a routing header or undetermined transport
! deny ipv6 any any routing
! deny ipv6 any any undetermined-transport
! permit link local traffic between routers
  permit ipv6 FE80::/10 FE80::/10
! permit rip traffic
  permit ipv6 FE80::/10 host FF02::9
! permit assigned TLAs to talk to our subnets, note that this is a significant departure from v4 bogon filtering in that since only 3 TLAs have actually been assigned, it is easier to expressly permit these TLAs then deny all other traffic than it is to block any of the special use, multicast, or other traffic normally associated with bogon filtering
  permit ipv6 2001::/16 host 3FFE:C15:C002:46::2
  permit ipv6 2001::/16 3FFE:C15:C002:47::/64
  permit ipv6 2001::/16 3FFE:C15:C002:48::/64
  permit ipv6 2001::/16 3FFE:C15:C002:49::/64
  permit ipv6 2002::/16 host 3FFE:C15:C002:46::2
  permit ipv6 2002::/16 3FFE:C15:C002:47::/64
permit ipv6 2002::/16 3FFE:C15:C002:48::/64
permit ipv6 2002::/16 3FFE:C15:C002:49::/64
permit ipv6 3FFE::/16 host 3FFE:C15:C002:46::2
permit ipv6 3FFE::/16 3FFE:C15:C002:47::/64
permit ipv6 3FFE::/16 3FFE:C15:C002:48::/64
permit ipv6 3FFE::/16 3FFE:C15:C002:49::/64
! permit ND messages
permit icmp any any nd-na
permit icmp any any nd-ns
! deny all other traffic
sequence 210 deny ipv6 any any log
!
ipv6 access-list outbound
! deny all traffic with a routing header or undetermined transport
! deny ipv6 any any routing
! deny ipv6 any any undetermined-transport
! permit link local traffic between routers
permit ipv6 FE80::/10 FE80::/10
! permit rip traffic
permit ipv6 FE80::/10 host FE02::9
! permit our subnets to talk to the TLAs (and the local router)
permit ipv6 3FFE:C15:C002:47::/64 host 3FFE:C15:C002:47::1
permit ipv6 3FFE:C15:C002:47::/64 2001::/16
permit ipv6 3FFE:C15:C002:47::/64 2002::/16
permit ipv6 3FFE:C15:C002:47::/64 3FFE::/16
permit ipv6 3FFE:C15:C002:48::/64 host 3FFE:C15:C002:47::1
permit ipv6 3FFE:C15:C002:48::/64 2001::/16
permit ipv6 3FFE:C15:C002:48::/64 2002::/16
permit ipv6 3FFE:C15:C002:48::/64 3FFE::/16
permit ipv6 3FFE:C15:C002:49::/64 host 3FFE:C15:C002:47::1
permit ipv6 3FFE:C15:C002:49::/64 2001::/16
permit ipv6 3FFE:C15:C002:49::/64 2002::/16
permit ipv6 3FFE:C15:C002:49::/64 3FFE::/16
! permit ND messages
permit icmp any any nd-na
permit icmp any any nd-ns
! deny all other traffic
deny ipv6 any any log
!
end
The configuration for the IPv6 portion of device FW is as follows. Note that bogon/TLA filtering is not done here because it has already been done on device ENT. For extra protection do the filtering in both places.

```
!  
version 12.3  
!  
hostname FW  
!  
! note this is an EFT image used for this testing. IPv6 stateful firewallowing is  
! not currently shipping in IOS as of this writing  
boot system tftp c2600-bino3s-mz.ipv6_eft 172.19.93.228  
!  
ipv6 unicast-routing  
!  
! Default values were used for the IPv6 firewallowing variables  
ipv6 inspect audit-trail  
ipv6 inspect max-incomplete low 150  
ipv6 inspect max-incomplete high 250  
ipv6 inspect one-minute low 100  
ipv6 inspect one-minute high 200  
ipv6 inspect udp idle-time 20  
ipv6 inspect tcp idle-time 1800  
ipv6 inspect tcp finwait-time 3  
ipv6 inspect tcp synwait-time 15  
ipv6 inspect tcp max-incomplete host 40 block-time 0  
ipv6 inspect name v6_fw tcp timeout 300  
ipv6 inspect name v6_fw udp  
ipv6 inspect name v6_fw icmp  
!  
interface FastEthernet0/0  
ipv6 address 3FFE:C15:C002:47::2/64  
ipv6 traffic-filter outside in  
ipv6 inspect v6_fw in  
ipv6 rip v6 enable  
!  
interface FastEthernet0/1  
ipv6 address 3FFE:C15:C002:49::1/64  
ipv6 traffic-filter inside in  
ipv6 inspect v6_fw in  
!  
interface Ethernet1/0  
ipv6 address 3FFE:C15:C002:48::1/64  
ipv6 traffic-filter dmz in
```
ipv6 inspect v6_fw in
no cdp enable
!
ipv6 router rip v6
redistribute connected
!
! Notice that the ACLs in the v6 portion of these ACLs are far more restrictive
! than the filtering done in v4. This is because the test infrastructure used
! in our lab used IPv4 which required additional permit statements. The v6
! filtering shown here is much closer to the filtering you might expect to
! actually put in place on a firewall. The notable exception is the permissive
! ICMP statements which should be locked down and the outbound access possible
! from the DMZ
!
ipv6 access-list dmz
! deny all traffic with a routing header or undetermined
! transport
deny ipv6 any any routing
deny ipv6 any any undetermined-transport
! ICMP filtering
permit icmp any any echo-request
permit icmp any any echo-reply
permit icmp any any packet-too-big
permit icmp any any time-exceeded
permit icmp any any parameter-problem
permit icmp any any nd-na
permit icmp any any nd-ns
deny icmp any any
! Permit SMTP transfer from pipeline to dell2
permit tcp host 3FFE:C15:C002:48::211 host 3FFE:C15:C002:49::228 eq smtp
! deny all other traffic to the internal network
deny ipv6 any 3FFE:C002:49::/64 log
! allow dmz systems to initiate DNS and web requests (in a production network
! this would be much more tightly locked down).
permit tcp 3FFE:C15:C002:48::/64 any eq domain
permit udp 3FFE:C15:C002:48::/64 any eq domain
permit tcp 3FFE:C15:C002:48::/64 any eq www
! deny all other traffic
deny ipv6 any any log
!
ipv6 access-list outside
! deny all traffic with a routing header or undetermined
! transport
deny ipv6 any any routing
deny ipv6 any any undetermined-transport
! permit link local traffic between routers
permit ipv6 FE80::/10 FE80::/10
! permit rip traffic
permit ipv6 FE80::/10 host FF02::9
! ICMP filtering
permit icmp any any echo-request
permit icmp any any echo-reply
permit icmp any any packet-too-big
permit icmp any any time-exceeded
permit icmp any any parameter-problem
permit icmp any any nd-na
permit icmp any any nd-ns
deny icmp any any
! permit any outside device to talk SMTP or DNS to pipeline
permit tcp any host 3FFE:C15:C002:48::211 eq smtp
permit tcp any host 3FFE:C15:C002:48::211 eq domain
permit udp any host 3FFE:C15:C002:48::211 eq domain
! permit any outside device to talk WWW or FTP to surftech
permit tcp any host 3FFE:C15:C002:48::210 eq www
permit tcp any host 3FFE:C15:C002:48::210 eq ftp
! Deny all other traffic
deny ipv6 any any log
!
ipv6 access-list inside
! deny all traffic with a routing header or undetermined transport
! ICMP filtering
permit icmp any any echo-request
permit icmp any any echo-reply
permit icmp any any packet-too-big
permit icmp any any time-exceeded
permit icmp any any parameter-problem
permit icmp any any nd-na
permit icmp any any nd-ns
! Note the addition of the router-solicitation permit since there are user stations on this subnet using address autoconfiguration
permit icmp any any router-solicitation
deny icmp any any
! permit the internal network to query the DMZ servers on the relevant services
permit tcp 3FFE:C15:C002:49::/64 host 3FFE:C15:C002:48::210 eq www
permit tcp 3FFE:C15:C002:49::/64 host 3FFE:C15:C002:48::210 eq ftp
permit tcp 3FFE:C15:C002:49::/64 host 3FFE:C15:C002:48::211 eq smtp
permit tcp 3FFE:C15:C002:49::/64 host 3FFE:C15:C002:48::211 eq domain
permit udp 3FFE:C15:C002:49::/64 host 3FFE:C15:C002:48::211 eq domain
! deny all other traffic to the DMZ
  deny ipv6 any 3FFE:C15:C002:48::/64
! allow outbound DNS and WWW requests to the IPv6 Internet
  permit tcp 3FFE:C15:C002:49::/64 any eq www
  permit tcp 3FFE:C15:C002:49::/64 any eq domain
  permit udp 3FFE:C15:C002:49::/64 any eq domain
! Deny all other traffic
  deny ipv6 any any log
!
end